A Novel Watermarking Scheme for JPEG Images

VIKAS SAXENA
Dept. of CSE and IT
Jaypee Institute of information Technology University
A-10, Sec-62, Noida
INDIA
vikas.saxena@jiit.ac.in

J.P. GUPTA
Jaypee Institute of information Technology University
A-10, Sec-62, Noida
INDIA
jp.gupta@jiit.ac.in

Abstract: - Image watermarking with both insensible detection and high robustness capabilities is still a challenging problem. Even if some of the watermarking areas involve huge financial implication, there are relatively fewer efforts presented, which primarily focus the sustainability against some attacks, which are specific to financial application area particularly. One of such application area is "Fingerprinting" and a major threat for this area is "Collusion Attack". This paper presents an inherently collusion attack resistant (ICAR) scheme for hiding a logo-based watermark in JPEG images. This scheme is based on averaging of low and middle frequency coefficients of block Discrete Cosine Transform (DCT) coefficients of an image. Experimental results show the robustness of the proposed scheme against the JPEG compression and other common image manipulations.

Key-Words: - Collusion attack, Discrete Cosine Transform (DCT), Image watermarking, JPEG compression.

1 Introduction

With digital multimedia distribution over World Wide Web, authentications are more threatened than ever due to the possibility of unlimited copying. Watermarking techniques are proposed to solve the problem of copyright protection and authentication of digital media.

Many watermarking methods for images have been proposed [1] - [4]. More and more researchers are joining this area and number of publications is increasing exponentially. Most of the work is based on idea known from spread spectrum communication [5], which is additive embedding a pseudo-noise watermark pattern and watermark recovery by correlation. Cox et al suggested using the DCT domain [6], which has been extensively studied because this transform is used in JPEG compression. Further advantage of using DCT domain includes the fact that this frequency transform is widely used in image and video compression and DCT coefficients affected by compression are well known.

Most of the images, present on WWW, are in Joint Photographic Experts Group (JPEG) format, where as relatively less work has been conducted for watermarking the JPEG images. More research exists for gray level images.

Therefore in this paper we propose a watermarking technique to hide the watermark data in JPEG images.

There are huge financial implications for watermarking schemes like fingerprinting, but no scheme has been developed, which is, by design, is resistant to at least one attack related to that area.

Collusion attack is the severe problem for "fingerprinting" [43]-[45]. So while designing the proposed watermarking scheme, we ensured that proposed scheme is inherently collusion attack resistant.

This paper uses the idea of Middle Band Coefficient Exchange (MBCE) scheme, which was discussed by Koch and Zhao [8]. It was further explained by Johnson and Katezenbeisser in [9]. Later Hsu and Wu also used the DCT based algorithm to implement the middle band embedding [10].

Our main motivation behind selecting middle-band coefficients exchange scheme as a base is that this scheme has already proven its robustness against those attacks which, any how, do not affect the perceptual quality much, such as JPEG compression attack.

Section 2 discusses the preliminaries. Section 3 describes the proposed method, section 4 discusses the results and the comparative study of proposed scheme with other similar, state-of-art schemes.

2 Preliminaries

2.1 Fingerprinting and Collusion attack

If monitoring and owner identification applications place the same watermark in all copies of the same content, then it may create a problem. If out of "n" number of legal buyer of content, one starts to sell the contents illegally, it may be very difficult to know who is redistributing the contents without permission. Allowing each copy distributed to be customized for each legal recipient can solve this problem. This capability allows a unique watermark to be embedded in each individual copy. Now if owner finds an illegal copy, he can find out who is selling his contents by finding the watermark, which belongs to only single legal buyer. This particular application area is known as fingerprinting. This is potentially valuable both as a deterrent to illegal use and as a technological aid to investigation.

Researchers working on fingerprinting area primarily focus on the "collusion attack". If attacker has access to more then one copy of watermarked image, he/she can predict/ remove the watermark data by colluding them. Network Technology research Center states on their website that they pay at least equal attention to watermark attacks/counter-attacks as watermark designs [43]. To facilitate pirate tracing in video distribution applications, different watermarks carrying distinguishing client information are embedded at source. If a few clients requesting for the same source data get their differently marked versions together, they may collude to remove or weaken the watermark leading to what is commonly called "collusion attack".

Collusion attacks are powerful attacks because they are capable of achieving their objective without causing much degradation in visual quality of the attacked data (sometimes, visual quality may even improve after attack.).

In their paper "Multi-bits Fingerprinting for Image", authors focused on collusion attack for fingerprinting application [44]. They state that the main difference between watermarking and fingerprinting is that different copies for each customer can be produced. This point is very helpful for attackers. Attackers compare several fingerprinting copies and find the location of the embedded information and destroy it by altering the values in those places where a difference was detected.

One more work, specially conducted against collusion attack can be found as "Collusion-resistant watermarking and fingerprinting (US Patent Issued on June 13, 2006)" [45].

