A Robust DCT based Digital Image Watermarking using Random Mid-band Coefficient Exchange Scheme for Gray Scale Images

Alisha Parnami
M.Tech Student,
ACEIT, Jaipur
Rajasthan, India

Ankit Gupta
Assistant Professor
ACEIT, Jaipur
Rajasthan, India

Gagan Parnami
Database Administrator
Manhattan Associates,
Bangalore
Karnataka, India

ABSTRACT
Various watermarking algorithm has been developed in recent years. The two-dimension DCT and its counterpart Inverse 2-D DCT, are the most complex parts in the DCT-based watermarking systems.

In this paper, the watermark to be inserted in the cover image is encrypted through a proposed encryption strategy to enhance the overall security instead of embedding the exact watermark bits. Every unique sequence of four bits is mapped to a unique sequence of length eight. These sequences are generated by a seeded pseudo-random generator. Due to this, size of the bits becomes double but the advantage is that the watermark cannot be detectable through normalized correlation. The encrypted watermark is inserted into the image using proposed randomized discrete cosine transform (DCT) based mid-band coefficients exchange scheme. To extract the original watermark, it is required to decrypt the extracted bits. Mapping with the same pseudo-random sequences is done. The strategy is robust against the blind watermark detection. Different Gray scale images of size (512* 512) have been used in this approach. The proposed method shows better results in terms of PSNR.

Keywords
DCT, Mid band Exchange coefficients, Normalized correlation, Pseudo random sequence, PSNR

1. INTRODUCTION
Digital media has made our life more colorful because of its advantages like easier to access, copy and distribute. But at the cost of series of malice activities like copyright infringement, information distortion, these make serious damages to both the producers and the users of the digital products. So we really need a new technology to protect the copyright, authenticity and integrity of the digital products. Watermarking is the emerging field in this background. Digital watermarks have been proposed for a variety of applications including authentication and copy protection of multimedia content.

A good digital watermarking algorithm is the one which finds a good balance between invisibility and robustness. Several watermarking algorithms are available in spatial domain and transformed (frequency) domain [6]. The study on DWT (Discrete Wavelet Transform) gives a lot of inspiration in frequency domain. The DCT is another common transform for image process in frequency domain [3], [5], [7].A spread-spectrum DCT domain watermarking technique for still digital images was analyzed[1].One of the first algorithms presented by Cox et al. used global DCT approach to embed a robust watermark in the perceptually significant portion of the Human Visual System (HVS) Initially, Koch, Rindfrey, and Zhao [2] proposed a method for watermarking images .Further, the authors embedded a watermark signal domain by modifying a number of predefined DCT coefficients.

Here in this paper the idea of Middle Band Coefficient Exchange is used which was discussed Johnson and katezenbeisser [4].Some authors proposed an efficient use of middle-band coefficients exchange to hide the watermark data [5], [9], [10]. Further in the research area of DCT based watermarking, invisible watermarking has been presented. [7], [11], [13]

The organization of this paper is as follows. The traditional DCT-based Mid-band Exchange Coefficient (MBEC) watermarking algorithm is discussed in Section 2. Section 3 introduces the proposed Random MBEC watermarking system. Section 4 presents the experimental results using the proposed technique and lastly, the main conclusions of the paper are summarized in Section 5.

2. THE MIDDLE BAND COEFFICIENT SCHEME [8]
The middle-band frequencies (FM) of an 8x8 DCT block are shown in Figure 1. In this Figure, FL is used to denote the lower frequency components of the block and FH is used to denote the higher frequency components. FM is chosen as embedding region to provide additional resistance to lossy compression techniques, while avoiding significant modification of the cover image. First, 8x8 DCT of an original image is taken. Then, two locations DCT (u1, v1) and DCT (u2, v2) are chosen from the FM region for comparison of each 8 x 8 block. These locations are selected based on the recommended JPEG quantization table shown in Table 1. If two locations are chosen such that they have identical quantization values, then any scaling of one coefficient will scale the other by the same factor to preserve their relative strength. It may be observed from Figure 2, that coefficient at location (4, 1) and (3, 2) or (1, 2) and (3, 0) are more suitable candidates for comparison because their quantization values are equal. The DCT block will encode a "1" if DCT (u1, v1) > DCT (u2, v2); otherwise it will encode a "0". The coefficients are swapped if the relative size of coefficients does not agree with the bit that is to be encoded.

