Proceeding Series of the Brazilian Society of Applied and Computational Mathematics, Vol. 2, N. 1, 2014.
Trabalho apresentado no CMAC-Sul, Curitiba-PR, 2014.

Algoritmos Rápidos para Cifragem de Imagens Utilizando Aproximações da DCT de Comprimento 8*

Thiago L. T. da Silveira†
Universidade Federal de Santa Maria
Depto de Eletrônica e Computação e LACESM
E-mail: thiago@inf.ufsm.br

Fábio M. Bayer
Universidade Federal de Santa Maria
Depto de Estatística e LACESM
E-mail: bayer@ufsm.br

Renato J. Cintra
Universidade Federal de Pernambuco
Grupo de Processamento de Sinais, Depto de Estatística
E-mail: rjdsc@stat.ufpe.org

Alice J. Kozakevicius
Universidade Federal de Santa Maria
Depto de Matemática e LANA
E-mail: alice.kozakevicius@gmail.com

RESUMO

1. Introdução

Criptografia é o estudo de técnicas matemáticas relacionadas a aspectos de segurança da informação, tais como confidencialidade, integridade e autenticidade de dados [4]. Vários processos de cifragem de imagens envolvem transformadas discretas, como a transformada discreta de Fourier [5], a transformada discreta de Hartley (DHT) [2] e, recentemente, a DHT binária (BDHT) [1]. A BDHT é uma aproximação de baixa complexidade computacional para a DHT e sua utilização em cifragem de imagens torna o método rápido e eficiente.

Seguindo o método de codificação de dupla fase aleatória introduzido por [5] e suportada por [1], este trabalho propõem uma investigação de alternativas rápidas e eficientes para cifragem de imagens com três contribuições distintas: (i) utilização da transformada discreta do cosseno (DCT) no algoritmo de cifragem; (ii) utilização de aproximações da DCT de complexidade multiplicativa nula; e (iii) consideração de decomposição da imagem original em sub-blocos, assim como em algoritmos de compressão de imagens, como JPEG. Os pontos (ii) e (iii) são objetivados com o intuito de reduzir o custo computacional envolvido no procedimento de cifragem, propondo algoritmos rápidos e eficientes para aplicações em tempo real.

2. Metodologia

Os métodos de cifragem e decifragem de imagens propostos em [1] podem ser descritos, respectivamente, por

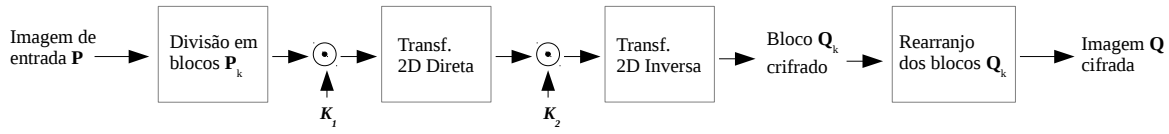
$$\mathbf{Q} = \mathbf{T}_N^\top \cdot \left(\left(\mathbf{T}_N \cdot (\mathbf{P} \odot \mathbf{K}_1) \cdot \mathbf{T}_N^\top \right) \odot \mathbf{K}_2 \right) \cdot \mathbf{T}_N, \tag{1}$$

$$\mathbf{R} = \left(\mathbf{T}_N^\top \cdot \left(\left(\mathbf{T}_N \cdot \mathbf{Q} \cdot \mathbf{T}_N^\top \right) \oslash \mathbf{K'}_2 \right) \cdot \mathbf{T}_N \right) \oslash \mathbf{K'}_1, \tag{2}$$

