ISSN 2250-3153

Analysis of Robust Watermarking Technique Using Mid Band DCT Domain for Different Image Formats

Mrs. Rekha Chaturvedi, Mr. Abhay Sharma, Mr. Naveen Hemrajani, Mr. Dinesh Goyal

Abstract- Aliquot watermarking is the unique idea in aliquot media for copyright protection. Various watermarking algorithm has been developed in recent years, but cognitive content of the intent, as they serve, they demarcated from each other. This context presents a new proposal for hiding a logo-based watermark in color still image. This dodge is based on averaging of central frequency coefficients of block Discrete Cosine Transform (DCT) coefficients of an image. It is unique from earlier dodge based on middle frequency coefficient by mean of high redundancy, to nurture malicious attacks. Here we propose algorithm of aliquot watermarking technique based on DCT (Discrete Cosine Transformation) using mid band for robustness. Through adjusting the block DCT coefficient of the image the watermarks are adumbered. We have been using the DCT mid band co-efficient for different image formats and the analysis appeared that the JPG image format's PSNR value on an average was lowest in contrast with others. The propound dodge also describes the expedient results that the method has unassailable robust.

Index Terms- eliquot watermarking, DCT coefficient, PSNR and SM.

I. INTRODUCTION

With aliquot multimedia distribution over World Wide Web, authentications are more threatened than ever due to the possibility of unlimited copying. So, watermarking techniques are proposed for copyright protection or authentication of aliquot media. various watermarking methods for image have been proposed [1]- [4].

Various researchers are joining this area and number of publications is increasing exponentially. Most of the work is based on ideas known from spread spectrum communication [5] which is additive embedding a pseudo noise watermark pattern and watermark recovery by correlation [6]. Cox et al suggested using the DCT domain [6], which has been extensively studied and transform used in JPEG compression. Further advantage of using DCT domain includes the fact that frequency transform is widely used in image and video compression and DCT coefficients affected by compression are well known. This dodge proposes an efficient use of middle-band coefficients exchange to hide the watermark data. This dodge uses the idea of Middle Band Coefficient Exchange which was discussed by Koch and Zhao [8] and further expressed by Johnson and katezenbeisser [9]. Later Hsu and Wu also used the DCT based algorithm to implement the middle band embedding [10]. This is based on middle-band coefficients exchange [42].

Our main motivation behind selecting middle-band coefficients exchange proposal as a base is that this proposal has proven its robustness.

Section 2 discusses the background studies. Section 3 describes the proposed method and section 4 discusses the results.

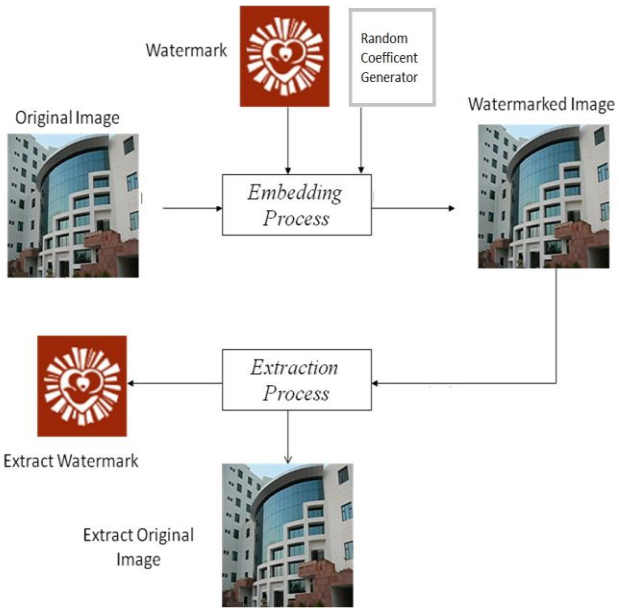

Figure 1: block diagram of watermarking process

Watermarking is easy to manipulate multimedia products and make its unauthorized duplication and distribution. This has resulted in copyright protection of eliquot contents on the Internet and protecting rights of buyer and establishing his ownership of legal copy.

II. MOTIVATIONS (MIDDLE-BAND COEFFICIENT EXCHANGE PROPOSAL)

Classical Middle-band based algorithm interchanges only Single pair of coefficients and it is quite identifiable by the attacker.

