Digital Watermarking of Images towards Content Protection

Ibrahim Alsonosi NASIR

BEng, MSc.

A thesis submitted for the degree of

Doctor of Philosophy

School of Computing, Informatics & Media

Department of Electronic Imaging and Media Communications

University of Bradford

2010

To My family,

Abstract

With the rapid growth of the internet and digital media techniques over the last decade, multimedia data such as images, video and audio can easily be copied, altered and distributed over the internet without any loss in quality. Therefore, protection of ownership of multimedia data has become a very significant and challenging issue. Three novel image watermarking algorithms have been designed and implemented for copyright protection. The first proposed algorithm is based on embedding multiple watermarks in the blue channel of colour images to achieve more robustness against attacks. The second proposed algorithm aims to achieve better trade-offs between imperceptibility and robustness requirements of a digital watermarking system. It embeds a watermark in adaptive manner via classification of DCT blocks with three levels: smooth, edges and texture, implemented in the DCT domain by analyzing the values of AC coefficients. The third algorithm aims to achieve robustness against geometric attacks, which can desynchronize the location of the watermark and hence cause incorrect watermark detection. It uses geometrically invariant feature points and image normalization to overcome the problem of synchronization errors caused by geometric attacks.

Experimental results show that the proposed algorithms are robust and outperform related techniques found in literature.

Acknowledgment

First of all, my strongly thanks to ALLAH the most merciful, without his help and blessing, this thesis would not have progressed.

I would like to express my sincere gratitude to my supervisor, Professor Jianmin Jiang for his supervision, advice, encouragement, guidance, and constant support helped me to finish my PhD research work.

I would also take this opportunity to thank my second supervisor Dr Stan Ipson for his ongoing support and precisely pinpointed comments and suggestions while reviewing my thesis and all the published works.

I would also like to thank Dr. Fouad for the valuable discussions, and suggestions and helps in my research work.

I would like to warmly thank my beloved family who has been a constant source of inspiration to me, especially to my wife, as well my father. My special gratitude is due to my brothers and sisters for their loving support. It is their love, strong support and encouragement that have helped me to complete this study.

Finally, I would like to thank all colleagues at the University of Bradford for the support and many useful discussions with them. I am also so grateful to my friends who constantly provided emotional support and took care of me in many aspects during the three years of studies.

Author's Contribution

Journal Papers

- I. Nasir, F. Khelifi, J. Jiang, and S. Ipson, "Robust Image Watermarking Scheme Based on Geometrically Invariant Feature Points and Image Normalization," *SUBMITTED* to Image and Vision Computing (Elsevier), 2010.

- I. Nasir, Y. Weng, J. Jiang, and S. Ipson, "Multiple spatial watermarking technique in color images", accepted by Signal, Image and Video Processing, (Springer), vol. 4(2), pp.145-154, 2010.

Conference Papers

- I. Nasir, F. Khelifi, J. Jiang, and S. Ipson, " A Robust Image Watermarking Scheme Based on Normalized Circular Image in DWT, " Accepted by Tenth IEEE International Conference on Information Science, Signal Processing and their applications, Malaysia,2010.

- I. Nasir, F. Khelifi, J. Jiang, and S. Ipson, " Robust Image watermarking scheme based on end-stopped wavelets feature detector, " The Seventh IASTED International Conference on Signal Processing, Pattern Recognition and Applications, Austria,2010, pp. 169-174.

- I. Nasir, Y. Weng, J. Jiang, and S. Ipson, "Robust Multiple Watermarking in Color Images with Correlation Coefficient Detector". The 8th IASTED International Conference on Visualization, Imaging and Image Processing, Spain, 2008, pp. 280-285.

- I. Nasir, Y. Weng, J. Jiang and S. Ipson, “Subsampling- based image watermarking in DCT compressed domain,” the 10th IASTED International Conference on Signal and Image Processing, USA, 2008, PP. 339-344,.

- I. Nasir, Y. Weng and J. Jiang, “Novel Multiple Spatial Watermarking Technique in Color Images,” Proc. 5th IEEE. Int. Conf. on Information Technology: New Generations, USA, 2008, pp. 777-782.

- I. Nasir, Y. Weng, J. Jiang, “A New Robust Watermarking Scheme for Color Image in Spatial Domain,” the 3rd Int. IEEE. Conf. on Signal-Image Technologies and Internet-Based System, China, 2007, pp. 942-947.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AWGN	Additive White Gaussian Noise
BER	Bit Error Ratio
CC	Correlation Coefficient
Db	Decibels
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
FDoG	First-derivative of Gaussian
FHT	Fast Hadamard Transform
HH	Diagonal Subband
HH3	Diagonal Subband at Resolution Level 3
HL	Horizontal Subband
HL3	Horizontal Subband at Resolution Level 3
HVS	Human Visual System
IDCT	Inverse Discrete Cosine Transform
JPEG	Joint Photographer Experts Group (Compression Technique-Image)
LH	Vertical Subband
LH3	Vertical Subband at Resolution level 3
LL	Approximation Subband
LL3	Approximation Subband at Resolution Level 3
LSB	Least Significant Bit
LSBs	Least Significant Bits
MSER	Maximally Stable Extremaly Region
NCC	Normalized Cross Correlation

PCA	Principal Component Analysis
PN	Pseudo Noise
PSNR	Peak Signal to Noise Ratio
RGB	Red-Green-Blue. The image color space where the image data is represented by the red, green, and blue bit planes of the image.
RST	Rotation, Scale and Translation Invariant
SIFT	Scale-Invariant Feature Transform
SSIM	Structural Similarity Index
TV	Television
XOR	Exclusive OR Logic Operation
YIQ	Color Components in NTSC color Space, where The Image Data is represented by Luminance and Chrominance data

CHAPTER ONE

1 INTRODUCTION AND THESIS ORGANISATION

1.1 Introduction

With the rapid growth of the internet and digital media technologies over the last decade, visual data such as image and video can be easily copied, altered and distributed over the internet without any loss in quality. Therefore, protection of the ownership of multimedia data has become a very significant and challenging issue.

