CHAPTER 2
REVIEW OF LITERATURE

Digital watermarking techniques have been investigated deeply for its technical and commercial feasibility in all media types like, digital photographic image (Lim *et al.*, 2001), audio (Sachs *et al.*, 2000), printed materials or document images (Kim *et al.*, 2003b) and video (Hussein and Mohammed, 2009). It is a proven method for reducing content piracy and improving the ability to identify, tract and manage digital media (Eskicioglu and Delp, 2001). It is widely used in applications of rights management, remote triggering, filtering/classification and e-commerce. It is a technique that is used to balance the need for content security with best possible consumer experience to enable media and entertainment industries to adapt the advanced facilities of the modern digital revolution while reducing the threat of content theft.

In the present scenario, systems that have the ability to protect content accurately, rapidly, reliably, without invading privacy rights, cost effectively, in a user-friendly manner and without drastic changes to the existing infrastructures are highly desired. As commercial incentives increase, many new technologies for person authentication, information hiding, copyright protection are being developed (Jadhao and Dole,2013), each with its own strengths and weaknesses and a potential niche market. This chapter reviews the various watermarking algorithms that uses techniques related to the research topic.

2.1. HISTORY OF DIGITAL WATERMARKING

Digital watermarking technology started as early as 1282 in Italy, where paper watermarks were used to indicate the paper brand and the mill that produced it. After this invention, the method quickly spread over Italy and then over Europe. Although originally intended for paper brand and mill identification, the technique was later enhanced to include paper format, quality and strength. They were also used to date and authenticate paper.

During 18th century, this technique was first used for installing anti-counterfeiting measures on money and other documents (http://www.ncd.matf.bg.ac.yu/casopis/05/Vuckovic/Vuckovic.pdf). They are still widely used as security features in currency today. These techniques were called watermarking only during the end of the 18th century. The first watermark, that is the base of today's technology, is the patent filed in 1954 by Emil Hembrooke for identifying music works.

It was only after 1995 interest in digital watermarking increased and several organizations began including watermarking technology in different standards. The Secure Digital Music Initiative (SDMI, 1999) adopted watermarking as a central component to their music protection system. The Copy Protection Technical Working Group (CPTWG) (Bell, 1999) considered watermarking technology for video content protection on DVDs. The International Organization for Standardization showed an interest in watermarking for designing MPEG standards (Cox *et al.,* 2008). VIVA (Depovere *et al.*, 1999) and Talisman (Hartung and Kutter, 1999), both sponsored by the European Union, employed the technology for broadcast monitoring.

The term "digital watermarking" came into existence only after 1988 and was coined by Komatsu and Tominaga (1988). Since after, there has been a huge interest in the field of digital watermarking and several different techniques have been proposed (Daniel and Monica,2010). Even though watermarks can be included with any digital content, this research is focused on image watermarking and the following sections review only those implementations that are related to this field.

Video watermarking was first introduced in 1996 when the video compression standard MPEG2 is published and widely applied. From then on, the related theoretical and technical work attracts more and more researchers. Besides academic perspective, its commercial implementations are also emphasized together with economic and engineering constraints. The rapid use of the Internet has led to the investigation of digital watermarking as a complementary technology to traditional protection mechanisms. Significant research efforts and review works presenting

unified characteristics of different methods have been reported for audio and image watermarking.

In the context of video watermarking, there is a great deal of non-uniformity in the presented approaches. As a method of intellectual content protection, digital watermarks have recently stimulated significant interest and become a very active area of research. Recent decades have envisaged many techniques proposed both in the academic as well as in the industry for watermarking, which can be classified into different types based on the offered functionalities.

Many digital watermarking schemes have been proposed in the literature for still images and videos. These techniques mostly work on the raw uncompressed video data (Ejima and Miyazaki, 2001) and recent approaches are embedding watermarks into compressed video data also (Hartung and Girod, 1998; Arena and Caramma, 2000).

2.2. IMAGE WATERMARKING TECHNIQUES USED FOR VIDEO WATERMARKING

Digital watermarking for video is a fairly new area of research which basically benefits from the results of still images. Many algorithms have been proposed in the scientific literature and three major trends can be isolated (Abdullah and Manaf 2007). The most simple and straightforward approach is to consider a video as a succession of still images and to reuse an existing watermarking scheme for still images. Another point of view considers and exploits the additional temporal dimension in order to design new robust video watermarking algorithms. The last trend basically considers a video stream as some data compressed according to a specific video compression standard and the characteristics of such a standard can be used to obtain an efficient watermarking scheme. Each of those approaches has its pros and cons as detailed in Table 2.1.

TABLE 2.1

MERITS AND DEMERITS OF VIDEO WATERMARKING

	Merits	Demerits
Image → Video	Inherit from all the results for still images	Computationally intensive
Temporal dimension	Video-driven algorithms which often permit higher robustness	Can be computationally intensive
Compression standard	Simple algorithms which make real-time achievable	Watermark inherently tied to the video format

In its very first years, digital watermarking has been extensively investigated for still images. Several interesting algorithms have been found and with areas, such as video, were researched and the basic concern was to try to reuse the previously found results (Doerr and Dugelay,2003). As a result, the watermarking community first considered the video as a succession of still images and adapted existing watermarking schemes for still images to the video. Almost all of the techniques discussed in the previous sections, can be applied and studied for video watermarking.

Exactly the same phenomenon occurred when the coding community switched from image coding to video coding. The first proposed algorithm for video coding was indeed Moving JPEG (M-JPEG), which simply compresses each frame of the video with the image compression standard JPEG (Joint Picture Experts Group). During embedding, the simplest method is to insert the same watermark in the frames of the video at a regular rate. During detection, all the frames are checked for the presence of the watermark. If the video has been watermarked, a regular pulse should be observed in the response of the detector (Barni *et al.*, 2000). However, such a scheme has no payload. The detector only tells if a given watermark is present or not but it does not extract any hidden message.

On the other hand, the host data is much larger in size than a single still image. Since one should be able to hide more bits in a larger host signal, high payload

watermarks for video could be expected. This can be easily done by embedding an independent multi-bits watermark in each frame of the video (Dittmann *et al.*, 1998). However, this gain in payload is counterbalanced by a loss of robustness.

The Differential Energy Watermarks (DEW) method was initially designed for still images and has been extended to video by watermarking the I-frames of an MPEG stream (Langelaar *et al.*, 1998). It is based on selectively discarding high frequency DCT coefficients in the compressed data stream.

