EFFICIENT WATERMARKING SCHEME IN SPATIAL DOMAIN BY USING SECOND LSB

Bilal Ahmed[1], Saleem Mian[2]

[1]Dept. Electrical Engineering, University of Engineering & Technology, Lahore, Pakistan.
[2]Faculty of Electrical Engineering, The University of Lahore, Lahore, Pakistan.
CONTACT: :bilalrouf@yahoo.com

ABSTRACT: *Due to diversified advancements in the field of information technology, digital data has become much important and popular in digital media. Postal mail is replaced with electronic mail, called email. digital signature become the symbol of security for digital data. So it become necessary to protect digital content. Against any illegal claim, It is an author's responsibility to provide the necessary proof that a particular content belongs to him. Watermarking of digital images is one of the techniques to provide such type of proof and protect data. In this technique, secret image, logo or information is embedded into host image which can be extracted later for identification purpose. Number of watermarking insertion techniques are proposed in spatial domain and frequency domain. In this paper a watermarking scheme in spatial domain using second least significant bit is proposed. Imperceptibility and robustness of proposed scheme is checked against different type of attacks. Results are compared with famous watermarking technique in frequency domain.*

Keywords-Digital Watermarking, Least Significant Bit LSB, DCT,Frequency domain watermarking, robustness.

1. INTRODUCTION

With the diversified development in the field of information technology, it became easy for everyone to access digital media like digital images ,text, soft wares and entertainment stuff. Due to easy access of digital data, illegal distribution of digital content also diversely increased. It is necessary to protect unauthorized distribution. For this purpose Digital Right Management (DRM) systems are invented. DRM systems help us to identify the ownership and authenticate the digital content [1]. Digital data like documents, text and images are encrypted to make them unavailable for unauthorized person without authentication or decryption key. Digital watermarking is technique to protect digital images. In this technique secret information, logo or trademark is inserted into host image (image which is being protected) which can later be extracted for identification or authentication purpose.

Watermarking can be classified as: the mode of insertion/encryption and the domain of insertion/ encryption [2]. According to the mode of encryption, there are two modes for insertion or encryption: first "additive mode" and other one is “substitutive mode". In additive mode, watermark, logo or digital signature is being added to host image components. whereas in substitutive mode, host image components are replaced with that of watermark, logo or digital signature. Both mods of encryption have their own advantages and disadvantages. According to second criterion of watermarking classification, watermarking is classified as: spatial domain watermarking and frequency domain watermarking [3]. Encryption in spatial domain is done by some direct operation on pixels of host image [4]. While in frequency domain, encryption is done by some process on frequency coefficients of host image [5]. Watermark bits (in case of spatial domain) or frequency coefficients should be shuffled within the host image randomly in a manner that they can't be manipulated and identified. Two main features, robustness and imperceptibility, defines the quality of watermarking algorithm or technique. Imperceptibility defines the visual strength of watermarked image. Robustness is a measure of strength of watermark against different attacks applied to watermarked image (host image after watermark embedded).

In Section 1 some concepts related to spatial domain watermarking and Discrete Cosine Transform (DCT) watermarking are discussed. In Section 2, algorithms of proposed watermarking scheme is presented. Some parameters to measure the performance and efficiency are discussed then. Experimental results are presented in section 3. Finally conclusion are given in section 4.

A. Spatial Domain

In this method of watermarking, embedding of watermark is done by direct insertion of pixels of watermark image into that of host image.

