



## Comparative Study on Hybrid Watermarking Techniques

Manjusha Tikariha\*

Electronics and Telecommunication  
BIT, Durg,  
India

Amar Kumar Dey

Electronics and Telecommunication  
BIT, Durg,  
India

---

**Abstract**— 21<sup>st</sup> century is the era of information where billions of bits are transmitted in every fraction of second; and with the advancement of internet, creation and modification of digital data (images, video and audio files, digital repositories, web publishing) has spread like fire. The information providers on internet are faced with the problem of how to transmit secure data in electronic means. This problem has given rise to research activity in this field of digital watermarking of electronic information. It imparts some secret information in to host image and this information is used for authentication. This paper presents an overview of the various concepts and research work in the field of hybrid watermarking techniques. In particular, the concept of hybrid based image watermarking is reviewed in details.

**Keywords**— Digital Watermarking, DCT, DWT, SVD, Hybrid Watermarking.

---

### I. INTRODUCTION

The rapid growth in the digital technology, image processing and Internet has made the reproduction of digitally created information simple and easy. The advancement in World Wide Web, MMS communication has made it possible to transmit and distribute this digitally created information in a fast and easy manner without any quality degradation. This new trend has several advantages which includes flexibility, cost effectiveness, etc., but at the same time, also possess some serious drawbacks. It allows hackers to manipulate / duplicate / access information illegally without the owners' knowledge. This has created a great concern on digital content security and is being studied seriously by several academicians and researchers. Content providers on the Internet are faced with the problem of how to secure electronic data. Due to these problems faced in the last few decades digital watermarking schemes have been proposed, where a small amount of imperceptible secret information is embedded into the digital content, which can be extracted at a later stage for copyright assertion, copy control, authentication, content integrity verification, broadcasting, etc [1],[2]. This problem has generated research activity in the area of digital watermarking of electronic content. The challenges are to introduce a digital watermark that is both transparent and highly robust to common signal processing and possible attacks. The two basic requirements for an effective watermarking scheme robustness and transparency conflict each other. Image watermarking is the process of inserting hidden information in an image by introducing modifications of minimum perceptual disturbance. Robustness, perceptual transparency, capacity and blind watermarking are four essential factors to determine quality of watermarking scheme [1]. Image watermarking techniques proposed so far can be divided into two groups accordingly processing domain of host image. One is to modify the intensity value of the luminance in the spatial domain [2],[3] and the other is to change the image coefficient in a frequency domain [4],[8]. More recently, different watermarking techniques and strategies have been proposed in order to solve a number of problems ranging from the detection of content manipulations, to information hiding (steganography), to document usage tracing. There are different types of attacks: geometrical attacks, noising attack, de-noising attack, compression attack and image processing attack. Geometrical attack causes synchronization errors during the extraction process of the watermark due to which the quality of the extracted watermark is affected [3]. Watermark has to be embedded in the invariant transform domain to counteract the synchronization errors. Current digital image watermarking techniques may be grouped into spatial-domain techniques and frequency-domain techniques. Compared to spatial domain watermarking techniques, frequency-domain watermarking techniques proved to be more effective with respect to achieving the imperceptibility and robustness requirements of digital watermarking algorithms [6]. Commonly used frequency-domain transforms are the Discrete Wavelet Transform (DWT), the Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD) [1]. However, DWT has been used in digital image watermarking more frequently due to its time/frequency decomposition characteristics and its resemblance to the theoretical models of the human visual system [10]-[11]. DWT-based watermarking algorithms could further be improved by combining DWT with DCT. The combination of the two transforms namely the DWT and the DCT could compensate for the drawbacks of each other, resulting in effective watermarking [18]-[21]. From the above we can say that by combining DCT and DWT we get the advantage of better amount of compression and scalability but if the image is rotated or altered then it can create a problem for this method that is the PSNR value would decrease so to overcome this we can combine DCT and DWT with SVD as it offer advantage such as stability, proportion invariance and rotation invariance [14].

