A NOVEL APPROACH FOR IMAGE WATERMARKING USING DCT AND JND TECHNIQUES

Mrs. R.J. Shelke,
Dept of Electronics Engineering,
Walchand Institute of Technology,
Solapur 413002, India

Dr. Mrs. S.S. Apte,
Dept of Computer Science & Engineering,
Walchand Institute of Technology,
Solapur 413002, India

ABSTRACT

Today's world is digital world. Nowadays, in every field there is enormous use of digital contents. Information handled on internet and multimedia network system is in digital form. The copying of digital content without quality loss is not so difficult. Due to this, there are more chances of copying of such digital information. So, there is great need of prohibiting such illegal copyright of digital media. Digital watermarking is the powerful solution to address this problem. Digital watermarking is the technology in which there is embedding of various types of information in digital content which we have to protect from illegal copying. This embedded information to protect the data is embedded as watermark. This paper introduces two novel techniques for image watermarking such as DCT and JND. The DCT based approach adapted to embed watermarks in DC, low, mid and high frequency components coefficient of DCT. The JND based approach gives robust and transparent scheme of watermarking that exploits the 'human visual systems' sensitivity to local image characteristics obtained from the spatial domain, improving upon the content based image watermarking scheme. In JND method, we consider texture, luminance, corner and the edge information in the image to generate a JND (Just Noticeable Distortion) mask that makes the addition of the watermark less perceptible to the human eye. The process of embedding and extraction of the watermark is done in the frequency domain for providing robustness. The image test data base includes (grey scale) host and watermark images of size 256*256 and the performance evaluation metrics used are PSNR (Peak Signal to Noise Ratio) and correlation.

KEYWORDS: Image Watermarking, DCT (Discrete Cosine Transform), DC Coefficients, JND mask *(*Just Noticeable Distortion*),* PSNR (Peak Signal to Noise Ratio), Correlation, JPEG, Filter, Noise.

INTRODUCTION

Digital watermarking is the process of embedding data into digital multimedia content and later can be extracted for a variety of purposes including copy prevention and control. At present, the main research directions of the information hiding include digital watermarking and hiding communication. Most watermark embedding processes are performed in either spatial domain or transform domain [6], [7], [8], [9]. The methods in transform domain, especially in DCT domain, are more popular for the following reasons:

1. The features of human vision system (HVS) can be incorporated into watermarking in the transform domain more effectively.
2. The energy of embedded signal in the transform domain will be spread over all pixels in the spatial domain.
3. They can be implemented in compressed domain since the international image and video compression standards, such as JPEG, MPEG, and H.261/263 are based DCT coding.

The DCT domain method is most widely used for its relatively low computational complexity, moreover, it is compatible with the international data compression standards, including JPEG, MPEG and H.261/263, so watermark can be easy embedded in the compression processing. The combination of two dominant image watermarking techniques gives affect robustness and perceptual quality. Robustness and perceptual quality are two of most basic requirements for image watermarking in most applications.

IMAGE WATERMARKING TECHNIQUES

The following section gives a brief idea about the two significant image watermarking techniques such as DCT and JND mask.

2.1 Image Watermarking using DCT

Most of the image watermarking algorithm in DCT domain uses 8*8 block approach. The 64 value DCT coefficient of an image block comprises of DC, low, mid and high frequency components as shown in figure 1 below. In nature image, the energy of each block is concentrated on the low frequency after DCT. It is known that embedding watermark in low frequency makes the watermark perceptible. On the other hand, to survive lossy compression, watermark information should not be inserted into the higher frequency.

