CHAPTER 2

LITERATURE SURVEY

2.1 DIGITAL IMAGE WATERMARKING

Watermarking has been an extremely active research area over the past three decades. For the technical and commercial feasibility in all media types like audio, digital photographic image, printed materials or compound document images, digital watermark has been investigated deeply. The properties of a digital watermark are given by Swanson et al (1996), Pitas (1996) and Cox et al (1997). The properties are 1) watermark should be perceptually invisible 2) extraction should be simple 3) detection should be accurate 4) more robust 5) should be able to determine the true owner. Following review articles contain references to a large number of watermarking systems and descriptions of the technologies implemented.

The properties of HVS model and its specific details are given in (Daly 1994, Eckert and Bradley 1998). HVS is used to investigate perceptual characteristics of human and how to insert the watermark image into the original image. Eskicioglu and Delp (2001) has given a proven method for reducing content privacy, improving the ability to identify the region and manage digital media. This method is widely used in applications of rights management, remote triggering, filtering/classification, e-commerce, etc. Overviews of different types of digital image watermarking techniques based on HVS are available in (Koz and Alper 2002). Adaptive digital image watermarking technique and geometric invariant digital image watermarking

2.2 FRAGILE AND SEMI-FRAGILE WATERMARKING

Fragile and semi-fragile watermarks are usually applicable in medical, forensic and military. Authentication is mainly classified based on the real time applications into two types namely, extract authentication or global authentication and selective authentication or local authentication. Extract authentication is accomplished by fragile watermarking. Fragile watermark is very sensitive and designed to detect every possible change in a marked image. Therefore, fragile watermarking algorithms are used in building content authentication system. Some applications do not need extract authentication and only need to verify some selective places in the work in order to be authenticated. For selective authentication, semi-fragile algorithms are used. A semi-fragile watermark is robust to acceptable content preserving manipulation such as lossy compression. Various techniques used for fragile and semi-fragile watermarking system are described by Chih-Ho and Li (2004), Wu et al (2005).

The existing fragile watermarking techniques are content based image authentication and recovery (Phen-Lan et al 2004), disordered image pattern (Shao-Hui Liu et al 2007), a public key cryptosystem (Hajime and Keiichi 2010), advanced video coding (Chuen-Ching and Yu-Chang 2010) and block-wise mechanism (Sergio and Asoke 2011). In semi-fragile watermarking scheme, effective analysis is carried out by nested lattice code (Chuhong et al 2006) and the content authentications of satellite images using
the Pinned Sine Transform (PST) (Ho et al 2005). The concept of lowest authenticable JPEG quality (LAJQ) (Chih-Hung et al 2007) and tamper-proofing (Nozomi and Koki 2007) are applied to the Joint Photographic Experts Group (JPEG) compressed images in semi-fragile watermarking scheme. Vector quantization and content based methods in DWT are used to improve the visibility for selective authentication is described by Cruz et al (2008) and Xiaojun and Xing (2011). New semi-fragile watermarking methods for the authentication of 3D models based on integral invariants are described (Sathiyaseelan et al 2011).

Fragile watermarks are difficult to be adapted with the applications of JPEG compression image. In fragile watermarking, the host image to be watermarked may be perceptually different. In this technique, anyone can remove the watermark easily. To make the watermark robust, some researchers had developed another watermarking scheme.

2.3 ROBUST IMAGE WATERMARKING

A watermark embedded in a host image must be robust to the distortions occurred during the normal usage of images. Those distortions include image enhancement, JPEG compression and geometrical modifications. The desirable properties are perceptual transparency, data capacity, robustness to image processing operation and computational complexity. Blind watermark is a robust watermarking technique. The primary applications of robust watermarking include copyright protection and content tracking.

Multipurpose watermarking scheme, robust and fragile watermarks are simultaneously embedded using cocktail watermark for copyright protection and content authentication is described by Chun-Shien and Hong-Yuan (2001). In robust watermarking schemes, space-time coding is
used in colour images, has an advantage of low visible distortion in the host image and it is very robust to various attacks are explained by Barni et al (2002). Pixel Value Mapping Algorithm (PVMA) and Pixel Position Shift Algorithm (PPSA) are the kind of lossless visible watermarking schemes discussed by Shu-Kei et al (2006).

