International Journal of Computer and Communication Technology

Volume 2 | Issue 1 Article 11

January 2011

A Robust Algorithm of Digital Image Watermarking Based on Discrete Wavelet Transform

Shital Gupta
Department of Computer Science & Engineering, LNCT, Bhopal, shitalbehare@yahoo.co.in

SANJEEV JAIN Professor
Madhav Institute of Technology and Science, Gwalior, dr_sanjeevjain@yahoo.com

A Robust Algorithm of Digital Image Watermarking Based on Discrete Wavelet Transform

Shital Gupta, Dr Sanjeev Jain
Department of Computer Science & Engineering, LNCT, Bhopal
shitalbehare@yahoo.co.in, dr_sanjeevjain@yahoo.com

Abstract

In this paper, a robust algorithm of digital image watermarking based on discrete wavelet transform is introduced It uses blind watermarking technique.

Digital image watermarking is one such technology that has been developed to protect digital images from illegal manipulations. In particular, digital image watermarking algorithms which are based on the discrete wavelet transform have been widely recognized to be more prevalent than others. This is due to the wavelets' excellent spatial localization, frequency spread, and multi-resolution characteristics, which are similar to the theoretical models of the human visual system.

Keywords:
Digital Image watermarking, DWT, Multiresolution

INTRODUCTION

Like every coin, which has two sides, the digital media also has its own share of problems. The ease of accessibility of digital media and the simplicity of the digital systems has rendered the contents over the digital media highly insecure. Digital entities can be easily duplicated, manipulated, or even tampered. Thus the question of copyright is associated with a digital entity that faces a severe threat from hackers. Engineers have accepted this challenge in a gallant way. Many techniques have been devised to protect the copyright of digital entities. The technique of digital watermarking is one of the growing fields in which this problem of copyright has been addressed elegantly. The digital watermark is a secret code or image hidden inside the original image, so as to claim for the copyright of that image. Thus the process by which the copyright information is embedded invisibly inside the original entity, which is to be protected from the illegal replication and distribution is known as “Digital Watermarking”.

The success of the watermarking Scheme largely depends upon the choice of the watermark structure and insertion strategy. The two main constraints involved in the problem of watermarking are those of maintaining the robustness of the watermark information while keeping visual perception of the original image intact. If the insignificant portions of the original image are used for hiding the watermark structure then the visual perceptions of the original image may remain unaffected but the robustness of the technique decreases. On the other hand if the

hiding is done in the significant portions of the original image then the robustness of the technique increases at the cost of visual perceptions.

In watermarking the attacks on the original data can be classified as Intentional and unintentional. Unintentional attacks include the common signal processing such as low pass filtering, median filtering, digital to analog and analog to digital conversion, re-sampling and requantization, and common geometric distortions such as rotation, translation, cropping and scaling. Intentional attacks include collusion and forgery. Watermarking techniques can be classified in several ways. According to the need of the original image for watermark extraction or detection, watermarking is classified to nonblind and blind watermarking techniques, such as , require that the original image exists when detecting the watermark, whereas, blind techniques do not. Another way to classify watermarking is by how the watermark is inserted; in the spatial domain, or in the transform domain. Early watermarking schemes that were introduced, worked in the spatial domain, where the watermark is added by modifying pixel values of the host image. Some of the spatial domain watermarking approaches were based on the modification of the least significant bit (LSB) of an image based on the assumption that the LSB data are insignificant Generally, spatial domain watermarking is easy to implement from a computational point of view, but too fragile to resist numerous attacks . In order to have more promising techniques, researches were directed towards watermarking in the transform domain, where the watermark is not added to the image intensities, but to the values of its transform coefficients. Then to get the watermarked image, one should perform the

