An Improved and Robust DCT based Digital Image Watermarking Scheme

Tribhuwan Kumar Tewari
Sr. Lecturer,
Jaypee Institute of Information Technology,
Sector 62. Noida

Vikas Saxena
Assistant Professor,
Jaypee Institute of Information Technology,
Sector 62,Noida

ABSTRACT
The need for displaying one's own multimedia content on the internet is increasing day by day. With the exponential growth of internet and high speed networks operating through out the world it's a challenging task to protect copyright of an individual's creation. Digital watermarking provides a viable solution to protect copyright and authenticate the ownership of an intellectual property. In this paper we propose a new DCT based additive watermarking scheme which provides higher resistance to image processing attacks mainly JPEG compression. In our approach the watermark is embedded in the mid frequency band of the DCT blocks only in the sub band which is carrying low frequency components and the high frequency sub band components remain untouched.

General Terms
Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Discrete Image watermarking, Joint Photographic Experts Group (JPEG), JPEG Quality Factor (Q), Peak Signal to Noise Ratio (PSNR)

Keywords
Averaged DCT blocks, pixel intensity,

1. INTRODUCTION
The recent development of network multimedia systems & explosion of fast communication network has discouraged & damped the multimedia content providers i.e. authors, publishers to grant the distribution of their document on the network environment. The intellectual property authentication has become an issue of concern**[1]** While a considerable efforts and a lot of economic resources are used for the creation of intellectual property particularly in industrial societies, the cost of reproducing such intellectual creations typically constitute only a small portion of the creation. However a creator always desires some rewards or incentives for his creation which he is not able to get due to low cost copying. More and more researchers are attracted to the area of image watermarking because of the property of the image as it has a lot of redundant information contained in it which can be exploited to be used for watermark insertion. Many watermarking methods for images are proposed. Watermarking techniques are broadly categorised into spatial domain and transform domain techniques. While the spatial domain techniques are having least complexity and high payload they can not withstand low pass filtering and common image processing attacks .The widely accepted schemes for watermarking are in transform domains i.e. DCT, DFT and DWT etc.**[2][3][4][5][6][7][8]** .Spread Spectrum based watermarking techniques exploited the Human Visual Systems(HVS) **[9][10][11].** The survey papers given by different researchers are handful of research material relating to watermarking techniques and it helps in understanding the entire concept as well as a motivation for proposing a new scheme**[12][13][14][15][16].**

Cox et. al uses DCT domain for watermark embed for the first time .As JPEG standard also uses DCT for image compression it is always a good idea to explore image watermarking and robustness of watermark in DCT domain. The paper is divided into following sections .Section 2 gives the description of the common DCT based watermark insertion technique which works as the base of our proposed algorithm section 3 gives the description of the proposed scheme Section 4 describes the results and the discussion on the results followed by the conclusion in Section 5.

2. 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 namely the high ,middle and low frequency bands thus making it easier to to choose the band in which the watermark is to be inserted. The literature survey reveals that mostly the middle frequency bands are chosen because embedding the watermark in a middle frequency band do not scatter the watermark information to most visual important parts of the image i.e. the low frequencies and also it do not overexpose them to removal through compression and noise attacks where high frequency components are targeted. **[17].**

Numerous watermarking techniques based on DCT are proposed. Although some of the watermarking techniques embed the watermark in the DC component i.e the low frequency component most technique utilizes the comparison of middle-band DCT coefficients to embed a single bit of watermark information into a DCT block. The middle-band frequencies ($F_{M)}$ of an 8*8 DCT block can be shown below in figure 2.1.

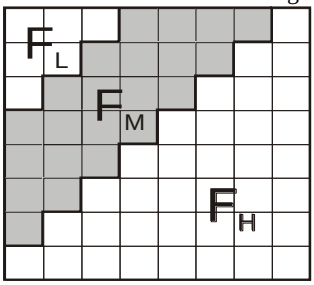


Figure 2.1 - Definition of DCT Regions [17]

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 F_H is used to denote the higher frequency components. F_M 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.

From the frequency band F_M two locations $M_i(u_1,v_1)$ and $M_i(u_2,v_{2)}$ are chosen as the region for comparison. The choice in selecting the two locations is dependent on the content of the JPEG quantization table given below in table 2.1. The two locations which have identical quantization values are chosen for embedding one watermark bit of information.

Table 2.1 Quantization values used in JPEG compression scheme [18]

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

From the table the coefficients at (4,1) and (3,2) or (1,2) and (3,0) would make suitable candidates for comparison, as their quantization values are equal. The DCT block will encode a "0" if $M_i(u_1,v_1) < M_i(u_2,v_2)$, otherwise it will encode a "1". The coefficients are then swapped if the relative size of each coefficient does not agree with the bit that is to be encoded [19]. This shows that the number of watermark bits that can be embedded is directly dependent on the number of pairs of locations in quantization table for which the value in the table is similar.