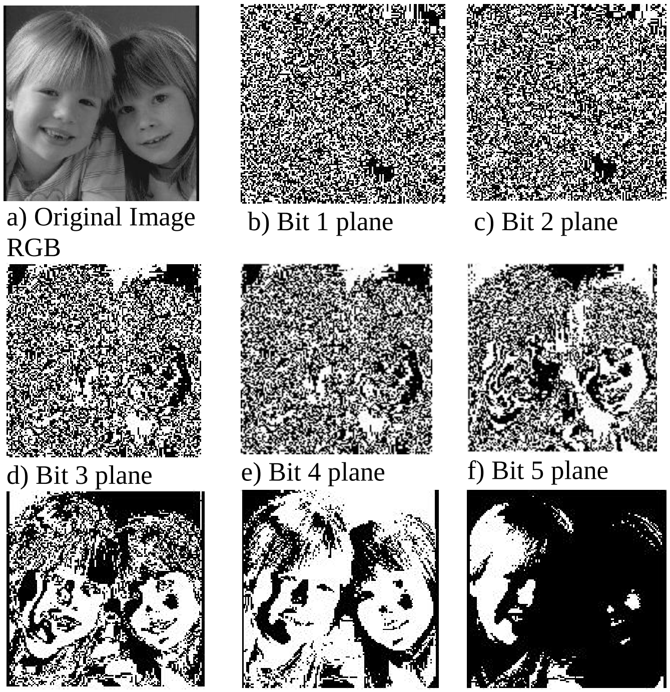
The main advantage of the spatial domain data embedding techniques over frequency domain data embedding is it's less complexity of calculation [2]. When image is divided into 8-bit planes, most of the visual information of image is present in most significant bits as shown in fig 1. Simplest form of spatial domain watermarking is to process "Least Significant Bit (LSB) [6] and watermark bits are embedded into LSB of host image.

B. Discrete Cosine Transform (DCT)

DCT converts pixels of an image or waveforms or sound , into different sets of frequencies. Lower spatial frequency components are more useful than the higher spatial frequency components [13]. To compress data, the least meaningful frequency components are stripped away within the safe limit of resolution loss. In the DCT coefficient matrix, high frequency components lies at left upper part of matrix and those with low frequency component lies right most bottom of the matrix. To embed invisible watermark, low frequency components are not modified because in doing so invisibility of watermark is lost. In the applications of DCT, lossy image compression is very important and famous. Some other frequency transforms are also used in watermarking like Discrete Wavelet transform (DWT), Haar Transform (HT) and Discrete Fourier Transform (DFT). DCT is almost the same as DFT. The only difference between these transform are, DCT involves with real numbers only.

In DCT watermarking , host image is divided into sub blocks of size M*N. where M and N are the no. of rows and columns of sub block matrix respectively. Watermark is inserted by using these blocks [7]. The Inverse Discrete Cosine Transform is used to extract the hided secret information or watermark. Digital Wavelet Transform (DWT) is also important frequency domain transform to embed watermark. Matlab built in functions are available to compute 1-D and 2-D DCT and DWT[3][8-10].

Figure 1. Image and its 8 bit planes



a) Original Image RGB b) Bit 1 plane c) Bit 2 plane

d) Bit 3 plane e) Bit 4 plane f) Bit 5 plane

g) Bit 6 plane h) Bit 7 plane i) Bit 8 plane

2. THE PROPOSED DIGITAL WATERMARKING SCHEMES

In spatial domain watermarking, most of the algorithms involve with modification of LSB. As shown in figure 1, most of the visual information is present at higher significant bits especially 5th,6th,7th and 8th bit planes. Modification in LSB do not have bad imperceptibility effect on watermarked image. In our proposed scheme of embedding watermark, we will embed watermark in 2nd & 3rd last significant bits instead of LSB.

C. Watermark Embedding & Extraction Algorithm In Spatial Domain

- Following algorithm steps are used to embed and recover watermark. We used host and watermark images with size 512x512 and 50x20 respectively.
- Read the host and watermark images.
- If watermark is of small size tiled it to fit the size of host image.
- Divide the host image into 8-bit planes.
- Insert watermark pixels into 2nd LSB plane of host image.
- To recover watermark, read watermarked image.
- Divide watermarked image into 8-bit planes and recollect the pixels from 2nd LSB plane.
- Flow chart for proposed scheme is shown in figure 2.

