INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Hybrid Watermarking Technique for Data Hiding in RGB Images

Mansi[1], Navneet Verma[2]

[1]M.tech Scholar, [2]Asst. Prof. CSE Dept
Geeta Engineering College, Naultha, Panipat
Haryana (India)

Abstract: *Digital watermarking is nothing but the technology in which there is embedding of various information in digital content which we have to protect from illegal copying. This embedded information to protect the data is embedded as watermark. In digital watermarking, a watermark is embedded into a cover image in such a way that the resulting watermarked signal is robust to certain distortion caused by either standard data processing in a friendly environment or malicious attacks in an unfriendly environment. Beyond the copyright protection, Digital watermarking is having some other applications as fingerprinting, owner identification etc. Digital watermarks are of different types as robust, fragile, visible and invisible. In this work, a comparative analysis of two most recent techniques used in digital image watermarking; they are DWT and hybrid DWT-SVD. Both these techniques are very much robust and imperceptible. In case of DWT, decomposition of the original image is done to embed the watermark and in case of hybrid DWT-SVD firstly image is decomposed according to DWT and then watermark is embedded in singular values obtained by applying SVD. Here, the techniques are compared on the basis of PSNR value at different values of scaling factor. For implementing the above digital image watermarking techniques, MATLAB R2013a is used.*

Keywords: *Data Hiding, Digital Watermarking, Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD).*

1. Introduction

Digital watermarking is that technology that provides and ensures security, data authentication and copyright protection to the digital media. Digital watermarking is the embedding of signal, secret information (i.e. Watermark) into the digital media such as image, audio and video. Later the embedded information is detected and extracted out to reveal the real owner/identity of the digital media. Watermarking is used for following reasons, Proof of Ownership Copying Prevention, Broadcast Monitoring, Authentication, and Data Hiding. Watermarking consists of two modules watermark embedding module and watermark detection and extraction module. Recently, the Internet becomes the most important media for information and data communication such as image, audio and video. However, some safety tools should be used to protect the transmission of critical data over the Internet.

Several algorithms have been proposed for watermarking, especially for image watermarking:

- In a robust blind digital image watermarking method based on singular value decomposition in wavelet domain to proof of ownership.
- In, a multi-watermarking scheme is proposed by embedding three independent binary watermarks in a grayscale digital image.

In a block based digital image watermarking algorithm is developed based on Singular Value Decomposition (SVD) mathematical technique. In, a multiple watermarking technique for e-commerce is introduced based on Discrete Wavelet Transform (DWT). Watermarking mechanisms are divided into two types: visible and invisible.

Watermarking techniques can be divided into three main groups:

• ***Spatial space watermarking:*** Watermarking in spatial space uses the spatial image space for embedding of hiding information.

• ***Frequency space watermarking:*** Frequency space watermarking uses the selected discrete orthogonal transforms (DCT, DWT) for embedding of the hiding information into the spectral coefficients or into the sequence coefficients, in generally.

• ***Parametric space watermarking:*** Parametric space watermarking includes algorithms, where a watermark is embedded into the image in its parametric space (typically in digital image watermarking techniques established on fractal image coding, where a watermark is inserted into the parameters of block's similarity or into the parameters of block's positions).

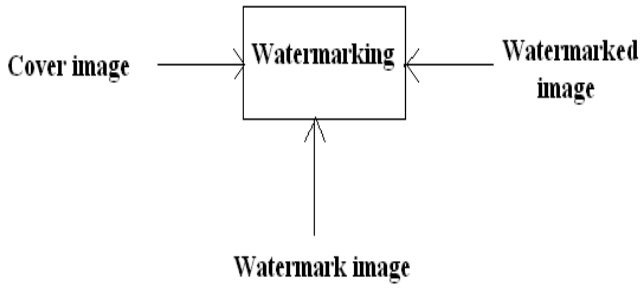

Figure 1: Block diagram of watermarking

2. Literature Review

Marek Candik et. al [1] discussed some basic principles of digital watermarking are presented. Presented methods use discrete orthogonal transforms for watermark embedding and watermark extracting too.

