

Robust Digital Watermarking of Images using Wavelets

P.RAMANA REDDY¹, DR. Munaga.V.N.K.PRASAD², DR D. SREENIVASA RAO³

Abstract:The central idea of this paper is to develop an algorithm that embeds the watermark information, with out much distortion to the image, while making it possible to extract the watermark by use of correlation. We 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. The operation of embedding and extraction of the watermark is done in the frequency domain, thereby providing robustness against common frequency-based attacks including image compression and filtering. We use spread spectrum algorithm for watermarking such as pseudo random sequences enabling an easier generation, encryption and a much better detection, of the watermark. Our watermarking scheme deals with the extraction of the watermark information in the absence of the original Image, i.e., blind watermarking. Hence we make use of correlation - based watermark detection. A performance evaluation is carried with regard to quality, compression ratio and different signal to noise ratios. These properties were chosen because they have the greatest impact on the implementation effort.

Key Words:Digital watermarking, wavelets, embedding, extraction, correlation, performance metrics.

I. INTRODUCTION

The use of Internet as a platform for distribution of digital media has grown in recent years causing serious concerns about unauthorized use and manipulation of this digital content. Attackers have the freedom to obtain copies of copyrighted multimedia information via the Internet, so protection of multimedia information has attracted lots of attentions. Digital watermarking is a method of securing the digital media by embedding additional information called digital signature or watermark into the digital contents such that it can be detected, extracted later to make an assertion about the multimedia data.

A watermark itself can be a random signal, a meaningful message, or a company's logo that can be used for ownership protection, copy control and authentication. In order to watermarking as a way of copyright protection, high robustness (the watermark should survive any kind of intentional or unintentional alterations) and low visibility (the watermark should not introduce perceptible artifacts) should be ensured, and only authorized users should gain access to the watermark data.

The image watermarking algorithms can be classified into

two categories: spatial-domain techniques (spatial watermarks) and frequency-domain techniques (spectral watermarks). The spatial-domain techniques directly modify the intensity values of some selected pixels while the frequency-domain techniques modify the values of some transformed coefficients [2]. The simplest spatial-domain image watermarking technique is to embed a watermark in the least significant bits (LSBs) of some randomly selected pixels. The watermark is invisible to human eyes but the watermark can be easily destroyed if the watermarked image is low-pass filtered or removing (zero out) the least significant bits of the pixel or upon JPEG compression.

The frequency-domain technique first transforms an image into a set of frequency domain coefficients [1], [3], [9], [13]. The transformation adopted may be discrete cosine transform (DCT), discrete Fourier transforms (DFT), or discrete wavelet transforms (DWT) etc. The watermark is then embedded in the transformed coefficients of the image such that the watermark is invisible and more robust for some image processing operations. Finally, the coefficients are inverse-transformed to obtain the watermarked image [4], [7].

II. PROPOSED WATERMARKING SCHEME

The wavelet decomposition decomposes the image into three spatial directions i.e. horizontal, vertical and diagonal. Hence wavelets reflect the anisotropic properties of HVS more precisely. The human visual system (HVS) is related to the perceptual quality [9], measured according to the sensitivity/sharpness of a human eye to see details in an image. Research into human perception indicates that the retina of the eye splits an image into several frequency channels each spanning a bandwidth of approximately one octave. The signals in these channels are processed independently. Similarly, in multiresolution decomposition, the image is separated into bands of approximately equal bandwidth on a logarithmic scale. It is therefore expected that use of the discrete wavelet transform will allow the independent processing of the resulting components without significant perceptible interaction between them, and hence makes the process of imperceptible watermarking more effective[10]. The multiresolution successive approximation not only enhances the resolution of an image, but also enhances the resolution of watermark simultaneously. This advantage of the DWT allows using higher energy watermarks in regions where the HVS is known to be less sensitive so that embedding watermarks in these regions provides to increase the robustness of the watermarking techniques. In this paper, a meaningful image watermark is embedded in the DWT domain. The watermark detection is a blind method i.e. is without the use of original image [1]. We

¹ Associate Professor, ECE Department, JNTU College of Engineering, Anantapur, INDIA.

² Assistant Professor, Institute for Development and Research in Banking Technology (IDRBT), Hyderabad, INDIA

³ Professor, ECE Department, JNTU College of Engineering, Hyderabad, INDIA

embed a watermark into an image by modifying coefficients of mid frequency bands i.e. LH and HL subbands, and extract the watermark by analyzing perturbation of coefficients from a suspected image.