The swapping of such coefficients should not alter the watermarked image significantly, as it is generally believed 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 $M_i(u_1,v_1) - M_i(u_2,v_2) > k$. Coefficients that do not meet this criteria are modified though the use of random noise as to then satisfy the relation. Increasing *k* thus reduces the chance of detection errors at the expense of additional image degradation [20].

Another category of DCT based watermarking techniques add a pseudo number sequence in the mid frequency band of the image to be watermarked. A strength factor k is used which gives robustness to the watermark. The value of k should be intelligently decided other wise imperceptibility of the watermarked image with the original un watermarked is reduced showing the distortions. For the mid frequency band of given DCT block x, y the embedding process can be shown using the equation shown below in figure 2.2.

$$I_{W\,x,y}(u,v) = \begin{cases} I_{x,y}(u,v) + k * W_{x,y}(u,v), & u,v \in F_M \\ Ix,y(u,v), & u,v \notin F_M \end{cases}$$

Figure 2.2 Embedding of CDMA watermark into DCT middle frequencies [9]

In these type of DCT techniques also 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 I_W [9].

The watermarking procedure can be made somewhat more adaptive by slightly altering the embedding process to the method shown below in figure 2.3

$$I_{W\,x,y}(u,v) = \begin{cases} I_{x,y}(u,v) * (1 + k * W_{x,y}(u,v)), & u,v \in F_M \\ Ix,y(u,v), & u,v \notin F_M \end{cases}$$

Figure 2.3 Image dependent DCT CDMA watermarks [17]

This slight modification scales the strength of the watermarking based on the size of the particular coefficients being used.

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. In our approach the PN sequence approach of DCT watermarking is used.

The general steps involved in DCT Block Based Watermarking Algorithm are given below:

1) Segment the image into non-overlapping blocks of 8x8.

2) Apply forward DCT to each of these blocks.

3) Apply some block selection criteria based on the knowledge of Human Visual

System(HVS).

4) Apply coefficient selection criteria (e.g. highest, mid ,lowest).

5) Embed watermark by modifying the selected coefficients.

6) Apply inverse DCT transform on each block.

Most algorithms using DCT are classified based on step 3 and 4 i.e. the main difference between most algorithms is that they differ either in the block selection criteria or coefficient selection criteria.

3. PROPOSED SCHEME

In an image adjacent pixels generally have almost the same intensity value .Neighboring pixel intensity can easily be predicted from a given pixel intensity. When the DCT is performed on an image this correlation is removed thus helping us in embedding the watermark in scattered form in different DCT coefficients.

The approach adopted by us is slightly different from the traditional DCT used for watermarking.

3.1 Watermark embedding algorithm

The algorithm which is used to embed a watermark on an image is given below

I. Segment the image I(i , j) into two sub band blocks with half the size of the original image i.e I1(i/2,j) & I2(i/2,j). I1(i/2,j) gives the high intensity pixels block & I2(i/2,j) give low intensity pixels block
I(i.j) =∑I(i/2,j)+I(i/2,j).

II. Break the I1(i,j/2) into blocks of size 8* 8.

III. Find the DCT of each of the block.

IV. Private key is used to generate two pseudo random no sequences of domain {-1,0,1} which are highly uncorrelated. [17][20]

V. Preprocess the watermark by converting the watermark in to a binary sequence.
W(m*n)->W(s * 1) where s=m*n

VI. Embed the watermark on each of the DCT block in the mid band of each coefficient block using the pseudo random number sequence and the watermark sequence.

VII. After embedding the watermark the inverse DCT operation is done on the sub band to obtain the averaged image band again.

VIII. Inverse operation of step 2 is done to obtain the watermarked image.

The insertion of the watermark in the mid band of the coefficient block of each averaged DCT block gives extra robustness to the watermark The use of the key gives security to the watermarking system. As the watermark is embedded in the mid frequency band of the transformed high pixel intensity image robustness against JPEG attack is highly increased.

3.2 Watermark extraction algorithm

The steps involved in the watermark extraction algorithm are given below.

Take the image which is suspected of having the watermark.

I. Repeat step I and II of watermark embed algorithm

II. Using the private key extract the watermark.

III. Compare the watermark with the original watermark..

IV. Similar watermark will prove the authenticity.

The following section will show the extracted watermark from the suspected image with some attacks. The percentage similarity between the original watermark & the retrieved watermark is calculated through the correlation function .