D. Watermark Embedding algorithm in DCT Domain.

- Read watermark and host images. We used host and watermark images with size 512x512 and 64x64 respectively.
- Convert colored host image into gray scale image.
- Calculate DCT of watermark image.
- Divide host image into sub blocks of size 8x8.
- Calculate DCT of each sub block.
- Get one DCT coefficient from sub block having middle frequency of host image then replace it with that of watermark image.
- Calculate inverse DCT of modified matrix to convert frequency coefficient matrix into image.
- Flow chart for DCT WM is shown in figure 3.

E. Watermark Extraction in DCT Domain

- Divide watermarked image into sub blocks of size 8x8.
- Compute DCT for each sub-block and extract relevant coefficient from the position where it was placed.
- Store these elements in a vector or single row array.in our case 1x2056 matrix.
- Arrange elements in this vector in matrix form of size 64x64.
- Calculate Inverse DCT of matrix obtain in previous step to convert frequency coefficient matrix into watermark image.

F. Performance Measurements

There are different parameters used to determine the quality of algorithm. In this paper we used three measures those are

- Normalized Cross Correlation (NCC).
- Peak Signal to Noise Ratio (PSNR).

1) Peak Signal To Noise Ratio(PSNR)

PSNR defines the imperceptibility strength to measure the visual effect between the host image and the watermarked image [11]. Formula for PSNR calculation is given by

$$PSNR_{dB} = 10\log_{10}\left[\frac{X^2}{\sum_{u=1}^{M}\sum_{v=1}^{N}\left[R(u,v)-\bar{R}(u,v)\right]^2}\right]$$

For u =1,2,3..M and v=1,2,3...N

X = Maximum variation in input image data type

R = Original image matrix.

R’ = Watermarked image matrix

u and v represent the rows and columns of host image respectively.

2) *Normalized cross correlation (NCC)*

The NCC is used to indicate the similarity between two signals. In this case, it can be used to find the similarity between extracted watermark and original watermark. The NCC value defines the robustness of watermark extracted[11]. It is calculated by using the formula.

$$NCC = \left[\frac{\sum_{y=1}^{M}\sum_{z=1}^{N}\left[R(y,z)\,\bar{R}(y,z) \right]}{\sum_{y=1}^{M}\sum_{z=1}^{N}\left[R(y,z) \right]^{2}} \right]$$

Where

R' = Extracted watermark image matrix.

R = original watermark image matrix.

M = Number of rows, N = Number of columns

y and z represent the rows and columns of image matrix respectively.

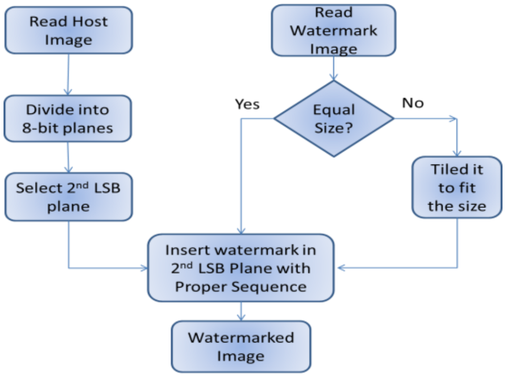


Figure 2. Flow chart of proposed watermarking scheme

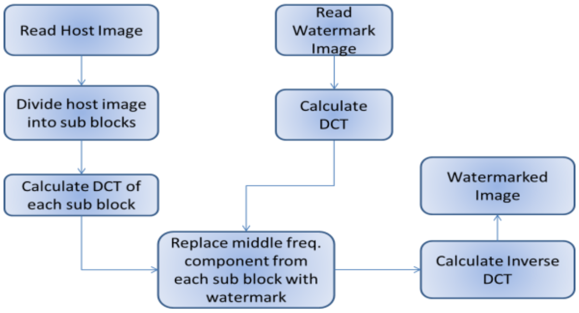
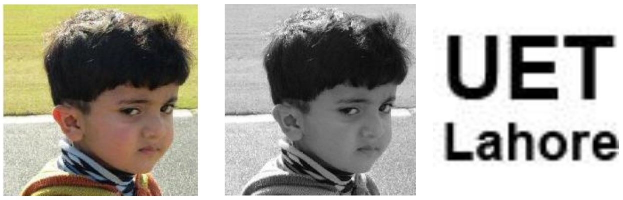

