Forgery Resistant Scrambled Image Watermarking

Priyanka Sharma, Shiv Kumar

Abstract*— Collusion is a mechanism where some secret information shared between many peers is forged to use for illegal purpose. The watermark embedded in an image is the secret information which can be used to claim the originality by its owner. The images delivered to different peers have different watermarks embedded into them. All those malicious attackers can compare the watermarked images to determine the common places where the watermark has been embedded; hence the watermark can be attacked through collusion. So a new technique for watermarking which is collusion resistant has been proposed here. This scheme uses averaged coefficients based discrete cosine transform to embed the watermark at different areas in different images. The main advantage of the scheme is that the image is scrambled before embedding of the watermark and descrambled after embedding. This leads to spreading of the watermarking information throughout the watermarked image and it is very difficult to detect it. The correlation results show that the watermark is very robust.

***Index Terms*— 4 to 8 bit encoding, DCT, Mid Band coefficient, Scrambling, Watermarking..**

I. INTRODUCTION

The watermark is a signal that contains useful certifiable information for the owner of the host media, such as company logo, producer's name, etc., which is embedded into the host media to be protected, such as digital audio, image and video, etc. A "watermark" is a pattern of bits inserted into a digital good that may be used to identify the content owners and/or the protected rights. Watermarks are designed to be completely invisible or, more precisely, to be imperceptible to humans and statistical analysis tools.

Many watermarking methods for images have been proposed. Paper [1] introduces a watermarking scheme, a method to protect the ownership of digital holograms using the DCT domain data as the ones to be watermarked. Robust digital image watermarking based on sub sampling paper [2] presents a robust digital watermarking scheme for copyright protection of digital images. Four sub images are obtained from the host image by using sub sampling. A novel support vector regression based color image watermarking scheme [3] outperform the Kutter_s method and Yu_s method against different attacks including noise addition, shearing, luminance and contrast enhancement, distortion, etc. Especially when the watermarked image is enhanced in luminance and contrast at rate 70%, our method can extract the watermark with few bit errors. A DCT-domain system for robust image watermarking [4] demonstrate that the watermark is robust to several signal processing techniques, including JPEG compression, low pass and median filtering, histogram equalization and stretching, dithering, Gaussian noise, resizing and multiple watermarking. Reddy and Prasad [5] begin by modifying the frequency coefficients of the image based on the Human Visual systems perception of image content, which is used to embed a watermark such that its amplitude is kept below the distortion sensitivity of the pixel and thus preserving the image quality. Hernandez [6] apply generalized Gaussian distributions to statistically model the DCT coefficients of the original image and show how the resulting detector structures lead to considerable improvements in performance with respect to the correlation receiver. A blind, low complex, fast, and highly resistant to attacks watermarking algorithm is proposed [7] for JPEG compressed images. In An improved DCT-based image watermarking technique watermark [8] is embedded into a digital image, based on the concept of mathematical remainder, by modifying the low-frequency coefficients in DCT frequency domain. The DWT separates an image to a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. One of the many advantages of the DWT is being able to model more accurately aspects [9] of the Human Visual System (HVS) as compared to the Fast Fourier Transform (FFT) or DCT.

The following paper is divided into Sections. Section 2 describes Digital Watermarking technology. Section 3 describes the Proposed Watermarking scheme. Section 4 describes the Result of proposed scheme and in Section 5 conclusion is described.

II. DIGITAL WATERMARKING SCHEME

The first step in the designing of a watermarking system is the definition of the embedding procedure. Watermarked image is a combination of cover image and watermark. The MBEC watermarking algorithm encodes one-bit of the binary watermark image into one 8x8 DCT sub-block of the host image. MBEC algorithm ensures that the difference of two mid-band coefficients is positive in case of the encoded value is 1. Otherwise, the two mid-band coefficients are exchanged. Classical middle-band based algorithm is quite robust against JPEG compression and common image manipulation operations.

Image watermarking with both insensible detection and high robustness capabilities is still a challenging problem for copyright protection up to now. Vikas Saxena [10] presents a new scheme for hiding a logo-based watermark in colored still image which is inherently collusion attack resistant. This scheme is based on averaging of middle frequency coefficients of block Discrete Cosine Transform (DCT) coefficients of an image.