Thus, instead of embedding any data, this scheme is hiding watermark data by means of interpreting "0" or "1" with relative values of two fixed locations in middle frequency region.

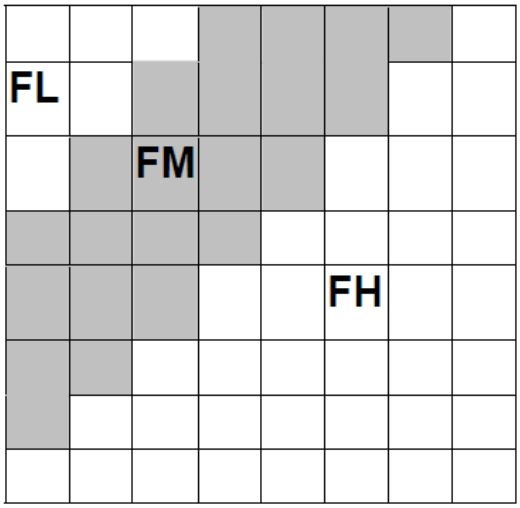

Figure 1: Frequency regions in 8*8 DCT

Swapping of such coefficients will not alter the watermarked image significantly, as it is generally believed that DCT coefficients of middle frequencies have similar magnitudes. Further, the robustness of the watermark can be improved by introducing a watermark "strength" constant *k*, such that DCT (u1, v1) – DCT (u2, v2) >*k*. If coefficients do not meet these criteria, they are modified by the use of random noise to satisfy the relation. Increasing *k* thus reduces the chance of detection errors at the expense of additional image degradation. By increasing k, larger coefficients remain larger even after lot of compression and thus help in decoding because their relative values decide the decoding of the watermark data. While extracting the watermark, again the 8x8 DCT of image in taken in which "1" is decoded if DCT (u1, v1) > DCT (u2, v2); otherwise a "0" is decoded.

Table 1: JPEG quantization Matrix

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

3. RANDOM MIDBAND EXCHANGE COEFFICIENT ALGORITHM

In this work, the 2 mid band coefficients are selected randomly and are generated by random sequence generator. First original image is broken up in 8*8 sub Images, then DCT of these images are taken. Watermark image which is to be embedded is converted in to linear vector. 4 bits of this linear vector watermark is to be encoded in 8bits. Mapping of 4 bits to 8 bits is unique and provide robustness to the proposed method. The robustness and uniqueness of this algorithm lies in the conversion of these 4 bit watermark sequences to 8 bit. These sequences are generated by a seeded pseudo-random generator. Due to this, size of the bits becomes double but the advantage is that the watermark cannot be detectable through normalized correlation.

While watermarking, we watermark each copy of image differently. There are 22 middle band coefficients in 8x8 DCT. For every copy of image, there will be 2 unique middle band coefficients to hide the watermark. So for every copy of image, those 2 coefficients will vary. We are simply selecting 2 coefficients randomly out of 22 coefficients lying in middle frequency band of 8x8 DCT so, can watermark 22C2 copies of a single image such that no two watermark images have same policy of watermark. While embedding, watermark image is converted into a string of "1"s and "0"s .Embedding process embed the watermark information within the original image by selected coefficients (frequency domain), in such a way that the watermark is undetectable to human eye and is achieved by minimizing the embedding distortion to the host image. The watermark extraction follows a reverse embedding algorithm, but with a similar input parameter set. The flow chart of the algorithm is as follows