Read Host Image
Divide host image into sub blocks
Calculate DCT of each sub block
Read Watermark Image
Calculate DCT
Replace middle freq. component from each sub block with watermark
Calculate Inverse DCT
Watermarked Image

Figure 3. Flow chart of DCT watermarking scheme

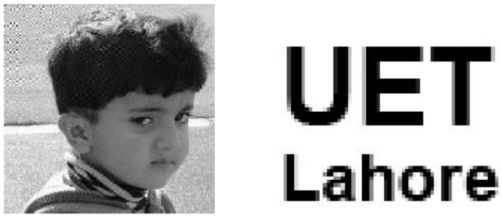
3.Experimental Results

Two watermarking schemes are simulated one our proposed scheme and other DCT watermarking proposed by gonzalez [14]. To measure the performance of proposed method, robustness and imperceptibility is measured against different attacks. More over results are further compared with two other watermarking schemes i-e FHT watermarking [15] and partial multi-map encryption [1].



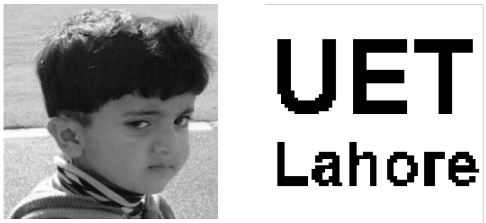
a) Host Image RGB b) Host Image Gray-scale c) Watermark

Figure 4. Host Image colored , Gray scale image and Watermark Image



PSNR= 19.13 db NCC = 1.00

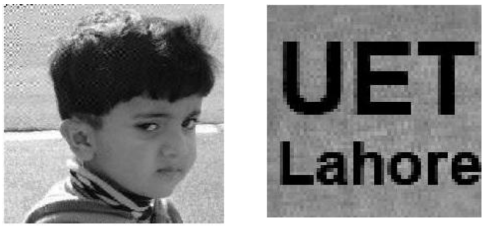
Figure 5. DCT WM image without any attack with PSNR=19.13 and extracted watermark with NCC=1.00



PSNR= 45.10 db NCC = 0.5213

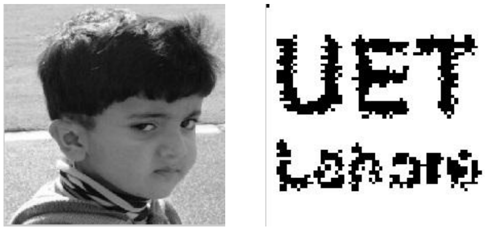
Figure 6. Proposed watermarked image without any attack with PSNR=45.10 and extracted watermark with NCC=0.5213

G. *Median Filter Attack*



PSNR = 22.49 dB NCC = 0.544

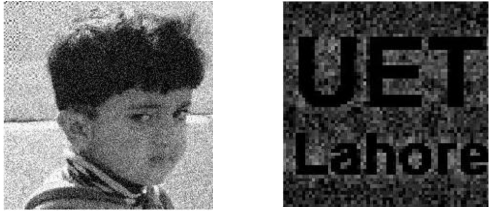
Figure 7. DCT domain watermarked image when median filter is applied as an attack and extracted watermark.



PSNR = 31.0 dB NCC = 0.51

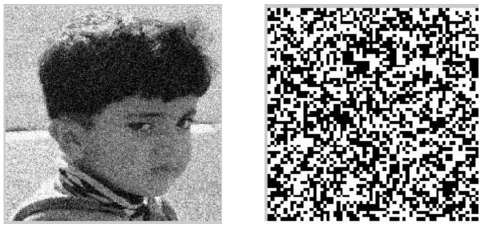
Figure 8. Proposed scheme watermarked image when median filter is applied as an attack and extracted watermark.

