Chapter-2

Review of Literature

2.1 Introduction

A number of digital watermarking algorithms have been proposed for embedding watermark in digital media like audio, video and images. In this Chapter, a review of existing digital image watermarking methods is given. In first part of this Chapter, review of frequency and spatial domain watermarking techniques is given. In its second part, review of feature point-based watermarking techniques is given. Third part of the Chapter covers the review of ZMs-based watermarking techniques. In fourth part of this Chapter, review of fragile and semi-fragile watermarking techniques is described. Finally, a review of other watermarking techniques based on Singular Value Decomposition (SVD), edge points and SS is given.

2.2 Frequency domain watermarking techniques

In frequency domain watermarking techniques, watermark can be inserted by modifying transform coefficients of the transformed host image. The methods developed in this domain are robust and are used for copyright protection applications. The transformations that are commonly used in watermarking are DCT, DFT and DWT. A few other transformations that have been used in watermarking are Fourier-Millen transform, Hadamard transform and Radon transform etc. The review of few frequency domain watermarking techniques is given as under.
2.2.1 Review of DFT-based watermarking techniques

The Fourier transform is the representation of an image as a sum of complex exponentials of varying magnitudes, frequencies, and phases. The Fourier transform plays a critical role in a broad range of image processing applications, including enhancement, analysis, restoration, and compression [40] [41].

A 2-dimensional discrete DFT \( F(u, v) \) of \( M \times N \) size image function \( f(x, y) \) for \( x = 0, 1 \ldots M-1 \) and \( y = 0, 1 \ldots N-1 \) is defined using Eq. (2.1)

\[
F(u, v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y)e^{-j2\pi(ax/M+by/N)}
\]  

(2.1)

where \( u \) and \( v \) are the frequency variables that lies in range of \( 0 \) to \( M-1 \) and \( 0 \) to \( N-1 \) respectively. \( F(u, v) \) is a complex-valued function.

From the given Fourier transform function \( F(u, v) \), image function \( f(x, y) \) can be computed by applying Inverse Discrete Fourier Transform(IDFT) using Eq. (2.2).

\[
f(x, y) = \frac{1}{M} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u, v)e^{j2\pi(ux/M+vy/N)}
\]  

(2.2)

where \( x \) and \( y \) lies in range of \( 0 \) to \( M-1 \) and \( 0 \) to \( N-1 \) respectively.

C.Y. Lin et. al [42] have proposed a watermarking algorithm that is robust to RST distortions. The watermark is embedded into a 1-dimensional signal obtained by first taking the Fourier transform of the image, resampling the Fourier magnitudes into log-polar coordinates, and then summing a function of those magnitudes along the log-radius
axis. In this method, authors have observed that if the image is rotated, the resulting signal is cyclically shifted. If it is scaled, the signal is multiplied by some value. And if the image is translated, the signal is unaffected.

**A.K. Kaushik et. al [43]** have proposed a novel design of a DFT-based digital watermarking system for images. In this technique, first of all, the original host image is splitted into the blocks then DFT transform is applied on each block. Then the Arnold scrambling is used to change the binary watermark and generate two unrelated pseudo-random sequences that are embedded in DFT domain of the transformed image and inverse DFT is applied to get watermarked image. The advantage of this method is that it is sufficiently robust and imperceptible.

**I. Djurovic et. al [44]** have proposed an image watermarking technique in the Fractional Fourier Transformation (FRFT) domain. This approach uses combination of the space and spatial/frequency domains, without introducing the multidimensional Radon-Wigner distribution. The FRFT is the rotation of the signal for an arbitrary angle in the time-frequency plain. This watermarking technique is robust against some important attacks like noise and cropping.

**E. Ganic et. al [45]** have defined that DWT and DCT domain watermarking schemes are not robust to geometric attacks such as rotation, scaling, and translation and proposed a DFT-based watermarking technique. In their paper, they have generalized a circular watermarking scheme by embedding one watermark in lower frequencies, and another in higher frequencies. Through experiments they have shown that if the circular watermark is embedded in higher frequencies, the percentage of false negatives is higher for one group of attacks (i.e., JPEG, Gaussian noise, blurring, and resizing), and lower for
another group of attacks (i.e., histogram equalization, contrast adjustment, gamma correction, scaling, rotation and cropping). Similarly, if the circular watermark is embedded in lower frequencies, the percentage of false negatives is lower for one group of attacks (i.e. JPEG, Gaussian noise, blurring, and resizing), and higher for another group of attacks (i.e. histogram equalization, contrast adjustment, gamma correction, scaling, rotation, and cropping).

**C. Zhu et. al** [46] have proposed a digital watermarking algorithm for Digital Elevation Model (DEM) data to protect their copyright. Their algorithm is based on the Human Visual System (HVS) and DFT. In this method, firstly, the location of watermarking is ascertained adaptively according to the features of DEM data. Then, the watermark information is embedded to the low frequency of the texture region. Finally, the DEM data is transformed by DFT and the data with watermarking information is obtained. Through experiments authors have demonstrated that their proposed algorithm not only satisfies the watermark transparency requirement, but also has little effect on the DEM elevation, the slope and the contour. In addition to this, their algorithm is robust to the some noise attacks.

The advantage of DFT over DCT and DWT is that DFT is RST invariant. Also the phase component of DFT is noise invariant, thus to achieve noise invariance, phase of DFT coefficients can also be used in watermarking. Inspite of the RST invariance of DFT, it is seldom used in watermarking because of its high computation complexity over DCT and DWT. **C.V. Serdean et. al** [47] have mentioned that both phase and amplitude of DFT are sensitive to compression attack.
2.2.2 Review of DWT-based watermarking techniques

DWT is the transformation that transforms the signals in time domain to a joint time-frequency domain. The key advantage of wavelet transform over fourier transform is temporal resolution i.e. it captures both frequency and location information (location in time). In Fourier transformation, we could get information about the frequencies present in a signal, but not where and when the frequencies occurred. In DWT, the wavelet is a little piece of a wave where a sinusoidal wave (as is used by Fourier transforms) carries on repeating itself within a finite domain. A wavelet transform involves convolving the signal against particular instances of the wavelet at various time, scales and positions. The wavelet transform is also called as joint time-frequency domain.

The Wavelet transform decomposes a signal into a set of basis functions. These basis functions are called wavelets. The wavelet transform is computed separately for different segments of the time-domain signal at different frequencies [48].

To compute the wavelet transform of an image $f(x, y)$, a 2-dimensional scaling function $\phi(x, y)$ and three 2-dimensional wavelets $\psi^H(x, y)$, $\psi^V(x, y)$ and $\psi^D(x, y)$ are required that are computed using Eq. (2.3) through Eq.(2.6) respectively [41] [48].

\[
\phi(x, y) = \phi(x)\phi(y) \quad (2.3)
\]

\[
\psi^H(x, y) = \psi(x)\phi(y) \quad (2.4)
\]

\[
\psi^V(x, y) = \phi(x)\psi(y) \quad (2.5)
\]

\[
\psi^D(x, y) = \psi(x)\psi(y) \quad (2.6)
\]
In Eq. (2.4), Eq. (2.5) and Eq. (2.6), wavelet functions measure the intensity variation for images along columns i.e. horizontal edges, along rows i.e. vertical edges and along diagonals respectively.

