INSERÇÃO DE MARCA D'ÁGUA EM IMAGENS USANDO MÚLTIPLOS DICIONÁRIOS PARA QUANTIZAÇÃO VETORIAL

Edson Mata da Silva Filho*, Paulo Hugo Espirito Santo*, Francisco Madeiro*

*Universidade de Pernambuco (UPE), Recife, 50720-001, Brasil

Emails: edsonmata@hotmail.com, paulo.hugo@poli.br, madeiro@poli.br

Abstract— The present paper introduces a watermarking technique with multiple codebooks for VQ (vector quantization), which doubles the storage capacity when compared to the technique originally presented by Wang, Jain e Pan. This technique uses genetic algorithms in order to partitioning the codebooks. Simulations results show that the proposed techniques are as robust as the original technique to a variety of attacks.

Keywords— Watermarking, Genetic Algorithm, Vector Quantization.

Resumo— Neste trabalho são introduzidas técnicas de marca d'água com múltiplos dicionários para QV (quantização vetorial), as quais têm o dobro da capacidade de armazenamento de informação quando comparadas com a técnica proposta originalmente por Wang, Jain e Pan. Esta técnica emprega algoritmos genéticos no particionamento de dicionários. Resultados de simulação mostram que as técnicas propostas são tão robustas quanto a técnica original para uma variedade de ataques.

Palavras-chave— Marca D'água, Algoritmos Genéticos, Quantização Vetorial.

1 Introdução

Dentre as técnicas de ocultação de informação, no contexto de imagens digitais, podem ser citadas a esteganografia e a a marca d'água. A esteganografia é geralmente definida como a técnica de ocultar informação. Assim, por exemplo, uma imagem digital pode "esconder" um texto, um sinal de voz, outra imagem digital. O foco da esteganografia é "o que é escondido". A marca d'água digital funciona como uma espécie de identificador, introduzido normalmente de forma imperceptível, por exemplo, pelo criador ou detentor dos direitos da imagem em que a marca é inserida. O objetivo, neste caso, é provar os direitos da imagem. O foco da marca d'água é "o objeto utilizado para fins de ocultação", como, por exemplo, a imagem de cobertura supramencionada.

Muitos métodos de ocultação de dados têm sido propostos para fins de segurança da informação (Weng and Pan, 2016; Parah et al., 2017; Bai et al., 2017; Reddy and Kumar, 2016; Chang et al., 2015). Esses métodos geralmente podem ser classificados em três tipos de acordo com o domínio em que atuam: domínio espacial (Parah et al., 2017; Chang et al., 2015; Bai et al., 2017), domínio da frequência (Weng and Pan, 2016; Reddy and Kumar, 2016), domínio comprimido (Bai Chang and Zhu, 2015; Tu and Wang, 2015; Wang, Jain and Pan, 2007). No último domínio, pode-se citar o uso de imagens comprimidas por quantização vetorial como objetos de cobertura para embutir dados secretos.

A quantização vetorial (QV) (Gersho and Gray, 1992) é uma técnica de compressão com perdas, que consiste no mapeamento Q de um vetor de entrada x pertencente ao espaço euclidiano K-dimensional, em um vetor pertencente a um subconjunto finito W de $\mathbf{R}^K$, ou seja, $Q : \mathbf{R}^K \rightarrow W$. Denomina-se dicionário, $W = \{w_i; i = 1, 2, \ldots, N\}$, este subconjunto finito, no qual cada elemento é denominado vetor-código, cujo número de componentes se denomina dimensão (K). O tamanho do dicionário é a quantidade de vetores-códigos, denotada por N.

A quantização vetorial também tem sido utilizada em esteganografia e marca d'água em imagens digitais (Chang, Nguyen and Lin, 2015; Wang, Jain and Pan, 2007; Wang et al., 2013; Shen and Ren, 2010; Qin, Chang and Chen., 2013; Li, Jia and Kuo, 2017; Tiwari, Sharma and Tamrakar, 2017). Um problema relevante no âmbito da QV é o projeto de dicionários. O desempenho de sistemas de processamento de sinais baseados em QV depende fortemente da qualidade dos dicionários projetados. Dentre as técnicas de projeto de dicionários, o algoritmo LBG (Linde-Buzo-Gray) (Linde, Buzo and Gray, 1980) destaca-se por sua ampla utilização. Alternativas ao algoritmo LBG tem sido apresentadas na literatura, como, por exemplo, algoritmos baseados em inteligências de enxames, a exemplo do algoritmo do vagalume (Severo et al., 2016), algoritmos baseados em lógica nebulosa, como é o caso das famílias de algoritmos K-means (Silva Filho et al., 2016), e algoritmos meméticos (Azevedo et al., 2008).

