Digital Image Watermarking using Hybrid Technique

Preeti
preetibarar99@gmail.com
M.Tech. Scholar, Department of CSE, BRCM CET, Bahal, Bhiwani, Haryana (India)

Mrs. Neha
neha@brcm.edu.in
Assistant Professor, Department of CSE, BRCM CET, Bahal, Bhiwani, Haryana (India)

***Abstract*:** In the modern era of Information and Communication Technology, there is a great exchange of information between the users and every user need more and more secure communication in order to provide security. Security issue in watermarking is due to enlargement of internet. Due to the development in computer networks, digital data can be easily copied, altered and distributed in an illegal manner. Therefore, copyright protection of digital data is an important research issue of information security. In order to provide the authenticity to multimedia data techniques like encryption, stenography, watermarking is used. After going through various high-quality research paper, it came to know that there are various methods exist for executing digital watermarking successfully as per requirement of applications. In our implemented work, first section is to collect high-quality data set from reliable sources followed by diverse attacks testing so that proposed method must be robust against different attacks. After comparative analysis, proposed method gives better result than existed techniques.

Keywords*-SVD, DWT, PSNR, LWT, DFT, Hadmard Code*

*****

I. INTRODUCTION

There has been tremendous researchmaking it possible the advanced technologies existence. But with these popular techniques using internet, there comes the drawback in term of security [1]. For secure data transmission there are various technique developed with pace of time as per requirement of a specific application which help to preserve the data available on internet. For secure data transmission, watermarking is one of the edge technologies utilized for this purpose. Spatial domain and transform domain are the watermarking types. As we know when huge numbers of pixels are integrated then digital image is formed and spatial domain watermarking method straight used on image pixels[2].When transform domain watermark method is used, coefficient can be altered by the utilization of many other techniques for example DCT, DFT. DCT is vigorous to JPEFG compression while prone towards geometric deformation [6]. It can be utilized mainly for compressing the images. DFT also stand against geometric attacks and normally this method used in rotation invariant and translation resistant [7-8]. The sub bands give the information about authentic image. LL sub band gives all particulars about an image at lower frequencies while rest of the sub band provide diagonally, vertically and horizontally information. L is considered for LPF and H for HPF. We can choose a particular sub band according to our requirements and watermark is embarked on it [9], [10]. There are so many methods exists for secure watermarking so that data can be preserved from unauthorized person as well as stand against various types of attacks.

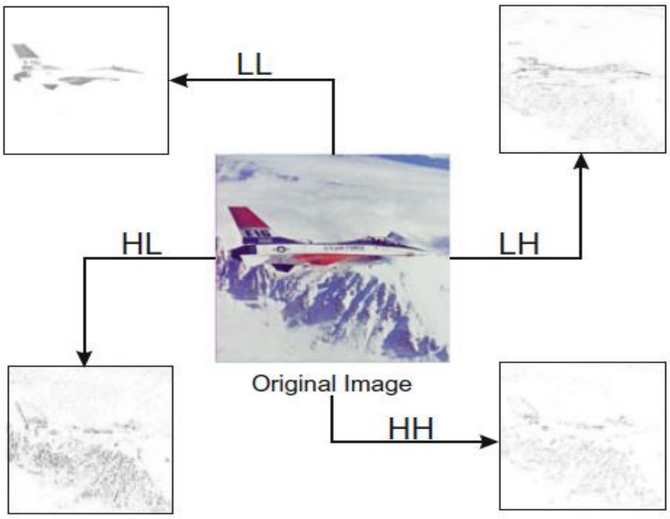


Figure 1 Image segmentation in different bands [7]

II. WATERMARKING

Inserting a digital data for example image, audio, video etc. with information and this digital data which cannot be easily detach is known as digital watermarking. With time more advanced technique came into domain of communication. Now a day to decrypt a cipher text is an easy task.Therefore need to design more robust technology which can provide better security to our data as compared to cryptography and limitations of cryptography overcome by stenography and watermarking. The procedure in which information is hiding over a cover image and that information cannot be accessed by third party is known as stenography. In watermarking concealed information is associated with cover object therefore we can say watermarking is almost similar to steganography. Therefore watermarking technique used for copyright preservation and holder authentication.