The main drawback of considering a video as a succession of independent still images is that it does not satisfactorily take into account the new temporal dimension. The coding community has made a big step forward when they decided to incorporate the temporal dimension in their coding schemes and it is quite sure that it is the advantage of the watermarking community to investigate such a path.

Many researchers have investigated how to reduce the visual impact of the watermark for still image by considering the properties of the Human Visual System (HVS) such as frequency, luminance and contrast masking. These studies can be easily extended to video with a straightforward frame-per-frame adaptation.

Motion is a very specific feature of the video and new video-driven perceptual measures need to be designed in order to be exploited in digital watermarking (Kim *et al.*, 1999). This simple example shows that the temporal dimension is a crucial point in video and that it should be taken into account to design efficient algorithms.

One of the pioneer works in video watermarking considers the video signal as a one-dimensional signal (Hartung and Girod, 1998). Let a sequence represent the watermark bits to be embedded, which is spread by a chip-rate cr. The spreading operation permits to add redundancy by embedding one bit of information into cr samples of the video signal. The obtained sequence is then amplified locally by an adjustable factor and modulated by a pseudo-random binary sequence. Finally, the spread spectrum watermark is added to the line scanned video signal, which gives the

watermarked video signal. On the detector side, recovery is easily accomplished with a simple correlation.

Other approaches have been investigated to integrate the temporal dimension. Temporal wavelet decomposition can be used for example in order to separate static and dynamic components of the video (Swanson *et al.*, 1998a). A watermark is then embedded in each component to protect them separately. The video signal can also be seen as a three-dimensional signal. This point of view has already been considered in the coding community and can be extended to video watermarking. 3D DFT can be used as an alternative representation of the video signal (Deguillaume *et al.*, 1999). The HVS is considered to define the embedding area which will not result in a visible watermark.

On the other hand, the obtained embedding area is modified so that it becomes immune to MPEG compression. Considering video as a three-dimensional signal may be inaccurate. The three considered dimensions are indeed not homogeneous: there are two spatial dimensions and one temporal dimension. This consideration and the computational cost may have hampered further work in this direction. However, this approach remains pertinent in some specific cases.

As many of the video watermarking techniques have been extended from image watermarking techniques, both image and video watermarking techniques are reviewed in this chapter.

2.3. VIDEO WATERMARKING ALGORITHMS

A variety of robust and fragile video watermarking methods have been proposed to solve the illegal copying and proof of ownership problems as well as to identify manipulations (Hussein and Mohammed,2009). Although several claims have been made in the development of robust digital watermarking methods, it is still difficult to handle combined or non-linear geometric transformations (Su, 2001). Video watermarking techniques, in general, can be divided into three categories (Figure 2.1) as listed below.

- **Spatial domain approach**, also called native domain where embedding and detection are performed on spatial pixel values (luminance, chrominance, colour space) or on the overall video frame characteristic,
- **Frequency domain techniques** where the spatial values are transformed, like DCT Discrete Cosine, FFT Fast Fourier Transformation, Wavelets or fractals,
- Format-specific approaches like watermarking of structure elements like Facial Animation Parameter of **MPEG-4 or motion vectors**.

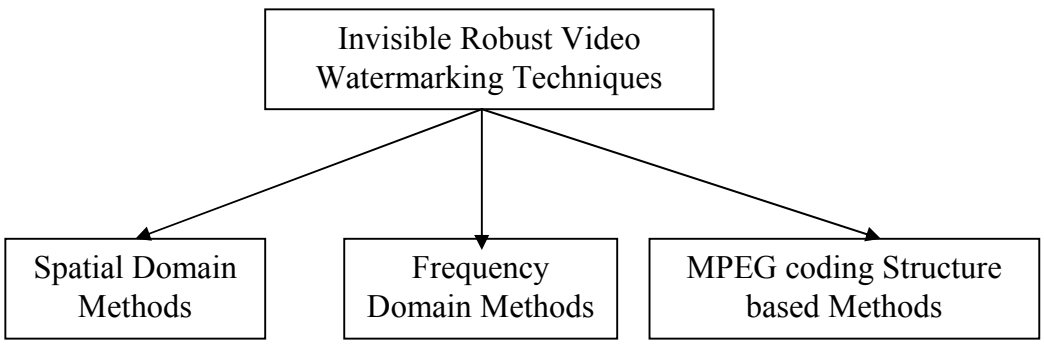

Figure 2.1 : General Categories of Video Watermarking Techniques

Most of the proposed video watermarking algorithms are based on the techniques of the image watermarking and applied to raw video or the compressed video(Gosavi and Warnekar,2010). As some issue in video watermarking is not present in image watermarking, such as video object and redundancy of the large amount video data, researchers have made use of those characteristics to develop different schemes. The following subsections discuss various methods proposed under each of the domains listed above.

2.3.1. Spatial Domain Watermarks

The spatial domain watermarking techniques embed the watermark by modifying the pixel values of the host image directly (Huang *et al.,* 2005; Kimpan *et al.,* 2004; Ren-Junn *et al.,* 2002; Wu and Guan, 2007; Verma *et al.*, 2006). The simplest of the spatial methods is to just flip the lowest-order bit of the chosen pixels in a grey scale or colour image. This method works well only if the image is subjected to any human or noisy modification. A more robust method can be achieved if the

watermark embedding process in a video frame is performed in the same way as a watermark is added to the paper. Such techniques may superimpose a watermark symbol over an area of the frame and then add some fixed intensity value for the watermark to the varied pixel values of the frame. The resulting watermark may be visible or invisible depending upon the value (large or small, respectively) of the watermark intensity.

More details about these algorithms can be found in a review paper by Hartung and Kutter (1999). The abundance of spatial-domain methods results from their simplicity and efficiency. Least Significant bit (LSB) technique is the most frequently used method (Lee and Chen, 2000). In LSB based techniques, the LSB of each pixel is used to embed the watermark or the copyright information. This technique is the most-straight forward method and uses the entire cover image to store the watermark, which enables a smaller object to be embedded multiple times. In case of attacks destroying data, a single surviving watermark can be considered a success. They are robust to attacks like cropping, noise, lossy compression, etc. But an attack that is set on a pixel to pixel basis can fully uncover the watermark, which is the major drawback of the system.