Manuscript published on 30 October 2012.
* Correspondence Author (s)
Priyanka Sharma*, M Tech (Computer Science) Pursuing , Arya College of engg & IT, Rajasthan Technical University, Kota, India.
Prof Shiv Kumar, Computer Science, Arya College of engg & IT, Rajasthan Technical University, Kota, India.

It is different from earlier schemes based on middle frequency coefficient by mean of high redundancy, to sustain malicious attacks. Experimental results show the robustness of the proposed scheme against the JPEG compression and other common image manipulations .

III. PROPOSED WATERMARK SCHEME

A new technique for watermarking which is collusion resistant has been proposed here. This scheme uses averaged coefficients based discrete cosine transform to embed the watermark at different areas in different images. The main advantage of the scheme is that the image is scrambled before embedding of the watermark and descrambled after embedding. This leads to spreading of the watermarking information throughout the watermarked image and it is very difficult to detect it. The correlation results show that the watermark is very robust.

A. Embedding of Watermark in averaged Block based DCT coefficients

Watermarks are designed to be completely invisible or, more precisely, to be imperceptible to humans and statistical analysis tools. Embedding of watermark is used to embed original image with a watermark image. In this process an image of 256x256 pixels, 512x512 pixels, 1024x1024 pixels, 2048x2048 pixels or any size is used as an input. Original image is scrambled using pseudo random number sequence. Fig 1 explains each step to embed watermark with cover image.

The main aim of image scrambling is to transform a meaningful image into a meaningless or disordered image in order to enhance the power to resist invalid attack and in turn enhance the security. The mainly used three kind of image scrambling types are scrambling in the space domain, scrambling in the frequency domain, and scrambling in the color or grey domain.

A binary random sequence is generated using equation 1. This PN sequence guides the permutation of the image. The size of this PN sequence is equal to the cover object. The no. of 1s in the PN sequence can be controlled for the sake of the analysis of the result and analyzing the effect of permutation.

$$PN = \{p||p\varepsilon\ (0, 1)\} \qquad (1)$$

For every bit value 1 in the PN sequence, the corresponding index in the image is exchanged with its diagonal counterpart using equation 2. Otherwise the image pixel is kept same.

$$I(i,j)=p*I(j,i)+p' * I\ (i, j) \qquad (2)$$

Here p ε PN and p′ is its complement. I is the cover image. So after one scan of the PN sequence the image is now permuted. To unpermute the image we apply the same strategy.

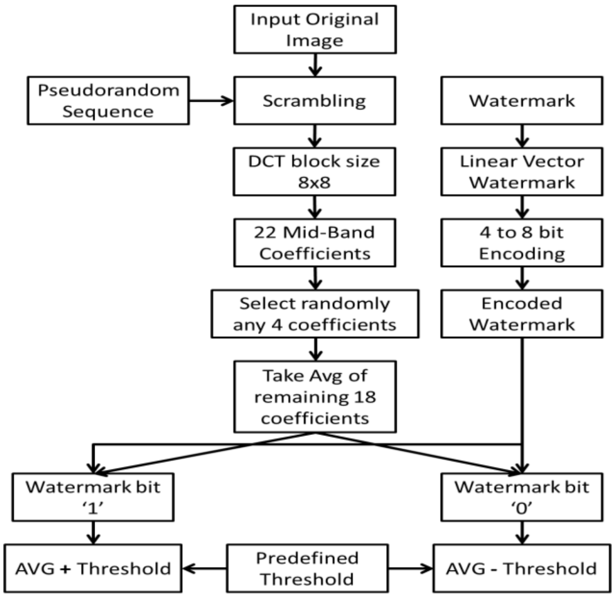


Fig 1 Flow Chart

The watermark can be inserted in the permuted image using DCT based technique explained before. After adding the watermark information the image is again repermuted using the same pseudo random sequence and the same logic for intensities exchange. This gives the watermarked image which has hidden information in it. The complete schema is shown in Fig 2. This part of the algorithm uses the same pseudo random sequence as it was used in the embedding procedure to again permute the watermarked image [11].