4. RESULTS AND DISCUSSIONS

The watermarked image is subjected to compression at different quality factor. The watermark from the compressed watermarked image is retrieved using the extraction process. The percentage similarity between the extracted watermark and the original watermark is calculated. The same procedure is repeated for different standard images and results are taken in the form of PSNR and correlation coefficient i.e. measuring correlation between original and retrieved watermark at different quality factor (Q) .The result is tabulated given below.

Table 4.1 Correlation Coefficient (CC) of the retrieved watermark at different quality factor on different images

quality-factor(Q)	Baboon	Lena	Boat
5	0.7593	0.935	0.8936
10	0.7746	0.959	0.9119
20	0.7975	0.9859	0.9436
40	0.7987	0.9859	0.9344
45	0.7975	0.9859	0.9425
50	0.7975	0.9859	0.9445
60	0.8027	0.9859	0.9468
80	0.792	0.9894	0.9468

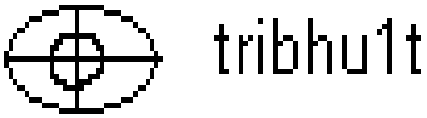
(a)Original (b) Averaged

(c)Watermarked (d) Compressed (Q=5)

Figure 4.1 Lena under gone different operation of watermarking

(a) Boat (b) Baboon

Figure 4.2 Standard images used for watermarking



(a) logo (b) name

Figure 4.3 Watermark used

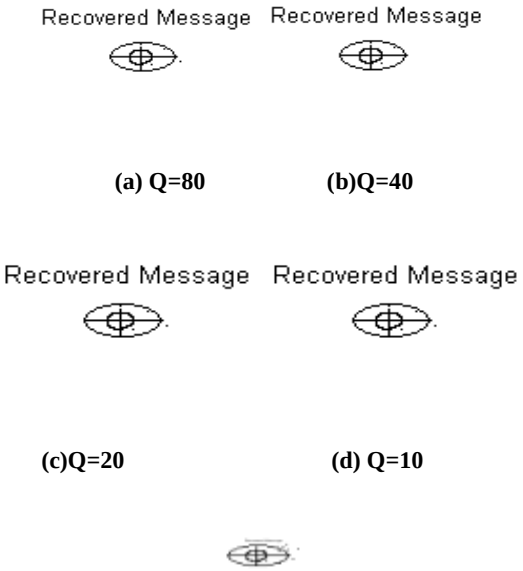


Figure 4.4 Extracted watermark for Lena image undergone compression for different Q

Table 4.2: Correlation coefficient & PSNR values for Lena image undergone different attacks

Attacks	PSNR	CC
Q=5	42.1364	0.935
Q =10	42.1447	0.959
Q = 20	42.1612	0.9859
Q = 40	42.1612	0.9859
Q = 45	42.1612	0.9859
Q = 50	42.1612	0.9859
Q = 60	42.1612	0.9859
Q = 80	42.2632	0.9894
cropped 1	42.1612	0.9859
cropped 2	42.1612	0.9859
Blur factor .1	42.1633	0.9894
Blur factor .2	42.1137	0.9052
Gaussian v = .01	42.1647	0.9484
Gaussian v = .02	42.1433	0.8844
Gaussian v = .04	42.1612	0.7267
Gaussian v = .06	42.1612	0.664
Gaussian v = 0.1	42.1633	0.5384
Gaussian v= 0.15	42.1137	0.3524
Salt & Pepper v =0.1	42.2334	0.8936
Salt & Pepper v =0.15	42.2324	0.8084
Salt & Pepper v = 0.2	42.1121	0.5476

In the table 4.2, v refers to the variance & Q refers to the quality factor.

For all the attacking operations Adobe Photoshop is used and the code is built in Mat lab 7. Corr2 function is used for finding the correlation between the original watermark and the retrieved watermark. Imnoise function is used to introduce both type of noise i.e. Gaussian, salt and pepper noise .The result shows that the method work best for the compression attack and tolerant against common image processing attacks. The proposed scheme is compared with the scheme proposed by Vikas Saxena et.al **[20]** and our proves to be better than it at a very high JPEG compression. The idea behind not using the LSB substitution (implementation technique with low complexity) for digital watermarking is its lack of even a minimal level of robustness. LSB embedded watermarks can easily be removed using techniques that do not visually degrade the image to the point of being noticeable. Furthermore if one of the more trivial embedding algorithms is used, the encoded message can be easily recovered and even altered by a 3rd party. Still it would appear that LSB will remain in the domain of steganography due to its tremendous information capacity

