International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 3– No.5 , July 2012 – www.ijais.org

Developing a Benchmark Model for Image Digital Watermarking

Rajwant Kaur
Lovely Professional University
G.T. Road, Phagwara, Punjab (INDIA) -144411

ABSTRACT
Digital watermarking is the process of conveying information by imperceptibly embedding it into the digital media. Benchmarking is used to evaluate the watermarking algorithms. Different benchmarks are available for digital watermarking. These benchmarks work efficiently but they are complex, difficult to understand, so a new benchmark is introduced in his paper which is GUI (Graphical user interface) based and implemented in MATLAB. It also includes brief introduction to digital watermarking, and DCT based watermarking.

Keywords
Digital Watermarking, Discrete cosine transform and Benchmarking

1. INTRODUCTION
The development of the internet using digital media such as digital images, audio or video have made the life much simpler but to protect the material we are using different methods or techniques. Out of different techniques or methods present, digital watermarking is one of them. Digital Watermarking is a branch of information hiding technique used to hide the information in a host or message signal. Many different algorithms are made for digital images, audio and video. Benchmarks are used evaluate the performance of watermarking algorithms. Benchmarking is plays a vital role in digital watermarking. Different benchmarks exist such as Stirmark, Checkmark, Optimark, Openmark, Matmark etc. In this paper we are going to check a DCT based watermarking algorithm using a benchmark model which is Graphical user interface (GUI), designed for image watermarking algorithms. The general requirements for digital watermarking are: Robustness, transparency and Capacity/data payload.

2. DIGITAL WATERMARKING
A digital watermark carries a message containing information about the creator or distributor of the image, or even about the image itself [1]. The idea of robust watermarking of images is to embed information data within the image with an insensible form for human visual system but in a way that protects from attacks such as common image processing operations. The goal is to produce an image that looks exactly the same to a human eye but still allows its positive identification in comparison with the owner's key if necessary. Requirements of watermarking:

- Robustness: It is an important requirement of the digital watermarking. A watermarking algorithm is called robust if the watermark should be able to survive accidental or malicious attempts of removal and common image processing tasks [2]. If the watermark data is placed in significant coefficients of an image then the robustness against image distortion is better achieved.
- Capacity: Capacity is the amount of information an image can store. The amount of information that can be embedded in a watermarked image is called data payload. The data payload in image watermarking means the number of bits encoded with the image. There is should be balance between robustness and capacity.
- Transparency: There should be perceptual similarity between the watermarked image and the original image. The watermark should be imperceptible, the quality of the original image should not be degraded after it is watermarked. The watermark should not degrade the quality of the content [3].

3. WATERMARKING TECHNIQUES
Watermarking techniques [4], [5] can be divided based on processing-domain are:

- Spatial domain: In this technique the watermark data is embedded in the pixel value. Using these approaches there will be minor changes in the pixel intensity. The former techniques embed the watermark in the least significant bits of image pixels. The first watermarking scheme that was introduced works directly in the spatial domain. It is possible to get perceptual information about the image by some image analysis operations, which is then used to embed a watermarking key, directly in the intensity values of predetermined regions of the image. Those techniques provide an effective way for embedding an invisible watermark into an original image but they are not immune to common image attacks.
- Transform domain: Adding of watermark is done in transform domain, to achieve the imperceptibility as well as robustness. In this method, transform coefficients are modified for embedding the watermark. Transform domain is also called frequency domain because values of frequency can be altered from their original. The most important techniques in transform domain are Discrete cosine transform (DCT) and Discrete Wavelet Transform (DWT) [6]. The direct understanding of the content of the image is allowed by the use of frequency domain. Therefore, characteristics of the human visual system (HVS) can be taken into account more easily when it is time to decide the intensity and position of the watermarks to be applied to a given image. In this benchmark we are testing a watermarking algorithm which is DCT based [1].

4. DCT BASED WATERMARKING

In this we are implementing the watermarking on the images using the frequency domain technique that is DCT (Discrete Cosine Transform). DCT is a popular and most commonly used transform domain watermarking technique. It transforms a signal from spatial domain to frequency domain. Due to good performance, it has been used in JPEG standard for image compression. DCT has been applied in many fields such as data compression, pattern recognition, and image processing [7].