A. Discrete Wavelet Transform (DWT)

The Fourier transform, which provides a representation of the transformed signal in the frequency domain, is widely used in signal processing. However, the loss of time information in a signal by Fourier transform will lead to the difficulty in processing [8]. The wavelet transform is an excellent time-frequency analysis method, which can be well adapted for extracting the information content of the image. A brief introduction to wavelet is as follows [16].

Applying a 1-D transform to all the rows of the input image and then repeating on all of the columns can be computed the 2-D transform. When one-level 2-D DWT is applied to an image, four transform coefficient sets are created. The four sets are LL, HL, LH, and HH, where the first letter corresponds to applying either a low pass or highpass filtering to the rows, and the second letter refers to the filter applied to the columns [4], [7]. The process of multiple frequency decomposition of one level is illustrated in Fig.1

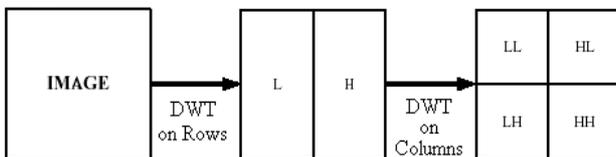


Fig.1 DWT Decomposition of Image

wavelet analysis of an original image can divide image into an approximate image LL and three detail images LH, HL and HH., the approximate image hold most of the information of the original image, while the others contain some details such as the edge and textures will be represented by large coefficients in the high frequency sub-bands [15]. The reconstruction of the image is achieved by the inverse discrete wavelet transform (IDWT).

B. Spread spectrum Watermarking

To overcome the limitations in watermarking due to methods like LSB (least significant bit) substitution and to make the system more robust against attacks, the watermark can be spread across the cover object by using more number of bits than the minimum required. This scheme of hiding the data ensures the survival of watermark under various attacks due to redundancy. Generally the message used to watermark is a narrow band signal compared to the wide band of the original image. Spread spectrum techniques [1] applied to the message allows the frequency bands to be matched before embedding the watermark through the original image. Spread spectrum technique also offer the possibility of protecting the watermark privacy using a secret key to control a pseudonoise generator. Pseudo noise sequences are used for watermarking because of their very good correlation properties, noise like characteristics, easier to generate and resistance to interference.

Pseudorandom sequences are used as the spreading sequences. Pseudonoise is generated by using matlab

function rand with initial seed and round the random numbers to its nearest integer and thus generating 0 and 1.

Cover image used for watermarking purpose is Lena image of size 512 X 512, bitmap, gray image is shown in Fig.2. The original image is decomposed into two level wavelet decomposition using Haar wavelet to obtain mid band frequency coefficients LH and HL.



Fig.2 Original Lena image for watermarking

Since ASCII codes cannot tolerate a single bit error, an attack can entirely change the meaning of that character, and thus the message. A highly redundant form of message, such as an image is used as a watermark. The watermark is a binary image of size 64 x 64 is used. The monochrome watermark image is converted into binary image of "1"s and "0"s: [5] which is shown Fig.3



Fig.3 watermark

The wavelet coefficients of mid frequency band [1] i.e. LH and HL subband frequencies are selected for embedding. Embedding the watermark in the low frequency bands will cause the perceptual changes in the image and embedding in high frequency bands will affect the robustness of the watermark, hence mid band frequencies i.e. LH and HL subbands are selected which will survive various frequency attacks.

C. Watermark Embedding

The pseudorandom sequences are generated with the key as the initial seed is added [1] to the selected horizontal and vertical DWT coefficients (HL, LH) of the original image according to the equation.

$$I_w(x, y) = I(x, y) + k \times W(x, y)$$

In which $I(x, y)$ representing the DWT coefficients of the original image, $I_w(x, y)$ is the watermarked image, K denotes the gain factor that is usually used to adjust the invisibility of the watermark. This process of watermark embedding is shown in Fig.4 which explains after wavelet coefficients are computed LH and HL are chosen, then depends upon the strength of watermark i.e either 0 or 1, then PN sequence will be added to HL & LH coefficients.

