CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION

Watermarks do not always need to be hidden. Watermarking can be broadly classified in two categories:

- Visible watermarking
- Invisible watermarking

Most of the literature has focused on the invisible digital watermarking as it has more applications in recent years.

2.1.1 Visible Watermarking

Visible watermarking was the first and most primitive way of watermarking. This makes the watermark visible on the cover object.

Luo et al (2006) proposed a visible watermarking technique to embed a perceivable image in a host image for copyright protection. Visible watermarking decreases the quality of original image.

Though visible watermarking has been used for very long time, it is not secure form of watermarking. This form of watermarking could only be used for owner identification purposes. For all other applications invisible watermarking is used.
Huang and Wu (2004) attacked the visible watermarking schemes and demonstrated that robustness of the visible watermarking schemes for digital images is doubtful and needs to be improved.

2.1.2 Invisible Watermarking

The watermark is perceptually invisible. Invisible watermarking retains the quality of original work. Invisible watermarking can be implemented by using number of techniques.

The simplest technique used in hidden watermarking is to hide the watermark in the Least Significant Bits (LSB) of the cover object. The advantage of this method is that, even if a part of the watermarked image is cropped the receiver can still get the required message, as the message is embedded multiple times. The message is considered to be very small as compared to the cover object.

For example, in an 8 bit file, each pixel is represented by 8 bits. If the Most Significant Bit (MSB) is changed it will have a big impact on the image. However, if the LSB is changed, it will have minimal effect.

If one changes two least significant bits in the image, the human eye could not find the difference of the last two bits being changed. For example, if we take 10001100 and change it to 10001111 or 10001110, it will seem like the same color to the human eye. So data are embedded in those bits. The following example illustrates this concept.

If the message converted to binary is 1101 0010, the first 4 pixels will be modified as follows:
- 1100 0101 becomes 1100 0111
- 1111 0010 becomes 1111 0001
- 1010 1111 becomes 1010 1100
- 0010 0010 becomes 0010 0010

The simple attack to make the watermark useless would be to change all the least significant bits as 1. So it is not a robust watermarking technique. One more fact under consideration should be that once the algorithm is discovered by the attacker it would be easy for him to change the watermark. This system has a major drawback as it cannot use a key to hide the data.

2.2 ROBUST IMAGE WATERMARKING DOMAINS

Watermarking algorithms can be classified into two categories according to domain of watermark insertion (Craver et al 1998). They are,

i) Spatial Domain Watermarking Techniques

ii) Transform or Frequency Domain Watermarking Techniques

2.2.1 Spatial Domain Watermarking

The most direct approach is watermarking in the spatial domain where pixel values are modified to encode the watermark signal.

Mukherjee et al (2004) presented an invisible spatial domain watermark insertion algorithm for buyer authentication in which the watermark can be recovered, even if the attacker tries to manipulate the watermark with the knowledge of the watermarking process. The process incorporates buyer specific watermarks within a single multimedia object, and
the same multimedia object has different watermarks that differ from owner to owner. Therefore recovery of this watermark not only authenticates the particular owner of the multimedia object but also could be used to identify the buyer involved in a forging process.

Wu (2006) presented an adaptive collusion attack on a buyer authentication watermarking scheme. Yoshida et al (2006) proposed an optimum detection scheme for additive watermarks embedded in spatial domain. A new spatial perceptual mask was proposed by Karybali and Berberidis (2006) which matches very well with the properties of the HVS.

Coltuc and Chassery (2007) proposed a very fast spatial domain digital image watermarking by using Reversible Contrast Mapping (RCM). The RCM scheme provides robustness against cropping. The other types of attacks were not discussed. Capacity and robustness formulas of a robust image watermarking in spatial domain was presented by Jun et al (2008).

Abraham and Paul (2011) proposed a novel method for watermarking gray scale images in spatial domain by modifying the least significant bits of the pixels in the image. The embedding process creates a watermarked image with hidden information that in future can proclaim its ownership details.