It is clear from Eq.(2.3) through Eq. (2.6) that in order to computed 2-dimensional scaling and wavelet function, product of 1-dimensional scaling and wavelet functions is used that is computed using Eq. (2.7) and Eq.(2.9) respectively.

\[
\phi_{j,k}(x) = 2^{j/2} \phi (2^j x - k)
\]  

(2.7)

where \( j, k \in \mathbb{Z} \), \( k \) determines the position of \( \phi_{j,k}(x) \) along the x-axis and \( j \) determines width of \( \phi_{j,k}(x) \). Value of \( \phi(x) \) in Haar Wavelet transform is computed using Eq.(2.8).

\[
\phi(x) = \begin{cases} 
1 & 0 \leq x < 1 \\
0 & \text{otherwise}
\end{cases}
\]  

(2.8)

The wavelet function is defined using Eq.(2.9).

\[
\psi_{j,k}(x) = 2^{j/2} \psi (2^j x - k)
\]  

(2.9)

where \( \psi(x) \) is defined using Eq. (2.10).

\[
\psi(x) = \begin{cases} 
1 & 0 \leq x < 0.5 \\
-1 & 0.5 \leq x < 1 \\
0 & \text{otherwise}
\end{cases}
\]  

(2.10)

Using the scaling and wavelet function defined in Eq.(2.7) and Eq.(2.9) , DWT of an image of size \( M \times N \) is defined using Eq. (2.11) and Eq. (2.12) respectively.
\[ W_\phi(j_0, m, n) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \phi_{j_0,m,n}(x, y) \] (2.11)

\[ W_\psi(j, m, n) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \psi_{j,m,n}(x, y) \] (2.12)

where \( i = \{H, V, D\} \) defines intensity variation along horizontal, vertical and diagonal direction. Value of \( j_0 \) is an arbitrary starting scale and \( W_\phi(j_0, m, n) \) coefficients define an approximation of image function \( f(x, y) \) at scale \( j_0 \) and the function \( W_\psi(j, m, n) \) coefficients add horizontal, vertical and diagonal details for scale \( j \geq j_0 \).

As shown in Fig. 2.1, four sub bands LL, HL, LH and HH are generated after applying 1-level DWT on input image.

From the given DWT function, image function \( f(x, y) \) can be computed by applying Inverse Discrete Wavelet Transform (IDWT) using Eq. (2.13).

\[ f(x, y) = \frac{1}{\sqrt{MN}} \sum_m \sum_n W_\phi(j_0, m, n) \phi_{j_0,m,n}(x, y) + \frac{1}{\sqrt{MN}} \sum_{i=HVD} \sum_m \sum_n W_\psi(j, m, n) \psi_{j,m,n}(x, y) \] (2.13)

DWT performs Multi Resolution Analysis (MRA) i.e. it analyzes the signal at different frequencies giving different resolutions. MRA is designed to give good time resolution and poor frequency resolution at high frequencies. At lower frequencies it gives good
frequency resolution and poor time resolution. DWT is good for signal having high frequency components for short duration and low frequency components for long duration like images and video frames.

S. Shahraeini et. al [49] have proposed a blind watermarking algorithm based on fractal model in discrete wavelet domain for copyright protection. The authors have presented an idea to hide a binary image as a watermark with fractal parameters in wavelet domain of host image. In this technique, fractal compression technique is used to encode a gray image and fractal codes are embedded into the wavelet coefficients of the gray image according to well-connected watermark algorithm. The authors have shown that their algorithm is robust against JPEG compression attack.

M. Barni et. al [50] have presented a watermarking algorithm operating in the wavelet domain. In contrast to conventional methods operating in the wavelet domain, in this technique, masking is accomplished pixel by pixel by taking into account the texture and the luminance content of all the image sub bands. The watermark consisting of a pseudorandom sequence is adaptively added to the largest detail band and is detected by
computing the correlation between the watermarked coefficients and the watermarking code.

**K. Wang et. al** [51] have presented a hierarchical watermarking framework for semi-regular meshes. This framework is based on wavelet transform of the semi-regular mesh. In this technique, three watermarks are inserted in different appropriate resolution levels obtained by wavelet decomposition of the mesh. The robust watermark is inserted by modifying the norms of the wavelet coefficient vectors associated with the lowest resolution level, the fragile watermark is embedded in the high resolution level obtained just after one wavelet decomposition by modifying the orientations and norms of the wavelet coefficient vectors and the high-capacity watermark is inserted in one or several intermediate levels by considering groups of wavelet coefficient vector norms as watermarking primitives. The advantage of this technique is that robust watermark inserted in it is able to resist all common geometric attacks even with a relatively strong amplitude, the fragile watermark is robust to content-preserving operations, while being sensitive to other geometric attacks.

**K. Hameed et. al** [52] have defined that DWT has a number of advantages over other transform such as progressive and low bit-rate transmission, quality, scalability, region-of-interest coding demand, more efficient and versatile image coding that can be exploited for both image compression and watermarking applications.

**N. Kashyap et. al** [53] have implemented a robust image watermarking technique for copyright protection based on 3-level DWT. In this technique, a multi-bit watermark is embedded into the low frequency sub-band of a host image by using alpha blending.
technique. This method has more imperceptibility as compared to 1-level and 2-level watermarking technique.

A. H. Ali et. al [54] have proposed an effective, robust, and an inaudible audio watermarking algorithm. This algorithm is effective due to the application of a cascade of two powerful mathematical transforms i.e. DWT and SVD.

S. Ramakrishnan et. al [55] have developed a hybrid image watermarking algorithm which satisfies both imperceptibility and robustness requirements. The authors have used singular values of wavelet transformation’s HL and LH sub bands to embed watermark. To increase and control the strength of the watermark, scale factor is used. A secret embedding key is used in this method to securely embed the fragile watermarks. It is also robust to counterfeiting attacks, even when the malicious attackers are fully aware of the watermark embedding algorithm. This technique is sensitive to image operations such as JPEG compression and malicious image attacks and thus, can be used for semi-fragile watermarking.

J. Husseind et. al [56] have presented a robust video watermarking method. In this method, data is embedded to the specific bands in the wavelet domain using motion estimation approach. HL and LH bands of DWT are used to add the watermark where the motion in these bands does not affect the quality of extracted watermark if the video is subjected to different types of malicious attacks. Watermark is embedded in an additive way using random Gaussian distribution in video sequences. This watermarking method has strong robustness against some attacks such as frame dropping, frame filtering and lossy compression.
H. A. Abdallah et. al [57] have presented a wavelet-based scheme for digital image watermarking. This watermark embedding scheme is blind, as it requires neither the original image nor any side information to recover the watermark. It is based on inserting the watermark bits into the coarsest scale wavelet coefficients. 3-level wavelet decomposition and a watermark of size equal to the detail sub-bands in the coarsest scale are used in this method. Only perceptually significant wavelet coefficients are used to embed the watermark bits. This scheme differs from the traditional wavelet-based schemes in the use of quantization and non-additive watermark embedding. It produces watermarked images with less degradation than the traditional wavelet-based schemes.