Earlier works include the work of van Schundel *et al.* (1994), who proposed a technique that used two methods to hide data into images. The first replaced the LSB of uncompressed image with a m-sequence invisible data while the second added the m-sequence data to the LSB of the image and used auto-correlation to detect it later on.

Macq and Quisquater (1995) briefly discussed the issue of watermarking digital images as part of a general survey on cryptography and digital television. The authors provided a description of a procedure to insert a watermark into the least significant bits of pixels located in the vicinity of image contours. As this method relies on modifications made on the LSBs, the watermark is easily destroyed.

In the same year, Rhoads (1995) described a method that adds or subtracts small random quantities from each pixel. Addition or subtraction is determined by

comparing a binary mask of bits with the LSB of each pixel. If the LSB is equal to the corresponding mask bit, then the random quantity is added, otherwise it is subtracted. This method does not make use of perceptual relevance, but it is proposed that the high frequency noise be pre-filtered to provide some robustness to low pass filtering.

Ratha *et al.* (2000) proposed a blind data hiding method applicable to fingerprint images compressed with WSQ (Wavelet-packet Scalar Quantization) standard. In this method, the quantizer integer indices were randomly selected and each watermark bit replaced the LSB of the selected coefficient. At the decoder, the LSB's of these coefficients were collected in the same random order to construct the watermark. Later, Wong and Memon (2001) used hash functions to embed the watermark in the Least Significant Bit (LSB) of fingerprint images. Yang (2008) used an inverted pattern approach to improve image quality of information hiding using LSB substitution.

Tanaka *et al.* (1990a, 1990b) introduced the idea of tagging digital data to secretly hide information and assure ownership rights first in 1990. Later, Caronni (1993) described an overall system to track unauthorized distribution of digital content. The method used spatial signal modulation, called tagging, to watermark digital content. A tag is a square with a constant value proportional to the maximum image brightness within the square and decaying outside the border. A selected area is tagged by adding or subtracting the tag and a random- zero mean-noise pattern.

In the same year, Tirkel *et al.* (1993) recognized the importance of digital watermarking and possible applications for tagging, copyright enforcement, counterfeit protection and controlled access to image data. In their approach, the watermark in the form of a m-sequence-derived PN code is embedded in the least significant bit (LSB) plane of the digital data. This method is actually an extension to simple LSB coding schemes in which the LSBs are replaced by the coding information.

The idea of using m sequences and LSB addition was extended and improved by the authors through the use of two-dimensional m-sequences, which resulted in

more robust watermarks (Tirkel *et al.*, 1995). A modified version of the method was presented by Schyndel *et al.* (1994) explicitly mentioning the term digital watermarking. About the same time Matsui and Tanaka proposed several watermarking techniques (Matsui and Tanaka, 1994).

Since the above techniques were introduced, interest and research activities in watermarking have increased significantly. In some recent work, Bender *et al.* (1995) proposed two methods for data hiding. In the first method, called "Patchwork", randomly selected pairs of pixels are used to hide one bit by increasing one pixel by one and decreasing the other pixel by one. In the Texture Block Coding, the second approach, the watermark is embedded by copying one image texture block to another area in the image with a similar texture. To recover the watermark, the autocorrelation function has to be computed.

Nikolaidis and Pitas (1996) and Pitas (1996, 1998) proposed signature casting on digital contents, which is based on the same basic idea as the patchwork algorithm proposed by Bender *et al.* (1995) and Langelaar *et al.* (1996, 1997) proposed an improved version of this idea. The frame is tiled into square blocks with a size being a multiple of eight. By iteratively modifying a pseudorandomly selected block, a single bit is embedded into the cover medium. To increase the performance of spread-spectrum watermarking in the spatial domain,

Kutter *et al.* (1997) proposed a method which exclusively works with the blue component (in the RGB colour space) of a frame to maximize the watermark strength, while keeping visual artifacts minimal. Extensions to this method allow increased robustness and even watermark recovery after geometrical attacks and printing-scanning (Kutter, 1998).

Delaigle *et al.* (1996, 1997) introduced watermarking adapted to the Human Visual System (HVS) using masking and modulation. In their scheme, the watermark in the form of a spatially limited binary pattern is low-pass filtered, frequency modulated, masked and then added to the host image. Wolfgang and Delp (1996, 1997) proposed a watermarking technique to verify image authenticity based on an

approach similar to the m-sequence approach suggested by Schyndel *et al.* (1994) for the one-dimensional case and Tirkel *et al.* (1995) for the two-dimensional case.

Watermark embedding based on quantization was proposed by Chen and Wornell (2001). Their method is called Quantized Index Modulation (QIM) and is based on a set of N-dimensional quantizers. Maes and Overveld (1998) proposed modifying geometric features of the frame and was based on a dense line pattern, generated pseudorandomly and representing the watermark.

The LSB technique was improved by Johnson and Katezenbeisser (1999), which included an additional security, by using a pseudo-random number generator to determine the pixels to be used for embedding based on a given "seed" or key.

The watermark system proposed by Ren-Junn *et al.* (2002) embeds the watermark in saturation on the HIS (Hue, Intensity, Saturation) colour space. The results proved that the system was able to resist only certain type of attacks. In a similar fashion, Huang *et al.* (2005) used the DC components of the colour image in the spatial domain to embed the watermark and their results showed robust performance with all types of attacks except for rotate and scaling attacks.

A variable block size based adaptive watermarking in spatial domain was proposed by Kimpan *et al.* (2004), where the original image was divided into different blocks of varied size and the watermark was embedded into the blocks by analyzing and adjusting the brightness of a block.

In a later period, Verma *et al.* (2006) proposed a probability block based watermarking method for colour image with fixed block size. In this method, the image was initially divided into blocks of size 8*8 and manipulated the pixel intensity to embed a watermark bit. The method posed a condition that the number of total bits of the watermark must be less or equal to the half of the total number of 8x8 blocks and redundant information is added to the watermark using convolution code. The disadvantage of using convolution code is that it required a constant high amount of decoding operations, even if few or no errors occurred (Hueske *et al.,* 2007).

Both these methods were robust against all common image processing operations, such as median filter, scaling, rotation, etc., but failed with the crop attack as the watermark bits were embedded into the whole image, hence some data was lost during cropping. Recently, a novel digital watermark algorithm based on chaotic maps was proposed by Wu and Guan (2007) where the chaotic maps were used to determine the pixel bit for embedding.