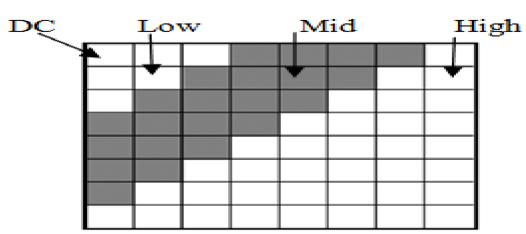


Fig: 2.1(a): Definition of DCT Regions

Cox at al suggests that a watermark should be placed in perceptually significant regions of an image if it is to be robust [1]. Traditional techniques select the mid-range frequency to embed the watermark. Kung et al embeds a watermark in the middle frequency coefficients using JPEG table [3]. Lie et al uses a multiple watermarking algorithm in middle frequency band [4]. Taskovski et al [10] and Yang et al [11] have even tried to embed watermark in low frequency coefficients. However, the DC coefficients are explicitly excluded from watermarking. The consideration behind this is to avoid block artifacts in watermarked images. Although most of the researchers focus on mid and low frequency coefficients, few researchers have claimed advantages of embedding a watermark in DC coefficient [12] [13] [14] [15]. The purpose of this technique is to present a approach which is used to embed image watermark in DC coefficients than the most popular mid or high frequency coefficients of DCT domain. The common framework employed for that includes dividing host image into non overlapping blocks, finding DCT, embedding watermark in DC coefficient *(u=0, v=0)* of DCT domain and getting watermarked spatial image after IDCT. The watermarked image is then tested against different attacks to evaluate performance metrics.

2.1.1 Analysis of DCT Coefficients

Jiwu Huang et al [9] [10] has done a quantitative analysis on magnitude of DCT coefficients. According to this, firstly, the magnitude of DC components is much larger than that of any ac components in general. The following fig. shows the average magnitude of DCT coefficients at different spatial frequencies for a few commonly utilized images, including “Lena,” “Pepper,” and “Baboon.” There, the horizontal axis represents the spatial frequency, specifically; $u+v, 0 \le u, v < 8$

The average magnitudes are calculated as below-

$$mag(0) = \frac{1}{K}\sum_{k=0}^{K-1} F_k(0,0)$$

$$mag(1) = \frac{1}{K}\sum_{k=0}^{K-1} \frac{1}{2}[F_k(0,1) + F_k(1,0)]$$

$$mag(i) = \frac{1}{K}\sum_{k=0}^{K-1} \frac{1}{(8-i-7)}(\sum_{u+v=i} F_k(u,v)) \ \ ;i = 0 \sim 14$$

The, Fig. 2 displays a huge discrepancy between DC coefficients and any AC coefficients in terms of magnitude. Image watermarking can be viewed as superimposing a weak signal (watermark) onto a strong background signal (image). The superimposed signals can be detected by Human Visual System (HVS) only if they exceed the detection threshold of HVS. According to Weber’s law [12], the detection threshold of visibility for an embedded signal is proportional to the magnitude of the background signal. This indicates that DC coefficients have much larger perceptual capacity than ac components.

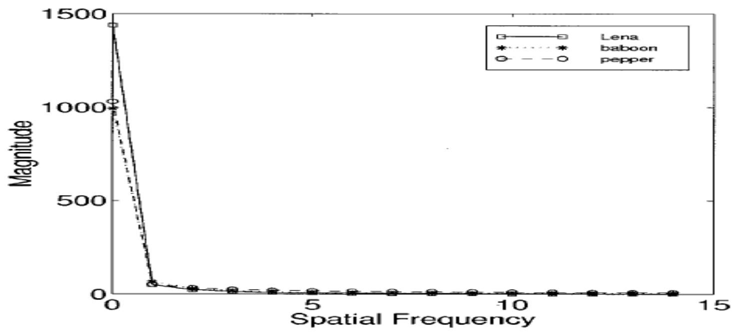


Fig: 2.1(b): Magnitudes of frequency coefficients

2.1.2 Embedding Image Watermark in DC Coefficient

Jiwu Huang et al [13] [14] has suggested an adaptive watermarking scheme based on texture masking and luminance masking. Firstly all host image blocks are classified into two categories: S1 with weak texture and S2 with strong texture. The strength of watermark components embedded into a blocks in S1 is weaker than that embedded into a blocks in S2, since HVS is more sensitive to a gray-level change in the blocks in S1 than in the blocks in S2. On the other hand, the blocks in S2 permits stronger watermark components to be inserted. The classification of blocks into S1 and s2 is on the basis of edge point density.

