Digital Image Watermarking Techniques: A Review

Pushpa Mala .S. *pushpasiddaraju@gmail.com*
Research Scholar, Jain University, Bengaluru, India
& Sambhram Institute of Technology, Bengaluru, India

D. Jayadevappa *devappa.22@gmail.com*
Dept. of Electronics & Instrumentation Engineering,
JSS Academy of Technical Education, Bengaluru, India

K.Ezhilarasan *murali981983@gmail.com*
Research Scholar, Jain University, Bengaluru, India
& Sambhram Institute of Technology, Bengaluru, India

Abstract

Advancements in science and technology have introduced the need to protect data, authenticate data, integrate data, assert ownership, content labelling and security. Digital Watermarking schemes protect all forms of digital data. Digital Image Watermarking can be applied to gray scale, halftone, color, medical and 3D images. The process of watermarking can be broadly classified into three phases namely embedding, attacking, and decoding for typical scenarios. Some of the watermarking schemes adopted in the past include vector quantization, spread spectrum, SVD, DCT, DFT, etc. It was observed that the spread spectrum was more robust and it had also been applied for patenting. In spite of this, the method could not withstand high amplitude noise. Hence, later DCT, DFT and Wavelets were used. These schemes were not robust to collusion attacks. In this review, we have identified the embedding and detection schemes of the existing watermarks over the past decade and analyzed the robustness of each of these methods. The different parameters considered to analyze the performance of the existing watermarking schemes are also discussed. Research under watermarking is a great field of interest involving multimedia security, forensics, data authentication and digital rights protection. This paper will be useful for researchers to implement a robust watermarking scheme.

Keywords: Digital Image Watermarking, Watermark Embedding, Watermark Detection, frequency domain, robust, reversible

1. INTRODUCTION

In this modern era, a tremondous growth in science and technology is noticed. This has led to a large number of e-commerce sites and applications. Intellectual property protection, data authentication, ownership and security are of great concern to the owners of a document. Every document includes digital information in some form or the other. Some of the information included may be pictures, others video etc. There is a need to protect these information from hackers. It is known that the hacker is always one step ahead of the creator. Cryptography and Stegenography are such scemes used where the former process the message and the later coceals the existence. These methods are not widely used since they are either less robust or partially robust to digital data modifications. Digital Watermarking was developed to achieve better robustness. A Watermark is a design impressed during creation and is used for copyright protection, data authentication, identifying the source, creator, owner, or authorised consumer of the document or image. It is also used to identify a document or an image that is modified or illegally distributed.

The general characteristics of Digital Image watermarking schemes are robustness, imperceptibility, capacity and security. Most of these characteristics are contradictory and make a

trade off to achieve robustness. The life cycle of a watermarking process includes embedding, attacking and extraction. In the course of literature studies, it is noted that several schemes to embed, detect and recover the watermark exist. These schemes adopted additive and multiplicative approaches in time domain. Different algorithms were developed adopting SS(Spread Spectrum)[6], DCT(Discrete Cosine Transform)[2], DFT(Discrete Fourier Transform), DWT(Discrete Wavelet Transform)[10], SVD(Singular Value Decomposition)[13], Ridgelets[19] and Contourlets[56] in frequency domain. Each scheme was evaluated for its performance by using image quality metrics such as Scaling, Cropping, AWGN (Additive White Gaussian Noise), PSNR (Peak Signal to Noise Ratio), SSIM (Structural Similarity Index Measure), Compression, Wrapping and Histogram Equalization. Although several such schemes performed well during evaluation there is still a need to develop more and more robust schemes due the rapid growth of the web technologies. In due course, it is also noted that some of the watermarking schemes can also be developed into protocols.

A watermark could be designed either for the source or for the destination. Watermarking at the source reduces piracy. Although most of them are designed for the source, some watermarking schemes are based for the destination instead of the source. While designing such watermarking schemes the features that were considered were transparency, robustness and capacity. Transparency here refers to the fact that the watermark be made visible in the image. It was also necessary to consider that the watermark stay unaltered when the imaged was illicitly tampered. As the number of watermarks increased, capacity could be defined as the ability to detect the watermarks with a low probability of error. The earliest techniques used were placing a watermark in the least significant bits or in the high frequency components. Such watermarks could be destroyed with simple quantization or low pass filtering. This process would sometimes affect or degrade the image quality.

2. FEATURES OF DIGITAL WATERMARKING SCHEMES

The following are some important features that a Digital Watermark exhibit.

1) **Robustness**- The watermark embedded must be robust refers to the capability of the watermark to survive a large number of signal processing operations, intentional and unintentional attacks.

2) **Imperceptibility**- Imperceptibility refers to the watermark being invisible to the HVS [Human Visual system]. This feature plays a vital role in content authentication.

3) **Security**- The watermark must be secure such that the hacker cannot remove the watermark. This can be accomplished by developing sophisticated algorithms and hence the watermark remains accessible only to authorized person.

4) **Verifiability**- The Watermark must be capable in determining ownership information.

5) **Computational Cost**- Computational simplicity is a feature that must be adopted so that the computational cost reduces.

6) **Watermark Detection**- Identifies the successful detection of the watermark at the detector end.

7) **Capacity**- Capacity describes how many information bits can be embedded. It can also be described as the possibility of embedding multiple watermarks.

8) **Tradeoff parameters**- There always exists a tradeoff between robustness, imperceptibility and capacity (Figure.1). Any watermarking scheme should be capable to overcome these tradeoffs.

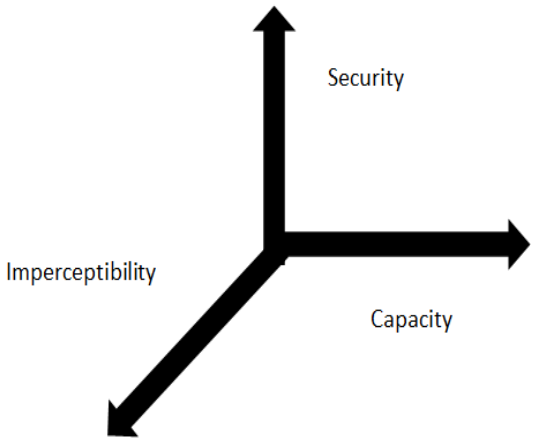

FIGURE 1: Tradeoffs in Digital Image Watermarking.

3. DIGITAL IMAGE WATERMARKING APPROACHES

In this section an attempt is made to classify watermarking schemes according to the characteristics of the embedded watermark.

3.1. Visible and Invisible Watermarking

Prior to 1998, watermarking schemes were widely classified as visible and invisible. A visible (perceptible) watermark is one which is visible to the HVS (Human Visual System). Visible watermarking scheme is that wherein a secondary image (watermark) is embedded into the primary image (host), such that the watermark is visible to the human eye. Huang and Tang[40] proposed a digital visible watermarking scheme wherein the intensity of the watermark was varied in the different regions of the image depending on the underlying content of the image and visual sensitivity to spatial frequencies. The proposed scheme modified the DWT coefficients of the host image. These schemes require large bit rates and strong strength than invisible watermarking schemes.