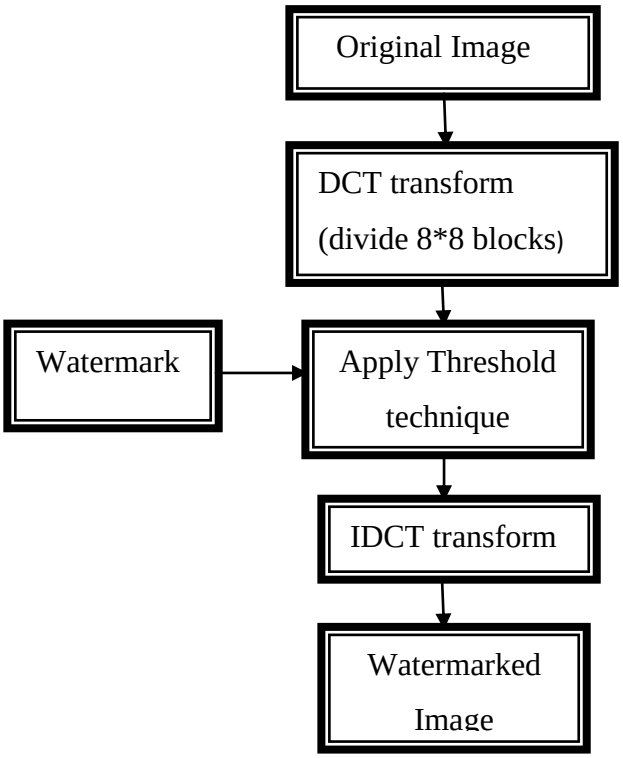

Fig 1: Flow Chart of Watermark Embedding

DCT block- based watermarking algorithm [8], [9] is given below:

Step 1: Segment the image into non-overlapping blocks of 8x8. In DCT the image is taken in a block dimension of 8*8 resulting in DCT blocks of dimension 8*8.

Step 2: Apply forward DCT to each of these blocks, the middle frequency band and is chosen for embedding information

.Step 3: The locations DCT (u, v) is chosen from the middle band for comparison of each 8 x 8 block, if DCT (u, v) equal to 'k', it will encode "1" otherwise "0".

Step 4: Now apply inverse DCT transform on each block.

While extracting the watermark, again the 8x8 DCT of image in taken in which "1" is decoded if DCT (u, v) = > k otherwise a "0" is decoded.

5. NEW BENCHMARK MODEL

Performance evaluation through the use of benchmarking frameworks has achieved more and more importance to speed up the research in the field of digital watermarking and stimulate a continuous improvement of the existing techniques by identifying the weaknesses and failings of different methods. Implementation of benchmark for image watermarking is done using the software MATLAB (GUI), Graphical User Interface.

As Stirmark does not know about the watermark embedding process of watermarked image because every user has his/her watermarking algorithms[10], Stirmark is limited to detecting a watermark at large scale, Checkmark lacks in ambiguity attacks, due to these reasons we are implementing a new benchmark (RK benchmark) for image watermarking. It uses the MATLAB programming. It is (a) Graphical user interface (b) consist of set of attacks such as simple attacks, detection-disabling attacks, removal attacks and ambiguity attacks, although it does not cover all of its types (c) one can apply the number of attacks on watermarked images automatically or manually (d) analysis based on quality measure parameters using a watermarking algorithm for different images (e) less evaluation time.

Layout design of RK benchmark is shown in Figure.2 This benchmark can be operated manually by using various buttons for each step and automatically by using one button named "All Results". Figure.3 and Figure.4 are operated manually by using Speckle noise on watermarked image, similarly it can be operated for other attacks also. Figure.3 consist of original cameraman image, watermarked image, embedded and extracted watermark analyzing watermarking algorithm without attacks and also showing their PSNR (Peak to signal noise ratio) and NC (Non-correlation) values. In Figure.4 watermarked images is shown with Speckle noise with variance, the variance values can be varied using the popup-menu button.