Various concepts and research work in the field of image watermark authentication are discussed (Radharani and Valarmathi 2010). Digital data entropy based robust watermarking scheme using Hadamad Transformation (HT) technique is described by Franklin et al (2011) and the scheme is more robust to attacks, such as, random noise, scaling and cropping attack. Blind robust watermark encryption under non-cascade phase retrieve algorithm and Random Fractional Fourier Transform (RFrFT) are explained in Deng et al (2011). Spatial and frequency domain techniques are the two categories of robust watermarking technique.

2.4 SPATIAL DOMAIN WATERMARKING

Spatial domain techniques are the one, which act directly on the image by modification of the values of the image pixels, in order to embed the watermark into the image. These techniques can modify the colour, luminance or brightness values of digital image pixels and can be easily implemented with minimum computation power requirements. Important spatial domain techniques are LSB technique, patchwork technique and digimarc algorithm.

One of the simplest techniques is LSB and it is explained in (Schyndel et al 1994, Pitas 1998). To fulfill all quality and functionality requirements in spatial domain, an invariant property of transform (O’Ruanaidh and Pun 1998, Bas et al 2002) and objective transform algorithms (Vleeschouwer et al 2001) are used. In most cases, spatial domain
watermarking is a non-blind technique to embed a watermark in the LSBs of some randomly selected pixels, described in Zhejiang and Migmin (2004).

Liu-Jan and Liu-Lizhi (2008) have developed an improved watermark detection algorithm for colour image based on a block probability in spatial domain. Digital watermark based on pixel averaging and unbiased watermark retrieval methods are described by Pramoun and Amomraks (2009). Review of spatial domain parameter estimation procedures and testing methods are clearly presented in Brown and Allemang (2009). Modulo operations are used to embed the watermark and extract it from the original image as described by Kumari et al (2010). Here, the number of bits embedded in a pixel is determined by the degree of modulo algorithm. In colour image zero-watermarking scheme, 2D colour histogram is used for embedding process and the results obtained from this technique are more robust to affine transformations, cropping, additive noise, filtering and JPEG compression which is also explained in Shengli et al (2010).

The watermarks are easily embedded and mathematically analyzed, in the case of spatial domain technique. However, the embedded watermark can be easily removed by simple image processing such as noise addition. This makes most of the current watermarking schemes to use the frequency domain techniques, such as DCT, DFT and DWT.

2.5 FREQUENCY DOMAIN WATERMARKING

In the case of lossy compression, spatial domain technique is not a reliable choice. In frequency domain, the watermark is applied to the whole image, so that the watermark cannot be removed, when cropping of the image is done. The frequency domain techniques are based on the usage of some invertible transformations like DCT, DFT, and DWT to the host image. Here, watermark is embedded by modifying the transform coefficients, in
accordance with image to be watermarked or its spectrum. Finally, inverse transform is applied to obtain the watermarked image. This approach distributes irregularly the watermark, over the image pixels after the inverse transform, thus making detection or manipulation of the watermark more difficult. These methods are more complicated and require more computational power.

2.5.1 Discrete Cosine Transform

In spread spectrum, DCT is used. DCT is preferred for watermarking because of its higher imperceptibility and that they are more robust to image manipulations. DCT represents an image as a sum of sinusoidal varying magnitude and frequency. DCT result images have higher visual quality than the spatial domain (Flipping). Therefore, DCT methods are normally selected for gray and colour image watermarking even though their algorithms are computationally complex.

A bit present in the information is encoded in a block using the relationship between the three quantized DCT that is available in Zaho and Koch (1995). Bors and Pitas (1996) developed the method to modify the DCT coefficient to fulfill the block selection constraint. Sequence of real number is used as a mark (Key) to embed the data in DCT domain is explained in Cox et al (1996 a) and Swanson et al (1996) and its results are proved that these watermarks are more robust in JPEG compression. Threshold technique is used to generate bidirectional coding, which acts as a private key for DCT domain watermarking is described by O’Ruanaidh et al (1996).

DCT is used to embed the watermark image in middle band frequency range is explained in (Weili and Aoki 1997). Adaptive watermarking technique in DCT is described by Dickinson and Tao (1997). Arranging the DCT coefficient in a zigzag order and adding them in mid
frequency range to preserve perceptual invisibility is explained by Barni et al (1998). The blocks chosen for embedding the watermark are selected based on gaussian network classifier and then linear DCT constraints are embedded in selected blocks which are clearly explained in (Bors and Pitas 1998). DCT coefficient is calculated according to the analysis of noise sensitivity of every pixel based on the local region content (texture, edges and luminance) and is clearly explained in Kankanhalli and Ramakrishan (1998). A blind technique, to transform an image based on the table lookup method in the frequency domain watermarking is explained in (Wu and Liu 1998). Public watermarking technique is used to embed a signature into image in Chae and Manjunath (1999).