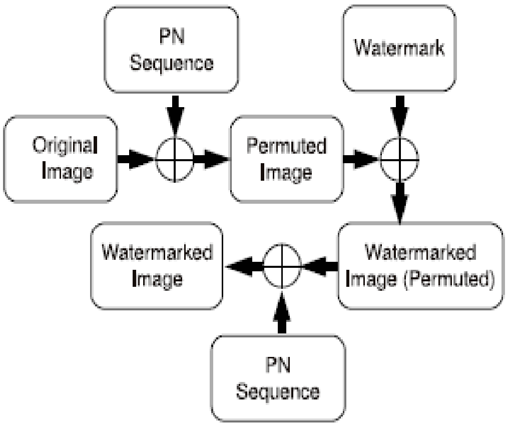


Fig 2: Embedding using PN Sequence

Now, scrambled image is divided into 8x8 blocks. For Example, if image size is 256x256 pixels, when dividing input image into 8x8 blocks, total number of block will be equal to 32x32=1024. In the next step of this technique one block is selected out of 1024 blocks at a time. This step is repeated 1024 times. In each step process calculate discrete cosine transform for each block.

The discrete cosine transform (DCT) represents an image as a sum of sinusoids of varying magnitudes and frequencies. The dct2 function computes the two-dimensional discrete cosine transform (DCT) of an image. The DCT has the property that, for a typical image, most of the visually significant information about the image is concentrated in just a few coefficients of the DCT. For this reason, the DCT is often used in image compression applications.

The two-dimensional DCT of an M-by-N matrix A is defined as follows.

$$B_{pq} = \alpha_p \alpha_q \quad (3)$$

$$\sum_{m=0}^{M-1}\sum_{n=0}^{N-1} A_{mn} \cos\frac{\pi(2m+1)p}{2M}\cos\frac{\pi(2n+1)q}{2N},\ \begin{matrix}0 \le p \le M-1\\ 0 \le q \le N-1\end{matrix} \quad (4)$$

Where

$$\alpha_q = \begin{cases} 1/\sqrt{M}, & p = 0 \\ \sqrt{2/M}, & 1 \le p \le M-1 \end{cases} \quad (5)$$

$$\alpha_q = \begin{cases} 1/\sqrt{N}, & q = 0 \\ \sqrt{2/N}, & 1 \le q \le N-1 \end{cases} \quad (6)$$

The values B_{pq} are called the DCT coefficients of A. (Note that matrix indices in MATLAB always start at 1 rather than 0; therefore, the MATLAB matrix elements A(1,1) and B (1,1) correspond to the mathematical quantities A_{00} and B_{00}, respectively.) The DCT is an invertible transform, and its inverse is given by

$$A_{mn} = \sum_{p=0}^{M-1}\sum_{q=0}^{N-1} \alpha_p \alpha_q B_{pq} \cos\frac{\pi(2m+1)p}{2M}\cos\frac{\pi(2n+1)q}{2N},\ \begin{matrix}0 \le m \le M-1\\ 0 \le n \le N-1\end{matrix} \quad (7)$$

Where

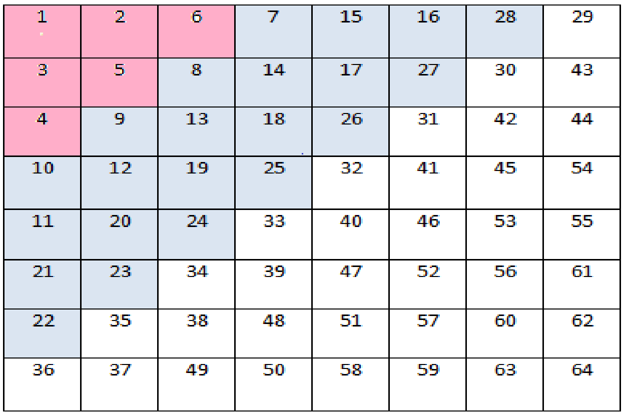
$$\alpha_p = \begin{cases} 1/\sqrt{M}, & p = 0 \\ \sqrt{2/M}, & 1 \le p \le M-1 \end{cases} \quad (8)$$

$$\alpha_q = \begin{cases} 1/\sqrt{N}, & q = 0 \\ \sqrt{2/N}, & 1 \le q \le N-1 \end{cases} \quad (9)$$

The inverse DCT equation can be interpreted as meaning that any M-by-N matrix A can be written as a sum of *MN* functions of the form

$$\alpha_p \alpha_q \cos\frac{\pi(2m+1)p}{2M}\cos\frac{\pi(2n+1)q}{2N},\ \begin{matrix}0 \le p \le M-1\\ 0 \le q \le N-1\end{matrix} \quad (10)$$

These functions are called the basic functions of the DCT. The DCT coefficients B_{pq}, then, can be regarded as the weights applied to each basis function. For 8-by-8 matrices, the 64 basis functions are illustrated by this image.