The paper is organized as below. Section 1 provides an introduction to watermarking systems, Section 2 describes a general model of watermarking systems, Section 3 discusses the commonly used frequency domain transform used for watermarking and Section 4 presents a review on hybrid based watermarking. A brief conclusion with future direction is presented in Section 5.

## II. GENERIC WATERMARKING SYSTEM

Digital watermarking algorithms are composed of three parts, namely, watermark embedding algorithm, watermark extraction algorithm and watermark detection algorithm [1]. A general watermark system phases is shown in Figure 1.

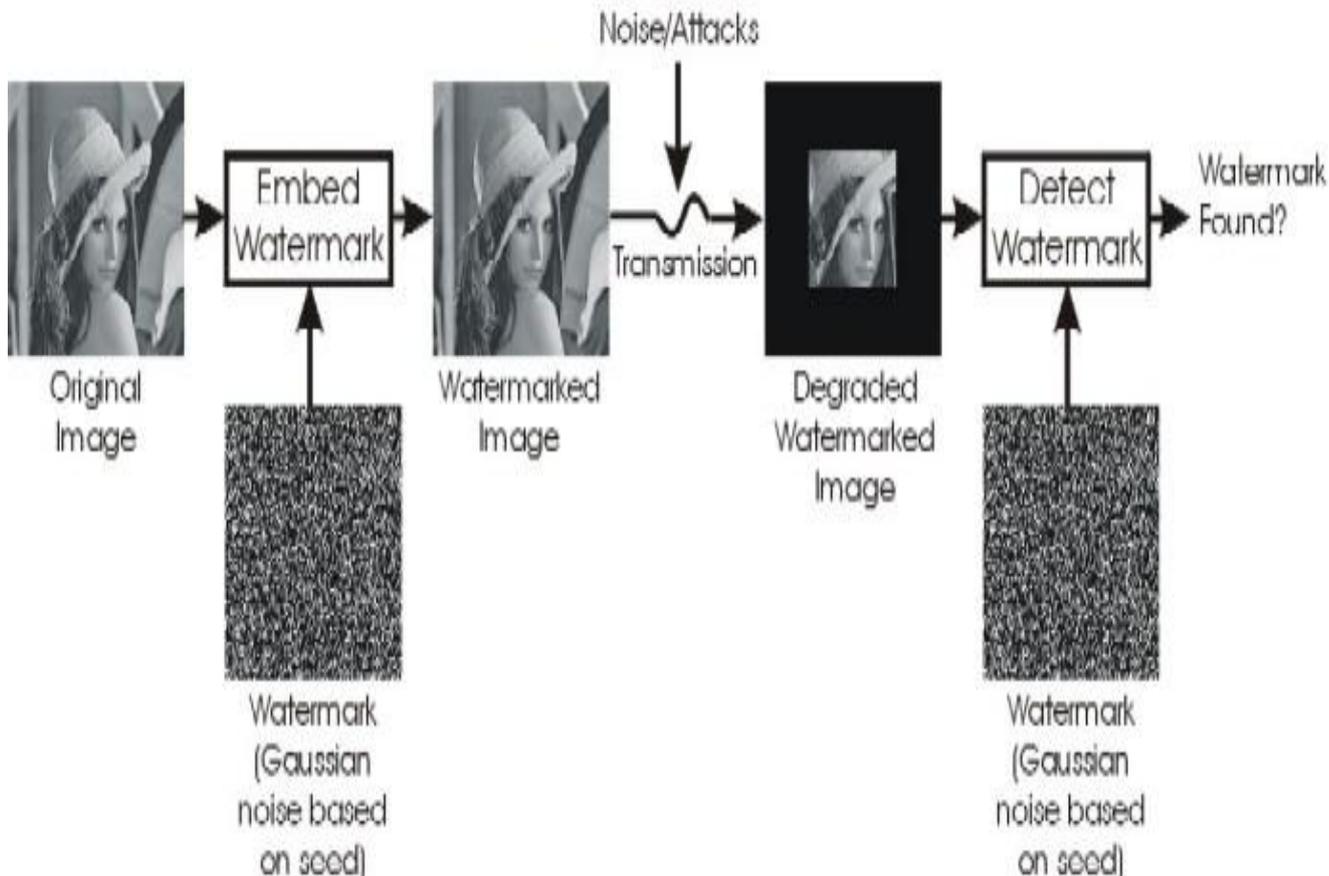


Fig 1: Watermark Lifecycle Phases

During embedding process, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. The watermarked signal is then transmitted or stored. If a person makes a modification, then the digital content is said to be attacked. A watermark attack is an attack on digital data where the presence of a specially crafted piece of data can be detected by an attacker without knowing the encryption key. Special attention has to be paid to the kind of attacks as they can help to develop better watermarking techniques and defined better benchmarks.

Any watermarking technique has to be evaluated to judge its performance. Three factors, as given below, must be considered while evaluating an image watermarking algorithm.

- Capacity, i.e. the amount of information that can be put into the watermark and recovered without errors;
- Robustness, i.e. the resistance of the watermark to alterations of the original content such as compression, filtering or cropping;
- Visibility, i.e. how easily the watermark can be discerned by the user.

The desired properties are high capacity, low distortion and high robustness to attacks or high security. These factors are interdependent; for example, increasing the capacity will decrease the robustness and/or increase the visibility. Therefore, it is essential to consider all three factors for a fair evaluation or comparison of watermarking algorithms.

## III. WATERMARKING TECHNIQUES:

Transform domain/frequency domain-

- DCT
- DWT
- SVD

Values of certain frequencies (normally low) are altered from their original. The watermark is applied to the whole image so as not to be removed during a cropping operation and also to make its verification difficult.