The main advantages of pixel based methods are that they are conceptually simple and have very low computational complexities and therefore are widely used in video watermarking where real-time performance is a primary concern. However, they also exhibit some major limitations. The need for absolute spatial synchronization leads to high susceptibility to de-synchronization attacks, lack of consideration of the temporal axis results in vulnerability to video processing and multiple frame collusion and watermark optimization is difficult using only spatial analysis techniques.

2.3.2. Frequency Domain Watermarks

In transform domain watermarking systems, watermark insertion is done by transforming the frames into the frequency domain using a Discrete Fourier Transformation (DFT), full-image DCT, block-wise DCT, wavelet, Hadamard Fourier-Mellin, or other transforms. It is often claimed that embedding in the transform domain is advantageous in terms of visibility and security. It has been shown that for maximum robustness, watermarks should be embedded into the same spectral components that the host data already populate. For images and videos, these are typically the low frequencies. Designing watermarking algorithms in the transform domain is not as simple as in the spatial domain.

Among the various techniques, Discrete Cosine Transformation (DCT), Discrete Fourier Transformation (DFT) and Discrete Wavelet Transformation (DWT) are the three main methods of data transformation. In transform domain technique, the watermark is embedded distributively in overall domain of an original data. Here, the host image is first converted into frequency domain by transformation techniques. The transformed domain coefficients are then altered to store the watermark information.

The inverse transformation is finally applied in order to obtain the watermarked image.

The main strength offered by transform domain techniques is that they can take advantage of special properties of alternate domains to address the limitations of pixel-based methods or to support additional features. For instance, designing a watermarking scheme in the Discrete Cosine Transformation (DCT) domain leads to better implementation compatibility with popular video coding algorithms such as Moving Picture Experts Group (MPEG) and in the shift and rotation-invariant Fourier domains facilitates the design of watermarks that inherit these attractive properties.

Besides, analysis of the host signal, in a frequency domain, is a prerequisite for applying more advanced masking properties of the HVS to enhance watermark robustness and imperceptibility. Generally, the main drawback of transform domain methods is their higher computational requirement.

Frequency domain watermarking was first introduced by Boland *et al.* (1995) and Cox *et al.* (1997), who independently developed perceptually adaptive methods based on modulation. Cox *et al.* drew parallels between their technique and spread-spectrum communication since the watermark is spread over a set of visually important frequency components. The watermark consists of a sequence of numbers x = x1, ..., xn with a given statistical distribution, such as a normal distribution N(0, 1) with zero mean and variance one. The watermark is inserted into the image V to produce the watermarked image V'. Three techniques are proposed for watermark insertion. The scheme can be generalized by introducing multiple scaling parameters to adapt to the different spectral components and thus reduce visual artifacts. To verify the presence of the watermark, the similarity between the recovered watermark, given by the difference between the original image, the possibly tampered image and the original watermark, is measured.

This section discusses the details of two frequently used methods, namely, Discrete Cosine Transformation and Discrete Wavelet Transformation along with

Principal Component Analysis (PCA), Independent Component Analysis (ICA) and Singular Value Decomposition (SVD) based methods.

- **DCT-Based Methods**

Efficient watermarking in the DCT domain was first introduced by Koch *et al.* (1994, 1995, 1998). As in the JPEG compression scheme, the image is first divided into square blocks of size 8x8 for which the DCT is computed. From a pseudorandomly selected block, a pair of midfrequency coefficients is selected from 12 predetermined pairs. To embed a bit, the coefficients are then modified such that the difference between them is either positive or negative, depending on the bit value.

Bors and Pitas (1996a, 1996b) suggested a method that modifies DCT coefficients satisfying a block site selection constraint. The image is first divided into blocks of size 8x8. Certain blocks are then selected according to a Gaussian network classifier decision. The middle range frequency DCT coefficients are then modified, using either a linear DCT constraint or a circular DCT detection region, to convey the watermark information.

Swanson *et al.* (1996a, 1996b) suggested a DCT-domain watermarking technique, based on frequency masking of DCT blocks, which is similar to the methods proposed by Smith and Comiskey (1996). Tao and Dickinson (1997) introduced an adaptive DCT-domain watermarking technique based on a regional perceptual classifier with assigned sensitivity indexes.

Podilchuk and Zeng (1997a, 1997b) introduced perceptual watermarking using the Just Noticeable Difference (JND) to determine an image-dependent watermark modulation mask. The watermark is embedded into selected coefficients in either the DCT or wavelet transformation domain. For DCT coefficients, the author suggests using a perceptual model defined by Watson, based on utilizing frequency and brightness sensitivity as well as local contrast masking. This model provides image-dependent masking thresholds for each 8 x 8 DCT block. Piva *et al.* (2002) described

another DCT-based method which exploits the masking characteristics of the HVS (Piva *et al.*, 1997).

A block-based semi-fragile watermarking approach is described in Zhuo *et al.* (2004) for protecting the image contents. The input image is divided into non-overlapping blocks of size 16 x 16 and k bits are extracted from each block. Signature for each block is represented as a vector. After quantization, the grey code is selected for embedding the signature. In this technique, the watermark encrypted and inserted by modulating the wavelet coefficients.

A subsample based watermarking technique was proposed by Liu *et al.* (2005), where the DCT coefficients of the subimages were utilized to store the watermark. The method was considered complex and involved high computations, because of the complicated calculations involved in the forward and inverse transformation process. The method, however, was robust against attacks than spatial domain methods.

Koch and Zhao (1995) and Bors and Pitas (1998) presented watermarking algorithms where the image was first transformed into DCT domain and the watermark was embedded in mid-frequency coefficients. The middle frequencies were robust against JPEG compression and had less perceptual distortion compared to the regions where the variation of intensities changed gradually.

Choubisa *et al.* (2011) proposed algorithm of digital watermarking technique based on DCT (Discrete Cosine Transformation) using permuting the image. Through adjusting the block DCT coefficient of the image the watermarks are invisible. The images are first permuted and then converting into block allowing to 8×8 pixel and thus the watermark images are embedded through adjusting their DCT coefficient. The proposed scheme proved that the method has strong robust.