Neste trabalho é introduzido um método de ocultação de um par de *bits* no domínio comprimido. Cada par de *bits* é associado a um dos quatro subdicionários em que o dicionário é particionado. De forma similar à proposta de Wang, Jain and Pan (2007), o particionamento é orientado por um algoritmo genético, com o qual se busca a menor distorção possível. A partir deste método são introduzidas três técnicas, as quais variam no tamanho do dicionário e no algoritmo de projeto de

dicionário. O objetivo é dobrar a carga de *bits* ocultos.

O trabalho encontra-se organizado de acordo com as seções a seguir. Na Seção 2 é apresentada a dinâmica da ocultação de marca d'água baseada em quantização vetorial. As técnicas propostas são apresentadas na Seção 3. Os resultados e os comentários finais são apresentados na Seção 4 e na Seção 5, respectivamente.

2 Marca D'Água Baseada em QV

As técnicas de inserção de marca baseada em QV associam grupos de vetores-código a *bits* da marca d'água a ser inserida. Dessa forma, a determinação do vizinho mais próximo restringe-se aos vetores-códigos do subdicionário relativo aos *bits* a serem ocultados. Ao se comparar com técnicas que empregam o dicionário sem particionamento, percebe-se que há uma redução do espaço de busca em técnicas que usam o particionamento, pois os vetores-códigos dos demais subdicionários não são considerados no procedimento de busca.

Uma técnica baseada em QV foi proposta por Wang, Jain e Pan (2007), a qual consiste em particionar um dicionário, com o objetivo de maximizar a *PSNR* (*Peak Signal to Noise Ratio*) da imagem marcada. A partição foi obtida com auxílio de um algoritmo genético. No final do processo, vetores do dicionário associados ao *bit* 0 (1) formam o subdicionário W_0 (W_1). A Figura 1 ilustra o particionamento de um dicionário de tamanho $N = 32$ em dois subdicionários.

Na inserção de cada *bit* da marca, primeiramente, é determinado qual subdicionário será usado e, em seguida, por meio da distância euclidiana, é selecionado o vetor-código que leva à menor distorção. Neste cenário, caso o *bit* a ser ocultado seja "0" então o subdicionário W_0 é selecionado, caso o *bit* seja "1" então o subdicionário W_1 é selecionado. Na extração da marca, determina-se a qual partição pertence cada vetor da imagem marcada. A marca d'água é recuperada pela sequência dos índices correspondentes dos subdicionários.

3 Técnicas Propostas

A técnica proposta em (Wang, Jain and Pan, 2007) (a partir deste ponto chamada de clássica) é capaz de ocultar 1 *bit* a cada bloco de 16 *pixels*.

Na primeira técnica (DIC256), um dicionário de tamanho 256 é projetado usando o algoritmo de projeto de dicionário LBG. Um algoritmo genético é usado para particioná-lo em quatro subdicionários. De acordo com a marca d'água a ser inserida o dicionário é particionado nos subdicionários W_{00}, W_{01}, W_{10} e W_{11}, os quais são associados, respectivamente, aos pares de *bits* 00, 01, 10 e 11 da marca d'água. Na Figura 2 é exemplificado o particionamento de um dicionário de tamanho $N = 32$ em quatro subdicionários usando a técnica supracitada. Dessa forma, um determinado bloco de *pixel* é selecionado de um subdicionário, de acordo com o par de *bits* a ser ocultado.

Na segunda técnica (2DIC128), dois dicionários de tamanho 128 são projetados usando os algoritmos de projeto de dicionários LBG e *fuzzy K-means*[1] (Silva Filho et al., 2016). Os dicionários projetados podem ter alguns vetores-código iguais. Para evitar isto, é feito um procedimento de intervenção que consiste em modificar os dois *bits* menos significativos de cada componente do vetores-código de um dos dicionários, com o objetivo de garantir que todos os vetores-códigos dos dois dicionários sejam distintos. Em seguida, cada um dos dicionários é particionado, usando um algoritmo genético, em dois subdicionários, conforme a técnica clássica, gerando então quatro subdicionários. A Figura 3 ilustra o particionamento de dois dicionários de tamanho $N = 128$ em dois subdicionários cada, usando a técnica 2DIC128. Note que há quatro subdicionários distintos, cada um associado a um único par de *bits*.

A terceira técnica (2DIC256) é semelhante à técnica 2DIC128, porém são projetados dicionários de tamanho 256 com os algoritmos de projeto de dicionários LBG e *fuzzy K-means*. Se necessário, o mesmo procedimento de intervenção descrito na técnica 2DIC128 é empregado.

A taxa de codificação é um aspecto importante em situações como na transmissão de dados, pois indica a quantidade de *bits* necessária para representar um *pixel* da imagem. Para as técnicas clássica, DIC256 e 2DIC128, a taxa de codificação é de $8/16 = 0{,}5$ *bpp*. Já para a técnica 2DIC256, a taxa de codificação é de $9/16 = 0{,}5625$ *bpp*.

