Spatial and Frequency Domain for Grey level Digital Images

Dharm Singh
Department of Computer Science &Engineering
College of Technology and Engineering, MPUAT
Udaipur, India

Naveen Choudhary
Department of Computer Science &Engineering
College of Technology and Engineering, MPUAT
Udaipur, India

Madhuri Agrawal
Department of Computer Science &Engineering
College of Technology and Engineering, MPUAT
Udaipur, India

ABSTRACT

With the gradual maturation of multimedia technology and the rapid development of network technology, it becomes more convenient to access and disseminate digital information, such as digital images, audio and digital video. Currently, the rapid escalation of the Internet has made the issue of protecting copyrights of digital contents very much important. Therefore digital watermarking technology is the most commonly researched and applied method to protect intellectual property rights. The paper acquaints the comparative study of Spatial and Frequency domain watermarking scheme for copyright protection of digital images with the purpose of defending against digital piracy. A novel scheme to embed and extract binary image watermarking in gray image based on LSB and DCT domain with their comparative results are also presented. The paper recommends frequency based techniques for achieving imperceptibility and robustness in digital image watermarking. By the use of Matlab software, the efficiency of the proposed watermarking scheme has been demonstrated via the experimental results.

Keywords

Spatial domain, frequency domain, LSB, DCT, PSNR, normalized Correlation (NC), attacks.

1. INTRODUCTION

With the rapid spread of computer networks and the further development of multimedia technologies, the copyright protection of digital contents such as audio, image and video, has been one of the most serious problems because digital copies can be made identical to the original. The digital watermark technology is now drawing attention as a new method of protecting copyrights of digital contents. A digital watermark is realized by embedding information data directly into digital contents with an imperceptible form for human audio-visual systems, and should satisfy the following requirements: The embedded watermark should not spoil the quality of the original contents and should not be perceptible. It should be difficult for an attacker to remove the watermark and should be robust to signal processing and geometric distortions. By it we can identify where the image came from or who has rights to it. A watermarking scheme should at least require the following properties: robustness, visual quality (imperceptibility), and security [1]. Additionally, the watermark should survive after various intentional and unintentional attacks. Such attacks may include image compression, smoothing, sharpening, geometric transformations (such as translation, rotation and scaling), additive noise, printing and scanning, and any other attempts to remove the watermark or confuse the watermark reading system [2].

Watermarking techniques may be classified in different ways. The classification may be based on the type of watermark being used, i.e., the watermark may be a visually recognizable logo or a sequence of random numbers. A second classification is based on whether the watermark is applied in the spatial domain or the transform domain. The earlier watermarking techniques were almost spatial domain approaches. The simplest method is based on embedding the watermark in the least significant bits (LSBs) of image pixels. However, spatial domain techniques are not resistant enough to image compression and other image processing. For example, a simple low-pass filtering may eliminate the watermark. Transform domain watermarking schemes such as those based on the discrete cosine transform (DCT) [3,4], the discrete wavelet transform (DWT) [5] or statistical moments [6] typically provide higher image fidelity and are much more robust to image manipulations.

The rest of the paper is organized as follows: Section 2 presents a brief review of the spatial domain watermarking technique and then the frequency domain based DCT technique is presented in Section 3. The experimental results are given in Section 4 and conclusions are summed up in Section 5.

2. SPATIAL DOMAIN WATERMARKING

In *spatial domain* methods, the watermark are embedded using LSB, Statistical, Feature based and Block based techniques. Spatial-domain techniques work with the pixel values directly. The images are generally manipulated by altering one or more of the bits of the byte that make up the pixels of the image. Generally, spatial domain watermarking is easy to implement from a computational point of view, but too fragile to resist numerous attacks [7].

2.1 Least significant bit (LSB)

LSB algorithm is very simple, strong, real time, embedded stack information and can be accurate resume embedded information. The embedding of the watermark is performed choosing a subset of image pixels and substituting the least significant bit of each of the chosen pixels with watermark bits. It is based on the substitution of LSB plane of the cover image with the given watermark [8]. The asset is image A and the watermark image is B. N is a parameter that shows the embedding depth. Suppose that we have 8-bit images. The algorithm says that: N left-sided bits of the image B should be replaced with the N right-sided bits of the image A for each pixel (represented in 8-bit format). In this way, most significant bits or equally important information of image B is watermarked in the place of least significant bits or details

of the image A. Fig. 1 shows the original rock_scene image and corresponding watermarked image.