DCT with variable block-size (Hyung et al 1999) and fixed block size algorithms (Hsu and Wu 1999) are developed to embed the image watermark; the results proved that the technique successfully survives the image processing operations, image cropping and JPEG lossy compression. DCT domain visible image watermarking technique for gray and colour images are described by Mohanty et al (2000) and Mohanty et al (1999).

2.5.2 Discrete Fourier Transform

DFT technique is required for watermarking to satisfy the important property of translation in variants. Circularly symmetric watermark embedding in Two Dimensional Discrete Fourier Transform (2D-DFT) is explained in (Solachidis and Pitas 1999), which is more robust to rotation and scaling attacks. The entire watermark is modulated by a binary pseudo-noise matrix and then modulated watermark is embedded into FT of cover image described by Kim et al (1999a). Watermark is added to a template in the FT domain to obtain more robustness than in the case of Linear Transformation (LT) is discussed in Pereira and Pun (2000). Fourier Mellin Wavelet (FMW) performs log-polar map (LPM) on DFT domain and needs an interpolation of
two dimensional Discrete Fourier Transform (2D-DFT) magnitude with large
dynamic range of neighboring coefficients pointed out by Langelaar et al

2.5.3  Discrete Wavelet Transform

DWT has been used over a long period of time in digital image
water marking, due to its time/frequency decomposition characteristics. This
resembles the theoretical model of HVS. In wavelet transform, an image is
decomposed into a set of band limited component, which can be reassembled
to reconstruct the original image without error. DWT has the advantages of
being closer to HVS and have a higher compression ratio than DCT.

First level discrete wavelet decomposition of watermark is
available in Kundur and Hatzinakos (1997). Multi-resolution private
watermark for digital image using DWT is described by Xia et al (1997) and
scheme uses binary code (Inoue et al 1999), Embedded Zero tree Wavelet
(EZW) (Shapiro 1993), pseudo-random sequence (Barni et al 1999) to
embed a watermark image. Tree level wavelet based multi-resolution
watermark is introduced by Kim et al (1999 b) and improved wavelet based
watermark technique is explained by Barni et al (2001). DWT is a
hierarchical sub-band system, where the sub-bands are logarithmically spaced
in frequency. DWT can be implemented using digital filters and down-
samplers are in literature (Gonzalez and Woods 2002). Wavelet based
watermarking algorithm for ownership verification of digital images using
private key are explained in Wang et al (2002). Composite image watermark
on DWT and DFT is described by Xiangui Kang et al (2003). Zero location
watermarking in Z-transform and wavelet domain watermarking in JPEG
compression are the various embedding techniques used in biomedical
images, mentioned in Anthony et al (2004). It provides good space of
frequency locations for analyzing the image features such as edges or textured areas.

A robust watermarking scheme using best tree wavelet packet transform is explained by Rawat et al (2009). The prominent watermarking techniques available for still images are DCT (Mohanty et al 2000) and DWT and Image Adaptive Discrete Wavelet Transform (IADWT) (Franco and Del 2008). Robust video DWT domain watermarking technique is described in Rini (2011). In this scheme the quantization model used for quantizing the wavelet coefficient is based on the characteristics of HVS.

Some of other transforms used to embed watermarks are multi-resolution transform and complex HT (Falkowski and Lip-San 2000), normalization based watermark (Alghoniemy and Tewfik 2000), Karhunen Loeve (KL) transform (Moulin and Ivanovic 2003), probability based watermark (Nasir et al 2007), quantization index modulation and distortion-compensated (Chen and Wornell 2001) and discrete pascal transform (Mahmoud et al 2008).

2.6 SPATIAL AND FREQUENCY DOMAIN ALGORITHMS

Each of the methods have certain advantages and disadvantages depending on a solution of concrete problem of information protection. It is well known that there are three main mutually conflicting properties of information hiding schemes: capacity, robustness and indefectibility. But these three properties can be found in a watermarking algorithm or technique, only with the idle case. At the same time, it is obvious that an image of quite acceptable quality can be obtained by means of combining and manipulating various watermarking algorithms in the spatial and frequency domains. George et al (2002) described a method of combining frequency and spatial
domain for low bit rate compressed image. Review of robust video watermarking techniques is available in Rini (2011).