transform inversely. Some of the transform based watermarking techniques used the Discrete Cosine Transform (DCT)[2,3,4,5,6] .The wavelet transform is another type of the transform domain. Wavelet based transform gained popularity recently since the property of multiresolution analysis that it provides. However, DWT [11]has been used in digital image watermarking more frequently due to its excellent spatial localization and multi-resolution characteristics, which are similar to the theoretical model of human visual system. Further performance improvements in DWT –based digital image watermarking algorithms could be obtained by combining DWT with DCT. The idea is based on the fact that combined transforms could compensate for the drawbacks of each other, resulting in effective watermarking. In this paper, we will describe a digital image watermarking algorithm based on combining two transforms; DWT and DCT. Watermarking is done by altering the wavelets coefficients of carefully selected DWT sub-bands, followed by the application of the DCT transform on the selected sub-bands. In order for a digital watermarking method to be effective it should be imperceptible, and robust to common image manipulations like compression, filtering, rotation, and scaling, cropping, collusion attacks among many other digital signal processing operations. In this paper, we will describe a digital image watermarking algorithm based on combining two transforms; DWT and DCT [13, 14]. Watermarking is done by altering the wavelets coefficients of carefully selected DWT sub-bands, followed by the application of the DCT transform on the selected sub-bands.

In this paper, we will describe a digital image watermarking algorithm based on combining two transform s DWT & DCT .Watermarking is done altering the wavelet coefficient of selected sub bands ,followed by the application of DCT transform on the selected subbands.The rest of this paper is organized as follows. Section 2 describes the watermarking embedding procedure in detail.In section 3 describes the watermarking extraction procedure. Section 4 describes the performance evalution.The conclusion in section 5.

2. Watermark Embedding Procedure

The main strength offered by transform domain techniques is that they can take advantage of special properties of alternate domains to address the limitations of spatial domain or to support additional features. We start the watermarking process by applying DWT to the host image, and afterwards performing the DCT to the selected DWT sub-bands. The agreement adopted by many DWT-based watermarking methods, is to embed the watermark in the middle frequency sub-bands HLX and LHX is better in perspective of imperceptibility and robustness. Consequently, HLX sub-bands in level three is chosen for Performing DCT on them. The Watermark embedding procedure is represented in

Figure 1.followed by a detailed explanation.

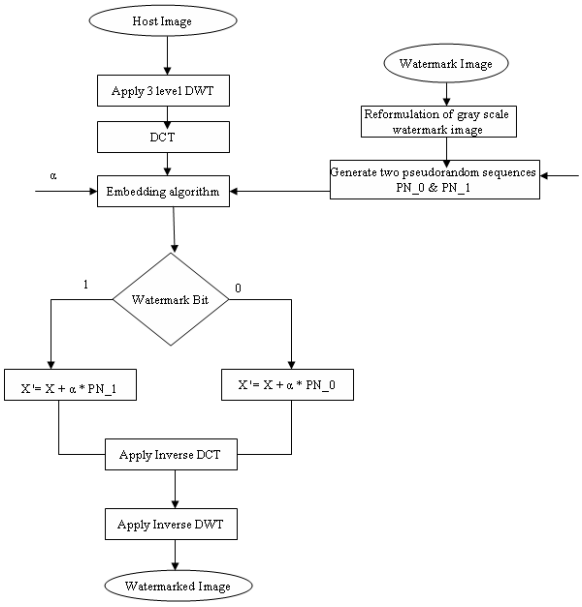


Fig1: Flowchart for watermark embedding technique

Step 1: Perform DWT on the host image to decompose it into four non-overlapping multiresolution coefficient sets: LL_1, HL_1, LH_1 and HH_1.

Step 2: Perform DWT again on two HL_1 and LH_1 sub-bands to get eight smaller sub-bands and choose four coefficient sets: HL_{12}, LH_{12}, HL_{22} and LH_{22} as shown in Figure 2. (a).

Step 3: Perform DWT again on four sub-bands:HL_{12}, LH_{12}, HL_{22} and LH_{22} to get sixteen smaller Subbands and choose four coefficient sets: HL_{13}, LH_{13}, HL_{23} and LH_{23} as shown in Figure 2. (b).

Step 4: Divide four coefficient sets: HL_{13}, LH_{13}, HL_{23} and LH_{23} into 4 x 4 blocks.

Step 5: Perform DCT to each block in the chosen coefficient sets (HL_{13}, LH_{13}, HL_{23} and LH_{23}).

Step 6: Re-formulate the grey-scale watermark image into a vector of zeros and ones.

Step 7: Generate two uncorrelated pseudorandom sequences by a key. One sequence is used to embed the watermark bit 0 (PN_0) and the other sequence is used to embed the watermark bit 1 (PN_1). Number of elements in each of the two pseudorandom sequences must be equal to the number of mid-band

elements of the DCT-transformed, DWT coefficient sets.