1	2	6	7	15	16	28	29
3	5	8	14	17	27	30	43
4	9	13	18	26	31	42	44
10	12	19	25	32	41	45	54
11	20	24	33	40	46	53	55
21	23	34	39	47	52	56	61
22	35	38	48	51	57	60	62
36	37	49	50	58	59	63	64

Fig 3: DCT

The discrete cosine transform (DCT) helps separate the image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality). Discrete cosine transform provides 64 DCT coefficients which are subdivided in three groups [12]:

- Low frequency DCT coefficients
- Mid band DCT coefficients
- High frequency DCT coefficients

For most images, much of the signal energy lies at low frequencies; these appear in the upper left corner of the DCT. Fig 3 shows position of low frequency (1-6), mid band (7-28), high frequency DCT coefficient (29-64).

This algorithm chooses shaded part for watermarking that is referred as mid band frequency. This shaded part contains 22-coefficients, from these 22-coefficients randomly select 4 coefficients, and take average of remaining 18 coefficients.

Watermark image size would be decided according to original image size. If number of blocks are 1024, then watermark image size should be equals to 32x32 pixels. If watermark size is less than specified pixels, add padded bit or increase image to increase pixels. In the other case if watermark size is greater than specified size, image is compressed to get 32x32 pixels. This watermark image has a format like jpeg, gif, bmp etc. Watermark image is converted into Linear Vector in which watermark bit will be specified in binary (0, 1) format. Linear vector is an array of 1024 bit either 1 or 0.

In the proposed algorithm I used 4 to 8 bit encoding to make a watermarked image more secured. 4 to 8 bit encoding/decoding is explained by the following steps:

1. Generate 16 unique random 8-bit sequences, each for value between 0-15.
2. Take 4 consecutive bits (in order) of the watermark sequence and replace it with the corresponding unique 8-bit random sequence.
3. Repeat above steps for whole watermark in sets of 4-bits.
4. Return.

This encoding scheme is called to prepare the watermark. The input to this module is a linear vector of the watermark bits. After 4 to 8 bit encoding size of the watermark is doubled. The reason why we incorporated 4 to 8 bit encoding is to increase the robustness of the watermarking procedure. The watermark is not embedded in its original form it is embedded in its encoded form, so even someone who is able to extract the watermark he is not able to decode the watermark until he knows the decoding table. This table is also generated randomly for different images. So the robustness of the watermarking in increased by one level.

Before embedding we assume Threshold in the range of 10 to 20. If watermark bit is 1, add average of 18 coefficients with threshold value. In the other case if watermark bit is 0, subtract averaged coefficient from threshold value. Output value of this step is replaced with the selected 4 coefficient. This step is continued till all watermarked bit are compared. After that select another block and repeat all steps again and again until all blocks embed with watermark bit. To check

A. Algorithm for Forgery Resistant Scrambled Image Watermarking

Embedding algorithm steps are:
Input: Cover image, Watermark
Output: Embedded Watermark image
Process:

1. Clearing all variables, Clear Output and closing Figs.
2. Input Original Image and Watermark must be an rgb image.
3. Convert both images into grayscale by eliminating the hue and saturation information while retaining the luminance. In the RGB colour model, a colour image can be represented by the intensity function.

$$I_{RGB} = (F_R, F_G, F_B) \quad (11)$$

Where $F_R(x, y)$ is the intensity of the pixel (x,y) in the red channel, $F_G(x,y)$ is the intensity of pixel (x,y) in the green channel, and $F_B(x,y)$ is the intensity of pixel (x,y) in the blue channel.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

If only the brightness information is needed, color images can be transformed to gray scale images.The transformation can be made by using proposed equation.

$$I_y=0.2989F_R+0.5870F_G+0.1140F_B \qquad (12)$$

Where F_R, F_G and F_B are the intensity of R, G and B component respectively and Iy is the intensity of equivalent gray level image of RGB image.