An invisible(imperceptible) watermark is one which is not visible to the HVS. Tzeng et al. [15] proposed a watermarking scheme which used optimization techniques to embed invisible watermarks in an image. It was assumed that any attack creates an invisible modification in the image. The proposed scheme was both blind and nonblind. The watermarked image was subjected to several blind attacks using programs like Photoshop Version 6, Photo impact Version 5 and malicious attacks like spreading noise, copy attacks and distortion. Invertibility and quasi-invertibility are such properties of invisible watermarking schemes for resolving the rightful ownership of the image. An invertible watermarking scheme is one that is susceptible to an attack that creates multiple claims of ownership for the same watermarked content. Noninvertible watermarking schemes, and subsequently the examples of such schemes are believed to be nonquasi-invertible as proposed by Craver *et.al* [1]. Wong and Memom [55] proposed a public watermarking scheme that could be made either visible or invisible based on the users choice for uncompressed images in spatial domain. This scheme could be further extended to compressed images in frequency domain too.

3. 2. Private and Public Watermarking

A private watermark can be detected by only authorized users i.e. normally the owner has private control over the watermark. Wang *et al.*[16] proposed an scheme in which they claimed that the owner had a private control over the watermark. Images were represented in vector form than in pixel format. Randomly generated orthonormal filter banks were used as private key. The watermark was embedded into the mid-frequency range, was invisible and robust to compression. The watermark was an image of real numbers obtained from wavelet coefficients. An algorithm was developed to scramble the watermark so that it differed from image to image. Piva *et al.* [37]

also proposed a public watermarking scheme, which did not need access to the original data for extracting the watermark.

3.3. Robust and Fragile Watermarking

Robust watermarks are generally used for copyright protection and ownership verification whereas fragile or semi-fragile watermarks are used in content authentication and integrity verification. Izquierdo and Guerra [21] proposed a block wise fragile watermarking scheme. Block wise watermarking was performed by partitioning the $N \times N$ image into small blocks A^k, where k = 1, 2…*l,* each of size $P \times Q$. The watermarked block was defined as À. The authentication procedure detected changes in À. The receiver of the image knew the secret keys to determine whether the block was authentic or fake. Zhao *et al.*[30] proposed a semi-fragile multipurpose watermarking scheme for cultural heritage imagery using DCT-DWT dual domain algorithm. The embedding process took place in Haar DWT domain and was generated in DCT domain. There was a trade-off in being robust to content preservation and the scheme was fragile towards malicious attacks. As will be discussed in the later sections, most of the watermarking schemes are robust.

3.4. Blind and Non-blind Watermarking

Blind watermarking schemes detect the watermark without accessing the original image. They require only the secret keys and are also public in nature. Nonblind watermarking schemes access the host image during the detection phase and are private in nature. Wong *et al.* [22] proposed multiple blind watermarking schemes for images namely SWE (Single Watermark Embedding), MWE (Multiple Watermark Embedding) and IWE (Iterative Watermark Embedding). SWE used two correlated secret keys to embed the watermark bit sequences into the image, MWE embedded multiple watermarks and minimized distortion energy, IWE embedded watermarks into JPEG compressed images. Another DCT based watermarking scheme was proposed by Chu [23] wherein the watermark was inserted in the sub images obtained by sub sampling. Lin *et al.* [45] also proposed a blind watermarking scheme for copyright protection. This method was based on the difference of the maximum wavelet coefficient and the second maximum wavelet coefficient to embed the watermark. Extraction of the watermark was done by designing a threshold value. It was noted by Meerwald *et al.* [50] that the above scheme had neglected security under intentional attack exploiting knowledge of implementation. Although modifications to the quantized coefficients location was adopted, the later too was prone to targeted attacks.

3.5 Spatial and Frequency Domain Watermarking

In Spatial domain, the watermark can be inserted into the host image by altering the pixel values of the host image while in frequency domain, the watermark is inserted into the coefficients of the transformed host image. Modasseri and Berger [39] have proposed an algorithm that was directly applied to the bit streams in compressed domain. The watermark was embedded into the bit stream as forced bit errors. Coltuc and Chassery [43] proposed another spatial domain watermarking scheme adopting reversible contrast mapping-an integer transform that applies to a pair of pixels. The watermark was embedded into the LSB's. This scheme seemed to be the lowest in computational capacity and was appropriate for real time applications. The approaches discussed later adopting DCT, DFT, DWT, ridgelets and contourlets are some frequency domain approaches.

4. FREQUENCY DOMAIN WATERMARKING APPROACHES

Watermarking algorithms have a long history dating prior to the 1990's. In this paper, the scope of review is limited to frequency domain techniques from the 1990's. A watermarking scheme suitable for one domain may not work well for the other. For example, fragile/semifragile watermarks are usually used for image authentication to verify whether the received image was modified during transmission or not, while robustness refers to content preservation.

Most of the work on robust digital watermarking was based on SS techniques. SS refers to a technique of transmitting a narrow bandwidth signal over a larger bandwidth. The signal energy

present over a wide range of frequencies was undetectable. During digital watermarking, the watermark was spread over a range of frequencies such that the energy in a single frequency range was so small that the watermark was not detected quiet easily. Such watermarks could be destroyed if high amplitude noise was added to all the frequency ranges. Applying frequency transformations to the data, significant regions of the spectrum could be highlighted. Any unintentional effects must not alter the significant regions of the spectrum else the image gets degraded. In order to place an n-length watermark into an $N \times N$ image, the $N \times N$ DCT of the image was computed and watermark was placed into the n highest magnitude coefficients (which are data dependent) of the DCT transformed image. Cox *et al.*[6] proposed a DCT-based spread spectrum watermarking technique. The watermark was developed from Gaussian distribution with zero mean and unit variance. The watermark was spread over all the frequencies and was not detectable since the energy in a single frequency was very small. This method was very popular and many early researchers adopted it. Altun *et al.* [47] considered optimal formulations of spread spectrum watermarking and proposed an algorithm for optimal embedding of the watermark that combined projections onto convex sets with a bisection parameter to determine the optimum watermarked image. They demonstrated optimal watermarking schemes to maximize its robustness to additive noise, compression, distortion minimizing the visibility of the watermark.