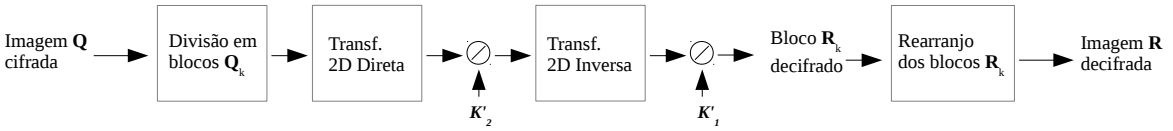
em que $\mathbf{T}_N$ é a matriz $N \times N$ da BDHT, $\mathbf{P}$ é a imagem original de tamanho $N \times N$, $\mathbf{Q}$ é a imagem cifrada, $\mathbf{R}$ é a imagem decifrada, $\mathbf{K}_1$, $\mathbf{K'}_1$, $\mathbf{K}_2$ e $\mathbf{K'}_2$ são matrizes $N \times N$ aleatórias chamadas de chave, $\odot$ é a operação de multiplicação elemento-a-elemento e $\oslash$ é a operação de divisão elemento-a-elemento. Se $\mathbf{K'}_1$ e $\mathbf{K'}_2$ forem iguais, respectivamente, a $\mathbf{K}_1$ e $\mathbf{K}_2$ então a imagem $\mathbf{R}$ será igual a imagem original $\mathbf{P}$.

*Este trabalho foi parcialmente financiado por CNPq, FACEPE e FIT/UFSM.
†Bolsista de Iniciação Tecnológica FIT/UFSM.

Propomos a substituição da BDHT bidimensional (2D) por outras transformadas 2D como a DCT, a DCT binária (BDCT) [1] e a clássica transformada de Walsh-Hadamard (WHT). Além disso, sugerimos o procedimento de divisão da imagem original em sub-blocos de tamanho $k \times k$, para $k = 8, 16, 32, 64$. Em contraste, em [1], são utilizadas transformadas com mesmas dimensões das imagens. A Figura 1 esquematiza graficamente o método de cifragem considerado.



(a) Cifragem



(b) Decifragem

Figura 1: Esquema de cifragem e decifragem de imagens.

3. Resultados e discussões

Uma vantagem direta da aplicação do método de sub-divisão da imagem original para o processo de cifragem é a redução do custo computacional. O custo computacional é avaliado pela complexidade aritmética que é dada pelo número de multiplicações e adições exigidas pela aplicação deste método. Algoritmos rápidos para transformadas discretas são comumente comparados em termos de sua complexidade aritmética, como figura de mérito para eficiência. A Tabela 1 apresenta as complexidades aritméticas associadas aos algoritmos de cifragem considerados. As complexidades da DCT exata de comprimento k, DCT_k, são determinadas por meio do algoritmo de Chen [3] e as imagens utilizadas em nosso experimentos são imagens 512×512 em escala de cinza de 8 bits.

Tabela 1: Comparação da complexidade aritmética dos algoritmos considerados

Transformada considerada	Número de sub-blocos	Complexidade de cada sub-bloco			Complexidade total		
		Mult.	Adições	Total	Mult.	Adições	Total
DCT_{512}	1	3936256	6293504	10229760	3936256	6293504	10229760
DCT_{64}	64	37376	61696	99072	2392064	3948544	6340608
DCT_{32}	256	7424	12416	19840	1900544	3178496	5079040
DCT_{16}	1024	1408	2368	3776	1441792	2424832	3866624
DCT_{8}	4096	256	416	672	1048576	1703936	2752512
WHT_{8}	4096	0	384	384	0	1572864	1572864
BDCT_{8}	4096	0	384	384	0	1572864	1572864

Os resultados da Tabela 1 evidenciam que quanto menor o tamanho do bloco, menor é a complexidade aritmética do algoritmo de cifragem associado. Os resultados do experimento computacional para comparação dos desempenhos dos procedimentos de cifragem considerando a DCT com diferentes tamanhos de sub-blocos são apresentados na Figura 2. Essa figura apresenta o índice de similaridade estrutural (MSSIM) [6] entre as imagens decifradas e a imagem original. A medida MSSIM varia no intervalo $[0, 1]$ e considera características do sistema visual humano diferentemente das medidas usuais, tais como a relação sinal-ruído de pico e o erro quadrático médio [6]. Para essa aplicação, os (i, j)-ésimos elementos de $\mathbf{K}'_1$ e $\mathbf{K}'_2$ foram definidos como $[\mathbf{K}'_1]_{i,j} = [\mathbf{K}_1]_{i,j} + \delta$ e $[\mathbf{K}'_2]_{i,j} = [\mathbf{K}_2]_{i,j} + \delta$, em que os elementos $[\mathbf{K}_1]_{i,j}$ e $[\mathbf{K}_2]_{i,j}$ são independentes e uniformemente distribuídos em $[-0.001; 0.001]$ e $-0.001 \leq \delta \leq 0.001$. Para $k = 8$, o gráfico com os valores de MSSIM decai mais rapidamente à medida que δ se afasta de zero, indicando que são necessárias chaves $\mathbf{K}'_1$ e $\mathbf{K}'_2$ com valores mais próximos de $\mathbf{K}_1$ e $\mathbf{K}_2$, respectivamente, para a boa reconstrução da imagem original. Ou seja, a abordagem em sub-blocos, além de fornecer menor custo, também mostra-se como uma opção mais segura para cifragem de imagens.

