

Códigos Reed-Solomon Aplicados a Sistemas de Marca D'Água Digital no Domínio da Frequência

Maxwell V. da Silva^{1,2}, Daniel C. Cunha^{1,3} e Juliano B. Lima^{1,4,5}

Resumo— Este trabalho realiza uma avaliação, por meio de simulações computacionais, de sistemas codificados de marca d'água no domínio da transformada wavelet discreta (DWT, *discrete wavelet transform*). A robustez do sistema é analisada em termos do comprimento dos códigos Reed-Solomon (RS) e dos algoritmos de decodificação utilizados. Dois cenários são investigados: transmissão da imagem marcada por um canal com ruído AWGN (*additive white Gaussian noise*) e compressão JPEG (*joint photographic expert group*) da imagem marcada. Os resultados indicam que, dependendo do cenário investigado, o comprimento do código e o algoritmo de decodificação atuam de forma distinta no aumento da robustez da marca d'água.

Palavras-Chave— Marca d'água digital, transformada wavelet discreta, códigos Reed-Solomon, decodificação por decisão suave.

Abstract— This paper evaluates, through computer simulations, a coded watermarking system in the discrete wavelet transform (DWT) domain. The robustness of the system is analyzed in terms of the length of Reed-Solomon (RS) codes and the decoding algorithms adopted. Two scenarios are investigated: transmission of the watermarked image by an additive white Gaussian noise (AWGN) channel and joint photographic expert group (JPEG) compression of the watermarked image. The results shows that, depending on the scenario investigated, the length of the code and the decoding algorithm carry on differently to increase the robustness of the watermark.

Keywords— Digital watermarking, discrete wavelet transform, Reed-Solomon codes, soft-decision decoding.

I. INTRODUÇÃO

As marcas d'água digitais têm recebido cada vez mais atenção de pesquisadores interessados em segurança de informação multimídia [1]–[3]. Diante da crescente facilidade para a distribuição de conteúdos como imagem, áudio e vídeo, procedimentos de marcação auxiliam, por exemplo, na detecção de manipulações e de cópias não autorizadas, bem como na identificação do detentor dos direitos sobre os conteúdos mencionados. Um exemplo de aplicação em que tais atributos são relevantes se dá na área da saúde, com o gerenciamento de imagens médicas [4]. Em técnicas de marca d'água voltadas para imagens, normalmente deseja-se

que a marca seja invisível, sob o aspecto visual propriamente dito e sob o aspecto estatístico. Além disso, se o objetivo é reconhecer a presença da marca, ainda que a imagem marcada tenha sofrido alterações maliciosas ou tenha sido corrompida por ruído ao longo de sua transmissão por um canal de comunicação, a técnica de inserção deve atender a certos requisitos de robustez [5].

Uma das formas de se aumentar a robustez da marca é por meio do uso de códigos corretores de erro. Diversos esforços têm sido desenvolvidos acerca da aplicação de códigos corretores de erro a sistemas de marca d'água digital [6]–[10]. Um aspecto considerado importante é propor esquemas de codificação que proporcionem robustez aos diversos tipos de ataque à imagem marcada, como, por exemplo, a compressão com perdas. Em [8], foi analisado o uso de códigos Bose-Chaudhuri-Hocquenghem (BCH) e de repetição a sistemas de marca d'água, assim como o desempenho de algoritmos de decodificação por decisão suave (SDD, *soft-decision decoding*). Em [9], foi investigada a utilização de códigos Reed-Solomon (RS) no aumento da robustez de imagens marcadas sujeitas a vários tipos de ataque, enquanto que, em [10], uma avaliação similar foi realizada, porém para códigos BCH. Em ambos os trabalhos ([9] e [10]), nada foi abordado quanto aos algoritmos de decodificação empregados.

Este trabalho realiza uma avaliação, por meio de simulações computacionais, de sistemas codificados de marca d'água no domínio da transformada wavelet discreta (DWT, *discrete wavelet transform*). Os códigos corretores de erro considerados são códigos RS de diversos comprimentos. A robustez do sistema é avaliada não apenas quanto ao comprimento dos códigos RS, mas também quanto ao algoritmo de decodificação utilizado. Dois cenários são investigados, quais sejam, a transmissão da imagem marcada por um canal com ruído aditivo Gaussiano branco (AWGN, *additive white Gaussian noise*) e a compressão JPEG (*joint photographic expert group*) da imagem marcada. Na Seção II, conceitos relativos aos códigos RS e ao algoritmo de Chase são apresentados. O sistema codificado de inserção/extração da marca é descrito na Seção III. Na Seção IV, resultados de simulação são apresentados. Por fim, a seção V apresenta as conclusões do trabalho.