A. Middle-band Coefficient Exchange Proposal

The middle-band frequencies coefficients (FM) of an 8x8 DCT block are shown in Figure 2. FL is used to denote the lower frequency coefficients of the Block, while FH is used to denote the higher frequency Coefficients. FM is chosen as embedding region to provide Additional resistance to lousy compression techniques, while avoiding significant modification of the cover image. First we have 8x8 DCT of original image. Then two

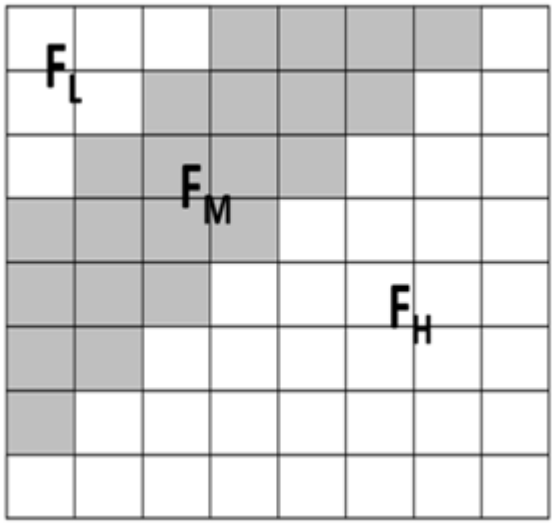

Figure 2: Showing mid-band coefficient that can be used for watermarking

locations DCT (u1, v1) and DCT (u2, v2) are chosen from the FM region for comparison of each 8x8 block. We should select the coefficients based on the recommended JPEG quantization table shown as Table-I. If two locations are selected such that they have identical quantization values in JPEG quantization table, then any scaling of one coefficient will scale the other by the same concept to preserve their relative strength. Based on Table-I, we observe those coefficients 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".

Table 1

16	11	10	16	24	40	51	61
12	12	14	19	26	48	16	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	108	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

Middle-Band Coefficient Exchange Algorithm having some draw back that by analysing 5- 6 watermarked copies one can easily find that there are some pattern that can be predicted by attacker.

III. WATERMARK EMBEDDING AND EXTRACTING PROCESS

In Watermarking we used different algorithms for different purpose. we have used Input and Transform block for changing secret and cover image .Random coefficient generator generate the 4 coefficients from 22 coefficient and also provides the layer which we can use for watermarking . Embedding process embed the watermark information within the original image by modifying all or selected pixel values (spatial domain); or 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 system block diagram for the embedding process is shown in Figure 3.

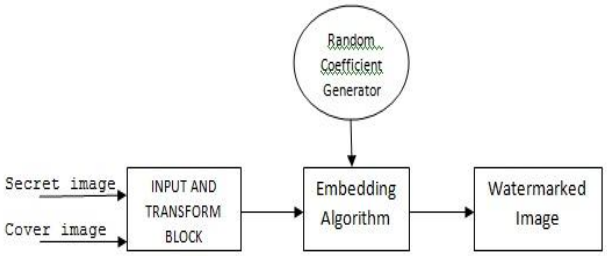

Figure 3: Watermark Embedding Process

The watermark extraction follows a reverse embedding algorithm, but with a similar input parameter set.
In this dodge we used the DCT domain for Watermark embedding and extracting process on permuted image.

IV. WATERMARK ALGORITHM

Algorithm 1: (Input & Transform Algorithm)
Step 1: Start
Step 2: Clearing variables and Clear output screen.
Step 3: Read Input Cover image and Defining block size for the image, one block will be watermarked with 1bit of watermark vector.
Step 4: Read Secret image and convert it into binary image.
Step 5: Reshaping the message to a linear vector watermark for the ease of Watermarking & Check the message isn't too large for cover image.
Output: Secret message (monochromatic) and 8*8 DCT Cover image.
Algorithm 2: (Random Coefficient Generator)
Step 1: Prepare a seed and random sequence for watermarking to select Coefficients for the mid band of the dct block.

```
seed=5;
jj=1;
for ii=1:4
kk=jj;
jj=ii*seed+2;
select(ii)=randi([kk,jj]);
end
```

Step 2: Define mid band DCT coefficients among the 64 DCT coefficients in a 8x8 block.
Step 3: Select the 4 coefficients from 22 coefficients for average comparison using seed.
Step 4: Selecting which layer to watermark from R, G, B.

Output (Random coefficient and one layer of RGB)

Algorithm 3: (Embedding Algorithm)

Step 1: Generate Images from Input& Transform Algorithm (Secret message monochromatic and Cover image of 8*8 DCT)

Step 2: Generate Ri from Random Coefficient Generator algorithm (selecting coefficient and one layer from R, G, B)

Step 3: For Each Block Repeat Step 4 to 5.