Podilchuk and Wenjun Zeng [2] have proposed two schemes based on a block- DCT framework where the typical block size for the DCT is 8×8. The two schemes are 1) a block-DCT scheme which has the advantage of direct watermark encoding of JPEG bit streams and 2) a wavelet-based scheme. The watermark encoder for the IA-DCT (Image Adaptive Discrete Cosine Transform) scheme is described by

$$X^*_{u,v,b} = \begin{cases} X_{u,v,b} + t^c_{u,v,b} w_{u,v,b} & \text{if } X_{u,v,b} > t^c_{u,v,b} \\ X_{u,v,b} & \text{otherwise} \end{cases} \quad (1)$$

where $X_{u,v,b}$ refers to the DCT coefficients, $X^*_{u,v,b}$ refers to the watermarked DCT coefficients, $w_{u,v,b}$ is the sequence of watermark values, and $t^c_{u,v,b}$ is the computed JND(Just Noticeable Difference) calculated from the visual model described by Watson [3].
The watermark insertion for IA-W (Image Adaptive Wavelet) is described by

$$X^*_{u,v,l,f} = \begin{cases} X_{u,v,l,f} + t^F_{l,f} w_{u,v,l,f} & \text{if } X_{u,v,l,f} > t^F_{l,f} \\ X_{u,v,l,f} & \text{otherwise} \end{cases} \quad (2)$$

where $X_{u,v,l,f}$ refers to the wavelet coefficient at position (u,v) in resolution level l and frequency orientation f, $X^*_{u,v,l,f}$ refers to the watermarked wavelet coefficient, $w_{u,v,l,f}$ is the watermark sequence, and $t^F_{l,f}$ corresponds to the computed frequency weight at level l and frequency orientation f for biorthogonal filters. The IA-DCT scheme was not robust to misalignments and JPEG compression while the IA-W scheme was comparatively robust. The watermark was embedded into DC components [54] in order to make the invisible watermark more robust by incorporating the feature of texture masking and luminance masking of HVS.

Kumsawat *et al.* [38] proposed spread spectrum watermarking scheme using discrete multiwavelet transform for copyright protection. Multiwavelets could simultaneously possess properties like orthogonality, symmetry and compact support. The watermark was embedded into the DMT (Discrete Multiwavelet Transform) coefficients by performing three level multiwavelet decomposition. Genetic algorithms were applied to achieve optimum performance. As discussed earlier, to reduce the probability of the watermark being detected the watermark signal must be

wide band and noise like. Chen and Leung [34] proposed a chaotic system to generate the noise-like signals. It was a nonlinear system and was robust to synchronization errors. An ergodic demodulator was developed to detect the chaotic watermark.

Furon and Duhamel [20] proposed an asymmetric watermarking scheme as an alternate to the SS approach. Another asymmetric approach was proposed by Kim *et al.*[31] which accommodated many embedded watermarks and had only one detection watermark. The proposed method adopted Phase Shift Transform and the watermark was embedded with reference keys. The detection was performed using a reference watermark.

Langelaar and Lagendigk [35] proposed the DEW (Differential energy watermarking) scheme. This scheme selectively discarded high frequency DCT coefficients in compressed domain. Hence the image was considered as a set of small blocks having size 8×8 . Each block was interpreted as a collection of 64 prequantized DCT coefficients. The set was then divided into different groups (*lc*- region) each containing blocks. A particular *lc*-region was divided into two sub regions A, B each containing n/2 blocks. Das *et al.*[36] presented two modifications for the DEW scheme. The first was where the energy difference was created by changes in low frequency DCT coefficients. The second was where a random permutation of blocks were used in such a way that in any *lc*-region, the energy of the *lc*-region A and B differ by a small quantity. The later scheme was more robust to the former scheme.

Watermarking modulation is a technique wherein the values of the transformed coefficients are replaced by watermark coefficients. Higher correlation values between the original image and the watermarked image indicates a genuine watermark. It was noted by Lu *et al.*[7] that this could be achieved if the transformed coefficients were along the same direction during the embedding and attacking process. They also noted that both [6] and [2] had adopted a random modulation technique. They had not considered the relationship between the signs of the modulation pair and hence they could not sustain most of the watermark attacking techniques. They proposed a complementary modulation strategy. Here, two watermarks which play complementary roles, in resisting various kinds of attacks were embedded. The cocktail watermark encoding algorithm proposed by them adopted complementary modulation rules and considered the sign of its wavelet coefficient and its watermarked value.

Lu and Liao [10] further adopted cocktail watermarking in another work where they embedded robust and fragile watermarks simultaneously that could be blindly extracted without access to host image. This was the first scheme which combined fragile and robust watermarking schemes. The host image's wavelet coefficients were quantized as masking threshold units. This method could not detect color changes if the color was modified. This could be overcome by randomly selecting positions among Y, Cb and Cr for watermarking. It was also noted that the watermark embedded using negative modulation was more robust to compression than that using positive compression. Liu and Chou [49] designed a robust and transparent scheme for color images. They transformed the host image into CIELAB color space, estimated the JND profile of the color components Y, C_b, C_r. These were used to embed the watermark by modulating the quantization indices of the coefficients in the significant portion of the color image. This scheme could be made more robust to malicious attacks and compression if the perceptual redundancy of color images was used to accurately locate embedding coefficients.

Lin and Chen [8] proposed a DCT watermarking scheme where the watermark of 64x64 was embedded into the LSB of the DCT coefficients of the host image. It was resilient to some image processing operations like cropping, uniform noise and JPEG compression to some degree. Unlike pseudo-random permutation of the watermark adopted by [8], Lu and Liao [9] used a watermark with visual recognizable patterns. The original image was decomposed into wavelet coefficients. Multi energy watermarking scheme based on qualified significant wavelet tree (QSWT) was used to achieve robustness against JPEG compression, image cropping, sharpening and median filtering. Suhail and Obaidat [29] too adopted DCT and proposed a scheme which was resistant to geometric manipulations and withstood cropping attacks. The

proposed scheme segmented the image based on Voronoi diagrams and the traditional pseudo random sequence was embedded in the DCT domain of each segment. Briassouli *et al.* [33] adopted symmetric alpha stable family of distributions to model the heavy tailed DCT coefficients. The watermark detector was designed based on Cauchy distribution. Cauchy detectors are robust in heavy tailed environments.

Solachidis and Pitas [11] proposed a watermarking scheme based on circularly symmetric watermarks applied in DFT domain. The authors considered a grey scale image I (n1, n2) of size $N \times N$.

The DFT of the image was given by

$$I(k_1,k_2) = \sum_{n_1=0}^{N_1-1}\sum_{n_2=0}^{N_2-1} i(n_1,n_2)e^{-j2\pi n_1 k_1/N_1 - j2\pi n_2 k_2/N_2} \qquad (3)$$

The magnitude and phase of the image were given by $M(k_1,k_2) = |I(k_1,k_2)|$ and $P(k_1,k_2)$ respectively. The watermark used, $W(k_1,k_2)$ was embedded in the DFT domain. Circular shifts in spatial domain did not affect the magnitude of the FT. It is also noted that scaling in spatial domain causes inverse scaling in frequency domain. Also rotation in spatial domain causes the same rotation in frequency domain. Since compression affected the high frequencies of FT, the watermark was added in the middle frequency range. This method was robust to filtering, noise addition, scaling, rotation, cropping and compression. It was also noted that there were practically zero errors since the detector output was always bigger than the chosen threshold for a watermarked image and smaller for a non watermarked image.