Ko et al (2005) proposed a new digital audio watermarking method to improve the weak points of conventional echo hiding techniques, such as a lenient decoding process, weakness against multiple encoding attacks, and so on. The basic idea of the proposed method is to spread an echo using Pseudo random Number (PN) sequences in the time domain.
2.2.2 Transform Domain Watermarking

A very common technique is the implementation of the watermark in the frequency domain using discrete transforms. Thus, the energy of the watermark is distributed over the entire image after the transformation back to the spatial domain, which enables the implementation of stronger watermarks with less perceptual impact. Frequency domains such as DCT, DFT and DWT are widely used in image watermarking. Other domains include Radon transform, fractals transform, chirp-Z transform, Hadamard transform, Singular Value Decomposition (SVD), Slant transform (SLT) and Fourier-Mellin Transform (FMT).

Cox et al (1997) invented the idea of using spread spectrum for embedding watermarks in the DCT domain. The host image is viewed as a communication channel, while the watermark as a signal to be transmitted. The watermark message is inserted throughout the perceptually important part of the signal spectrum. The watermark cannot be destroyed without damaging the watermarked image. It is not a blind watermarking scheme as the original image is required for watermark extraction.

DCT domain watermarking technique for copyright protection of still digital images is analyzed by Hernandez et al (2000). The DCT is applied in blocks of 8 × 8 pixels. The watermark can encode information to track illegal misuses.

A method called differential energy watermarking was proposed by Langelaar and Langendijk (2001). A macroblock which composes of several 8x8 DCT blocks is divided into two parts to embed a watermark bit. High-frequency DCT coefficients in the compressed bitstream are selectively discarded to produce an energy difference between two parts of the same macroblock, where the energy difference is determined by the watermark bit.
This scheme has three parameters: the number of 8x8 DCT blocks in a macroblock, JPEG quantization step size, and a minimal cutoff index for watermarking. By adjusting these three factors, appropriate marking systems are obtained for different applications.

A DCT-based blind image watermarking algorithm is described by Chu (2003), where the original image is not required for watermark recovery, and is achieved by inserting the watermark in subimages obtained through subsampling. Briassouli et al (2005) proposed and analyzed an improved blind watermark detector for DCT-transformed images based on the statistical properties of the DCT coefficients.


Lu et al (2007) presented a digital watermarking scheme based on the DCT and SVD. In this method, selected mid-band DCT coefficients from 8x8 block DCT are selected to form blocks which are later decomposed into three matrices, i.e. U, S and V. Finally the original watermark is also partitioned into blocks and then embedded into the matrix S. Haj (2007) described the performance of the combined DWT-DCT watermarking algorithm. A DC-based watermark to improve the robustness was proposed by Lee et al (2007) in DCT domain. Guo and Lu et al (2008) presented a robust and semi-blind watermarking by embedding information into low frequency coefficients of DCT.

Zeng and Qiu (2008) proposed a novel blind robust watermarking scheme which embeds a digital watermark into the DCT coefficients of the
host image based on HVS. Watermark extraction utilizes Independent Component Analysis (ICA) technique which is a blind source separation procedure without requiring the host image and the original watermark. Chen and Kao (2007) presented a reversible image watermarking approach that works on quantized DCT coefficients. Karabat and Keskinoz (2008) presented new spread spectrum watermarking system in DCT domain employing reference watermarks to estimate the channel and attacks.


Pei and Guo (2003) proposed a low computational complexity noise balanced error diffusion technique for embedding watermark into error-diffused halftone images.

Lu et al (2005) presented a multipurpose digital image watermarking method based on the multistage Vector Quantizer (VQ) structure, which can be applied to image authentication and copyright protection. In this method, the semi-fragile watermark and the robust watermark are embedded in different VQ stages using different techniques.

Dong et al (2005) presented two watermarking approaches that are robust to geometric distortions. The first approach is based on image normalization and the second approach is based on a watermark resynchronization scheme aimed to alleviate the effects of random bending attacks. Lu et al (2006) proposed a media hash dependent image watermarking scheme that can withstand geometric distortions and watermark estimation attacks. A new method to reduce the host interference in spread spectrum watermarking detector was presented by Sedghi and Suzuki (2007).

A novel watermarking scheme was presented by Boato et al (2007) which allow to insert and reliably detect multiple watermarks sequentially embedded into a digital image for the applications such as multimedia document tracing, data usage monitoring, and multiple property management.

Thodi and Rodriguez (2007) proposed reversible watermarking technique which enables the decoder to not only extract the watermark, but also perfectly reconstruct the original image from the watermarked work.

