ADAPTIVE WATERMARKING OF COLOR IMAGES IN THE DCT DOMAIN

Ibrahim Nasir, Jianmin Jiang and Stanley Ipson
School of Computing, Informatics and Media,University of Bradford, Bradford BD7 1DP, U.K.

Keywords: DCT domain, DC components, Classification, Adaptive embedding, Watermarking, Color images.

Abstract: This paper presents a new approach of embedding watermarks adaptively in DC components of color images with respect to analysis of the image luminance in the YIQ model or the blue channel in the RGB model. The embedding strength is determined by the classification of DCT blocks, which is simply implemented in the DCT domain via just analyzing the values of two AC coefficients rather than using method such as Sobel, Canny, or Prewitt. Furthermore, a new combination algorithm of both watermark extraction and blind detection is designed, where the watermark is extracted directly in the spatial domain without knowledge of the original image. Experimental results demonstrated that the embedded watermark is robust to the attacks including JPEG-loss compression, JPEG2000, filtering, scaling, small cropping, small rotation-crop and self-similarities attacks.

1 INTRODUCTION

Recently, digital watermarking techniques have been utilized to maintain the copyright of digital data by identifying the owner or distributor of digital data. There are some contradictory requirements in the watermarking process that, on one hand, the embedded watermark should not affect the image quality in a visible manner, but on the other, the watermark should still be extractable from the watermarked media after intentional or unintentional attacks (Petitcolas et al., 1999) and (Hartung et al., 1999).

A wide variety of image watermarking algorithms has been proposed to provide copyright protection of digital images. Most existing watermarking algorithms use key-generated pseudorandom patterns as watermarks and focus mainly on embedding watermarks into the low or the middle frequency coefficients of grey-scale images. The extension to color images is accomplished by marking the image luminance (Kutter, 1998), or by processing each color channel separately. Kutter et al. (1997) proposed a method based on embedding a watermark by modifying a selected set of pixel values in the blue channel, since the human eye is less sensitive to changes in this band. Fleet and Heeger (1997) proposed a method, which takes into account the characteristics of the human visual system (HVS) with respect to color perception. They suggested embedding the watermark into the yellow-blue channel of color images and using S-CIELAB space to measure the color reproduction error. However, their method can only resist printing and rescanning attacks. Barni et al. (2002) introduced another color image watermarking method based on the cross-correlation of RGB channels. However, it has relative high computing costs and low processing speed since the full-frame DCT is used for three color channels. Tsai et al. (2004) provided a solution of embedding the watermark on a quantized color image.

Instead of using AC coefficients to embed a watermark, Huang et al. (2000) suggested that more robustness can be achieved if the watermark is embedded into the DC coefficients of the DCT and demonstrated that the DC coefficients provide more perceptual capacity than AC coefficients. Based on Huang et al. suggestion, watermarks were embedded in DC coefficients of images (Huang et al., 2005) and (Nasir et al., 2008). In (Huang et al., 2005), the watermark embedded into DC coefficients of a color image directly in the spatial domain, followed by a saturation adjustment technique performed in the RGB color space. The main weaknesses of the method presented in (Huang et al., 2005) are as follows: (i) The detection process requires the original image, which may not necessarily available in some applications; (ii) The image contents are not

Nasir I., Jiang J. and Ipson S. (2010).
ADAPTIVE WATERMARKING OF COLOR IMAGES IN THE DCT DOMAIN.
In *Proceedings of the International Conference on Signal Processing and Multimedia Applications*, pages 171-177
DOI: 10.5220/0002895601710177

taken into account when embedding the watermark and, as a result, the maximum-possible imperceptibility and robustness of the embedded watermark cannot be guaranteed. In (Nasir et al., 2008), the watermark was embedded into DC coefficients of gray-scale images without taking into account the content of the image.