2.2 Middle-band Coefficient Exchange Scheme and its limitation

The middle-band frequencies coefficients (F_M) of an 8x8 DCT block are shown in Fig. 1.

F_L is used to denote the lower frequency coefficients of the block, while F_H is used to denote the higher frequency coefficients. F_M is chosen as embedding region to provide additional resistance to lossy compression techniques, while avoiding significant modification of the cover image. First we take 8x8 DCT of original image. Then two locations DCT (u_1, v_1) and DCT (u_2, v_2) are chosen from the F_M region for comparison of each 8x8 block. We should select the coefficients based on the recommended JPEG quantization Table shown as Table1. If two locations are chosen such that they have identical quantization values in JPEG quantization Table, then any scaling of one coefficient will scale the other by the same factor to preserve their relative strength. Based on TableI, 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 (u_1, v1) > DCT (u_2, v2); otherwise it will encode a "0".

So, instead of embedding any data, this scheme is hiding watermark data by means of interpreting "0" or "1" with relative values of 2 fixed locations in F_M region.

The coefficients are swapped if the relative size of each coefficient does not agree with the bit that is to be encoded [8] [9].

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, we can improve the robustness of the watermark by introducing a watermark "strength" constant k, such that DCT (u_1, v_1) – DCT (u_2, v_2) > k. If coefficients do not meet these criteria, we modify by the use of random noise to then satisfy the relation. Increasing k thus reduces the chance of detection errors at the expense of additional image degradation [8] [9]. While extracting the watermark, we again take the 8x8 DCT of image, decode a "1" if DCT (u_1, v1) > DCT (u_2, v2); otherwise it will decode a "0" to form the watermark.

Experimental results show that Middle-Band Coefficient Exchange is quite efficient against JPEG compression, Cropping, Noising and other common

image manipulation operations. But above scheme has one serious drawback. If only one pair of coefficient is used (say (4, 1) and (3, 2)) to hide the watermark data then it is vulnerable to collusion attack. By analyzing 4 -5 watermarked copies of image, one can easily find out that these coefficients always have a certain pattern and attacker can predict the watermark as well as destroy it.

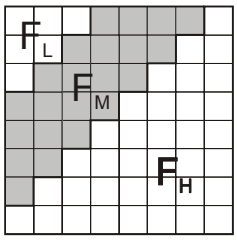

Fig. 1: Frequency regions in 8x8 DCT

Table1: JPEG quantization Table

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 Proposed Scheme

Like classical Middle band coefficient exchange scheme, we considered FM region of 8x8 DCT blocks. Instead of swapping only one pair of coefficient, we swapped more than one coefficient pair to introduce redundancy and then introduced randomness to inject ICAR nature. JPEG image format don't store the pixel's actual value but it stores the image in frequency domain. So, we need to convert the JPEG image into its equivalent spatial domain image (YCbCr to RGB) and then take 8x8 block DCT on its color channels to get the FM region.

Since JPEG is a very high compressed format, we knew that as soon as we convert this spatial domain image into JPEG format, lots of coefficients would change their values. This would create problem in recovering the watermark data if we consider the relative strengths of coefficients pairs of FM region only. Along with this, whenever any attack will be conducted on the image, it will be very difficult to recover the watermark data from FM region just by using the relative value of coefficients. We must, therefore, provide extra robustness by involving some data items whose value doesn't changes much during the image compression, manipulation or attacks. In each pair (X, Y) of data items, which are deciding the decoding of watermark data, at least one data item, X or Y, must be very robust i.e. its value should not get changed. To resolve this issue, we decided to take the advantage of JPEG compression-decompression scheme itself. In an 8x8 DCT block, large value of the top-left corner is called the DC coefficient. The remaining 63 coefficients are called the AC coefficients. This DC coefficient is the major dominating value while decompressing. This DC value alone can regenerate the best approximated image by taking the IDCT. If this value is altered then, image is heavily affected. So, we decided to take the contribution of this DC coefficient apart from coefficients from F_M region to interpret the watermark data, to make our scheme robust. If the relative value of two data items has to interprate "0" or "1", we decided to choose the "Average (Av)" of DC coefficient and all 22 coefficints of FM regions as a data item, because this avarage is very less susceptible to change. As long as attacker is not chnaging the perceptual quality of the image up to a great extant, the avrage of DC and all 22 Coefficients from FM region will not alter much. We hide the watermark data by using the relative value of the Av and chosen 4 coefficients from FM region. More details of the watermark embedding algorithms are described in section III.B. To ensure ICAR property, we watermarked each copy of a single JPEG image with different policy.

The proposed watermarking scheme can be defined as a 7-tuple (X, W, P, T, G, E, D) where:

1. X denotes the set of instances Xi, of a particular JPEG image, (If N copies of an image are to be watermarked, then $0 \le i \le N$);
2. W denotes the monochrome watermark logo;
3. P denotes the set of policies Pi , $0 \le i \le N$;
4. "T" is the "watermark strength parameter".
5. G denotes the policy generator algorithm G: Xi $\rightarrow$Pi;

   Each Xi will have a unique Pi, i.e. a different policy to hide the watermark data.
6. E denotes the watermark embedding algorithm, E: Xi x W x Pi $\rightarrow$Xi';
7. D denotes the watermark detection algorithm, D: Xi' x Pi$\rightarrow$ W';

   Where W' represents the extracted watermark.