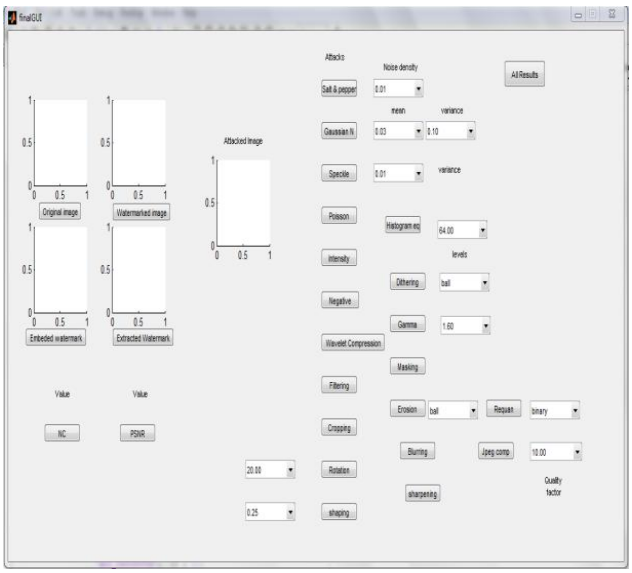

Fig 2: Layout design of GUI based RK benchmark

Now operating automatically four different images are watermark embedded/extraction and attacked images. The comparative analysis results of four different images are shown by different plots, as well as each attack image is stored in user specified path. Figure.5 shows Lena Image with speckle noise having 10 different values of variance and

PSNR values. Extracted watermark from the attacked images, NC values is shown in Figure.6. All extracted watermarks are not visible this means the watermarking algorithm is not efficient. Similarly results can be shown for rest of the three images.

Analysis of four watermarking images using plot is shown in Figure.7. Four host images are selected, they are gray-scale pictures of size 256 x256 .The images are identified by their names Baboon/Mandrill, Cameraman, Lena and Pepper. Baboon/Mandrill represents images with large areas of complex texture and includes homogeneous areas, Cameraman is chosen for its flat and high contrast regions, Lena has a mixture of characteristics (e.g. smooth background, big carves and the hat in the image includes complex textures) and Pepper provides luminosity changed (that is light reflection surfaces). By applying Speckle noise on four watermarked images the value of PSNR for each image varies and is shown in Figure.7. The acceptable limit of PSNR is 30 to 50 dB. Lena image have PSNR value between 74dB to 55 dB which is average value than the rest of the three images. As Lena image have mixture of characteristics showing high PSNR than other images.

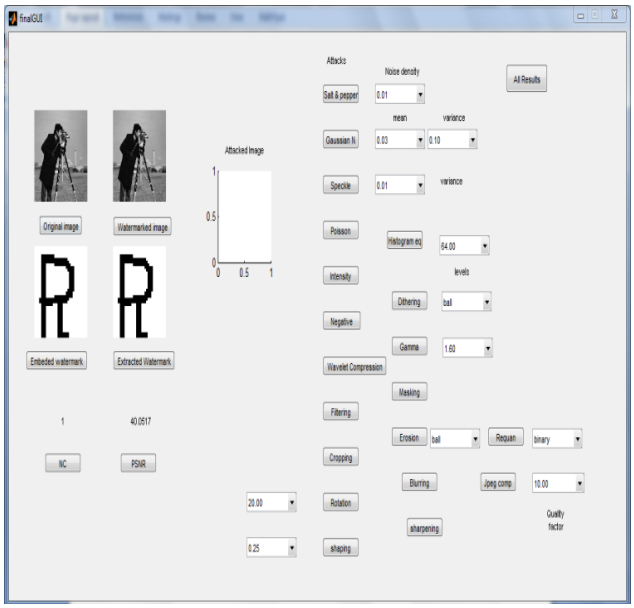

Fig 3: Layout consists of Original image, watermarked image, embedded watermark and extracted watermark with NC and PSNR

While the Cameraman and Pepper images have approximately similar values of PSNR. Mandrill Image showing least value of PSNR is heavily textured image. In Figure.8, NC of extracted watermark from the four attacked images. Non-correlation (NC) values limits are between 0 and 1.The value 0 showing no watermark extracted and value 1 showing the complete extraction of watermark. Different values of variance showing the effect on the extraction of watermark which ranges from 0.96 to 0.5. The value closer to 1 is showing better extraction of the watermark. In Figure.8 the Cameraman image is showing better results of extracted watermark than the other images. Watermarked image will be dilating using different structuring elements such as disk, line, square, diamond, and rectangle. Pepper image be dilate as shown in Figure.9 and extracted watermark are shown in Figure.10.Graphs of PSNR and NC are shown in Figure.11 and Figure.12