M. M. Sathik et. al [58] have proposed an inventive watermarking scheme. According to this technique, the low frequency sub band of wavelet domain and the rescaled version of original image are utilized in the watermark construction process. A scrambled version of watermark is obtained with the help of Arnold Transform. The operation of embedding and extraction of watermark is done in high frequency domain of DWT since small modifications in this domain are not perceived by human eyes. This watermarking scheme deals with the extraction of watermark information without any requirement of original image.

The advantages of using DWT in watermarking are:

1. DWT-based watermarking techniques support high capacity.

2. DWT allows watermark to be inserted in both local region and global region of the image due to which it is robust against scaling and cropping.

3. Computation complexity of DWT is less as compared to DFT.
Inspite of the above advantages, DWT have a few drawbacks. According to S.Lagzian [59], DWT does not provide shift invariance due to down sampling of its sub bands. Also the cost of computing DWT as compared to DCT may be higher. The complexity of calculating wavelet transform depends on the length of the wavelet filters, which is at least one multiplication per coefficient. Computation of DWT coefficients uses floating-point calculations and demands longer data length which increases the cost of computation.

2.2.3 Review of DCT-based watermarking techniques

DCT is transformation that linearly transforms data into the frequency domain, where the data can be represented by a set of coefficients. It represents an image as a sum of sinusoids of varying magnitudes and frequencies [40]. The advantage of DCT is that the energy of the original data or most of the visually significant information about the image is concentrated in only a few low frequency components of DCT depending on the correlation in the data. For this reason, DCT is often used in image compression applications.

The DCT coefficients $B(p, q)$ for an image of size $M \times N$ is defined using Eq.(2.14).

$$B(p, q) = \alpha_p \alpha_q \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \cos \frac{\pi (2x+1)p}{2M} \cos \frac{\pi (2y+1)q}{2N}$$  \hspace{1cm} (2.14)

where $0 < p \leq M-1$ and $0 < q \leq N-1$. 

47
\[ \alpha_p = \begin{cases} 1/\sqrt{M}, & p = 0 \\ 2/\sqrt{M}, & 1 \leq p \leq M - 1 \end{cases} \quad \text{and} \quad \alpha_q = \begin{cases} 1/\sqrt{N}, & q = 0 \\ 2/\sqrt{N}, & 1 \leq q \leq N - 1 \end{cases} \tag{2.15} \]

From the given DCT function, image function \( f(x, y) \) can be computed by applying Inverse Discrete Cosine Transform (IDCT) using Eq. (2.16)

\[
f(x, y) = \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} \alpha_p \alpha_q B(p, q) \cos \left( \frac{(2x+1)p}{2M} \right) \cos \left( \frac{(2y+1)q}{2N} \right) \tag{2.16}
\]

where \( 0 < x \leq M - 1 \) and \( 0 < y \leq N - 1 \).

**R. M. Zhao et al [60]** have presented a blind digital image watermarking algorithm in the DCT domain, in which an average value of DCT coefficient is set as a threshold that is used in watermark embedding process. In the process of embedding, the watermark image is processed by Arnold transformation and the host image is divided into some blocks that are transformed into coefficients in the DCT domain. The average value of coefficients selected from the same location in DCT blocks is calculated and the selected coefficients in each DCT block are modified into a value which is not less than the negative threshold or not more than the positive threshold. This method has good imperceptibility and is robust against the common image processing operations such as JPEG compression, filtering, noise contamination, cropping and scaling.

**A.K. Naik et al [61]** have presented an efficient blind digital image watermarking algorithm using mapping technique. In this algorithm, an entire image or pattern is directly embedded into the original image. The embedding process is based on changing the selected DCT coefficients of the host image to odd or even values depending on the
binary value of watermark DCT coefficients. This method offers a significant advantage of providing biometric image compression and authentication without introducing any significant degradation in the image quality. Moreover this watermarking scheme is blind and does not require any additional data for watermark extraction.

H. Elazhary et. al [62] have proposed a blind watermarking technique for grayscale images in the DCT domain. In this technique, the authors have used the combination of three techniques: Torus Automorphism (TA) permutation, a pseudo-random number generator, and visual cryptography to achieve high degree of robustness against intentional attacks. Here, the host image is divided into blocks of size $4 \times 4$ pixels and TA permutation is used to disarrange the watermark bits. Then a pseudo-random number generator is used to determine the sequence of host image blocks for embedding the permuted watermark bits. The robustness against unintentional attacks is achieved in this method by watermarking the low frequency DCT components and also by utilizing the more relative values of these low frequencies instead of their absolute values. This technique is very robust against several types of unintentional attacks including: median filtering, blurring, sharpening, Gaussian noise addition, salt and pepper noise addition, and JPEG compression.

A. N. Gindy et. al [63] have proposed a blind and robust watermarking technique for embedding watermark information into the host image. In this technique, watermark information is embedded in sixteen low-frequency band coefficients of the DCT sub-blocks. In this method, watermark is embedded by changing the selected DCT-coefficients of the host image to odd or even values depending on the bit value of binary watermark.
Y. Li et. al [64] have proposed an adaptive blind watermarking algorithm based on compressed DCT and Watson’s visual mode. A normalized masking deduced from Watson’s model according to the principle of maximum possible quantization error, is used in this algorithm to simplify the computation for watermark insertion. Watermark information is adaptively embedded in the host image based on the deduced masking and relationship of four-adjacent-blocks. Arnold transformation is used in it to encrypt the watermark signal with a secret key and the watermark is extracted without the original image. This technique is also resistant to Gaussian noise, mean filter, JPEG compression etc.

S. Saryazdi et. al [65] have proposed a blind watermarking scheme in which the host image is first divided into $4 \times 4$ non-overlapping blocks. For each block, first five AC coefficients of its DCT are estimated using Discrete Cosine (DC) coefficients of its neighbor blocks. A gray-level watermark is then added into estimated values. Since watermark insertion process used in this method does not change the DC coefficients, therefore watermark is extracted by estimating AC coefficients (computed using DC coefficients of neighbor blocks) of $4 \times 4$ blocks of watermarked image and then comparing them with their actual values. The advantage of this technique is that it has high capacity and is robust against noise attack.

W.Y. Chen et. al [66] have proposed digital image watermarking technique in which a watermark is embedded in the host image by DCT transform. In this technique, the lower-band coefficient of DCT blocks are used to embed the watermark, thus it is robust against the JPEG compression attack. In order to improve imperceptibility, the authors have suggested embedding of only one bit in each coefficient of a DCT block.
G. Zhu et. al [67] have proposed a watermarking technique based on the DC components. In their algorithm, watermark is embedded by adjusting the DCT coefficients of the host image. The host image is divided into blocks of 8×8 pixels, then these blocks are further subdivided into four non-overlapping blocks of 4×4 pixels, and the watermarks are embedded by adjusting their DCT coefficients. This technique is highly robust against various attacks.