The watermark $W = \{x_i; 0 \le i < n\}$ is composed of a random number sequence of length *n*, which obeys the Gaussian distribution *N (0,1)* , where *n=K* . The watermark is embedded by modifying the DC coefficients as follows:

$$F'_k(u,v) = F_k(u,v)(1+\alpha x_k) \quad if\ u = v = o$$
$$= F_k(u.v) \quad otherwise$$

Where $F_k\ (u,\ v)$ is the DCT coefficient in k^{th} block and $F'_k(u,v)$ is corresponding watermarked coefficient.

The detection of watermarks is carried out straightforwardly by employing correlation technique. The corrupted watermark is extracted from attacked watermarked image and correlated with original watermark sequence. If correlation greater than a threshold then it confirms existence of watermark.

2.2 Image Watermarking using JND mask

It proposes a visible watermarking scheme embedding watermark image into a host image. It utilizes the perceptual information of the image content and to provide some perceptual criteria in the watermarking process. This directly results in providing the watermark less visibility in watermarked image.

2.2.1 Generation of JND mask

The process of embedding a watermark in an image can be regarded in the same way as adding noise to the image. These distortions are proportional to the amplitude of the embedded signal. Consequently, an image can be distorted only to a certain limit without making the difference between the original and the altered one perceptible. This limit varies according to the image content and is called JND. To estimate the JND mask four important image characteristics are considered: texture, edge, corner and luminance. This means that these areas are the most suitable ones in which to hide the watermark signal. In contrast to that, edge information of an image is the most important factor for the human vision perception. Consequently, edges have the lowest just noticeable distortion values. Similarly, smooth image areas have a general band pass characteristic. They influence human perception and consequently their JND values are also comparatively low.

1. Texture: It is defined as the visual quality of the surface of the object, exposed in an image by variances in tone, depth and shape. To determine a measure for the texture information within each block based on the energy in the AC coefficients we use the mathematical expression:

$$P_T = \log(\sum_{i=1}^{63} v_i^2) \text{ .... } (1)$$

Here the 64 DCT coefficients of the 8 x 8 block that is being considered. We must note that the value of the DC component of the DCT coefficients is not considered when calculating the texture value. For each block the obtained values of are first scaled to the range of [0, 64] and then the normalized values are assigned to the corresponding blocks.

$$M_T = \frac{64 * P_T}{\max(P_T)} \text{ .... } (2)$$

Hence for an image matrix of size 256 X 256 will have a matrix of size 32 X 32 where each one of those values corresponds to the texture information of each 8 x 8 block.

2. Edge: Edges are extracted from the pixel domain and this information is useful in determining the amount of watermark information that can be embedded in the image. Normalized edge information for each block is calculated using the formula:

$$M_E = \frac{64 * P_E}{\max(P_E)} \text{ .... } (3)$$

Where, P_E is the cardinality of set of pixels at edge locations in each block while max P_E is the maximum value of P_E over the entire image blocks.

3. Corner: Corners have long been recognized as visual information carriers [16]. An improved corner detection algorithm based on curvature scale space (CSS) with adaptive threshold and dynamic region of support is used. Methods employing CSS to detect corners have been very successful and it is believed to perform better than the other corner detectors [16], [17].