Step 8: Embed the two pseudorandom sequences, PN_0 and PN_1, with a gain factor α in the DCT coefficients. If we donate X as the matrix of the midband coefficients of the DCT transformed block, then embedding is done as follows:

If the watermark bit is 0 then

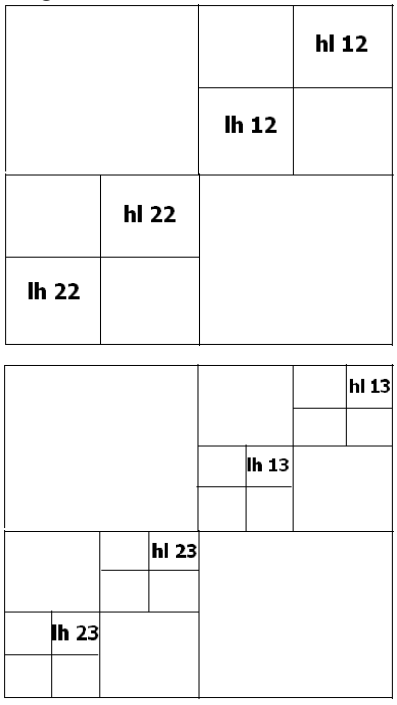
$X' = X + \alpha * PN\_0$ (1)

If the watermark bit is 1 then

$X' = X + \alpha * PN\_1$ (2)

Step 9: Perform inverse DCT (IDCT) on each block after its mid-band coefficients have been modified to embed the watermark bits as described in the previous step.

Step 10: Perform the inverse DWT (IDWT) on the DWT transformed image, including the modified coefficient sets, to produce the watermarked host image



(a) (b)

Figure2.(a)Four multi-resolution DWT Subbands of the original image in level 2 ; (b) four selected multiresolution DWT coefficient sets of the host image in level 3.

3. Watermark Extraction Procedure

The watermark extraction procedure is shown in fig 3.The Combined DWT-DCT algorithm is a blind watermarking algorithm & in this the original host image is not required to extract watermark.

transformed 4x4 blocks of the selected DWT coefficient sets of the host image. Embedding is not applied to all coefficients of the DCT block, but only to the mid-band DCT

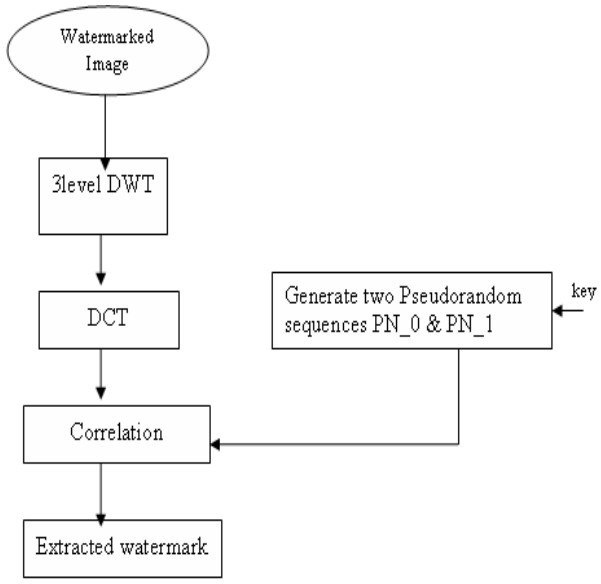


Fig3: Flowchart for watermark extraction

Step 1: Perform DWT on the pre-filtered watermarked image to decompose it into four nonoverlapping multi-resolution coefficient sets: LL_1, HL_1, LH_1 and HH_1.

Step 2: Perform DWT again on two sub-bands HL_1 and LH_1 to get eight smaller sub-bands and choose four coefficient sets: $_{HL12,}$ LH_{12}, HL_{22} and LH_{22} as shown in figure 2 a.

Step 3: Perform DWT again on four sub-bands:HL_{12}, LH_{12}, HL_{22} and LH_{22} to get sixteen smaller subbands and choose four coefficient sets: HL_{13}, LH_{13}, HL_{23} and LH_{23} as shown in figure 2 b.

Step 4: Divide four coefficient sets: HL_{13}, LH_{13}, HL_{23} and LH_{23} into 4 x 4 blocks.