2.7 HARDWARE IMPLEMENTATION

Implementation of any existing watermarking algorithm is not a difficult task. But the speed of embedding a watermark into an image decreases as the complexity of the algorithm grows on. To provide flexibility to the user who wants to copyright their images taken through a digital camera, it is better to provide the watermarking scheme in the digital camera itself rather than through a software procedure. This reduces the complexity of producing a copyrighted image (taking an image and then passing it through watermarking software to get the image copyrighted). In digital cameras JPEG is the most popular standard which produce high quality picture. Explanation of VLSI architecture and FPGA prototyping of a digital camera for image security and authentication is available in Oluwayomi et al. (2006).

Most of the available systems would be hard to name or compare. Some of the hardware implementations are listed. Hardware implementation of digital video watermarking algorithm is explained in Nebu et al. (2003). A systems level design for embedded watermark technique using camera system (DSC) is described in Tsai and Lu (2001). Garimella et al. (2003) has described VLSI implementation of the fragile invisible digital watermarking technique in spatial domain for 8-bit gray scale images. Here, the standard ASIC design flow for a 0.13\(\mu\)m CMOS technology has been used to implement the algorithm. The area of the chip is 3453\(\times\)3453\(\mu\)m\(^2\) and the power consumption is 37.6\(\mu\)W.

Content based visible watermark (Mohanty et al 1999) and invisible watermark (Mohanty and Nayak 2004) are explained and implemented in
hardware. In invisible watermarking technique, the key is used for embedding the watermark in the host image and the watermark scheme is evaluated by using stir mark. The host image is required for retrieval of watermark image. XCV50-BG256-6 device is used for implementation. Tefas and Pitas (2001) and Bartolini et al (2001) also implemented invisible robust watermarking algorithms in hardware.

al (2009). This method is more robust against the various attacks like communication signals noise and median filter.

A comparative study on the performance of novel robust spatial domain digital image watermarking with DCT is available in Rajesh et al (2010). Multiple binary images watermarking in spatial and frequency domains technique is explained by Ganesan and Tarun (2010). FPGA and ASIC implementation of robust invisible spatial domain prototype algorithm is tested in Virtex–E by Karthigaikumar and Baskaran (2011). Here, the host image is required for retrieval of watermark image.

In combination of spatial and transformed watermarking scheme, the watermarked image is split into two parts depending on the information. To improve the perceptibility of watermarked image the essential part is hided in the block of the host image using transform domain. The remaining part of the watermark image is embedded in spatial domain explained in Frank and Scott (2003). Heuristic method is described in Chin-Chen et al (2006) and it explains how the extracted watermark image quality can be enhanced. Multiple binary images watermarking in spatial and frequency domain techniques are available in Ganesan and Tarun (2010).

A comparative study on the performance of novel robust spatial domain digital image watermarking with DCT based watermarking is explained in Rajesh et al (2010). Gray, colour and biometric images are chosen as watermark and it is embedded in an original image under block based algorithm described in Dogan et al (2011). This algorithm is modeled by using verlog hardware description language (VHDL) and it is implemented on XC2V500-6FG256 device in Xilinx. To test the implementation results of watermark in software and hardware, performance analysis report is required.
2.8 PERFORMANCE ANALYSIS REPORT

A fair benchmark, which is used to test the image watermarking systems, is explained in Kutter and Petitcolas (1999). Internet image library (IIL) is used for copyright protection in the internet and their analysis reports are available in Pei-Chun et al (1999). A blind digital image/video watermarking multi-resolution pyramid transform technique is proposed and their performance results are available in Qiang and Huang (2000). Robustness of the spatial and frequency domain multiple data embedding technique watermark is tested by introducing several attacks and testing the watermark strength, as is in Samuel et al (2010). The analysis of watermark techniques using Zernike moment and DCT performance are evaluated in Ekta and Anu (2011).

Some of the software watermarking algorithms and techniques portray us the ways in evolving a new watermarking algorithm, which is implemented in the hardware with a higher throughput. Review of the performance analysis of the existing techniques help us in the comparison of the robustness and quality of our proposed work. This helped us a great deal to start this thesis with different features in the domain and also to optimize the existing systems.