a) Algorithm for watermark embedding: A frequently case of watermarks are binary images, dimension of watermark is generally smaller than dimension of original image. Input parameters in process of watermark embedding are original image I, watermark W and user's key style of watermark permutation. First operation with the watermark is reordering

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

of its pixels by using pseudorandom permutation. The algorithm of watermark permutation must be pseudorandom because watermark must be reconstructed.

b) General algorithm for watermark extraction: Input parameters in process of watermark extraction are original image, watermarked image and user's key (algorithm of watermark permutation). For the original image we compute discrete orthogonal transformation; on the original image we compute discrete orthogonal transformation too. We compare used spectral coefficients in both images. Because watermarked image may be modified (noise corruption, attack of data, etc.), may be also changed coefficients, that weren't modified in process of watermark embedding..

Pei-Yu Lin et. al [2] The dual watermarking scheme employs the property of sub sampling to simultaneously embed dual watermarks into the perturbed block pairs of sub images without influencing each other. The reconstructed image possesses high fidelity approximating that of the original image, which can be widely applied for protecting valuable images.

a) Dual Watermarking Scheme: Although the visible and invisible watermarking mechanisms apply to different applications, they are used to protect the ownership of the multimedia from being attacked. Hence, the essential of copyright verifiability is the most significant challenge to design a watermarking scheme. To enhance the robustness of the invisible watermarking mechanism, color versions of one or more of the figures are used different combinational method that embeds distinct watermark parts into the host image. With two invisible watermarks, this scheme can resist the cropping attack.

Gamal Attiya et. al [3] A hybrid image watermarking technique was proposed and evaluated using several test images. In this proposed technique, two watermark images are first fused then the fused watermark is embedded using the DWT–SVD watermarking algorithm. Spatial domain has many disadvantages that do not allow for the exploitation of this subsequent processing in order to increase the robustness of the watermark. It is generally preferable to hide watermarking information in noisy regions and edges of image, rather than in smoother regions. Thus, working in transform domain becomes more attractive. Therefore many techniques are used for image watermarking such as, Discrete Wavelet Transform (DCT), Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD) and Least Significant bit (LSB). Prabhishek Singh et. al [4] surveyed various aspects for digital watermarking like overview, framework, techniques, applications, challenges and limitations. Apart from it a brief and comparative analysis of watermarking techniques is presented with their advantages and disadvantages which can help the new researchers in related areas.

DIGITAL WATERMARKING APPLICATIONS:

a) Copyright protection
b) Digital right management
c) Tamper proofing
d) Broadcast monitoring
e) Fingerprinting
f) Access control
g) Medical application
h) Image and content authentication
i) Annotation and privacy control
j) Media forensics
k) Content protection for audio and video content
l) Communication of ownership and objects
m) Document and Image security
n) Audience measurement

Namita Chandrakar et. al [5] Different techniques of digital image watermarking based on spatial and frequency domain techniques studied in this paper. According to our study it is clear that spatial domain is most widely used technique because the watermark can successfully & easily be recovered if the image has been cropped or translated, as compared to frequency domain. On the other hand frequency domain provides more security but at the same time recovery of watermark at the receiver end is more difficult because the complexity increases. Successful recovery of watermark cannot be provided by the frequency domain techniques. Amitav Mahapatra et. al [6] Robust watermarking schemes are applied for proving ownership claims whereas fragile watermarking is applied to multimedia content authentication. Robust watermarks should be able to survive a wide range of friendly operations and malicious attacks, whereas fragile watermarks are intolerable to both malicious and content preserving operations. Fragile watermarking techniques are designed with a goal to identify and report every possible tampered region in the watermarked digital media. Semi-fragile watermarks are intermediate in robustness between the two and are also used for image authentication. Some critical applications like medical imagining and forensic image archiving also requires the fragile watermarks to be reversible. Y. Shantikumar Singh et al [8] compared many watermarking algorithms are reviewed in the literatures which show advantages in systems using wavelet transforms with SVD.

