A Statistical Comparison of Digital Image Watermarking Techniques

Vivek Tomar
Student, M.Tech. [CSE]
ASET, Amity University, Noida

Deepti Mehrotra, Ph.D
ASCS, Sector-44, Noida

Ankur Choudhary
ASET, Amity University, Noida

ABSTRACT

Due to the rapid advancement in internet technology and evolution of high speed networks operating throughout the world, protection of multimedia content is urgently required. So, it has become a challenging task to protect copyright of an individual's creation. Digital watermarking provides a viable and promising solution to protect copyright and authentication of the ownership. In this paper, we have performed a statistical comparison of different Digital Image Watermarking techniques (LSB, DCT based and DWT based) that can be used to protect copyright of digital Image. We have also provided the statistical comparison of these techniques that can help us to know the pros and cons of these techniques. This statistical comparison can further be used to improvise and propose new techniques for the same.

Keywords

DCT (Discrete cosine transform), DWT (Discrete wavelet transform), FFT (Fast Fourier transform), PSNR (Peak signal to noise ratio), IDCT (Inverse Discrete cosine transform), IDWT (Inverse Discrete wavelet transform), JPEG (Joint photographic expert group), LSB (Least significant bit), HVS (Human Visual System), BER (Bit Error Rate).

1. INTRODUCTION

The continuous rapid growth of the Internet technology has given us the various new possibilities, like publicly available access to information scattered around the world, distributed project work, and fast and reliable means of electronic communication. But now it requires solution of a major issue of copyright protection and authentication of digital media. The fact that legislation is unable to cope with its rapid rate of change also makes it very attractive to people with dishonorable motives. The intellectual property authentication has become an important issue **[4].** Keeping these drawbacks of digital age in mind, we are in the urgent need of the digital analogy of the methods that we have been using since ancient times. This requirement for techniques which can be used to protect our content has given birth to a new field of digital watermarking. More and more researchers are attracted to the area of digital image watermarking because of the property of the image as it has a lot of redundant information contained in it. This information can be easily exploited for watermark insertion.

Watermarking techniques are broadly categorized into two categories.

1. Spatial domain techniques.
2. Transform domain techniques.

The spatial domain techniques are having least complexity and high payload and they cannot even withstand low pass filtering and common image processing attacks. The commonly accepted watermarking schemes are LSB, DCT, DFT and DWT etc. **[5][6][7][8][9]**. LSB substitution cannot be considered as a good technique for digital watermarking because of robustness. Cox et. al **[1]** used DCT domain for watermark embedding for the first time. JPEG images use DCT for image compression. So it's always a good idea to explore robustness of watermark in DCT domain. A more robust technique using DCT is proposed in **[9]** and **[10].** This paper has been divided into six sections. Section 2 describes the LSB technique for watermark insertion. Section 3 describes the common DCT based watermarking technique. Section 4 gives the description of the DWT based approach for watermark insertion. Section 5 describes the results and discussion followed by the conclusion in Section 6.

2. LSB WATERMARKING

This is the most straight forward method for watermark embedding. In this method, the embedding of watermark is done into the least-significant-bits of the cover object **[2]**. This technique is helpful because most of the watermarks are lost due to attacks like cropping, a single surviving watermark can fulfill our task.

LSB substitution is a very simple technique but it has many drawbacks. This technique may survive against various transformations. But any addition of noise or lossy compression can easily degrade the image quality or remove watermark. Even simple attacks can remove the watermark such as, setting the LSB bits of each pixel to one. This attack poses negligible impact on the cover object **[10]**. Furthermore, once the algorithm is discovered, the embedded watermark could be easily modified by an attacker.

An improvement on basic LSB substitution **[3]** has also been proposed. In this technique, we use a pseudo-random number generator to determine which pixels to use for embedding. These pixels are selected with the help of a key. In this way, we can make the watermark more secure as it cannot be easily visible to the attacker. This algorithm is still vulnerable to attacks such as replacing the LSB's with a constant. Even in locations that are not used for inserting the watermark, there will be a negligible effect on the cover image. LSB modification proves to be a simple and fairly powerful tool for stenography, but it lacks the basic robustness that watermarking applications require.