O espaço de memória requerido para armazenar o dicionário também é um requisito importante. Para as técnicas clássica, DIC256 e 2DIC128, são necessários 4096 *bytes* (16×256) de memória, enquanto para a técnica 2DIC256 são necessários 8192 *bytes* (16×512) de memória.

Convém ressaltar que as técnicas ora propostas diferem do método introduzido por Silva Filho, Santo e Madeiro (2017), no qual o particionamento do dicionário W é realizado em duas etapas: particiona-se W em W_0 e W_1; e, em seguida, particiona-se W_0 em W_{00} e W_{01}, e particiona-se W_1 em W_{10} e W_{11}.

3.1 Procedimento de Ocultação

Os passos para ocultação de uma marca d'água são apresentados a seguir:

[1] Neste trabalho optou-se por utilizar os algoritmos LBG e *fuzzy K-means*, entretanto, quaisquer técnicas de projeto de quantizadores vetoriais poderiam ser utilizadas para a obtenção dos dicionários de tamanho 128.

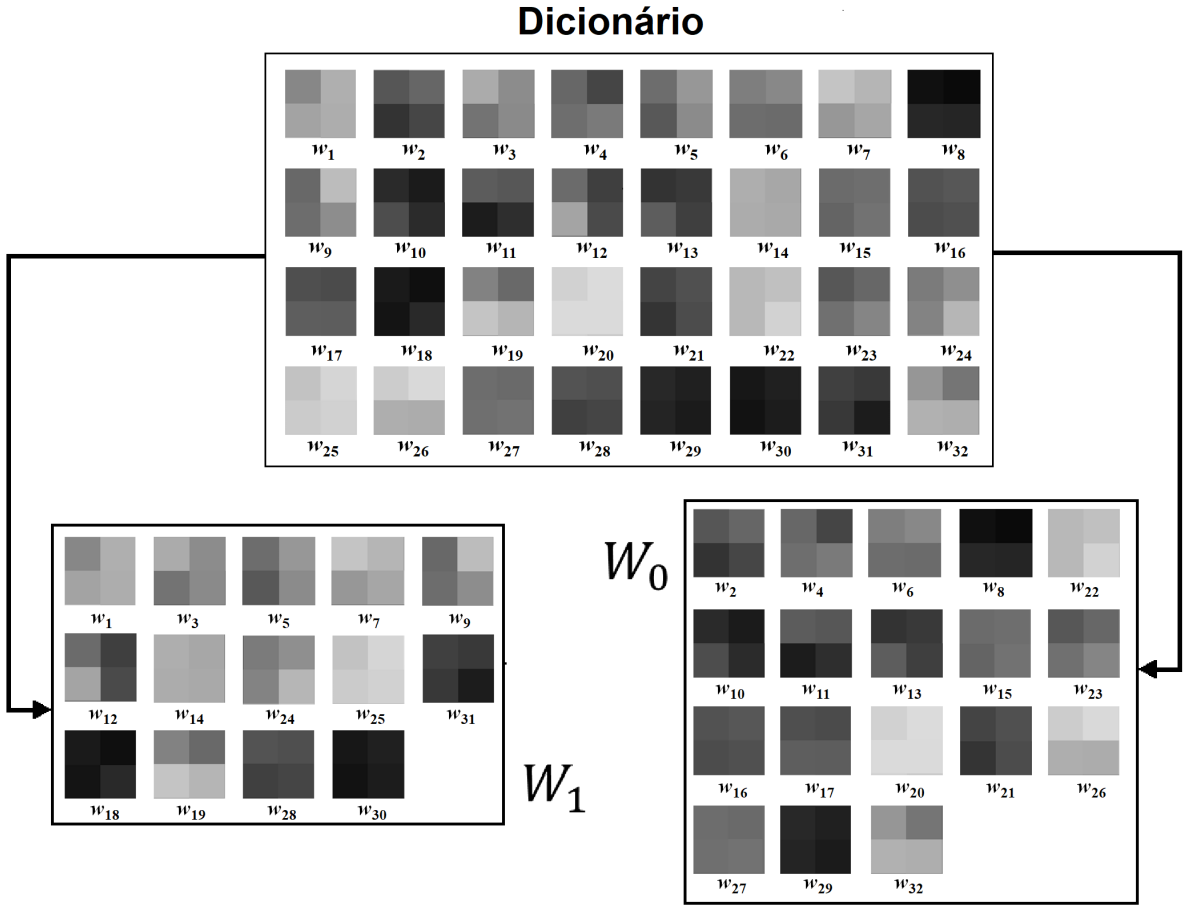


Figura 1: Particionamento do dicionário com a técnica clássica.