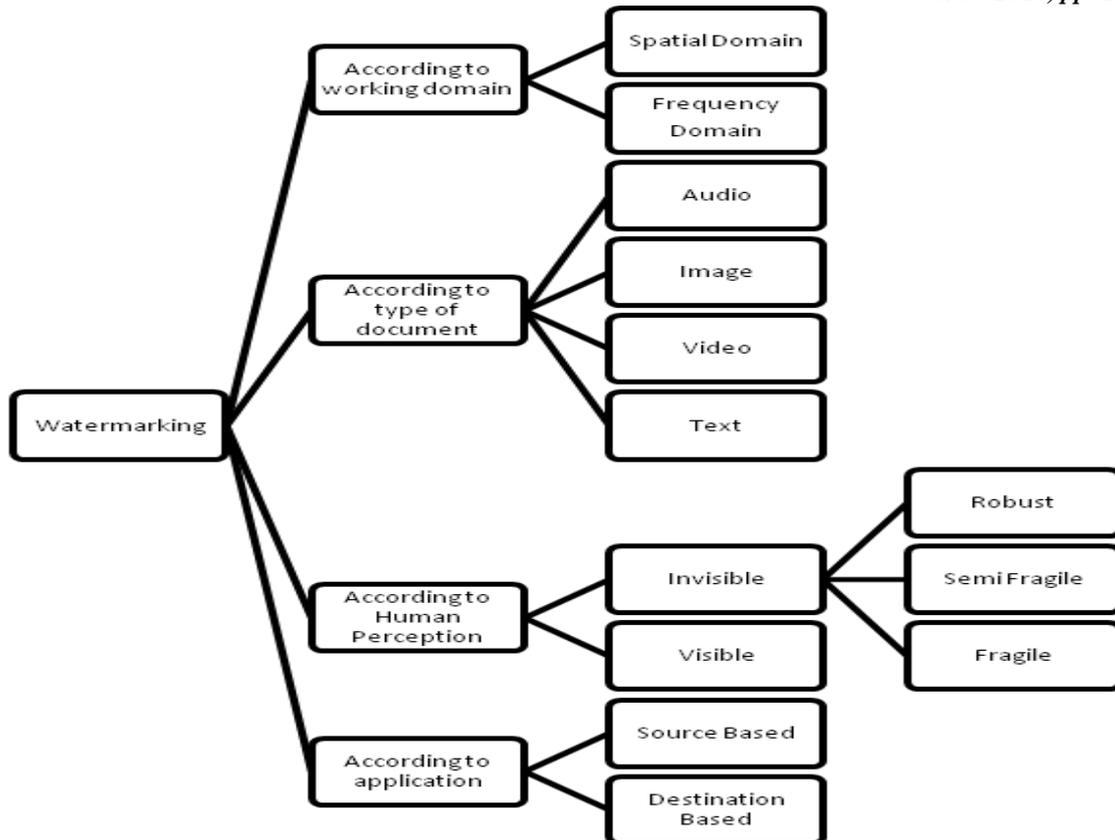


Fig 2: Categories of watermark techniques

#### IV. BASICS OF FREQUENCY DOMAIN METHODS

##### A. Discrete Cosine Transform (DCT)

The discrete cosine transform (DCT) represents an image as a sum of sinusoids of varying magnitudes and frequencies [1],[ 3]. For an input image, X, of size N x N the DCT coefficients for the transformed output image, Y, are computed according to (1). X (i, j) is the intensity of the pixel in row i and column j of the image, and Y (u, v) is the DCT coefficient in row u and column v of the DCT matrix.

$$Y(u, v) =$$

$$C_u C_v \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \frac{\cos((2j+1)y\pi)}{2N} \frac{\cos((2i+1)x\pi)}{2N}$$

Where,

$$C_u C_v = \sqrt{\frac{1}{N}} \text{ for } u, v=0 \text{ and}$$

$$C_u C_v = \sqrt{\frac{2}{N}} \text{ for } u, v = 1, 2, \dots, (N-1)$$

Performing DCT of an image gives rise to three different frequency coefficient sets: low frequency, mid frequency and high frequency coefficient sets as shown in fig 2. The DCT has a special property that most of the visually significant information of the image is concentrated in just a few coefficients of the DCT [1]-[3]. This is referred to as the ‘Energy compaction property’.

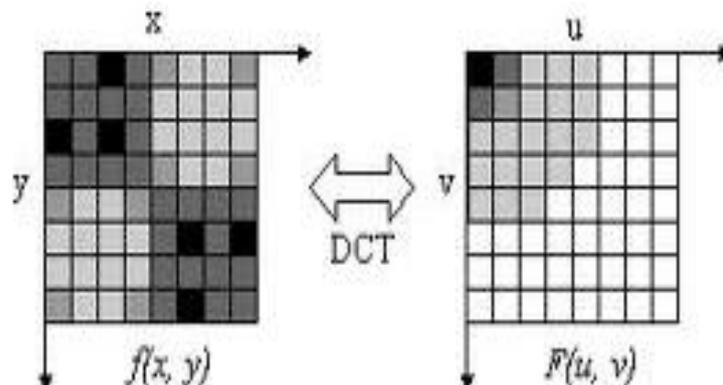


Fig 3. The DCT operation-Original picture and its corresponding DCT mapping.

Most of the signal energy is concentrated at the low frequency coefficients, which contains the most important visual parts of the image. And high frequency coefficients of the image are usually removed through compression and are more prone to noise attacks. Hence watermark is embedded in the mid frequency coefficients so that the visibility of the image is not affected and the watermark is not removed by compression or noise attacks. One limitation of the mentioned authentication schemes is that it has blocks artifacts means loss of some information. Therefore, it is desirable that watermarking schemes are capable of perfectly recovering the original media after passing the authentication process. Schemes with this capability is DWT based watermarking schemes as in this the watermark is weighted in order to decrease visual artifact.

### B. Discrete Wavelet Transform (DWT)

Wavelet transform decomposes an image into a set of band limited components which can be reassembled to reconstruct the original image without error [3]-[5]. For 2-D images, applying DWT corresponds to processing the image by 2-D filters in each dimension. The filters divide the input image into four non-overlapping multi-resolution sub bands, a lower resolution approximation image (LL1), horizontal (HL1), vertical (LH1) and diagonal (HH1) detail components. The process can be repeated to obtain multiple scale wavelet decomposition as shown in fig 3.