L. Parameswaran et. al [6] have proposed a novel approach for content-based watermarking for image authentication that is based on Independent Component Analysis (ICA). In this approach, ICA is applied to blocks of the host image to determine mixing matrix that represents the features of image blocks. The Frobenius norms of the mixing matrix are taken as the content-based features of the host image. These features are embedded as watermark in a mid-frequency DCT coefficient of a block. This watermark authentication technique is robust against incidental image processing operations, but is able to detect malicious tampering and locate the tampered regions.

B. Chandramohan et. al [68] have presented a novel oblivious and robust multiple image watermarking scheme using Multiple Descriptions (MD) and QIM of the host image. In this technique, watermark is embedded in two stages. In the first stage, host image is decomposed into two descriptions, one with odd pixel intensities and the other with even pixel intensities. Then DCT of the odd and even descriptions is computed and DC coefficients of all the blocks of odd description are modified as per watermark bits. The second description is used for reference at extraction time. In the second stage, a copy of the watermark is again embedded in the watermarked image generated at the first stage using DCT coefficients modification with QIM. This achieves robustness against
both local and global attacks. This algorithm is highly robust against different attacks on the watermarked image and returns high PSNR and NC. The advantage of using DCT in watermarking is that DCT-based watermarking techniques are robust against compression, as DCT coefficients are compression invariant. Also the computation complexity of DCT is very low as compared to DFT and DWT. But the drawback of DCT is that it is not RST invariant.

2.2.4 Review of hybrid watermarking techniques

As each of the transform has its own pros and cons, researchers have developed a few hybrid transform-based watermarking techniques in which combination of more than one transformations are used to embed watermark in robust manner.

D. Sudiana et. al [69] have presented three watermarking schemes based on SVD, combined DFT-SVD, and DCT-SVD. In the first scheme, both of insertion and extraction process are directly computed using SVD. In the combined schemes, after applying the DFT and DCT to the host image, authors have mapped the DCT and DFT coefficients into four quadrants. A zig-zag and unzig-zag algorithm is then applied in DCT-SVD. The advantage of this technique is its robustness against Gaussian blur, Gaussian noise, JPEG compression, and rescaling. The authors have analyzed that the watermark embedding technique based on DFT-SVD scheme is more robust to Gaussian noise and rescaling attack. Whereas, for JPEG compression attack, SVD and DCT-SVD schemes are more robust as compared to DFT-SVD schemes.

S. Wang et. al [70] have described a blind method for inserting invisible watermark into host image by using DM technique in a dual-transform domain. In this method,
watermark is embedded into a digital image that uses two layers of orthogonal transforms, pseudorandom data shuffling and a dither modulation technique. Two layers of 2-dimensional orthogonal transforms are applied in this method (DCT and DFT), before dither modulation. Prior to DFT, the candidate DCT coefficients are pseudo-randomly shuffled to remove correlation between adjacent data points. The watermark embedded according to this technique is sufficiently transparent and robust. The authors have found a tradeoff between invisibility, robustness, and embedding capacity that has been achieved by appropriately choosing the system parameters and the candidate coefficients for embedding.

2.2.5 Review of other transform-based watermarking techniques

In the literature of digital image watermarking, a number of transformations other than DCT, DFT and DWT have also been used for embedding watermark in transform domain. Review of such watermarking techniques is given as under.

M. Malkin et. al [71] have proposed a watermarking technique based on the Randlet transform. Randlet transform is a transform that is based on randomly-chosen basis functions. Due to the randomized nature of the transform, it is used in watermarking applications, particularly in the cases where security against an attacker in covering the watermark is desired. This method is also robust against perceptually insignificant image modifications including malicious attacks. In this method, watermark is embedded by quantizing the values of Randlet transform coefficients.

C. Zhang et. al [72] have described a watermarking method which is suitable for both copyright protection and information hiding. They have presented a method based on the
morphological mathematics properties of the Mojette transform and the Mojette Phantoms. In their proposed technique, the mojette phantoms are used not only as the embedded watermark, but also used as the mark which are inscribed with certain meaningful information and then embedded in the host image. The watermark embedded with this method is robust against various attacks.

I. Usman et. al [73] have presented a lossless reversible data hiding method using Integer Wavelet Transform and Genetic Programming (GP) based intelligent coefficient selection scheme. In this method, GP is used to embed watermark in the host image using amplitude of the wavelet coefficients and their sub bands, and returns an imperceptible watermarked image. In this method, information is embedded into the least significant bit-plane of those high frequency wavelet coefficients that are intelligently selected by the GP module. This approach not only extracts the hidden information, but also recovers the original image content. The advantage of this technique is that this technique is very effective in terms of both high capacity and imperceptibility.

S. P. Maity et. al [74] have proposed a digital image watermarking scheme using the characteristics of the HVS, spread transform technique and statistical information measure. In this method, spread transform scheme is implemented using the transform coefficients of both the host and the watermark signal. Watermark embedding strength is adaptively adjusted using frequency sensitivity, luminance, contrast and entropy masking of HVS model. The Hadamard transform is used in this watermarking technique to transform the host image into frequency domain. This technique has higher image fidelity, greater reliability of watermark detection and higher data hiding capacity at high degree of compression.
T.S.H. Anthony et. al [75] have proposed a robust and efficient digital image watermarking algorithm using the fast Hadamard transform for the copyright protection of satellite images. In their proposed method, an entire image or pattern such as a company’s logo or trademark is embedded directly into the original satellite image as a watermark. In this method, watermark is inserted into Hadamard coefficients of sub-blocks of the original host image. The advantage of Hadamard transform is that it has more useful middle and high frequency bands, for hiding the watermark, as compared to other high coding gain transforms like DCT at high noise environment. DCT coefficients are suitable for watermarking when the channel noise is low but in high noise environment, the Hadamard transform bands remain intact. The authors have evaluated the performance of their method on the Stirmak benchmark and found that this method is 60% robust against all Stirmark attacks. Due to the simplicity of the fast Hadamard transform, their method has less time complexity and ease of hardware implementation.

2.3 Review of spatial domain watermarking techniques

In spatial domain watermarking techniques, watermark is embedded directly in the host image by modifying intensity of selected pixels. These techniques are very sensitive against geometric as well other signal processing attacks, hence are preferred to be used in fragile and semi-fragile watermarking techniques. Review of a few spatial domain watermarking techniques is as under.

B. Surekha et. al [76] have proposed three public image watermarking techniques. The first one, called Single Watermark Embedding (SWE) that used the concept of Visual Cryptography (VC) to embed a watermark into a digital image. The second one, called
Multiple Watermarks Embedding (MWE) in which SWE is extended to embed multiple watermarks simultaneously in the same host image. Finally, in Iterative Watermark Embedding the same binary watermark is iteratively embedded in different positions of the host image, to improve the robustness. In VC method, the original image is divided into two shares such that, each pixel in the original image is replaced with a non-overlapping block of two sub-pixels. Anyone who holds only one share will not be able to reveal any information about the watermark. Here, the watermark is not embedded physically into the digital image. Instead, this method constructs a public share and a private share to embed and extract a binary watermark from the host image. The authors have shown that their techniques satisfy all the properties of digital watermarking such as invisibility, security, capacity and low computational complexity.

