# Uma Marca d'Água Digital baseada na Transformada do Cosseno sobre Corpos Finitos

Juliano Bandeira Lima e Ricardo M. Campello de Souza

***Resumo*— Este artigo apresenta uma nova técnica de marca d'água digital para imagens em escala de cinza, baseada na transformada do cosseno sobre corpos finitos. O principal atrativo do esquema proposto é que não há necessidade de operações aritméticas de ponto-flutuante, o que proporciona maior simplicidade e precisão na sua implementação. Resultados de simulação dos procedimentos de inserção e extração da marca são apresentados.**

***Palavras-Chave*— Marcas d'água digitais, Transformadas sobre Corpos Finitos.**

***Abstract*— This paper presents a new digital watermarking technique for gray scale images based on the finite field cosine transform. The main advantage of the proposed scheme is that it is free from any floating-point arithmetic operation, which provides more simplicity and accuracy in its implementation. Simulation results of the mark insertion and extraction procedures are presented.**

***Keywords*— Digital Watermarking, Finite Field Transforms.**

## I. INTRODUÇÃO

A partir da última década, o uso e a distribuição de informação multimídia digital cresceram de modo desenfreado. A popularização da rede mundial de computadores permitiu o acesso a imagens e a arquivos de áudio e vídeo, disponibilizados em qualquer parte do planeta. No entanto, a facilidade de comunicação e a de partilha de recursos, proporcionadas pela tecnologia, possuem também aspectos negativos. A liberdade com que se pode copiar e comercializar a mídia digital tem comprometido o direito que os autores possuem sobre suas criações (fotos, desenhos, músicas, entre outras).

Diante disso, tornou-se necessário o desenvolvimento de métodos para proteger e verificar a autenticidade de uma imagem, por exemplo. Surgiu, então, a versão digital do termo "marca d'água". Nesse contexto, marcar significa introduzir informação adicional que identifique o detentor dos direitos autorais sobre um produto. A marca d'água digital precisa ser imperceptível, isto é, inalterar qualquer característica visível da informação original. A marca também deve ser robusta dentro de certos limites, sobrevivendo a ataques maliciosos que tenham o intuito de destruí-la [1].

As marcas d'água para imagens digitais podem ser processadas no domínio espacial ou no da freqüência. No domínio espacial, a marca LSB (*Least Significant Bit*) é uma das mais simples e conhecidas, entretanto, esta técnica limita bastante a quantidade de informação que se pode esconder. Esta marca também é facilmente apagada, caso a imagem sofra compressões com perdas [2]. Neste mesmo domínio, há, ainda, outros métodos baseados na superposição da imagem original e da marca [2].

As técnicas realizadas no domínio da freqüência consistem em aplicar transformadas discretas, como a de Fourier e a do Cosseno, à imagem original [3], [4]. A marca d'água é inserida alterando-se os valores dos coeficientes destas transformadas. Calculando-se a transformada inversa, obtém-se a imagem marcada. Nestes métodos, uma das dificuldades é a implementação eficiente de algoritmos. O cálculo de transformadas reais implica o uso de aritmética de ponto-flutuante e, naturalmente, exige arredondamento, aspectos que se refletem na velocidade do processamento e na precisão.

Em 2004, Aoki *et al* propuseram uma marca d'água frágil para imagens em escala de cinza baseada na transformada de Fourier de corpo finito (TFCF) [5]. O procedimento eliminou os erros de arrendondamento e simplificou os cálculos, realizando-os apenas com aritmética inteira.

Neste trabalho, é apresentada uma marca d'água baseada na transformada do cosseno sobre corpos finitos (TCCF), recentemente introduzida por Souza *et al* [6]. Além de aproveitar a facilidade de cálculo inerente às transformadas inteiras, o esquema sugerido realiza uma espécie de "espalhamento" da marca d'água. O resultado disto é um sistema simples e robusto a diversas manipulações da imagem marcada.