- **DWT-Based Methods**

As for schemes working in other transform domains, the watermark is usually given by a pseudo-random 2-D pattern. Both the image and watermark are decomposed using a 2-D wavelet transform and in each subband of the image a weighted version of the watermark is added. Watermark decoding is, as usual, based on a normalized correlation between the estimate of the embedded watermark and the watermark itself. Various wavelet-based schemes have been proposed (Inoue *et al.*, 1998; Kundur and Hatzinakos, 1997; Xia *et al.*, 1997; Zhu *et al.*, 1998). The differences between the schemes usually lie in the way the watermark is weighted in order to decrease visual artifacts.

Wang *et al.* (1998) used wavelet coefficients to embed the watermark in the proper locations of the image. They used Multi-Threshold Wavelet Method (MTWM) (Wang and Kuo, 1997) and successive subband quantization to search for the significant coefficients. The watermark is added by quantizing the significant coefficient in the significant subband by using different weights. Nevertheless, the main drawback is that it is an informed technique and need original image at the receiving end. The suitable locations can be pointed out for watermark embedding using the secret key.

Alternatively, Bender *et al.* (1996) used a secret key to select the proper wavelet coefficients for embedding the watermark. The selected coefficients were first divided into two halves where first half is incremented by one while the other half is decremented by one. The same key is supposed to be available on the receiving side, which was used to select the embedding coefficients. This approach is thus based on statistical change in the image, which is very straightforward and it only verifies the existence of the watermark.

Kundur and Hitzinakos (1997) proposed a robust watermarking approach based on wavelet transformation. In this method, both the original image and the authentication watermark are decomposed upto L level using wavelet transformation. The host image is divided into blocks, whose significant bit coefficients were used to

embed the watermarks. The significant measure is a numerical measure based on information about the HVS. The watermark was extracted using an inverse procedure of the embedding process. This is an informed technique where the original unwatermarked image is required.

Similar to this work, Liu *et al.*(2006) developed a robust watermarking approach based on the wavelet transform using original image X and its reference image X' for watermark embedding. The watermark W is the binary image with W(x, y) = {1, -1} and embedded according to the original and its reference image. The reference image is obtained by applying the first level decomposition to the original image and assigns zeros to all its detailed coefficients. It then applies the inverse wavelet decomposition. Proper locations are obtained based on some constraints to make a trade-off between robustness and imperceptibility and then the watermark is embedded in the coefficients, which are randomly selected from the proper locations.

A wavelet based fragile watermarking approach was proposed by Kundur and Hatzinakos (1999), where the watermark is embedded in the DWT domain by quantizing the wavelet coefficients. Different decomposition levels grant the tamper detection within the image in localized spatial and frequency domain. The aim is to present an authentication technique that hides watermark into some wavelet subbands of the to-be-authenticated image. This scheme is capable to detect the malicious and the incidental manipulations. Furthermore, security is a particular concern that is often overlooked. It is extremely difficult for an attacker to create a faked image that appears to be authentic.

Al-Taweel and Sumari (2009) proposed a novel DWT-based video watermarking algorithm based on a three-level DWT using Haar filter which is robust against geometric distortions such as Downscaling, Cropping and Rotation. It is also robust against Image processing attacks such as Low Pass Filtering (LPF), Median filtering and Weiner filtering. Furthermore, the algorithm is robust against Noise attacks such as Gaussian noise, Salt and Pepper attacks. The embedded data rate is high and robust. The experimental results show that the embedded watermark is

robust and invisible. The watermark was successfully extracted from the video after various attacks.

Ghosh *et al.* (2012) proposed a novel watermarking technique where both visible and invisible watermarks are embedded in a video. Kashyap and Sinha (2012) have implemented a robust image watermarking technique for the copyright protection based on 3-level Discrete Wavelet Transformation (DWT). In this technique a multi-bit watermark is embedded into the low frequency sub-band of a cover image by using alpha blending technique. The insertion and extraction of the watermark in the grayscale cover image is found to be simpler than other transformation techniques. The proposed method is compared with the 1-level and 2-level DWT based image watermarking methods by using statistical parameters such as Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE). The experimental results demonstrate that the watermarks generated by the proposed algorithm are invisible and the quality of watermarked image and the recovered image are improved.

Bhatnagar and Raman (2012) proposed a Wavelet Packet Transformation (WPT)-based robust video watermarking algorithm. A visible meaningful binary image is used as the watermark. First, sequence of frames are extracted from the video clip. Then, WPT is applied on each frame and from each orientation one sub-band is selected based on block mean intensity value called robust sub-band. A watermark is embedded in the robust sub-bands based on the relationship between wavelet packet coefficient and its 8-neighbour (D8) coefficients considering the robustness and invisibility.

- **PCA-Based Watermarking Techniques**

In the literature, different schemes are proposed (Ali et al.,2012) to achieve more robustness and imperceptibility. Mirza *et al.* (2007) proposed a new digital video watermarking scheme based on Principal Component Analysis. A video file is a continuous collection of static images and each image is composed of three colour channels, the proposed algorithm embed a watermark in the three colour channels RGB of an input video file. An imperceptible watermark is embedded into the three different RGB

channels of the video frame separately using PCA transform. The main advantage of this approach is that the same or multi-watermark can be embedded into the three colour channels of the image in order to increase the robustness of the watermark. Furthermore, using PCA transform allows to choose the suitable significant components into which to embed the watermark. The preliminary results show a high robustness against most common video attacks, especially frame dropping, cropping and rescaling for a good perceptual quality.

Mostafa *et al.* (2009) presented a novel technique for embedding a binary logo watermark into video frames. PCA is applied to each block of the two bands (LL – HH) which result from Discrete Wavelet transformation of every video frame. The watermark is embedded into the principal components of the LL blocks and HH blocks in different ways. The scheme is tested by applying various attacks. Experimental results show no visible difference between the watermarked frames and the original frames and show the robustness against a wide range of attacks such as MPEG coding, JPEG coding, Gaussian noise addition, histogram equalization, gamma correction, contrast adjustment, sharpen filter, cropping, resizing and rotation. The proposed scheme is an imperceptible and a robust hybrid video watermarking scheme. Combining the two transforms improved the performance of the watermark algorithm.

Sinha *et al.* (2011) proposed a comprehensive approach for watermarking digital video by using a hybrid digital video watermarking scheme based on Discrete Wavelet Transformation (DWT) and Principal Component Analysis (PCA). PCA helps in reducing correlation among the wavelet coefficients obtained from wavelet decomposition of each video frame thereby dispersing the watermark bits into the uncorrelated coefficients. The video frames are first decomposed using DWT and the binary watermark is embedded in the principal components of the low frequency wavelet coefficients. The imperceptible high bit rate watermark embedded is robust against various attacks that can be carried out on the watermarked video, such as filtering, contrast adjustment, noise addition and geometric attacks.