II. CÓDIGOS REED-SOLOMON E DECODIFICAÇÃO BASEADA EM CONFIABILIDADE

Neste trabalho, assume-se a utilização de códigos RS, que são códigos BCH não-binários que possuem a propriedade de

1 Pós-Graduação em Engenharia de Sistemas (PPGES), UPE, Recife-PE, Brasil.

2 Núcleo de Tecnologia da Informação (NTI), UFPE, Recife-PE, Brasil.

3 Centro de Informática (CIn), UFPE, Recife-PE, Brasil.

4 Depto. de Matemática, CCEN-UFPE, Recife-PE, Brasil.

5 Pós-Graduação em Engenharia Elétrica (PPGEE), UFPE, Recife-PE, Brasil.

E-mails: maxwell.volnei@ufpe.br, dcunha@cin.ufpe.br e juliano@dmate.ufpe.br. Este trabalho foi parcialmente financiado pela FACEPE (IBPG-0642-3.04/10).

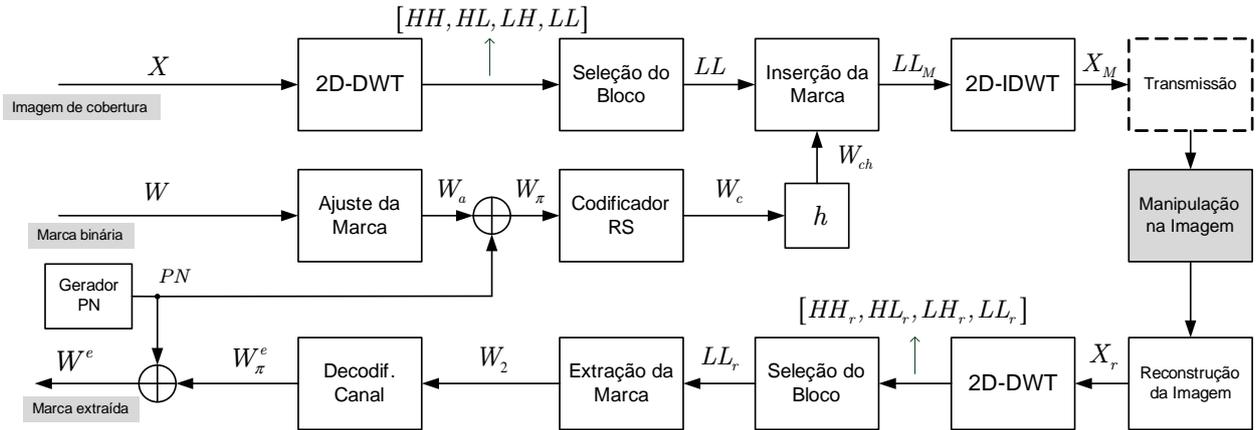


Fig. 1: Diagrama do sistema codificado de inserção/extração de marca d'água digital baseado em DWT.

distância máxima de separação e uma poderosa capacidade de correção de erros em rajada [11]. Dentre as aplicações recentes que empregam códigos RS, pode-se citar comunicações por espalhamento espectral e sistemas de gravação óptica, tais como CDs, DVDs e discos *Blu-ray* [12].

Considere um código de bloco q -ário $C(n, k, d)$, em que n , k e d representam o comprimento da palavra-código, o número de símbolos de informação e a distância mínima do código, respectivamente. Assume-se que $q = 2^m$ e que cada símbolo q -ário, γ_j , é mapeado em um vetor de m bits $\omega_j = \phi(\gamma_j)$, em que $\omega_j = [\omega_{ij}], 1 \leq i \leq m, \omega_{ij} \in \{0, 1\}$. O vetor ω_j é então modulado no vetor σ_j , tal que $\sigma_{ij} = -1$, se $\omega_{ij} = 0$ e $\sigma_{ij} = +1$, se $\omega_{ij} = 1$. O vetor resultante $\mathbf{s} = [\sigma_j], 1 \leq j \leq n$ (correspondente à modulação da palavra-código $\mathbf{w} = [\omega_j], 1 \leq j \leq n$) é então transmitido.