A seção a seguir trata de alguns aspectos teóricos da TCCF e introduz sua definição para o caso bidimensional. Os esquemas de inserção e extração da marca d'água proposta são apresentados na seção III. Na seção IV, os resultados obtidos nas simulações são exibidos e analisados. A seção V contém as principais conclusões deste artigo e sugestões para trabalhos futuros.

## II. A TRANSFORMADA DO COSSENO SOBRE CORPOS FINITOS

### A. Preliminares Matemáticos

Antes de introduzir a TCCF, é necessário apresentar alguns conceitos básicos [6].

*Definição 1:* O conjunto de inteiros gaussianos sobre GF$(p)$ é o conjunto GI$(p) = \{a + jb, a, b \in \text{GF}(p)\}$, onde $p$ é um primo tal que $j^2 = -1$ não é um resíduo quadrático de $p$. Esta condição é satisfeita apenas por primos $p \equiv 3(mod\ 4)$ [7].

O corpo de extensão GF$(p^2)$ é isomórfico à estrutura "complexa" GI$(p)$ [8]. A partir da definição acima, os

Juliano Bandeira Lima e Ricardo M. Campello de Souza¸ Departamento de Eletrônica e Sistemas, Grupo de Processamento de Sinais, Centro de Tecnologia e Geociências, Universidade Federal de Pernambuco, Recife, Brasil, E-mails: juliano_bandeira@hotmail.com, ricardo@ufpe.br.

elementos de GF($p^2$) podem ser representados na forma $a + jb$.

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

*Definição 3 (funções k-trigonométricas):* Seja $\zeta$ um elemento de ordem $N$, não-nulo, de GI($p$), onde $p \equiv 3(mod\ 4)$. As funções k-trigonométricas cosseno e seno de $\angle(\zeta^i)$ (arco do elemento $\zeta^i$) sobre GI($p$), são $\cos_k\angle(\zeta^i) := (2^{-1}\text{mod } p)(\zeta^{ik} + \zeta^{-ik})$ e $\text{sen}_k\angle(\zeta^i) := (2^{-1}\text{mod } p)(\zeta^{ik} - \zeta^{-ik})/j,\ i, k = 0, 1, \ldots, N-1$.

As funções k-trigonométricas são denotadas simplesmente por $\cos_k(i)$ e $\text{sen}_k(i)$.

Sobre o corpo dos números reais, a transformada discreta do cosseno (DCT) é definida pelo par

$$\begin{aligned} C[k] &:= \sum_{n=0}^{N-1} x[n]\cos\left[\tfrac{(2n+1)k\pi}{2N}\right] \\ x[n] &= \sum_{k=0}^{N-1} \beta[k]C[k]\cos\left[\tfrac{(2n+1)k\pi}{2N}\right], \end{aligned} \quad (1)$$

onde $\beta[k] = \begin{cases} \frac{1}{2}, & \text{se } k = 0 \\ 1, & \text{se } k \neq 0. \end{cases}$

Essa é a chamada DCT tipo II.

### *B. A Transformada Discreta do Cosseno de Corpo Finito*

Seja $f = (f_i)$ um vetor de comprimento $N$ sobre GF($p$). Para definir sua DCT usando k-cossenos, é necessário utilizar o lema que se segue.

*Lema 1 (lema do k-cos):* Se $\zeta \in$ GI($p$) tem ordem multiplicativa $2N$, então

$$A = \sum_{k=1}^{N-1} \cos_k(i) = \begin{cases} N-1, & \text{se } i = 0 \\ -1, & \text{se } i \text{ for par } (\neq 0) \\ 0, & \text{se } i \text{ for ímpar.} \end{cases} \quad (2)$$

*Demonstração:* Vide [6]. ■

A partir desse lema, pode-se definir a TCCF [6].

