

SUBSAMPLING-BASED IMAGE WATERMARKING IN COMPRESSED DCT DOMAIN

Ibrahim Nasir , Ying Weng, Jianmin Jiang and Stan Ipson
School of Informatics, University of Bradford
BD7 1DP, UK

{I.A.Nasir, Y.Weng, J.Jiang1, S.S.Ipson}@Bradford.ac.uk

ABSTRACT

In this paper, a new embedding strategy for watermarking is presented based on DC components of subimages in compressed discrete cosine transform (DCT) domain. These subimages are obtained through subsampling the host image. More robustness has been achieved when watermarks are embedded in perceptually significant DC components. Furthermore, the original image is not required in the extraction process. Experimental results show that the proposed scheme successfully makes the watermark perceptually invisible and robust for a wide range of attacks, including JPEG-loss compression, filtering, scaling, and cropping attacks.

KEY WORDS

Watermarking, compressed DCT domain, DC components, subimages and subsampling

1. Introduction

Digital watermarking techniques have recently been widely proposed for copyright protection and authentication of digital media. An imperceptible signal or a pattern called a watermark that contains useful certifiable information to identify the ownership is embedded into the host media, which can be digital image, audio and video, etc. The watermark can be detected or extracted later to make an assertion about the host media. The watermark embedding should not alter the quality and the visually of the host media. On the other hand, the watermark should still be detected from the watermarked media under intentional or unintentional attacks [1, 2]. Overviews on image watermarking techniques can be found in [1, 3].

Watermarking techniques can be classified into two categories: spatial domain watermarking techniques and frequency domain watermarking techniques. In spatial domain techniques, the watermark embedding is achieved by directly modifying the intensity pixel values of the host image whereas in transform domain techniques, the host

image is first converted into frequency domain by transformation method, such as the discrete Fourier transform (DFT), discrete cosine transform (DCT) or discrete wavelet transform (DWT), etc. Then, the transform domain coefficients are altered to embed the watermark. The inverse transform is finally applied to obtain the watermarked media. Due to the complicated calculations of forward and inverse transform, these methods generally are more complex than spatial domain methods; however, transformation domain methods are more robust against attacks than spatial domain methods [4].

In recent few years, many watermarking schemes have been proposed [5-11]. Cox et al. [5] proposed a method using the full-frame DCT with an additive white Gaussian noise (AWGN) sequence embedded into the perceptually most significant DCT coefficients of the image in order for the watermark to be robustness. Cox et al. claimed that the method is quite robust against signal manipulation. However, the watermark detection process requires the original image, which is usually not provided to the detector in most applications. Chu [6] proposed a method based on a random perturbation of the DCT coefficients corresponding to different subimages. The results in [6] show that this method is weak under low pass filtering and JPEG compression attacks. Lu et al. [7] proposed a method that subsampling the host image into four subimage and using the full-frame DCT and then the watermark is embedded into selected pair of AC components of the DCT of subimages. In [8], a random watermark sequence is embedded into DFT domain of four subsampled images. Huang et al. [9] argue that more robustness can be achieved if a watermark is embedded in DC components since dc component have much large perceptual capacity than any AC components. In [10], the watermark is embedded into DC components of color image directly in spatial domain. In [11], singular values of the watermark image in embedded in DC components of the Hadamard transform (FHT). The main weakness of the proposed methods in [9, 10, 11] is that the original image is required for the watermark detection process, which clearly constrains the application scenarios of these methods.

In this paper, we propose a novel image watermarking scheme in compressed DCT domain. The watermark is embedded in DC components of the host image and the original image is not required in the extraction process. The rest of this paper is structured as follows. Section 2 describes the proposed embedding and extracting algorithms. In section 3, the experimental results are shown. Conclusions are drawn in section 4.