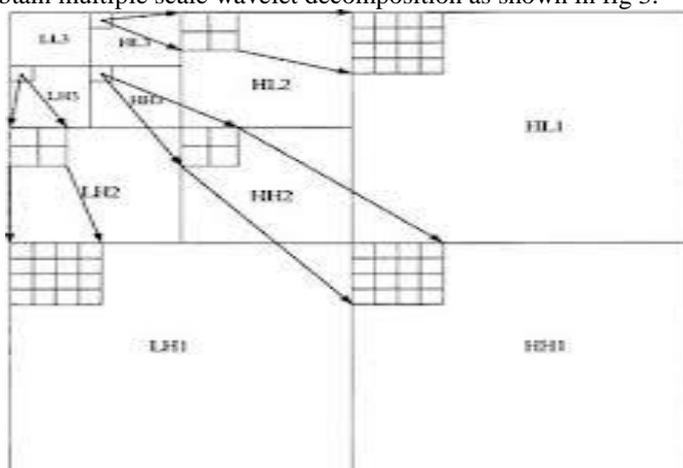


Fig 4. Wavelet Decomposition

One of the advantages of DWT over DCT is that it can more accurately model the aspects of the HVS as compared to DCT [3]-[5]. In general most of the image energy is concentrated at the LL subband and hence embedding watermarks in this sub band may degrade the image quality, but embedding watermark in this subband can provide higher robustness. On the other hand, the detail subbands LH, HL and HH include the edges and textures of the image and the human eye is generally not much sensitive to changes in these subbands. Hence embedding watermarks in these subbands can provide higher imperceptibility, without being perceived by human eye. But the noise attacks and lossy compression results in data loss at high frequencies and hence the robustness may suffer for the watermarks embedded in the HH subband. Hence many of the watermark embedding schemes opts for the LH or HL subband for embedding the watermark in order to provide both imperceptibility and robustness [6].

### C. Singular value decomposition (SVD)

Recently, Singular Value Decomposition (SVD) was explored for watermarking [4]. The SVD was originally developed by geometers, who wished to determine whether a real bilinear form could be made equal to another by independent orthogonal transformations of the two spaces it acts on. Singular Value Decomposition is an optimal method for matrix decomposition. SVD is known for its stability, proportion invariance and rotation invariance properties. SVD is a general linear algebra technique which is used for packing the maximum signal energy into a few coefficients as possible.

The SVD theorem decomposes a digital image  $A$  of size  $M \times N$ , as:

$$A = U S V^T$$

Where,  $U$  and  $V$  are of size  $M \times M$ , and  $N \times N$  respectively.  $S$  is a diagonal matrix containing the singular values. In watermarking trial, SVD is applied to the image matrix; then watermark resides by altering singular values (SVs). The singular values reflect the intrinsic properties of the image, with strong stability; therefore the image won't have a big change when given a small disturbance. The properties of SVD [14].

## V. HYBRID WATERMARK TECHNIQUES

### A. Joint DCT-DWT

The idea of applying two transform is based on the fact that combined transforms could compensate for the drawbacks of each other, resulting in effective watermarking. DWT has excellent spatial localization, frequency spread and multi-resolution characteristics, which are similar to the theoretical models of the human visual system (HVS). DCT based watermarking techniques offer compression while DWT based watermarking techniques offer scalability. These desirable properties are used in this combined watermarking technique. This method provide high imperceptibility as well as high robustness against different attacks such as JPEG compression, Gaussian noise, Salt & Pepper noise,

Speckle noise, Scaling, Cropping etc, however ,fail for rotation attack. Further studies are needed on improving the robustness of the algorithm against rotation attack [18]-[20].

### **B. DCT-DWT-SVD**

The two most commonly used methods are based on DCT-SVD and DWT-SVD. The commonly present disadvantages in traditional watermarking techniques such as inability to withstand attacks are absent in SVD based algorithms. They offer a robust method of watermarking with minimum or no distortion. DCT based watermarking techniques offer compression while DWT based compression offer scalability. Thus all the three desirable properties can be utilized to create a new robust watermarking technique.