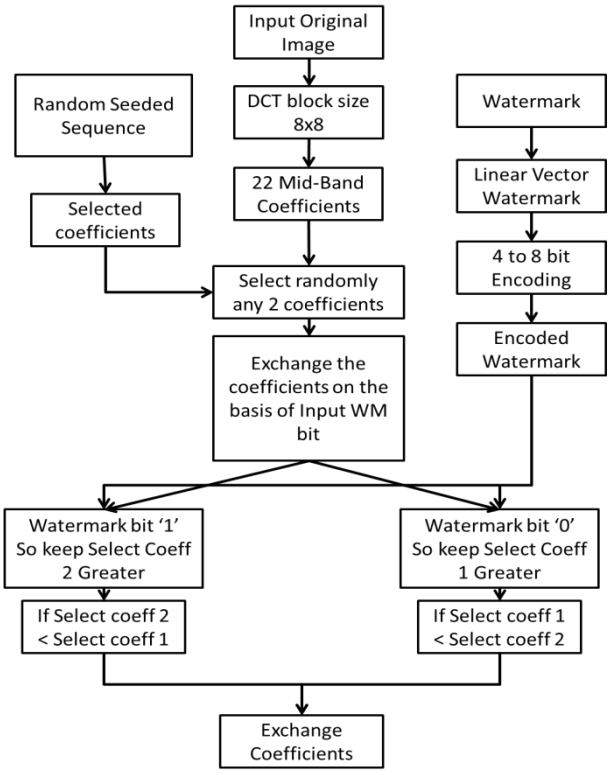

Figure3: Flow chart

Algorithm

3.1 Transform Algorithm

1. Load the gray scale host image which is to be watermarked (original image). The size of the original image is 512 × 512.
2. Load the watermark image. The size of the watermark is 32×32.
3. The host image is divided into a number of blocks; the size of each block is 8×8.

4. Guarantee that the number of host image blocks is equal to or greater than the number of watermark pixels.
5. Convert the watermark image in to a linear vector of '1' and '0'.
6. For each host image block compute the DCT transform coefficients.

3.2 4 bit to 8 bit Encoding

1. Take 4-4 bits (one by one) of linear vector watermark convert these bits in to decimal and store in array 'index'.
2. Take any 16 values from random permutation of the integers in the range N (here N=255, as it is a decimal value of 8 bits) for convenience we take 1st 16 values. Put these values in array 'map'.
3. Now mapping will be done, it will convert 4 bits sequence to 8 bit depending on the value at index in map array.

$$\text{Mapstr (ii,:)=map(index(ii)+1,:)}$$

3.3 Random coefficient generator

This step ensures that attacker cannot conclude the location of watermark data. In this step, 2 coefficients out of 22 mid band coefficients are chosen randomly. For every copy of image these 2 coefficients will vary and generated with the help of 'seed' Variable randomly.

1. Choose a seed variable for the random selection of 2 values, these coefficients are in the variable ' select '

$$\text{seed} = 5;$$

$$\text{jj} = 1;$$

$$\text{For} \quad \text{ii} = 1{:}\,2$$

$$\text{kk} = \text{jj};$$

$$\text{jj} = \text{ii} * \text{seed} + 2;$$

$$\text{select(ii)} = \text{Randi([kk, jj])};$$

$$\text{End}$$

2. Define 22 mid band DCT coefficients among the 64 DCT coefficients in a 8x8 block.
3. Chose 2 coefficients from above 22 coefficients depending on value 'select' in step 1 and put in to variable ' selectcoeff '

3.4 Watermarking embedding algorithm

In this algorithm, each 8 x 8 DCT block of an image is used to hide a single bit of watermark image. This embedding algorithm is based on some mathematical evaluation of 2 randomly selected mid band coefficients of Fm region which provides robustness to the proposed method. Algorithm is as follows:

1. If the watermarked bit to be embed is black (i.e. 0) then selectcoeff (1) >selectcoeff (2), if the above condition does not meet we need to swap them. If the watermark bit to be embed is white (i.e. 1) then selectcoeff (2) >selectcoeff (1), if this condition does not meet we need to swap them.