2. Proposed watermarking algorithm

There are two concerns in building a strong watermarking scheme: the watermark structure and the embedding strategy [5]. In our scheme, a binary logo image is used as a watermark W , which represented by

$$W(i, j), 0 \leq i, j < M, W(i, j) \in \{0, 1\}$$

Where (i, j) represents the pixel coordinates of the binary watermark image and M denotes the size of the watermark. The watermark is encrypted to obtain pseudo random sequences, which are uncorrelated to the original watermark. The watermark encryption process can be defined as a function given by $W^* = E(W, C)$

where $E(\cdot)$ denotes the encrypted function, W^* denotes the encrypted watermark, C is a chaotic binary sequence, which is generated randomly by using a secret key. The encrypted watermark can be obtained by

$$W^* = W \oplus C$$

Where \oplus denotes the XOR operation between the original watermark and the chaotic binary sequence. Fig.1 shows the original and the encrypted watermark.



Fig.1: (a) Original watermark, (b) Encrypted watermark.

2.1 Watermark embedding algorithm

Suppose V denotes the original gray scale image to be protected by a binary watermark W . The original image with size $M \times N$ can be subsampled into four images as follows:

$$V_1(i, j) = V(2i, 2j)$$

$$V_2(i, j) = V(2i, 2j + 1)$$

$$V_3(i, j) = V(2i + 1, 2j)$$

$$V_4(i, j) = V(2i + 1, 2j + 1)$$

Where $i = 0, 1, 2, \dots, M/2 - 1, j = 0, 1, 2, \dots, N/2 - 1$.

Since the subimages V_i 's are highly correlated, it is expected that $V_i \approx V_j$ for $i \neq j$.

The watermark embedding process is described as follows:

- Four subimages V_1, V_2, V_3, V_4 are obtained by subsampling the host image.
- The original watermark is encrypted as explained in section 2 and converted into a vector W_l^* .
- A secret key is used to generate a random sequence $S_l = \{(i, j), i, j \in \{1, 2, 3, 4\}, i \neq j\}$, which serves as a dc coefficient selector, with the length equal to the length of the watermark.
- According to random sequence S_l two subimages are selected and DCT is applied to an overlapping block of 8×8 of two selected subimages.
- One pair of the selected DC coefficients of a block of 8×8 $\{(DC_i, DC_j), (i, j \in S_l)\}$ is situated to embed a watermark bit and leaving the AC coefficients unmodified.

In order to embed watermark bits into DC coefficients of blocks of 8×8 of selected subimages; the following operation is done. If $W_l^* = 0$ and $DC_i > DC_j$, then swapping i, j in S_l , and if $W_l^* = 1$ and $DC_i < DC_j$, then swapping i, j in S_l . Based on modified S_l the watermark embedding algorithm is given by

$$DC_{Avg} = \frac{DC_i + DC_j}{2}, DC_{Def} = \frac{|DC_i - DC_j|}{2}$$

$$\text{If } \frac{DC_{Def}}{DC_{Avg}} \leq \beta$$

$$DC_i^* = DC_i + \alpha(2W_l^* - 1).DC_{Avg}$$

$$DC_j^* = DC_j + \alpha(2W_l^* + 1).DC_{Avg}$$

else

$$DC_i^* = DC_i$$

$$DC_j^* = DC_j$$

Where α is the watermark embedding strength and β is the threshold, DC_i and DC_j are the DC components of blocks of 8×8 of the two selected subimages, DC_i^* and DC_j^* are the watermarked DC components.

- The watermarked subimages can be formed by performing the inverse DCT into the watermarked blocks, and the watermarked image is obtained by composing these watermarked subimages.

In our scheme, we apply DCT only into selected blocks of 8×8 of subimages and use DC components of those selected blocks to embed the watermark. While in [7] uses the DCT of full-frame of the four subimages and then the watermark is embedded into selected AC components.

2.2 Watermark extraction algorithm

The watermark extraction is performed without knowledge of the original image. Suppose V^* is an image to be tested for watermark extraction. The watermark extraction process is summarized as follows:

- Sub sampling the input image V^* into four subimages as explained in the watermark embedding process.
- Determine the watermark embedding positions by using the same DC random coefficient selector S_l that used in the embedding process.
- DCT is applied into blocks of 8×8 of selected subimages.
- The watermark extraction bit is determined by comparing the DC coefficient values of selected subimages as follows:

$$W_i^* = 1 \quad \text{If } DC_i^* \geq DC_j^*$$

$$\text{else}$$

$$W_i^* = 0$$

Where W_i^* is the extracted bit, DC_i^* and DC_j^* are DC coefficient values of blocks of 8×8 of the selected subimages. After extraction of all watermark bits, the watermark bits are reshaped into a matrix, and the inverse encryption is applied to obtain the extracted binary watermark image.