Based on the fact that the magnitude of DC coefficients is much larger than any AC coefficients, DC coefficients can provide more perceptual capacity than AC coefficients. On the other hand, DC coefficients are less affected than any AC coefficients when the watermarked is attacked by JPEG compression, lowpass filtering and subsampling operations. Therefore, DC coefficients are suitable for embedding watermark (Huang et al., 2005). Motivated by those observations, in this paper, we propose a new adaptive and blind image watermarking method, which is based on the principle of embedding a watermark in the DC coefficients of subimages in the DCT domain. These subimages are obtained through subsampling the original luminance component Y or the blue component B of color images in the YIQ or the RGB color models respectively. In comparison with existing reported work, our proposed method possesses significant advantages, which can be highlighted as: (i) The watermark is embedded in the DC coefficients to provide more robustness than using AC coefficients; (ii) The watermark is extracted without knowledge of the original non-watermarked image; (iii) The watermark is extracted directly in the spatial domain rather than applying the DCT again to the watermarked image; (iv) The strength of the watermark is determined adaptively to the contents of the host image to guarantee the best possible perceptibility and robustness of the embedded watermark; (v) the DCT and its inverse are applied only to the selected blocks, which are used to embed the watermark.

The rest of this paper is structured as follows. Section 2 describes the adaptive determination of watermarking strength; Section 3 and 4 present the embedding and the extraction processes and Section 5 presents some experimental results. Conclusions are drawn in Section 6.

2 ADAPTIVE DETERMINATION OF WATERMARKING STRENTH

A major challenge in designing a watermarking algorithm is to find a strategy that satisfies the conflicting objectives that, on one hand, the added watermark is imperceptible to the human eyes but, on the other, it should be robust to removal attacks. The best way to achieve better trade-offs between imperceptibility and robustness requirements is to take the characteristics of the non-watermarked image into account when embedding the watermark. Chang et al (2005) proposed a technique for extracting 5 edge patterns directly in the DCT domain, and proved that DCT blocks of size 8×8 can be classified as certain type of edge patterns. Jiang et al. (2008) suggested that three edge patterns rather than five are sufficient to describe and characterize the visual content of the image in the DCT domain. Therefore, the proposed method exploits this block classification scheme to analyze the visual content and hence determine the watermark embedding strength.

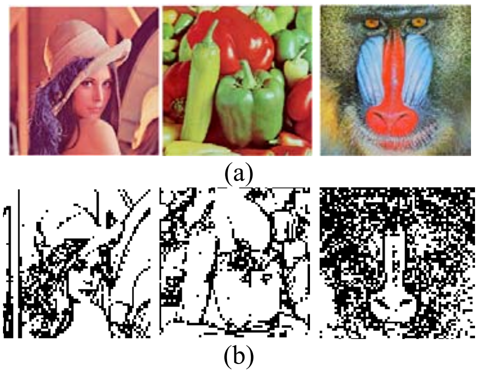
Via exploitation of Jiang's classification scheme, all DCT blocks can be further analyzed as smooth or non-smooth based on the specific values of the two DCT coefficients. Non-smooth blocks are then further classified to determine if they contain both vertical and horizontal edges or contain one of the edge patterns. To determine the embedding strength, we proposed the following adaptive scheme

$$\alpha = \begin{cases} \alpha_{\text{smooth}} & \text{if } \max(\delta_0, \delta_{\pi/2}) < \lambda_1 \\ \alpha_{\text{texture}} & \text{else if } \min(\delta_0, \delta_{\pi/2}) \geq \lambda_2 \\ \alpha_{\text{edge}} & \text{otherwise} \end{cases} \quad (1)$$

where α stands for the embedding strength and, $\delta_0 = |X(1,0)|$, $\delta_{\pi/2} = |X(0,1)|$ are the absolute value of the DCT coefficients X(1,0) and X(0,1), respectively, λ_1 and λ_2 are thresholds. The derivation of δ_0 , $\delta_{\pi/2}$ does not require any addition or multiplication and only two DCT coefficients are used to classify DCT blocks.

Figure 1 demonstrates the classification results obtained by applying the proposed method to images with different textures. As an example, Lena includes large smooth areas with sharp edges; Peppers includes large smooth areas without sharp edges and Baboon includes textured areas.