- **Passo 1**: Dividir a imagem de cobertura X em M blocos, $X = \{x_1, x_2, \ldots, x_M\}$.
- **Passo 2**: Projetar o(s) dicionário(s) com o(s) algoritmo(s) LBG (e *fuzzy K-means*).
- **Passo 3**: Particionar o(s) dicionário(s) de acordo com cada técnica (DIC256, 2DIC128 ou 2DIC256) gerando quatro subdicionários, W_{00}, W_{01}, W_{10} e W_{11}.
- **Passo 4**: Dado um vetor de entrada x_i, $1 \leq i \leq M$, e um par de *bits* da marca d'água, denotado por $g_i \in \{00, 01, 10, 11\}$, seleciona–se o subdicionário W_{g_i}.
- **Passo 5**: No subdicionário W_{g_i} selecionado no Passo 4, busca-se o vetor-código de maior similaridade, obtendo o vetor de saída x'_i.
- **Passo 6**: Repetir os passos 3-4 até todos os *bits* da marca d'água serem ocultados.
- **Passo 7**: Reconstruir a imagem X' concatenando os vetores de saída $\{x'_1, x'_2, \ldots, x'_M\}$.

3.2 Procedimento de Extração

Os passos para extração da marca d'água são apresentados a seguir:

- **Passo 1**: Dividir a imagem marcada X' em M blocos, $X' = \{x'_1, x'_2, \ldots, x'_M\}$.
- **Passo 2**: Para um vetor x'_i, $1 \leq i \leq M$, execute a pesquisa pelo vetor-código de maior similaridade;
- **Passo 3**: Determine os pares de *bits* ocultos de acordo com o subdicionário ao qual pertence o vetor-código selecionado no Passo 2.
- **Passo 4**: Repetir os passos 2 e 3 até todos os pares de *bits* ocultos, $\{g'_1, g'_2, \ldots, g'_M\}$, serem extraídos.
- **Passo 5**: Obter a mensagem oculta (a marca) a partir da concatenação dos pares de *bits* ocultos $\{g'_1, g'_2, \ldots, g'_M\}$.

4 Resultados

As simulações foram realizadas usando imagens de cobertura de 512×512 *pixels*, 8 *bpp*, ilustradas na Figura 4. Foram usadas quatro imagens binárias de dimensões 128×128 *pixels* como marcas d'água, apresentadas na Figura 5.

As técnicas DIC256 e 2DIC128 foram comparadas com a técnica clássica com tamanho de dicionário 256. A técnica 2DIC256, por sua vez, foi também comparada com a técnica clássica, mas com tamanho de dicionário 512. Todas as técnicas de marca d'agua foram avaliadas em termos da qualidade da marca recuperada, de forma a avaliar a robustez das técnicas a diferentes ataques,