The Normalized cross correlation is used to measure the similarity between the original watermark and the extracted watermark and also to make the binary decision on whether a given watermark exists or not. It is compared with the appropriate threshold T . Fig.2 shows the watermark detector response with 1000 watermark seeds. The threshold T is chosen to be 0.6 for the watermark decision. The Normalized cross correlation (NCC) is given by

$$NCC = \frac{\sum_i \sum_j W(i, j) \cdot W^*(i, j)}{\sum_i \sum_j (W(i, j))^2}$$

Where $W(i, j)$ and $W^*(i, j)$ are the pixel values at the position (i, j) of the original and the extracted watermark, respectively.

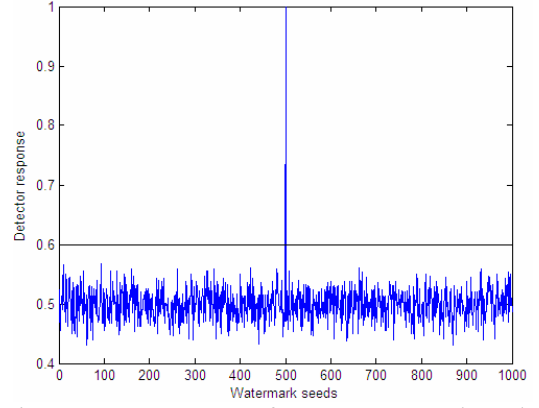


Fig.2: Detector response for 1000 watermark seeds.

3. Experimental results

The performance of the proposed scheme is tested on the popular images; Lena, Barbara, peppers and Baboon gray-scale images of size 512×512 . The logo used for watermarking is a binary image of size 32×32 . The choice of the embedding strength α is tradeoff between image distortion and robustness. It is chosen as $\alpha = 0.02$. β is chosen as $\beta = 0.05$. Peak signal to noise ratio (PSNR) is used to evaluate the perceptual distortion of the proposed scheme, PSNR is given by

$$PSNR = 10 \log_{10} \frac{255^2}{MSE}$$

$$MSE = \frac{1}{m \times n} \sum_{i=1}^m \sum_{j=1}^n [(x(i, j) - x^*(i, j))]^2$$

Where $x(i, j)$ and $x^*(i, j)$ depict a pixel at location (i, j) of the original and the watermarked images, respectively. m and n denote the size of the image. Fig. 3 illustrates the invisibility of the watermark. Original Lena, Barbara images are shown in Fig. 3(a) and 3(c), respectively. Watermarked Lena and Barbara images are shown in Fig. 3(b) and 3(d), respectively. The MSE and PSNR between watermarked and original Barbara image is 1.438 and 47.553, respectively, 1.70 and 45.8065 for Lena image. Therefore, there is no obvious perceptual distortion between watermarked image and original image, the embedded watermark does not degrade the quality of original host image. The extracted watermark is shown in Fig. 4.



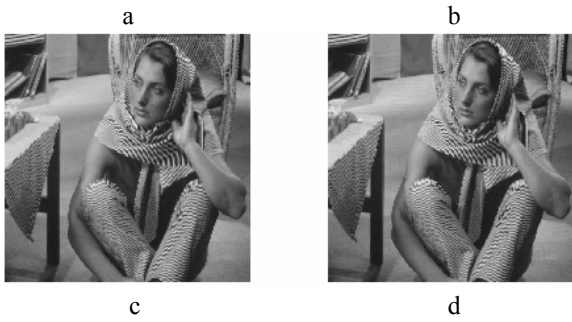


Fig. 3: (a) Original Lena image; (b) Watermarked Lena image; (c) Original Barbara image; (d) Watermarked Barbara image.