Hide 0: coefficient 1 >coefficient 2

Hide 1: coefficient 2 >coefficient 1

2. Take Inverse DCT of each block to reconstruct the watermark Image.
3. Display the gray level Watermarked image.

3.5 Watermark extraction algorithm

1. Input watermarked image
2. Process the image in blocks and perform DCT of Each block
3. Reshape the transformed image from step 2 in to linear message vector

$$\text{If selectcoeff (1)} > \text{selectcoeff (2)}$$
$$\text{Then WM bit} = 0$$
$$\text{Otherwise WM bit} = 1$$

4. Convert this linear extracted watermark into eight bit sequences.
5. Convert this 8 bit sequence to 4 bit sequence.
6. Reshaping the extracted message vector to 2D binary watermark image
7. Display Recovered Image.
8. Calculating PSNR and Similarity ratio between the embedded and the extracted watermark.

4. SIMULATION RESULTS

The above algorithm is applied on images like Lena and Baboon. For this purpose, MAT LAB software is used. Peak Signal to Noise Ratio (PSNR) and Similarity Factor(SM) has been calculated for analysis. In order to test the performance of this watermarking algorithm, we have used 512*512 gray images of Lena and Baboons in JPEG format. The original and extracted watermark is shown in figure 4. The cover images and the watermarked images of Baboon and Lena are shown in figure 5 and 6 respectively.

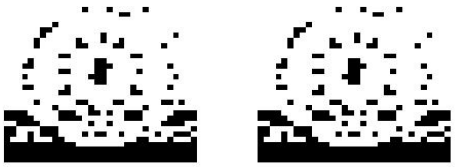

Figure 4: original watermark and recovered watermark

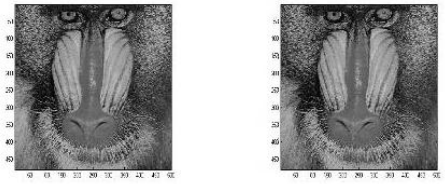

Figure 5: Original Baboon Image and watermarked image

Figure 6: Original Lena Image and Watermarked Image

The PSNR is defined as:

$$\text{PSNR} = 10 \log_{10} \left[\frac{(255)2}{MSE}\right] db$$

Where MSE is the mean square error of two images of N x N pixels is defined as

$$MSE = \frac{1}{\text{N2}} \sum_{\text{i=1}}^{\text{N}} \sum_{\text{j=1}}^{\text{N}} \left(\text{P ij} - p_{ij}^{'}\right) 2$$

Where P_{ij} is the original pixel value and $p_{ij}^{'}$ is the reconstructed pixel value. When SNR approaches infinity, the original image and output image are totally the same.

The similarity factor has value [0, 1] calculated using following figure 7. If SM = 1 then the embedded watermark and the extracted watermark are same. Generally value of SM>.75 is accepted as reasonable watermark extraction.

$$SM = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} W_M(i,j) W_M^*(i,j)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} W_M(i,j)^2 \times \sum_{i=1}^{M}\sum_{j=1}^{N} W_M^*(i,j)^2}}$$

Figure 7: Value of SM between the watermark and extracted watermark

In figure 7 $W_M(i, j)$ refers to watermark image and $W_M^*(i, j)$ refers to extracted watermark

The PSNR value of watermarked Lena is 54.91 db while the watermarked Baboon is 39.17 db and SM is 1.Table 2 clearly shows better results in terms of PSNR as compare to reference algorithm [11]. For comparison purpose, only gray scale images in jpeg format is considered through reference.
After extracting the watermark, the normalized cross-correlation (NCC) is calculated to evaluate the effectiveness of our scheme. The normalized cross-correlation is calculated between the original watermark and the watermarked image. It is also used to find correlation between cover image and watermarked image. NormxCorr2 function is used for finding the correlation Imnoise function is used to introduce both type of noise i.e. Gaussian, salt and pepper noise.