No receptor, a sequência recebida \mathbf{r} é dada por

$$\mathbf{r} = \mathbf{s} + \mathbf{n}, \quad (1)$$

em que $\mathbf{r} = [\rho_j], 1 \leq j \leq n$, tal que $\rho_j = [\rho_{ij}], 1 \leq i \leq m$ e \mathbf{n} é o vetor com amostras de ruído AWGN.

A maioria das aplicações que utiliza códigos de bloco faz uso de uma regra de decodificação incompleta chamada decodificação BDD (*bounded distance decoding*). Esta regra consiste em decodificar todos os padrões de erro de peso menor ou igual à capacidade de correção $t = \lfloor \frac{d-1}{2} \rfloor$ do código, em que $\lfloor \cdot \rfloor$ é o operador piso, i.e., ele determina o menor inteiro mais próximo do valor de seu argumento. Para aumentar o valor de t e, conseqüentemente, melhorar o desempenho do decodificador, é comum a utilização de algoritmos de decodificação SDD. O algoritmo SDD considerado neste trabalho é a variante 2 do algoritmo de decodificação baseada em confiabilidade proposto por Chase [13] e será denotado por algoritmo CH2.

Basicamente, o algoritmo CH2 necessita de dois parâmetros de entrada. O primeiro deles é a sequência binária gerada por decisões abruptas das saídas dos filtros casados. O segundo parâmetro é a própria sequência de valores reais observada na saída do canal, denotada por $\alpha = [\alpha_j], 1 \leq j \leq nm$. Estes valores reais representam o nível de confiabilidade referente a cada bit da palavra recebida. Quanto maior for

o valor de confiabilidade, menor é a probabilidade de o bit correspondente ter sido afetado fortemente pelo ruído.

O algoritmo CH2 consiste em uma seqüência de passos descrita a seguir:

- 1) A partir de \mathbf{r} , obter a seqüência $\mathbf{y} = [\psi_j], 1 \leq j \leq n$, em que $\psi_j = [\psi_{ij}], 1 \leq i \leq m$, tal que $\psi_{ij} \in \{0, 1\}$, gerada pela quantização abrupta de \mathbf{r} .
- 2) Determinar as p posições menos confiáveis de \mathbf{r} e criar um conjunto \mathbf{B} com 2^p padrões de teste \mathbf{b}_l , em que cada padrão \mathbf{b}_l é uma das possíveis seqüências binárias de tamanho nm geradas a partir das combinações de 0's e 1's nas p posições menos confiáveis;
- 3) Criar um conjunto Λ de palavras-código candidatas λ_l , as quais serão obtidas pela decodificação algébrica (no caso, o algoritmo de Berlekamp-Massey (BM) [14]) da seqüência $\mathbf{y}_l = \mathbf{y} \oplus \mathbf{b}_l$, em que $\mathbf{b}_l \in \mathbf{B}$ e \oplus representa a operação de soma módulo-2. A quantidade de palavras-código candidatas, $|\Lambda|$, pode ser menor que 2^p , caso alguma seqüência \mathbf{y}_l não seja decodificada com sucesso pelo algoritmo de decodificação algébrica.
- 4) A palavra decodificada \mathbf{d}_l será a palavra-código candidata λ_l cuja distância Euclidiana quadrática entre as seqüências \mathbf{r} e σ^{λ_l} (versão modulada de λ_l) seja mínima, isto é,

$$\min_l d_E^2(\mathbf{r}, \sigma^{\lambda_l}) = \min_l \sum_{i=1}^{nm} (r_i - \sigma_i^{\lambda_l})^2. \quad (2)$$

Pela descrição apresentada, percebe-se que o algoritmo CH2 possui maior complexidade de decodificação do que o algoritmo BM, uma vez que este último compõe uma das etapas do algoritmo CH2. Desse modo, o desempenho do algoritmo CH2 tende a ser superior ao do algoritmo BM para códigos RS [15].