Step 5: Perform DCT on each block in the chosen coefficient sets (HL_{13}, LH_{13}, HL_{23} and LH_{23}).

Step 6 Regenerate the two pseudorandom sequences (PN_0 and PN_1) using the same key which used in the watermark embedding procedure.

Step 7: For each block in the coefficient sets: HL_{13}, LH_{13}, HL_{23} and LH_{23} calculate the correlation between the mid-band coefficients and the two generated pseudorandom sequences (PN_0 and PN_1). If the correlation with the PN_0 was higher than the correlation with PN_1, then the extracted watermark bit is considered 0, otherwise the extracted watermark is considered 1.

Step 8: The watermark is reconstructed using the extracted watermark bits, and compute the similarity between the original and extracted watermarks.

4. Performance Evaluation

We evaluated the performance of the image watermarking algorithms using a 256*256 'Rose' as the original cover host image, and a 20*50 grey-scale image of the expression 'copyright' as the watermark image. The two images are shown in Fig. 4 and 5, respectively. In our Experiment we have set gain factor α=0.2.

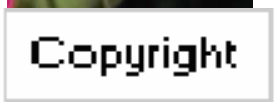
Imperceptibility: Imperceptibility means that the perceived quality of the host image should not be distorted by the presence of the watermark. As a measure of the quality of a watermarked image, the peak signal to noise ratio (PSNR) is typically used. PSNR in decibels (dB) is given below in Eq.3

$$\mathrm{PSNR}_{dB} = 10 \cdot \log_{10}\left(\frac{\mathrm{MAX}_I^2}{\mathrm{MSE}}\right) = 20 \cdot \log_{10}\left(\frac{\mathrm{MAX}_I}{\sqrt{\mathrm{MSE}}}\right) \quad (3)$$

Robustness: Robustness is a measure of the immunity of the watermark against attempts to remove or degrade it, internationally or unintentionally, by different types of digital signal processing attacks [17]. In this chapter, we will report on robustness results which we obtained for four major digital signal processing operations (attacks): Gaussian noise, image compression and image rotation image cropping. The three attacks are a few, however, they are good representatives of the more general attacks. That is the Gaussian noise is a watermark degrading attack, JPEG compression is a watermark removal attack and cropping is a watermark dispositioning geometrical attack. We measured the similarity between the original watermark and the watermark extracted from the attacked image using the Normalized correlation factor given below in Eq 4

$$\textit{Normalized Correlation } (NC) = \frac{\sum_i \sum_j w(i,j)\tilde{w}(i,j)}{\sum_i \sum_j [w(i,j)]^2} \quad (4)$$

. This provides objective judgment of the extracting fidelity. If NC>T, a preset threshold, it indicates that the extracted corrupted watermark can be identified by human eyes. Here T is selected to be 0.75 representively in our work. The performance analysis results are cited inTable 1.



(a)

(b)

Fig. 4a: 'Rose' host image. 4b: Original Watermark

Fig 5a: Watermarked image Fig5b Extracted Watermark, PSNR=41.1613

Figure 5(a) shows the watermarked “Rose” image and the PSNR(peak signal to noise ratio)of the watermarked “Rose” image is about 41.1613 dB.Figure 5(a) demonstrates the watermark embedded with the proposed algorithm is invisible. Figure 5(b) shows the recovered watermark & it is the same as original one.

The compression is the one of the most important attack the watermark should be resistant to this attack.

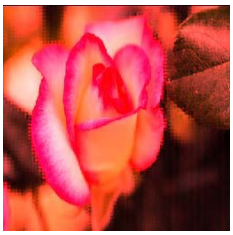


Fig6:The watermark retrieved from the watermark image “Rose” after jpeg Compression (Compression ratio=0.77 and psnr 41.1613 NC=1)

Cropping is a geometric manipulation in practical applications. The watermark turns out very resistant against cropping algorithm.

Fig7:The watermarked retrieved from the watermarked image after cropping. cropping 25% with NC=0.7576

Rotation is a geometric distortion in practical applications. The watermark turns out very resistant against Rotation algorithm.

Fig 8 The watermarked retrieved from the watermarked image after rotation. rotation 20 degree anticlockwise with NC=0.5598.