Principle of Watermarking: There are mainly three different steps involved for a watermarking system:

- Embedding
- Attack
- Detection

In first step which is embedding, host image and cover image are accepted by an algorithm to generate a watermarked image. After that watermarked image or data is then communicated to another person. When this person alters the communicated data, process in known as an attack and there are various attacks available which can be targeted on data. Now in last step which is detection,to extract watermark from attacked signal an algorithm is applied.During communication process if signal was not altered then watermark is still present, and it can be fetched. If the image is imitated, then the information is also carried in the copy.

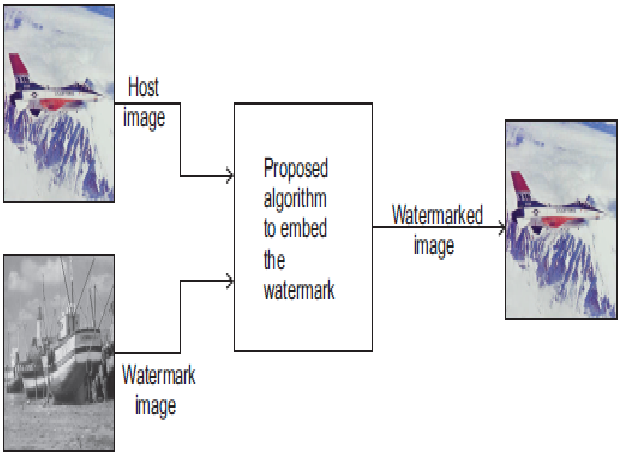


Figure 2 Fundamental Principle of Watermarking [3]

The authentic image and appropriate watermark are inserted by implementing any one technique out of various available to us. Now at the receiver side reverse process is executed to extract watermark image from watermarked image. As there are various techniques available through which watermark inserted on the cover image. In this process a secret key is used for inserting and extraction for security reason so that unauthorized person cannot access the data.

Limitations: Watermarking technique having many advantageous, but every technique has some limitation. The watermarked object can be under threat if attacks are bombarded intentionally or unintentionally. There is much software available that can be used for performing attack on any solid watermarked system. The main purpose of the attacks is preventing the watermarked system to perform its assigned work.

Removal Attack: The main objective of this attack is eliminating watermark data from watermarked object. This type of attack utilizes the fact that watermark is generally appear a noise for host signal.

Interference attack: As the name clarifies, in this type of attack supplementarynoise added to watermarked object. There are some examples of this category are listed as quantization, averaging, denoising, lossy compression and noise storm.

Geometric attack: The factors affecting the geometry of an image like flips, rotations, crops must be noticeable. The crop attacks from bottom of an image and from RHS are examples of this category.

Security Attack: Particularly when watermark algorithm gets known attackers can try performing modifications rendering watermark not valid, otherwise estimating modifying the watermark. Watermark algorithm is fully secured when any distortion, detection or forgery in not possible on the embarked data. But there are some drawbacks as given below:

- Watermarking technique unable to stop imitating an image but it helps to locate genuine owner of imitated image.
- If image manually manipulated, then from image watermarkdisappear.

III. EXISTING TECHNIQUE

Existed technique proposed a transformdomain method which utilizing YCbCr color space to enhance performance level of a watermarking system. Existed method having integration of various techniques: 2 Level DWT, DFT along with Singular Value Decomposition

DWT: By this technique an image is disintegrated into four different wavelets or segments. Out of these four segments a single sub band can be selected as per our requirements and application and then watermark is inserted. Through this technique compression of image executed effectively. To assist this there, exist various filter like Symlets, Haar, Coiflets and Daubechies.

DFT: There are various mathematical tools exist which are used to transform time domain signal into frequency domain and Fourier transform is one of them used to transform signal from spatial domain to frequency domain. DFT provide constructivediffusion of energy.

SVD: Singular Value Decompositionis a matrix defragmenting process to get tiny set ofvalues which has optimal data content. SVD technique is very popular and used in various applications like matrix operation and data reduction in machine learning. This technique has minimal truncating error along with robustness characteristics against various types of attack like Gaussian, blur, edge etc. on watermarked image

IV. PROPOSED HYBRID TECHNIQUE

A. Lifting Wavelet Transform

Wavelet transform decomposesdata (image) into different spatial domain and independent frequencies and it is time domain analysis technique. When the image is DWT transformed, then image is segmented into four regions which are HH, HL, LH and LL. Out of these LL is low frequency segment and rest are high frequency segments. Figure 1 shows the one level DWT decomposition process. In DWT method blurring effect is generated by wavelet filter and this is one of the major drawbacks of DWT technique, along with some ringing noise produced at the edges of an images. LWT overcome this drawback of existed technique and besides this in proposed technique processing time also minimized which is also a milestone.