3. DCT DOMAIN WATERMARKING

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 which are high, middle and low frequency bands. This makes it easier to choose the band in which we are going to insert the watermark. The literature survey reveals that mostly the middle frequency bands. The embedding of watermark in a middle frequency band does not scatter the watermark information to most visual important parts of the image i.e.

the low frequencies. It does not overexpose them to removal through compression and noise attacks where high frequency components are targeted **[7]**.

There are various watermarking techniques based on DCT. One such technique utilizes the comparison of middle-band DCT coefficients to encode a single bit into a DCT block **[11]**. F_M is the middle frequency component of the 8x8 DCT block, F_L is the lowest frequency component of the block, and F_H is the higher frequency component. F_M is chosen as the embedding region as to provide additional resistance to lossy compression techniques, while avoiding significant modification of the cover image **[7]**.

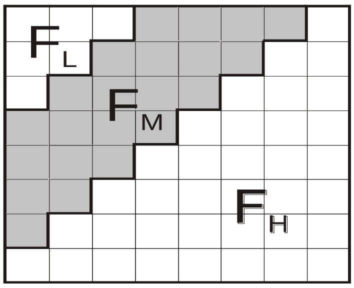

Figure 3.1 - Definition of DCT Regions [7]

Then we choose two locations i.e. B_i (u_1, v_1) and B_j (u_2, $v_{2)}$ from the F_M region for comparison. These locations can be choosen randomly. But to provide extra robustness, we can choose the coefficients on the basis of JPEG quantization table shown below in table 3.1.

JPEG quantization table have two locations with identical quantization values. We can feel confident that any scaling of one coefficient will scale the other by the same factor with preserving their relative size.

Table 3.1 - Quantization values used in JPEG compression scheme

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Looking at the table, we can see that the coefficients (4, 1) and (3, 2) or (1, 2) and (3, 0) can be suitable candidates for comparison, as their quantization values are equal. The DCT block will encode a '1' if B_i (u_1, v_1) > B_j (u_2, v_2); otherwise it will encode a '0'. The coefficients that do not fulfill the criteria fit the bit to be encoded are then swapped **[7]**.

Swapping of such coefficients should not significantly alter the watermarked image, as it has been proved that DCT coefficients of middle frequencies have similar magnitudes. The robustness of the watermark can be improved by introducing a watermark strength constant '*k*', such that B_i (u_1, v_1) - B_j (u_2, v_2) > *k*. The coefficients which will not fulfill the above criteria are modified though the use of a random noise to satisfy the relation. This strength factor '*k*' can be used to increase the chances of error detection but only at the expense of image degradation.

The steps involved in any technique which is based on DCT are as follows:

1) Divide the entire image into 8x8 sized non-overlapping blocks.
2) Take the DCT of each block of size 8x8.
3) Apply a block selection criteria based on the knowledge of Human Visual System (HVS).
4) Use some coefficient selection criteria for embedding.
5) Embed the watermark by modifying the selected coefficients.
6) Take the inverse DCT of each block.

Almost all the algorithms for digital watermarking based on DCT are classified on the basis of step 3 and 4 i.e. the main differentiation between these algorithms is on the basis of block selection criteria or coefficient selection criteria **[7]**.

4. DWT DOMAIN WATERMARKING

Wavelet domain is another promising domain for watermark embedding. When DWT (Discrete Wavelet Transform) applied to an image, It separates the image into four different components which are lower resolution approximation image (LL), horizontal (HL), vertical (LH) and diagonal (HH) detail components. This process of separation can be iterated to compute multi-level wavelet decomposition, as in the 2-level discrete wavelet transform shown below in figure 4.1.

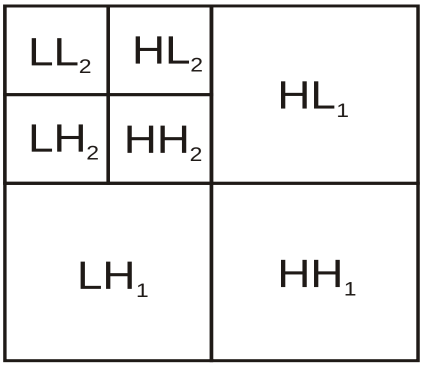

Figure 4.1 – 2-level Discrete Wavelet Transform [6][9]

One of the advantages of the wavelet transform is that it is believed to be more accurate model aspects of the HVS as compared to the FFT or DCT. This technique allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution detail bands {LH, HL, HH}. Robustness of our watermark can be increased by embedding watermark in this region with no additional impact on image quality **[9][12]**.