4. Scramble Gray Scale Cover image using PN Sequence
5. Reshaping the watermark to a linear vector watermark
6. Check that the message for cover.
   a) If watermark message is greater than cover image, therefore a message will be displayed.
   b) If watermark message in less than cover image, then it is padded with ones so the small watermark image scale up to the max message length for cover image.
   c) If watermark message is equals to cover image, do nothing.
7. Use 4 to 8 bit encoding scheme to watermark and reshape the encoded watermark to 2D image to produce encoded watermark.
8. Processing the image in blocks and calling DCT watermark embedding algorithm

8.1 Choose middle band coefficient for the further process that have 22 coefficients. Randomly select 4 coefficients form 1st block.

8.2 Calculate DCT for each block of size 8X8.

8.3 Calculate the average (AVG) of remaining 18 middle band coefficients.

8.4 From 1st block of image compare each value with the watermark bit.

8.4.1 If Watermark bit is ‘1’: For all 4 chosen coefficients in step 8.1, assign the value of coefficients which is (Threshold + AVG).

8.4.2 If Watermark bit is ‘0’: For all 4 chosen coefficients in step 8.1, assign the value of coefficients which is (Threshold-AVG).

8.5 Take IDCT to reconstruct the watermarked image W.

9. Repermute the watermarked image W using the same PN sequence.

B. Extraction of Watermark from averaged Block based DCT coefficients

Watermark extraction is reverse procedure of watermark embedding. To extract the watermark from the watermarked image, we calculate average “AVG” in same way as in embedding algorithm. Owner should have a record of all policies used to watermark the image. 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 AVG - Threshold, Interpret “0”and;
2) If at least 1 out of 4 chosen coefficients are AVG + Threshold, interpret “1”.

IV. EXPERIMENTAL RESULT

In order to test the new watermarked algorithm, fig 4 is given as input for Cover image.

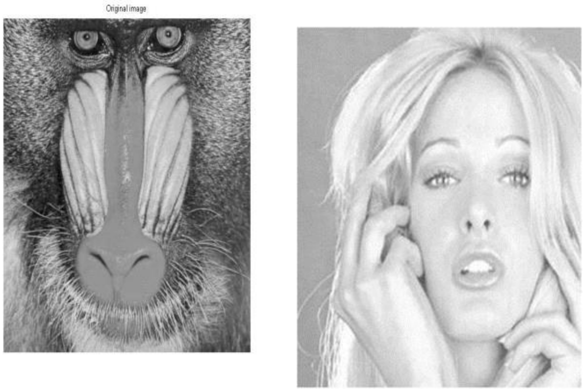


Fig 4 Cover Image

Fig 5 describes to a permuted image, leads to spreading of the watermarking information throughout the watermarked image. In this process cover image size is scaled to 1024 X 1024

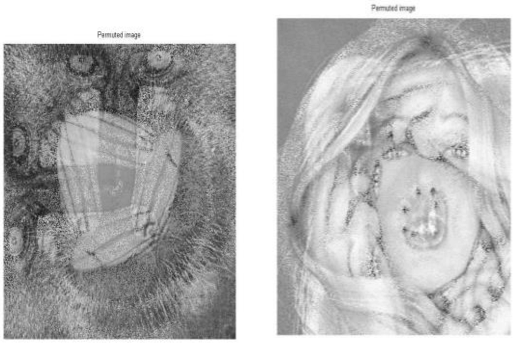


Fig 5 Permuted image

Fig 6 describes watermarked image after repermutation.

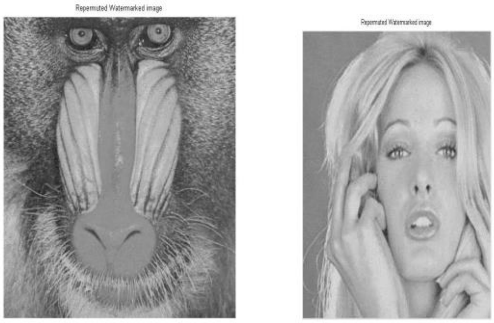


Fig 6 Watermarked Image

The blind watermark detection can be used as an attack to illegally detect the watermark. Here it is assumed that the attacker knows the watermark and the block size to divide the image into blocks. The attacker is able to divide the image into blocks and he would either apply linear correlation or the normal correlation between the watermarked block and the watermark. Since the block does not contain the original watermark but only the encoded watermark thus the correlation fails. The Figure 7 shows the plot for the correlation between the original and the watermarked image. A peak in the center of the surface means that both of the images are same and first is contained in the second. Some small peaks are due to embedded watermark.