(i) Singular Value Decomposition (SVD)

Singular Value Decomposition (SVD) is a numeric analysis of linear algebra which is used in many applications in image processing. It is used to decompose a matrix with a little truncate error according to the equation below:

$$A = USVT$$

Where A is the original matrix, U and V is orthogonal matrices with dimensions M x M and N x N respectively, S is a diagonal matrix of the Eigen values of A and T indicates matrix transposition. The decomposition of the cover image and added the watermark using a scale coefficient α to get the following equation:

$$S + \alpha W = UW\ SW\ VW\ T$$

Multiplying matrices U, VT and SW result in the marked image

AW: $$AW = USW\ VT$$

This technique improves watermark robustness and resistance against many kinds of attacks.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Nidhi Bisla et al [9] On comparing the values of PSNR at different values of scaling factor, it is concluded that the hybrid technique DWT-SVD is much better than DWT technique. As at every value of scaling factor, value of peak signal to noise ratio is more in case of the hybrid technique. Less the value of PSNR more will be the degradation in the quality of the original image. This shows that after watermarking, the quality of original image degrades more when DWT technique is used for embedding the watermark in comparison with DWT-SVD technique embedding.

In this paper Mohamed M. et. al [11], a DICOM image security technique based on the reversible watermarking method is proposed, this technique provides system authentication service, image integrity service and patient information confidentiality service; it is reversible because the original medical image can be retrieved at the receiver side without any distortion. The Digital Imaging and Communications in Medicine (DICOM) is the standard for formatting, storing and exchanging the medical images and associated information; moreover, DICOM support the connection of networked printers, such as laser imagers.

3. Methodology

3.1 Discrete Wavelet Transform (DWT)

Wavelet domain is a promising domain for image embedding. DWT is an orthogonal transform similar to the Discrete Cosine Transform that can be used for the audio and video compression, speech recognition, feature extraction, finger print, watermarking and many other applications in biomedical engineering [10]. It decompose an image in basically three spatial directions i.e., horizontal, vertical and diagonal in result separating the image into four different components namely LL, LH, HL and HH. Here first letter refers to applying either low pass frequency operation or high pass frequency operations to the rows and the second letter refers to the filter applied to the columns of the cover image. LL level is the lowest resolution level which consists of the approximation part of the cover image. Rest three levels i.e., LH, HL, HH give the detailed information of the cover image [10].

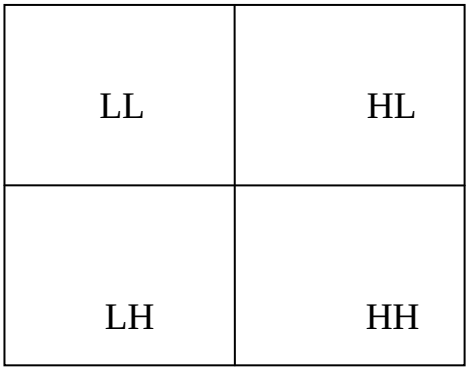

Figure 1: Single level 2-D DWT

3.1.1 Proposed DWT data hiding embedding algorithm:

The embedding algorithm for DWT based watermarking is shown in figure 3. The algorithm works as follows:

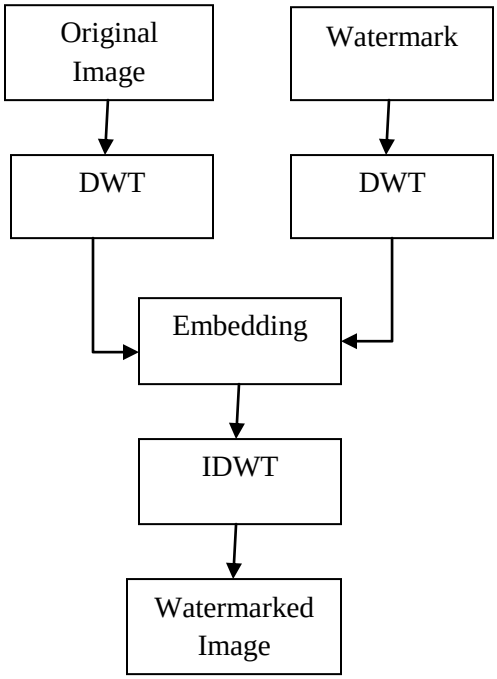

Figure 2: DWT based embedding

3.1.2 Proposed DWT data hiding extraction algorithm:

The extraction algorithm for DWT based watermarking is shown in figure 4.