Copyright protection of multimedia data has been accomplished by utilizing encryption techniques to prevent non-authorized users access to digital media content. Encryption protects media content during its transmission from the sender to receiver. However, encryption techniques do not completely solve the problem, because once media content is decrypted, there is no more protection to prevent an authorized user from illegally duplicating, modifying and distributing digital media content.

Recently, digital watermarking techniques have been utilized to maintain the copyright of digital data by identifying the owner or distributor of digital data. Digital watermarking is based on the science of steganography or data hiding. Steganography comes from the Greek meaning ‘covered writing’ [1]. The goal of steganography is to hide a message in media content in such way that the presence of a message cannot be detected. Watermarking is the process of embedding hidden information called a watermark into the digital media, such that the watermark is imperceptible, robust and

difficult to remove or alter. Digital watermarking can be used on many types of digital media including images, video, text and audio recordings.

The works presented in this thesis is focused on the digital watermarking of images for copyright protection. This introductory chapter outlines the problems addressed in this thesis, the research objectives and summarizes the thesis contributions.

1.2 Problem Identification

Digital watermarking is an effective method for copyright protection of media contents. It has attracted much attention and many proposed methods have been developed. However, digital watermarking technology still faces many challenges in both robustness and security requirements.

Problem 1: Digital watermarking can be achieved by utilizing either frequency domain techniques, in which a watermark data is embedded by modifying the frequency domain coefficients of the host image or by directly embedding a watermark into the spatial domain. In general, spatial domain methods are conceptually simpler and have lower computational complexities. However, they are less robust against attacks such as JPEG compression, low-pass filter and cropping attack. For example, they are comparatively less robust to cropping attacks because the watermark bits are embedded into the whole image so some data must be lost through cropping. Consequently, an algorithm that embeds the watermark in the spatial domain and achieves more robustness needs to be developed.

Problem 2: In general, to improve the robustness of watermarking algorithms against attacks, the watermark embedding strength should be as high as possible. However, this may affect the quality of the watermarked image. A higher embedding strength causes a lowering of quality of the watermarked image. It is obvious that the robustness and imperceptibility requirements are in conflict to each other. Consequently, a new watermark embedding strategy need to be developed to satisfy the conflicting objectives of causing image content changes that are imperceptible to the human eye while being extremely robust against detection or removal either intentional or unintentionally.

Problem 3: The most challenging design requirement for watermarks is to achieve robustness to geometric attacks. Examples of geometric attacks include rotation, shearing, translation, cropping, row and column removal. Such attacks can desynchronize the location of the embedded watermark and hence cause incorrect watermark detection. For example, in translation attack, the position of each pixel in an input image is mapped into a new position in the output image. As a result, the watermark can not be detected correctly due to changing of pixels locations. In such a case, a watermark synchronization process is required to determine the watermark location during the watermark embedding and detection processes. In non-blind methods, in which the original image is available in the detection process, the cost for resynchronization can be reduced by comparing the original image with the watermarked image. For blind methods, in which the original image is not required in the detection process, the most obvious way to achieve resilience against de-synchronization attack is to use invariant-transform domains. However, watermarking methods involving invariant domains are usually vulnerable to cropping and they are difficult to implement due to the log-polar mapping. Consequently, a watermarking

method that does not require the original image in the detection process as well as being robust to geometric attacks needs to be developed.

1.3 Research Objectives

The objectives of this research are to develop novel image watermarking algorithms, which overcome the identified problems and satisfy the watermarking requirements. The research themes are concerned with image watermarking for copyright protection applications. The objectives can be summarized as follows:

(i) A new robust color image watermarking scheme, which works in the spatial domain and achieves more robustness against different attacks such as, cropping attack.

(ii) A new strategy for embedding watermarks in an adaptive manner in the DCT domain to achieve better trade-offs between imperceptibility and robustness requirements.

(iii) Develop a new image watermarking approach to overcome the synchronization errors, which may be introduced by geometric attacks, such as rotation, shearing and translation, etc. The approach based on geometrically invariant feature points.

1.4 Thesis Contributions

The main contributions in this thesis can be summarised as follows in terms of the three research topics including watermarking of color images in spatial domain, adaptive watermarking of images in the DCT domain to achieve a trade-off between the

conflicting requirements, and image watermarking using local invariant features to overcome of synchronization error caused by geometrical distortions.

1. The development of a multiple spatial watermarking technique for the copyright protection of color images. Unlike previously proposed techniques, the proposed technique is based on dividing a binary watermark logo into parts and embedding each part into different regions of the blue component of color images in order to improve the robustness against attacks. How the robustness of the spatial domain watermarking technique can be improved by embedding multiple watermarks is demonstrated.

2. The development of adaptive image watermarking technique in the DCT domain. Here the main contributions can be highlighted as: (i) the proposed technique embeds a watermark in an adaptive manner via classification of DCT blocks with three levels: smooth, edges, texture, implemented in the DCT domain by only analyzing the values of two AC coefficients rather than by using methods such as Canny, Sobel or Prewitt for detecting the image edges. This adaptive technique is capable to achieve a better trade-off between watermark imperceptible and robustness requirements; (ii) Blind watermark embedding and extraction in the DCT domain: embedding a watermark into DC components of the DCT makes the proposed method more robustness to common attacks. The blind watermarking method does not require the original image at the detection process, which makes the proposed method portable to many applications.