Tsui and Zhang [46] proposed two vector watermarking schemes, the Quaternion Fourier Transform (QFT) and Spatiochromatic DFT (SCDFT), done in the frequency domain of the chromatic components. The SCDFT utilizes chromatic information ignoring luminance which would result in destroying the watermark and was not robust. Using QFT the watermark was spread uniformly along the chromatic and luminance components of the image and was robust.

Initially, research in digital image watermarking had been focused on grey scale images. As technology advanced, extension to color images was done considering image luminance or processing each color channel independently. A DCT domain watermarking is proposed by [12] where the watermark is hidden by modifying the subset of DCT coefficients of each color channel. The first 'k' coefficients are skipped to obtain an improved invisible watermark. The watermark was casted three times to obtain high robustness. The RGB bands were extracted from a given image, the DCT of each band was computed and the coefficients recorded in zigzag pattern. Three vectors V_r, V_b, V_g were obtained and modified to embed the watermark. The modified vectors were reinserted in the zigzag scan of the corresponding channel and inverse DCT was performed to obtain the individual watermarked bands. This watermarking scheme provided a tradeoff between accuracy and effectiveness.

Singular Value Decomposition (SVD) watermarking scheme was proposed by Liu and Tan [13]. Here the SVD '$\mathbf{A}$' of an $N \times N$ image was computed to obtain two orthogonal matrices '$\mathbf{U}$', '$\mathbf{V}$' and a diagonal matrix '$\mathbf{S}$'. The watermark matrix '$\mathbf{W}$' was added into the matrix '$\mathbf{S}$' and SVD was performed on the new matrix to obtain '$\mathbf{U_w}$', '$\mathbf{V_w}$' and '$\mathbf{S_w}$. The watermarked image 'A_w' was then obtained by multiplying the matrices '$\mathbf{U}$', '$\mathbf{S_w}$', '$\mathbf{V_w}^T$' through the following steps

$$\mathbf{A} = \mathbf{U}\,\mathbf{S}\,\mathbf{V}^T \qquad (4)$$

$$\mathbf{S} + \boldsymbol{\alpha}\mathbf{W} = \mathbf{U_w}\mathbf{S_w}\mathbf{V_w}^T \qquad (5)$$

$$A_w = \mathbf{U}\,\mathbf{S_w}\mathbf{V}^T \qquad (6)$$

The watermark was extracted by reversing the above steps. For a given scale factor α, the error between the original and the watermarked image was controlled by the spectral norm of the watermark. This method was compared with [6] and it was found that the method was more robust than the later. This method was filed for patenting too due to its high robustness than [6]. Zhang and Li [41] stated that the extracted watermark using the above method was not the embedded watermark. It was the reference watermark. During watermark detection, the SVD matrices depend on the reference watermark which biases false detection.

Wavelet transforms are used in digital watermarking schemes. It is important to know how the wavelet transform can be used in watermarking schemes. The basic idea of the DWT for a two-dimensional image is described as follows. The image is first decomposed into four parts of high, middle, and low frequencies (i.e., LL1, HL1, LH1, HH1 subbands) by critically subsampling horizontal and vertical channels using subband filters, where LL1 represent approximate wavelet coefficients. The subbands labelled HL1, LH1, and HH1 represent the detail wavelet coefficients. To obtain the next coarser scaled wavelet coefficients, the sub- band LL1 is further decomposed and critically subsampled. This process is repeated several times and further, from these DWT coefficients, the original image can be reconstructed. This reconstruction process is called the Inverse DWT (IDWT). The coefficient computation is complicated and time consuming for a common wavelet filter and this can be overcome by using reversible wavelet transform that maps integers to integers [14] based on lifting framework. Lu and Liao [10] adopted wavelets in their cocktail watermarking scheme as discussed earlier. Wei *et al.*[5] proposed a method wherein the watermark was inserted in wavelet coefficients and its amplitudes were controlled by the wavelet coefficients so that the watermark noise did not exceed the JND of each wavelet coefficient. Celik *et al.*[44] proposed four different approaches for securely embedding spread spectrum watermarks at the client side using one time pads, stream switching, joint decryption and LUT(Look up Table) based ciphers.

Watermarking can be incorporated into image capture pipeline or geometric properties of an image. Geometric properties based watermarking schemes were still in the early areas of research during the 1990's. Tang and Hang [25] proposed a robust watermarking scheme that was robust to geometric distortion and signal processing attacks adopting Mexican Hat Wavelet Scale interaction for feature extraction. Other methods for feature extraction are the Harris detector and the Achard-Rouque adopted by Bas *et al.*[26].

The Marr wavelet [27], [28] is rotation invariant. The mother wavelet function is defined by

$$\psi(\overrightarrow{x}) = (2 - \left\|\vec{x}\right\|^2 e^{-\left\|\vec{x}\right\|^2/2}, \quad \text{where } \left\|\vec{x}\right\| = \left(x^2 + y^2\right)^{1/2} \tag{7}$$

The 2D FT is given by

$$\psi^*(\overrightarrow{k}) = \left\|\vec{k}\right\|^2 \; e^{-k\left\|\vec{k}\right\|^2/2} \tag{8}$$

where $\left(\vec{k}\right)$ represents the 2D spatial frequency.

The feature extraction method uses the following quantities

$$P_{i,j}\left(\vec{k}\right) = \left|M_i\left(\vec{x}\right) - \gamma . M_j\left(\vec{x}\right)\right| \tag{9}$$

$$M_i\left(\vec{x}\right) = \left(2^{-i}\psi(2^{-i}.\vec{x}\right) * A \tag{10}$$

where $M_i(\overrightarrow{x})$ represents the response of the Mexican Hat Wavelet Filter. $P_{i,j}(\overrightarrow{k})$ is the interaction between scales *i* and *j* with γ as the scaling factor. The scheme was designed for both color and grey scale images. The Wavelet filtering was adopted using FFT. Marr wavelet allows for different degrees of robustness against distortion, cropping affects only few feature points, and is band limited reducing noise sensitivity problem in feature extraction.

The embedding process is outlined as follows

- The feature extraction method generated reference centers of disks.
- Image normalization was done to select the location for the watermark.
- Coordinate transformation coefficients between original normalized images were generated.
- Location of blocks in original image for watermarking was determined from the normalized image.
- The coordinates were transformed from normalized image to original image.
- A 2D FFT was applied to each disk and the watermark was embedded in Transform domain.
- 2D IFFT was performed on the watermarked blocks to replace the original image blocks.

A secret key was used in the watermark detection process. It was concluded that the scheme can be further improved if the feature points were more robust under severe geometric distortions.