A novel watermarking algorithm was proposed in contourlet domain with ICA by Xu et al (2006). Salahi et al (2008) described a new blind spread spectrum image watermarking in contourlet domain. Lin et al (2006) described a sub-sampling and Phase Shift Keying (PSK) based watermarking scheme which can resist the permutation attacking. An image watermarking scheme based on histogram was proposed by Fang and Zhao (2006). This scheme was developed to resist geometric attacks. Peng et
al (2006) proposed a new type of multi-user digital watermarking based on Code division Multiple Access (CDMA), which aims at the demand of multi-user copyright sharing protection.


Robust blind watermarking method for three dimensional volumes was presented by Solachidis and Pitas (2007). A bivalued watermark is embedded in the DFT magnitude of the three dimensional volume. Konstantinides et al (2009) presented a new approach to blind three dimensional mesh watermarking, with high imperceptibility and robustness against similarity transformations, connectivity attacks, mesh simplification, unbalanced resampling, smoothing and noise addition. Khawne et al (2007) presented a study of image watermarking using robust SVD in L1-norm subspace. The watermarked image attacked by noise is greatly degraded. This results in the effects of transparency and robustness of the watermarked image. Although the watermarking in SVD domain is sensitive to noise and outliers, incorporating L1-norm regression to the watermarking algorithm can help handling the missing data caused by noise and help increasing the robustness of the watermarking algorithm. A method for enhancing the image quality of watermarked binary images containing text, drawings, graphs and tables was described by Ebisawa et al (2007). Huang et al (2007) discussed the optimization of robust watermarking with genetic algorithms. A novel fast

A capacity variable watermarking algorithm for engineering graphic based on complex number system was proposed by Huang et al (2008). Guo and Yang et al (2008) presented two watermarking approaches in fractal coding images. The first method, namely Mean Classified Fractal Coding (MCFC), partitions the domain blocks of an image into groups according the mean values. The second method, namely Hierarchical Block Matching Fractal Coding (HBMFC), utilizes different domain block sizes to enlarge the searching pool with slightly sacrificing the coding gain. Wang et al (2008) presented three blind watermarking methods that can embed several bits binary data into a vector image without changing its appearance. Zhang and Boston (2008) proposed a new image watermarking method called stylometric watermarking.

Sun et al (2008) proposed an invisible digital watermarking scheme based on SVD. In this method, the image is divided into 8×8 sub blocks, and then each block is decomposed by SVD. The second and third singular values of each block are exchanged if the watermark bit is 1, so the order of the singular values are not in the original descending order any more. This change of relationship of the order will be detected in the extraction process.

Lai et al (2008) introduced an image watermarking scheme using SVD and micro-genetic algorithm. In an SVD based watermarking scheme, the singular values of the cover image are modified by multiple scaling
factors to embed the watermark image. The proper values of scaling factors are optimized and obtained efficiently by means of the micro-genetic algorithm. A feature based robust watermarking algorithm against geometric transformation was proposed by Tang and Wang (2008).

Hsieh et al (2001) proposed a non-blind watermarking scheme based on the two-band wavelet transform and the qualified significant wavelet tree, which is robust to JPEG compression, image cropping, median filtering and etc.

Wang and Lin (2004) proposed wavelet tree based blind watermarking scheme for copyright protection. The wavelet coefficients of the host image are grouped into so-called super trees. The watermark is embedded by quantizing super trees. The trees are quantized so that they exhibit a large enough statistical difference, which will later be used for watermark extraction. Each watermark bit is embedded in perceptually important frequency bands.

Bao and Ma (2005) proposed digital image watermarking scheme using a Quantization Index Modulation (QIM) process via wavelet domain SVD. That scheme is robust against JPEG compression but extremely sensitive to filtering and random noising.

Ng and Garg (2005) analysed a maximum-likelihood detection scheme that is based on modeling the distribution of the image DWT coefficients using a Laplacian probability distribution function.


A genetic algorithm based watermarking optimal technique in DWT domain was proposed by Ning et al (2007). Lin et al (2008) grouped every seven non-overlap wavelet coefficients of the host image into a block. The largest two coefficients in a block are called significant coefficients and their difference is called significant difference. The local maximum wavelet coefficient in a block is quantized by comparing the significant difference value in a block with the average significant difference value in all the blocks. The maximum wavelet coefficients are so quantized that their significant difference between watermark bit 0 and watermark bit 1 exhibits a large energy difference which can be used for watermark extraction. Boubchir et al (2008) presented Bayesian wavelet-based denoising attack on image watermarking.