3. The development of a robust image watermarking via geometrically invariant feature points and image normalization techniques. Here the major contributions can be highlighted as: (i) combining the advantages of using image normalization and geometrically invariant feature points, which are extracted using an end-stopped wavelets detector to reduce synchronization errors caused by geometric attacks; (ii) presenting a new reliable blind watermark embedding and extraction method based on quantization of DCT coefficients, which does not require the original image; (iii) consideration of the local properties of feature points to detect the watermark even when some feature are cropped. The proposed scheme is shown to have superior performance and demonstrates robustness to common signal processing attacks and geometrical attacks including rotation, cropping translation, row and column removal, shearing, and linear geometric transformation attacks.

1.5 Thesis Organization

The rest of this thesis is composed of six chapters and the organization of the main contents can be summarized as follows.

Chapter Two presents a general view of digital watermarking. It is divided into four main parts, which are general watermark concepts and applications, watermark classification, general framework for image watermarking and requirements of a robust image watermarking scheme.

Chapter Three provides a comprehensive literature review on the existing state-of-arts of image watermarking techniques, which are classified into three main broad categories; the first includes spatial domain watermarking techniques, the second

includes the frequency domain watermarking techniques and the third is feature domain techniques, which take into account regions, boundaries, invariant features, and object features to overcome the watermark synchronization issue caused by geometric distortions.

Chapter Four firstly presents an overview of previous colour image watermarking techniques. Then, the details of a novel multiple digital watermarking techniques based on the blue channel of color images and the block probability is described. The proposed watermarking scheme described in this chapter is tested using different images and evaluated with existing work.

Chapter Five presents a new approach for adaptive image watermarking by exploiting the discrete cosine transform based image compression techniques to embed watermarks in an adaptive manner. It firstly presents the limitation of existing work, an overview of the proposed method and the principle of using a subsampling technique in the image watermarking process. It then describes the proposed watermarking algorithm design, which consists of adaptive determination of watermarking strength, adaptive embedding of watermarks and the proposed watermark extraction process. Finally, it provides experimental results, discussion and evaluation with existing algorithm to demonstrate the performance of the proposed scheme.

Chapter Six presents a robust image watermarking scheme using visually significant feature points and image normalization. This chapter firstly provides a description of the feature extraction method and the image normalization process that are used in the proposed scheme. Then, it describes the proposed watermark embedding and extraction

processes. Finally, the performance of the proposed scheme is evaluated using different types of attacks and compared with the related existing work.

Chapter Seven summaries the research work presented in this thesis and also provides some suggestions for future investigation.

CHAPTER TWO

2 OVERVIEW OF DIGITAL WATERMARKING

2.1 Introduction

This chapter presents an overview of digital watermarking divided into four major sections. These are the concept of digital watermarking and applications, watermarking classification, the general framework for image watermarking and the requirements of digital watermarking.

2.2 General Watermark Concept and Applications

Digital watermarking has been claimed to be ultimate solution for copyright and authentication of media contents such as images, audio recordings, videos, etc. The idea behind digital watermarking is to imperceptibly embed a small amount of secret information, which is called a watermark, in the multimedia content so that it can be detected or extracted later to make an assertion about the host media. Embedding the watermark should not alter the visual quality of the host media. On the other hand, the watermark should still be extractable from the watermarked media after intentional or unintentional attacks [2, 3].

2.2.1 Definition of a digital watermark

The watermark is a signal or a pattern, which contains certifiable information useful to the owner of the host media, such as the product's name, company logo, etc., which is embedded into the host media to be protected.

2.2.2 Digital watermarking applications

Watermarking technology has a wide range of potential applications, which are listed below. Detailed discussions of these applications can be found in [4-6].

1. Copyright protection
2. Authentication
3. Fingerprinting
4. Copy protection
5. Data Hiding
6. Broadcast Monitoring

As mentioned early, to provide proof of the copyright, a digital watermark can be embedded in the media content so that it can be extracted later to prove the ownership of the host media. The digital watermarking can be also used to confirm authenticity of digital media by designing a watermark in such a way that any modification of the content either destroys the watermark, or create a mismatch between the content and the watermark. If the watermark is present, and properly matches the content, the user of the content can be assured that it has not been altered since the watermark was embedded. If any tampering has occurred in the content, the same alteration will also occur in the watermark so it can also provide information about the part of the content that has been altered. In fingerprinting application, additional information associated with the digital content should contain unique information about the user, rather than about the owner of the digital content. This unique information is called a fingerprint

and can be defined as characteristics of an object that tend to distinguish it from other similar objects. It enables the intellectual property owner to trace the source of illegal copies by embedding unique watermarks into copies for different customers. (i.e. a 'serial number' assigned by the vendor to a given purchaser). In this manner, the owner of data object can identify the original buyer of the redistributed copy by extracting the watermark. In copy protection, watermarking can be used to control data copying devices and prevent users from illegally copying the digital media when the watermark present in the media content indicates that the media content is copy protected. In data hiding applications, secret information can be embedded into media content and transmitted from one computer to another, without anyone else knowing that this information is being sent. Digital watermarks can be also used to monitor broadcasted content such as TV or radio. For example, verifying advertising broadcasts by embedding watermarks into commercial advertisements. An automated system can be used to monitor whether the advertisements are broadcasted at the correct times. The work in this thesis is intended to focus on the copyright protection application.