Ali *et al.* (2012) proposed a wavelet based watermarking technique with the combination of PCA transform. DWT is computationally more efficient than other transform methods like DFT and DCT. Due to its excellent spatio-frequency localization properties, the DWT is very suitable to identify areas in the host video frame where a watermark can be embedded imperceptibly. PCA is basically used to hybridize the algorithm as it has the inherent property of removing the correlation amongst the data i.e. the wavelet coefficients and it helps in distributing the watermark bits over the sub-band used for embedding thus resulting in a more robust watermarking scheme that is resistant to almost all possible attacks. The watermark is embedded into the luminance component of the extracted frames as it is less sensitive to the HVS.

Yassin *et al.* (2012) introduced a comprehensive approach for digital video watermarking, where a binary watermark image is embedded into the video frames. Each video frame is decomposed into sub-images using 2 level DWT then the Principle Component Analysis (PCA) transformation is applied for each block in the two bands LL and HH. The watermark is embedded into the maximum coefficient of the PCA block of the two bands. The proposed scheme is tested using a number of video sequences. Experimental results show high imperceptibility where there is no noticeable difference between the watermarked video frames and the original frames. The proposed scheme shows high robustness against several attacks such as JPEG coding, Gaussian noise addition, histogram equalization, gamma correction and contrast adjustment.

Karpe and Mukherji (2013) present a novel technique for embedding a binary logo watermark into video frames, based on Discrete Wavelet Transformation (DWT) and Principal Component Analysis (PCA). PCA is applied to each block of two bands (LL–HH) which results from DWT of every video frame. The video frames are first decomposed using DWT and the binary watermark is embedded in the principal components of the low frequency wavelet coefficients.

- **ICA Based Techniques**

DCT and DWT are the two transformation techniques that are widely used in the watermark embedding process. Recently, researchers have started using ICA for watermarking. Gonzalez *et al.* (2001) applied ICA to the blocks of the host image and the watermark image. The least-energy independent components of the host are replaced by the high-energy independent components of the watermark image. For watermark extraction the demixing matrices of both the watermark and the host images are required.

This was followed by the work of Yu *et al.* (2002), where the host image, the key image and the watermark image as the independent sources. Embedding was done by the weighted addition of the key and the watermark to the host. For watermark extraction, two more mixtures were obtained by adding the key and the watermark using different weights. ICA was then applied to these mixtures to separate the host, the key and the watermark. The host and the key both are required for watermark extraction.

Liu *et al.* (2003) used ICA for detection of the watermark which is a random sequence embedded in low-frequency DCT coefficients. Original DCT coefficients are required for watermark detection and for creating a second mixture needed for ICA. Bounkong *et al.* (2003) applied ICA to each block of the host image and obtained its independent components, where the watermark was embedded. In the extraction phase, ICA was applied to each block to obtain the independent components, which was dequantized to extract the watermark.

Recently, ICA was also used by Nguyen and Patra (2004) for upsizing and downsizing. Hien *et al.* (2006) combined ICA and Redundant DWT (RDWT) for successful multilogo watermarking.

- **SVD-Based Techniques**

A third transform called the Singular Value Decomposition (SVD) is also gaining interest in watermarking. The SVD for square matrices was discovered

independently by Beltrami in 1873 and Jordan in 1874 and extended to rectangular matrices by Eckart and Young in the 1930s. It was not used as a computational tool until the 1960s because of the need for sophisticated numerical techniques. In later years, Gene Golub demonstrated its usefulness and feasibility as a tool in a variety of applications (Kahaner *et al.*, 1989). SVD is one of the most useful tools of linear algebra with several applications in image compression (Waldemar and Ramstad, 1997; Aase *et al.*, 1999) and other signal processing fields (Konstantinides *et al.*, 1997; Karkarala and Ogunbona, 2001). Because of its robust nature and the property of maintaining visual quality, SVD in watermarking has been most exploited (Lai *et al.*, 2008; Narasimhulu and Prasad, 2011; Makhloghi *et al.*, 2011).

Raval and Rege (2003) combined wavelets and SVD for developing an adaptive authentication system which utilizes singular values of the blocks within the wavelet subband of the host image. The authors argued that if the watermark is embedded in the low frequency components, it is robust against low pass filtering, lossy compression and geometric distortions. On the other hand, if the watermark is embedded in high frequency components, it is robust against contrast and brightness adjustment, gamma correction, histogram equalization and cropping and vice-versa. Thus, to achieve overall robustness against a large number of attacks, the authors proposed to embed multiple watermarks in low frequency and high frequency bands of DWT. Similarly, adaptive DWT-SVD domain image watermarking scheme was also proposed by Li *et al.* (2007). Ali and Manasrah (2007) described an approach for non-invertible copyright protection of digital images using DWT and SVD.

Ganic and Eskicioglu (2004a, 2004b) developed an authentication technique based on quantization of largest singular values of image blocks in spatial domain was presented. Lee *et al.* (2005) presented a secure SVD-based content authentication watermarking scheme by embedding the watermark into maximum singular values of randomly ordered blocks. Both these methods have good localization but the perceptual quality of watermarked image is not so good even at a high PSNR. That is because they apply the same quantization step size for all blocks in the spatial domain which may have different characteristics.

Dili and Mwangi (2007) projected an image watermarking method using SVD and wavelet transformation. A robust image watermarking scheme in which a binary image is embedded in the singular values of selected DWT blocks in the horizontal and vertical sub-bands of a 1-level decomposition of a gray-scale image was proposed. The embedded blocks are selected by a secret key to enhance imperceptibility. A watermarked image that is perceptually indistinguishable from the original is obtained. The watermarking retrieval is non-blind and require the use of parameters extracted during the watermarking process. The performance of the proposed algorithm is tested by comparing the retrieved watermark to the original watermark. Computer simulation results showed that the algorithm is robust to common signal processing attacks such as Gaussian noise, cropping and low pass filtering. It is also resistant to JPEG compression.

Bhatnagar and Raman (2009) described a new robust watermarking scheme based on DWT-SVD. Their paper described a new semi-blind reference watermarking scheme based on Discrete Wavelet Transformation (DWT) and Singular Value Decomposition (SVD) for copyright protection and authenticity. They were using a grey scale logo image as watermark as an alternative of randomly generated Gaussian noise type watermark.