This method utilizes the wavelet coefficients of the cover image to embed the watermark. Any of the four sets of wavelet coefficients can be used to watermark the image. The DCT coefficients of the wavelet coefficients are calculated and singular values decomposed. The same procedure is applied to the watermark also. The singular values of the cover image and watermark are added to form the modified singular values of the watermarked image. The modified DCT coefficients form the singular value decompositions triangular matrices. Then the inverse DCT transform is applied followed by the inverse DWT. This is the algorithm that clubs the properties of SVD, DCT and DWT. This is a technique that has never been used before. Watermark embedded using this algorithm is highly imperceptible. This scheme is robust against all sorts of attacks. It has very high data hiding capacity [22]-[24].

In this method, the watermark is embedded very deep into the cover image since three transform (DCT, DWT, SVD) are taken before embedding the watermark which help in resilience the attacks. This method can be used for copyright protection, tamper detection, fingerprinting, authentication and secure communication. This hybrid method is robust to JPEG compression, noise adding attacks, contrast adjustment attack, cropping attack, rotation attack and other signal proceeding attacks. Better robustness is obtained at the expense of increased computation time.

The different watermarking schemes are compared and given in Appendix.

## **VI. CONCLUSION**

The literature review shown in appendix reveals the fact that there are numerous innovative and inventive watermarking approaches. In this paper we have studied about different method. Now research is oriented towards hybrid based watermarking schemes. Mostly used transforms are DCT and DWT. The DCT based method offer better compression and DWT offer better scalability but if the watermarked image is rotated or altered then it can create a problem while extracting watermark that is the PSNR value would decrease .Another important transform used now a days is SVD .It is known for its stability, proportion invariance and rotation invariance properties. When all this three transforms are combined in hybrid form they compensate drawback of each other resulting in a better watermarking method. Thus due to combination of various method we use the term Hybrid method. Further, the review reveals the fact that even though abundant information on hybrid based watermarking schemes are published; a performance evaluation of various schemes is absent. The performance evaluation of existing hybrid based watermarking schemes is the major issue.

## **REFERENCE**

- [1] Ingemar J. Cox, Matthew L. Miller, Jeffrey Adam Bloom (2002) "Digital Watermarking: Principles and Practice book".
- [2] Cox, Ingemar J., Matthew L. Miller, and Jeffrey A. Bloom. "Watermarking applications and their properties." In *itcc*, pp. 6-10. 2000.
- [3] Voloshynovskiy, Sviatolsav, Shelby Pereira, Thierry Pun, Joachim J. Eggers, and Jonathan K. Su. "Attacks on digital watermarks: classification, estimation based attacks, and benchmarks." *Communications Magazine*, IEEE 39, no. 8 (2001): 118-126.
- [4] Barni, Mauro, Christine I. Podilchuk, Franco Bartolini, and Edward J. Delp. "Watermark embedding: hiding a signal within a cover image." *Communications Magazine*, IEEE 39, no. 8 (2001): 102-108.
- [5] Radharani, S., and M. L. Valarmathi. "A study on watermarking schemes for image authentication." *International Journal of Computer Applications* 2, no. 4 (2010): 24-32.
- [6] Hsu, Chiou-Ting, and Ja-Ling Wu. "Hidden digital watermarks in images." *Image Processing*, IEEE Transactions on 8, no. 1 (1999): 58-68.
- [7] Huang, Jiwu, Yun Q. Shi, and Yi Shi. "Embedding image watermarks in DC components." *Circuits and Systems for Video Technology*, IEEE Transactions on 10, no. 6 (2000): 974-979.
- [8] Ahmidi, Narges, and Reza Safabakhsh. "A novel DCT-based approach for secure color image watermarking." In *Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on*, vol. 2, pp. 709-713. IEEE, 2004.
- [9] Lin, Shinfeng D., Shih-Chieh Shie, and Jim Yi Guo. "Improving the robustness of DCT-based image watermarking against JPEG compression." *Elsevier- Computer Standards & Interfaces* 32.1 (2010): 54-60.
- [10] Xia, Xiang Gen, Charles Boncelet, and Gonzalo Arce. "Wavelet transform based watermark for digital images." *Optics Express* 3, no. 12 (1998): 497-511.
- [11] Barni, Mauro, Franco Bartolini, and Alessandro Piva. "Improved wavelet-based watermarking through pixel-wise masking" *Image Processing*, IEEE Transactions on 10, no. 5 (2001): 783-791.
- [12] Kashyap, Nikita, and G. R. Sinha. "Image watermarking using 2-level DWT" *Advances in Computational Research* 4, no. 1 (2012).