III. SISTEMA DE MARCA D'ÁGUA CODIFICADO BASEADO EM WAVELET

Em uma imagem digital, uma marca d'água pode ser inserida e extraída no domínio espacial ou no domínio da frequência. A técnica considerada neste trabalho enquadra-se na segunda classe mencionada e emprega a DWT. A DWT

atua em um sinal por meio de filtros, a partir dos quais são obtidas sucessivas sub-bandas com frequências mais baixas e frequências mais altas. Na Fig. 1, apresenta-se um diagrama em blocos do sistema de inserção/extração de marca d'água digital baseado em DWT.

Considere uma imagem de cobertura X , com dimensões 512×512 pixels e 8 bits por pixel (bpp), submetida à DWT bidimensional (2D-DWT) e decomposta em quatro sub-bandas não sobrepostas com dimensões 256×256 pixels; essas sub-bandas são identificadas por LL , HL , LH e HH . A Fig. 2 mostra o resultado deste procedimento aplicado à imagem Lena. Na referida figura, as sub-bandas LL , HL , LH e HH podem ser observadas, respectivamente, de cima para baixo e da esquerda para a direita. Dessa forma, a sub-banda LL está localizada no canto superior esquerdo [2].

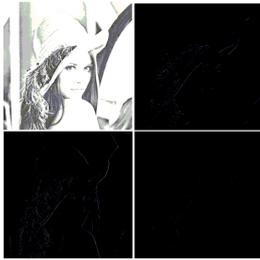


Fig. 2: Resultado da aplicação da 2D-DWT sobre a imagem Lena.

Em seguida, uma imagem binária W , que será usada como marca d'água, é ajustada aos parâmetros (n e k) do código RS antes da codificação. Basicamente, o ajuste mencionado se refere à retirada de bits da marca para que os valores de suas dimensões se tornem múltiplos do número de símbolos de informação do código. Dessa forma, assume-se que T_a é a quantidade de bits da marca ajustada (denotada por W_a) e é dada por

$$T_a = \left\lfloor \frac{RC}{mk} \right\rfloor mk, \quad (3)$$

em que R e C representam, respectivamente, as dimensões horizontal e vertical da marca W . Assim sendo, a marca W_a é composta por $\lfloor RC/mk \rfloor$ vetores, cada um com mk bits.

O passo seguinte consiste em somar uma matriz pseudo-aleatória PN à marca W_a , de modo que uma versão embaralhada $W_\pi = W_a \oplus PN$ seja obtida. A matriz pseudo-aleatória é usada para reforçar a segurança no intuito de impedir que terceiros não autorizados restaurem e, possivelmente, modifiquem a marca d'água. A marca W_π é então aplicada ao codificador RS, originando a marca codificada W_c . Após a codificação, a marca W_c é multiplicada por um fator h , denominado de profundidade da marca, resultando em W_{ch} . A profundidade da marca tem o objetivo de permitir que a marca, ao ser extraída, tenha melhor qualidade.

Das sub-bandas geradas pela 2D-DWT, seleciona-se a sub-banda com as menores frequências (LL) para a inserção da marca. Embora a referida sub-banda seja a mais sensível a degradações que a imagem venha a sofrer, utilizá-la aumenta a robustez da marca para o caso da compressão JPEG [2].

Com isso, a sub-banda LL tem os seus coeficientes somados a W_{ch} , resultando em uma sub-banda modificada, denotada por LL_M . A sub-banda LL_M substitui a sub-banda original na reconstrução da imagem, que é executada por meio da transformada wavelet discreta inversa (IDWT, *inverse discrete wavelet transform*) bidimensional, representada pelo bloco 2D-IDWT. Após essa operação, a imagem marcada X_M é obtida. Utilizando essa estratégia de inserção e $h = 6$, obtém-se um valor de PSNR (*peak signal-to-noise ratio*) próximo a 51 dB entre a imagem original e a marcada, o que é um valor perceptualmente aceitável [3].