2.3 Watermarking Classification

Watermarks and the watermarking techniques can be classified as shown in Figure 2.1 in which three main categories of digital watermarks are identified according to embedding domain, human perception and media content types. The embedding domain category can be divided into classes: spatial domain and frequency domain techniques. According to the type of media content, the watermarking techniques can be classified into four types: images, video, audio recordings and text watermarking. In terms of human perception, the digital watermarks can be divided into two types, visible and invisible. Visible watermarks create noticeable changes in the host media when embedded so they are visible when the content is viewed. An example is provided by

television channels in which a TV log is visibly superimposed on the corner of the TV picture. Invisible watermarks are embedded into a host media in such a way that the alternation made to the host media is perceptually invisible and so cannot be detected by just viewing the digital content. Invisible watermarks are most often used as an evidence of ownership of multimedia content. The class of invisible watermarks may be divided further into two subclasses, fragile and robust. Fragile watermarks are designed to indicate any modification made to digital media [7]. They can be used to confirm authenticity of digital media. In contrast, robust watermarks are designed to be resilient to intentional or unintentional attacks [8]. They are used for digital copyright protection purpose. Within the subclass of robust watermarks, two types of watermarking techniques are defined, blind and non-blind [9]. The latter requires that the original media be present during the detection process in order to detect the watermark. In contrast, blind watermarking technique does not require the original media during the detection process. The robustness of non-blind watermarking techniques comes at the expense of practicality as the host media is required for watermark detection; this type may be impractical for applications where the watermark is intended as data for a large number of end-users to detect. Examples of such applications are broadcast digital radio or high definition digital TV. However, they may be suitable for other applications such as an online stock photograph shop, where a private library of digital media is maintained by a business, and watermarked media versions are sold to consumers. The work described in Chapter 4 of this thesis focuses on non-blind robust image watermarking in the spatial domain, whereas the works described in chapters 5 and 6 focuses on blind robust image watermarking in the frequency domain.

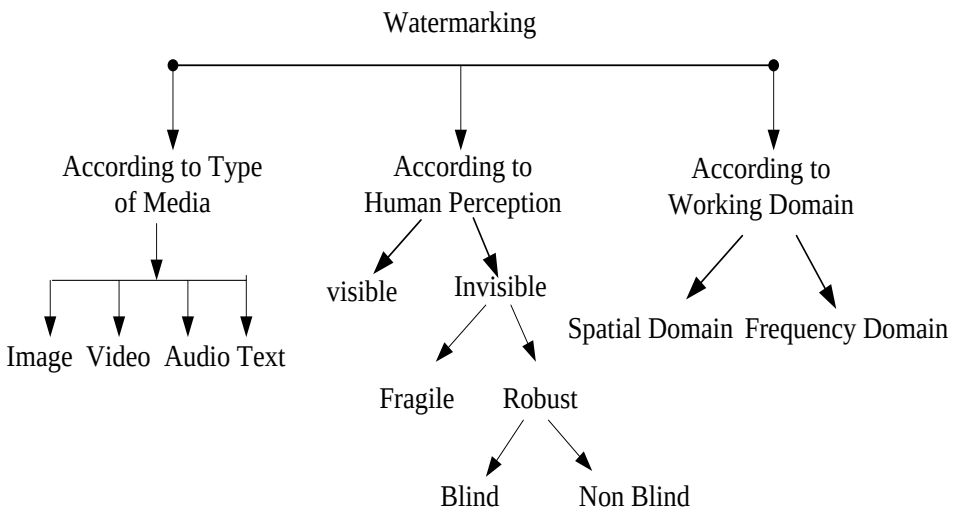


Figure 2.1 Watermarking techniques.

2.4 General framework for image watermarking

Figure 2.2 shows a block diagram of a generic watermarking system, which can be described as a problem of communication over a distorting channel. In this communication system, the transmitter essentially comprises encoding and embedding modules, while the receiver comprises detection and decoding modules. The communication system is designed to cope with carrier signal interface and channel distortions. In a similar way to a communication system, the watermarking system involves watermark encoding, watermark embedding, watermark detecting and the watermark decoding processes. A secret key may be used to embed a watermark into the cover media and the embedded watermark cannot be extracted without knowing the secret key. Transmitted over the channel communication, the watermarked media may be modified intentionally or unintentionally. For example, the watermarked media may be attacked by lossy compression, noise, geometric distortions, etc. Under these circumstances the watermark should be extracted or detected correctly by the extraction process. In the following section, the general watermark embedding and detection processes for image watermarking are described in more detail.

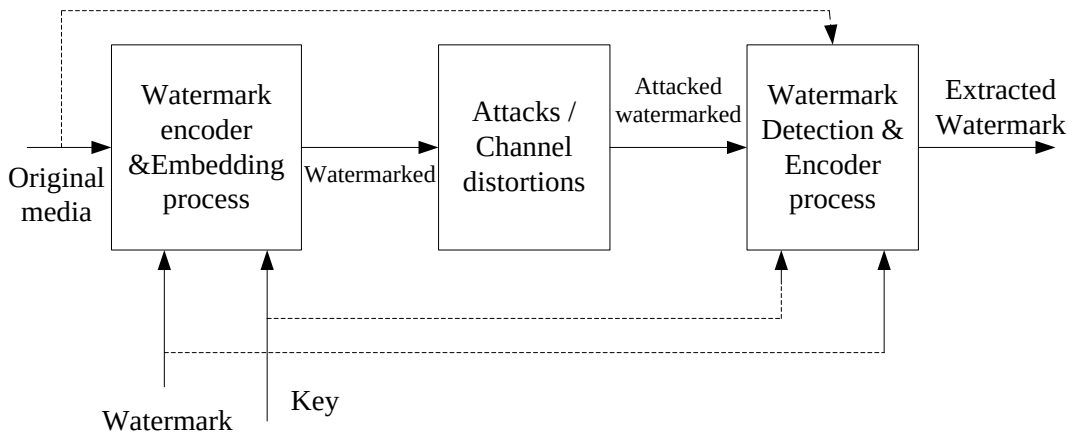


Figure 2.2 Block diagram of a generic watermarking system.