Step 4: Take Average avg1 of 18 remaining Coefficient. On the basis of Ri and Average

If the watermark bit to embed is 0 then for all 4 chosen coefficients, change the value of coefficients which is 'T' less than the average

```
for ll=1:4
beval=avg1-T;
Assign the value of beval.
end
```

If the watermark bit to embed is 1 then for all 4 chosen coefficients, change the value of coefficients which is 'T' greater than the average

```
for ll=1:4
beval=avg1+T;
Assign the value of beval;
end
```

Here 'T' indicates the strength of watermark.

Step 5: Take Inverse DCT to reconstruct the Watermark Image.

Step 6: Join the other two components of a RGB

(Three layers image other than the depth. Here the depth is 1 so other layers are 2 & 3. Joining process so called concatenation of the three layers)

Step 7: Display watermarked RGB image

Algorithm 4: Watermark Extraction Algorithm:

Step 1: Input watermarked image

Step 2: Process the image in blocks perform DCT of Each block

Step 3: find average of remaining 18 coefficients

Step 4: for every block

a) If at least 1 out of 4 chosen coefficients is less than average then we Interpret "0" bit as watermark
b) If at least 1 out of 4 chosen coefficients is greater than average then we Interpret "1" bit as watermark

Step 5: Reshaping the extracted message vector to 2D binary watermark image

Step 6: Calculating similarity ratio between the embedded and the extracted watermark

Step 7: End.

V. SIMULATION RESULTS

In our simulation we apply the above algorithm for different formats of the image. For this purpose we have use mat lab software. Peak Signal to Noise Ratio (PSNR) and Similarity Factor(SM) has been calculated for analysis.

For test the performance of this watermarking proposal, we have used 256×256 color images which are of different format such as bmp, jpg and png. The original watermark is shown in figure 4. The watermarked images and the extracted watermark are shown in figure 5-7.

The PSNR is defined as:

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

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

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

Where P_{ij} is the original pixel value and p'_{ij} is the reconstructed pixel value.

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

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

Where W_M is Original Watermark and W_M^* is detected watermark.

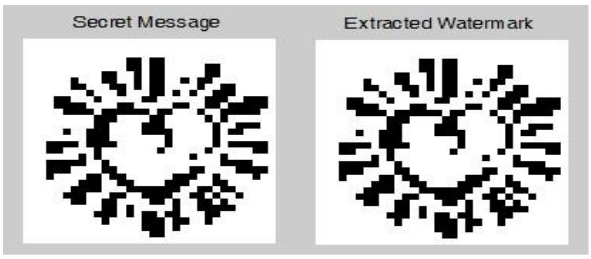

Figure 4: Original Watermark and extract watermark

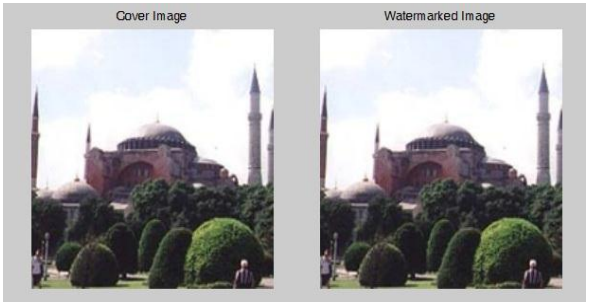

Figure 5: Cover Image and Watermarked image for BMP format

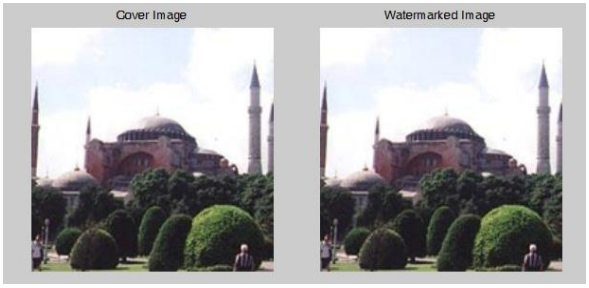

Figure 6: Cover image and Watermarked image for JPEG format

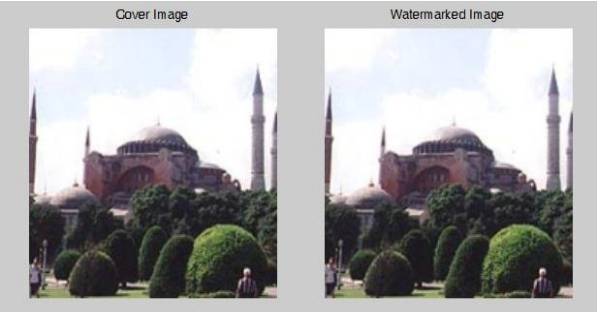

Figure 7: Cover Image and Watermarked Image for PNG format

The following Table 2 shows the PSNR of the different watermarked images and the Similarity factor (SM) of their extract watermarks.