B. Walsh Hadmard Transform

Fourier transform can be executed on both real and complex numbers and Hadamard transform is a sample of a class of Fourier transforms.Hadamard transform execute various operation like linear, orthogonal and symmetric on 2^m real number. The Hadamard transform can be considered as being built of DFTs.

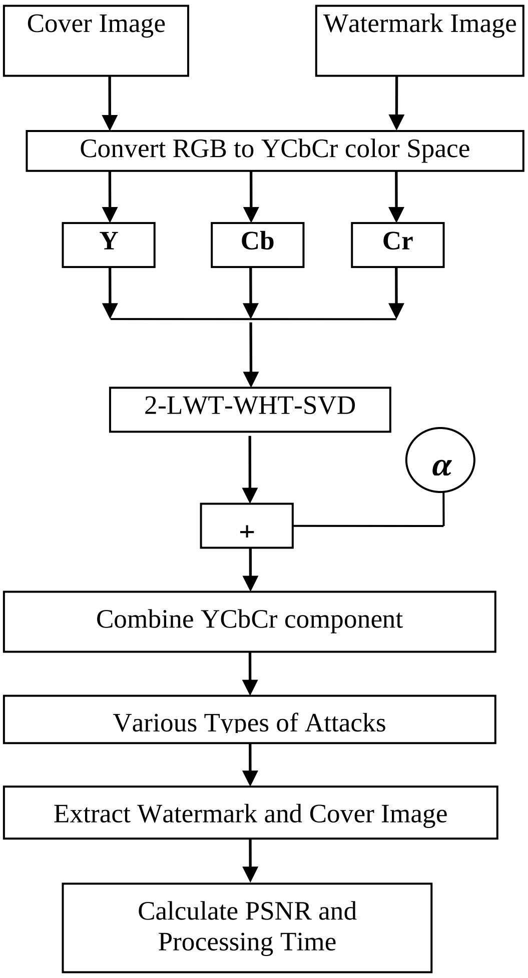

Cover Image
Watermark Image
Convert RGB to YCbCr color Space
Y
Cb
Cr
2-LWT-WHT-SVD
α
+
Combine YCbCr component
Various Types of Attacks
Extract Watermark and Cover Image
Calculate PSNR and Processing Time

Figure 3 Block Diagram of Proposed Architecture

It disintegrates a random input vector into a superposition of Walsh functions. Hadamard transform matrix consist only two types of elements either 1 or -1 and this matrix is an orthogonal square matrix. $H1$ is the smallest Hadamard matrix which is represented as [15]

$$H_1 \;= \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Higher size matrix computed with help of smallest Hadamard matrix as shown below:

$$H_2 = H_1 \times H_1 = \frac{1}{\left(\sqrt{2}\right)^2}\begin{bmatrix} H_1 & H_1 \\ H_1 & -H_1 \end{bmatrix}$$

In general formula for computing higher order matrix is depicted below:

$$H_n = H_{n-1} \times H_1 = \frac{1}{\left[\sqrt{2}\right]^n}\begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix}$$

C. Singular Value Decomposition

SVD technique is very popular and used in various applications like matrix operation and data reduction in machine learning. Let us consider a matrix M of order m×n and matrix may be real or complex does not matter and SVD technique segmented this matrix into three different matrixes as:

$$M = USV^T$$

Here V is known as a unitary matrix (real or complex) of order n × n. U is also a unitary matrix of order m×m (real or complex). S is a rectangular diagonal matrix which having non-negative real numbers on the diagonal of order m×n. One of the great edges of SVD technique is during utilization of singular matrix to insert watermark, minimum values of host images are changed due to which minimal changes take place in image and little changes can be discarded. [1] [2].

V. PERFORMANCE COMPARISON BETWEEN EXISTING AND HYBRID TECHNIQUE

In this section existed technique and proposed hybrid technique result will be analyzed for various parameters for example peak signal to noise ratio, processing time for embedding and extracting an image. First of all there is a requirement of data set on which watermarking process will be executed. There are various sources available from where data set can be fetched.