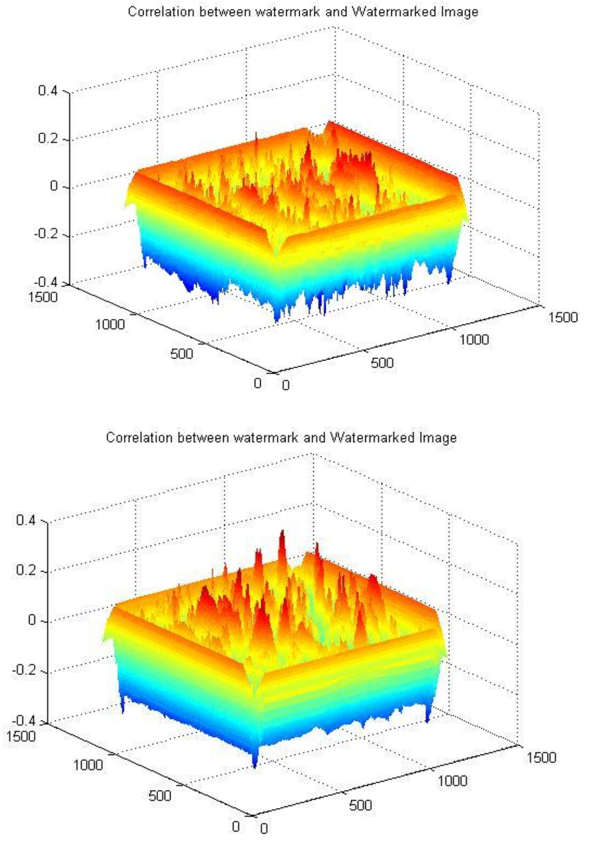


Fig 7 Correlation between watermark and Watermarked image

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 into a peak if the watermark presence in the watermarked image is detected. The Figure 8 clearly shows the correlation result which appears as randomly distributed noise so blind detection is failed.

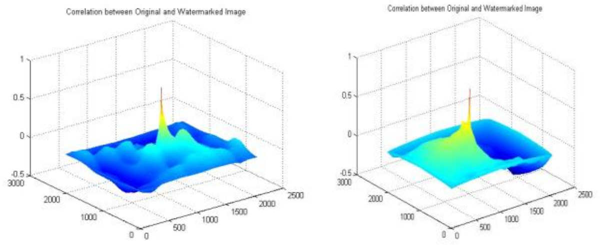


Fig 8 Correlation between Original and watermarked image

4.1 Result analysis for PSNR and SM:

A. PSNR:

Peak Signal to noise ratio (PSNR) is used to check quality of watermarked image. PSNR is used for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. We have used three 1024 x 1024 cover image Baboons, girl, Nature_beauty to check performance of proposed watermarking algorithm. Given a watermarked image f and a cover image g, both of size M×N, the PSNR between f and g is defined by:

$$PSNR\ (f\ ,g) = 10\ \log_{10}(255^2/MSE(f\ ,\ g)) \qquad (13)$$

Where

$$MSE(f,g) = \frac{1}{M*N}\sum_{i=1}^{m}\sum_{j=1}^{n}\ (f_{ij} - g_{ij})^2 \qquad (14)$$

The PSNR value approaches infinity as the MSE approaches zero; this shows that a higher PSNR value provides a higher image quality. At the other end of the scale, a small value of the PSNR implies high numerical differences between images. Table 1 displays peak signal to noise ratio between watermarked image and original cover image.