Na Fig. 1, o bloco “Manipulação na Imagem” pode significar, por exemplo, a transmissão da imagem por um canal com ruído AWGN ou uma compressão JPEG. Essas interferências resultam em degradações na imagem marcada e, conseqüentemente, na marca d'água a ser extraída. No caso do envio da imagem marcada X_M por um canal ruidoso, é necessário converter os pixels de X_M em bits e, em seguida, mapear os bits nos sinais de uma modulação digital. Neste trabalho, assume-se o uso de modulação binária antipodal, conforme descrição dada na Seção II. Tais operações estão representadas pelo bloco identificado por “Transmissão” na Fig. 1.

A extração da marca é realizada seguindo passos análogos aos empregados na inserção, porém em ordem reversa. É assumido que o sistema de extração necessita da imagem original, ou seja, é um sistema considerado informado [5]. Primeiramente, os sinais ruidosos são demodulados e os bits obtidos são convertidos para pixels no bloco “Reconstrução da Imagem”, gerando a imagem ruidosa X_r . A partir de X_r , são obtidas as sub-bandas LL_r , HL_r , LH_r e HH_r , das quais a sub-banda LL_r é selecionada para que a extração da marca seja efetuada.

A recuperação propriamente dita da marca tem início pela extração da marca codificada W_2 , tal que

$$w_2^i(j) = \frac{LL_r(i,j) - LL_M(i,j)}{h}, \quad (4)$$

em que $w_2^i(j)$ representa o valor de cada componente (pixel) da versão recuperada W_2 da marca codificada e LL_r é a sub-banda da imagem, no domínio da 2D-DWT, em que a marca foi inserida, após as manipulações mencionadas (transmissão por canal ruidoso ou compressão JPEG).

A etapa seguinte na recuperação da marca d'água consiste na decodificação da marca W_2 por meio da utilização de um algoritmo de decodificação de códigos RS. A marca W_2 possui $\lfloor RC/mk \rfloor$ sequências w_2^i de tamanho nm , às quais é aplicado um algoritmo de decodificação (BM ou CH2). No caso de se utilizar o algoritmo CH2, definido na Seção II, a confiabilidade α_j de cada posição de uma sequência w_2^i é dada por $|w_2^i(j)|$. A regra de decisão que determina a sequência binária w_{2b}^i , obtida com base em w_2^i , é dada por

$$\begin{cases} w_{2b}^i(j) = 1, & |w_2^i(j)| > 0,5 \\ w_{2b}^i(j) = 0, & |w_2^i(j)| \leq 0,5 \end{cases} \quad (5)$$

em que $w_{2b}^i(j)$ é a j -ésima componente da i -ésima sequência w_{2b}^i , com $1 \leq j \leq nm$, $1 \leq i \leq \lfloor RC/mk \rfloor$.

Após a decodificação, a marca W_{π}^e , de dimensões $\lfloor RC/mk \rfloor \times mk$, é somada à mesma sequência PN utilizada após o ajuste da marca d'água, com o objetivo de desembaralhar a marca obtida pelo decodificador e gerar a marca extraída W^e .

IV. RESULTADOS DE SIMULAÇÃO

Foram realizadas simulações computacionais de um sistema codificado de marca d'água digital, considerando duas possibilidades para o bloco "Manipulação de Imagem" indicado na Fig. 1. A primeira possibilidade foi a transmissão da imagem marcada por um canal com ruído AWGN, enquanto a segunda possibilidade foi a compressão JPEG da imagem marcada. Em ambos os casos, foram utilizadas inicialmente as imagens Lena (formato BMP) e Boat (formato TIFF) (Figs. 3(a)-3(b)) como imagem de cobertura, todas em escala de cinza, com dimensões 512×512 pixels, 8 bpp e extraídas de [16]. Na Fig. 3(c), é mostrada a imagem (formato TIFF) que foi utilizada como marca d'água, cujas dimensões são 64×64 bits.

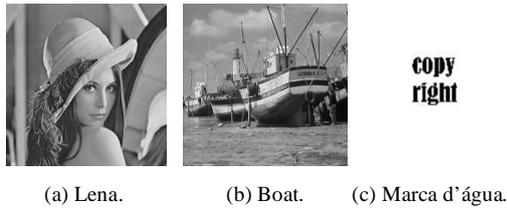


Fig. 3: Imagens usadas nas simulações computacionais.