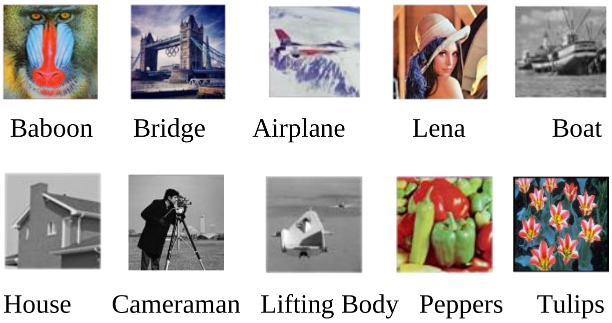


Figure 4 Dataset for Experimental

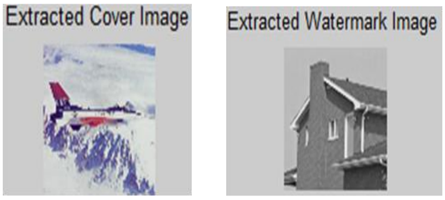


Figure 5 Extracted cover and watermark image

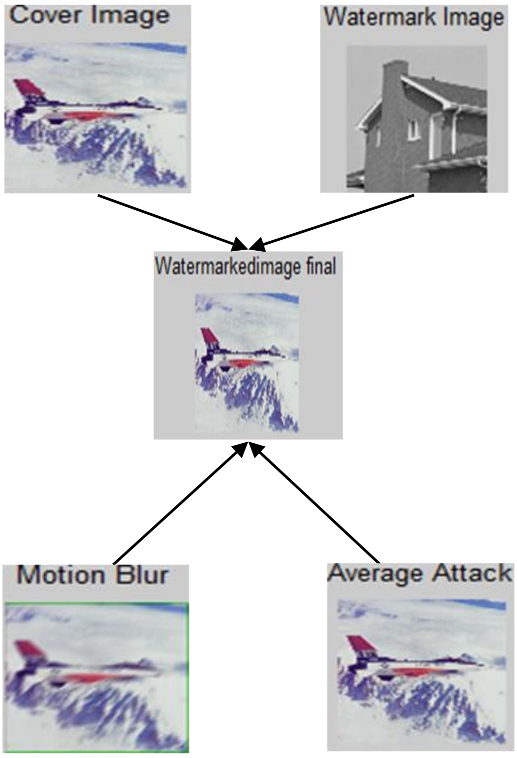


Figure 6 Complete output overview of Algorithm

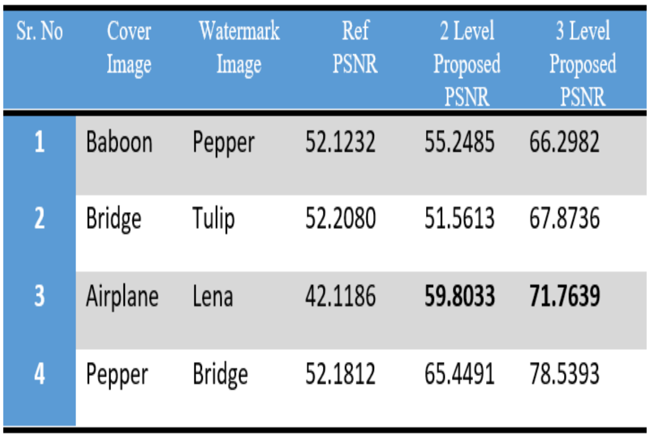
Following equation are used to determine RMSE and PSNR of cover image and watermarked image.

$$\mathrm{RMSE(x)} = \sqrt{\frac{1}{\mathrm{N}}||\mathrm{x}-\mathrm{x}^{\wedge}||^2 = \frac{1}{\mathrm{N}}\sum_{\mathrm{i}=1}^{\mathrm{N}}(\mathrm{x}-\mathrm{x}^{\wedge})^2}$$

Where N represent cover image size, x represents cover image and x^ depicts watermarked image

$$\mathrm{PSNR(x)} = \frac{20 * \log((255))}{\mathrm{RMSE(x)}}$$

TABLE I PSNR COMPARITIVE ANALYSIS AMONG EXISTED AND PROPOSED TECHNIQUE FOR WATERMARKING.