Liu and Chou [49] utilized the color features of the HVS to design the watermarking scheme. Dejey and Rajesh [24] adopted Discrete Wavelet Transform-Fan Beam Transform (DWT-FBT) and proposed two nonblind color image watermarking schemes. The first was a wavelet fan beam watermarking on luminance and chrominance and the other, wavelet fan beam watermarking on chrominance only. The proposed schemes provided for a trade off on capacity, robustness and imperceptibility. The schemes were robust to blurring, sharpening and histogram equalization attacks.

Bi *et al.*[42] used Mallet's Multiband Discrete Wavelet Transform and Empirical Mode Decomposition and proposed a blind watermarking scheme. Selecting a dilation factor $M \geq 2$, 1D scaling and a wavelet filter $H_l(\xi)$, $0 \leq l \leq M-1$, the original image was decomposed. The watermark bits were embedded in suitable sub images. The robustness of the watermark was tested against JPEG compression, Black and White Noise, Gaussian Noise, ConvFilter and rotation scaling effects. Multiwavelet watermarking was robust against compression attacks, cropping and scaling. Wavelets are suitable for attacks on the mid frequencies against multiwavelets for low and high frequency ranges.

Bhatnagar et *al.*[62] applied fractional wavelet packet transform(FRPWT) in digital watermarking. The host image was decomposed using fractional wavelet packet transform and a grey scale image was used as the watermark compared to the previous randomly generated Guassian Noise. A secret key known only to the creator was used to change the frequency bands at all sublevels. The reference image was obtained by inverse fractional wavelet transform. Since FRPWT depends on the transform order all along the axis to decompose and reconstruct the image, this method was more robust and secure to copyright protection. This method avoided ambiguity problem faced by SVD methods. This method was tested on host images of size 256 x 256 and the watermark size was 64 x 64.

Sparse representation of an image could be achieved by DCT or DWT. Wavelets performed well for 1D piecewise smooth functions. Higher order wavelets could not see the smoothness along the edges. Contourlets represent image edges sparsely, employ iterative filter banks and allow for different number of directions at each scale. [56] – [60] proposed contourlets based watermarking schemes. These schemes adopted directional information of images edges. Akhaee et al. [61] proposed a multiplicative watermarking approach in contourlet domain. The proposed blind watermarking scheme was robust to AWGN and compression attacks.

Ridgelets [17]-[18] deal with line singularity issues faced in 2D wavelets. Kalantari et al. [19] proposed a robust watermarking method in the ridgelet domain. To adapt to curved edges, the image is partitioned into blocks so that the curved edge formed a straight edge. The watermark is inserted into the blocks with high entropy by modifying the amplitude of the ridgelet coefficients. The distribution of the ridgelet coefficients is unknown. Due to this a host distribution independent

decoder working near the optimal point is used. To achieve maximum robustness the decoder is optimized by taking into consideration the Guassian noise attack.

Curvelets is another multiscale transform developed by Candues *et al.* [64]. This transform could efficiently represent edges and singularities along curves. Curvelets also have the capability of better recovery under noisy circumstances. Leung *et al.*[63] adopted curvelets and proposed a watermarking scheme leading to the addition of a HVS adopting the orientation parameter of the curvelets. The proposed scheme is robust against image processing methods. Zhang *et al.* [65] proposed a multipurpose blind watermarking scheme adopting multiscale curvelet transform. Here, single level watermark was embedded onto the significant coefficients by quantization in individual frequency scales. The coefficient selection is done on the concept, that, the coefficient energy was proportional to its sensitivity. This scheme provided for image authentication and copyright protection and was robust to Gaussian low pass filtering, contrast enhancement and Gaussian noise contamination.

Besides watermark embedding, optimum recovery of the watermark is important for all applications. Several techniques have been proposed to recover the watermark. Barni *et al.* [52] addressed the problem of watermark recovery. The architecture of an optimum decoder for an additive/ multiplicative watermark embedded in the DFT domain was derived by relying on Baeyes Decision theory. A statistical analysis to model the DFT coefficients was used to derive the actual structure of the decoder and the decoder was further simplified. Bian and Liang [53] proposed a watermark detector that applied Bessel K PDF which performed well even on weak watermarks. Most of the schemes described above adopted inverse transform to extract the watermark efficiently.

5. EVALUATING WATERMARKS

Initially most of the watermarking techniques adopted a different test series, different images, and different methodologies. It was highly difficult to obtain a comparative description without reimplementing and testing them separately. But the implementation would be quiet different due to the change in test benches, which would further suggest sometimes weaker implementation or mismatches in the results. Hence, evaluation methodologies were required with common benchmarks. This would result in a less detailed table of results along with a reliable summary of the proposed schemes.

5.1. Performance Evaluation Metrics

Petitcolas and Fabien [51] stated that the first step of the evaluation procedure is to identify the target of evaluation algorithms. A full scheme evaluation is the collection of functionality services to which a level of assurance is globally applied and for each of which a specific level of strength is selected. Six to seven levels of assurances are globally accepted. Levels of perceptibility ranges from not perceptible to slightly perceptible to completely perceptible. Assurance levels to access perceptibility are through human perceptual models. Another metric is to consider geometric distortions. Detection probabilities of the watermark and bit error rate measurements are the accessing parameters for robustness. The level of robustness ranges from no robustness to provable robustness. Robustness is also tested with a random payload of a given size, if the application size is fixed. Speed is a parameter that varies from hardware to software implementations. Difference in statistical properties of the original and the watermarked image leads to detection attacks. Very few watermarking schemes consider this criterion.

In brief, the following are some quality measures to evaluate the performance of watermarked images. The two most important metrics are PSNR and BER. Others include MSE and SSIM.

1) **PSNR**- Peak Signal to Noise Ratio determines the quality of the recovered watermark.

   $$PSNR = 10 \log_{10} \left(\frac{N \times N}{MSE} \right) \qquad (11)$$

   where N=peak signal value of the original signal

2) **BER** – Bit Error Ratio is the number of error bits in the overall bits received. This metric compares the host image and the watermarked image.

$$BER = \frac{C}{H \times W} \quad (12)$$

where H and W represent the height and width of the watermarked image. C indicates the number of bits received in error.

Transform Adopted	Concept & Details	Results & Summary
SS	Watermark is distributed over a wide range of frequencies	Larger bandwidth is required to transmit a narrow bandwidth signal. Not robust against high amplitude noise.
DCT	Watermark is spread over a range of frequencies and hence not detectable	Not robust to misalignments and compression attacks.
DFT	Watermark is added in the mid frequency ranges	Robust to filtering, noise addition, scaling compression, rotation and cropping attacks.
DWT	Watermark is embedded in mid frequency ranges	Orthogonal and symmetrical, reconstruction. Perform well for 1D functions. Comparatively robust to misalignments and compression attacks, geometric distortions, signal processing attacks, histogram equalisation attacks.
Multiwavelets	Watermark is embedded into low and high frequency ranges.	Robust against compression, cropping and scaling.
Contourlets	Watermark can be embedded along different direction of the curved edges	Robust to AWGN and compression attacks.
Ridgelets	Deal with line singularity issues faced in 2D wavelets	Maximum robustness against Gaussian noise attacks
Curvelets	Can represent edges and singularities along curves	Better recovery under noise conditions. Robust to Gaussian low pass filtering, contrast enhancement and noise contamination.
Shearlets	Multiscale geometric analysis, high frequency ranges	Performed well compared to DCT and DWT

TABLE 1: Comparative Study of Frequency Domain Watermarking Schemes.