Image Name	**PSNR Value(watermarked image, Cover image)**
Baboons	+32.35 dB
girl	+36.35 dB
Nature_beauty	+31.22 dB

Table1 PSNR between watermarked image and cover image

B. Similarity Factor:

This term is used to check difference of bit between two images. The similarity factor has value [0, 1] calculated using equation 15. If *SM* = 1 then the embedded watermark and the extracted watermark are same. Generally value of *SM* > .75 is accepted as reasonable watermark extraction.

$$SM = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}\ w(i,j)*w'(i,j)}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}\ w(i,j)^2*\sum_{i=1}^{m}\sum_{j=1}^{n}\ w'(i,j)^2}} \qquad (15)$$

The expression has *w* and *w*' as the original and the detected watermark from watermarked image.In order to check similarity between extracted watermark form Baboons, girl, Nature_beauty watermarked image and original watermark is 1, 0.9891 and 1 simultaneously in the proposed scheme.

V. CONCLUSION AND FUTURE SCOPE

In the proposed strategy, the watermark embedding is done using DCT frequency transform in different blocks of the image. The watermark is encoded through 4 to 8 bit encoding before watermarking. This strategy is completely new and effective for coding decoding process. The transformations are applied depending upon the high and low frequency regions of the image after performing statistical analysis. The strategy is effective against most image processing attacks. Experimental results demonstrate that the watermarks are difficult to detect blindly because of the noise like appearance of the encoded watermark. The tables and figures in the performance analysis demonstrate the maximum possible extraction through any of the methods.

The watermark is also secure against collusion attacks justified with the reasons. The high watermark detection ratio (SM) values prove that the watermark is extractable even after the application of variety of attacks. Watermarks embedded in at least one of the selected coefficients can be successfully restored. The main disadvantages of this scheme are high processing time since all the methods are block based and increased size of encoded watermark. 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.

REFERENCES

[1] Hyun-Jun Choi; Young-Ho Seo; Ji-Sang Yoo;Dong-Wook Kim" Digital watermarking technique for holography interference patterns in a transform domain" Kwangwoon University, 447-1,Hansung University,Pages136-792, Republic of Korea,2007.

[2] W. Lu et al " Robust digital image watermarking based on subsampling" Applied Mathematics and Computation 181, 886–893, 2006.

[3] Rui-min Shen, Yong-gang Fu " A novel image watermarking scheme based on support vector regression" The Journal of Systems and Software 78, 1-8, 2005.

[4] *M. Barni et al.* "A DCT-domain system for robust image watermarking"*Signal Processing 66, 357-372, 1998.*

[5] P.RAMANA REDDY, DR. Munaga. V.N.K.PRASAD "Robust Digital Watermarking of Images using Wavelets" International Journal of Computer and Electrical Engineering, Vol. 1, No. 2, 1793-8163, June 2009

[6] Hernandez, J.R. ;Amado, M. ; Perez-Gonzalez, F. "DCT-domain watermarking techniques for still images: detector performance analysis and a new structure" Image Processing, IEEE Transactions on,*Vol* 9 , Issue: 1 , 55 - 68 , Jan 2000

[7] Gangyi Jiang; Mei Yu ; Shoudong Shi ; Xiao Liu ; Yong-Deak Kim "New blind image watermarking in DCT domain ", IEEE *Xplore,*1580 - 1583 vol.2 , 26-30 Aug. 2002

[8] S.D. Lin et al." Improving the robustness of DCT-based image watermarking against JPEG compression/ Computer Standards & Interfaces" 32, 54–60,2010.

[9] J. Ryan, "Method and Apparatus for Preventing the Copying of a Video Program," *United States Patent,* 4,907-930, 1990.

[10] Vikas Saxena, J.P Gupta" Collusion Attack Resistant Watermarking Scheme for Colored Images using DCT" IAENG International Journal of Computer Science, 34:2, IJCS_34_2_02,November,2007.

[11] Gunjan, Reena, Maheshwari, Saurabh, Gaur, M., Laxmi, Vijay, "Permuted Image DCT Watermarking", Computational Intelligence in Security for Information Systems, Springer, vol. 85, pp. 163-171.

[12] Saurabh Maheshwari, Reena Gunjan, Vijay Laxmi, and M.S. Gaur, "Robust Multi-modal Watermarking using Visually Encrypted Watermark", The 19th International Conference on Systems, Signals and Image Processing, IWSSIP 2012, IEEE, vol. pp. 72-75.