H. *Addition of Gaussian Noise*



PSNR = 19.6 d**B** NCC = 0.19

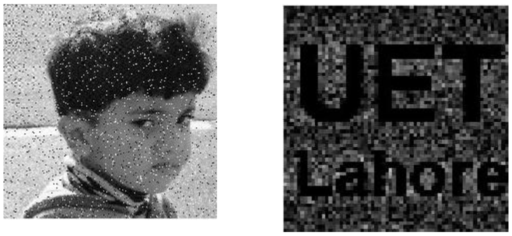
Figure 9. DCT domain watermarked image when gaussian noise is added as an attack and extracted watermark.



PSNR = 20.376 dB NCC = 0.311

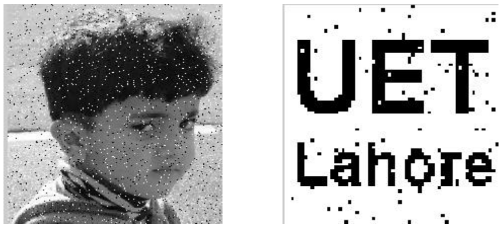
Figure 10. Proposed schem watermarked image when Gaussian noise is added as an attack and extracted watermark

I. *Addition of Salt & Pepper Noise*



PSNR = 17.6 d**B** NCC = 0.29

Figure 11. DCT domain watermarked image when Salt & Pepper Noise is added as an attack and extracted watermark.



PSNR = 17.828 dB NCC = 0.036

Figure 12. Proposed schem watermarked image when Salt & Pepper noise is added as an attack and extracted watermark.

Some other filtering ,compression and rotation attacks are applied on both 2nd LSB and DCT watermarking schemes. Results are summerized in table. Blank boxes indicate that these attacks were not used by relavent authos.

Table 1. PSNR table for 2nd LSB, DCT, FHT and PMME agaisnt different attacks.

	Second LSB	DCT	PMME	FHT
without attack	45.1073	19.15	11.49	20.12
Low Pass Filter	29.29	21.677	-	23.075
Median Filter	31.72	22.49	-	20.81
High Pass Filter	21.77	10.12	-	11.156
Gaussian Noise	20.81	19.6	17.1	18.482
Salt & Pepper Noise	17.784	17.34	11.66	17.206
rotation 10 degree	11.35	11.3	11.94	-
rotation 20 degree	9.277	9.213	11.35	-
jpeg 10 %	40.106	26.83	12.21	-
jpeg 25 %	36.01	26.58	12	-

Table 2. NCC table for 2nd LSB, DCT, FHT and PMME agaisnt different attacks.

	Second LSB	DCT	FHT	PMME
Low Pass Filter	0.311	0.62	0.559	-
Median Filter	0.51	0.544	0.815	-
Gaussian Noise	0.311	0.19	0.436	1
Salt & Pepper Noise	0.51	0.203	0.43	1
High Pass Filter	0.3026	0.203	0.99	-
rotation 10 degree	0.1651	0.001	-	1
rotation 20 degree	0.0231	0.00189	-	1
compression 10%	0.3415	0.21	-	0.92
compression 25%	0.3071	0.2098	-	1
without attack	0.5213	1	-	1

J. *Graphical representation of comparison with various schemes*

Now results of proposed watermarking schemes are compared graphically with DCT, FHT and PMME.