The white areas shown in Figure 1 are classified as smooth, and thus any small change incurred by watermarking could be visible. As a result, the corresponding watermark should have a low embedding strength. Similarly, the black areas in Figure 1 are classified as edge or textured blocks, and hence changes incurred by watermarking would be less visible. Therefore, the watermark embedding



(a)

(b)

Figure 1: (a) Host images, (b) Classified images.

strength should be arranged as follows:

$$\alpha_{smooth} < \alpha_{edge} < \alpha_{texture}$$

3 ADAPTIVE EMBEDDING OF WATERMARKS

The proposed embedding algorithm can be applied to color images in the YIQ (Luminance, Hue, and Saturation) or in the RGB (Red, Green, and Blue) color models. In the YIQ color model, the gray-scale information is separated from color information; therefore, the Luminance component Y is selected to embed the watermark. In the RGB color model, the blue component B is selected to embed the watermark because the human eyes are less sensitive to changes in this color component (Kutter, 1997). The proposed embedding algorithm consists of five steps. In the first step, four subimages are produced by subsampling the luminance component (Y) or the blue component (B) of a color image as given in (Chu, 2003). In the second step, the embedding positions of the watermark are specified by a secret key, which is used to generate a random sequence $S_L = \{(i,j), i, j \in (1,2,3,4), i \neq j\}$, with the length equal to the length of the watermark, which serves as blocks selector. where L=1, 2,…, the length of the watermark. In the third step, the DCT is applied to non-overlapping blocks of size 8×8 of the two selected subimages, which are selected according to random sequence S_L. In the fourth step, the watermark embedding strength (α) is determined according to the block pattern classification as given in (1). In the final step, watermark bits are embedded in pairs of DC coefficients of the selected blocks of size 8×8 $\{(DC_i, DC_j), (i, j \in S_L)\}$ and leaving the AC coefficients unchanged. The procedure of embedding watermark bits in DC coefficients of blocks of size 8×8 is achieved as follows: 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. Using the modified S_L, the watermark embedding algorithm is defined as follows:

$$DC_{Avg} = \frac{DC_i + DC_j}{2} \tag{2}$$

$$DC_{Diff} = \frac{|DC_i - DC_j|}{2} \tag{3}$$

$$DC_{Threshold} = \frac{DC_{Diff}}{DC_{Avg}} \tag{4}$$

$$DC_i^* = \begin{cases} DC_i & \text{if} \, (DC_{Threshold} > \beta) \\ DC_i + \alpha . DC_{Avg} & \text{elseif} (DC_{Threshold} \leq \beta) \,\&\, (W_L = 1) \\ DC_i - \alpha . DC_{Avg} & \text{otherwise} \end{cases} \tag{5}$$

$$DC_j^* = \begin{cases} DC_j & \mathit{if} \, (DC_{Threshold} > \beta) \\ DC_j + \alpha . DC_{Avg} & \mathit{elseif} \, (DC_{Threshold} \leq \beta) \,\&\, (W_L^* = 0) \\ DC_j - \alpha . DC_{Avg} & \mathit{otherwise} \end{cases} \tag{6}$$

where α is the watermark embedding strength and β is the threshold, DC_i and DC_j are the DC coefficients of the blocks inside the two selected subimages, DC_i^* and DC_j^* are the watermarked DC coefficients, W_L stands for watermark bit and L=1, 2,…, the length of the watermark. The values of the selected pairs of DC coefficients (DC_i, DC_j) are altered if they do not satisfy the embedding threshold β. The embedding depends on the watermark bits as given in Equations (5) and (6). In the case of embedding a watermark bit ‘1’, the value of the DC_i will be increased and the value of the DC_j will be decreased. In the case of embedding a watermark bit ‘0’, the value of the DC_i will be decreased and the value of the DC_j will be increased. The values of the increment and decrement are made large enough depending on the watermark embedding strength α. The proposed method applies the DCT and its inverse only to the selected 8×8 blocks of subimages and uses the DC coefficients of those selected blocks to embed the watermark.