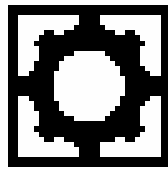


Fig. 4: Extracted watermark with NCC=1

To verify the robustness of the proposed method, various common signal processing and geometric attacks are applied to the watermarked images. The attacks including, Jpeg compression, Gaussian low pass filtering, low pass filtering, median filtering noise addition, scaling and cropping attacks. The results of Jpeg compression attack for watermarked Lean, Baboon and Barbara images are shown in Fig. 5. As can be seen from Fig. 5, the detector response can still declare the existence of the watermarks correctly even under Jpeg attack with quality 10.

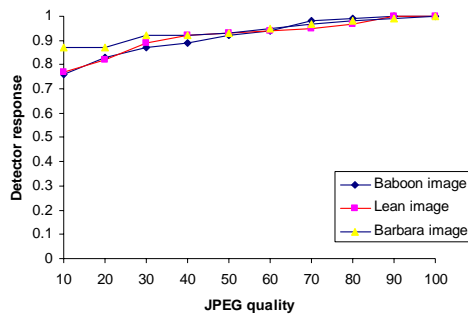


Fig. 5: Results of Jpeg compression attacks

Results in Fig. 6 show the detector response with different scale factors of scaling attack. The watermark is detected even when the watermarked images Lean, Barbara and Baboon is scaled to 50% down.

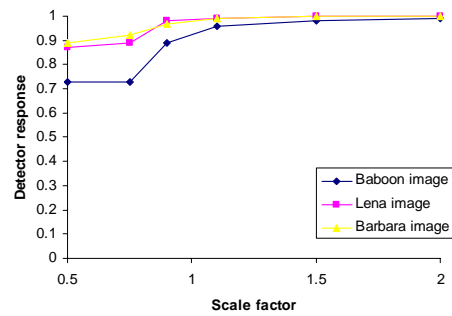


Fig. 6: Results of scaling attacks

Fig. 7 shows the extracted watermarks from watermarked images under several signal processing attacks, including JPEG compression with quality 10,20 and 30; scaling with factor of 0.5, 0.9 and 2; median filtering ; Gaussian low-pass filtering ; low pass filtering; salt and pepper noise. All the extracted watermarks can be identified and the detector's response is finer to declare the existence of the watermarks.

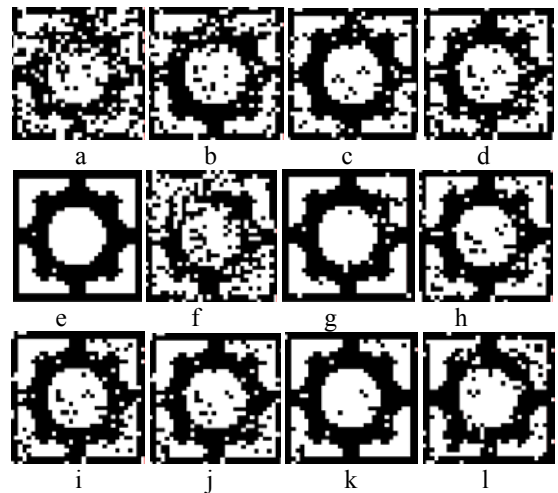


Fig. 7: Extracted watermarks after (a), (b) and (c) JPEG compression with quality 10, 20, and 30, respectively; (d) and (e) scaling image by 1/2 and 2; (f), (g) and (h) 3*3, 5*5 and 9*9 median filtering; (i) and (j) 3*3 and 5*5 Gaussian low pass filtering; (k) 5*5 low pass filtering; (l) adding 0.03 salt and pepper noise.

Results of cropping attack are shown in Fig.8 and 9; the watermark can be detected even when watermarked images Baboon and Lena are cropped by 25 % or 50%, respectively.