4. Luminance: It is defined as the way the human eye perceives brightness of different colours. This mean value of luminance of a local block can be estimated by the formula, using DCT domain approach as

$$D_L = \left\{ \frac{DC_b}{DC_{mean}} \right\}^{\alpha} \quad \ldots\ldots\ldots\ (5)$$

Where, DC_b is the DC coefficient of the DCT for block b,
DC_{mean} is the DC coefficient of the mean luminance of the display α is the parameter that is used to control the luminance sensitivity. The value of α is set to 0.649 as per the model used by the authors [19]. The luminance factor is calculated by measuring the average pixel value of the gray scale image for that block.

$$M_L = \frac{P_L}{64} \ldots\ldots\ldots\ldots\ (6)$$

Where P_L is the sum of all the pixel values in the block and M_L is the average of the luminance values within all block.
The factors obtained from texture, edges and the corners of the image put together are called as the spatial masking values, as they are obtained directly by analyzing the pixels in the spatial domain. After obtaining the four values corresponding to the texture, edges and corners the initial mask is generated using the equation:

$$J_I = M_T - \frac{1}{2}(M_E + M_C) \quad \ldots\ldots\ (7)$$

Hence a correction to the initial mask is introduced and the final JND parameter value for each block is calculated as:

$$J_F = J_I + \quad (128 - M_L)2 \ldots\ldots\ldots\ (8)$$

Where J_I is the initial JND parameter value and ML is the average of the luminance values within the considered block.

2.2.2 Watermark Embedding

The host image as well as watermark image used is gray scale images of size 256 * 256. The visible block based watermarking process in DCT domain is represented in figure 2.2 and explained below:

a. The host image I and watermark image W each are 256*256 gray scale images.
b. The host image and the watermark image are divided into blocks of size 8X8.
c. The DCT coefficients for each block of the host image as well as watermark image are calculated.
d. For each block of the host image I, final JND mask (JF) is generated using Texture, Edge, Luminance and Corner information as described in section 2 Eq A.
e. JND mask values (JF) of each block is then scaled to the range of 0.01 to 0.1 to generate JFscaled for each block.
f. Watermark image is then embedded into host image using the formula

$$W_{mk}(i,j) = \{(1 - JND_{scaledk}) * H_k(i,j)\} \quad + \quad \{JND_{scaledk} * W_k(i,j)\}$$

Where k is the block number (k= 1 to 1024), $H_k(i,j)$ is $(i,j)^{th}$ DCT coefficient of k^{th} block of host image, $W_k(i,j)$ is $(i,j)^{th}$ DCT coefficient of k^{th} block of watermark, $W_{mk}(i,j)$ is $(i,j)^{th}$ DCT coefficient of k^{th} block of watermarked image, $ND_{scaledk}$ is the scaled JND mask value for block k (k=1 to1024).
g. Inverse DCT for each block of the watermarked image is calculated to bring watermarked image back into spatial domain. The scaled JND value of the host image controls the strength of watermark for each block.

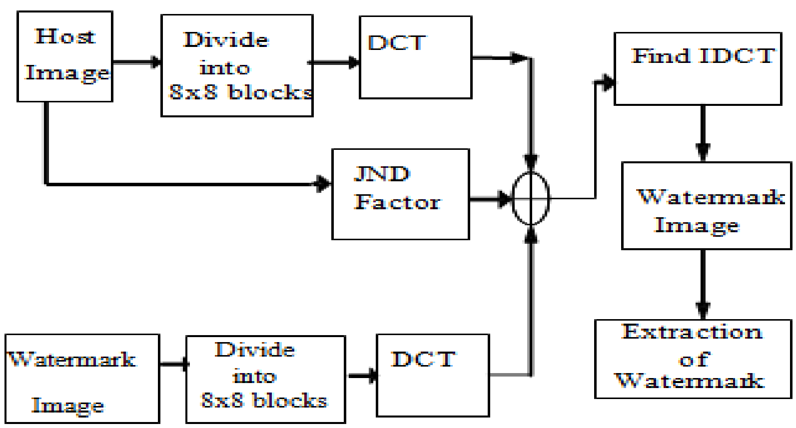


Fig: 2.2: Block diagram of content based watermarking

2.2.3 Watermark Evaluation

A Visible Watermark should have desirable properties such as the watermark should spread in a large area of the image in order to avoid its deletion. The watermark must be difficult to remove. Rather, removing a watermark should be more costly and labor intensive than purchasing the image from the owner. However, in order to evaluate and compare performance of different approaches below performance metrics are used.