The parameter "T" is analogous to "k" of classical MBCE scheme. In classical MBCE scheme, relative strength of 2 coefficient's value of FM region decides the decoding of "1" or "0". If the relative strength of 2 values has to decide the decoding of "0" or "1" then larger value should remain larger even after image manipulations. So, we adjust these values in a way, that the difference between the 2 values becomes larger than a certain threshold value. We name this threshold value as "Watermark Strength Parameter" because this value decides the robustness of watermark data. Certainly, it has an impact on the image perceptibly. So, we have to decide this threshold value in such a way that, our image doesn't loose its quality much. The value of "T" may differ for each image. Out of these 7 tuples, last 3 tuples are algorithms, which are discussed below:

3.1 G, The policy generator algorithm

To ensure ICAR nature, we need to watermark each copy Xi of an JPEG image X differently. Therefore, we need a different watermarking policy for each copy of the image to be watermarked. Here "Policy" means that, for every copy of the image, there will be unique combination of 4 middle band coefficients. First we had to convert the source JPEG image into its equivalent true colored 24-bit BMP image. Then, to generate a policy, we simply take 8x8 DCT of a chosen color channel of the input image Xi and randomly select 4 coefficients out of 22 middle band coefficient of FM region, from any of the red, green or blue color channel. So, numbers of policies that can be generated are $^{22}C_4$=7315 which means that 7315 copies of a single image can be watermarked such that no two watermarked images have same policy. This step ensures that attacker cannot conclude the location of watermark data by colluding many watermarked copies of an image. This also depicts that our proposed scheme is an ICAR scheme. Policy generator algorithm also returns the color channel to be used to carry the watermark.

3.1.1 Color Channel Selection

Bossen et al.[46] have stated that the watermarks should be embedded mainly in the BLUE color channel of an image, because human eye is least sensitive to change in BLUE channel. But we found, the suitability of color channel, to hide the watermark data, dependent on the image itself. We explored that the color channel, which should be used, can be found on the basis of the amount of the color present in the image or on the basis of histogram of each color channel (i.e. color with spreader histogram should be given priority). We found that for few images, BLUE channel may not give the optimum results. We proposed that the color channel with the lowest "Standard Deviation (SD)" should be selected. More details and result related to this issue are given in the section 4.3.

3.2 E, The watermark embedding algorithm

In this algorithm, each 8x8 DCT block of an image is used to hide a single bit of watermark logo. As we have stated, our embedding algorithm is based on averaging the coefficients of F_M region and the DC coefficient and we are hiding "1" or "0" by using the relative values of 4 coefficients with this "Av". The algorithm is given as below:

1. Repeat steps 2-12 for i=1…..n;
   // where 'n' is the number of copies of a single image to be watermarked//
2. INPUT (Xi);
3. Convert the Xi into its equivalent spatial domain 24-bit colored image.
4. Take 8x8 block DCT of Xi;
5. INPUT(W);
6. Convert W into a string S=(Sj | Sj={0,1}, for j=1…..length of the watermark);
7. Let L=STRING_LENGTH(S);
   // L is the length of watermark data. If L=1000, then first 1000 DCT block of Xi are used//
8. Pi=CALL(G);
   //All generated Pi s shell be stored in an author's database for the detection propose in future. Let the Pi for chosen Xi be, Pi={(5,1), (4,2), (6,3) and (5,4)} in the chosen color channel *//*
9. Calculate the average "Av" of remaining 18 middle band coefficients and DC coefficient.

   Av= [DCT (0,0)+ Sum(22 Middle band coefficients)- Sum (4 chosen coefficients chosen by Pi]/ 19.
10. Repeat steps 11-12 for r=1…..L;
11. *//Now like classical MBCE scheme, relative strength of average "Av" and chosen 4 coefficients in step 7 will interpret "0" or "1" of watermark data. To hide "0", for all 4 chosen coefficients in step 7, we assigned the value of coefficients which is 'T' less then the average "Av". To hide "1", for all 4 chosen coefficients in step 7, we assigned the value of coefficients which is 'T' greater then the average "Av".//*

    Read Sr;

    If (Sr=0)

    Then

    DCT(5,1)=Av - T;

DCT(4,2)=Av - T;
DCT(5,4)=Av - T;
DCT(6,3)=Av - T;

Else
DCT(5,1)=Av + T;
DCT(4,2)=Av + T;
DCT(5,4)=Av + T;
DCT(6,3)=Av + T;