- **Other Methods**

O'Ruanaidh *et al.* (1996) proposed watermarking by the modification of the phase in the frequency domain using DFT. To embed a bit the phase of a selected coefficient of an N1xN2, DFT is modified by adding a small δ. The phase must satisfy negative symmetry for the watermarked image to be real, which leads to the additional modification.

In another publication, O'Ruanaidh and Pun (1997) explicitly design a watermarking technique invariant to translation, rotation and scaling. The method is a hybrid between DFT and log-polar mapping. A variation of their idea based on the Radon transform was proposed by Wu *et al.* (1999).

The authors of Kim *et al.* (2003c) presented a robust image watermarking technique based on an invariant pattern recognition using radon transform. The scheme can have useful applications in the area of medical imaging. The invariant features were used as a watermark and the extracted features were selected for embedding purpose. The Root Mean Square Error (RMSE) was used as a similarity measure and this technique has the ability to resist the geometric distortions.

Khan and his team (Khan, 2006a, 2006b, Khan *et al.*, 2008) performed experimental studies and improved the watermarking method proposed by Loo (2003) used a spread spectrum watermarking approach based on complex wavelet transform. The results showed that the method was improved to resist some attacks.

Some proposed methods in frequency domain focus on embedding two or three watermarks and are discussed in the following paragraphs. The authors of Cheng *et al.* (2004), proposed an algorithm which was based on embedding the watermark image in three times at three different frequency bands, namely, low, medium and high and the results proved that the watermark cannot be totally destroyed by either low pass, medium or high pass filter. In Chun-Shien *et al.* (2000), two complementary watermarks were embedded into the host image in order to make it difficult for attackers to destroy both of them.

Chrysochos *et al.* (2008) presented a new robust watermarking scheme. The algorithm is based on a chaotic function and a correlation method for detection, operating in the frequency domain. The scheme is blind and comparing to other chaos related watermarking methods, experimental results exhibit satisfactory robustness against a wide variety of attacks such as filtering, noise addition, geometric manipulations and JPEG compression with very low quality factors. The scheme also outperforms traditional frequency domain embedding both in terms of robustness and quality.

The main benefit obtained from these techniques is that they can take advantage of properties of alternate domains to address the limitations of pixel-based methods or to support additional features. For example, using DCT in the watermark algorithm lead to better implementation compatibility with popular video coding

algorithms like MPEG-2 and in the shift and rotation-invariant Fourier domains facilitates the design of watermarks that inherit these attractive properties. Besides, analysis of the host signal in a frequency domain is a prerequisite for applying more advanced masking properties of the HVS to enhance watermark robustness and imperceptibility. Generally, the main drawback of transform domain methods is their higher computational requirement.

2.3.3. MPEG-Based Watermarking Schemes

There is a number of MPEG-2 and MPEG-4-based techniques that have been proposed, including approaches based on GOP (Group of Pictures) modification (Linnartz and Talstra, 1998), high frequency DCT coefficient manipulation (Chung *et al.,* 1998), DCT block classification (Holliman *et al.,* 1997).

Vassaux *et al.* (2002) proposed a video object watermarking which is based on the structure of MPEG-4. In their method, a scrambling technique that allows adapting any classical spread spectrum watermarking scheme operating in the spatial domain to the MPEG-4 was proposed. This technique could be easily added to the embedding and detection schemes without changing the watermarking algorithm. It modified some predefined pairs of quantized DCT coefficient in the luminance block of pseudo-randomly selected MBs and was based on spread-spectrum techniques. In this method, the image was first divided into equal sized blocks, where a binary sequence generated using secret key is embedded to the image.

Swanson *et al.* (1997) presented an object-based transparent watermarking procedure for copyright protection into video sequences. To address issues associated with video motion and redundancy, individual watermarks were created for objects within the video. Each watermark was created by shaping a pseudo-random sequence according to the perceptual masking characteristics of the video. This resulted in a watermark that could adapt to each video and ensured invisibility and robustness. Furthermore, their experimental results showed that the noise like watermark was statistically undetectable to prevent unauthorized removal.

Another video object-based watermarking was proposed by Lu and Liao (2001), which was mainly developed to resist rotation and flipping attacks. In this technique, a robust watermarking scheme for video object protection was proposed, where the video object was segmented initially. For each segmented video object, a watermark was embedded using a new technology that used eigen vectors of a video object. Using eigen vectors solved the asynchronous problem caused by object placement and was proved to be robust in terms or rotation and flipping.

Mobasseri (1998) proposed direct sequence watermarking using m-frames. This scheme applied a direct sequence spread spectrum model to the watermarking of the digital video. First, the video signal was modeled as a sequence of bit planes arranged along the time axis. Watermarking of this sequence is a two layer operation. A controlling m-sequence, first establishes a pseudorandom order in the bit plane stream for later watermarking. Watermark, defined as m-frames, supplant the tagged bit planes. Moreover, attempts in corrupting the image to destroy the watermark render the video useless before damaging the seal itself. The watermarked video was also robust to video editing attempts such as subsampling, frame reordering etc. The watermark is also identifiable from a very short segment of video. Individual frames extracted from the video also contained the copyright information.

Video watermarking techniques that use MPEG-1, MPEG-2 and MPEG-4 coding structures as primitive components are primarily motivated by the goal of integrating watermarking and compression to reduce overall real-time video processing complexity. Compression in block-based schemes like MPEG-2 is achieved by using forward and bi-directional motion prediction to remove temporal redundancy and statistical methods to remove spatial redundancy. One of the major drawbacks of schemes based on MPEG coding structures is that they can be highly susceptible to re-compression with different parameters, as well as conversion to formats other than MPEG.

2.4. HVS-BASED TECHNIQUES

The notion of using watermark as a masking phenomena with constraints of non-visibility is performed using the HVS properties. Much research has been done to increase the robustness and the data hiding capacity of watermarking techniques based on perceptual properties of the Human Visual System (HVS). Kay and Izquierdo (2001) used a content based estimation of Just Noticeable Difference (JND) in frequency domain. To estimate the JND three image characteristics were considered, namely, texture, edgeness and smoothness. Their results proved that this technique was resilient to most common attacks like geometric image transformations.