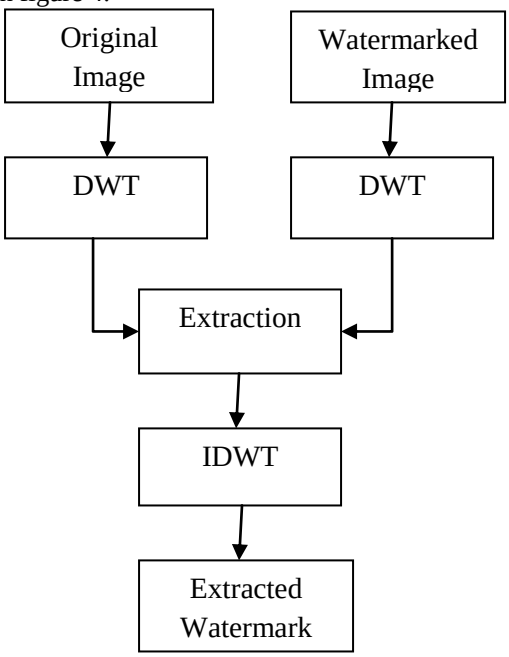

Figure 3: DWT based extraction

3.2 Singular Value Decomposition (SVD)

Singular Value Decomposition is a linear algebra transform which is used for factorization of a real or complex matrix with numerous applications in various fields of image processing. As a digital image can be represented in a matrix form with its entries giving the intensity value of each pixel in

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

the image, SVD of an image M with dimensions m x m is given by [10]:

$$M = USV^T \quad (1)$$

Where, U and V are orthogonal matrices and S known as singular matrix is a diagonal matrix carrying non-negative singular values of matrix M. The columns of U and V are called left and right singular vectors of M, respectively. They basically specify the geometry details of the original image. Left singular matrix i.e., U represents the horizontal details and right singular matrix i.e., V represents the vertical details of the original image. The diagonal values of matrix S are arranged in decreasing order which signifies that the importance of the entries is decreasing from first singular value to the last one.

This feature is employed in SVD based compression techniques.

There are two main properties of SVD to employ in digital watermarking schemes [2, 10]:

1. Small variations in singular values do not affect the quality of image.
2. Singular values of an image have high stability.

3.3 Hybrid DWT-SVD

Hybrid technique is a fusion of two techniques. Here, DWT and SVD are used together to improve the quality of digital watermarking and hence increases the robustness and imperceptibility of an image.

3.3.1 Proposed hybrid DWT-SVD data hiding embedding algorithm: The embedding algorithm for DWT-SVD based watermarking is shown in figure 6.

3.3.2. Proposed hybrid DWT-SVD data hiding extraction algorithm: The extraction algorithm for DWT-SVD based watermarking is shown in figure 7.

4. Implementation and Results

In this section, the practicability of the proposed image hiding approaches has been demonstrated. Moreover, comparison between DWT and DWT-SVD techniques has been done in terms of image imperceptibility, robustness and size of the resultant images. Test images are RGB images with size 256 × 256 pixels. The proposed DWT and hybrid DWT-SVD data hiding techniques are coded using MATLAB.

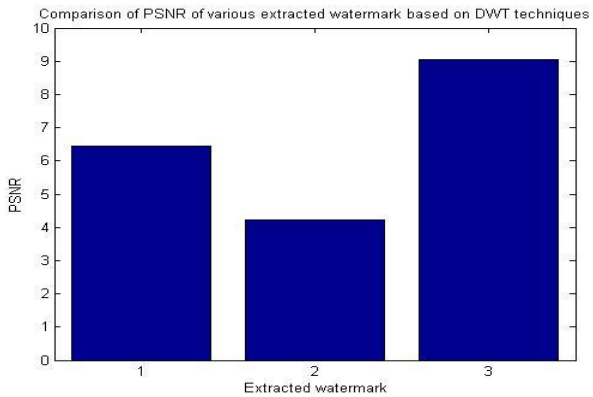

Figure 4: Comparison of PSNR of various extracted watermark based on DWT technique