*Definição 4:* A transformada discreta do cosseno de corpo finito da seqüência $f = (f_i)$, $i = 0, 1, \ldots, N-1$, $f_i \in$ GF($p$), é a seqüência $C = (C_k)$, $k = 0, 1, \ldots, N-1$, $C_k \in$ GI($p$), de elementos

$$C_k := \sum_{i=0}^{N-1} 2 f_i \cos_k\left(\frac{2i+1}{2}\right), \quad (3)$$

onde $\zeta \in$GI($p$) tem ordem multiplicativa $2N$.

A TCCF inversa é dada pelo seguinte teorema.

*Teorema 1 (A fórmula de inversão):* A TCCF inversa da seqüência $C = (C_k)$, $k = 0, 1, \ldots, N-1$, $C_k \in$ GI($p$), é a seqüência $f = (f_i)$, $i = 0, 1, \ldots, N-1$, $f_i \in$ GF($p$), onde

$$f_i = \frac{1}{N} \sum_{k=0}^{N-1} \beta_k C_k \cos_k\left(\frac{2i+1}{2}\right) \quad (4)$$

e $\beta_k = \begin{cases} (2^{-1}\text{mod } p), & \text{se } k = 0 \\ 1, & \text{se } k \neq 0. \end{cases}$

*Demonstração:* Vide [6]. ■

Para a aplicação proposta neste trabalho, é necessário que se introduza a versão bidimensional da TCCF. Uma generalização das expressões 3 e 4 leva à definição do par 2D-TCCF.

*Definição 5 (2D-TCCF):* A transformada discreta do cosseno de corpo finito da matriz $f = (f_{i_1,\, i_2})$, $i_1, i_2 = 0, 1, \ldots, N-1$, $f_{i_1,\, i_2} \in$ GF($p$), é a matriz $C = (C_{k_1,\, k_2})$, $k_1, k_2 = 0, 1, \ldots, N-1$, $C_{k_1,\, k_2} \in$ GI($p$), de elementos

$$C_{k_1,\, k_2} := \sum_{i_1=0}^{N-1} \sum_{i_2=0}^{N-1} f_{i_1,\, i_2} 2\cos_{k_1}\left(\frac{2i_1+1}{2}\right) 2\cos_{k_2}\left(\frac{2i_2+1}{2}\right). \quad (5)$$

onde $\zeta_1, \zeta_2 \in$ GI($p$) tem ordem multiplicativa $2N$

*Teorema 2:* A 2D-TCCF inversa da matriz $C = (C_{k_1,\, k_2})$, $k_1, k_2 = 0, 1, \ldots, N-1$, $C_{k_1,\, k_2} \in$ GI($p$) é a matriz $f = (f_{i_1,\, i_2})$, $i_1, i_2 = 0, 1, \ldots, N-1$, $f_{i_1,\, i_2} \in$ GF($p$), onde

$$f_{i_1,\, i_2} = \frac{1}{N^2} \sum_{k_1=0}^{N-1} \sum_{k_2=0}^{N-1} C_{k_1,\, k_2}\, \beta_{k_1} \cos_{k_1}\left(\frac{2i_1+1}{2}\right) \beta_{k_2} \cos_{k_2}\left(\frac{2i_2+1}{2}\right)$$

e $\beta_{k_1}, \beta_{k_2} = \begin{cases} (2^{-1}\text{mod } p), & \text{se } k = 0 \\ 1, & \text{se } k \neq 0. \end{cases}$

*Demonstração:* Vide [6]. ■

É importante dizer que, selecionando-se um elemento $\zeta$ unimodular, garante-se que as funções k-trigonométricas assumam apenas valores pertencentes a GF($p$), ou seja, a transformada será real [6]. Outro aspecto relevante é que, na definição da 2D-TCCF, as duas dimensões possuem o mesmo comprimento. Isto significa que a transformada de uma matriz $N \times N$ (ou de uma imagem quadrada) é obtida usando a mesma estrutura que calcula a transformada de uma seqüência de comprimento $N$.