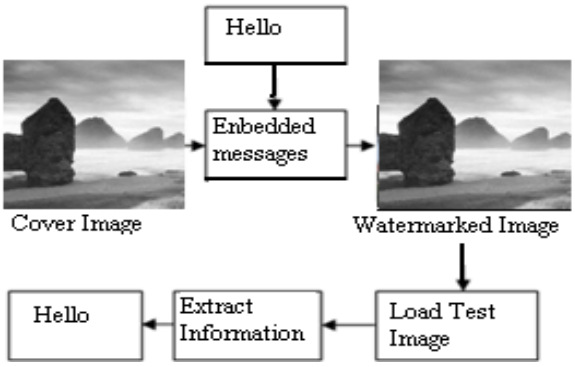


Fig 1: Least Significant bit substitution [9]

Extraction of the watermark is performed by extracting the least significant bit of each of the selected image pixels. If the extracted bits match the inserted bits, then the watermark is detected. The function takes input as a cover image and a watermark while the other function should take input as a watermarked image and give the extracted watermark as output. The functions should be called as lsb_embed and lsb_recovered.

3. FREQUENCY DOMAIN WATERMARKING

In *frequency domain* methods, the watermark information is embedded in the transform domain. The general approach used is by mapping the image to be watermarked into the transform domain using Discrete Cosine Transform (DCT), the Discrete Fourier Transform (DFT), or the Wavelet Transform. In order to achieve robustness, imperceptibility, and security, the frequency domain watermarking techniques are often used.

3.1 Discrete cosine transform (DCT)

Discrete-Cosine-Transform or DCT is a popular transform domain watermarking technique. The DCT allows an image to be broken up into different frequency bands namely low frequency sub band, mid-frequency sub-band and high frequency sub-band thus making it easier to to choose the band
in which the watermark is to be inserted. It represents an image as a sum of sinusoids of varying magnitudes and frequencies.

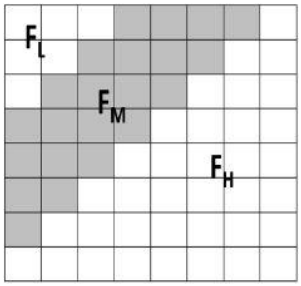


Fig 2: Definition of DCT Regions [10]

DCT of the image is taken in a block dimension of 8*8 resulting in DCT blocks of dimension 8*8. A DCT block consists of three frequency bands. FL is used to denote the lowest frequency components of the block, while FH is used to denote the higher frequency components. FM is the middle frequency band and is chosen for embedding copyright information. This provides additional resistance to lossy compression techniques which targets the high frequency components, while avoiding significant modification of the cover image.

The idea in this algorithm is very similar to DFT amplitude modulation. The popular block-based DCT transform segments an image non-overlapping block and applies DCT to each block. DCT-based watermarking is based on two facts. The first fact is that most of the signal energy lies at low-frequencies sub band which contains the most important visual parts of the image. The second fact is that high frequency components of the image are usually removed through compression and noise attacks. The watermark is therefore embedded by modifying the coefficients of the middle frequency sub band so that the visibility of the image will not be affected and the watermark will not be removed by compression. Block based DCT is one of the commonly used transform. Overall, this digital watermarking algorithm is robust in lossy compression and low-pass filtering [11].
The Two dimensional *DCT* of an *M* by *N* matrix is defined as follows [12]:

$$C(p,q) = a_p a_q \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} I(m,n)\cos\frac{\pi 2(m+1)p}{2M}\cos\frac{\pi(2n+1)q}{2N}$$

And the inverse DCT (or IDCT) is given by:

$$I(m,n) = \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} a_p a_q\, C(p,q)\cos\frac{\pi 2(m+1)p}{2M}\cos\frac{\pi(2n+1)q}{2N}$$