1. PSNR: For quantitative measurements, the cover image perceptibility is determined using PSNR values. Two common performance evaluation metrics are combined to form the fitness function; the

Peak Signal to Noise Ratio (PSNR) PSNR of watermarked image should not go below some level after attack so we can use PSNR for performance evaluation between different outputs we got from various algorithms. The Peak Signal to Noise Ratio (PSNR) is utilized to evaluate image quality. There has been much emphasis on the robustness of watermarks to common signal processing operations such as compression and signal filtering. To check the visual distortions of watermark image we calculate the Peak Signal to Noise Ratio (PSNR). The peak signal to noise ratio (PSNR) is calculated by using the following mathematical Expression:-

$$PSNR = 20\log_{10}\left(\frac{255}{\sqrt{MSE}}\right) \quad \ldots\ldots\ldots (9)$$

Where MSE is the root mean square error and 255 is the maximum value of luminance level.

2. Correlation: The correlation factor measures the similarity between the original watermark and the watermark extracted from the attacked watermarked image (robustness) [12]. The correlation factor may take values between 0 (random relationship) to 1 (perfect linear relationship). Formula:

$$\rho = \frac{x}{(row * column)} \quad \ldots\ldots\ldots (10)$$

Where,

$$x = \sum_{i=1}^{N}(W_i * B_i)$$

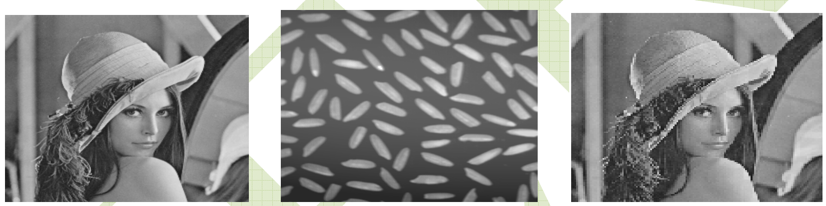
Where, W = watermarked Image, B = Watermark Image.

2.2.4 Attacks

Watermarked images are affected by various attacks such as cropping, salt & pepper noise and rotation etc. These attacks can destroy the inserted watermark, so that the copyright problem may arise. The effect of these attacks can be reduced by properly inserting the watermark with effective algorithm. In this proposed watermarking technique the watermarked image is subjected to three types of distortions: compression, noise, and filter. Watermarked images have been compressed using JPEG compression. Our scheme performs excellently against JPEG compression and moderately well against common spatial attacks. Gaussian noise with zero mean is introduced to verify as to what extent our proposed scheme can withstand noise. To test the strength of watermark image on the host image, we pass the watermarked image through filter. The watermarked image in spatial domain is passed through a LOG (Laplacian of Gaussian filter) and Median filter. Median filter is similar to an averaging filter; each pixel output is set to the median of the pixel values in the neighbourhood of the corresponding input pixel, as specified by the window size. The window size of 3 x 3 is used for our experiments.

3. Experimental Results

Several experiments have been conducted to test performance of the proposed strategy. In this section some selected results are reported, some experiments are conducted to demonstrate the performance of the proposed content based watermarking based on grayscale images. The test images, 'Lena 'as a host image and 'Rice' as a watermark image both of size 256*256 are used. From the following figures, it is observed that there is no perceptually noticeable difference in the images due to watermarking. Numerical value of the performance metrics, PSNR is quite high and correlation almost equal to one, these shows that watermark embedding does not degrade the visual quality of the image. Robustness of the proposed scheme against normal signal processing operation such as compression, noise and filtering has been evaluated on all the watermarked images. In this, watermarking technique the watermarked image is subjected to three kinds of distortions: compression, noise, and filter. We then test our scheme for its robustness against different types of noise. Salt and pepper noise has been added to the watermarked image. This is done by introducing noise into the watermarked Lena of size 256*256. Gaussian noise with zero mean is introduced to verify as to what extent our proposed scheme can withstand noise. From the results in following table 3 (c), we can examine that for a Gaussian noise of 2%, the watermark recovery is moderate, with very few detection errors. From the table we infer that the PSNR values for attacks like LOG filter and Gaussian noise are poor, whereas the same is good for Salt & Pepper Noise attack. In almost all attacks, the correlation reduces and there are slight changes in PSNR relation.