Sr. No	Cover Image	Watermark Image	Ref PSNR	2 Level Proposed PSNR	3 Level Proposed PSNR
1	Baboon	Pepper	52.1232	55.2485	66.2982
2	Bridge	Tulip	52.2080	51.5613	67.8736
3	Airplane	Lena	42.1186	**59.8033**	**71.7639**
4	Pepper	Bridge	52.1812	65.4491	78.5393

Table Idepicts comparative analysis between base methodand proposedmethod for PSNR (peak signal to noise ratio). From result it is very clear that proposed hybrid technique is better than existed technique.

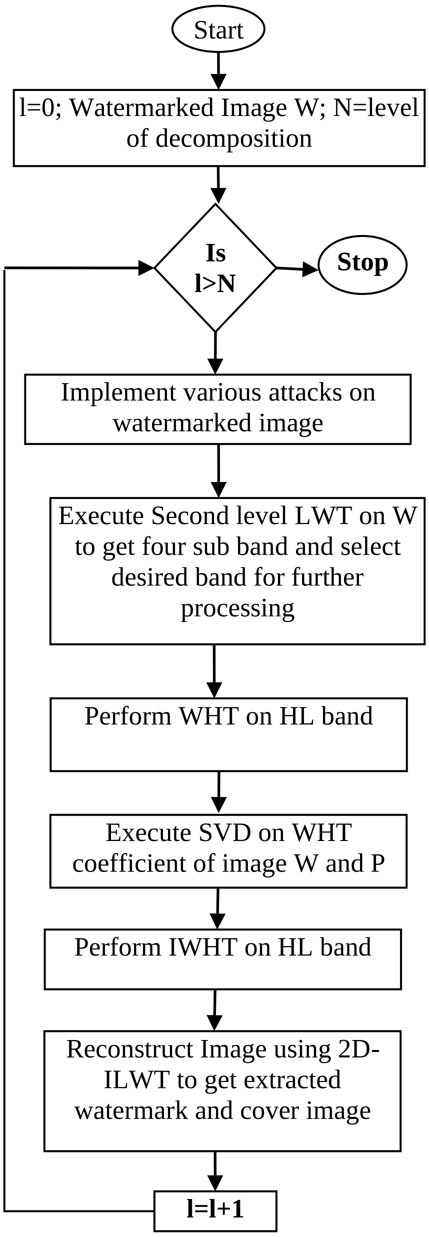
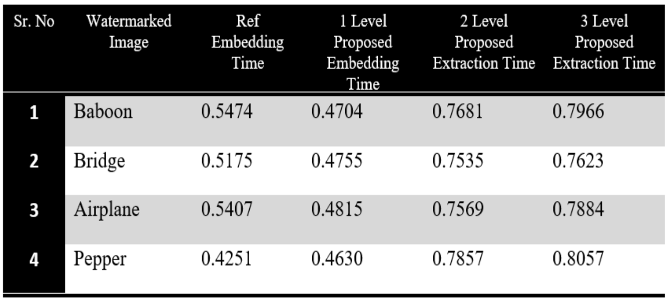

Start
l=0; Watermarked Image W; N=level of decomposition
Is l>N
Stop
Implement various attacks on watermarked image
Execute Second level LWT on W to get four sub band and select desired band for further processing
Perform WHT on HL band
Execute SVD on WHT coefficient of image W and P
Perform IWHT on HL band
Reconstruct Image using 2D-ILWT to get extracted watermark and cover image
l=l+1

Figure 7 Extraction System Flow Chart

TABLE II TIMECOMPARITIVE ANALYSIS AMONG EXISTED AND PROPOSED TECHNIQUE FOR EMBEDDING.



Sr. No	Watermarked Image	Ref Embedding Time	1 Level Proposed Embedding Time	2 Level Proposed Extraction Time	3 Level Proposed Extraction Time
1	Baboon	0.5474	0.4704	0.7681	0.7966
2	Bridge	0.5175	0.4755	0.7535	0.7623
3	Airplane	0.5407	0.4815	0.7569	0.7884
4	Pepper	0.4251	0.4630	0.7857	0.8057

Table IIdepicts comparative analysis among proposed and existed method for embedding time. It means how much time taken by proposed technique to process host and cover image.