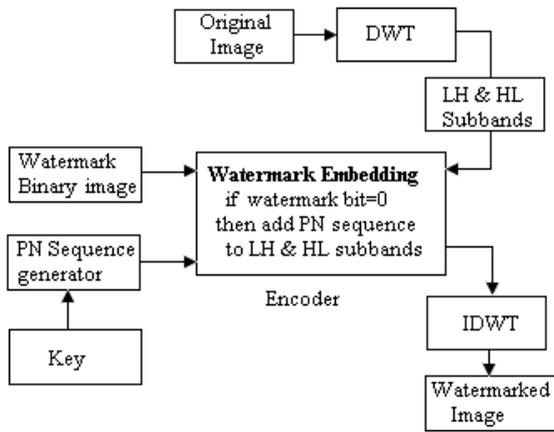


Fig.4. Watermark embedding process

D. Watermark Extraction

Our watermarking scheme deals with the extraction of the watermark information in the absence of the original image, i.e., blind watermarking. Hence correlation measure [1], [11] is used to detect the watermark. The correlation is calculated between the generated PN sequence matrix and subband coefficients of watermarked Image for each of the pixels in the watermark string and if it exceeds a particular threshold then the watermark is said to be detected. The threshold for the decision is set as the mean of the correlation value for all the pixels, The watermark extraction process is shown in Fig 5

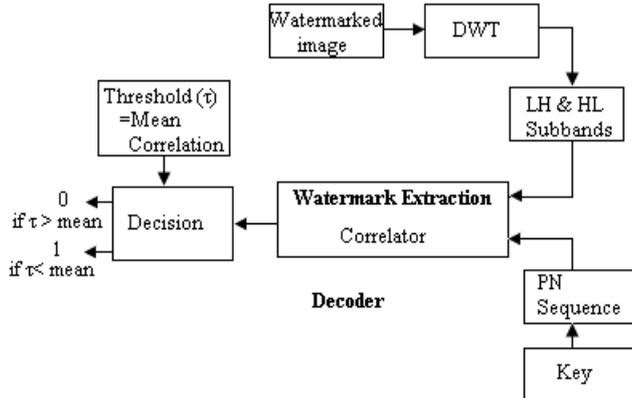


Fig.5 Watermark Extraction Process

During computation in the first level resolution the watermark is called detected, if the correlation between the extracted bits and the original bits is above a threshold. If there is no watermarked detected then, the decoder adds the second resolution level. Once again, if the correlation between the extracted bits and the original bits is above a threshold then the watermark is detected [17].

III. PERFORMANCE EVALUATION OF WATERMARKING SCHEME

In our investigation, the performance evaluation is done based on three performance metrics [12]; these are imperceptibility, execution time, and robustness against common signal processing operations.

A. Measuring Imperceptibility:

In order to measure the quality of the image at the output of

the decoder, mean square error (MSE) and peak to signal to noise ratio (PSNR) ratio measurement [10] these measures will indicate quality of image with watermarking process. The mean square error is evaluated by

$$MSE = \frac{1}{M * N} \sum_{n=0}^{N-1} (I_w - I)^2$$

and the PSNR is evaluated by the formula

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

Where I_{peak} is the peak values of the input Image (usually 255 is the maximum value of luminance level)

Similarity factor [6] is also evaluated which establishes the similarity of pixel intensities between the original image and the watermarked image. This helps us to calculate the changes in the perceptual quality of the image more precisely. The formula for SIM is shown below:

$$SIM = \frac{\sum_i \sum_j I(i, j) * I_w(i, j)}{\sum_i \sum_j I_w(i, j)^2}$$

Where $I(i, j)$ is the original image and $I_w(i, j)$ is the watermarked image. The similarity factor should be equal to 1.

B. Robustness

Robustness can be evaluated by applying various kinds of normal signal distortions and attacks that are relevant for the target application. The robustness can be assessed by measuring detection probability of the watermark after signal distortion. A quality estimation parameter to check the robustness of the extracted watermark, named as Bit Correct Rate (BCR) is computed as an index [15] to the objective of robustness of the watermark. The bit correct ratio (BCR) is defined as the ratio of correctly extracted bits to the total number of embedded bits. The Bit correct rate is expressed using the formula.

$$BCR = \frac{\text{Total No. of correctly detected watermark bits}}{\text{Total No. of embeded watermark bits}}$$

The Bit correct rate should be equal to 1.

C. Execution Time

Another important tool for evaluating the speed of algorithm is measurement of the amount of time required to embed a watermark into a host image, and then extract it afterwards. In our investigation, actual time in CPU cycles will be used as a measure of execution time.

D. Simulation results

Watermark embedding in the original image Lena. The difference image shown in Fig 6 is the absolute difference of the pixel intensities of the watermarked image and the original image.



Fig.6. Watermarked image and Difference image

Watermarked Image and the extracted watermark for the gain of 0.4 and at level II decomposition is shown in Fig. 7



Fig: 7 Extracted watermark

Simulation results of watermarking algorithm with varying gain factor are shown in Table 1.