(a) Host Image (b) Watermark Image (c) Watermarked Image

Fig: 3. (a): Host Image, watermark Image and Watermarked Image.

Salt & pepper Gaussian noise Jpeg compression

Median filter LOG filter Cropping

Fig: 3. (b): Recovered images from different attack

Sr.	I, W	DC		High		Mid		Low	
		PSNR	ρ	PSNR	P	PSNR	P	PSNR	P
Set A: Watermarking without any attack									
1	L + R	75.79	1.00	76.68	1.00	76.63	1.00	76.35	1.00
2	L + F	73.94	1.00	74.80	1.00	74.77	1.00	73.92	1.00
3	C + R	74.18	1.00	75.39	1.00	75.32	1.00	75.14	1.00
4	C + F	73.65	1.00	74.55	1.00	74.50	1.00	74.38	1.00
Set B: Watermarking with LOG filter attack									
1	L + R	72.39	0.67	72.80	0.69	72.76	0.68	72.64	0.67
2	L + F	71.39	0.48	72.24	0.53	72.17	0.52	71.77	0.49
3	C + R	70.46	0.69	70.94	0.70	70.91	0.71	70.83	0.69
4	C + F	70.18	0.53	70.58	0.54	70.55	0.55	70.49	0.53
Set C : Watermarking with Median filter attack									
1	L + R	73.84	0.77	74.38	0.79	74.33	0.78	74.16	0.77
2	L + F	72.47	0.59	73.09	0.61	73.08	0.61	72.95	0.58
3	C + R	71.81	0.79	72.47	0.80	72.42	0.80	72.32	0.79
4	C + F	71.43	0.64	71.96	0.66	71.92	0.66	71.84	0.64
Set D: Watermarking with Salt and Pepper noise attack									
1	L + R	75.15	0.98	75.70	0.98	75.79	0.98	75.45	0.98
2	L + F	73.44	0.94	74.40	0.97	73.42	0.98	73.43	0.98
3	C + R	73.62	0.98	74.62	0.98	74.73	0.98	74.47	0.98
4	C + F	73.32	0.96	73.97	0.94	74.03	0.95	73.94	0.96
Set E: Watermarking with Compression attack									
1	L+R	73.95	0.64	74.50	0.66	74.46	0.66	74.29	0.65
2	L+F	72.67	0.45	73.29	0.47	72.94	0.56	73.17	0.45
3	C+R	72.66	0.67	73.47	0.68	73.43	0.69	73.30	0.68
4	C+F	72.30	0.50	72.92	0.52	72.88	0.51	72.79	0.50
Set F: Watermarking with Cropping attack									
1	L+R	74.92	1.00	75.64	1.00	75.60	1.00	75.38	1.00
2	L+F	73.12	1.00	74.10	1.00	73.35	1.00	73.34	1.00
3	C+R	73.58	1.00	74.61	1.00	74.56	1.00	74.40	1.00
4	C+F	73.11	1.00	73.90	1.00	73.86	1.00	73.76	1.00
Set G: Watermarking with Gaussian attack									
1	L+R	73.78	0.49	74.34	0.51	74.29	0.51	74.16	0.49
2	L+F	72.50	0.35	73.14	0.37	72.50	0.60	72.54	0.59
3	C+R	72.73	0.48	73.57	0.50	73.50	0.50	73.40	0.48
4	C+F	72.34	0.34	72.97	0.35	72.94	0.35	72.88	0.33