## III. A MARCA D'ÁGUA PROPOSTA

A técnica que este trabalho propõe possui esquemas de inserção e extração da marca d'água similares àqueles que empregam transformadas reais. Inicialmente, tem-se uma imagem digital em escala de cinza, onde cada pixel assume valores de 0 a 255. Nela, será introduzida como marca uma outra imagem em preto-e-branco (pixels com valores 0 ou 1).

### *A. O esquema de inserção da marca*

O procedimento consiste em calcular a 2D-TCCF da imagem original reduzida módulo $p$ ($I_p$) e, neste domínio, inserir a marca. De fato, a informação a ser incorporada corresponde a uma seqüência pseudo-aleatória (PN), em que cada trecho de $L$ bits é invertido segundo o valor de um bit da marca d'água. Esta operação, que é denotada por $*$, é representada na figura 1.

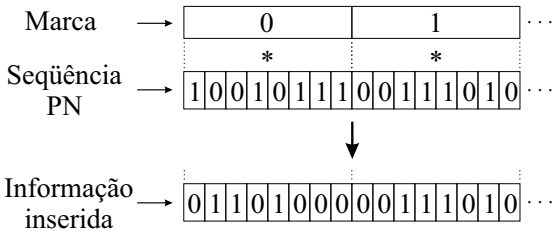


Fig. 1. Informação a ser incorporada à imagem original ($L = 8$ bits).

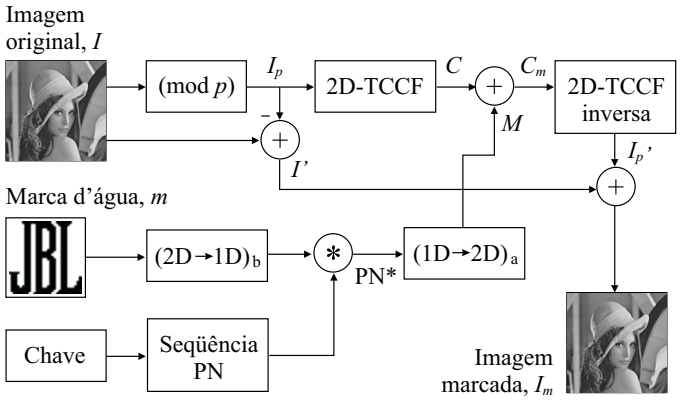


Fig. 2. Esquema de inserção da marca d'água baseada na TCCF.

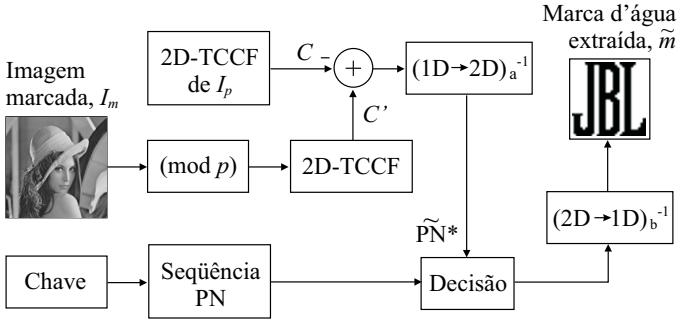


Fig. 3. Esquema de extração da marca d'água baseada na TCCF.

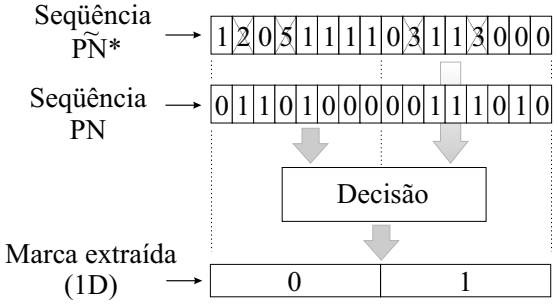


Fig. 4. Funcionamento do bloco "Decisão" na extração da marca d'água ($L = 8$ bits.)