Para avaliar a robustez da marca extraída, foi adotada a correlação cruzada normalizada (NCC, *normalized cross correlation*) [10]. A NCC determina o grau de similaridade entre a marca ajustada W_a e a versão extraída W_e , sendo definida por

$$NCC = \frac{\sum_{i=1}^R \sum_{j=1}^C w_a^i(j) w_e^i(j)}{\sum_{i=1}^R \sum_{j=1}^C (w_a^i(j))^2}, \quad (6)$$

em que $w_a^i(j)$ e $w_e^i(j)$ representam, respectivamente, as componentes da marca ajustada e da marca extraída. Dessa forma, quanto maior o valor de NCC, maior a semelhança entre as imagens.

A Fig. 4 mostra a NCC entre as marcas W_a e W_e para o cenário da transmissão por um canal com ruído AWGN, sendo Lena a imagem de cobertura utilizada. Foram analisados os códigos RS $C_1(15, 9, 7)$ e $C_2(63, 57, 7)$, assim como os algoritmos de decodificação BM e CH2. Os comprimentos dos códigos RS adotados foram escolhidos no intuito de manter a distância mínima, além de serem típicos da literatura. Para o algoritmo CH2, foi assumido que $p = 4$. No caso do sistema não-codificado, $W_2 \oplus PN$ foi considerada a marca extraída. Para fins de simplificação, o sistema com o código RS $C_1(15, 9, 7)$ e algoritmo BM será denotado como C_1 -BM e os demais sistemas usarão notação similar. A NCC obtida para cada valor de relação sinal-ruído (SNR, *signal-to-noise*

ratio) levou em conta 50 transmissões da imagem Lena pelo canal.

Pode-se observar que, na faixa de SNR considerada (0 a 10 dB) na Fig. 4, todos os sistemas codificados apresentaram maior robustez do que o sistema não codificado. Também é possível verificar que a seleção do melhor sistema depende do valor da SNR de operação. Por exemplo, para SNRs abaixo de 2 dB, os sistemas que utilizam o algoritmo CH2 se mostraram mais robustos (sendo o sistema C_2 -CH2 o melhor deles) do que os sistemas que utilizam o algoritmo BM. Adicionalmente, verifica-se que o aumento da NCC proporcionado pela adoção do algoritmo CH2 foi superior àquele fornecido pelo aumento do comprimento do código. Na faixa de SNR de 2 a 4,6 dB, o sistema C_2 -CH2 permaneceu como a melhor opção, confirmando a expectativa de que o aumento do comprimento do código e a adoção de um algoritmo SDD eleva a robustez do sistema. No entanto, na faixa de SNR de 4,6 a 7 dB, o sistema C_2 -CH2 foi superado pelos sistemas C_1 -BM e C_1 -CH2. Esse fato é relevante, pois mostra que nem sempre a escolha de um código mais longo e do algoritmo de decodificação mais eficiente (CH2, no caso) resulta na maior robustez. Por fim, para SNRs acima de 8 dB, a robustez dos sistemas codificados equivale à do sistema não codificado. Resultados semelhantes foram obtidos para as imagens Baboon, Elaine e Peppers.

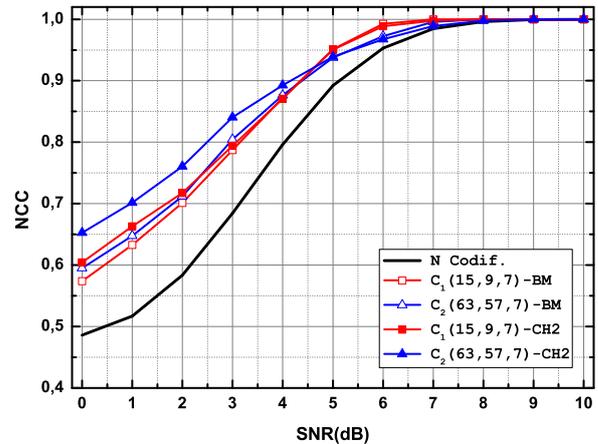


Fig. 4: Correlação cruzada normalizada entre as marcas W_a e W_e em função da relação sinal-ruído de canal para diferentes códigos RS e algoritmos de decodificação (BM e CH2). A imagem de cobertura usada foi Lena.