3) **SSIM** – Used to measure the similarity between two images as an improvement on PSNR and MSE. This metric is calculated on various windows of an image. Consider two windows *p,q* of size N X N, then

$$SSIM = \frac{\left(2\mu_p\mu_q + C_1\right)\left(2\sigma_{pq} + C_2\right)}{\left(\mu_p^2 + \mu_q^2 + C_1\right)\left(\sigma_p^2 + \sigma_q^2 + C_2\right)} \quad (13)$$

where

- μ_p , μ_q is the average of *p* and *q respectively*
- σ_p^2 is the variance of *p*
- σ_q^2 is the variance of q

- σ_{pq}^{2} is the covariance of p and q
- C_1 and C_2 are variables used to stabilize the denominator

4) **MSE** – Mean Square Error is defined as average squared difference between the reference image and the distorted image.

$$\text{MSE} = \frac{1}{pq}\left[\sum_{i=1}^{p}\sum_{j=1}^{q}\left(N(i,j)-W(i,j)\right)^{2}\right] \quad (14)$$

Where,

p and q = height and width of the image respectively,

$N(i,j)$ = pixel values of the original image

and $W(i,j)$ = pixel values of the watermarked image.

5.2. Watermarking Attacks

The watermarked image is subjected to various attacks. Boato *et al.* [48] proposed the first benchmarking tool to evaluate watermarking robustness based on GA (Genetic Algorithms). Robustness was evaluated in terms of perceptual quality measured by WPSNR (Weighted Peak Signal to Noise Ratio). The watermarked image was subjected to JPEG2000 compression, AWGN, resizing and amplitude scaling. The attacks to which a watermarked image is subjected can be broadly classified as intentional and non-intentional attacks. Hartung et al.[66] classified attacks as simple attacks(noise addition, cropping, compression), disabling attacks(geometric distortion, rotation, cropping), ambiguity attacks and removal attacks. In this section we describe intentional and non-intentional attacks in brief.

1) Compression Attacks- During compression using JPEG and JPEG2000 standards, lossy compression techniques produce irreversible changes to the watermarked images wherein the watermark may become fragile whilst lossless compression techniques are more robust in recovering the watermark.

2) Interference Attacks- These attacks add noise to the watermarked image. Salt and pepper noise, denoising, averaging, AGWN etc.

3) Signal Processing Attacks- These attacks include lossy compression, linear, nonlinear and adaptive filtering, denoising and noise addition.

4) Geometric Attacks- Most of the watermarking techniques is not robust to geometric attacks. These attacks are rotation, cropping, flipping, scaling, row-column removal and resizing.

5) Cryptographic Attacks- The security of the system can be determined by detecting the weakness in the code, cipher, protocols and the management entrapping the system. These attacks include cipher text only, plain text only and chosen text that can be chosen plaintext or chosen cipher text.

6) Collusion Attacks- Such attacks are common where the attacker has access to more than one copy of the watermarked image. The attacker can predict the watermark by colluding them. These attacks can be linear or nonlinear. They are powerful due to their capability of achieving their objective and the degradation is very low.

7) Active Attacks – These attacks are those that try to break the system. They tend to alter the watermark or remove the watermark. These are done by viruses.

8) Passive Attacks- These attacks look at sensitive information which can be subjected to other attacks.

9) Histogram Equalization attacks- These attacks normally tend to enhance image intensities. These include brightness, contrast adjustments.

A brief summary of the watermarking schemes is given in Table 1. A comparative analysis on watermarking attacks using Fractional Wave Packet Transform is depicted in Table 2. The image considered is Lena (256 X256) and the watermark used is the Logo.

Attack	No Attack	Median Filtering	Salt and Pepper Noise	Gaussian Filter
PSNR	50.491	22.256	35.7823	28.181

TABLE 2: PSNR for various attacks

6. CONCLUSION

Embedding the watermark in low frequency components is robust to low pass filtering, compression and geometric attacks while embedding the watermark in high frequency components is robust to histogram equalization and geometric attacks. A multitransform approach, wherein the watermark can be embedded in both the high frequency and low frequency components dealing with line singularities is left as an open area for research to achieve maximum robustness. An attacker having multiple copies of the watermarked image can remove the watermark by collusion attack. A watermarking scheme which is transparent, robust to geometric distortions and collusion attacks can be designed by adapting multiwavelets.

A watermarking scheme that is robust to desynchronisation attacks is still a challenging issue. It is noted that most of the watermarking schemes could resist rotation, scaling, translation and other affine transforms but very few were resilient to cropping attacks. There exists a trade-off between imperceptibility and robustness, and imperceptibility and capacity. In the process of designing a robust watermark, it is necessary to consider collusion attacks which are still an open area for researchers. Hence, digital watermarking is an interesting area which provides an open space for research.

7. REFERENCES

[1] Craver, S.; Memon, N.; Boon-Lock Yeo Yeung, M .M., "Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implications," IEEE Journal on Selected Areas in Communications, vol.16, no.4, pp.573-586, May 1998.

[2] Podilchuk, C.I.;Wenjun, Zeng, "Image-adaptive watermarking using visual models," IEEE Journal on Selected Areas in Communications, vol.16, no.4, pp.525-539, May1998.

[3] Watson A. B., “DCT quantization matrices visually optimized for individual images,” in Proc. SPIE Conf. Human Vision, Visual Processing, and Digital Display IV, vol. 1913, pp. 202– 216, Feb. 1993.

[4] Chiou-Ting Hsu; Ja-Ling Wu, "Multiresolution watermarking for digital images," IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, vol.45, no.8, pp.1097-1101, Aug 1998.

[5] Wei, Z.H.; Qin, P.; Fu, Y. Q., "Perceptual digital watermark of images using wavelet transform," IEEE Transactions on Consumer Electronics, vol.44, no.4, pp.1267-1272, Nov 1998.

[6] Cox I. J.; Kilian J.; Leighton F. T.; and Shamoon T., “Secure spread spectrum watermarking for multimedia,” IEEE Transactions on Image Processing, vol. 6, pp. 1673–1687, 1997.

[7] Chun-Shien Lu; Shih-Kun Huang; Chwen-Jye Sze; Hong-Yuan Mark Liao, "Cocktail watermarking for digital image protection," IEEE Transactions on Multimedia, vol.2, no.4, pp.209-224, Dec 2000.

[8] Lin, S.D.; Chin-Feng Chen, "A robust DCT-based watermarking for copyright protection," IEEE Transactions on Consumer Electronics, vol.46, no.3, pp.415-421, Aug 2000.