12. Take IDCT to reconstruct Xi;
13. Convert Xi back to its JPEG format.
14. End.

3.3 D, The Watermark detection algorithm

Watermark extraction is the reverse procedure of watermark embedding. To extract the watermark from the watermarked JPEG image, first we converted it into its equivalent 24 bit colored images and then calculated the average "Av" in a same way, as in embedding algorithm. Owner has a record of all policies used to watermark the images. Based on "policies"; owner of the image can recover watermark using following rule:

1) If at least 1 out of 4 chosen coefficients are less then Av, *Interpret "0"; and*
2) If at least 1 out of 4 chosen coefficients are greater then Av, *interpret "1".*

The detection algorithm steps are as follows:

1. INPUT(Xi');
   // Xi' is the attacked copy of a watermarked image//
2. Convert Xi into its equivalent 24 bit colored image;
3. Take 8x8 block DCT of Xi' and calculate Av;
4. For all Pi in author's database, repeat the steps 5.
   // If initially 10 copies were watermarked, then out of 10 policies, for 1 policy, watermark will be recovered correctly. To explain further steps, we are assuming that now algorithm is in a loop where Pi is {(5,1) (4,2) (5,4) and (6,3)}, which was used to watermarked this particular Xi'.//
5. Repeat the steps 5 for j=1….L;
   // L is the length of watermark data. A single bit will be recovered form one 8x8 DCT block//
   Take j'th DCT block to form j'th bit of watermark as follows:

If DCT(5,1)<=Av
T1=1 else T1=0;
If DCT(4,2)<=Av
T2=1 else T2=0;
If DCT(5,4)<=Av
T3=1 else T3=0;
If DCT(6,3)<=Av
T4=1 else T4=0;
If(T1+T2+T3+T4>=1)
Decode "0"

If DCT(5,1) > Av
T1=1 else T1=0;
If DCT(4,2) > Av
T2=1 else T2=0;
If DCT(5,4) > Av
T3=1 else T3=0;
If DCT(6,3) > Av
T4=1 else T4=0;
If(T1+T2+T3+T4 >= 1)
Decode "1"

End;

6. Store W', the recovered watermark;
7. END.

It may be observed from both the algorithm that, even if attacker alters the values of the coefficient of F_M region, if "Av" is not changed much, then we can recover the watermark data correctly and attacker cannot aim to attack the image in such a manner, which modifies the "Av".

4 Results

We tested our scheme on 4 test images Leena, Mandrill, Pepper and Goldhill.

We measured the image quality in terms of Peak Signal to Noise Ratio (PSNR) and Correlation Coefficient (CC).

The PSNR is most commonly used as a measure of quality of reconstruction in image compression etc. It is most easily defined via the mean squared error (**MSE**) which for two $m \times n$ monochrome images I and K where one of the images is considered a noisy approximation of the other is defined as:

$$MSE = \frac{1}{mn} \sum_{I=O}^{M-1} \sum_{J=0}^{N-1} \left\| I(I,J) - k(I,J) \right\|^2$$

PSNR is defined as:

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

Here MAX I is the maximum pixel value of the image.

Fig. 2: Test images of leena, mandrill, pepper and goldhill.
(Courtesy:"
ImageProcessing/VideoCodecs/Programming"
http://www.hlevkin.com)

We are computing CC as:

$$CC = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{\left(\sum_m \sum_n (A_{mn} - \bar{A})^2\right)\left(\sum \sum \left(B_{mn} - \bar{B}\right)^2\right)}}$$

Where $\bar{A}$ = mean 2(A), and $\bar{B}$ = mean2(B).

All results were found using MATLAB and all image manipulation are done using Adobe Photoshop. Fig. 3 shows the watermark logo used in proposed scheme.

Fig. 3. Watermark logo used

4.1 ICAR nature

Our proposed scheme does not require any test to check its robustness against the collusion attack, as it is designed in such a way that, the attacker cannot analyze the pattern by colluding many watermarked copies. We needed to check the performance of the proposed scheme against the JPEG compression and other common image manipulations and known attacks.

4.2 Value of T

Firstly, we had to choose an appropriate value of "T", which affects least the image quality as well as optimizes the recovery of the watermark data. We embedded the watermark logo in test images at various values of T (ranging 50 to 250, at step size 50) and then calculated the PSNR of recovered watermark logos. Our experiments suggested that, at T=150, for the Lena, Mandrill and Pepper test images, there was, approximately, no loss in the perceptual quality of the images and recovered watermark logos were of very fine quality. For the other values of T, either the PSNR of the watermarked image was poor (Higher T) or the quality of the extracted watermark for poor (Lower T). Fig. 5 shows the watermark logos obtained from Lena, Mandrill, Pepper and Goldhill. It was observed that for Goldhill test image, recovery was not good. Therefore we continued to experimented the same process for the Goldhill test image, at various values of T, and we found that at T=100, Goldhill test image was giving the best recovered logo without much loosing its perceptibility. Fig. 6 shows the goldhill test image after the watermark logo was embedded and the recovered logo. Therefore, considering the *"imperceptibility versus Robustness"* trade-off, we fixed up the value of T equals to 150 for the further tests for Lena, Mandrill, and Pepper JPEG test images, and T=100 for the Goldhill test image.