Fig. 8 (a) cropping image by 25%; (b) extracted watermark with NCC=0.87



Fig. 9 (a) cropping image by 50%; (b) extracted watermark with NCC= 0.74

We have also implemented the method presented by Lu et al. [7] for gray-scale images in order to evaluate our proposed method and to compare the performance difference between embedding the watermark into DC components and AC components of the DCT. Table 1 shows the experimental results of our method and Lu's method with some attacks.

Table 1: Normalized cross correlation computed from Lu's [7] and our methods after various attacks.

Attack operations	Attack operation on Lena image			
	Lu's method		Our method	
	PSNR	NCC	PSNR	NCC
Attack free	43.405	1.0	45.806	1.0
Jpeg 80	38.827	0.89	40.460	0.97
Jpeg 50	37.382	0.87	38.854	0.93
Jpeg 20	35.400	0.85	36.462	0.84
Scaling 1/2	36.050	0.88	37.007	0.87
Scaling 2	40.482	0.96	42.592	1.0
Median filter 5	35.605	0.93	36.467	0.96
Gaussian low pass filter 3*3	30.470	0.88	30.429	0.91
Jpeg30+Gaussian low pass filter 3*3	39.876	0.86	41.012	0.87
Jpeg30+low pass filter 3*3	32.442	0.87	33.558	0.84
Salt&pepper 0.03 +median filter	37.094	0.73	36.364	0.96
Gaussian noise 0.03	31.963	0.72	30.289	0.92
Salt&pepper noise 0.1	32.849	0.67	36.530	0.82

4. Conclusion

A new image watermarking scheme based on embedding a binary watermark image into DC components of subimages

that obtained through subsampling the host image is presented. The watermark extraction process is performed without knowledge of the original image. The experimental results show that the proposed scheme is robust against various signal processing operation and geometric attacks including JPEG compression, filtering, scaling, and cropping attacks. Furthermore, it is also a secure scheme; the watermark can not be extracted without knowing the secret key. Further investigation for increasing robustness by using adaptive embedding strength α depending on blocks characteristics is on the way.

References

- [1] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, Information hiding-a survey, *Proceedings of the IEEE*, 87(7), 1999, 1062-1078.
- [2] F. Hartung and M. Kutter, Multimedia watermarking techniques, *Proceedings of the IEEE*, 87(7), 1999, 1079-1107.
- [3] C. De Vleeschouwer, J. F. Delaigle, and B. Macq, Invisibility and application functionalities in perceptual watermarking an overview, *Proceedings of the IEEE*, 90(1), 2002, 64-77.
- [4] A. A. Reddy and B. N. Chatterji, A new wavelet based logo-watermarking scheme, *Pattern Recognition Letters*, 26(7), 2005, 1019-1027.
- [5] I.J. Cox, J. Killian, T. Leighton, and T. Shamon, Secure spread watermarking for multimedia, *IEEE Trans. on Image Processing*, 6(12), 1997, 1673-1687.
- [6] W. C. Chu, DCT-based image watermarking using subsampling, *IEEE Transactions on Multimedia*, 5(1), 2003, 34-38.
- [7] W. Lu, H. Lu, and F.-L. Chung, Robust digital image watermarking based on subsampling, *Applied Mathematics and Computation*, 181(2), 2006, 886-893.
- [8] F. Yonggang, S. Ruimin, and S. Liping, Robust image watermarking scheme based on subsampling, *Proc. 3rd Int. Conf. on Information Technology and Applications*, Sydney, 2005, 361-365.
- [9] H. Jiwu, Y. Q. Shi, and S. Yi, Embedding image watermarks in dc components, *IEEE Transactions on Circuits and Systems for Video Technology*, 10(6), 2000, 974-979.
- [10] P. S. Huang, C. S. Chiang, C. P. Chang, and T. M. Tu, Robust spatial watermarking technique for colour images via direct saturation adjustment, *IEE Proc. Vision, Image and Signal Processing*, 152(5), 2005, 561-574.
- [11] E. E. Abdallah, A. B. Hamza, and P. Bhattacharya, A robust block-based image watermarking scheme using fast Hadamard transform and singular value decomposition, *Proc. 18th Int. Conf. on Pattern Recognition*, Hong Kong, 2006, 673-676.