As Figs. 5 e 6 ilustram a NCC entre as marcas W_a e W_e para o cenário da compressão JPEG, sendo Boat e Lena, respectivamente, as imagens de cobertura utilizadas. Foram analisados os códigos RS $C_1(15, 9, 7)$ e $C_3(127, 121, 7)$, assim como os algoritmos de decodificação BM e CH2. Assim como no cenário da transmissão, foi assumido que $p = 4$ para o algoritmo CH2 e $W_2 \oplus PN$, a marca extraída para o sistema não-codificado. A NCC foi obtida em função do fator de qualidade da compressão JPEG, denotado por $Q(\%)$, o qual variou entre 10% e 100%. O valor $Q = 10\%$ representa a compressão com maior degradação da imagem, enquanto $Q = 100\%$ representa ausência de compressão. Na Fig. 5, observa-se que para a faixa de Q de 10 a 85%, o sistema

C_3 -CH2 apresentou maior robustez. Por outro lado, para a faixa de Q de 54 a 80%, houve sistemas codificados que apresentaram robustez menor do que o sistema não-codificado, quais sejam, C_1 -CH2 e C_1 -BM.

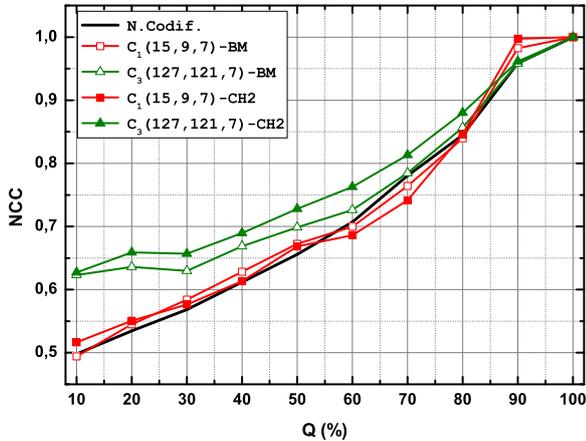


Fig. 5: Correlação cruzada normalizada entre as marcas W_a e W_e em função do fator de qualidade de compressão JPEG para diferentes códigos RS e algoritmos de decodificação (BM e CH2). A imagem de cobertura usada foi Boat.

Na Fig. 6, a maior robustez também foi verificada para o sistema C_3 -CH2, porém para a faixa de Q de 10 a 80% e os sistemas que apresentaram robustez inferior à do sistema não-codificado foram C_1 -CH2 (Q variando de 36 a 75%) e C_1 -BM (Q variando de 46 a 75%). Por fim, ressalta-se que, para as duas imagens verificadas e boa parte dos valores de Q testados, a robustez proporcionada pelo aumento do comprimento do código foi superior àquela obtida com a adoção do algoritmo CH2, diferente do ocorrido para o cenário da transmissão. Assim como no primeiro cenário investigado, resultados semelhantes foram obtidos para as imagens Baboon, Elaine e Peppers.

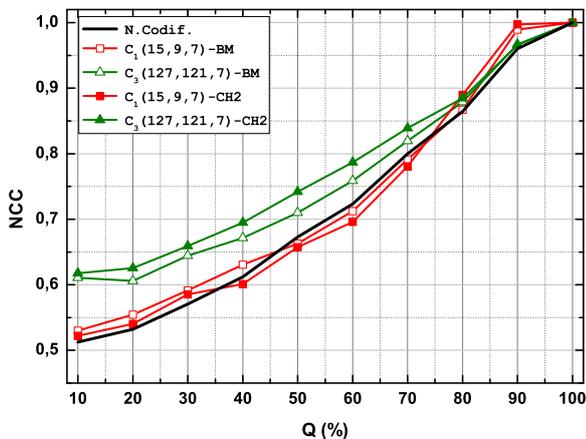


Fig. 6: Correlação cruzada normalizada entre as marcas W_a e W_e em função do fator de qualidade de compressão JPEG para diferentes códigos RS e algoritmos de decodificação (BM e CH2). A imagem de cobertura usada foi Lena.