4.3 Color channel selection and performance against JPEG compression

Standard deviation (SD) depicts the spread of the frequency values in a range. If the histogram of a chosen color channel of a particular image has less spread, then that image has less number of frequencies of the chosen color channel. Since, it is the color channel, i.e., the particular color frequencies that shell actually carry the watermark data, we concluded that, SD must have played an important role.

To explore the relationship between the selection of a color channel to carry the watermark data and the efficiency of recovery, we decided to experiment on SD of all 3 color channel. Table 2 shows the standard deviation of all 3 color channels for test images.

First, we hide the watermark data in the BLUE channel of all 4 test images. Then, we compressed watermarked images using JPEG technique at various quality factors, and then recovered the watermark logos.

Fig. 4. Watermarked test images generated by keeping T=150

Fig. 5: Extracted watermark logos from watermarked lena, mandrill, pepper and goldhill test images respectively at T=150.

Fig. 6: Goldhill test image after hiding the watermark logo and the recovered logo at T=100.

Table2. SD values of color channels for test images.

	Leena	Mandrill	Pepper	Goldhill
R channel	49.05	55.5	45.17	56.6
G channel	52.88	47.78	75.05	54
B channel	34.06	61.7	44.29	61

We calculated the PSNR and CC values of extracted logo. Table 3 summarizes the results. It was found that, extracted watermark from Mandrill and Goldhill test images were having poor values of PSNR and CC. Therefore, for these two images, we repeated the above process by using "GREEN' Channel. The qualities of the extracted watermark logos from these two images were improved. Therefore, we have related the performance of our scheme with color channel selection. As, it may be observed from the Table 2, for Leena's and Pepper's test images, BLUE channel have lesser SD, whereas for Mandrill's and Goldhill's images, GREEN channel has lesser SD. So it was concluded that, lesser the SD, better is the recovery of the watermark data. This fixed up the BLUE channel for Leena's and Pepper's watermarking and GREEN channel for rest two images. It is clear from Table 3 and Table 4 that after using GREEN channel for Mandrill's and Goldhill's images, performance was increased. It may be further observed from Table 4 that, our proposed scheme is quite robust against JPEG compression.

4.4 Performance against Image Manipulation

We performed the following attacks on the watermarked test images:
Attack-1: Equalize the Histogram;
Attack-2: Add 10 % Uniform noise;
Attack-3: Adjust the brightness to +40 and contrast to +25;
Attack-4: Adjust the hue and saturation to +10 each;
Attack-5: Flip Horizontal; and
Attack-6: Apply uniform scaling (Zoom).

Our proposed scheme sustained all the attacks and qualities of extracted watermark logos were very fine. Table 5 summarizes the CC of extracted logos, from all test images. Fig. 7 shows the recovered logos from attacked images.

4.5 Comparative Study with similar, state-of-art Schemes

We compared the performance of the proposed scheme, against JPEG compression, with other similar schemes, which are DCT based and well-known for their robustness against JPEG compression.
The schemes chosen were:

A. Scheme-A: Correlation based Technique [9];
B. Scheme-B: The Classical Middle Band coefficient exchange scheme ;

Table 3. PSNR and CC of extracted logo by using BLUE channel for all images

JPEG Quality Factor		Leena	Mandrill	Pepper	Goldhill
Q=60	PSNR	20.89	10.53	24.87	12.53
	CC	84.78	51.8	90.55	54.8
Q=40	PSNR	21.67	9.756	25.41	12.11
	CC	86.25	46.11	91.16	48.54
Q=20	PSNR	19.59	9.27	23.50	9.88
	CC	82.59	41	88.95	45.76

Table 4. PSNR and CC of extracted logo by using BLUE and GREEN channels for images.

JPEG Quality Factor		Leena (BLUE), T=150	Mandrill (GREEN) T=150	Pepper (BLUE) T=150	Goldhill (GREEN) T=100
Q=60	PSNR	20.89	20.81	24.87	22.31
	CC	84.78	85.78	90.55	91.45
Q=40	PSNR	21.67	20.682	25.41	23.32
	CC	86.25	84.98	91.16	92.56
Q=20	PSNR	19.59	20.682	23.50	21.43
	CC	82.59	84.97	88.95	91.45

C. Scheme-C: Scheme presented in [42] and [48], which is Collusion attack resistant watermarking scheme for gray images. This scheme swaps 4 pairs of coefficients in F_M region in correlation with low band coefficients. We are naming this scheme as Scheme-C;and

D. Scheme-D: We are named our proposed scheme as Scheme-D.

We re-implemented the first 3 chosen scheme's ideas for JPEG colored images. In their work "A Novel DCT-based Approach for Secure Color Image Watermarking" [47] author have compared their proposed scheme against JPEG compression with Tsai [49], cox [50] and Fridrich [51] approaches, but they have given the results only up to JPEG Quality factor Q=20.