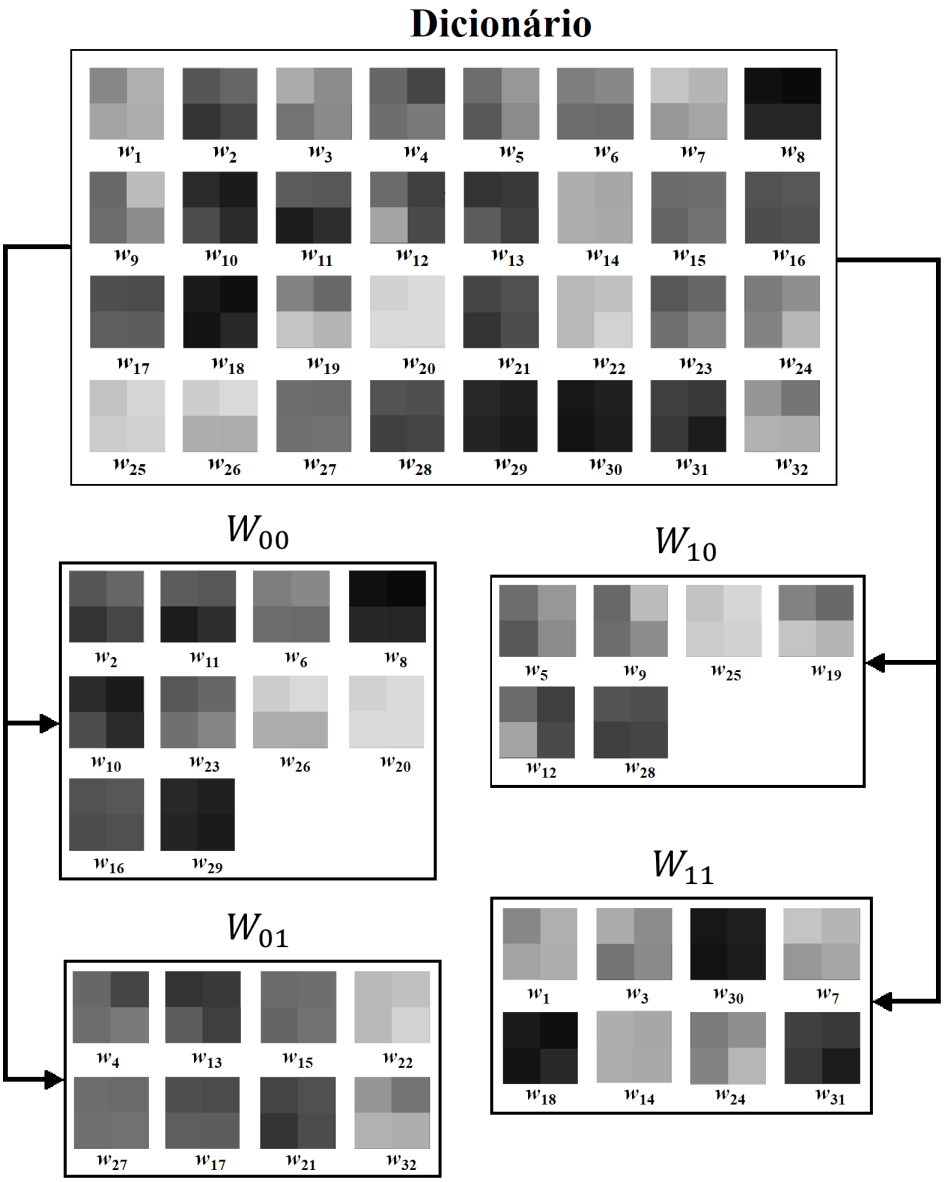


Figura 2: Particionamento do dicionário com a técnica DIC256.

a saber: compressão JPEG com fator de qualidade (QF) 40%, 60% e 80%; filtros de média e mediana; corte no 3^o quadrante; deslocamento de linha (*shift*) para baixo. A métrica usada na avaliação da qualidade das marcas recuperadas foi a *Bit-Correct Rate* (*BCR*), dada por

$$BCR(G, G') = \left(1 - \frac{\sum_i^{L_w} |g_i - g'_i|}{L_w}\right) \times 100,$$

em que L_w representa o tamanho (número de *bits*) da marca d'água, g_i e g'_i são o i-ésimo *bit* da marca d'água original, G, e da marca d'água extraída, G', respectivamente. Quanto maior for o valor de *BCR*, mais parecida com a marca d'água original é a marca extraída após os ataques.

As Tabelas 1 e 2 apresentam os valores de *BCR* da marca EMSF, para a técnica clássica e para as técnicas propostas.

Na Tabela 1, considerando o ataque de compressão, observa-se que os valores de *BCR* para a técnica DIC256 estão próximos da técnica clássica para $N = 256$. Ainda considerando o ataque de compressão, observa-se na Tabela 2 que os valores de *BCR* para a técnica 2DIC256 são inferiores aos obtidos com a técnica clássica para $N = 512$. A degradação das marcas foi maior quando se empregaram dicionários de tamanho $N = 512$.

Já para os ataques de média, mediana e *shift*, os valores de *BCR* para as técnicas propostas foram menores do que na técnica clássica, independentemente do tamanho do dicionário. Para estes ataques, os baixos valores de *BCR* indicam que as marcas foram fortemente degradadas.

Ilustrando o que se observa nas Tabelas 1 e 2, são apresentadas nas Figuras 6 e 7 as marcas EMSF extraídas após os ataques de compressão JPEG com QF80% e de mediana, usando a ima-