Table 2 : Comparison of PSNR values (db) for images

Type of Gray image (JPEG)	This Algorithm	Reference Algorithm [11]
Lena Image	54.91	50.25
Baboon image	39.17	34.78

Table 3 : PSNR values for images undergone different attacks

Attack	Lena PSNR (db)	Baboon PSNR (db)
Gaussian Blur factor(.2) v=.01	38.13	37.79
Gaussian v=.02	37.12	37.31
Gaussian v=.04	35.54	37.76
Salt &pepper v=.1	36.23	35.1
Salt &pepper v=.15	35.28	34.8
Salt &pepper v=.2	34.91	34.61

In table 3, v refers to variance

Table 4: PSNR values for Lena image under JPEG compression

Sr. No.	Quality Factor	PSNR(db)
1	15	43.21
2	20	42.43
3	50	42.34
4	80	41.87

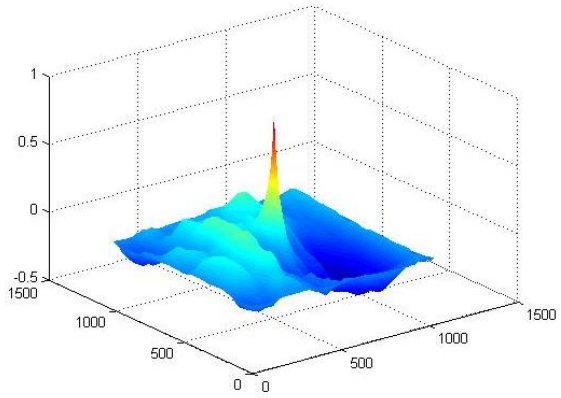

Figure8: Correlation between the original Lena image and the watermarked Lena image

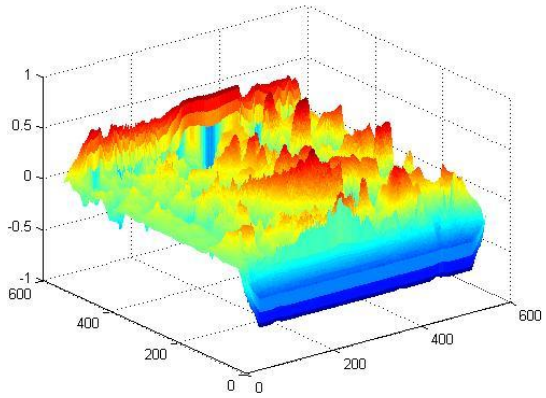

Figure9: Correlation between the watermark and watermarked image for Lena Image

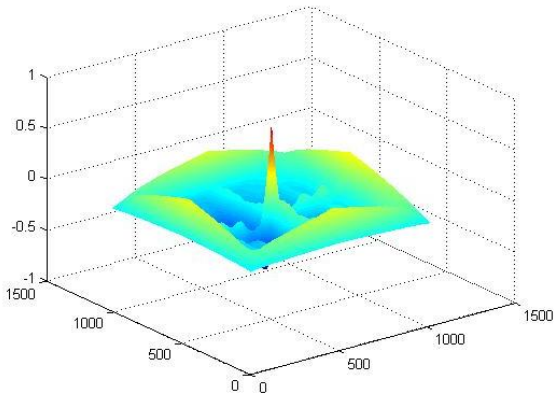

Figure10: Correlation between the Original baboon image and watermarked Baboon image

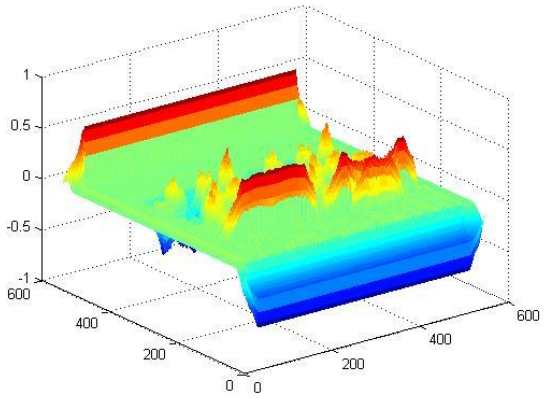

Figure11: Correlation between the watermark image and the watermarked image for Baboon Image