4 WATERMARK ETRACTION PROCESS

The proposed extraction algorithm can be divided into four stages, which include: (i) producing four subimages by subsampling the luminance component (Y) or the blue component (B) of a color image, which is subjected to watermark extraction; (ii) specifying the extraction positions of the watermark using the secret key; (iii) DC coefficients are computed directly in the pixel domain by simple averaging the pixels inside each block as given in (7); and (iv) The watermark extracted bits are determined by comparing the DC coefficients values of selected subimages as given in equation (8).

$$DC = \frac{1}{\sqrt{64}} \sum_{x=0}^{7} \sum_{y=0}^{7} f(x,y) \qquad (7)$$

where $f(x,y)$ stands for the intensity pixel value at location (x,y).

$$W_L = \begin{cases} 1 & \text{if} \quad DC_i^* \geq DC_j^* \\ 0 & \text{otherwise} \end{cases} \qquad (8)$$

where W_L is the extracted bit, $L \in \{1,2,....,N\}$, N represents the length of the watermark, DC_i^* and DC_j^* are DC coefficient values of 8×8 blocks of the selected subimages.

The Correlation coefficient (CC) given in (Huang et al., 2005) is used to measure the similarity between the original watermark and the extracted watermark. An appropriate threshold T is used to make the binary decision as to whether a given watermark is present or not. Figure 2 shows the watermark detector response with 1000 watermark seeds, only one of which is the correct watermark. The threshold T was set as 0.4 and when CC value exceeded this, the existence of the watermark was declared.

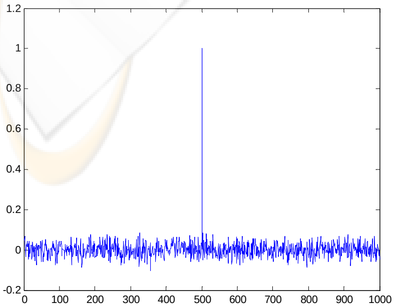


Figure 2: Detector responses for 1000 watermark seeds.

The proposed extraction algorithm possesses the following advantages; (i) The watermark is extracted directly from the watermarked images and yet such extraction is conducted directly in pixel domain rather than applying DCT again to the watermarked image; and (ii) The extraction process is not required the un-watermarked image; which makes the proposed method applicable in a wider range of application than those which require the un-watermarked image for detection.

To achieve the security requirement of the proposed method, the embedding positions of the watermark are determined by a secret key. Therefore, the watermark can not be extracted without knowing the secret key, whose length is equal to the watermark length, long enough to make it impractical for hacking. To achieve the robustness requirement, DC coefficients are selected to embed the watermark because they can provide more perceptual capacity than the AC coefficients and they are less affected than any AC coefficient when the watermarked image is attacked by JPEG compression, low pass filtering or subsampling operations. To achieve better tradeoffs between the requirements for imperceptibility and robustness, the watermark embedding strength is determined adaptively to the image features. The embedding capacity of the proposed scheme depends on the size of the image. For the image with size *M*×*N,* the maximum embedding capacity is given as below

$$C = \left[\frac{M}{8}\right] \times \left[\frac{N}{8}\right] / 2 \qquad (9)$$

5 EXPERIMENTAL RESULTS

In the experiments, the logo used for watermarking was a binary image of size 32×32 and the values of λ_1 and β are defined as given in (Jianmin et al., 2008) and (Lu et al., 2006). The values of watermark embedding strength in the YIQ color model are $\alpha_{smooth} = 0.01$, $\alpha_{texture} = 0.04$, $\alpha_{edge} = 0.025$ and in the RGB color model are $\alpha_{smooth} = 0.07$, $\alpha_{texture} = 0.2$, $\alpha_{edge} = 0.1$. These empirical values are appropriate for various tested images. In the embedding process, the distortion of an image depends on the threshold *β,* the watermark strength *α*, and the length of the watermark. The threshold *β* controls the difference between the watermarked *DC* coefficients. The higher *β*, the more embedding distortion is introduced on the watermarked image as given in equations (5) and (6). Meanwhile, the embedding of the watermark is controlled by the watermark strength α. The classification of the image determines where the watermark should be strong and where the watermark should be weak. The watermark strength α is lower in smooth regions and higher in texture regions. The higher α, the more the distortion is introduced on the watermarked image. Hence, there is a tradeoff between robustness and imperceptibility.