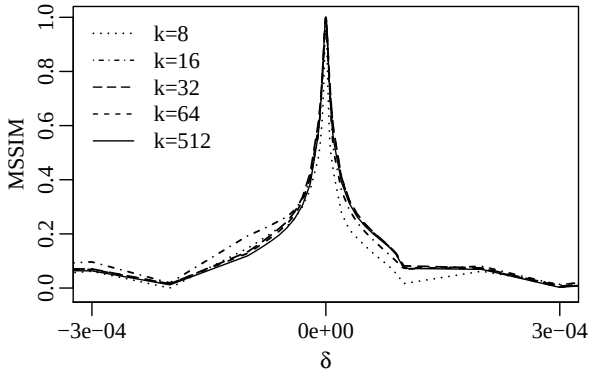


Figura 2: MSSIM das imagens decifradas utilizando a DCT_k, com $k = 8, 16, 31, 64$ e 512.

Com base nos resultados anteriores, destacando o bom desempenho da utilização de $k = 8$, optou-se por utilizar aproximações da DCT de complexidade multiplicativa nula, conforme Tabela 1, nomeadamente a WHT e a BDCT, como substituição da DCT de comprimento 8. A Figura 3 ilustra qualitativamente os resultados da cifragem por meio de alguns dos algoritmos rápidos considerados.

(a) WHT_8 (b) WHT_8 (c) WHT_8 (d) BDCT_8 (e) BDCT_8 (f) BDCT_8

Figura 3: Resultados da cifragem na imagem Elaine utilizando WHT_8 (a,b,c) e BDCT_8 (c,d,e): (a) cifrada, (b) decifrada com $\delta = 0.001$, (c) decifrada com chaves corretas ($\delta = 0$), (d) cifrada, (e) decifrada com $\delta = 0.001$, (f) decifrada com chaves corretas ($\delta = 0$).

O procedimento de sub-divisão da imagem original para utilização de transformadas de menores comprimentos é bastante promissor. A utilização de transformadas aproximadas para a DCT de comprimento 8 resulta em algoritmos rápidos e úteis para aplicações em tempo real, ao mesmo tempo que mantém a segurança da imagem cifrada. Em trabalho futuro, serão investigadas transformadas discretas específicas para cifragem e a utilização de transformadas de baixa complexidade computacional de outros comprimentos.

Palavras-chave: *Cifragem de imagens, DCT aproximada, Processamento de imagens*

Referências

[1] S. Bouguezel, M. Ahmad, and M. Swamy, *Binary discrete cosine and Hartley transforms*, IEEE Transactions on Circuits and Systems I: Regular Papers, 60 (2013), pp. 989–1002.

[2] L. Chen and D. Zhao, *Optical image encryption with Hartley transforms*, Optics Letters, 31 (2006), pp. 3438–3440.

[3] W. H. Chen, C. Smith, and S. Fralick, *A fast computational algorithm for the discrete cosine transform*, IEEE Transactions on Communications, 25 (1977), pp. 1004–1009.

[4] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 5 ed., 2001.

[5] S.-C. Pei and W.-L. Hsue, *The multiple-parameter discrete fractional Fourier transform*, IEEE Signal Processing Letters, 13 (2006), pp. 329–332.

[6] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, *Image quality assessment: from error visibility to structural similarity*, IEEE Transactions Image Processing, 13 (2004), pp. 600–612.