Therefore, we compared our proposed scheme, for very less JPEG quality factors such as Q=5 and Q=10. Most of the schemes started loosing their efficiency at these quality factors. Fig 8 shows the graph of CC values of recovered logos obtained from JPEG compressed (at Q=10 and Q=5) images, which were watermarked using all chosen schemes. It may be observed from Fig 8 that

Table 5. CC of the extracted logos.

	Leena (BLUE), T=150	Mandrill (GREEN) T=150	Pepper (BLUE) T=150	Goldhill (GREEN) T=100
Histogram Equalization	83.82	82.15	84.04	81.30
Uniform Noise (10%)	57.97	80.64	58.37	79.75
Brightness (+40) & Contrast(+25)	81.05	77.13	80.69	76.25
Hue and saturation adjust (10 each)	86.09	85.62	86.36	85.65
Horizontal Flip	97.01	96.98	96.56	96.36
Uniform scaling	92.31	91.67	92.41	92.27

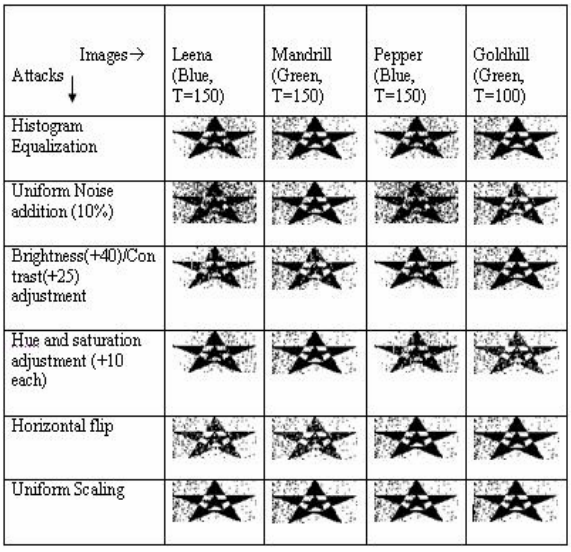

Fig. 7. Extracted logos from attacked watermarked images.

no scheme, other than the proposed one, was able to extract the watermark logo at Q=10 and Q=5.

So, we can conclude that, all other schemes were very robust against JPEG compression attack, but if we compressed the watermark images at very low quality factors (less then Q=20), proposed scheme outperformed the other schemes.

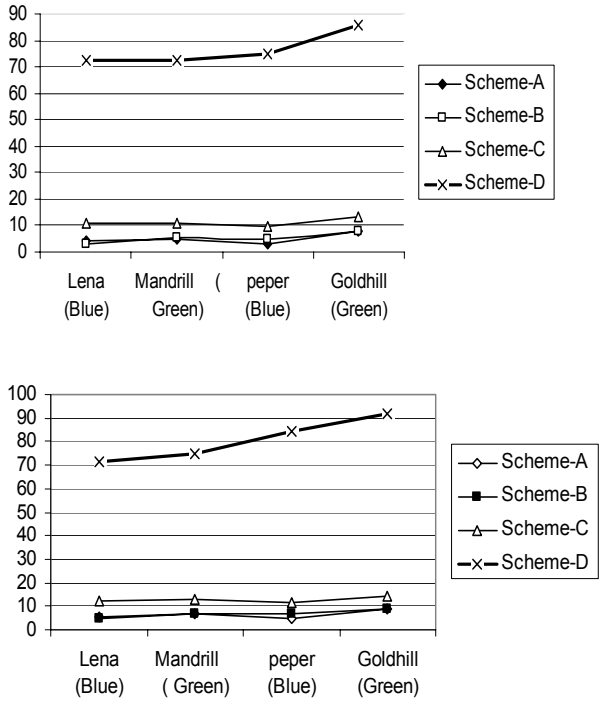

Fig. 8. Comparison of correlation coefficients at Q=10 and Q=5 respectively

Thus, the proposed scheme is not only an ICAR scheme, but also enhances the performance. Results indicated that, the proposed scheme recovers the watermark even from highly attacked images which is compressed up to Q=5 quality factor of JPEG (i.e. after 95-99% size reduction). In addition to this, the proposed scheme is resisting common image manipulations like cropping, scaling, flipping, histogram equalization, brightness- contrast adjustment, Hue-saturation alteration and Gaussian noise.

5 Conclusions

This paper presents a scheme for JPEG image watermarking based on average of DC coefficient and middle-band coefficients of DCT domain. Experimental results prove that proposed scheme is robust against collusion attack as well as outperforms other schemes against JPEG compression. It also sustains the common image manipulations. Further work may be carried out for JPEG2000 format, as this is the upcoming image format and coupling the presented scheme with some special geometrical attack resistant image watermarking schemes.

References:

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

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

[3] 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

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

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

[6] 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.

[7] 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.

[8] Z. Zhao, and E. koch, "Embedding Robust Labels Into Images For Copyright Protection*", Proc. of International Congress on Intellectual Property Rights for Specialised Information, Knowledge and New Technologies*", Vienna, Austria, August 21-25,1995, pp. 242-251.