A peak in the centre of the surface in figure 8 and 10 depicts that both of the images are same and first is contained in the second. Some small peaks are due to embedded watermark. The correlation between the watermark and the watermarked image can be done by the attacker for blind watermark detection to determine the presence of watermark in the watermarked image. The correlation plot should result in to a peak if the watermark image is detected. The figure 9 and 11 clearly shows correlation result which appears as randomly distributed noise so blind detection is failed.

5. CONCLUSION

This paper presents a scheme for image watermarking based on random selection of 2 middle-band coefficients of DCT domain. Moreover, sequence of 4 bit is mapped in to unique sequence of 8 bits. This provides robustness to the proposed method. This method gives better results in terms of PSNR. In the proposed strategy, the watermark embedding is done using DCT frequency transform in different blocks of the image. Since the method is block based so processing time is high. The proposed future work is to reduce the complexity of the method, use of public and private key exchange method to exchange secret keys. Also this strategy can be mixed with linear transformation resistant methods of watermarking to increase the domain of resisting attacks.

6. ACKNOWLEDGMENTS

We would like to express our gratitude to experts Prof Dhananjay Gupta, Principal Arya College of Engineering and I.I (ACEIT), Associate Prof. Kirti Vyas (ACEIT) for their guidance and contributions. We would like to thank our family members for the support and care.

7. REFERENCES

[1] J.R.Hemandz. , M.Amado "DCT domain watermarking techniques for still images as detector performance analysis and a new structure," in IEEE Transactions on Image Processing, 2000, vol. 9, pp. 55-68

[2] Jian Zhao & Eckhard Koch .Embedding Robust labels For Copyright Protection in Int. Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies, Vienna, August 1995

[3] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "A DCT Domain System for Robust Image Watermarking," Signal Processing, vol. 66, no. 3, pp. 357-372, May 1998.

[4] Neil F Johnson and Stefan C. Katzenbeisser "A survey of steganography techniques

[5] C.T.Hsu, and J.L.Wu., "Hidden Signatures in Images", Proc. IEEE International Conf. on Image Processing, ICIP-96, Vol. 3, pp.223-226.

[6] Lin Liu "A Survey of Digital Watermarking Technologies"

[7] Heather Wood " Invisible digital watermarking in the spatial and dct domain for colour images"

[8] Vikas Saxena, J.P.Gupta" collusion Attack Resistant Watermarking Scheme for Colored Images using DCT" IAENG International Journal of computer Science, IJCS_34_2_02

[9] Hassan I. Saleh "Efficient Mid-band Exchange Watermarking System"

[10] T.K. Tewari and Vikas Saxena "An Improved and Robust DCT based Digital Image Watermarking Scheme" International Journal of Computer Applications (0975 – 8887),Vol. 3 – No.1, June 2010

[11] Rekha Chaturvedi, Naveen Hemrajani e.tal "Analysis of Robust Watermarking Technique Using Mid Band DCT Domain for Different Image Formats" , International Journal of Scientific and Research Publications, Vol. 2, Issue 3, March 2012 1 ISSN 2250-3153

[12] Ritu Pareek, P.K.Ghosh "DCT based image watermarking for Authentication and Copyright Protection" International Journal of Engineering and Advanced technology" ISSN-2249-8958 Vol. 1, Issue- 3, Feb 2012.

[13] SK.Sofia, C. Rajendra "Study on image broadcast using watermark and security techniques" IJARCET ,Vol. 1 , issue 3 , june2012

[14] Dasu Vaman Ravi Prasad "An Improved Invisible Watermarking Technique for Image Authentication", IJARCSSE , Vol. 3 , issue 9 , Sep 2013