The wavelet based transform has recently gained popularity because of the property of multiresolution analysis that it provides. However, DWT 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 **[6]**. Performance improvements in DWT based digital image watermarking algorithms could be obtained by combining it with DCT. The idea is based on the fact that combined transforms could compensate for the drawbacks of each other, resulting in effective watermarking.

Table 5.1 – Statistical Comparison of Robustness

S.No.	Technique	Attack on watermarked image	Elapsed Time For Embedding	PSNR	Elapsed Time For Recovery	Correlation	Bit Error Rate
1	DCT	Blurring	1.9656	3617.1	0.8424	0.9717	0.0720
		Scaled to half size			0.5928	0.0372	0.6280
		Scaling to 75%			1.0920	0.9755	0.0710
		Resizing of scaled image			0.9048	0.9595	0.0730
		Rotation of 5 degrees and rotated back			1.0608	0.0103	0.3410
		Cropping			1.1544	0.5538	0.1170
2	DWT	Blurring	14.601	729.67	20.748	0.6374	0.0300
		Scaled to half size			5.694	0.0441	0.5050
		Scaling to 75%			20.763	0.7128	0.0090
		Resizing of scaled image			20.779	0.2349	0.3190
		Rotation of 5 degrees and rotated back			20.732	0.0387	0.5010
		Cropping			20.6857	-0.0232	0.5060
3	LSB	Blurring	0.7176	122200	0.4524	N/A	0.4910
		Scaled to half size			0.2496	N/A	0.4820
		Scaling to 75%			0.4836	N/A	0.4860
		Resizing of scaled image			0.4368	N/A	0.4820
		Rotation of 5 degrees and rotated back			0.5928	N/A	0.9160
		Cropping			0.5304	N/A	0.4850

5. RESULTS AND DISCUSSIONS

We have performed extensive simulations on Host/Cover image using Matlab 7.0. The Cover image and the watermark we have took, both are in .jpeg format. The watermark is embedded into image and several attacks like Blurring,Scaling, Rotation, Cropping etc has been performed on the Watermarked Image. After that, the watermark is retrieved using the extraction process. Then the robustness of the techniques are compared on the basis of parameters like time required for Embedding and Extraction, PSNR, BER, Correlation between the original watermark and the Extracted watermark etc are measured which are shown in the above table 5.1.

Fig. 5.1 (a)
Cover Image

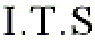

Fig. 5.1 (b)
Original Watermark

Fig. 5.2 (a)
DCT Watermarked Image

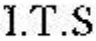

Fig. 5.2 (b)
Recovered Watermark

Fig. 5.3 (a)
De-Blurred Image

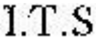

Fig. 5.3 (b)
Recovered Watermark

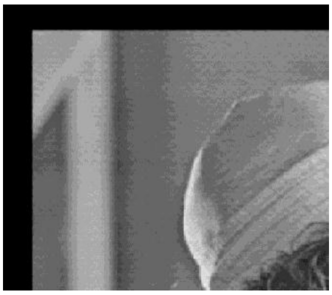

Fig. 5.4 (a)
Rotated-Back Image

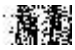

Fig. 5.4 (b)
Recovered Watermark

Fig. 5.5 (a)
DWT Watermarked Image

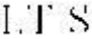

Fig. 5.5 (b)
Recovered Watermark

6. CONCLUSION

The statistical comparison of different watermarking techniques for digital images shows robustness. There is still much scope for improvement while working on image watermarking. Still there are some attacks like rotation on which all the proposed watermarking algorithm or methods shows approximately no reluctance.

On the basis of statistical comparison we can conclude, LSB substitution cannot be considered as a very good technique for digital watermarking. It provides a less robustness as we can see in the table 5.1. The watermarks that are embedded using LSB technique can easily be removed without visually degrading the quality of image. If one of the more trivial embedding algorithms is used, the encoded message can be easily recovered and even easily altered by an attacker. Although it takes a very less time for embedding even then it should not be desirable to use.