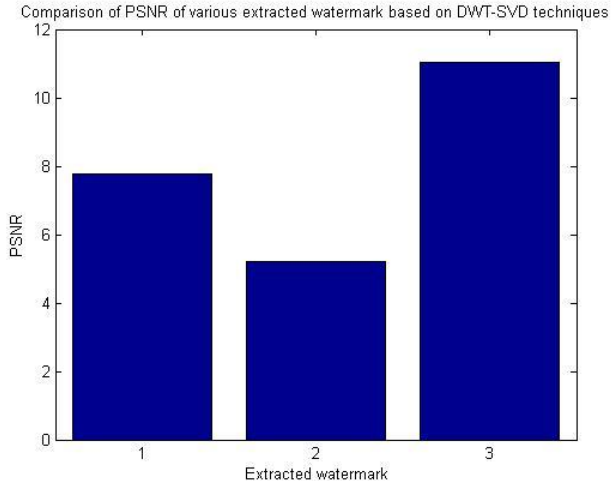

Figure 5: Comparison of PSNR of various extracted watermark based on DWT-SVD technique

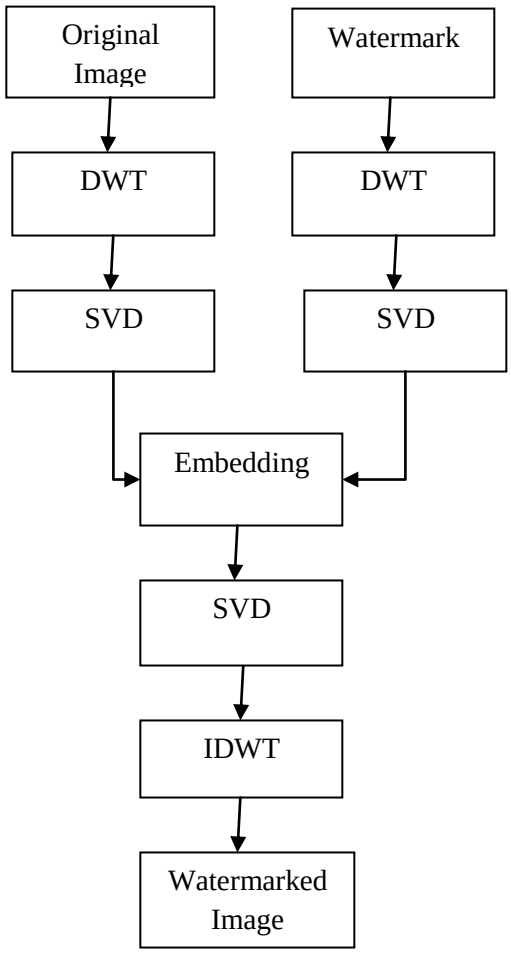

Figure 6: DWT-SVD based embedding

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

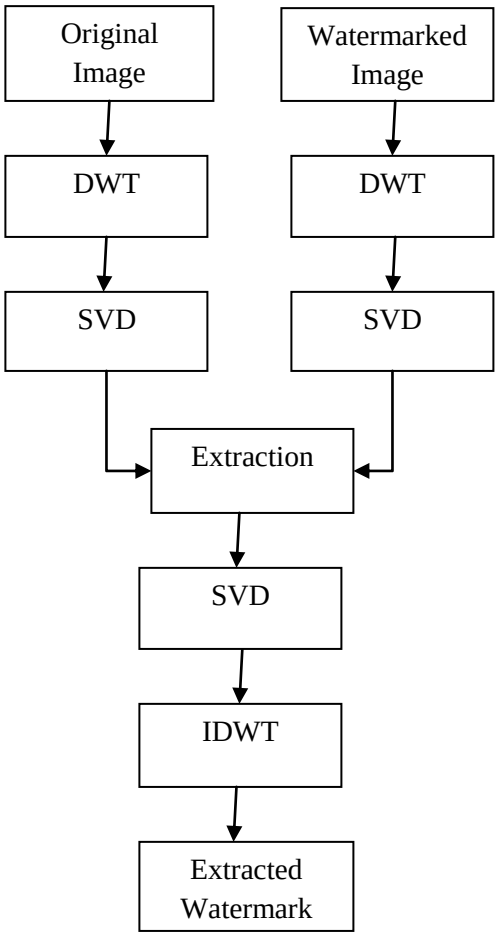

Figure 7: DWT-SVD based extraction

Figure 8: Host Image

Figure 9: Watermark Image

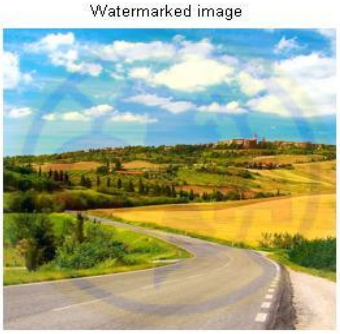

Figure 10: DWT based watermark embedding

Figure 11: DWT based watermark extraction

Figure 12: DWT-SVD based watermark embedding

Figure 13: DWT-SVD based watermark extraction

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

5. Conclusion and Future Work

DWT and DWT-SVD watermarking technique are applied to ensure the copyright protection and security of content or images and to increase the robustness of image. After applying both the watermarking techniques and comparing the values of PSNR at different values of scaling factor α, it is concluded that the hybrid DWT-SVD technique is much better than DWT technique. As at every value of scaling factor, value of peak signal to noise ratio (PSNR) is more in case of the hybrid technique. Less the value of PSNR more will be the degradation in the quality of the original image. This shows that after watermarking, the quality of original image degrades more when DWT technique is used for embedding the watermark in comparison with DWT-SVD technique embedding.

Although this scheme is able to hide sensitive information effectively and avoid disputes attention, it cannot completely resist various attacks during transmission in wireless sensor networks. Therefore, improvement in its robustness as well as security against various attacks may be considered as a future scope by using encryption algorithm with the help of secret key so that essential data can be prevented from unauthorized access.

References