Table 3 (c): Experimental Analysis with various attacks

CONCLUSION

From experimental analysis, it has been observed that the watermarks should be embedded in perceptually significant components; DC coefficients are explicitly excluded from watermark embedding. Content based watermarking is a capable approach for solving a wide variety of problems associated with distribution, copyright management and authentication control of digital images. The focus is on the fine tuning of the scaling factor for content based watermarking using DCT. Content of image is evaluated using certain characteristics such as Edge, Texture, Corner and Luminance. Host image sets and watermark image sets include gray scale images each and all combinations of host and watermark images are verified. Performance evaluation metrics used are PSNR and correlation. It is observed that Watermarked image with JND is superior as compared to that of without JND.

REFERENCES

[1] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "*Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Processing, vol. 6, pp. 1673–1687, Dec. 1997.*

[2] Ingemar J. Cox, Matt L. Miller, "*A Review of Watermarking & Importance of Perceptual Modeling", Proceedings of Electronic Imaging", February 1997*

[3] C.M.Kung,et al., "*Watermark Technique using frequency Domain", Digital Signal Processing, 2002 – IEEE, 729 - 731 vol.2, 0-7803-7503-3.*

[4] Wen-Nung Lie, Guo-ShiangLin and Ta-Chun Wang, "*Robust Image Watermarking on the DCT Domain",ISCAS2000-IEEE international symposium on circuits and system,May28-31,2000,Geneva,Switzerland.*

[5] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking, Morgan Kaufmann Publishers, 2002.*

[6] Craver, S., Memon, N., Yeo, B.-L. and Yeung, M. M., *Resolving rightful ownership with invisible watermarking techniques: limitations, attacks and implications, IEEE Journal on Special Areas in Communications, 1998 ,16(4): 573-5861.*

[7]Cox I. J., Kilian J., Leighton F. T. and Shamoon T., *Secure spread spectrum watermarking for multimedia, IEEE Trans. Image Processing, 1997, 6(12): 1673-1687.*

[8] Koch E. and Zhao J., *Toward robust and hidden image copyright labeling, in Proc. IEEE Workshop on Nonlinear Signal and Image Processing, 1995, pp. 452-455.*

[9] Hsu Chiou-Ting, Wu Ja-Ling. *Hidden Digital Watermarks in Images, IEEE Trans. on Image Processing, 1999, 8(1):58-68.*

[10]Dimitar Taskovski and et al, "*Digital image watermarking using GenLOT", IEEE MELECON 2002,May 7-9,2002,Cairo,Egypt.*

[11] Shuangyuan Yang and et al, "*A Robust Adaptive Image Watermarking Algorithm", 2004 IEEE international conference and Expo (ICME).*

[12] Fengsen Deng and Bingxi Wang, "*A Novel Technique for Robust watermarking in the DCT Domain", IEEE international conference, Neural Network and Signal Processing, Dec 14-17, 2003, Nanjing, China.*

[13] Jiwu Huang, Yun Q.Shi and Yi Shi, "*Embedding image watermarking in DC components Domain", IEEE transactions on circuits and system for video Technology,Vol.10,No.6,Sept 2000.*

[14] Barni M,Bartolini F,Cappellini V.A ,(1998). "*DCT-domain system for robust image watermarking". Journal of Signal Processing, Vol. 66, No. 3, pp.357-372.*

[15] Gaorong Zeng and Zhengding Qui, "*Image Watermarking Based on DC Component in DCT", International Symposium on Intelligent Information Technology Application Workshop.]*

[16] A. B. Watson, "*Efficiency of an image code based on human vision," J. Opt. Soc. Amer. A, vol. 4, no. 12, pp. 2401–2417,Dec. 1987*

[17] B. Zhu and A. H. Tewfik, "*Low bit rate near-transparent image coding," in Proceedings of the SPIE International Conference on Wavelet Applications for Dual Use, Orlando, FL, 1995, vol. 2491, pp. 173–184.*

IJIERT