Where

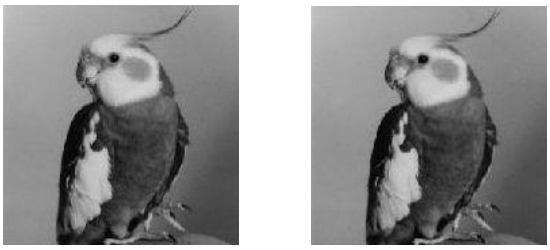
$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}} & ,p=0 \\ \sqrt{\frac{2}{M}} & ,1 \le p \le M-1 \end{cases}$$

$$\alpha_q = \begin{cases} \frac{1}{\sqrt{N}} & ,q=0 \\ \sqrt{\frac{2}{N}} & ,1 \le q \le N-1 \end{cases}$$

The values $C(p, q)$ are called the DCT coefficients of image *I*.

3.1.1 DCT based Embedding Methodology

The technique embeds the watermark in the DCT domain to increase the robustness of the watermarking scheme against JPEG compression. There are two major processes, encoding and embedding processes. In the encoding process the image is break into 8 x 8 blocks then apply the DCT function and computing all the image blocks separately and converting them into frequency components based on the frequency domain and having the whole details and components of the cover image and the watermark converted from the spatial domain into the frequency domain. Secondly, the embedding process is where the DCT is taken for each 8x8 block of the image. For each DCT block, the middle frequency components F_M are added to the pseudo number sequence W, multiplied by a gain factor (k). Coefficients in the low and high frequencies are copied over to the transformed image unaffected. Each block is then inverse-transformed to give us our final watermarked image. The embedding algorithm needs to carefully choose where to embed the watermark bits in the 8x8 block. As a result, the watermarked image will be attained.



Cover Image **Watermarked Image**

Fig 3: Embedding Technique for 256 x 256 pixel image using DCT

Cover Image **Watermarked Image**

Fig 4: Embedding Technique for 512 x 512 pixel image using DCT

3.2.2 DCT based Extraction Methodology

Watermark detection could be attained by a blind detection either non-blind watermark detection. For detection of the watermark in the image, the image is broken up again into same 8*8 blocks, and a DCT performed. The same PN sequence is then compared to the middle frequency values of the transformed block. If the correlation between the sequences exceeds some threshold T, a "1" is detected for that block; otherwise a "0" is detected. Again k denotes the strength of the watermarking, where increasing k increases the robustness of the watermark. It can be done in two operations, detecting and extracting process. Through the first operation, we need to have the cover image, the watermarked image either the watermark signature and break them up into 8 x 8 blocks. Then we apply the DCT function and transform them into the frequency domain. The extracting process can then start by identifying the middle frequency components (FM region) for the images and selecting their two coefficients by means of the quantization table. So that reduced images can be generated and applied to the watermark blocks and start to detect the bits where the watermark was embedded into therefore, the watermark signature will be extracted. The main difference between most algorithms is that they differ either in the block selection criteria or coefficient selection criteria.

Fig5: Extraction Technique for 256 x 256 pixel image using DCT

Fig6: Extraction Technique for 512 x 512 pixel image using DCT

4. EXPERIMENTAL RESULTS

We carry on a large number of simulation experiments of both watermarking algorithms under the environment of MATLAB R2008b. In the experiments, we evaluated the performance of the algorithm using a 512x512x8 bit standard gray 'rock_scene.bmp' image, shown in Figure 4, and also with a 256x256x8 bit grey-scale image 'bird.bmp' having a 'message_copyright' as the watermark image, Figure 5. For quantitative evaluation, PSNR (Peak Signal-to-Noise Ratio) is introduced to evaluate the performance of the proposed scheme and image quality, which is defined as

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

$$MSE = \sum_{i=0}^{n-1}\sum_{j=0}^{m-1}((a_{i,j} - b_{i,j})^2)/(n*m)$$

Where m × n is the image size, ai,j and bi,j are the corresponding pixel values of two images[13].

3.2.2.1 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.