S.P. Maity et. al [77] have proposed a computationally efficient and blind digital image watermarking technique. In watermark insertion process, average brightness of the homogeneity regions of the cover image is used for watermark embedding. Spatial mask of suitable size is used to hide data with less visual impairments. The selection of the required block is based on variance of the block and watermark insertion exploits average brightness of the blocks. Using experiments, the authors have shown the resiliency of their scheme against large blurring attack like mean and Gaussian filtering, non linear filtering like median, image rescaling, symmetric image cropping, lower order bit manipulation of gray values and lossy data compression like JPEG with high compression ratio and low PSNR values.

C. Obimbo [78] have proposed LSB-based watermarking technique in which secret information is embedded in an image by modifying least significant bit in spatial domain.
This method offers better performance in terms of capacity, invisibility and robustness through an image-adapting coding.

2.4 Review of feature point and descriptor-based watermarking techniques

One of the common watermark attacks that removes or destroys the watermark information from a watermarked image is synchronization attack. Under this attack, position of watermark is changed due to some geometric operation like translation or rotation. To avoid the effect of synchronization attack, RST invariant feature points are used in watermarking process to select the location where the watermark information is to be embedded. A review of feature point-based watermarking techniques is given as under.

Y.D. Pan et. al [79] have combined the features (relation of coefficients) in DCT domain with content features (edges or texture) of JPEG image into multi-features, which are useful to authenticate the images from both spatial and frequency domains. The authors have proposed a novel invertible data embedding mechanism. They have empirically shown that their algorithm is sensitive to intended tampers while accepting appropriate JPEG compression, and further can locate corrupted areas. As compared to conventional authentication scheme based on features extracted from single domain, the probability of “miss alarm” in this method is lower.

H. Lee et. al [80] have addressed a novel, robust and blind watermarking method for digital images using local invariant features. The authors have proposed a watermarking method that is robust to geometric distortions. In order to resist geometric distortions,
authors have used a local invariant feature of the image called the Scale Invariant Feature 
Transform (SIFT) which is invariant to translation and scaling distortions. The watermark 
is inserted into the circular patches generated by the SIFT. Rotation invariance is 
achieved using the translation property of the polar-mapped circular patches. This method 
is robust against geometric distortion attacks as well as signal-processing attacks.

L. Verstrepen et. al [81] have described a synchronization system based on SIFT feature 
points. These points are characterized as being a localized feature containing semantic 
information of the image and can usually be retrieved after the image is attacked. The 
authors have used a more robust SIFT algorithm for feature point detection called Global 
SIFT and an adaptation of the circular spatial watermarking algorithm using mean QIM 
method. This method has high detection rate and robustness of the watermarks after 
geometric attacks.

V.R. Doncel et. al [82] have extended an existing algorithm which achieves polygonal 
line watermarking by modifying the Fourier descriptors magnitude in an imperceptible 
way. Watermarks embedded by this technique can be detected in rotated, translated or 
scaled polygonal lines. The detection of such watermarks is carried out through a 
correlator detector. The authors have analyzed the statistics of the Fourier descriptors to 
devise an optimal blind detector. This method is highly imperceptible and robust.

P. Bas et. al [83] have presented a new approach for watermarking of digital images 
providing robustness to geometrical distortions. The authors have classified the 
geometrical distortions into two classes: global transformations such as rotations and 
translations and local transformations such as the Stirmark attack. The authors have 
proposed an embedding and detection scheme where the watermark is bound with a
content descriptor defined by salient points. The embedding of the signature is done by extracting feature points of the image and performing a Delaunay tessellation on the set of points. The watermark is embedded using a classical additive scheme inside each triangle of the tessellation. The detection is done using correlation properties on the different triangles. The authors have empirically proved that their scheme is robust to different manipulations.

H.Y. Lee et. al [84] have addressed the problem of content-based synchronization for robust watermarking. The authors have reviewed representative content-based approaches and proposed a new synchronization method based on SIFT method. The SIFT is invariant to noise, spatial filtering, geometric distortions, and illumination changes of the image.

Z. Wenyin et. al [85] have presented a multilevel, semi-fragile spatial watermarking method based on Local Binary Pattern (LBP) operators by using the local pixel contrast for the embedding and extraction of watermarks. Authors have empirically shown that their watermarking method is robust against commonly-used image processing operations, such as additive noise, luminance change, contrast adjustment, color balance, and JPEG compression. It also achieved good invisibility, fragility, and image tamper detection and localization with less computational cost.

D.H. Im et. al [86] have presented a blind watermarking algorithm for vector graphic images. Their algorithm is resilient to both global and local geometrical distortions. In this method, the polygonal line is represented by the wavelet descriptor and an additive watermarking scheme is used to embed the watermark by slightly modifying the wavelet descriptor that caused invisible distortions to the coordinates of the vertices. The authors
have demonstrated that their algorithm outperforms the algorithm based on the Fourier descriptor.

**C. Li et. al [87]** have proposed a novel scheme to protect biometric templates using LBP-based authentication watermarking. In this scheme, the m-LSBs of biometric templates are set to zeros. Then, the modified biometric templates are partitioned into non-overlapping image blocks. The LBP feature of these image blocks are obtained, and the authentication watermark bits are generated from these features. A series of message patterns are generated according to authentication watermark bits. In order to resist vector quantization attack and collage attack, each message pattern is embedded into the m-LSB of another image block which is selected by a position sequence. The authors have proved that their algorithm maintained recognition rate in the template-based authentication system and it not only has superior localization and security, but also tolerates low-noise pollution while maintaining sensitivity to malicious manipulations.

**R. Krishnamoorthi [88]** have proposed an invisible digital watermarking algorithm with orthogonal polynomials based transformation for copyright protection of digital images. In this algorithm, a visual model is utilized to determine the watermarking strength necessary to invisibly embed the watermark in the mid frequency AC coefficients of the cover image, chosen with a secret key. The visual model is designed to generate a just noticeable distortion mask by analyzing the low level image characteristics such as textures, edges and luminance of the cover image in the orthogonal polynomials based transformation domain. As the secret key is required for both embedding and extraction of watermark, it is not possible for an unauthorized user to extract the embedded
watermark and hence it is secure. This scheme is robust to common image processing distortions like filtering, JPEG compression and additive noise.