To evaluate the watermark imperceptibility, fifteen different images are tested including Lena, Peppers, Baboon, F16-plane, Barbara, Tiffany, Lake and Couple, etc. The Peak signal to noise ratio (PSNR) is adopted to evaluate the perceptual distortion of the proposed scheme. The PSNR values of the fifteen watermarked images are between 42 and 50 dB. These values are all greater than 30.00 dB, which is the empirically tested threshold value for the image without any perceivable degradation (Qi et al., 2007). Taking Peppers image as examples, the un-watermarked and the watermarked images are shown in Figure 3.

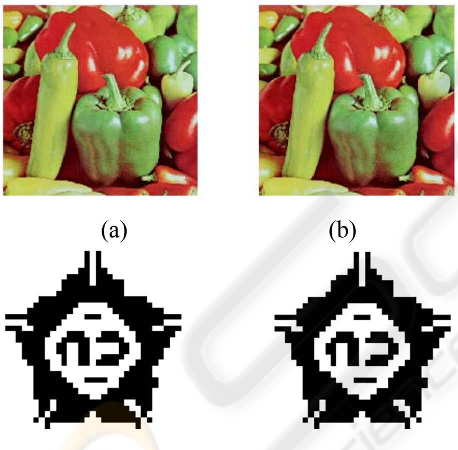

(a) (b)
(c) (d)

Figure 3: (a) Original Peppers image; (b) Watermarked image; (c) original watermark; (d) extracted watermark.

It can be seen that the differences between the corresponding watermarked and un-watermarked images are imperceptibly. The PSNR values between the original and the watermarked images are shown in Table 1.

Various common signal processing and geometric attacks were applied to the watermarked images. Most of these were performed using the benchmark software StirMark 4.0 (Petitcolas et al., 1998) and (Petitcolas et al., 2000). As an example, figure 4 shows the extracted watermarks from watermarked Lena image after filtering attacks include: low-pass, median, Gaussian and mean filtering attacks with 3×3 windows size. As seen, all the extracted watermarks can be visually identified and the detector's response correctly declares the existence of the watermark.

Table 1: PSNR between original and watermarked images.

	Lena	Peppers	Baboon
Proposed YIQ scheme	45.67	43.44	44.37
Proposed RGB scheme	45.75	43.98	43.50
Scheme in (Huang et al., 2005)	44.06	43.23	42.42

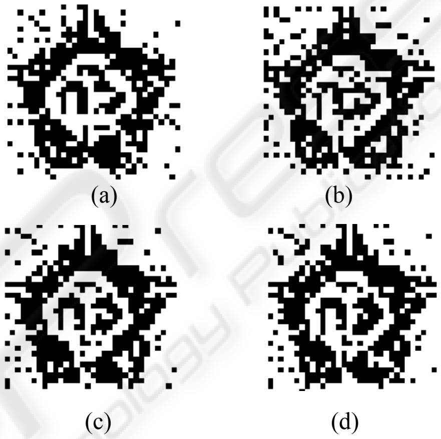
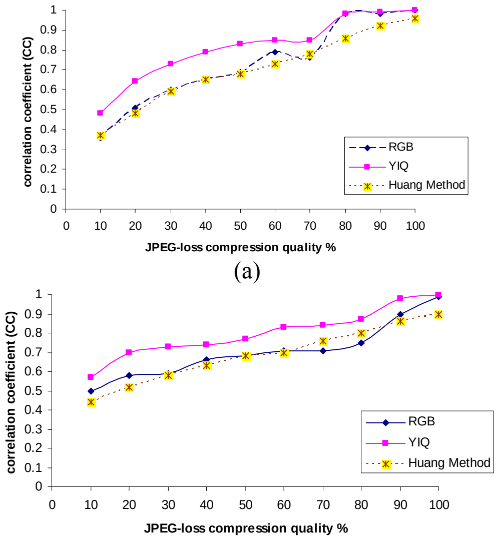

(a) (b)
(c) (d)

Figure 4: Results of attack by (a) low-pass filtering; (b) median filtering(c) Gaussian filtering (d) mean filtering.