2.4.1 Watermark Embedding and Extraction Processes

Simple image watermark embedding and extraction processes are shown in Figure 2.3 and Figure 2.4, respectively. In the embedding process, a watermark W, which is often a binary logo image or a pseudo-random binary sequence generated by a secret key, is embedded into a host image I in either the spatial or transform domains. In the former, the pixel intensity is manipulated directly to embed the watermark. In the latter, the host image is first converted into a new domain by transforms, such as the discrete Fourier transform (DFT), the discrete cosine transform (DCT) or the discrete wavelet transform (DWT), etc., the transform domain coefficients are altered to embed the watermark and finally the inverse transform is applied to obtain the watermarked image. Due to the extra steps taken in both forward and inverse transformations, frequency domain techniques are generally more complex than spatial domain techniques; however, the transform domain techniques have been found more robust against attacks than spatial domain methods, when the watermarked images are tested after having been subjected to common signal processing attacks [10]. This is because in the frequency domain, the watermark can be embedded into the significant band (e.g. low frequency band), which

less effected by attacks such as JPEG compression and low-pass filter attacks. These transformation methods are briefly described in Section 2.4.2.

In the embedding process, the watermark may be encrypted or permuted to produce pseudo random sequences, which are uncorrelated with the original watermark. Also a secret key may be used to determine the embedding location of the watermark. The most common approaches for embedding a watermark into a host image are additive and multiplicative. To describe these approaches, suppose I denotes an original image to be watermarked by a binary watermark image W, the watermarked image I^*, which can be obtained using the additive embedding approach as follows

$$I^*(i, j) = I(i, j) + \alpha . W^*(i) \tag{2-1}$$

where $W^*(i)$ is the encrypted watermark bits and α is the watermark embedding strength. In a multiplicative embedding approach, the watermark can be embedded as follows

$$I^*(i, j) = I(i, j) . \left(1 + \alpha . W^*(i)\right) \tag{2-2}$$

The additive embedding approach has been widely used in watermarking techniques due to its simplicity. On the other hand, multiplicative embedding approach is more efficient because it is image dependent and exploits the characteristics of the human visual system (HVS) in a better way [11].

The extraction process of a watermark may be either non blind, or blind. In the former, the original image is required to extract the watermark as given below

$$W^* = D(I^*, I, Key) \tag{2-3}$$

Where D denotes the extraction function of the watermark, I and I^* denote the original and the watermarked images, respectively and Key is a private user key. In the blind extraction process, the extraction of a watermark is achieved without knowledge of the original image as described below

$$W^* = D(I^*, Key) \tag{2-4}$$

The extracted watermark is compared with the original watermark to make a binary decision on whether a given watermark exists or not. The comparison is usually based on a correlation measure and threshold as given below

$$D\,(W, W^*) = \begin{cases} 1 & C \geq \delta \\ 0 & \text{otherwise} \end{cases} \tag{2-5}$$

where D is the decision function, C is the correlation or similarity value and δ is a threshold. '1' indicates a watermark exists, while '0' indicates that a watermark does not exist. There are various methods to measure the similarity between the extracted and the original watermarks; some of them are described in Section 2.4.3.

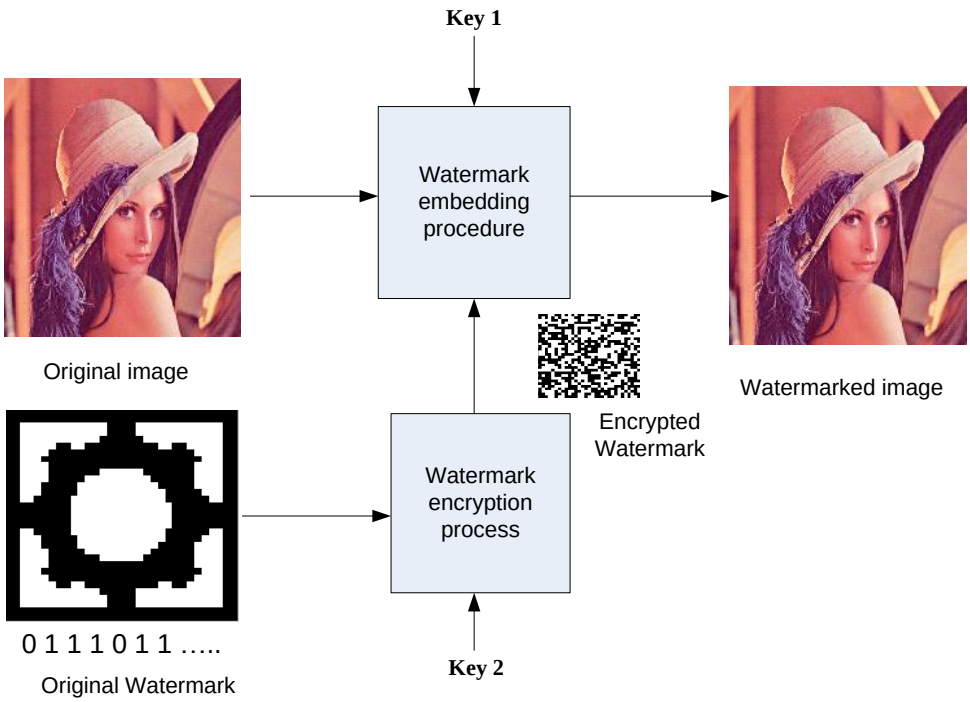


Figure 2.3 Image watermarking embedding process.