3.2.2.2 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. If the extracted watermark image is absolutely tally with the origin watermark image, the normalized Correlation (NC)=1. Otherwise the NC is between 0 to 1. The extracted watermark image is more tally with the origin watermark image, the NC is more bigger. Table I shows the similarity (correlation) values between the original watermark and the extracted watermark for LSB technique while Table 2 shows the same similarity (correlation) values for DCT technique [14].

$$NC = \frac{\sum_{i=0}^{N}\sum_{j=0}^{M} W(i,j) * W^*(i.j))}{\sum_{i=0}^{N}\sum_{j=0}^{M}[W(i,j)]^2}$$

Where,
W (i, j) = Original watermark image
W*(i, j) = Extracted watermark image
N and M = Width and height of the watermark image

Table 1. Showing Experimental Results for the LSB watermarking technique

Parameters	LSB	
Image	Rock_scene.bmp	Bird.bmp
Image Size	512x512	256x256
PSNR	191.170	145.430
MSE	-3.0349	-3.0233
MAE	-3.0349	-3.0233
NC	1.0000	0.9867

Table 2. Showing Experimental Results for the DCT watermarking technique

Parameters	DCT	
Image	Rock_scene.bmp	Bird.bmp
Image Size	512x512	256x256
PSNR	267.187	190.658
MSE	-1.8491	-2.8230
MAE	-9.1296	5.9657
NC	1.0000	1.0063

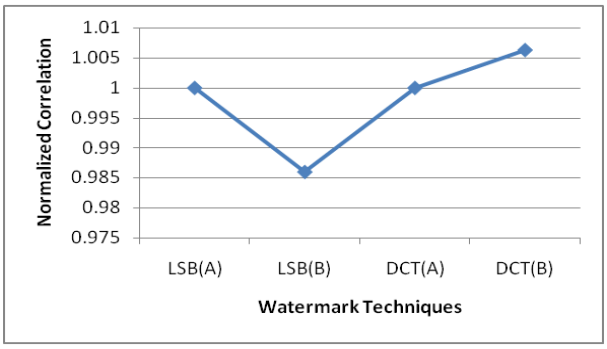


Fig7: NC obtained by LSB and DCT domain for both images

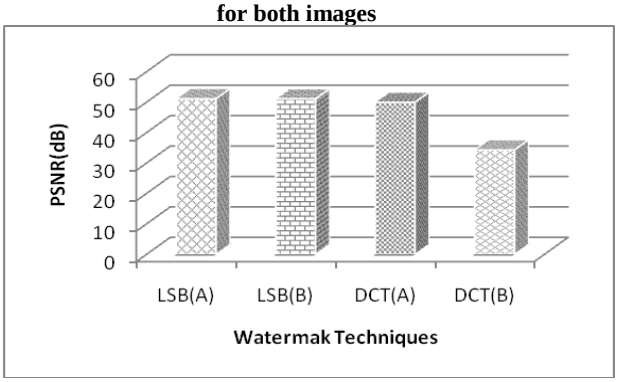


Fig8: PSNR obtained by LSB and DCT domain for both images

To test the robustness of the schemes, some typical signal processing attacks such as filtering, gaussian noise, salt & pepper noise, cropping and rotation are also performed.

Table 3. Showing PSNR (dB) values undergone different attacks for the 512x512 image

Attacks	Rock_scene image	
	LSB	DCT
Median Filtering(3,3)	32.5976	32.6498
Median Filtering(5,5)	30.0846	30.0960
Gaussian noise	20.4221	20.4078
Salt & pepper	17.9871	17.9785
Cropping_50	26.1553	26.1598
Cropping_100	14.0664	14.0665
Rotation_45	6.2192	6.2322
Rotation_90	8.1400	8.1614

5. CONCLUSION

In this paper, a study of watermarking based scheme on Least Significant Bit (LSB) and the discrete cosine transform (DCT) under spatial n frequency domain has been conducted respectively. These have been applied successfully in 512x512 and 256x256 pixel digital images. In contrast to the spatial-domain-based watermarking, frequency domain based techniques can embed more bits of watermark and are more robust to attack. Online application of watermarking for video in the spatial domain becomes cumbersome due to associated high computational complexities involved. On the other hand, Watermarking in the DCT domain needs preprocessing operations such as inverse entropy coding and inverse quantization. However computation cost of frequency domain is higher comparatively but they are mainly used for copyright protection rather than authentication as in the case of spatial domain. Here values for peak signal to noise ratio (PSNR) and normalized correlation (NC) are measured. The results indicate the DCT method introduces low noise and hence ensures lesser visible distortions. The experimental results clearly demonstrate the much improved performance of the DCT domain in terms of imperceptibility and robustness as compared to the LSB domain.