[1] Marek Candik, Dagmar Brechlerova "DIGITAL WATERMARKING IN DIGITAL IMAGES" in IEEE-ICCST, pp: 43-46, in year 2008.

[2] Pei-Yu Lin, Jung-San Lee, and Chin-Chen Chang," Dual Digital Watermarking for Internet Media Based on Hybrid Strategies" in IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 19, NO. 8, AUGUST 2009.

[3] Ezz El-Din Hemdan, Nawal El-Fishaw, Gamal Attiya, Fathi Abd El-Samii "Hybrid Digital Image Watermarking Technique for Data Hiding" in 30th NATIONAL RADIO SCIENCE CONFERENCE (NRSC 2013) April 16-18, 2013, National Telecommunication Institute, Egypt.

[4] Prabhishek Singh, R S Chadha "A Survey of Digital Watermarking Techniques, Applications and Attacks" in International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013.

[5] Namita Chandrakar, Jaspal Bagga "Performance Comparison of Digital Image Watermarking Techniques: A Survey" in International Journal of Computer Applications Technology and Research Volume 2– Issue 2, 126 - 130, 2013, ISSN: 2319–8656.

[6] Sasmita Mishra, Amitav Mahapatra,Pranati Mishra "A Survey on Digital Watermarking Techniques" in International Journal of Computer Science and Information Technologies, Vol. 4 (3) , 2013,pp. 451-456.

[7] Manoranjan Kr Sinha , Dr. Rajesh Rai, Prof. G. Kumar "Literature Survey on Digital Watermarking" in International Journal of Computer Science and Information Technologies, Vol. 5 (5) , 2014,pp. 6538-6542.

[8] Y. Shantikumar Singh, B. Pushpa Devi, and Kh. Manglem Singh "A Review of Different Techniques on Digital Image Watermarking Scheme" in International Journal of Engineering Research (ISSN : 2319-6890), Volume No.2, Issue No.3, pp : 193-199, 01 July 2013.

[9] Nidhi Bisla, Prachi Chaudhary "Comparative Study of DWT and DWT-SVD Image Watermarking Techniques" in International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013 ISSN: 2277 128X.

[10] Mohamed M., Abd-Eldayem "A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine" in Cairo University Egyptian Informatics Journal, December 2012.