2.5 Review of Zernike moments-based watermarking techniques

From the literature review made for spatial and transform domain watermarking techniques, it is observed that DCT and DWT-based watermarking techniques are not rotation invariant. DFT is rotation invariant but its computation complexity is very high and it is sensitive to the compression attack. Similarly, spatial domain watermarking techniques are not very robust against RST attacks. Thus, researchers have analyzed the importance of ZMs and have used them to embed watermark information in robust manner and recover the watermark at low BER and achieve high imperceptibility. Although the ZMs computation is very time consuming, C. Singh et. al [89][90][91] have proposed the algorithms for fast computation of ZMs and have used ZMs in various application areas like image retrieval [92], face recognition[93][94], edge detection[95]. A review of few watermarking techniques based on ZMs is given as under.

Q. Chen et. al [96] have proposed an image watermarking system based on ZMs. This is because the magnitudes of ZMs have the desirable invariance property against image rotation. ZMs can be employed as watermark signal to achieve robustness against image rotation. Based on whether the image is RST attacked or not, two watermark detection algorithms are proposed by the authors. The first algorithm can reconstruct the embedded watermark with the ZMs vector extracted from the testing image if it does not undergo any RST attacks. The second algorithm extracts the feature vector in the form of
magnitudes of ZMs from the testing image and employs the Mean Square Reconstruction Error (MSRE) to detect the watermark.

S.W. Foo et. al [97] have proposed a novel feature-based image watermarking scheme based on ZMs which have invariance properties. In this scheme, feature points are first extracted from host image and several circular patches centered on these points are generated. The patches are used as carriers of watermark information because they can be regenerated to locate watermark embedding positions even when watermarked images are severely distorted. Local ZMs are then calculated for these patches. DM is adopted to quantize the magnitudes of these moments followed by false alarm analysis. This scheme is very robust against image processing operations and geometric attacks.

S. Xiang et. al [98] have analyzed that the audio ZMs in lower orders are very robust to common signal processing operations, such as MPEG compression, low-pass filtering, etc. Based on these observations, authors have proposed a robust watermark scheme by embedding the bits into the low-order moments. By analyzing and deducting the linear relationship between the audio amplitude and moments, watermark is embedded in low-order moments in time domain by scaling sample values directly. In this method, audio Zernike transform is performed by mapping audio into 2-D form. The authors have empirically shown that their algorithm achieves robust performance due to the superiorities of low-order moments exploited for watermarking.

I.A. Ismail et. al [99] have employed a robust image-watermarking algorithm using accurate ZMs. The moments are computed in polar coordinates, where both approximation and geometric errors are removed. Accurate ZMs are used in image watermarking and are proved to be robust against different kind of geometric attacks. The
authors have empirically proved that the accurate ZMs achieve higher degree of robustness than those approximated ones against rotation, scaling, flipping, JPEG compression and affine transformation. They have also concluded that by computing accurate ZMs, the embedded watermark bits can be extracted at a low error rate.

X. Kang et. al [100] have proposed a fast watermark resynchronization method based on ZMs, which requires only search over scaling factor to combat RST geometric distortion and significantly reduces the computation load. The authors have applied the proposed method to circularly symmetric watermarking. The authors have defined that according to the theorem they have used and the rotation invariance property of ZMs, the rotation estimation only requires performing DFT on ZMs correlation value once. Thus for RST attack, both rotation angle and scaling factor can be estimated by searching for the scaling factor to find the overall maximum DFT magnitude. With the estimated rotation angle and scaling factor parameters, the watermark can be resynchronized. In watermark detection, the normalized correlation between the watermark and the DFT magnitude of the test image has been used. This technique is robust to global RST distortion as well as JPEG compression. The authors have found that in their proposed technique, the watermark is robust to print-rescanning and randomization-bending local distortion in Stirmark 3.1.

Y. Xin et. al [101] have proposed a multi-bit geometrically robust image watermarking algorithm using ZMs. In this method, some ZMs of an image are selected, and their magnitudes are dither-modulated to embed an array of bits. The watermarked image is obtained via reconstruction from the modified moments and those left unmodified. In watermark extraction process, the embedded bits are estimated from the invariant
magnitudes of the ZMs using a minimum distance decoder. In this method, the hidden message can be decoded at low error rates. The method is found to be robust against image rotation, scaling, flipping and a variety of other distortions such as lossy compression.

X. Yao et. al [102] have proposed a content-based authentication scheme for tampering detection and localization of binary images. In their proposed method, the watermark is generated by the feature vector of the original binary image, and embedded back into the image by a structural method. This feature vector is the set of ZMs of the host image. It can tell the degree of the tamper in the binary image. The watermarked image is authenticated by comparing the distance between the extracted watermark and the feature vector of the test image. Once the tampering is detected, the tampered areas are located by comparing different components of the distance.

H. Liu et. al [103] have proposed a content-based semi-fragile watermarking algorithm for image authentication. In this technique, ZMs of the image are used to generate feature vector. The watermark is generated by quantizing the magnitude of these ZMs and is then embedded into DWT sub bands. As it is usually hard to locate the tampered area by using global features in the content-based watermarking scheme, in this technique authors have proposed a structural embedding method to locate the tampered areas by using the separability of ZMs-based feature vector. Due to use of the semi-fragilities of the feature vector and the watermark, this authentication scheme is robust to content-preserved processing, while being fragile to malicious attacks.

J. Chen et. al [104] have presented a new approach to embed watermark that is based on method to modify the block average in wavelet domain. In this method, if geometric
attacks are applied on the watermarked image, the distortions in the watermarked image can be figure out using Zernike transform and then watermark can be retrieved from distorted watermarked image. Authors have proved that their method is not only robust to geometric attacks, but also to JPEG and Checkmark attacks.

K.M. Hung et. al [105] have proposed a robust watermark system that utilizes good geometry invariant characteristic of Zernike moment and comparison of the average energy of wavelet packet. The authors have empirically proved that their method is robust against scaling, rotation, blurring, cut and JPEG attacks. The use of the ZMs has improved the robustness against geometric attacks greatly.

M. Abolghasemi et. al. [106] have presented a data hiding detection method based on ZMs of DWT coefficients of an image and Support Vector Machine(SVM). The authors have used ZMs of DWT sub band coefficients of an image as features for steganalysis and used SVM for classification of stego and non-stego images. In this method, sample mean and sample variance of ZMs of DWT sub bands coefficients are used as features for training of a SVM classifier. This method has 95.8% detection ratio.

C T. Hsieh et. al [107] have proposed a new invariant semi-fragile digital watermarking technique based on eigen values and eigenvectors of real symmetric matrix generated by the four pixel pairs of the host image. A signature bit for detecting the malicious tampering of an image is generated using the dominant eigenvector and the multi-rings Zernike transform is used to achieve geometric invariance. This method is robust to the geometric distortions even when the image is under malicious attacks. The authors have proved that their algorithm can resist high quality JPEG compression and improves the detection performance in presence of various types of malicious attacks.
C.W. Kao et. al [108] have presented a novel content-based image authentication framework which embeds the semi-fragile image feature into the host image based on wavelet transform. In this framework, two features of a target image from the low frequency domain are used to generate two watermarks: ZMs for classifying intentional content modification and Sobel edge features for indicating the modified location. The authors have designed a systematic method for automatic order selection of ZMs and for detecting if the processing on the watermarked image is malicious or not. An important advantage of their approach is that this technique can tolerate compression and noise to a certain extent while rejecting common attack of the image like rotation.