The watermarking techniques in which the watermark is embedded in transform domains are typically better candidates for watermarking then spatial, for both reasons of robustness as well as visual impact. Embedding in the DCT domain proved to be highly resistant to JPEG compression as well as significant amounts of random noise. By anticipating which coefficients would be modified by the subsequent transform and quantization, we were able to produce a watermarking technique with moderate robustness, good capacity, and low visual artifacts. But as all the DCT based images suffers from visual artifacts as DCT is done on the blocks our approach is no exception. But the visual quality is good & its not with remarkable change. Nonetheless the visual quality can be improved by the slight introduction of blur. Robustness can be improved significantly when the subsequent degradation techniques are known. This holds particularly true in the case of compression techniques, where the compression algorithms are well known. .The wavelet domain as well proved to be highly resistant to both compression and noise, with minimal amounts of visual degradation. A final note is that of geometric transforms. Geometric transforms are one of the most difficult for a watermarking technique to deal with**[11]** Embedding domains may be chosen that display both shifting or rotational invariance such as Cartesian and Polar DCT, however these domains are typically resistant to only a specific geometric distortion and not the complete set. We have here with our approach tried to explore the DCT as well as the DWT domain for digital image watermarking for grey scale images. We would like to extend the same for colored images.

5. CONCLUSION

The study of different watermarking techniques for digital images shows that its worth. exploring the image because of its redundant nature. There is still scope for improvement while working on image watermarking. Still there are some attacks to which all the watermarking algorithm or methods shows approximately no reluctance. Through our approach of watermark embed and extraction in which wavelet as well as DCT domain is exploited, we can conclude that it is robust against the intentional compression attack as our target images are those that can be put on the internet with least possible

7. REFERENCES

1 Primo Braga, C.A, C. Fink, & C. Paz Sepulveda, "Intellectual Property Rights and Economic Development", technical report ,The World Bank, Wasinghton D.C 2000.

2. Solachidis, V & Pitas, I 2001, 'Circularly Symmetric Watermark Embedding in 2-D DFT Domain', in IEEE Transactions on Image Processing, vol. 10, no. 11, pp. 1741-1753.

3. De Rosa, A., Bami, M., Bartolini, F., Cappellini, V., Piva, A. "Optimum Decoding of Non-additive Full Frame DFT Watermarks", in Procedings of the 3rd Workshop of Information Hiding, 1999, pp.159-171.

4. 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.

5. Falkowski, B.J., Lim, L.S., 'Image Waternarking 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-DomainWatermarking 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. 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. October25-28, 2004.

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

9. P.G.Flikkema, "Spread Spectrum techniques for wireless communication", IEEE Signal Processing 14, pp. 26-36, May 1997.

10. I.J. Cox, J.Kilian, T.Leighton and T. Shamoon, "Secure Spread Spectrum watermarking for Multimedia," IEEE Tras. on Image Processing , Vol. 6,No12, 1997, pp. 1673-1687.

11. Ruanaidh, J. J. K. O., Pun, T., "Rotation, scale and translation invariant spread spectrum digital image watermarking," Signal Process,vol. 66, no. 3, pp. 303-317, 1998.

12.]F.Hartung, and M. Kutter, "Multimedia Watermarking techniques", Proceddings of IEEE, Vol. 87, No 7, July 1999, pp. 1079-1107.

13. M. Arnold, M. Schmucker, and S.D. Wolthusen, "Techniques and application of Digital Watermarking and Content Protection", Eds.Northwood ,Artech House, 2003.

14. Saraju P. Mohanty , "Digital Watermarking: A Tutorial Review", URL: http://www.csee.usf.edu/~smohanty/ research/Reports/WMSurvey1999Mohanty.pdf http://citeseer.ist.psu.edu/mohanty99digital.htm

15. W. Bender, D. Gruhl, N. Morimoto, and A. Lu. "Techniques for data hiding". IBM Systems Journal, Vol. 35.(3/4), 1996, pp. 313-336

16. N. Johnson, ,and S. Katezenbeisser , "A Survey of Steganographic Techniques", Eds. Northwood, MA:ArtecHouse,43, 1999

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

18. Rafael C. Gonzalez, Richard E. Woods,"Digital Image Processing", Upper Saddle River, New Jersey, Prentice Hall, Inc., 2002 pp 484.

19. F.A.P. Petitcolas, , "Watermarking Schemes Evaluation" ", in IEEE Signal Processing Magazine, Vol 17, pp 58-64, September 2000

20. Hsu, C.-T., Wu, J.-L., "Multiresolution Watermarking for Digital images", in IEEE Transactions on Circuits and Systems - II: Analog and Digital Signal Processing, vol. 45, no. 8, pp. 1097-1101, August 1998.

21. Vikas Saxena, J.P Gupta "Towards increasing the Robustness of Image Watermarking Scheme Against JPEG Compression" IMECS vol II, pp 1903- 1906, Marc