DCT domain watermarking technique expressly designed to exploit the peculiarities of color images was presented by Barni et al (2002). Dainaka et al (2006) proposed dual-plane watermarking for color pictures which is immune to rotation, scale, translation, and random bending. A blind print-scan resilient watermarking scheme was proposed by Li (2007) which can resist
printing and scan process. Wu et al (2007) presented a new secret text hiding
 technique, where the secret text is embedded into the low frequency sub-band
 of the saturation component of a color image via redundant DWT. Benhocene
 et al (2008) proposed a new approach for modeling color attacks of color
 image watermarking based on chaotic sequences. Qin et al (2010) proposed
 color image watermarking algorithm based on Arnold transform. Qiang and
 Hongbin (2010) proposed new color image watermarking scheme based on
 image self-embedding techniques. Li and Li (2008) proposed a Random Index
 Modulation (RIM) based fragile watermarking scheme for authenticating
 color images.

 Lu and Liao (2001) proposed a multipurpose watermarking scheme,
in which robust and fragile watermarks are simultaneously embedded, for
 copyright protection and content authentication. A new fragile watermarking
 scheme which can be applied to authenticate three dimensional polygonal
 watermark algorithm to protect hardware description language based
 intellectual property. A novel semi-fragile digital watermarking method based
 on SLT for image authentication and self restoration was introduced by Zhao
 scheme based on a pyramid structure. Khan et al (2007) implemented a
 reversible watermarking technique for mobile agent’s data security. Wang et
 al (2007) proposed fragile watermarking scheme for binary images with
 reversibility. Tsai et al (2007) presented a scheme based on fragile
 watermarking technique for guaranteeing the database integrity.

 Zhang and Wang (2008) proposed fragile watermarking scheme
 capable of perfectly recovering the original image from its tampered version.
 A new self-embedding and fragile watermarking technique which was used
for image integrity authentication was brought up by Che et al (2008). Luo
and Li (2008) introduced a document watermarking arithmetic which can
resist the attack of the print-scan and be fragile to print-copy-scan with high
algorithm which is mainly applied to binary document image based on the wet
paper code. Gao and Gu (2008) proposed a new watermarking based
reversible image authentication algorithm. In order to fingerprint digital maps,

Li et al (2006) proposed for robust audio watermarking in wavelet
domain. The proposed watermarking scheme is effective against common
signal processing manipulations and attacks, such as Gaussian noise
corruption, resampling, requantization, MPEG layer 3 (MP3) compression
and digital to analog - analog to digital conversion.

Erkucuk et al (2006) introduced novel watermark representation for
audio watermarking, where they embedded linear chirps as watermark
signals. The extracted chirps are then post processed at the receiver using a
line detection algorithm based on the Hough Radon transform (HRT). This
method correctly detects the embedded watermark message after common
signal processing operations for bit error rates up to 20%. The new watermark
representation and the post processing stage based on HRT significantly
improve the performance of the watermark detection process and can be
combined with existing watermark embedding/extraction algorithms for
increased robustness.

Zhou and Zhou (2007) proposed a robust audio watermarking
presented a scheme to combine recognition and estimation of audio data
modification using watermarking with content-based authentication. Xiang
and Huang (2007) proposed a multibit audio watermarking method based on
the two statistical features in the time domain, the histogram shape and the modified mean value. Gulbis et al (2008) presented a gap building scheme to improve the performance content based audio data authentication.

Unoki and Hamada (2008) presented a robust audio watermarking method, which is based on the concept of embedding inaudible watermarks (e.g., a copyright data) into an original sound by controlling the phase characteristics of the sound in relation to the characteristics of cochlear delay. Hiratsuka et al (2008) investigated the accuracy of estimated synchronization positions for audio digital watermarking using the modified patchwork algorithm on analog channels.

Suzuki et al (2006) showed that employing Low Density Parity Check (LDPC) coding for audio watermarking raised the watermark detection rate by around 15 percentage points for an additive white Gaussian noise and by around 20 points from around 60% to around 80% in an actual reverberation environment. Channel capacity analysis of spread spectrum audio watermarking system for transmission of hidden information through a noisy environment was performed by Sedghi et al (2006). Xu et al (2006) proposed digital audio watermarking algorithm based on DWT which is robust to lossy compression and other major attacks.