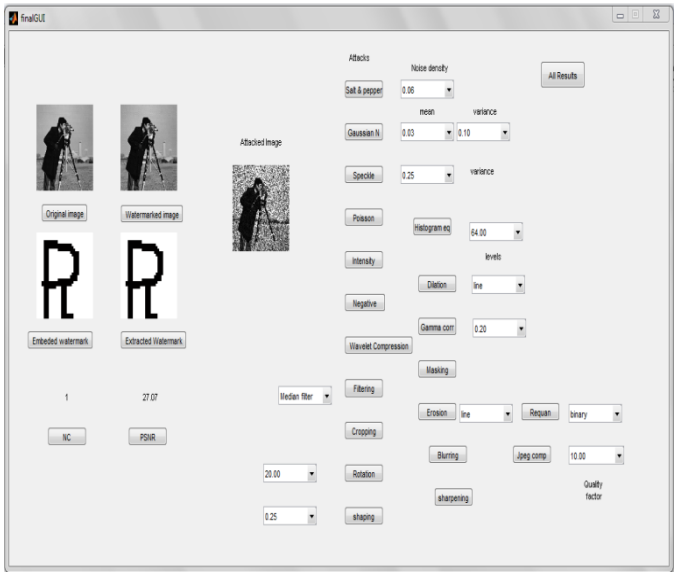

Fig 4: Attacked Image (Speckle Noise)

In Figure.12, NC varies from 0.86 to 0.54. Lena image has less NC values than the other images while Cameraman image has high values of NC. Dilation using the line structuring elements gives the high NC which show better results of the extracted watermark from the images. Dilation using rectangle structuring elements gives the lowest NC of the extracted images. This means that dilation using rectangle effects the images more. Similarly results can also be seen for other attacks such as Gaussian Noise, Speckle noise, Erosion, Rotation, Scaling, Histogram equalization etc.

6. CONCLUSION

Watermarking algorithms are developing day by day, so the need of benchmarking is also increasing. Benchmarking tools are also an important part of the digital watermarking. This GUI based benchmark is easy to use and helps to evaluate the watermarking algorithm. In this benchmark, further more number of attacks can be added for better analysis of image watermarking algorithm and to make it compatible for audio and video watermarking. Also evaluation time can be decrease.

TABLE 1: COMPARISON OF BENCHMARKING TOOLS [11]

Tools	Language	Cover	Simple Attacks	Detection-disabling Attacks	Ambiguity Attacks	Removal Attacks
Stirmark	C/C++	Image	Yes	Yes		Yes
Checkmark	Matlab	Image	Yes	Yes		Yes
Optimark	C/C++	Image	Yes	Yes	Yes	
Mesh Benchmark	C/C++	Image	Yes	Yes		
RK Benchmark	Matlab	Image	Yes	Yes	Yes	Yes

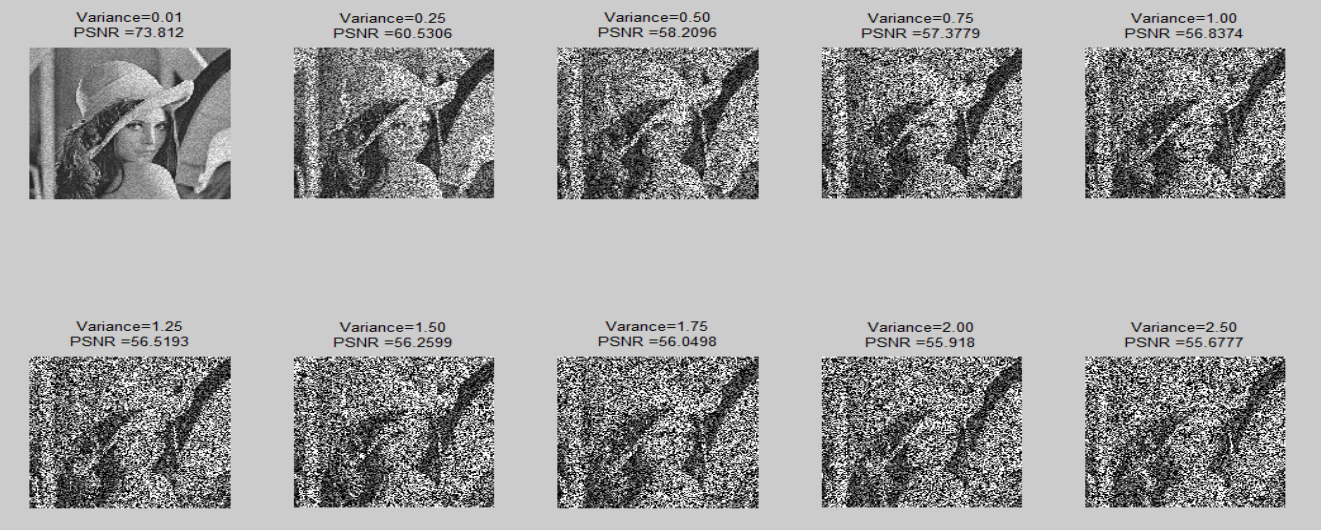

Fig 5: Attacked image (Speckle noise with different values of variance and PSNR)