2.6 Review of fragile and semi-fragile watermarking techniques

A number of watermarking techniques for image authentication have been proposed in literature. The requirements of image authentication are different from copyright protection applications. Hence, a number of fragile and semi-fragile techniques are proposed in literature for image authentication. Review of such techniques is given as under.

S.K. Lee et. al [109] have proposed a new reversible image authentication technique where if the image is authentic, the distortion due to embedding can be completely removed from the watermarked image after extracting the watermark. This technique utilized histogram characteristics of the difference image and modified pixel values slightly to embed more data than other lossless data hiding algorithm. The authors have shown that their technique has low time complexity and can detect any modifications of the watermarked image.
C. Li et. al [110] have proposed a novel self-recovery watermarking scheme based on dual-redundant-ring structure. In this method, all blocks of target image form a ring in a manner that the watermark of an image block is hidden in 1-LSB of its next block N1, and the copy of this watermark is embedded into 2-LSB of another block whose position is determined by the position of N1. The validity of test image block is determined by comparing the number of inconsistent blocks in the block-neighborhood with that of its mapping block. Other detection results are generated in the same way by comparing the test block with copy block of its next block. The advantage of this method is that the combination of two detection marks improves tamper detection accuracy, while two copies of watermark provide a second chance for tamper recovery.

P. Sidiropoulos et. al [111] have proposed a fragile watermarking technique that combined the requirements of localization and invertibility. In this method, watermark is embedded in spatial domain while scanning the host image in row-wise manner. Moreover, watermark embedded in this scheme is dependent on the original image and due to the use of non-linear watermark embedding procedure it is secure and robust against malicious attacks.

H. Wang et. al [112] have proposed a novel, fast and self-restoration scheme resisting to JPEG compression for semi-fragile watermarking. In the watermark embedding process, ten watermarks (six for authentication and four for self-restoration) are embedded into each 8×8 block of the original image. Then mean pixel values of four 4×4 sub-blocks are utilized to restore its corresponding first four DCT coefficients of 8×8 blocks for image content recovering.
R. Chamlawi et. al [113] have proposed a secure semi-fragile watermarking, with a choice of two watermarks to be embedded. This technique is based on integer wavelet domain and has made use of semi-fragile watermarks to achieve better robustness. A self-recovering algorithm is employed by the authors where the image digest is hidden into some wavelet sub bands to detect possible malevolent object manipulation undergone by the image (object replacing and/or deletion). The semi-fragility has made this scheme tolerant for JPEG lossy compression as low as quality of 70%, and has located the tampered area accurately. Since the private key is used for embedding the watermark, this watermarking system ensured more security as compared to the conventional techniques.

M. Schlauweg et. al [31] have proposed a semi-fragile watermarking technique that extracted image content dependent information, which is hashed afterwards and encrypted using secure methods known from the classical cryptography. The image data is partitioned into non overlapping $4 \times 4$ blocks in the spatial domain. The mean values of these blocks form n-dimensional vectors, which are quantized to the nearest lattice point neighbors. Based on the changed vector values, a hash is calculated and asymmetrically encrypted, resulting in a digital signature. Traditional dual subspace approaches divide the signal space into a region for signature generation and a region for signature embedding. In this scheme error correction coding is applied to gain the robustness of the embedded signature against non-malicious distortions.

W. Xiaoyun et. al [114] have proposed a secure semi-fragile watermarking scheme for image authentication based on integer wavelet transform with parameters. In this technique, the wavelet base is chosen by a parameter for watermark embedding and it is not possible to extract the watermark without the exact parameter and thus it is very
secure. Also it has improved computational complexity due to the use of parameterized integer wavelet transform and it can tolerate JPEG lossy compression to a quality factor as low as 40, while being sensitive to malicious attacks and able to locate the tampered area accurately.

**E. T. Lin et. al [22]** have described a semi-fragile watermark for still images that can detect information altering transformations even after the watermarked content is subjected to information preserving alterations. This technique is based on extending a simple spread-spectrum watermarking technique with a modified detector that performs correlations of pixel differences in the spatial domain. The detection process is performed on each block of the image as opposed to using the entire image, so that regions of alterations can be identified. In this method, the watermark is constructed in the DCT domain to generate a smooth watermark that will resist being damaged by JPEG compression. Pseudo-random zero-mean, unit variance Gaussian distributed numbers are used for the watermark and are located in each DCT block. Each block has a different watermark but watermark is embedded in all the block in identical way.

**C.M. Kung et. al [115]** have proposed two watermarking techniques i.e. robust watermarking and image authentication technique. The robust watermarking scheme is proposed in the frequency domain that can be used to prove the ownership. The signature process is used to prove the integrity of the image. The input of the signature process is the edge properties extracted from the image. The signature can be correctly verified when the image is incidentally damaged for example due to lossy compression. This scheme provided a high degree of robustness against JPEG compression attacks.
L. Tong et. al [116] have proposed a semi-fragile watermarking technique that accepts JPEG lossy compression on the watermarked image to a pre-determined quality factor, and rejects malicious attacks. The authenticator can identify the positions of corrupted blocks, and recover them with approximation of the original ones. In addition to JPEG compression, adjustments of the brightness of the image within reasonable ranges are also acceptable using its authenticator. This method is secure due to the use of secret block mapping function which controls the signature generating/embedding processes. The authentication in this method is based on two invariant properties of DCT coefficients before and after JPEG compressions. They are deterministic so that no probabilistic decision is needed in the system. The first property shows that if a DCT coefficient is modified to an integral multiple of a quantization step, which is larger than the steps used in later JPEG compressions, then this coefficient can be exactly reconstructed after later acceptable JPEG compression. The second one is the invariant relationships between two coefficients in a block pair before and after JPEG compression. Therefore, the second property is used to generate authentication signature, and first property is used to embed it as watermarks. There is no perceptible degradation between the watermarked image and the original. In addition to authentication signatures, the recovery bits can also be embedded for recovering approximate pixel values in corrupted areas.
2.7 Review of other watermarking techniques

Other than above discussed watermarking methods, research has been made on a number of other watermarking techniques that are based on edge detection methods, SVD and SS techniques. A review of such watermarking schemes is given as under.

**P. Ramesh et. al [117]** have proposed a watermarking technique and embedded the watermark transparently at the edges of digital image where deformation is less identifiable. To identify the edges, Sobel edge detection algorithm is used because it is inexpensive in terms of computations and the gradient approximation which it produces, is relatively simple, in particular for high frequency variations in the image.

**J. N. Ellinas et. al [118]** have presented a robust watermarking algorithm using the wavelet transform and edge detection method. In this method, the watermark is embedded transparently with the maximum possible strength. The watermark embedding process is carried over the sub band coefficients that lie on edges, where distortions are less noticeable, with a sub band level dependent strength. Also, the watermark is embedded to selected coefficients around edges, using a different scale factor for watermark strength, that are captured by a morphological dilation operation. This method is efficient in terms of both transparency and robustness to various attacks such as median filtering, Gaussian noise, JPEG compression and geometrical transformations.