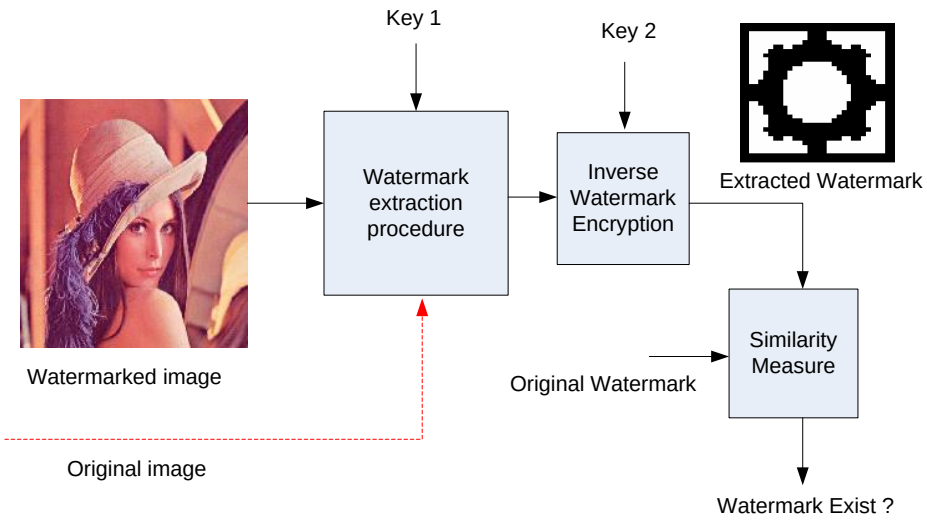


Figure 2.4 Image watermarking extraction process.

2.4.2 Transformation domain Methods

As mentioned earlier, there are three commonly used image transforms for watermarking in frequency domain. Theses are the DFT, DWT and DCT. The DFT generally produces complex-valued frequency domain coefficients. The DWT can be used to split an image into individual bands comprising a lower resolution approximation component (LL) and horizontal (HL), vertical (LH) and diagonal (HH) detail components. The Wavelet domain provides superior modelling of the human visual system (HVS). However, the computational complexity of the DWT is greater than the DCT [12]. Moreover it is not rotation, scale and translation (RST) invariant [13]. Detailed descriptions of the DFT and the Wavelet transform can be found in [14, 15], respectively and are beyond the scope of this work. The DCT is a popular domain for image processing where an image is broken down into different frequency bands and represented by a combination of DC and AC components. The image can be recovered from the DCT domain by a two-dimensional inverse transform [16]. Generally, a DCT can be applied directly to a full-frame image or after an image is initially partitioned into non-overlapping 8×8 blocks, applied independently on the subimage blocks [16].

In the latter case, any change in transform coefficients will affect the image locally, whereas in the full-frame DCT, the change will affect the entire image. Figure 2.5 shows the definition of frequency bands in a DCT block of 8×8. The forward and the inverse DCT to an image $f(x, y)$ are given by

$$F(u, v) = \alpha_u \alpha_v \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \cos\left[\frac{(2x+1)u\pi}{2M}\right] \cos\left[\frac{(2y+1)v\pi}{2N}\right] \tag{2-6}$$

$$f(x, y) = \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} \alpha_u \alpha_v F(u, v) \cos\left[\frac{(2x+1)\pi u}{2M}\right] \cos\left[\frac{(2y+1)\pi v}{2N}\right] \tag{2-7}$$

Where

$$u = 0,1,2,3,.....M-1,\ V = 0,1,2,3,.....N-1,\ x = 0,1,2,.....M-1,\ y = 0,1,2,....., N-1,$$

$$\alpha_u = \sqrt{1/M}, u = 0 \text{ and } \alpha_u = \sqrt{2/M}, 1 \le u \le M-1$$

$$\alpha_v = \sqrt{1/N}, v = 0 \text{ and } \alpha_v = \sqrt{2/N}, 1 \le v \le N-1$$

M and N are the row and the column sizes of the image

In this thesis, the operations of computing the forward and the inverse DCT will be denoted by DCT and IDCT, respectively.

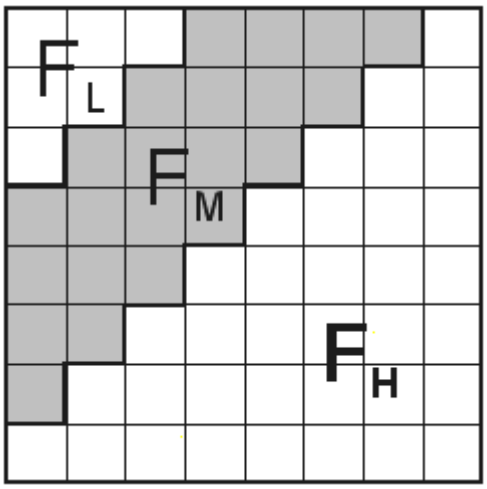


Figure 2.5 Definition of frequency bands in a DCT block.