TABLE 1: SIMULATION RESULTS WITH VARYING GAIN FACTOR

| Image: Lena Gray image of size 512x512 | | | | Decomposition level: II Level | |
|---|------|-------|-------|----------------------------------|-------|
| S.No | Gain | MSE | PSNR | SIM | BCR |
| 1 | 0.1 | 0.588 | 50.42 | 1 | 0.932 |
| 2 | 0.2 | 1.365 | 46.77 | 1 | 0.986 |
| 3 | 0.4 | 4.508 | 41.59 | 1 | 1 |
| 4 | 0.6 | 9.810 | 38.21 | 1 | 1 |
| 5 | 0.8 | 17.17 | 35.78 | 1 | 1 |
| 6 | 1.0 | 26.69 | 33.86 | 1 | 1 |
| 7 | 1.2 | 38.39 | 32.28 | 1 | 1 |

The simulation results show that the PSNR value is high around 50.42 for a gain of 0.1 this is because at low gain factor lesser will be the modifications of the wavelet coefficients and hence results in better quality of the watermarked image. The similarity factor is close to unity even for high gain factor, as the wavelet coefficients are modified to a level below the perceptual level. The robustness of extracted logo is high around 0.932 when the gain factor is low this is because at low gain factor the embedding strength will be less and as the gain factor increases the Bit correct rate increases this is because high gain factor increases the embedding strength and increases the robustness of the watermark.

E. Attacks on watermarked image:

Common signal processing procedures such as noise addition, image compression, median filtering as well as geometrical attacks such as cropping is used for the analysis of the watermarked image.

3.5.1 Compression: Image Compression will result in loss of redundant data and thus affecting the robustness of watermark. The watermarked images are compressed using different quality percentages ranging from 10 to 90 percent with a gain of 0.4 and II level decomposition. Figure 8 shows watermarked image and decompressed image after compression. The recovered logo contains huge artifacts this is due to the loss of data containing the watermark information due to compression. In spite of high compression the extracted watermark is highly recognizable



Fig.8. Simulation results of compression

Recovered watermark is shown in Fig 9 for different quantization with gain factor from 10 to 90% for level II decomposition.

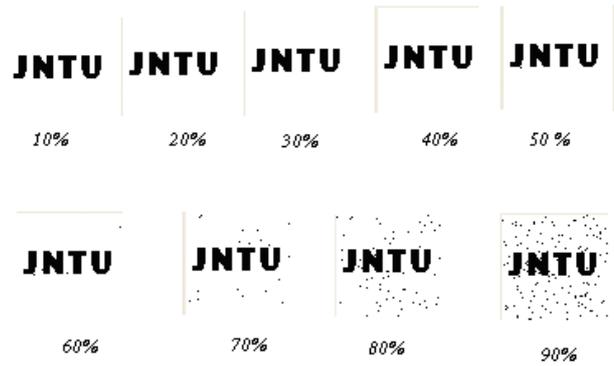


Image: Bird, Gain 0.6, Decomposition Level: II

Fig.9. Recovered watermarks for compression

TABLE 2: SIMULATION RESULTS: COMPRESSION

| Image: Lena Gray image of size 512x512 Attack : Compression | | | | | Decomposition level: II Level Gain: 0.4 | |
|---|-----|-------|-------|-------|---|-------|
| S.No | % Q | CR | MSE | PSNR | SIM | BCR |
| 1 | 10 | 2.11 | 11.84 | 37.39 | 1 | 0.99 |
| 2 | 20 | 3.82 | 21.95 | 34.71 | 1 | 0.99 |
| 4 | 40 | 7.57 | 41.18 | 31.98 | 1 | 0.984 |
| 6 | 60 | 11.46 | 62.86 | 30.14 | 1 | 0.961 |
| 8 | 80 | 15.84 | 84.45 | 28.86 | 1 | 0.927 |
| 9 | 90 | 17.99 | 95.73 | 28.32 | 1 | 0.940 |

The simulation results show that the PSNR value and Mean square error is increasing as the quantization increases this is because as the compression ratio increases the loss of redundant data in the image. The similarity factor is unity and thus the imperceptibility of the image is less affected. The robustness of the watermark is greatly affected this is because loss of data containing the watermark information increases with the increase in compression ratio various results are listed in Table.2

3.5.2 Noise addition The watermarked images corrupted with a scaled Gaussian noise of zero mean and different variances and with salt and pepper noise with different densities.