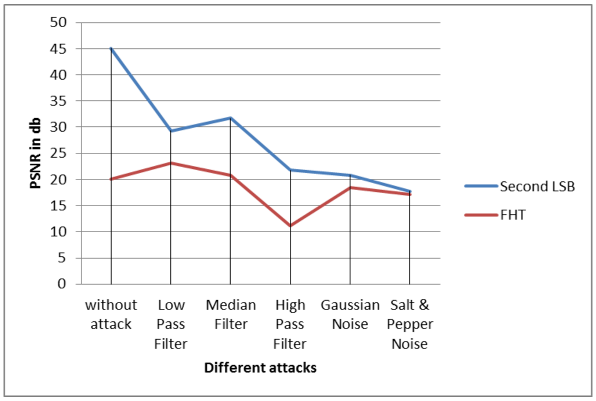


Figure 13. PSNR comparison with FHT

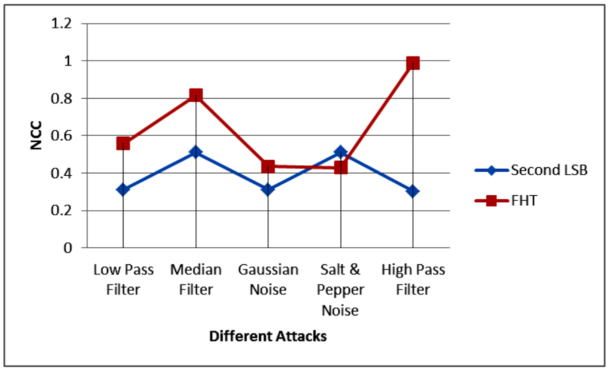


Figure 14. NCC comparison with FHT

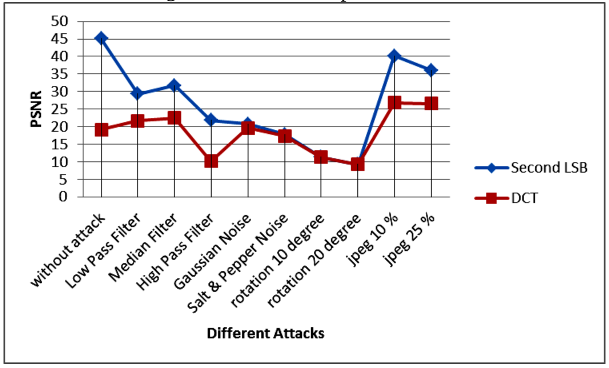


Figure 15. PSNR comparison with DCT

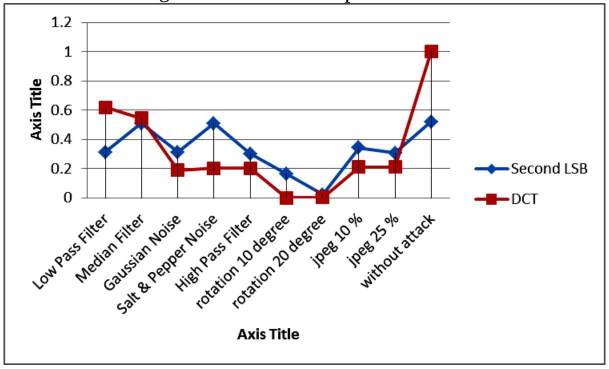


Figure 16. NCC comparison with DCT

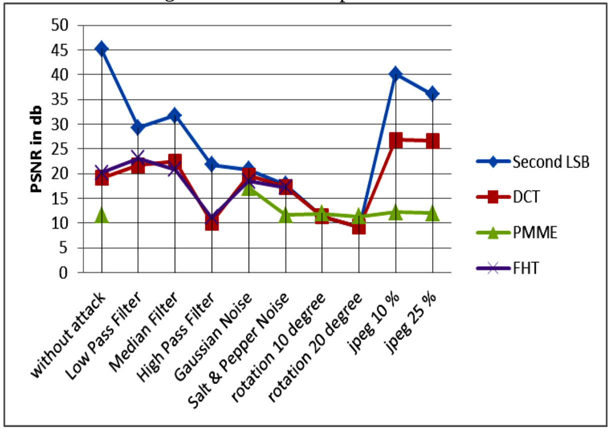


Figure 17. PSNR comparison of 2nd LSB with DCT, FHT and PMME

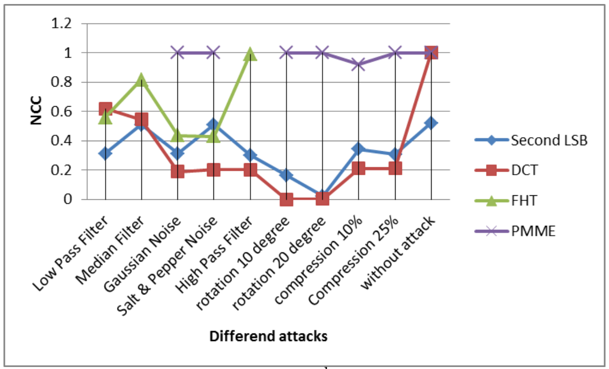


Figure 18. NCC comparison of 2nd LSB with DCT, FHT and PMME

4.CONCLUSION

Watermarking scheme for spatial domain is proposed in which 2nd last lsb plane is used to embed watermark instead of lsb plane.experimental results and comparison with dct , fht, pmme shows that imperceptibility of proposed scheme is much better than all mentioned watermarking schemes.proposed scheme is not as much robust against all the attacks as other schemes are. Less robustness of proposed scheme is not surprising and can be justified as. Attacks used in this these are not frequent in practical watermarking applications like passport ,id cards etc. but imperceptibility is major issue in such type of applications. more over, it is easy to handle images practically in spatial domain as compared to frequency domain. proposed idea can further be used for practical implementation of real time simulations like video processing but mortal has to bear tradeoff between imperceptibility and robustness.

REFERENCES

1. White paper, “Digital Watermarking: A Technology Overview.” Wipro Technologies, USA, 2001.
2. Houtan Haddad Larijani, Gholamali Rezai Rad. “Proceedings of the International Conference on Computer and Communication Engineering”13-15 may, 2008 Kuala Lumpur, Malaysia.
3. Neeraj Bhargava, M.M Sharma, A.S. Garhwal, M. Mathuria. “Digital Image Authentication System Based on Digital Watermarking” 2012 International Conference on Radar, Communication and Computing (ICRCC), pp.185-189, 21-22 December, 2012.