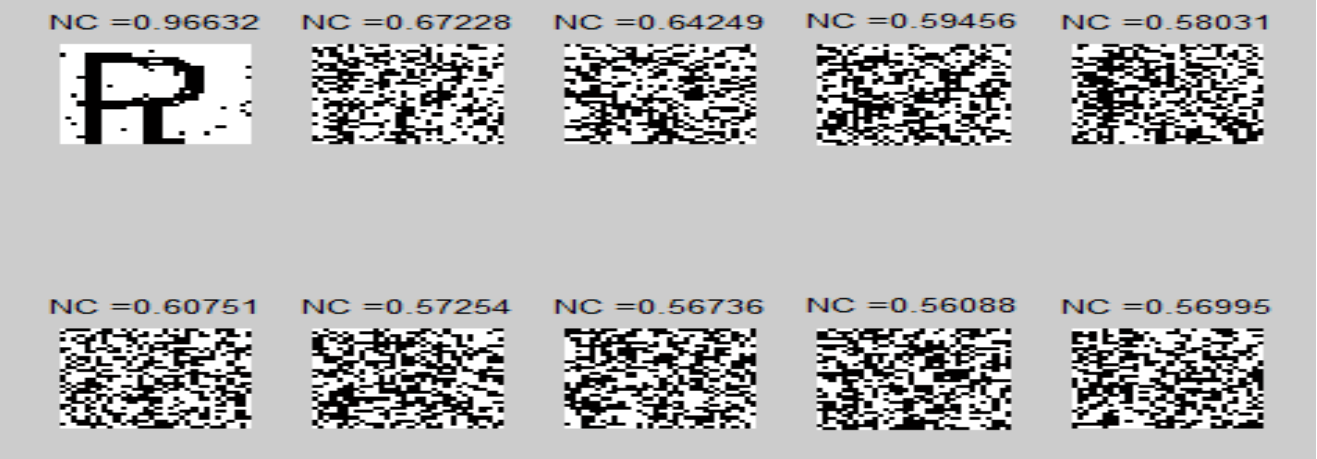

Fig 6: Extracted watermark from the attacked image and NC

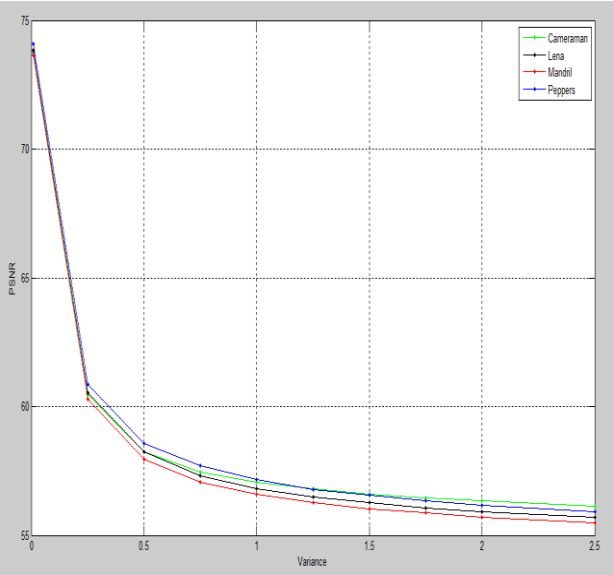

Fig 7: PSNR values of attacked watermark images the (Speckle noise with different variance)

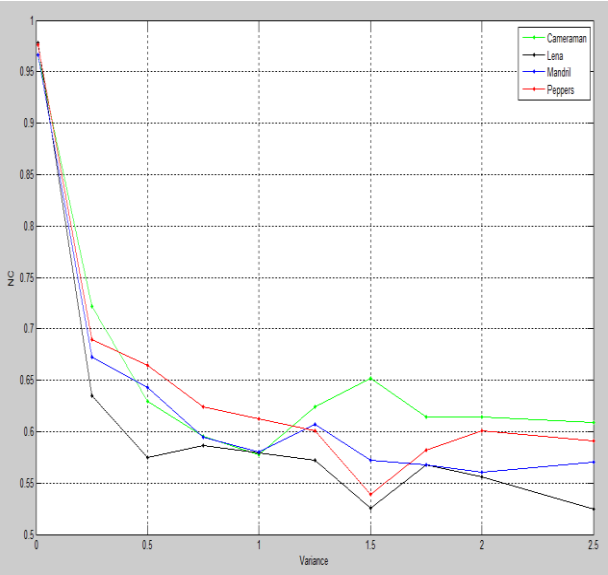

Fig 8: NC vs. Noise density of four extracted watermarks from attack images

Fig 9: Dilation on Pepper image using different structuring elements (disk, square, diamond, line, rectangle)