2.4.3 Performance Evaluation of Watermarking Systems

The success of a watermarking system is evaluated using a series of measures including perceptual quality of the watermarked image, the similarity between the embedded and extracted watermark, robustness to signal processing and geometric attacks. These measurements are described as follows:

1. Perceptual quality

Embedded a watermark introduces distortion in the watermarked images. However, this distortion should not alter the visual quality of the host image and hence, the difference between the original image and the watermarked image should not be distinguishable. In order to evaluate the performance of the watermarking algorithm, the perceptual distortion that has been introduced in the watermarked image due to the embedding process of the watermark should be evaluated. In this work quantitative measures are adopted to measure the perceptual distortion of the watermarked images. These measures are the Peak Signal to Noise Ratio (PSNR) and the Structural similarity (SSIM) index. For grey images, the watermarked image quality is evaluated by computing the PSNR value using the following equation [17]:

$$\mathrm{PSNR} = 10\mathrm{Log}_{10}\left[\frac{255^2}{\frac{1}{m\times n}\sum_{i=1}^{m}\sum_{j=1}^{n}\left[I(i,j)-I^*(i,j)\right]^2}\right] \tag{2-8}$$

where I and I^* are the original and the watermarked images with pixel size of m × n. The number 255 means that the image used is digitized to 8-bit. For coloured images, the PSNR value can be calculated as the mean PSNR for the three RGB colour layers using the following equation:

$$\mathrm{PSNR}_{\mathrm{RGB}} = \frac{1}{3}\sum_{i}^{3}\mathrm{PSNR}\,(i) \tag{2-9}$$

Perceptual quality is dependent upon the intended application of a watermarking system. The higher the PSNR value, the better the quality of the watermarked image.

For assessing perceptual image quality, the objective method called the Structural similarity (SSIM) index is also used. This method attempts to quantify the difference between the original image and the watermarked image using a variety of known properties of the human visual system. A detailed description of SSIM can be found in [18].

2. The similarity between the embedded and extracted watermark

The watermark may be a company logo image or a signature representing the author; therefore, it useful to measure how well the extracted watermark correlates with the original. A threshold value may then be set to decide whether the extracted watermark is acceptable or not. There are various ways to measure the similarity between the extracted and the original watermarks. In this work, the correlation coefficient and the normalized cross correlation coefficient are used to measure the similarity between the embedded and extracted watermarks. The Pearson's correlation coefficient (CC) is calculated as follows:

$$\rho(w, w^*) = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}\left(w(i,j) - \tilde{m}_w\right)\left(w^*(i,j) - \tilde{m}_{w^*}\right)}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}(w(i,j) - \tilde{m}_w)^2}\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}(w^*(i,j) - \tilde{m}_{w^*})^2}} \tag{2-10}$$

where $w(i, j)$ and $w^*(i, j)$ are the original and extracted watermarks, respectively. $\tilde{m}_w$ and $\tilde{m}_{w^*}$ are the mean values of the original and extracted watermarks, respectively.

$-1 \leq \rho \leq 1$. $\rho = 1$ indicates perfect correlation, while an extremely low value reveals that the watermarks are dissimilar.

The normalized cross correlation coefficient (NCC) is calculated as follows:

$$\rho(w, w^*) = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} w(i,j)\ w^*(i,j)}{\sum_{i=1}^{m}\sum_{j=1}^{n} w(i,j)^2} \tag{2-11}$$

where $0 \leq \rho \leq 1$. $\rho = 1$ indicates perfect correlation.

3. Robustness against signal processing and geometric attacks

In watermarking applications, the robustness of watermarks to attacks is essential to the system [19]. In general, these attacks can be classified into two broad categories, signal processing and geometric attacks. While signal processing attacks attempt to reduce the watermark energy, geometric attacks may induce synchronization errors between the encoder and the decoder of the watermark. Common signal processing attacks include JPEG-lossy compression, median filtering, Gaussian, filtering, lowpass and mean filtering and added noise. Geometric attack includes, rotation, scaling, cropping, translation, shearing, affine transformation, linear geometric transformation, and row and column removal attacks. In addition, a benchmark should be used to evaluate and compare the robustness of a watermarking system with similar existing methods.

2.5 Requirements for a Robust Watermarking Scheme

A robust watermarking scheme must satisfy the following requirements. The watermark should not alter the quality of the original media, it should survive common distortions, it should be perceptually invisible, it should require little computation to embed or detect and should carry many bits of information. The requirements are application

dependent. In this section, the common requirements which should be fulfilled by a robust watermarking scheme are listed and briefly discussed; more detailed discussions of these requirements can be found in [2, 3, 20-22].

2.5.1 Imperceptibility

One may expect that the embedding of a watermark should be imperceptible to ensure there is no visual degradation on the watermarked media. However, there is a conflicting between imperceptibility and other requirements such as robustness. Therefore, the characteristics of the host media should be taken into account when embedding the watermark to achieve better trade-offs between imperceptibility and robustness. These conflating requirements are discussed in Section 2.5.5. Figure 2.6 illustrates the imperceptible degradation resulting from embedding a watermark into a host image.

(a) (b)

Figure 2.6 Imperceptible degardation (a) original image, (b) Altered image.