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

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

[11] G Langelaar et.al. *"Watermarking Digital Image and Video Data: A State-of-art Overview"*,IEEE Signal Processing Magzine, September 2000, pp 20-46

[12] W. Bender, D. Gruhl, and N. Morimoto, "*Techniques for data hiding,"* in *Proc. SPIE, Storage and Retrieval or Image and Video Databases III*, vol.2420, San Jose, CA, Feb. 9-10, 1995, pp. 165-173.

[13] G. Caronni, "*Assuring ownership rights for digital images,"* in *Proc. Reliable IT Systems, VIS '95,* ermany, 1995, pp. 251-263.

[14] J. Fridrich, *"Robust bit extraction from images,"* in Proc. IEEE ICMCS'99 Conf., Florence, Italy, June 7-11, 1999.

[15] A. Hanjalic, G.C. Langelaar, P.M.B. van Roosmalen, J. Biemond, and R.L. Lagendijk, *Image and Video Databases: Restoration, Watermarking and Retrieval* (Advances in Image Communications, vol. 8). New York: Elsevier Science, 2000.

[16] F. Hartung and B. Girod, *"Digital watermarking of raw and compressed video,"* in Proc. SPIE 2952: Digital Compression Technologies and Systems for Video Communication, Oct. 1996, pp. 205-213.

[17] T. Kalker, G. Depovere, J. Haitsma, and M. Maes, *"A video watermarking system for broadcast monitoring,"* in Proc. SPIE Electronic Imaging '99, Security and Watermarking of Multimedia Contents, San Jose, CA, Jan. 1999, pp. 103-112.

[18] G.C. Langelaar, J.C.A. van der Lubbe, and R.L. Lagendijk, *"Robust labeling methods for copy protection of images*," in Proc. SPIE Electronic Imaging '97, Storage and Retrieval for Image and Video Databases V, San Jose, CA, Feb. 1997, pp. 298-309.

[19] I. Pitas and T.H. Kaskalis, *"Applying signatures on digital images,"* in Proc. IEEE Workshop on Nonlinear Signal and Image Processing, Neos Marmaras, Thessaloniki, Greece, June 20-22, 1995, pp. 460-463.

[20] I. Pitas, *"A method for signature casting on digital images,"* in Proc. ICIP-96, IEEE Int. Conf. Image Processing, vol. III, Lausanne, Switzerland, Sept. 15-17, 1996, pp. 215-218.

[21] R.G. van Schyndel, A.Z. Tirkel, and C.F. Osborne, *"A digital watermark,"* in Proc. IEEE Int. Conf. Image Processing, vol. 2, Austin, TX, Nov. 1994, pp. 86-90.

[22] J.R. Smith and B.O. Comiskey, *"Modulation and information hiding in images,"* in Preproc. Information Hiding, University of Cambridge, U.K., May 1996.

[23] R.B. Wolfgang and E.J. Delp, *"A watermark for digital images*," in Proc.IEEE Int. Conf. Image Processing, vol. III, Sept. 16-19, 1996, Lausanne, Switzerland, pp. 219-222.

[24] R.B. Wolfgang and E.J. Delp, *"A watermarking technique for digital imagery: Further studies,"* in Proc. Int. Conf. Imaging Science, Systems, and Technology, Las Vegas, NV, June 30-July 3, 1997.

[25] R.B. Wolfgang and E.J. Delp, *"Overview of image security techniques with applications in multimedia systems,"* in Proc. SPIE Conf. Multimedia Networks: Security, Displays, Terminals, and Gateways, vol. 3228, Dallas, TX, Nov. 2-5, 1997, pp. 297-308.

[26] R.B. Wolfgang and E.J. Delp, *"Fragile watermarking using the VW2D watermark"* in Proc. Electronic Imaging *'99*, vol. 3657, San Jose, CA, Jan. 25-27, 1999, pp. 204-213.

[27] W. Zeng and B. Liu, *"On resolving rightful ownerships of digital images by invisible watermarks,"* in *Proc*. ICIP 97, IEEE Int. Conf. Image Processing, Santa Barbara, CA, Oct. 1997, pp. 552-555.

[28] F.M. Boland, J.J.K. Ó Ruanaidh, and C. Dautzenberg, *"Watermarking digital images for copyright protection,"* in Proc. IEE Int. Conf. on Image Processing and Its Applications, Edinburgh, U.K., July 1995, pp. 326-330.

[29] I.J. Cox, J. Kilian, T. Leighton, and T. Shamoon, *"Secure spread spectrum watermarking for multimedia*," NEC Res. Insti., Princeton, NJ, Tech. Rep. 95-10, 1995.

[30] I.J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "*A secure, robust watermark for multimedia,"* in Preproc. Information Hiding, Univ. of Cambridge, U.K., May 1996.

[31] I.J. Cox, J. Kilian, T. Leighton, and T. Shamoon, *"Secure spread spectrum watermarking for images, audio and video,"* in Proc. 1996 Int. Conf. Image Processing, vol. 3, Lausanne, Switzerland, Sept. 16-19, 1996, pp. 243-246.