4. P. S. Huang, C. S. Chiang, C. P. Chang, and T. M. Tu, "Robust spatial watermarking technique for colour images via direct saturation adjustment," Vision, Image and Signal Processing, IEEE Proceedings, vol. 152, pp.561-574, 2005.
5. M. Kallel, I. F. Kallel, M. S. Bouhlel, "Medical Image watermarking Scheme for Preserving the Image history", Proceedings of ICTTA'06, 2006.
6. A. Z. Tirkel, G. Rankin, R. Schyndel and G. F. Osborne, "Electronic Watermark", DICTA, pp. 666-672, USA(TX), 1993
7. F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information Hiding- A survey," Proceedings of the IEEE, Special Issue on Protection of Multimedia Contents, vol. 87, no. 7, July 1999, pp. 1062 -1078.

8. Mohammad Nuruzzaman, “Digital Image Fundamentals in MATLAB”, Book, ISBN 1-4208-6965-5 (sc), 2005.
9. P. B. Khatkale, K. P. Jadhav and M.V. Khasne, “Digital Watermarking Technique for Authentication of Color Image”, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, vol. 2, Issue 7, July 2012
10. Lora G. Weiss, “Wavelet and Wideband Correlation Processing”, IEEE Signal Processing Magazine, January, 1994, pp. 13-32
11. William K.pratt,digital image processing,fourth edition,wiley-interscience,John wiley and sons,inc.,California,2007.
12. M. Ali Qureshi, “Comparative Analysis and Implementation of Efficient Digital Image Watermarking Schemes”, International Journal of Computer and Electrical Engineering, ISSN1793-8163, vol. 4, Issue 4, August 2012.
13. http://www.cs.sfu.ca/CourseCentral/365/mark/material/notes/Chap4/Chap4.2/Chap4.2.html
14. R.C. Gonzalez, R.E. Woods, “Digital Image Processing”, Upper Saddle River, New Jersey, Prentice Hall, Inc., 2002.
15. M. Ali Qureshi, “Comparative Analysis and Implementation of Efficient Digital Image Watermarking Schemes”, International Journal of Computer and Electrical Engineering, ISSN1793-8163, vol. 4, Issue 4, August 2012.
16. El-Mahallawy, “Robust Blind and Secure Biometric watermarking based on partial multi-map chaotic encryption, 4th IFIP inter. Conference, 2011.