Figure 5 (a) and (b) show experimental results from JPEG attacks to the watermarked images 'Lena' and 'Peppers'. As shown, the robustness achieved by embedding the watermark in the luminance component Y is better than embedding the watermark in the blue component. This is because the blue component has characteristic of the highest frequency range than the red and the green components of the RGB and these high frequency components may be discarded by lossy compression quantization. As shown, the proposed method performs better than Huang's method under JPEG compression attack.

Self-similarities (SS) attacks in different color space were applied to the watermarked images. As an example, the results for the Lena image is shown in figure 6. As seen, the proposed method performs well under self similarities attacks.



(a)

(b)

Figure 5: Results of attack by JPEG-loss compression (a), (b) and (c) detector response CC versus JPEG compression quality for Lena and Peppers images, respectively.

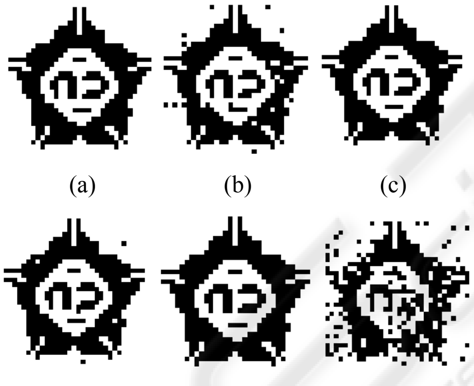


Figure 6: Extracted watermarks after self-similarities attacks where (a), (b) and (c) from RGB color space and (d), (e) and (f) from YIQ color space .(a) and (d) extracted after ss1 attack, (b) and (e) extracted after ss2 attack, (c) and (f) extracted after ss3 attack.

Table 2 summarizes some experimental results by applying several common image processing and some geometric attacks on Peppers and Baboon images watermarked using the proposed method and Huang's method (Huang et al., 2005). It can be seen that, the proposed method performs better than Huang's method under common image processes and some geometric attacks, such as JPEG compression, JPEG2000, scaling by 200%, self-similarities. The extracted watermark can also be correctly identified by the proposed method after filtering attacks. However, Huang's method performs better than our method for filtering attacks. This is because the un-watermarked image was used in the extraction process in Huang's method. By contrast, the proposed method does not require the un-watermarked image, which is not available for most application. The experimental results of the proposed methods show that more robustness can be achieved when the watermark is embedded adaptively to features of the host image.

Table 2: Comparison between the proposed method and Huang's method (Huang et al., 2005) under common image processing and geometric attacks.

	Attack operation on Peppers and Baboon images					
	Huang's method		Proposed method			
	Peppers Baboon		Peppers		Baboon	
			RGB	YIQ	RGB	YIQ
Attack operation	CC	CC	CC	CC	CC	CC
Jpeg 100	0.90	0.59	0.99	1.0	1.0	1.0
Jpeg 50	0.68	0.53	0.68	0.77	0.93	0.95
Jpeg 20	0.52	0.45	0.58	0.70	0.78	0.78
JPEG2000 100	0.98	0.98	1.0	1.0	1.0	1.0
JPEG2000 50	0.68	0.44	0.67	0.71	0.72	0.74
JPEG2000 20	0.56	0.41	0.63	0.68	0.61	0.56
Scaling 2.0	0.90	0.74	0.99	0.97	1.0	0.94
Scaling 0.5	0.88	0.75	0.64	0.70	0.52	0.54
Median filter 7×7	0.81	0.53	0.61	0.56	0.46	0.45
Gaussian filter	0.90	0.90	0.62	0.73	0.69	0.65
3×3	0.94	0.60	1.0	0.96	1.0	0.78
SS1(self	0.93	0.64	0.86	1.0	0.85	1.0
similarity)	0.50	0.42	0.97	0.71	1.0	0.54
SS2	0.57	0.59	0.73	0.75	0.76	0.75
SS3						
Crop 25%						

6 CONCLUSIONS

We have presented a new adaptive color image watermarking scheme based on embedding the watermark adaptively to the features of the host color image in perceptually significant DC coefficients in the DCT domain.