Fig 10: NC of extracted watermarks from attack images

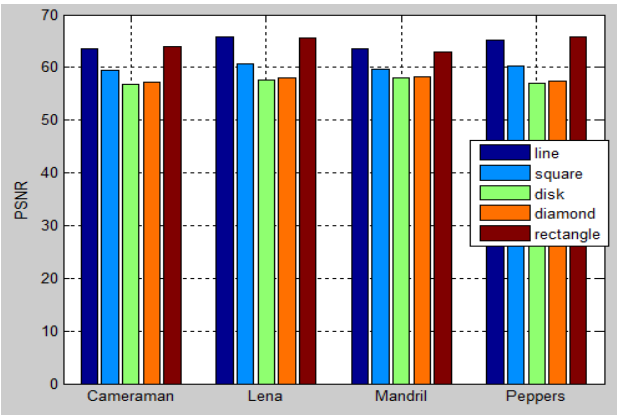

Fig 11: Four watermarked images (Dilation) PSNR

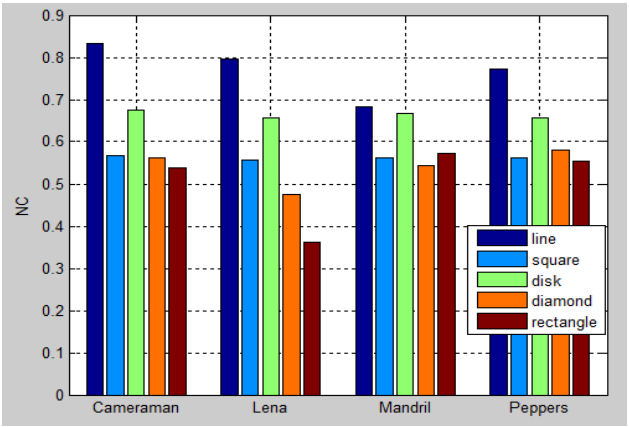

Fig 12: NC of extracted watermarks from four attacked images

7. REFERENCES

[1] Vallabha VH, "Multiresolution watermark based on wavelet transform for digital images".

[2] Jian Liu and Xiangjian He "A review study on digital watermarking", 2005 IEEE.

[3] Mitra Abbasfard "Digital image watermarking robustness: a comparative study", 2009.

[4] Vidyasagar M. Potdar, Song Han, Elizabeth Chang, "A survey of digital image watermarking techniques", 3rd International Conference on Industrial Informatics ©2005 IEEE.

[5] J.Samuel Manoharan, Dr.Kezi C.Vijila, A.Sathesh "Performance analysis of spatial and frequency domain multiple data embedding techniques towards Geometric attacks", International Journal of Security (IJS), Volume (4) : Issue (3)

[6] Ali Al-Haj, "Combined DWT-DCT digital image watermarking", Journal of Computer Science 3 (9): 740-746, 2007 ISSN 1549-3636 © 2007 Science Publications

[7]] Edin Muharemagic and Borko Furht, "Survey of watermarking techniques and applications"

[8] Baisa L. Gunjal, R.R. Manthalkar "An overview of transform domain robust digital image watermarking algorithms", Volume 2 No. 1 ©2010-11 CIS Journal.

[9] Mona M. El-Ghoneimy "comparison between two watermarking algorithms using DCT coefficient and LSB replacement", Journal of Theoretical and Applied Information Technology ©2005 - 2008 JATIT.

[10] S. Voloshynovskiy, S. Pereira, T. Pun, J.J. Eggers and J.K. Su "Attacks on digital watermarks: classification, estimation-based attacks and benchmarks", IEEE Communications Magazine, August 2001.

[11] Thi Hoang Ngan Le, Kim Hung Nguyen, Hoai Bac Le "Literature survey on image watermarking tools, watermark attacks, and benchmarking tools" 2010 Second International Conferences on Advances in Multimedia.