VI. CONCLUSION

Watermarking allow great edge to our data so that unauthorized person unable to steal our crucial information. There are various techniques and algorithms exist through which watermarking can be executed on data to preserve information. There are various attacks exist like blur, average, crop and Gaussian which may destroy prime information from image, but watermarked images stand against all these odds. Inour research work Digital Image Watermarking carried out successfully using Lifting Wavelet Transform, WHT and Singular Value Decomposition. Blurring and ringing effect occur due to wavelet filter in DWT is overcome by proposed technique LWT which decomposes the image into different spatial domain and independent frequencies. Besides this one of the edge benefits of LWT computational time which is very fast. Proposed work depicted that computational time and PSNR values are better in our integrated technique. Our proposed work is also robust to stand against various types of attack like blur attack, motion attack and average attack.

VII. FUTURE SCOPE

As there are various color space available like HSV, CMYK therefore proposed algorithm can be extended to these color spaces. Further PSNR values can be examined for individual channel against various types of attacks

REFERENCES

[1] Piyush Pandey, Rakesh Kumar Singh, "Novel Digital Image Watermarking Using LWT-WHT-SVD in YCbCr Color Space" International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 6, June 2017

[2] Varsha Purohit, Bhupendra Verma, "A New Approach for Image Watermarking Using 3LWT-Walsh Transform-SVD in YCbCr Color Space" IJSRD - International Journal for Scientific Research & Development| Vol. 5, Issue 02, 2017

[3] Rajeev Dhanda and Dr. K. K Paliwal, "Hybrid Method For Image Watermarking Using 2 Level LWT-Walsh TransformSVD in YCbCr Color Space" International Journal on Recent and Innovation Trends in Computing and Communication Volume: 5 Issue: 11.

[4] Salma Hussainnaik, Farooq Indikar Reshma H Husennaik, "Review on Digital Watermarking Images" 2017 IJEDR | Volume 5, Issue 2 | ISSN: 2321-9939.

[5] N.Vinay Kumar, Prof.A.Venkat Ramana, DR.C.Sunil Kumar and V.Raghavendra, "An Enhanced invisible Digital Watermarking Method for Image Authentication", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 22 (2017) pp. 12016-1202.

[6] Mehdi Khalili and Mahsa Nazari, "Non Correlation DWT Based Watermarking Behavior in Different Color Spaces" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 1, 2016.

[7] Advith J, Varun K R and Manikantan K, "Novel Digital Image Watermarking Using DWT-DFT-SVD in YCbCr Color Space" International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS), 24-26 Feb 2016, **DOI:** 10.1109/ICETETS.2016.7603032

[8] Namita Chandrakar, Jaspal Bagga, "Performance Analysis of DWT Based Digital Image Watermarking Using RGB Color Space" International Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882 Volume 4, Issue 1, January 2015.

[9] D.Vaishnavia, T.S.Subashinib, "Robust and Invisible Image Watermarking in RGB Color space using SVD" International Conference on Information and Communication Technologies (ICICT 2014).

[10] Amit Kumar Singh, Mayank Dave, Anand Mohan, "Hybrid Technique for Robust and Imperceptible Image Watermarking in DWT–DCT–SVD Domain" The National Academy of Sciences, pp. 351–358 India 2014, 19 July 2014

[11] Pravin M. Pithiya and H.L.Desai, "DCT Based Digital Image Watermarking, Dewatermarking & Authentication" International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 2 Issue 3 May 2013.

[12] Dr. H. B. Kekre, Dr. Tanuja Sarode and Shachi Natu, "Performance Comparison of DCT and Walsh Transforms for Watermarking using DWT-SVD" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No. 2, 2013.

[13] Anuradha, Rudresh Pratap Singh, "DWT Based Watermarking Algorithm using Haar Wavelet," International Journal of Electronics and Computer Science Engineering, Vol. 1, No. 1, 2012.

[14] Rahim Ansari, Mrutyunjaya M Devanalamath, K. Manikantan and S. Ramachandran, "Robust Digital Image Watermarking Algorithm in DWT-DFT-SVD Domain for Color Images" 2012 International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 19-20, Mumbai, India

[15] Huang–Chi Chen, Yu–Wen Chang, Rey–Chue Hwang, "A Watermarking Technique based on the Frequency Domain," Journal of Multimedia, Vol. 7, No. 1, 2012
Anjul Singh Akash Tayal , "Choice of Wavelet from Wavelet Families for DWTDCT-SVD Image Watermarking" International Journal of Computer Applications (0975 – 888) Volume 48– No.17, June 2012.