Salt and pepper noise: Fig 10 shows the simulation results of watermarked image corrupted with Salt and Pepper noise at a gain factor of 0.4 for level II decomposition and the extracted watermark after extraction more results are shown in Table 3 different noise intensities.



Fig.10. Simulation results of Salt & Pepper noise

TABLE 3: SIMULATION RESULTS FOR SALT & PEPPER NOISE

| Image: Lena Gray image of size 512x512 Noise : Gaussian noise | | | | Decomposition level: II Level Gain: 0.4 | |
|---|-------------------|---------|-------|---|-------|
| S.No | Variance of noise | MSE | PSNR | SIM | BCR |
| 1 | 0.02 | 1248.09 | 17.16 | 0.936 | 0.983 |
| 2 | 0.04 | 2319.09 | 14.47 | 0.888 | 0.986 |
| 4 | 0.06 | 3267.19 | 12.98 | 0.850 | 0.953 |
| 6 | 0.08 | 4067.58 | 12.03 | 0.821 | 0.926 |
| 8 | 0.1 | 4774.37 | 11.34 | 0.796 | 0.955 |

Gaussian noise: Fig 11 shows the simulation results of watermarked image corrupted with Gaussian noise of zero mean and varying the variance of the noise and the extracted watermark after extraction results are shown in Table 4 different noise intensities.



Fig.11.Simulation results for Gaussian noise

TABLE 4 : SIMULATION RESULTS FOR GAUSSIAN NOISE ADDITION

| Image: Lena Gray image of size 512x512 Noise : Salt and pepper | | | | Decomposition level: II Level Gain: 0.4 | |
|--|------------------|---------|-------|---|-------|
| S.No | Density of noise | MSE | PSNR | SIM | BCR |
| 1 | 0.02 | 378.75 | 22.34 | 0.983 | 0.997 |
| 2 | 0.04 | 730.67 | 19.49 | 0.967 | 0.998 |
| 4 | 0.06 | 1122.82 | 17.62 | 0.948 | 0.997 |
| 6 | 0.08 | 1485.60 | 16.41 | 0.931 | 0.972 |
| 8 | 0.1 | 1848.98 | 15.46 | 0.914 | 0.967 |

The simulation results shows that PSNR is less and the mean square error of the watermarked image is high this is due to the corruption of the image with noise of high density. The similarity factor of the corrupted image with respect to the original Image is decreasing as the density of the noise is increasing. The robustness of the watermark is also affected because more number of coefficients will be modified due to addition of noise and hence results in bad recovery of watermark.

Filtering: Median filtering is a nonlinear operation often used in image processing to reduce high frequency noise in an Image. Median filtering is more effective than convolution

when the goal is to simultaneously reduce noise and preserve edges. Each output pixel contains the median value in the m-by-n neighborhood around the corresponding pixel in the input Image. The simulation results are shown in Fig 12 more results are shown in Table 5 for different sizes of masks.



Fig :12 Simulation results for median filter

TABLE 5: SIMULATION RESULTS FOR MEDIAN FILTER SIZE

| Image: Lena Gray image of size 512x512 Attack: Median Filter | | | | Decomposition level: II Level Gain: 0.4 | |
|--|-------------|--------|-------|---|-------|
| S.No | Filter size | MSE | PSNR | SIM | BCR |
| 1 | 3x3 | 20.76 | 34.95 | 1 | 0.99 |
| 2 | 5x5 | 50.46 | 31.10 | 1 | 0.87 |
| 4 | 7x7 | 82.69 | 28.95 | 1 | 0.780 |
| 6 | 9x9 | 112.71 | 27.61 | 1 | 0.755 |

The simulation results shows that PSNR value is decreasing as the size of median filter is increasing and the Mean square error is increasing with size of the median filter this is due to as the size of median filter increases the median of the output pixel will decreases and thus affects the PSNR and MSE. The similarity factor is less affected and is unity, this is because the median filter removes the high frequency components of the image which are less perceptual, but the robustness of the image is affected this is due to the loss of more coefficients containing the watermark information.

Cropping

Cropping is a geometrical attack where a small portion of the watermarked image is cut/removed as an attempt to remove the significant portion of the image to remove the watermark. The recovered watermark for cropping block of size 32 x 32 portion of the image is shown in the Fig 13 some more results are shown in Table 6 for different cropping sizes at different locations of watermarked image.