Pooyan and Delforouzi (2007) presented a robust method of audio watermarking in the wavelet domain. In this method, the watermarked data is encrypted, then combined with a synchronization code and embedded in low frequency coefficients of wavelet transform. Kondo and Nakagawa (2008) proposed a watermarking algorithm for stereo audio signals which embeds data using delay values of the high frequency channel signals.

A watermark-based error detection technique has been proposed by Chen et al (2005) for wireless video communications. By embedding a fragile watermark into quantized DCT coefficients during the encoding, the error detection capability of the decoder can be greatly improved compared to syntax-based error detection schemes. Su et al (2005) proposed simple spatially localized image dependent video watermark based on a novel framework for collusion resistance.

Barni et al (2005) presented a scheme for the watermarking of MPEG-4 video objects. This scheme works directly in the compressed domain thus reaching a high degree of flexibility and ease of use. A set of robust MPEG-2 video watermarking techniques was proposed by Wang and Pearmain (2006), focusing on commonly used typical geometric processing for bit-rate reduction, cropping, removal of any rows, arbitrary-ratio downscaling, and frame dropping. Echizen et al (2007) proposed video watermarking method uses human vision models of color information to control watermark strength and has immunity to rotations, scale changes, translations and random distortion. Liu et al (2007) proposed the differential energy modulation algorithm for video watermarking.


Liu et al (2008) proposed a video watermarking algorithm based on the correlation of adjacent luminance blocks in the MPEG-4 video coding standard bit-stream. In the algorithm, the watermark is embedded in the DCT coefficients of inter frames and predicted frames. Zhu et al (2008) proposed a video watermarking method for Wyner-Ziv video coding system, preserving the watermark info well for both the key frame and the Wyner-Ziv frame. This watermarking method is validated to be correct, robust, invisibility and secure.


2.3 ATTACKS ON ROBUST IMAGE WATERMARKING

Robust watermarks can be used in many applications, e.g. copyright protection. To serve its purpose, a robust watermark should survive common image processing and other non-hostile operations. These modifications on the image are referred to as attacks (Chen et al 2000).

The attacks can cause removal or desynchronization of watermark information while maintaining the visual quality of the image. Although the appearance of the attacked image does not suffer serious changes, the attack will result in watermark detection failure. The common attacks on watermark robustness can be categorized as follows.
2.3.1 Image Degradation

Image degradation operations can damage robust watermarks by removing parts of the image or by adding noise to the image. The image parts that were discarded or replaced may carry watermark information. Examples of these operations are noise insertion, partial cropping, row removal, and column removal. Gaussian noise insertion is a type of image degradation process. The amount of Gaussian noise is controlled by its mean and variance.

2.3.2 Image Enhancement

These are generally convolution operations that could desynchronize watermark information in an image. Some examples for image enhancement are sharpening, histogram equalization, smoothening, median filtering, Gaussian filtering, and contrast enhancement. Median filtering is a type of non-linear filtering that produces a smoother image. Contrast adjustment is part of signal enhancement manipulation. It can be used to change the appearance of an image to be brighter or darker.

2.3.3 Image Compression

Image compression is very useful for reducing storage space and thus saving transmission costs. Images processed using high quality compression can retain their aesthetic value, yet reduce their file size. Lossy compression methods are more destructive compared to lossless compression methods. Watermark information can be recovered with an inverse operation if it is compressed by lossless compression methods. However, lossy compression such as JPEG compression involves irreversible changes to the image. Therefore, watermark information may be lost and recovery may not be possible. JPEG compression is one of the common compression attacks on
digital images. With JPEG compression, one makes a trade-off between image quality and file size by specifying its compression quality factor.

2.3.4 Image Transformations

Image transformations can be useful in restoring distorted images. However, they pose a severe threat to robust watermarks due to their desynchronization effects. Indeed, they are one of the major challenges in robust watermarking. Many types of linear transformations can be modeled as a combination of basic transforms. For example, geometric transforms can be constructed using rotation, scaling, and translation (RST). Some researchers focus on RST robustness because it is a fundamental problem (Lin et al 2001). A broader class of image transformations is affine transformation. It includes other transforms such as aspect ratio change, shearing, reflection, and projection. Global geometrical distortion such as rotation is a big challenge. A small degree of rotation usually retains visual appearance while damaging watermark information.