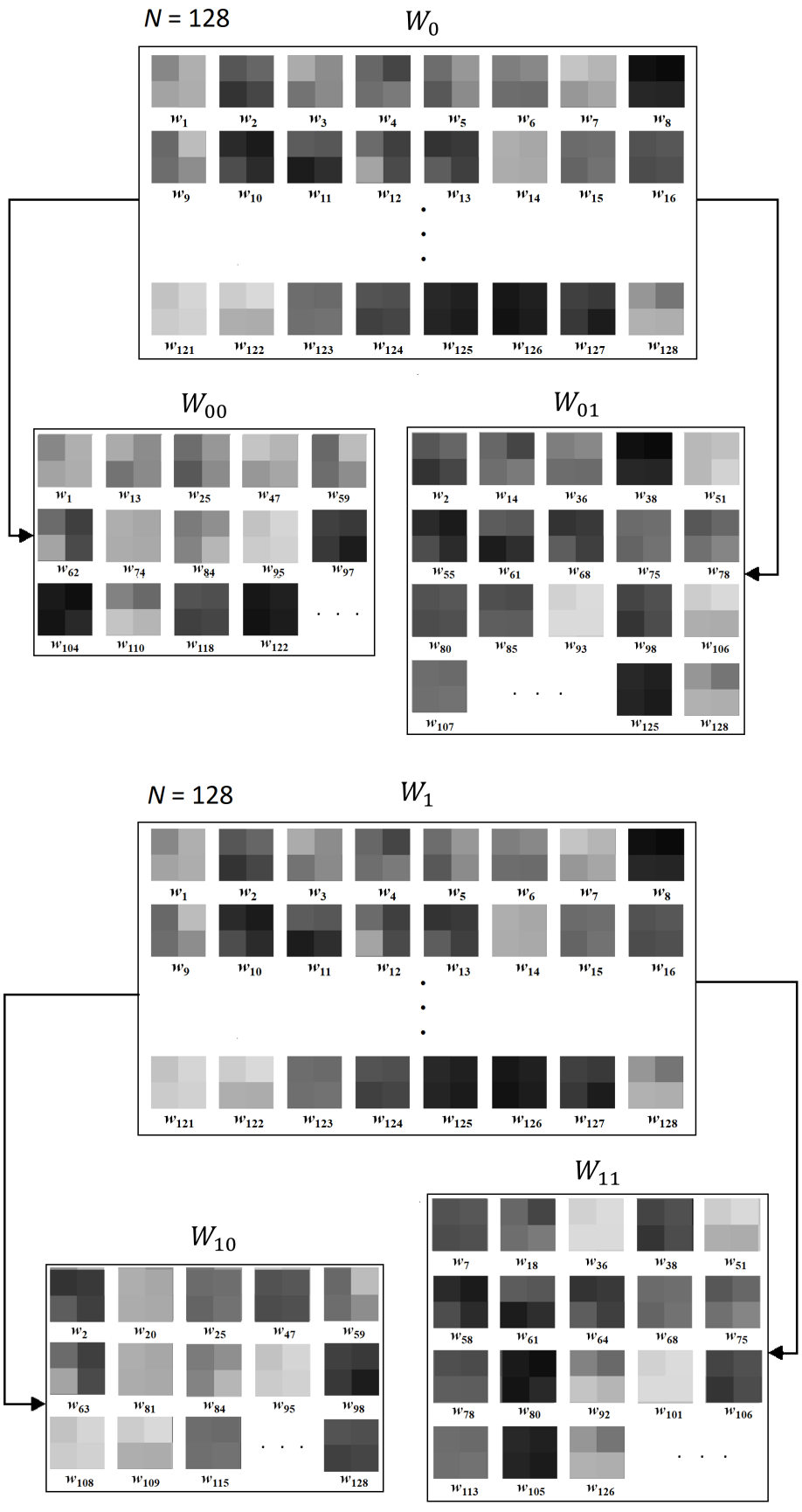


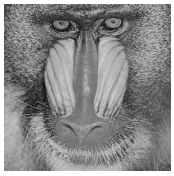
Figura 3: Particionamento dos dicionários com a técnica 2DIC128.

Tabela 1: *BCR* da marca da EMSF extraída após os ataques, para as imagens Mandrill, Lena e Walkbridge para as técnicas com dicionários de tamanho 256.

Ataques	**BCR(%)**								
	Técnica Clássica			**DIC256**			**2DIC128**		
	Mandrill	**Lena**	**Walk.**	**Mandrill**	**Lena**	**Walk.**	**Mandrill**	**Lena**	**Walk.**
QF40%	97,96	87,54	98,82	97,31	86,35	98,37	93,12	78,81	92,57
QF60%	99,66	92,96	99,88	99,33	93,62	99,79	97,15	86,38	96,26
QF80%	99,99	97,86	100,00	99,99	98,52	100,00	99,64	92,52	99,07
Corte	97,71	97,71	97,71	100,00	100,00	100,00	100,00	100,00	100,00
Média	81,79	81,85	81,63	66,81	74,18	71,20	68,43	73,50	67,19
Mediana	88,06	92,33	88,39	76,72	88,09	84,38	78,42	87,47	79,77
Shift	75,35	81,30	72,52	62,52	80,35	66,61	66,91	78,89	65,30

Tabela 2: *BCR* da marca EMSF extraída após os ataques, para as imagens Mandrill, Lena e Walkbridge para as técnicas com dicionários de tamanho 512.