- [13] Kashyap, Nikita, and G. R. Sinha. "Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT)." *International Journal of Modern Education & Computer Science* 4.no.3 (2012).
- [14] Liu, Ruizhen, and Tieniu Tan. "An SVD-based watermarking scheme for protecting rightful ownership." *Multimedia, IEEE Transactions on* 4, no. 1 (2002): 121-128.
- [15] Li, Yuhui, Wei Gou, and Bo Li. "A New Digital Watermark Algorithm Based on the DWT and SVD." In *Distributed Computing and Applications to Business, Engineering and Science (DCABES), 2011 Tenth International Symposium on*, pp. 207-210. IEEE, 2011.
- [16] Rao, V. Srinivasa, et al. "Discrete cosine transform vs discrete wavelet transform: An objective comparison of image compression techniques for JPEG encoder." *International Journal of Advanced Engineering and Applications*(2010): 87-90.
- [17] Katharotiya, Anilkumar, Swati Patel, and Mahesh Goyani. "Comparative Analysis between DCT & DWT Techniques of Image Compression." *Journal of information engineering and applications* 1.2 (2011): 9-17.
- [18] Al-Haj, Ali. "Combined DWT-DCT Digital Image Watermarking." *Journal of computer science* 3.9 (2007).
- [19] Kasmani, Saied Amirgholipour, and Ahmadreza Naghsh-Nilchi. "A new robust digital image watermarking technique based on joint DWT-DCT transformation." *Convergence and Hybrid Information Technology, 2008.ICCIT'08.Third International Conference on*. Vol. 2. IEEE,2008.
- [20] Deb, Kaushik, Md Al-Seraj, Mir Md Kowsar, and Iqbal Hasan Sarkar. "A joint DWT-DCT based watermarking technique for avoiding unauthorized replication." In *Strategic Technology (IFOST), 2012 7th International Forum on*, pp. 1-5. IEEE, 2012.
- [21] Angshumi Sarma and Amrita Ganguly. "Image Watermarking in DCT-DWT domain" *IRNet Transactions on Electrical and Electronics Engineering (ITEEE) ISSN 2319 – 2577, Vol-1, Iss-2, 2012*
- [22] Jose, Sneha, Rajesh Cherian Roy, and Sreenesh Shashidharan. "Robust image watermarking based on DCT-DWT-SVD method." *International Journal of Computer Applications* 58, no. 21 (2012): 12-16.
- [23] C S Rawat Sneha and M Shivamkutty "A Novel Digital Image Watermarking Using Hybrid Technique" *VESIT , International Technological Conference-2014 (I-TechCON), Jan. 03 – 04, 2014*
- [24] Navas, K. A., Mathews Cheriyan Ajay, M. Lekshmi, Tampy S. Archana, and M. Sasikumar. "DWT-DCT-SVD based watermarking." In *Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008. 3rd International Conference on*, pp. 271-274. IEEE, 2008.