6. Future Work

Further studies could go towards improving the watermarking program and adding extra functionality. One of the method includes having multiple watermarks for a single image, so that different parts of the image have a different watermark. Also concentration can be on improving the technique for robustness to withstand geometric attacks such as cropping,scaling and rotation. A Video is a sequence of images, called as frames, and these frames are more or less same with slight changes and thus position of patches may not vary considerably in adjacent patches. This property may be exploited to derive a new technique for watermarking on videos. The Hybrid watermarking and Hybrid Fractal-Wavelet Data Hiding Technique also has a very bright scope as it includes the properties of different techniques that withstand the single method in watermarking by overcome its shortcomings. With the help of these new techniques the noise level in the watermarked image can be reduced and thus the error reduces which leads to the decline in distortion level in the extracted image. The less the distortion level the more the similarity factor/normalized correlation of the image can be observed.

6. REFERENCES

[1] Manker, V. H., Das T. S., Saha S. and sarkar S. K. 2008 Robust image watermarking under pixel wise masking framework. First International Conference on Emerging Trends in Engineering and Technology, ICETET

[2] Guo, H., and Georganas N. 2002 Multi-resolution Image Watermarking Scheme in the Spectrum Domain. *Proceeding of IEEE Canadian Conference on Electrical and Computer Engineering*, pp. 873-878.

[3] Cox, I. J., Kilian, I., Leighton T., and Shamoon T. Secure Spread Spectrum watermarking for Multimedia. *IEEE*

Transaction on Image Processing, Vol. *6*, pp. 1673-1687

[4] Guo, H. and Georganas N. May 2002 Multi-resolution Image Watermarking Scheme in the Spectrum Domain. *Proceeding of IEEE Canadian Conference on Electrical and*

Computer Engineering, pp. 873-878.

[5] Hsieh, M.S., and Tseng D.C. Oct.2001 Hiding digital watermarks using multiresolution wavelet transform. *IEEE Transactions on indusrriol electronics*, vol. 48, No. 5, pp 875-882

[6] Pawlak, M. and Xin, Y. May 2002 Robust Image Watermarking: An Invariant Domain Approach. *Proceedina_ of. IEEE Canadian Conference on Elecmrical and Computer Engineering*, pp. 885-888,

[7] Pla, O.G, Lin E.T, and Delp E.J 2004. A Wavelet Watermarking Algorithm Based on a Tree Structure. *Tech. Rep*., Polytechnic University of Catalonia, Spain,

[8] Xiaolong, Li, Yang Bin, and Daofang Cheng. 2009 A generalization of LSB matching, IEEE Signal Processing Letters, vol. 16, pp. 69-72.

[9] Kelkar Yashovardhan, Shaikh Heena Analysis of Robustness of Digital Watermarking Under Various Attacks, *IP Multimedia Communications A Special Issue from IJCA*

[10] Langelaar G., Setyawan I., Lagendijk R.L. 2000 Watermarking Digital Image and Video Data, in IEEE Signal Processing Magazine, Vol 17, pp 20-43

[11] Dongyang, Teng, Renghui Shi, Xiaoqun Zhao 2010 DCT Image Watermarking Technique Based on the Mix of Time-domain. 978-1-4244-6943-7/10, IEEE, pp. 826-830

[12] Wiseto, I., Agung P. 2002 *Watermarking and Content Protection for Digital Images and Video*. thesis of PhD in University of Surrey

[13] Arya, M.S. Siddavatam, R. Ghrera, S.P. 2011. A Hybrid Semi-Blind Digital Image Watermarking Technique using Lifting Wavelet Transform – Singular Value, Decomposition, Electro/Information Technology (EIT) 2011 IEEE International Conference,pp.1 - 6

[14] Jin, Cong 2008 Digital Watermark Theory & Technology. Beijing: Tsinghua University Press.