[9] Ming-Shing Hsieh; Din-Chang Tseng; Yong-Huai Huang, "Hiding digital watermarks using multiresolution wavelet transform," IEEE Transactions on Industrial Electronics, vol.48, no.5, pp.875-882, Oct 2001.

[10] Chun-Shien Lu; Liao, H.Y.M., "Multipurpose watermarking for image authentication and protection," IEEE Transactions on Image Processing, vol.10, no.10, pp.1579-1592, Oct 2001.

[11] Solachidis, V.; Pitas, I., "Circularly symmetric watermark embedding in 2-D DFT domain," IEEE Transactions on Image Processing, vol.10, no.11, pp.1741-1753, Nov 2001.

[12] Barni, M.; Bartolini, F.; Piva, A., "Multichannel watermarking of color images," IEEE Transactions on Circuits and Systems for Video Technology, vol.12, no.3, pp.142-156, Mar 2002.

[13] Ruizhen Liu; Tieniu Tan, "An SVD-based watermarking scheme for protecting rightful ownership", IEEE Transactions on Multimedia, vol.4, no.1, pp.121-128, Mar 2002.

[14] Chen, Tao; Wang, Jingchun, "Image Watermarking method using integer-to-integer wavelet transforms", Tsinghua Science and Technology , vol.7, no.5, pp.508-512, Oct. 2002.

[15] Jengnan Tzeng; Wen-Liang Hwang; I-Liang Chern, "Enhancing image watermarking methods with/without reference images by optimization on second-order statistics," IEEE Transactions on Image Processing, vol.11, no.7, pp.771-782, Jul 2002.

[16] Yiwei Wang; Doherty, J.F.; Van Dyck, R.E.,"A wavelet-based watermarking algorithm for ownership verification of digital images,” IEEE Transactions on Image Processing, vol.11, no.2, pp.77-88, Feb 2002.

[17] Do, M.N.; Vetterli, M., "The finite ridgelet transform for image representation," IEEE Transactions on Image Processing, vol.12, no.1, pp.16-28, Jan 2003.

[18] E. J. Candès and D. L. Donoho, “Ridgelets:Akey to higher-dimensional intermittency?,” Phil. Trans. R. Soc. Lond. A., pp. 2495–2509, 1999.

[19] Kalantari, N.K.; Ahadi, S.M.; Vafadust, M., "A Robust Image Watermarking in the Ridgelet Domain Using Universally Optimum Decoder," IEEE Transactions on Circuits and Systems for Video Technology, vol.20, no.3, pp.396-406, March 2010.

[20] Furon, T.; Duhamel, P., "An asymmetric watermarking method," IEEE Transactions on Signal Processing, vol.51, no.4, pp.981-995, April 2003.

[21] Izquierdo, E.; Guerra, V., "An ill-posed operator for secure image authentication," IEEE Transactions on Circuits and Systems for Video Technology, vol.13, no.8, pp.842-852, Aug 2003.

[22] Wong, P.H.; Au, O.C.; Yeung, Y. M., "Novel blind multiple watermarking technique for images," IEEE Transactions on Circuits and Systems for Video Technology, vol.13, no.8, pp.813-830, Aug. 2003.

[23] Chu, W.C., "DCT-based image watermarking using subsampling," IEEE Transactions on Multimedia, vol.5, no.1, pp.34-38, March 2003.

[24] Dejey. R. S.; Rajesh, D.; “Robust discrete wavelet fan beam Transforms based color image watermarking”, IET Transactions on Image Processing, vol 5, no 4, pp315–322.

[25] Chih-Wei Tang; Hsueh-Ming Hang, "A feature-based robust digital image watermarking scheme," IEEE Transactions on Signal Processing, vol.51, no.4, pp.950-959, Apr 2003.

[26] P. Bas, J. M. Chassery, and B. Macq, “Robust watermarking based on the warping of pre-defined triangular patterns,” Proc. SPIE Security and Watermarking of Multimedia Contents- II, vol. 3971, pp. 99–109, 2000.

[27] J.P. Antoine and P. Vandergheynst, “Two-dimensional directional wavelets in image processing,” International. J. Image. Syst. Technol., vol. 7, pp. 152–165, 1996.

[28] D. Marr, Vision. San Francisco, CA: Freeman, pp. 54–61, 1982.

[29] Suhail, M.A.; Obaidat, M.S., "Digital watermarking-based DCT and JPEG model," IEEE Transactions on Instrumentation and Measurement, vol.52, no.5, pp.1640-1647, Oct. 2003.

[30] Yang Zhao; Campisi, P.; Kundur, D., "Dual domain watermarking for authentication and compression of cultural heritage images," IEEE Transactions on Image Processing, vol.13, no.3, pp.430-448, March 2004.

[31] Tae Young Kim; Hyuk Choi; Lee, Kiryung; Kim, Taejeong, "An asymmetric watermarking system with many embedding watermarks corresponding to one detection watermark," IEEE Signal Processing Letters, vol.11, no.3, pp.375-377, March 2004.

[32] Bao, P.; Xiaohu Ma, "Image adaptive watermarking using wavelet domain singular value decomposition," IEEE Transactions on Circuits and Systems for Video Technology, vol.15, no.1, pp.96-102, Jan. 2005.

[33] Briassouli, A.; Tsakalides, P.; Stouraitis, A., "Hidden messages in heavy-tails: DCT-domain watermark detection using alpha-stable models," IEEE Transactions on Multimedia, vol.7, no.4, pp.700-715, Aug. 2005.

[34] Siyue Chen; Leung, H., "Ergodic chaotic parameter modulation with application to digital image watermarking," IEEE Transactions on Image Processing, vol.14, no.10, pp.1590-1602, Oct. 2005.

[35] Langelaar, G.C.; Lagendijk, R.L., "Optimal differential energy watermarking of DCT encoded images and video," IEEE Transactions on Image Processing, vol.10, no.1, pp.148-158, Jan 2001.

[36] Das, T.K.; Maitra, S.; Mitra, J., "Cryptanalysis of optimal differential energy watermarking (DEW) and a modified robust scheme," IEEE Transactions on Signal Processing, vol.53, no.2, pp.768-775, Feb. 2005.

[37] Piva A.; Barni M.; Bartolini F.; and Cappellini V., “DCT-based water- mark recovering without resorting to the uncorrupted original image,” in Proc. IEEE Int. Conf. Image Processing, vol. 1, pp. 520–523, Oct. 1997.

[38] Kumsawat, P.; Attakitmongcol, K.; Srikaew, A., "A new approach for optimization in image watermarking by using genetic algorithms," IEEE Transactions on Signal Processing, vol.53, no.12, pp.4707-4719, Dec. 2005.

[39] Mobasseri, B.G.; Berger, R.J., "A foundation for watermarking in compressed domain," IEEE Signal Processing Letters, vol.12, no.5, pp.399-402, May 2005.