**R. Liu et. al [13]** have proposed a novel watermarking algorithm based on SVD. Authors have analyzed and proved that their watermarking method is both secure and robust. The advantage of using the singular values of an image is that it has very good stability, i.e., when a small perturbation is added to an image, its singular values do not change significantly.
E. Ganic et. al [119] have presented a hybrid scheme based on DWT and SVD. In other DWT-based scheme, the DWT coefficients are modified with the data that represents the watermark. Whereas in this technique, after decomposing the cover image into four bands, the SVD is applied to each band, and the same watermark data is embedded by modifying the singular values. Due to the modification in all frequencies, this technique is robust to a wide range of attacks.

R. A. Ghazy et. al [120] have presented a block-based digital image watermarking scheme that is dependent on the mathematical technique of SVD. In this technique, the host image is divided into blocks, and then the watermark is embedded in the singular values of each block separately. This segmentation and watermarking process makes the watermark much more robust to the attacks such as noise, compression, cropping. Watermark detection is implemented by extracting the watermark from the SVs of the watermarked blocks.

J. Song et. al [121] have proposed a novel blind watermark algorithm based on DWT and SVD. In this technique, Tent chaotic mapping is applied into encryption of the original watermark. After decomposing the cover image into four sub-bands (LL3, HL3, LH3 and HH3) with 3-level DWT, the encrypted watermark is decomposed using the DWT and the singular values of LL3, HL3, LH3, and HH3 are modified with DWT coefficients of the watermark. This technique returns the watermarked image of better quality and is robust to a wide range of attacks.

A. Mansouri et. al [122] have proposed a robust and non-blind image watermarking. In this technique, the SVD of image is modified in Complex Wavelet Transform (CWT) domain, where CWT provides higher capacity than the real wavelet domain. As
appropriate sub-bands are modified here, it preserved the quality of the watermarked image. The additional advantage of this method is its robustness against most of the common attacks. The authors have empirically shown that the performance of their method is best in comparison with the pure SVD-based as well as hybrid methods.

A. Basso et. al [123] have proposed a block-based watermarking scheme based on the SVD. In this technique, a pseudo-random Gaussian sequence is embedded as a watermark by modifying the angles formed by the right singular vectors of each block of the original image. The authors have concluded that their scheme is resistant against common signal processing operations and attacks while preserving the quality of the original image.

S.W. Foo et. al [124] have proposed a normalization-based robust image watermarking scheme which encompasses SVD and DCT technique. In this technique, the host image is first normalized to a standard form and divided into non-overlapping image blocks. SVD is applied to each block and by concatenating the first singular values of adjacent blocks of the normalized image, a SV block is obtained. DCT is then carried out on the SV blocks to produce SVD-DCT blocks. A watermark bit is embedded in the high frequency band of a SVD-DCT block by imposing a particular relationship between two pseudo-randomly selected DCT coefficients. An adaptive frequency mask is used to adjust local watermark embedding strength. Watermark extraction is done in inverse process. The watermark extracting method is blind and efficient. The authors have shown that the quality degradation of watermarked image caused by the embedded watermark is visually transparent. This method is robust against various image processing operations and geometric attacks.
I.J. Cox et. al [20] have presented a secure (tamper-resistant) algorithm for watermarking images, and a methodology for digital watermarking that may be generalized to audio, video, and multimedia data. The authors have advocated that a watermark should be constructed as an independent and identically distributed Gaussian random vector that is imperceptibly inserted in a spread-spectrum-like fashion into the perceptually most significant spectral components of the data. The authors have defined that the insertion of a watermark under this system made the watermark robust to signal processing operations (such as lossy compression, filtering, digital-analog and analog-digital conversion, requantization, etc.), and common geometric transformations (such as cropping, scaling, translation, and rotation) provided that the original image is available. In such cases, the watermark detector unambiguously identifies the owner. Also due to the use of Gaussian noise, strong resilience to multiple-document, or collusion attacks are ensured.

V. Mezaris et. al [125] have presented a novel approach for image indexing using content-based watermarking. In this technique, color image segmentation and watermarking in order to facilitate content-based indexing, retrieval and manipulation of digital images is used. A novel segmentation algorithm is applied on reduced images and the resulting segmentation mask is embedded in the image using watermarking techniques. In each region of the image, indexing information is additionally embedded. This system is endowed with content-based access and indexing capabilities which can be easily exploited via a simple watermark detection process.

A. Parthasarathy et. al [126] have proposed a robust and transparent scheme of watermarking that exploits the human visual system’s sensitivity to frequency, along with
local image characteristics obtained from the spatial domain, improving upon the conventional content-based image watermarking scheme. The authors have used the underlying idea of generating a visual mask based on the human visual systems perception of image content. This mask is used to embed a decimal sequence while keeping its amplitude below the distortion sensitivity of the image pixel. The authors have considered texture, luminance, corner and the edge information in the image to generate a mask that makes the addition of the watermark less perceptible to the human eye. The operation of embedding and extraction of the watermark is done in the frequency domain thereby providing robustness against common frequency-based attacks including image compression and filtering. The authors have used decimal sequences for watermarking instead of pseudo random sequences, providing a greater flexibility in the choice of sequence.

R. Liu et. al [127] have proposed a new general additive watermarking model based on the content of digital images, called as content-based watermarking model. This model is designed to address two important issues of digital watermarking. One is the requirement of robustness. In order to improve robustness and security, the embedded watermark is designed to be orthogonal to the feature vector of the original image, which means that watermark embedding process is image content dependent. The second issue is watermark detection. Content-based watermarking model presented a statistical approach for watermark detection based on the Neyman-Pearson criterion and described a method for computing the probability of false alarm and missing rejection during watermark detection. The authors have applied content-based watermarking model to the popular DCT and obtained very promising results.
2.8 Summary

In this Chapter of the thesis, a review of existing robust and fragile/semi-fragile watermarking techniques based on DCT, DFT, DWT and other transformations is given. A review of watermarking techniques based on feature points, descriptors and moments such as ZMs is also given along with their relative advantages and drawbacks over other watermarking techniques. It is concluded from the review that existing DFT-based watermarking techniques are more robust against geometric attacks as compared to DCT and DWT-based watermarking techniques but they have very high computation complexity and likewise ZMs-based watermarking techniques are also very robust against geometric attacks and have the advantage of low complexity as compared to DFT-based watermarking techniques.

The relative advantages of ZMs-based watermarking techniques led us to work on magnitude and phase of ZMs for proposing new watermarking techniques that achieve our objectives of high capacity and imperceptibility in addition to robustness. From the descriptor-based watermarking techniques, we chose a dense descriptor i.e. Weber’s descriptor to develop a robust watermark authentication algorithm that can be used with any transform-based or ZMs-based watermarking technique to authenticate the presence of a watermark in an image. Further, we have also developed a fragile image authentication technique based on this descriptor.