DCT domain based technique has been proved to be highly robust for all types of attacks except rotation and cropping. It works really well specifically for JPEG compression. By anticipating which coefficients would be modified by the subsequent transform and quantization, we can be able to achieve a fair amount of robustness with good capacity, and low visual impact. Robustness can even be improved significantly if the subsequent degradation techniques are known. This observation holds true when the compression algorithms used are known.

The wavelet domain has also proved to be a robust technique. It also has a very little effect on the image quality. Although this Wavelet based approach has more computational requirements as compared to other two techniques. This becomes more impressive when we consider that the wavelet technique is one of the most primitive currently known. Modified wavelet-domain techniques will definitely improve on the computational requirements and robustness. The combination of DCT and Wavelet domain must be one of the promising techniques in this area.

Table 6.1 – Conclusion Table

Technique	Attack	Robustness Level
DCT	Blurring	High
	Scaled to half size	Low
	Scaling to 75% of original size	High
	Resizing of scaled image	High
	Rotation of 5 degrees and rotated back	Low
	Cropping	Medium
DWT	Blurring	Medium
	Scaled to half size	Medium
	Scaling to 75% of original size	High
	Resizing of scaled image	Medium
	Rotation of 5 degrees and rotated back	Low
	Cropping	Low
LSB	Blurring	Low
	Scaled to half size	Low
	Scaling to 75% of original size	Low
	Resizing of scaled image	Low
	Rotation of 5 degrees and rotated back	Low
	Cropping	Low

7. REFFERENCES

[1] I. Cox, J. Killian, T. Leighton, T. Shamoon, “Secure Spread Spectrum Watermarking for Multimedia,” IEEE Trans. Image Processing, Vol. 6, No. 12, pp. 1673-1687, 1997.

[2] N.F. Johnson, S.C. Katezenbeisser, “A Survey of Steganographic Techniques” in Information Techniques for Steganography and Digital Watermarking, S.C. Katezenbeisser et al., Eds. Northwood, MA: Artec House, Dec. 1999, pp 43-75.

[3] R.B. Wolfgang, C.I. Podilchuk, and E.J. Delp, “Perceptual watermarks for digital images,” Proc. IEEE, no. 7, pp. 1108-1126, July 1999.

[4] Primo Braga, C.A, C. Fink, & C. Paz Sepulveda, “Intellectual Property Rights and Economic Development”, technical report, The World Bank, Washington D.C 2000.

[5] Falkowski, B.J., Lim, L.S., 'Image Watermarking Using Hadamard Transforms', in IEE Electronics Letters, United Kingdom, vol. 36, no.3, pp. 211-213, February 2000.

[6] P. Meerwald, and A.Uhl, “A Survey of Wavelet- Domain Watermarking Algorithm,” in P.W. Wong and E.J.Delp,(eds.), Proceedings of Electronic Imaging 2001,Securityand Watermarking of Multimedia Contents III, San Jose, CA, January 2001, pp. 505-515.

[7] Mohamed A. Suhail, Mohammad S. Obaidat, “Digital Watermarking-Based DCT and JPEG Model”, IEEE Transactions On Instrumentation And Measurement, Vol. 52, No. 5, October 2003.

[8] Tao, P., Eskicioglu, A.M., "A Robust Multiple Watermarking Scheme in the Discrete Wavelet Transform Domain", in Symposium on Internet Multimedia Management Systems, Philadelphia, PA. October 25-28, 2004.

[9] Lee, C., Lee, H., "Geometric attack resistant watermarking in wavelet transform domain," in Optics Express vol. 13, no. 4, pp. 1307-1321 2005.

[10] Vikas Saxena, J.P Gupta “Towards increasing the Robustness of Image Watermarking Scheme against JPEG Compression” IMECS vol II, pp 1903- 1906, Marc.

[11] T.K. Tiwari, Vikas Saxena “An Improved and Robust DCT based Digital Image Watermarking Scheme” International Journal of Computer Applications (0975 – 8887) Volume 3 – No.1, June 2010.

[12] Shital Gupta, Sanjeev Jain “A Robust Algorithm of Digital Image Watermarking Based on Discrete Wavelet Transform” Special Issue of IJCCT Vol.1 Issue 2, 3, 4; 2010 for International Conference [ACCTA-2010], 3-5 August 2010.