Ataques	**BCR(%)**					
	Técnica Clássica (512)			**2DIC256**		
	Mandrill	**Lena**	**Walk.**	**Mandrill**	**Lena**	**Walk.**
QF40%	94,53	80,47	96,59	88,92	74,04	90,59
QF60%	98,43	86,67	99,29	93,93	81,54	96,53
QF80%	99,85	95,11	99,99	97,77	88,95	99,21
Corte	77,29	97,71	77,29	100,00	100,00	100,00
Média	74,10	75,16	76,39	63,98	68,19	63,79
Mediana	81,43	84,59	85,23	72,31	81,72	75,92
Shift	70,73	74,47	69,68	60,10	67,51	63,18


(a) Mandrill


(b) Lena


(c) Elaine

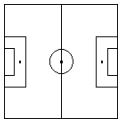

(d) Walkbridge


(e) Boat


(f) Lake

Figura 4: Imagens de cobertura 512×512 *pixels*, 8 *bpp*.

(a) EMSF


(b) Campo


(c) Formas


(d) Rose

Figura 5: Imagens usadas como marcas, 128×128 *pixels*, 1 *bpp*.

gem de cobertura Walkbridge. As marcas apresentadas na Figura 6 foram inseridas usando as técnicas clássica, DIC256 e 2DIC128. As marcas inseridas usando a técnica clássica com $N = 512$ e 2DIC256 são apresentadas na Figura 7.

As técnicas propostas têm o dobro de capacidade de ocultação de informação quando comparadas com técnica clássica. Apesar disso, conforme se observa na Figura 6, as marcas extraídas pelas técnicas 2DIC128 e DIC256 apresentam pouca ou nenhuma degradaçãos visual ocasionada pelo ataque de compressão JPEG com QF80%. Já para o ataque de mediana, a degradação visual foi mais severa para todas as técnicas analisadas. Observou-se uma severa degradação visual para os ataques de média, mediana e *shift*. A maior severidade do ataque de mediana, quando comparado com o ataque de compressão JPEG com QF 80% também pode ser observada na Figura 7.

5 Conclusões

As técnicas introduzidas foram projetadas para ter o dobro da capacidade de armazenamento de informação da técnica clássica proposta por Wang, Jain and Pan (2007). Cada bloco da imagem passa a ocultar dois *bits* em vez de um único *bit* ocultado com a técnica clássica. Mesmo assim, a técnica DIC256 manteve-se tão robusta quanto a técnica clássica para os ataques de compressão e de corte para $N = 256$. Nos ataques de média, mediana e *shift* observa-se que a marca extraída a partir de todas as técnicas foi severamente degradada, ainda que a técnica clássica tenha apresentado maiores valores de *BCR* que os obtidos com as técnicas propostas.

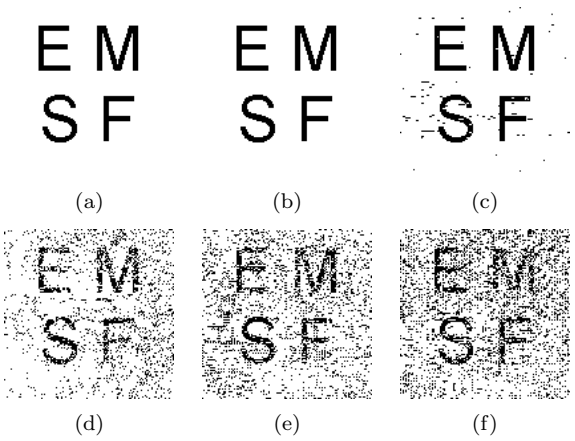


Figura 6: Marca EMSF extraída após os ataques de compressão com QF80% e mediana, para técnicas com $N = 256$ vetores-código, usando a imagem de cobertura Walkbridge. (**a**) Clás. QF80%; (**b**) DIC256 QF80%; (**c**) 2DIC128 QF80%; (**d**) Clás. Mediana; (**e**) DIC256 Mediana; (**f**) 2DIC128 Mediana.

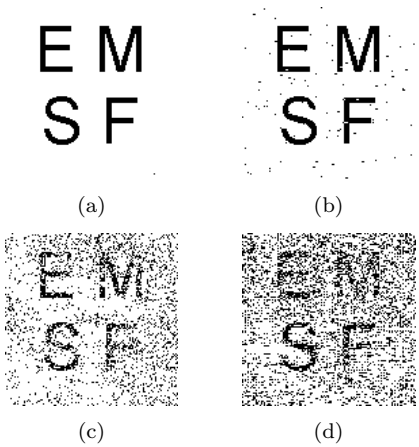


Figura 7: Marca EMSF extraída após os ataques de compressão com QF80% e Mediana, para técnicas com $N = 512$ vetores-código, usando a imagem de cobertura Walkbridge. (**a**) Clássica com QF80%; (**b**) 2DIC256 com QF80%; (**c**) Clássica com Mediana; (**d**) 2DIC256 com Mediana.

Além disso, as técnicas DIC256 e 2DIC128 tem a mesma taxa de codificação ($0,5$ *bits*/amostra) e requerem o mesmo espaço de memória para armazenamento do dicionário que a técnica clássica com $N = 256$. O emprego de dois dicionários projetados por algoritmos de projetos de dicionários distintos e de maneira independente não se mostrou uma alternativa atraente, como se observa nos resultados de *BCR* associados às técnicas 2DIC128 e 2DIC256.