A figura 2 detalha o esquema de inserção da marca d'água. A chave, definida por quem assina a imagem, é a semente que origina a seqüência PN. A seqüência PN* que, mapeada em duas dimensões, possui o mesmo tamanho da imagem original, é somada a $C$. O procedimento é finalizado calculando-se a transformada inversa e readicionando $I' = I - I_p$.

Para que esta marca atenda de modo satisfatório o requisito da "invisibilidade", é importante escolher adequadamente o valor de $p$. Na figura 2, somar $M$ a $C$ significa alterar determinados coeficientes da 2D-TCCF. Entretanto, para uma transformada num corpo finito, adicionar apenas uma unidade a um elemento no domínio da freqüência pode modificar em até $(p-1)$ unidades os elementos de sua transformada inversa. Portanto, para que o valor de cada pixel da imagem original seja alterado o menos possível, deve-se escolher um número $p$ pequeno.

Com base nestas implicações, fixou-se $p = 7$ para a implementação das simulações que serão apresentadas. Atrelados ao valor de $p$ estão o tamanho da transformada, $2 \times 2$, o elemento unimodular $\zeta = 2 + j2$, cuja ordem é $8$, e o corpo de extensão GI$(7)$.

### *B. O esquema de extração da marca*

Para que a marca d'água proposta seja extraída, é necessário conhecer a semente que gera a seqüência PN utilizada em sua inserção, bem como a 2D-TCCF da imagem original reduzida módulo $p$. A figura 3 apresenta o esquema que realiza este procedimento.

Inicialmente, calcula-se a diferença $(C' - C)$ entre a 2D-TCCF da imagem marcada e da imagem original, ambas reduzidas módulo $p$. A matriz resultante desta operação é mapeada numa seqüência PÑ* de comprimento igual ao da seqüência PN. O bloco "Decisão" compara estas duas seqüências e, para cada $L$ pares de bits comparados, observa o número de coincidências e o de inversões. Se o número de coincidências predominar, decide-se pelo bit 1. Em caso contrário, decide-se pelo bit 0 (figura 4). A composição da marca é finalizada ao se realizar o mapeamento bidimensional desta nova seqüência obtida.

A operação representada na figura 1, que pode ser vista como uma espécie de espalhamento da marca, tem a função de tornar mais seguro o procedimento de extração. Se a imagem marcada tiver sofrido alguma alteração, certamente, a seqüência PÑ* conterá valores diferentes de $0$ e $1$. Tais valores são tratados como indeterminados, neutros no processo de decisão de cada bit que compõe a marca. Assim, quanto maior o valor de $L$, maior será o número de bits válidos para uma extração correta.

É importante ressaltar ainda que os mapeamentos dimensionais realizados na extração da marca correspondem ao inverso dos mapeamentos utilizados na inserção da mesma. Qualquer erro na ordenação das informações que compõem esses esquemas comprometeria o método por completo.

## IV. Simulações e Resultados

Um dos maiores interesses das técnicas de proteção de informação digital é garantir que suas marcas não serão apagadas, caso a imagem sofra manipulações. Com o objetivo de

analisar o comportamento do método proposto neste aspecto, os esquemas de inserção e extração da marca d'água foram implementados no $Matlab$©. Os resultados das simulações realizadas são apresentados a seguir.

Originalmente, considerou-se uma imagem em escala de cinza, de tamanho $128 \times 128$, livre de qualquer marca d'água e que não tenha sofrido compressão (lenna.bmp). O passo seguinte foi realizar a inserção de uma marca representada por uma imagem em preto-e-branco, de tamanho $32 \times 32$. Na figura 5, são apresentadas estas duas imagens e uma terceira, obtida ao final do procedimento descrito.