Table1: Results for different image formats

Type of Image	PSNR1	PSNR2	PSNR3
BMP (image1)	42.09	37.40	38.77
JPG (image2)	35.90	34.37	36.06
PNG (image3)	40.94	39.21	37.48

As Table showing that PSNR for Bmp image format is high as compare to other image format like Jpg and Png. This clearly shows that this watermarking proposal is extremely well for watermarking Bmp image formats it also provides robustness against different type of security attacks.

The watermarked image and extracted image have SM >.75 this shows Watermarked image has very good quality so that it is not easily visible by human eyes. Figure 8 shows the graph between different image formats against PSNR values.

.

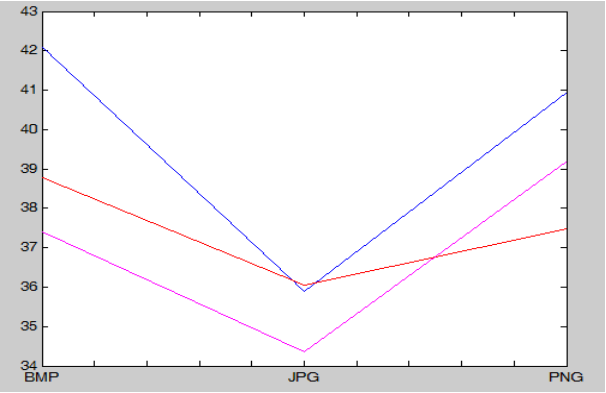

Figure 8: Graph between PSNR values and BMP, JPG, PNG

VI. CONCLUSION

This paper presents a analysis of image watermarking For different formats of images. This algorithm is based on average of middle-band coefficients of DCT domain. Including the random no generator algorithm makes the scheme more robust Experimental results prove that proposed scheme is robust and outperforms for BMP image format. It will be a great research area where changing in the layers of RGB can prove better results.

ACKNOWLEDGMENT

We would like to express our gratitude to experts Professor Naveen Hemrajani, Dean (Engineering), Associate Prof. Dinesh Goyal (HOD, CS Department) for their guidance and contributions. We would also like to thank for the valuable informations they provided us. We would like to thank our family members for the love and care.

REFERENCES

[1] J. R. Hemandez, 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] Q. Du, "Color image eliquot watermarking algorithm based on DCT and quantifying," in Journal of Soochow university, 2006, vol. 26, pp. 47-51.

[3] Z. M. Zhang, L. Wang, "Semiblind image watermarking algorithm in DCT domain with chaotic encryption," in Computer Engineering, 2003, vol. 29, pp. 10.

[4] L. S. Liu, R. H. Li, Q. Gao, "Method of embedding eliquot watermark into the green component of color image," in Journal of XianJiaotong university, 2004, vol. 38, pp. 1256-1259.

[5] S. Z. Yu, "A color image-adptive watermark based on wavelet transform," in Computer Simulation, 2006, vol. 23, pp. 132-134.

[6] L. Wei, H. T. Lu, F. L. Chung, "Robust eliquot image watermarking based on subsampling," in Applied Mathematics and Computation, 2006, vol. 181, pp. 886-893.

[7] N. Bourbakits and C. Alexopoulos, "Picture data encryption using scan patterns", Pattern Recognition, Vol. 25, No. 6, 1992, pp. 567–581.

[8] C. C. Chang and H. M. Tsai, "A generalized secret sharing proposal", Journal of Systems and Software, Vol. 36, No. 3, 1997, pp. 267–272.

[9] C. C. Chang, J. Y. Hsiao, and C. S. Chan, "Finding optimal LSB substitution in image hiding by using dynamic programming strategy", Pattern Recognition, Vol. 36, No.7, 2003, pp.1583–1595.

AUTHORS

First Author – Rekha Chaturvedi, M.Tech, Email id - rekhachaturvedi12@gmail.com.
Second Author – Abhay Sharma, M.Tech, Email id - abhaysharma2004@gmail.com
Third Author – Naveen hemrajani, Phd, Email id - navin_h@yahoo.com.