Recently this work was improved by Parthasarathy and Kak (2007). In this work, they considered the texture, luminance, corner and edge information of an image to create a mask that makes the watermark addition to the image less perceptible to the human eyes. The embedding and extraction are done in frequency domain, thereby gaining robustness against common attacks like compression and filtering. The results provided are encouraging.

Much research has been done to increase the robustness and the data hiding capacity of watermarking techniques based on perceptual properties of the Human Visual System (HVS) (Swanson *et al.*, 1998b; Cox and Miller, 1997; Wolfgang and Delp, 1996). The development and improvement of accurate human vision models help in the design and growth of perceptual masks that can be used to efficiently hide the watermark information, thereby, increasing its security.

Similarly, in the work proposed by Kankanhalli (1998) the noise sensitivity of each pixel based on the local region image content such as texture, edge and luminance information was used to obtain the JND mask for the image to be watermarked. Then each bit of the watermark is spread spatially and shaped by pseudo-noise sequence such that its amplitude is kept below the noise sensitive of the pixel into which it is inserted. Experimental results proved that the technique was resistant to compression, cropping and noise attacks.

Parameswaran (2005) proposed a content dependent image signature for authentication using wavelet domain. Most of the work in the literature uses DCT domain for content based watermarking. This work differed by using wavelet for image authentication. This work was followed by Parameswaran and Anbumani (2006) proposed a robust image watermarking scheme to withstand geometric attacks using content based watermarking techniques. The watermarking was performed in four steps, namely, image normalization, content based watermark generation, watermark embedding and watermark extraction. Wavelet domain was used to construct the content dependent watermark and the watermark was embedded in the mid-frequency coefficients in the wavelet domain. The experimental results proved that the scheme proposed was very effective and was able to withstand attacks like copy attack, crop attack, protocol attacks and cryptographic attacks.

Later in 2007, Li and Si proposed a fragile watermarking scheme based on DWT domain which was able to resist all kinds of manipulations and had the ability to localize the tampered regions. To achieve high transparency while providing protection to all coefficients, the embedder algorithm involved all the coefficients within a hierarchical neighborhood of each sparsely selected watermarkable coefficient during the watermark embedding process. The way the non-watermarkable coefficients are involved in the embedding process is content-dependent and nondeterministic, which allowed the proposed scheme to put up resistance to the so-called vector quantization attack, Holliman-Memon attack, collage attack and transplantation attack.

Xie *et al.* (2008) proposed a novel content based watermarking technique in ridgelet domain. The blocks were classified using image texture characteristics and to improve the robustness middle frequencies of the subband was used. The watermarks were embedded in the most important energetic directions of the pieces with strong texture which are less sensitively to human's vision. Experimental results showed that the watermarked scheme was robust to noise, cut and other intensive attacks.

Kim and Lee (2004) presented a content based fragile watermarking scheme for image authentication. This model was able to tolerate incidental distortions and indicated tampered regions in case of malicious manipulation. The watermark was extracted based on the image content and was inserted into the DCT block.

2.5. REAL-TIME WATERMARKING

Real-time property is another additional specification of video watermarking, which did not play a predominant role with still images. When a person wants to embed a watermark or to check the presence of a watermarking an image, a few seconds is an acceptable delay. However, such a delay is unrealistic in the context of the video. Frames are indeed sent at a fairly high rate, typically 25 frames to obtain a smooth video stream. At least the embedder or the detector and even sometimes both of them, should be able to handle such a rate. In the context of broadcast monitoring, the detector should be able to detect an embedded watermarking real-time.

In a VOD environment, the video server should be able to insert the watermark, identifying the customer, at the same rate that the video is streamed. In order to meet the real-time requirement, the complexity of the watermarking algorithm should obviously be as low as possible. Moreover, if the watermark can be inserted directly into the compressed stream, this will prevent full decompression and recompression and consequently, it will reduce computational needs. This philosophy has led to the design of very simple watermarking schemes.

Exploiting the very specific part of a video compression standard can lead to very efficient algorithms. An MPEG encoded video stream basically consists of a succession of Variable Length Code (VLC). A watermark can consequently be embedded in the stream by modifying those VLC code words (Langelaar and Lagendijk, 2001). The MPEG standard uses indeed similar VLC code words i.e. with the same run length, the same VLC size and a quantized level difference of one. Such VLC code words can be used alternatively in order to hide a bit.

Another way of achieving real-time is to split the computations. The basic idea is to perform intensive computations once for all on the provider side and then simple client-dependent processing on request. This can be seen as some sort of preprocessing (Cox and Miller, 2002). Blind watermarking schemes, i.e. which do not consider the data to be watermarked, are the simplest but are usually avoided in order to obtain good detection statistics. However, if some preprocessing operations are performed before, then such a scheme may be efficient. As a result, blind watermarking can be used reliably later on client request.

When considering real-time, the watermarking algorithm, named Just Another Watermarking System (JAWS), designed by Philips Research is often considered as a reference. The JAWS algorithm was originally designed for broadcast monitoring and is actually one of the leading candidates for watermarking in DVD. The real-time requirement is met by using simple operations at video rate and only a few complex ones at a much lower rate (Kalker *et al.*, 1999).

2.6. CHAPTER SUMMARY

From the literature study, it can be understood that research in the area of video watermarking is strongly motivated by an increasing need from the copyright owners to reliably protect their rights. Because of the large economic stakes, digital watermarking in video domain is promised to a great future. New applications are likely to emerge and may combine existing approaches. This technology is still in its infancy and is far from being as mature as for still images. Quite all possible image processing techniques have been investigated for still images watermarking. On the other hand, many video processing techniques have not been tried and the line is consequently not exhausted.

As a conclusion, spatial domain methods are simple and fast, but are not robust against attacks. In comparison, transform domain watermarking techniques are more robust. Compressed domain methods are fast, robust, but are bound to the compression standard and moreover, any transcoding to a different standard would destroy the watermark.

Many more investigations and novel algorithms are required to improve the process of video watermarking. This research work, in this line proposes enhanced video watermarking techniques for uncompressed and compressed video data. In any watermarking algorithm, the place of embedding the watermark is very important and has to be chosen carefully, so that no distortion is visible. For this purpose, the study introduces techniques that selects frames and regions that have minimum impact on the visual quality of the video after the insertion of watermark. The technique used for this purpose is explained in detail in the next chapter (Chapter 3, Methodology).