The proposed watermark embedding process takes into account the content of the image to achieve the maximum-possible imperceptibility and robustness of the embedded watermark. The experimental results show that the proposed technique succeeds in making the watermark perceptually invisible and also robust against various signal processing operation and some geometric attacks. The results demonstrate that more robustness is achieved when the watermark embedded in the Luminance component rather than using the blue component.

The performance of the proposed scheme could be improved by taken into account the correlation between RGB bands and color gradients. Moreover, robustness against geometric attacks could be improved by using reference points, which act as synchronization marks between the watermark embedding and detection.

REFERENCES

F. Petitcolas, R. Anderson, and M. Kuhn, 1999. Information hiding-a survey, *Proc. IEEE*, 87(7), pp. 1062-1078.

F. Hartung and M. Kutter, 1999. Multimedia watermarking techniques, *Proc. IEEE*, 87(7), pp. 1079-1107.

M. Kutter, 1998. Watermarking resisting to translation, rotation, and scaling, in: *Proc. Of the SPIE Conf. on Multimedia Systems and Applications*, pp. 423-431.

M. Kutter, F. Jordan, F. Bossen, Digital signature of color image using amplitude modulation, 1997. in: *Proc. Of Storage and Retrieval for Image and Video Database V,* SPIE, vol. 3022, pp. 516-526.

D. Fleet, D. Heeger, 1997. Embedding invisible information in color images, in *Proc. IEEE Int. Conf. on Image Processing*'97, vol. 1, pp. 532-535.

M. Barni, F. Bartlini, A. Piva, 2002. Multichannel watermarking of color image, *Proc. IEEE Trans. On Circuit Systems for Video Technology*, vol. 12(3), pp. 142-156.

P. Tsai, Y.C. Hu, C.C. Chang, 2004. A color image watermarking scheme based on color quantization, Signal Process, pp. 95-105.

J. Huang, Y. Shi, and S. Yi, 2000. Embedding image watermarks in dc components, *Proc. IEEE Transactions on Circuits and Systems for Video Technology*, vol. 10, no. 6, pp. 974-979.

P. S. Huang, C. S. Chiang, C. P. Chang, and T. M. Tu, 2005. Robust spatial watermarking technique for colour images via direct saturation adjustment, *IEEE Proceedings -Vision, Image and Signal Processing*, vol. 152 (5,7), pp. 561-574.

I. Nasir, Y. Weng, J. Jiang, S. Ipson, 2008. Subsampling-based image watermarking in compressed DCT domain, *Proc. 10 the IASTED Int. Conf. on signal and image processing*, pp. 339-344.

K. K. H. S. Chang, A compressed domain scheme for classification block edge patterns, 2005. *Proc. IEEE Transactions on Image Processing*, vol. 14(2), pp.145-151.

J. Jianmin, Q. Kaijin, X. Guogiang, 2008. A block-edge-pattern based content descriptor in DCT domain, *Proc. IEEE Transactions on Circuits and Systems for Video Technology*, vol. 18(7), pp. 994-998.

W. C. Chu, 2003. DCT-based image watermarking using subsampling, *Proc. IEEE Transactions on Multimedia, vol. 5*(1), pp. 34-38.

W. Lu, H. Lu, and F. Chung, 2006. Robust digital image watermarking based on subsampling, *Applied Mathematics and Computation*, vol. 181, pp. 886-893.

X. Qi and J. Qi, 2007. A robust content-based digital image watermarking scheme, *Signal Processing*, 87 (6), 1264-1280.

F. A. P. Petitcolas, 2000. Watermarking schemes evaluation, *Proc. IEEE Signal Processing Magazine, vol. 17*(5, pp. 58-64.

F. Petitcolas, R. Anderson, and M. Kuhn, 1998. Attacks on copyright marking systems, *Proc. 3rd Int. Int. workshop on Information Hiding*, vol. 1525, Lecture Notes in Computer Science, pp. 218-238.