V. CONCLUSÕES

Este trabalho realizou uma avaliação, por meio de simulações computacionais, da robustez de sistemas codificados de marca d'água no domínio da DWT em cenários de transmissão por um canal ruidoso e compressão JPEG. A robustez foi avaliada em termos do comprimento dos códigos e dos algoritmos de decodificação utilizados. Foram considerados os códigos RS e os algoritmos de decodificação BM e CH2. Para a transmissão por canal ruidoso, os resultados indicaram que o uso de códigos RS nos sistemas de marca d'água eleva a robustez do sistema. Além disso, a adoção do algoritmo CH2 proporciona bons resultados para regiões de baixa SNR. No caso da compressão JPEG, foi verificado que o aumento da robustez da marca d'água com a utilização de esquemas de codificação e controle de erros depende mais do comprimento do código do que do algoritmo de decodificação utilizado.

AGRADECIMENTOS

Este trabalho foi parcialmente financiado pela FACEPE.

REFERÊNCIAS

- [1] A. V. Subramanyam et. al., "Robust watermarking of compressed and encrypted JPEG2000 images," *IEEE Trans. Multimedia*, vol. 14, n. 3, Part 2, pp. 703-716, 2012.
- [2] S. K. Amirgholipour and A. R. Naghsh-Nilchi, "Robust digital image watermarking based on joint DWT-DCT," *Int. Journal of Digital Content Technology and Its Applications*, vol. 3, n. 2, pp. 42-54, 2009.
- [3] J. P. Yeh et. al., "Watermarking technique based on DWT associated with embedding rule," *Int. Journal of Circuits, Systems and Signal Process.*, vol. 4, n. 2, pp. 72-82, 2010.
- [4] A. Giakoumaki et. al., "Multiple digital watermarking applied to medical imaging," In: *Proc. of the IEEE 27th Annual Int. Conf. of the Engineering in Medicine and Biology Society (EMBS 2005)*, pp. 3444-3447, Shanghai, CN, 2005.
- [5] I. Cox et. al. *Digital Watermarking and Steganography*. 2nd ed., Morgan Kaufmann, 2007.
- [6] Y. Chen and J. Chen, "Digital image watermarking based on mixed error correcting code," *J. Inf. Security*, vol. 2012, n. 3, pp. 156-161, 2012.
- [7] W. Wang, "Applying BCH error correcting code in digital watermarking", D. Jin and S. Lin (Eds.): *Advances in Electronic Commerce, Web Applications and Communication*, AISC 148, vol. 1, pp. 405-410, Springer-Verlag, 2012.
- [8] S. Baudry et. al., "Analyses of error correction strategies for typical communication channels in watermarking," *Signal Processing*, vol. 81, pp. 1239-1250, 2001.
- [9] N. Terzija et. al., "Impact of different Reed-Solomon codes on digital watermarks based on DWT," In: *Proc. of the Multimedia and Security Workshop at ACM Multimedia*, pp. 1-5, Juan-les-Pins, FR, 2002.
- [10] P. Cika, "Watermarking scheme based on discrete wavelet transform and error-correction codes," In: *Proc. of the 16th Int. Conf. on Systems, Signals and Image Process. (IWSSIP 2009)*, pp. 1-4, Chalkida, GR, 2009.
- [11] I. S. Reed and G. Solomon, "Polynomial codes over certain fields," *J. Soc. Ind. Appl. Math.*, vol. 8, pp. 300-304, 1960.
- [12] J. Lee and K. A. S. Immink, "An efficient decoding strategy of 2D-ECC for optical recording systems," *IEEE Trans. Consumer Electronics*, vol. 55, n. 3, pp. 1360-1363, 2009.
- [13] D. Chase, "A class of algorithms for decoding block codes with channel measurement information," *IEEE Trans. Inf. Theory*, vol. IT-18, n. 1, pp. 170-182, 1972.
- [14] E. Berlekamp, "Nonbinary BCH decoding," In: *Proc. of the Int. Symp. Inf. Theory (ISIT)*, vol. 14, n.2, pp. 242, San Remo, IT, 1967.
- [15] O. Aitsab and R. Pyndiah, "Performance of Reed-Solomon block turbo code," In: *Proc. of the IEEE Global Telecommunications Conf. (GLOBECOM 1996)*, vol. 1, pp. 121-125, London, UK, 1996.
- [16] The USC-SIPI Image Database, University of South California. Disponível em: <http://sipi.usc.edu/database/>. Acesso em 20/09/2012.