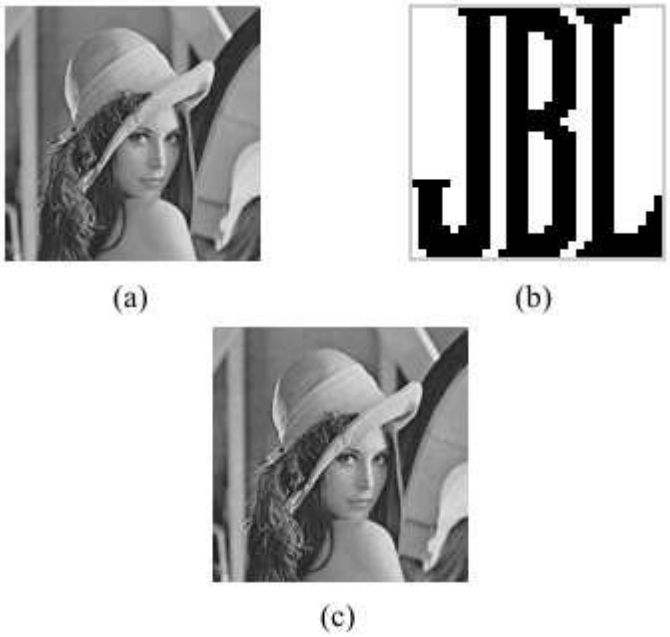


Fig. 5. (a) Imagem original, $128 \times 128$ (lena.bmp). (b) Marca d'água, $32 \times 32$. (c) Imagem marcada. PSNR $= 38,9808$ dB.

Com o objetivo de medir o quanto a inserção da marca d'água modifica a imagem original, calculou-se a relação sinal-ruído de pico (PSNR). Para a imagem em questão, obteve-se PSNR $= 38,9808$dB, valor cujo significado visual pode-se observar na figura 5.

A próxima etapa da simulação foi realizar a recuperação da marca d'água a partir da imagem apresentada na figura 5.c. Como se tem enfatizado, a técnica proposta neste artigo emprega uma ferramenta matemática baseada em aritmética inteira. Por conta disto, os procedimentos de inserção e de extração (figuras 2 e 3) são precisos, proporcionando a recuperação de uma marca idêntica à que foi inserida (desde que a imagem não tenha sofrido alterações).

Finalmente, foram modificadas determinadas características da imagem marcada com o objetivo de analisar o reflexo de tais manipulações sobre a marca extraída. A medida do quanto a marca d'água foi corrompida é dada pela correlação normalizada (CN) entre a marca recuperada e a marca inserida [9]. Este parâmetro é calculado pela equação:

$$\mathrm{CN} = \frac{\sum_i \sum_j w(i,j)\tilde{w}(i,j)}{\sum_i \sum_j [w(i,j)]^2}, \qquad (6)$$

onde $w$ representa a marca inserida e $\tilde{w}$ a marca recuperada. Quanto mais próximo de 1 for o valor de CN, maior similaridade haverá entre as duas marcas.


Fig. 6. (a) Imagem marcada com brilho acentuado em 30%. (b) Marca d'água recuperada. CN $= 0,9796$.

A figura 6. a corresponde à imagem marcada com brilho acentuado em 30%. Este tipo de alteração equivale a somar ao valor de cada pixel uma constante inteira. Na TCCF $2 \times 2$ ($p = 7$), o efeito desta manipulação é neutro. Deste modo, é possível recuperar a marca com bastante clareza (figura 6. b), havendo erro apenas devido ao *overflow* (pixels que excederam 255). Para este caso, obteve-se CN$= 0,9796$.


Fig. 7. (a) Imagem marcada com 25% de sua informação destruída. (b) Marca d'água recuperada. CN $= 0,8662$.

Na figura 7. a, é apresentada a imagem marcada com uma região completamente destruída. Na parte inferior da marca recuperada (figura 7. b), observa-se que linhas alternadas foram corrompidas. Essa característica é reflexo do modo como a marca foi espalhada e dos mapeamentos dimensionais utilizados no procedimento de inserção. Ainda assim, com CN$= 0,8662$, consegue-se identificar claramente a presença da marca original.