From the other data in Table 1, we can see that the performance of our algorithm against the compression and denoising attack. Additional, the proposed watermarking algorithm is robust to most of the image processing attacks. Thus the proposed watermarking algorithm can be used for protecting the copyrights of digital images. It can be observed from table 1 that the proposed method provides better results in geometrical rotation and cropping attack.
However, the image rotation attack can break the watermark by desynchronizing the spatial relationships between the original and watermarked images.

5. CONCLUSION

The discrete wavelet transforms (DWT) and the discrete cosine transform (DCT) have been applied successfully in many in digital image watermarking. In this paper, we described a combined DWT-DCT digital image watermarking algorithm. Watermarking was done by embedding the watermark in the first, second level and third level DWT sub-bands of the host image, followed by the application of DCT on the selected DWT sub-bands. Implementation results show that the imperceptibility of the watermarked image is acceptable. The watermarks can be extracted from the most of the common image processing attack with high Normalized correlation values. In conclusion, in DWT-based digital watermarking applications, combining appropriate transforms with the DWT may have a positive impact on performance of the watermarking system.

Attack	**PSNR**	**NC**
No Attack	41.1613	1
JPEG Compression	38.6302	1
Salt & Pepper (20%)	35.3782	0.9983
Rotation (20degree)	17.7241	0.5598
Cropping (25%)	30.2715	0.7576

Table1.Results of the experiments using PSNR and NC metrics for Fidelity and robustness

References

[1] Y. Kim, Kwon, and R. Park, "Wavelet Based Watermarking Method for Digital Images Using the Human Visual System", Proceeding of IEEE International symposium on circuits and systems, Vol. 4, pp. 80-83. July 1999.
[2] Lin, S. and C. Chin, "A Robust DCT-based Watermarking for Copyright Protection," IEEE Trans.Consumer Electronics, 46(3): 415-421, 2000.
[3] Wu, C. and W. Hsieh, "Digital watermarking using zero tree of DCT," IEEE Trans. Consumer Electronics, vol. 46, no. 1, pp: 87-94, 2000.
[4] Nikolaidis, A. and I. Pitas, "Asymptotically optimal detection for additive watermarking in the DCT and DWT domains," IEEE Trans. Image Processing, 2(10): 563-571, 2003.

[5] Chu, W, "DCT-Based Image Watermarking Using Sub sampling," IEEE Trans. Multimedia, 5(1): 34-38, 2003.
[6] Deng, F. and B. Wang, "A novel technique for robust image watermarking in the DCT domain," in Proc. of the IEEE Int. Conf. on Neural Networks and Signal Processing,vol. 2, pp: 1525-1528, 2003.
[7] M.S. Hsieh, and D.C. Tseng , "Hiding digital watermarks using multi-resolution wavelet transform", IEEE Transactions on industrial electronics, vol. 48, No. 5, pp 875-882, Oct, 2001.
[8] H. Guo, and N. Georganas, "Multi-resolution Image Watermarking Scheme in the Spectrum Domain," proceeding of IEEE Canadian Conference on Electrical and Computer Engineering, pp. 873-878, May, 2002.
[9] Reddy, A. and B. Chatterji, "A New Wavelet Based Logo-watermarking Scheme," Pattern Recognition Letters,26(7): 1019-1027, 2005
[10] Wang, S. and Y. Lin, "Wavelet Tree Quantization for Copyright Protection Watermarking," IEEE Trans. Image Processing, vol. 13, no. 2, pp: 154-164, 2004.
[11] Tay, P. and J. Havlicek, "Image Watermarking Using Wavelets," in Proc. of the IEEE Midwest Symposium on Circuits and Systems, pp: 258-261, Oklahoma, USA, 2002.
[12] Wolfgang, R., C. Podilchuk and E. Delp, "Perceptual Watermarks for Digital Images and Video," Proc. of the IEEE, vol. 87, no. 7, pp: 1108-1126, 1999.
[13] Tsai, M. and H. Hung, "DCT and DWT based Image Watermarking Using Sub sampling," in Proc. of the IEEE Fourth Int. Conf. on Machine Learning and Cybernetics, pp: 5308-5313,China, 2005.
[14] Ali Al-Haj, "Combined DWT-DCT Digital Image Watermarking" Journal of Computer Science 3 (9): 740-746, 2007.