## VII. APPENDIX

**Comparison Table for various Watermarking Schemes.**

S.No.	Reference	Method	Result
<b>DCT based Watermarking Schemes</b>			
1	8	Modifies the middle coefficient of DCT of original image to embed the watermark.  Three methods are implemented (HVS,2D periodic Torus permutation function and post-preprocessing algorithm) to improve robustness and security.	Higher quality watermarked image is obtained with PSNR=57.9 dB  After attack NC=1 is reduced to NC=0.8 i.e. less degradation of image.
2	7	Quantitative analysis on the magnitudes of DCT components of host images based on HVS.	When attack is applied average PSNR value = 43 dB is reduced as low as 13dB.
3	9	Pseudorandom permutation FDCT, middle frequency coefficient of DCT	When attack is applied average PSNR value = 40.83 dB is reduced as low as 31.27 dB. Image resampling and image rotation, are still challenging to our current work,
4	6	Based on concept of mathematical remainder by modifying the low frequency coefficient of DCT. Torus automorphism permutation	Suitable for highly JPEG compressed image
<b>DWT based watermarking scheme</b>			
5	11	Operate in the wavelet domain; masking is accomplished – pixel by pixel by taking into account the texture and luminance contents of all the subbands.	Average PSNR=36 dB After attack by image cropping result was surprisingly high.
6	10	Pseudo random codes are added to the large coefficients at the high and middle frequency bands of the DWT (haar wavelet) of an image.	Result show that DWT is better than DCT by using EZW and halftoning.
7	12	2-level DWT and alpha bending technique	Best result obtain at k=0.98 Shows that 2 level DWT is better than

			1 level DWT.
8	13	3-level DWT by alpha bending embedding technique.	3 level DWT is better than 2 level DWT
<b>DCT Vs DWT</b>			
9	16	DCT with scalar quantization and Huffman coding based JPEG encoder.  DWT-3level wavelet with SPIHT	In DWT method , when attack is introduced PSNR vary from 38.36 to 30.13 whereas in case of DCT its value vary by 38.04 to 28.50. Thus DWT is better in terms of variations.
10	17	DCT-Quantization DWT-Analysis is computed by filter bank HPF (detail part), LPF (approximation part) and downsampling.	DWT technique is much efficient than DCT technique in quality and efficiency wise but in performance time wise DCT is better than DWT.
<b>Joint DCT-DWT based watermarking scheme</b>			
11	18	Combined DWT and DCT using pn sequence. DWT-2-level subband (HL <sub>2</sub> ,HH <sub>2</sub> ) DCT-middle frequency	Comparison of DWT and DCT-DWT is analyzed. Psnr value obtained by DWT (HL <sub>2</sub> /HH <sub>2</sub> ) is 80 dB/77 dB where as in case of joint DCT-DWT it is 97 dB. After attack NC value in DWT reduces to 0.447 from 1 where as its value in DCT-DWT reduces only to 0.968.
12	21	Two different methods of image watermarking are described, using combined DCT-DWT transform. In the first approach, the two smaller sub bands of the HL sub band LH <sub>2</sub> and HL <sub>2</sub> are used to embed the watermark and in the second approach all the four smaller subbands of the HL subband are used to embed the watermark.	The imperceptibility and robustness of the four subband method psnr=43 dB is comparatively higher than the two subband method i.e. 40 dB. But for rotation attack psnr is as low as 8.63.
13	20	Joint DCT-DWT technique based on low frequency watermarking with weighted correction.	Results show that the proposed algorithm apparently preserves superior image quality and robustness under various attacks
14	19	Embed the watermark in the special middle frequency of DCT in the subbands of 3 levels DWT transformed of a host image.	Results show that the imperceptibility of the watermarked image is acceptable but for rotation attack psnr is reduced from 37.67 dB to 8.63. Further studies are needed on improving the robustness of the algorithm against rotation attack.
<b>DCT-DWT-SVD based watermarking scheme</b>			
15	22	The watermark is embedded very deep into the cover image since three transform (DCT, DWT, SVD) are taken before embedding the watermark which help in resilience the attacks.	Better robustness is obtained at the expense of increased computation time
16	24	Non-blind transform domain watermarking based on DWT-DCT-SVD	Watermark can be recovered even with the help of an attacked watermarked image
17	23	DCT is applied to the selected HL/LH sub band of DWT. Using a Zig-zag sequence the DCT coefficients are mapped to the four quadrants and SVD is applied to each quadrant.	This method found to be more robust as compared to DCT-SVD and DWT-SVD. Average psnr obtained by DWT-SVD is 71.1788 dB and by DWT-DCT-SVD are 90.6518 dB.