Apresenta-se na figura 8 as marcas recuperadas ao se realizar outras duas manipulações na imagem. A figura 8. a corresponde à marca extraída quando se comprime, segundo o padrão JPEG, a imagem original em 30% do seu tamanho (CN$= 0,6747$). Ao se incrementar em 10% o contraste da imagem marcada, extrai-se com similaridade CN$= 0,7175$ a marca apresentada na figura 8. b.

A partir dos resultados apresentados nas figuras 6, 7 e 8, pode-se analisar alguns aspectos do método proposto. A técnica baseada na transformada do cosseno sobre corpos finitos é pouco sensível a manipulações que alteram a imagem


Fig. 8. (a) Marca recuperada ao se comprimir, segundo o padrão JPEG, o arquivo original em 30% do seu tamanho, CN$= 0,6747$. (b) Marca recuperada ao se incrementar em 10% o contraste da imagem marcada, CN$= 0,7175$.

marcada de modo uniforme (brilho) ou esparso (destruição total de determinadas regiões, baixos níveis de compressão). Como a TCCF implementada possui tamanho $2 \times 2$, é importante que o maior número possível destes blocos "sobreviva" a alterações.

Imaginando que cada manipulação sofrida pela imagem marcada possa ser modelada como a adição de um ruído (matriz com o mesmo tamanho da imagem), observa-se que a marca d'água sugerida é mais robusta quando a variância deste ruído é pequena. Para que a marca não seja corrompida, quanto maior a variância, menos denso deve ser o ruido, isto é, um menor número de pixels da imagem marcada deve ser alterado.

## V. Conclusões

Neste artigo, foi apresentada uma técnica de marca d'água para imagens digitais baseada na transformada do cosseno sobre corpos finitos. Definiu-se uma versão bidimensional desta transformada, adequando-a ao processamento de imagens. O método proposto, que necessita realizar apenas operações com números inteiros, torna os cálculos mais simples, rápidos e precisos.

Os resultados obtidos permitiram uma caracterização preliminar do método quanto à robustez. A teoria desenvolvida e as simulações realizadas indicam que as transformadas em corpos finitos constituem uma ferramenta a partir da qual técnicas de marca d'água mais refinadas podem ser propostas.

## Referências

[1] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques", *Proceedings of the IEEE*, v. 87, p. 1079-1107, Julho 1999.

[2] N. F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen", *IEEE Computer*, v. 31, p. 26-34, Fevereiro 1998.

[3] M. A. Suhail and M. S. Obaidat, "Digital Watermarking-Based DCT and JPEG Model", *IEEE Trans. on Instrumentation and Measurement*, v. 52, p. 1640-1647, Outubro 2003.

[4] J. J. K. O Ruanaidh, W. J. Dowling and F. M. Boland, "Watermarking Digital Image for Copyright Protection", *IEE Proc. Vis. Image Signal Processing*, v. 143, p. 250-256, Agosto 1996.

[5] H. Tamori, N. Aoki and T. Yamamoto, "A Fragile Digital Watermarking Technique by Number Theoretic Transform", *IEICE Trans. Fundamentals*, v. E85, p. 1902-1904, Agosto 2002.

[6] M. M. C. de Souza, H. M. de Oliveira, R. M. C. de Souza and M. M. Vasconcelos, "The Discrete Cosine Transform over Prime Finite Fields", *Lecture Notes in Computer Science, LNCS 3124*, p. 482-487, Springer-Verlag, 2004.

[7] D. M. Burton, *Elementary Number Theory*. McGraw Hill, New York, 4ª Ed., 1998.

[8] R. E. Blahut, *Fast Algorithms for Digital Signal Processing*. Addison-Wesley Reading, 1985.

[9] W. Luo, G. L. Heileman and C. E. Pizano, "Fast and Robust Watermarking of JPEG Files", *Proc. of the Fifth IEEE Southwest Symposium on Image Analysis and Interpretation*, p. 158-162, Santa Fe, New Mexico, 2002.