Fig.13 Extracted logo for Cropping of watermarked image

TABLE 6: SIMULATION RESULTS FOR CROPPING

| Image: Lena | Decomposition |
|-------------|---------------|
|-------------|---------------|

| Gray image of size 512x512 Attack : Cropping | | | | level: II Level Gain: 0.4 | |
|---|------------|-------|-------|------------------------------|-------|
| S.No | Block size | MSE | PSNR | SIM | BCR |
| 1 | 8x8 | 7.17 | 39.57 | 1 | 0.999 |
| 2 | 16x16 | 16.12 | 36.05 | 1 | 0.999 |
| 3 | 32x32 | 73.07 | 29.41 | 0.99 | 0.999 |
| 4 | 64x64 | 411.9 | 21.98 | 0.969 | 1 |

The simulation results show that the PSNR and MSE are greatly affected this is due to cropping some portion of the image. The robustness of the watermark is less affected this is because the watermark is actually spread in the entire image not just in any one portion of the image.

Execution Time:

The embedding time of the encoder is around 40 to 50 Sec. and the extraction time of the decoder is around 180 to 200 sec this is because the decoder checks for the level I decomposition and second level decomposition as well for the presence of watermark.

IV. CONCLUSIONS:

This paper emphasized on the digital watermarking provides a comprehensive evaluation algorithm that embeds and extracts the watermark information effectively. The extraction is done without using original image hence it is a blind watermarking scheme. The experimental results show that our scheme is highly robust against various of image processing operations such as, filtering, cropping, compression, Gaussian noise and salt and pepper noise. Our observations regarding the proposed watermarking scheme are summarized below.

The simulation results shows that high quality image i.e. watermarked Image with high PSNR is obtained by embedding the watermark at low gain, but this will affect the robustness of watermark. Also embedding the watermark at high level decomposition (II Level Decomposition) improves both the quality of watermarked image and the robustness of watermark. The watermark embedding at a gain above 0.6 and at second level decomposition the watermarked image sustains various frequency and spatial attacks and results in good recovery of the watermark. Also the algorithm is a secured scheme only the one with the correct key can extract the watermark.

Future work concentrates on coding strategies to reduce the extracted watermark bit error and modification of the embedding technique to combat the multiple watermarking problem.

REFERENCES:

- [1] Arvind Kumar Parthasarathy and Subhash Kak, "An Improved Method of Content Based Image Watermarking" IEEE Transaction on broadcasting, Vol. 53, No. 2, June 2007, PP 468-479.
- [2] Ibrahim Nasir, Ying Weng, Jianmin Jiang, "A New Robust Watermarking Scheme for Color Images in Spatial Domain"
- [3] Deepa Kundur and Dimitrios Hatzinakos, "Digital watermarking using multiresolution wavelet decomposition"
- [4] Xiang-Gen Xia, Charles G. Boncelet and Gonzalo, " Wavelet transform based watermark for digital Images ", OPTICS EXPRESS, 7 December 1998, Vol. 3, No. 12, PP 497-511
- [5] 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, Publication: 17 November 2007
- [6] D. Taskovski, S. Bogdanova, M. Bogdanov" Digital watermarking in wavelet domain"
- [7] Maha Sharkas, Dahlia ElShafie, and Nadder Hamdy "A Dual Digital-Image Watermarking Technique" Transaction on Engineering, Computing and Technology, Vol 5, April 2005 ISSN 1305-5313
- [8] Rafael C. Gonzalez, R.E.Woods, Steven "Digital image processing using MATLAB"
- [9] Peter Meerwald " Digital image watermarking in the wavelet transform domain : P.Hd thesis"
- [10] Houng- Jyh Mike Wang, Po-Chyi Su and C.-C. Jay Kuo "Wavelet-based digital image watermarking" OPTICS EXPRESS, 7 December 1998, Vol. 3, No. 12, PP 491-496
- [11] M. Kuttera and F. A. P. Petitcolas "A fair benchmark for image watermarking systems"
- [12] Selena Kay and Ebroul Izquierdo" Robust Content based Image Watermarking"
- [13] Chirawat Temi, Somsak Choomchuay, and Attasit Lasaku, " A Robust Image Watermarking Using Multiresolution Analysis of Wavelet-Proceedings" of ISCIT2005
- [14] Abou Ella Hassanien, "A Copyright Protection using Watermarking Algorithm" Informatica, 2006, Vol. 17, No. 2, PP 187-198
- [15] www.amara.com/current/wavelet.html: An introduction about Wavelets- Amara Graps:
- [16] Vallabha V Hampiholi: Multiresolution, " Watermark Based on Wavelet Transform for Digital images"