[32] C.-T. Hsu and J.-L. Wu, *"Hidden signatures in images,"* in Proc. ICIP-96, IEEE Int. Conf. Image Processing, vol. III, Lausanne, Switzerland, Sept. 16-19, 1996, pp. 223-226.

[33] A. Piva, M. Barni, F. Bartolini, and V. Cappellini, "*DCT-based watermark recovering without resorting to the uncorrupted original image,"* in Proc. ICIP 97, IEEE Int. Conf. Image Processing,, Santa Barbara, CA, Oct. 1997, pp. 520-527.

[34] C. Podilchuk and W. Zeng, *"Perceptual watermarking of still images,"* in Proc. 1997 IEEE 1st Workshop Multimedia Signal Processing, Princeton, NJ, June 23-25, 1997, pp. 363-368.

[35] J.J.K. Ó Ruanaidh, W.J. Dowling, and F.M. Boland, *"Watermarking digital images for copyright protection,"* Proc. Inst. Elec. Eng. Vision, Image, and Signal Processing, vol. 143, no. 4, pp. 250-256, Aug. 1996.

[36] S. Rupley, *"What's holding up DVD?"* PC Mag., vol. 15, no. 20, pp. 34, Nov. 19, 1996.

[37] R.B. Wolfgang, C.I. Podilchuk, and E.J. Delp, *"Perceptual watermarks for digital images*

and video," Proc. IEEE, vol. 87, pp. 1108-1126, July 1999.

[38] M. Barni, F. Bartolini, V. Cappellini, A. Lippi, and A. Piva, "*A DWT-based technique for spatio-frequency masking of digital signatures,"* in Proc. SPIE/IS&T Int. Conf. Security and Watermarking of Multimedia Contents, vol. 3657, San Jose, CA, Jan. 25-27, 1999, pp. 31-39.

[39] F.M. Boland, J.J.K. Ó Ruanaidh, and C. Dautzenberg *"Watermarking digital images for copyright protection,"* in Proc. IEE Int. Conf. on Image Processing and Its Applications, Edinburgh, U.K., July 1995, pp. 326-330.

[40] D. Kundur and D. Hatzinakos, *"A robust digital image watermarking scheme using wavelet-based fusion,*" in Proc. ICIP 97, IEEE Int. Conf. Image Processing, Santa Barbara, CA, Oct. 1997, pp. 544-547.

[41] X.-G. Xia, C.G. Boncelet, and G.R. Arce, *"A multiresolution watermark for digital images,"* in Proc. ICIP 97, IEEE Int. Conf. Image Processing, Santa Barbara, CA, Oct. 1997, pp. 548-551.

[42] Vikas Saxena, J.P. Gupta, *"A Novel Collusion Attack Resistant Watermarking Scheme for Color Images"*, IAENG International Journal of Computer Science, Volume 34 Issue 2, Pages 171-177, December 2007, ISSN: 1819-656X.

[43] Network Technology research Center, Nanyang Technological University, Singapore, http://www.ntu.edu.sg/ntrc/research.htm

[44] W. Kim, S.H. Lee, H.-W. Jang, and J. Kim, *"Multi-bits Fingerprinting for Image"* http://www.actapress.com/PaperInfo.aspx?PaperID=15683

[45] Collusion-resistant watermarking and fingerprinting,
US Patent Issued on June 13, 2006.
http://www.patentstorm.us/patents/7062653.html

[46] F. Bossen M. Kutter, F. Jordan, *"Digital signature of color images using amplihlde modulation,"* in Proc. of SPlE storage and retrieval for image and video databases, San lose, USA, vol. 3022-5, February 1997, pp. 518-526.

[47] N Ahmidi ,R. Safa. , *"A Novel DCT-based Approach for Secure Color Image Watermarking" ,* Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04), IEEE 2004.

[48] Vikas Saxena, J.P. Gupta, "Collusion Attack Resistant Watermarking Scheme for Images Using DCT", Proceedings of IEEE 15th Signal Processing and Communication Applications Conference, 11-13 June 2007, Turkey.

[49] C-S Tsai, C-C Chang, T-S Chen, and M -H Chen, *"Distributed multimedia databases: Techniques and Applications*", National Chung Chang University, and National Taichung Institute of Technology, Taiwan, 2001

[50] I.J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "*Secure spread spectrum watermarking for multimedia*," IEEE Trans. On Image Processing, Vol. 6, No. 12, 1997, pp. 1673-1687.

[51] J. Fridrich, *"Combing low-frequency and spread spectrum watermarking,"* SPIE Symposium on Optical Science Engineering and Instrumentation, San Diego, USA, July 1998.

[52] E. Koch and J. Zhao, *"Towards robust and hidden image copyright labeling,"* IEEE International Workshop on Non- Linear Signal and Image Processing, Neos Marmaras, Greece, June 1995, pp. 452-455.