[40] Biao-Bing Huang; Shao-Xian Tang, "A contrast-sensitive visible watermarking scheme," IEEE Transactions on MultiMedia, vol.13, no.2, pp.60-66, April-June 2006.

[41] Xiao-Ping Zhang; Kan Li, "Comments on "An SVD-based watermarking scheme for protecting rightful Ownership", IEEE Transactions on Multimedia, vol.7, no.3, pp.593-594, June 2005.

[42] Ning Bi; Qiyu Sun; Daren Huang; Zhihua Yang; Jiwu Huang, "Robust Image Watermarking Based on Multiband Wavelets and Empirical Mode Decomposition," IEEE Transactions on Image Processing, vol.16, no.8, pp.1956-1966, Aug. 2007.

[43] Coltuc, D.; Chassery, J. M., "Very Fast Watermarking by Reversible Contrast Mapping", IEEE Signal Processing Letters, vol.14, no.4, pp.255-258, April 2007.

[44] Celik, M.U.; Lemma, A.N.; Katzenbeisser, S.; Van der Veen, M., "Lookup-Table-Based Secure Client-Side Embedding for Spread-Spectrum Watermarks", IEEE Transactions on Information Forensics and Security, vol.3, no.3, pp.475-487, Sept. 2008.

[45] Wei-Hung Lin; Shi-Jinn Horng; Tzong-Wann Kao; Pingzhi Fan; Cheng-Ling Lee; Yi Pan, "An Efficient Watermarking Method Based on Significant Difference of Wavelet Coefficient Quantization", IEEE Transactions on Multimedia, vol.10, no.5, pp.746-757, Aug. 2008.

[46] Tsz Kin Tsui; Xiao-Ping Zhang; Androutsos, D., "Color Image Watermarking Using Multidimensional Fourier Transforms", IEEE Transactions on Information Forensics and Security, vol.3, no.1, pp.16-28, March 2008.

[47] Altun, H.O.; Orsdemir, A.; Sharma, G.; Bocko, M.F., "Optimal Spread Spectrum Watermark Embedding via a Multistep Feasibility Formulation", IEEE Transactions on Image Processing, vol.18, no.2, pp.371-387, Feb. 2009.

[48] Boato, G.; Conotter, V.; De Natale, F. G B; Fontanari, C., "Watermarking Robustness Evaluation Based on Perceptual Quality via Genetic Algorithms", IEEE Transactions on Information Forensics and Security, vol.4, no.2, pp.207-216, June 2009.

[49] Liu, K. C.; Chou, K. H.; “Robust and transparent watermarking scheme for color images”, IET transactions on Image Processing, vol 3, no. 4, pp.228–242.

[50] Meerwald, P.; Koidl, C.; Uhl, A., "Attack on “Watermarking Method Based on Significant Difference of Wavelet Coefficient Quantization”, IEEE Transactions on Multimedia, vol.11, no.5, pp.1037-1041, Aug. 2009.

[51] Petitcolas; Fabien A. P., "Watermarking schemes evaluation", IEEE Signal Processing Magazine, vol.17, no.5, pp.58,64, Sep 2000.

[52] Barni, M.; Bartolini, F.; De Rosa, A.; Piva, A., "A new decoder for the optimum recovery of nonadditive watermarks", IEEE Transactions on Image Processing, vol.10, no.5, pp.755-766, May 2001.

[53] Bian, Y.; & Liang, S., “Locally Optimal Detection of Image Watermarks in the Wavelet Domain Using Bessel K Form Distribution”, IEEE Transactions on Image Processing, vol.22, no.6, pp.2372–2384, June 2013.

[54] Jiwu Huang; Shi, Y.Q.; Yi Shi, "Embedding image watermarks in dc components", IEEE Transactions on Circuits and Systems for Video Technology, vol.10, no.6, pp.974-979, Sep 2000.

[55] Wong, P.W.; Memon, N., "Secret and public key image watermarking schemes for image authentication and ownership verification", IEEE Transactions on Image Processing, vol.10, no.10, pp.1593-1601, Oct 2001.

[56] M. Jayalakshmi; S. N. Merchant; and U. B. Desai, "Digital watermarking in contourlet domain", in Proc. 18th Int. Conf. Pattern Recognition, 2006, vol. 3, pp. 861–864.

[57] M. Jayalakshmi; S. N. Merchant; and U. B. Desai, "Blind watermarking in contourlet domain with improved detection," Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06).

[58] Xueqiang, L.; Xinghao, D.; and Donghui, G., "Digital watermarking based on non-sampled contourlet transform," in Proc. IEEE Int.Workshop Anti-counterfeiting, Security, Identification, pp. 138–141, 2007.

[59] Li, H.; W, Song; and Wang, S., "A novel blind watermarking algorithm in contourlet domain," in Proc. 18th Int. Conf. Pattern Recognition, vol. 3, pp. 639–642, 2006.

[60] Xiao S.; Ling H.; Zou F.; and. Lu, Z., "Adaptive image watermarking algorithm in contourlet domain," Proc. Japan-China Joint Workshop on Frontier of Computer Science and Technology, pp. 125–130, 2007.

[61] Akhaee, M.A.; Sahraeian, S.M.E.; Marvasti, F., "Contourlet-Based Image Watermarking Using Optimum Detector in a Noisy Environment," IEEE Transactions on Image Processing, vol.19, no.4, pp.967- 980, April 2010.

[62] Bhatnagar,G.; Raman,B.; Wu,Q.M.J., "Robust watermarking using fractional wavelet packet transform", IET Transactions on Image Processing, vol 6, no.4, pp.386-397, June 2012.

[63] Leung, H.Y.; Cheng, L.M.; Cheng, L.L., "Digital Watermarking Schemes using Multiresolution and Curvelet and HVS Model", Proceedings of 8th International Workshop, IWDW 2009, Guildford, UK, vol 5703, pp 4-13, August 24-26, 2009.

[64] Candès E. J.; Demanet, L.; Donoho, D. L.; and Ying, L., "Fast discrete curvelet transforms," Tech Rep., Appl. Comput. Math., California Inst. Technol., 2005. [On line]. Available: http://www.curvelet.org.

[65] Chune Zhang; Cheng, L. L.; Zhengding Qiu; Cheng, L.M., "Multipurpose Watermarking Based on Multiscale Curvelet Transform," IEEE Transactions on Information Forensics and Security, vol.3, no.4, pp.611-619, Dec. 2008.

[66] F. Hartung; J. K. Su; B. Girod, "Spread spectrum watermarking: Malicious attacks and counterattacks," pp. 147-158, 1999.

[67] Khalifa, O.O.; Binti Yusof, Y.; Abdalla, A.H.; Olanrewaju, R.F., "State-of-the-art digital watermarking attacks," 2012 International Conference on Computer and Communication Engineering (ICCCE), pp.744-750, July 2012.