Agradecimentos

Este trabalho contou com apoio financeiro do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) e da Fundação de Amparo a Ciência e Tecnologia do Estado de Pernambuco (FACEPE).

Referências

Azevedo, C. R. B., Azevedo, R. A., Bispo Júnior, E. L., Ferreira, T. A. E., Lopes, W. T. A. and Madeiro, F. (2008). Um algoritmo memético para a otimização de quantizadores vetoriais, *Learning & Nonlinear Models* **6**(1): 3–15.

Bai, J., Chang, C.-C., Nguyen, T.-S., Zhu, C. and Liu, Y. (2017). A high payload steganographic algorithm based on edge detection, *Displays* **46**: 42–51.

Bai, J., Chang, C.-C. and Zhu, C. (2015). A reversible data hiding scheme using ordered cluster-based VQ index tables for complex images, *in* Z. Y. Image and Graphics (eds), *ICIG 2015. Lecture Notes in Computer Science*, Springer, Cham.

Chang, C.-C., Nguyen, T. S. and Lin, C.-C. (2015). A reversible compression code hiding using SOC and SMVQ indices, *Information Sciences* **300**: 85–99.

Chang, I.-C., Hu, Y.-C., Chen, W.-L. and Lo, C.-C. (2015). High capacity reversible data hiding scheme based on residual histogram shifting for block truncation coding, *Signal Processing* **108**: 376–388.

Gersho, A. and Gray, R. M. (1992). *Vector quantization and signal compression*, Springer, Massachusetts, USA.

Li, S., Jia, Y. and Kuo, C. C. J. (2017). Steganalysis of QIM steganography in low-bit-rate speech signals, *IEEE/ACM Transactions on Audio, Speech, and Language Processing* **25**(5): 1011–1022.

Linde, Y., Buzo, A. and Gray, R. M. (1980). An algorithm for vector quantizer design, *IEEE Transactions on Communications* **28**(1): 84–95.

Parah, S. A., Ahad, F., Sheikh, J. A. and Bhat, G. (2017). Hiding clinical information in medical images: A new high capacity and reversible data hiding technique, *Journal of Biomedical Informatics* **66**: 214–230.

Qin, C., Chang, C.-C. and Chen, K.-N. (2013). Adaptive self-recovery for tampered images based on vq indexing and inpainting, *Signal Processing* **93**(4): 933 – 946.

Reddy, M. and Kumar, A. (2016). Secured data transmission using wavelet based steganography and cryptography by using AES algorithm, *Procedia Computer Science* **85**: 62–69.

Severo, V., Leitão, H., Lima, J., Lopes, W. and Madeiro, F. (2016). Modified firefly algorithm applied to image vector quantisation codebook design, *International Journal of Innovative Computing and Applications* **7**(4): 202–213.

Shen, J.-J. and Ren, J.-M. (2010). A robust associative watermarking technique based on vector quantization, *Digital Signal Processing* **20**(5): 1408 – 1423.

Silva Filho, E. M., Bandeira, S., de Mattos Neto, P. S. G., Lopes, W. and Madeiro, F. (2016). Accelerating families of fuzzy K-means algorithms for vector quantization codebook design, *Sensors* **16**(11).

Silva Filho, E. M., Lima, P. H. E. S. and Madeiro, F. (2017). Marca d'água em imagens usando algoritmos genéticos e múltiplos dicionários para quantização vetorial, *ENCOM - Encontro Anual do Iecom em Comunicações, Redes e Criptografia*, IECOM, pp. 31–32.

Tiwari, A., Sharma, M. and Tamrakar, R. K. (2017). Watermarking based image authentication and tamper detection algorithm using vector quantization approach, *AEU - International Journal of Electronics and Communications* **78**: 114 – 123.

Tu, T.-Y. and Wang, C.-H. (2015). Reversible data hiding with high payload based on referred frequency for VQ compressed codes index, *Signal Processing* **108**: 278–287.

Wang, F.-H., Jain, L. C. and Pan, J.-S. (2007). VQ-based watermarking scheme with genetic codebook partition, *Journal of Network and Computer Applications* **30**(1): 4–23.

Wang, W.-J., Huang, C.-T., Liu, C.-M., Su, P.-C. and Wang, S.-J. (2013). Data embedding for vector quantization image processing on the basis of adjoining state-codebook mapping, *Information Sciences* **246**: 69 – 82.

Weng, S. and Pan, J.-S. (2016). Integer transform based reversible watermarking incorporating block selection, *Journal of Visual Communication and Image Representation* **35**: 25–35.