2.5.2 Robustness

Robust watermarking is necessary in the areas of copyright protection, such as ownership identification, copy control, copy prevention, fingerprinting, etc. Robustness

means that a watermarking algorithm still works correctly when the watermarked media is subjected to signal processing and geometric distortions, such as, lossy compression techniques, filtering, cropping, scaling, rotation, etc. For content authentication application, the watermarks should be fragile, i.e., the watermarks should be destroyed whenever the content is modified so that any modification to content can be detected. The reader is referred to [23, 24] for more information about fragile and semi-fragile watermarks.

Robustness comprises two separate issues [25]; the first is that whether or not the watermark is still present in the data after distortion, the second issue is whether the watermark detector can detect it. For instance, geometric attacks, such as translation, rotation, etc. may induce synchronization errors between the encoder and the decoder of the watermark. As a result, the embedded watermark may still exist in the watermarked media but the decoder is no longer able to detect the watermark. Robustness against signal processing attacks is better achieved if the watermark is embedded in perceptually significant regions of the host media, however, this may induce visual degradation of the watermarked media. Therefore, trade-offs between the robustness and imperceptibility should be made. This work proposes novel solutions for such challenges (Refer to Chapter 5).

2.5.3 Security

Security is an important requirement, which can be regarded as the ability to assure secrecy and integrity of the watermark information [26]. A secret key may be used to determine the value of the watermark and the embedding location of the watermark. Using a secret key ensures that only authorized users are able to detect or modify the watermark. In order to match security requirements, one must be ensure that the number of possible keys is sufficiently large that exhaustive search becomes computationally

infeasible. The watermark may be also encoded and decoded using a secret key in order to increase security of the watermarking system. In the present work, secret keys are used to boost the security of the proposed schemes as can be seen in chapters 4, 5 and 6.

2.5.4 Capacity

Capacity refers to the amount of information that can be embedded into a host media. Higher capacity may cause a lower quality of the watermarked media. This is because more embedded bits will induce more embedding distortions in the watermarked media. Thus, there is a conflict between capacity and imperceptibility requirements. Capacity can be assessed by calculating the ratio of capacity to reliability. The theoretical capacity of an embedded watermark has been examined using information-theoretic concepts. Capacity issues are discussed in reference [27, 28].

2.5.5 Trade-offs among requirements of a watermarking scheme

The requirements of a watermarking scheme conflict with each other. For example, to reduce distortions during the embedding process, the watermark may be embedded into the perceptually insignificant region (high frequency band) of the host media. However, the watermark can be easily removed without affecting the host media [29]. Therefore, the watermark may be embedded into the significant region (low frequency band) of the host media to increase the robustness. However, modifying the low frequency components has more effects on an image quality. As can been seen, there is a conflict between imperceptibility and robustness requirements. The major challenge to researchers in this field is how to design a watermarking system that satisfies the three conflicting requirements shown in Figure 2.7, which means that if one improves, the other two may deteriorate. In this work, to satisfy these conflicting requirements, a new adaptive image watermarking strategy is presented in Chapter 5.

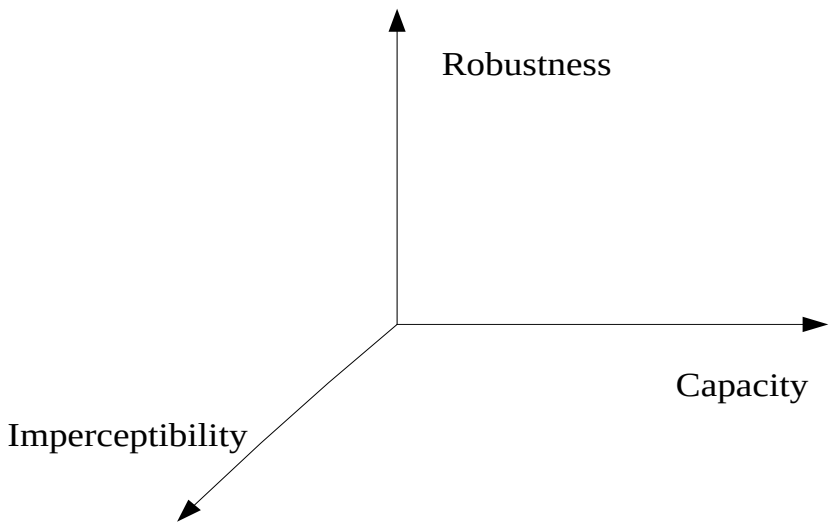


Figure 2.7 Trade-offs in robust watermarking.

2.6 Chapter Summary

The goal of this chapter was to provide overview of digital watermarking includes the concept of the watermark, watermarking applications and requirements of a robust image watermarking scheme. A general framework for image watermarking was described and discussed. The additive and multiplicative embedding approaches were described. The watermark may be embedded in either the spatial or transform domains. The common requirements which should be fulfilled by a robust watermarking scheme were discussed. It has been shown that there is a conflict between imperceptibility and robustness requirements. In the next chapter, literature review of existing state of the art is presented.

CHAPTER THREE

3 LITERATURE REVIEW OF EXISTING STATE OF THE ART

3.1 Introduction

This chapter presents several types of digital watermarking techniques found in the academic literature. Theses can be classified into three main broad categories. The first includes spatial domain watermarking techniques, in which watermark embedding is achieved by directly modifying the pixel intensity values of the host image. The second category includes frequency domain techniques, which embed the watermark by modifying the transform domain coefficients. The third category includes the feature domain techniques, which take into account regions, boundaries, invariant features and object features to overcome the watermark synchronization issue caused by geometric distortions. Overviews on digital watermarks techniques can be found in [2, 8, 13]. A classification scheme for existing digital image watermarking techniques is shown in Figure 3.1 in which the three main embedding domains already mentioned are identified.

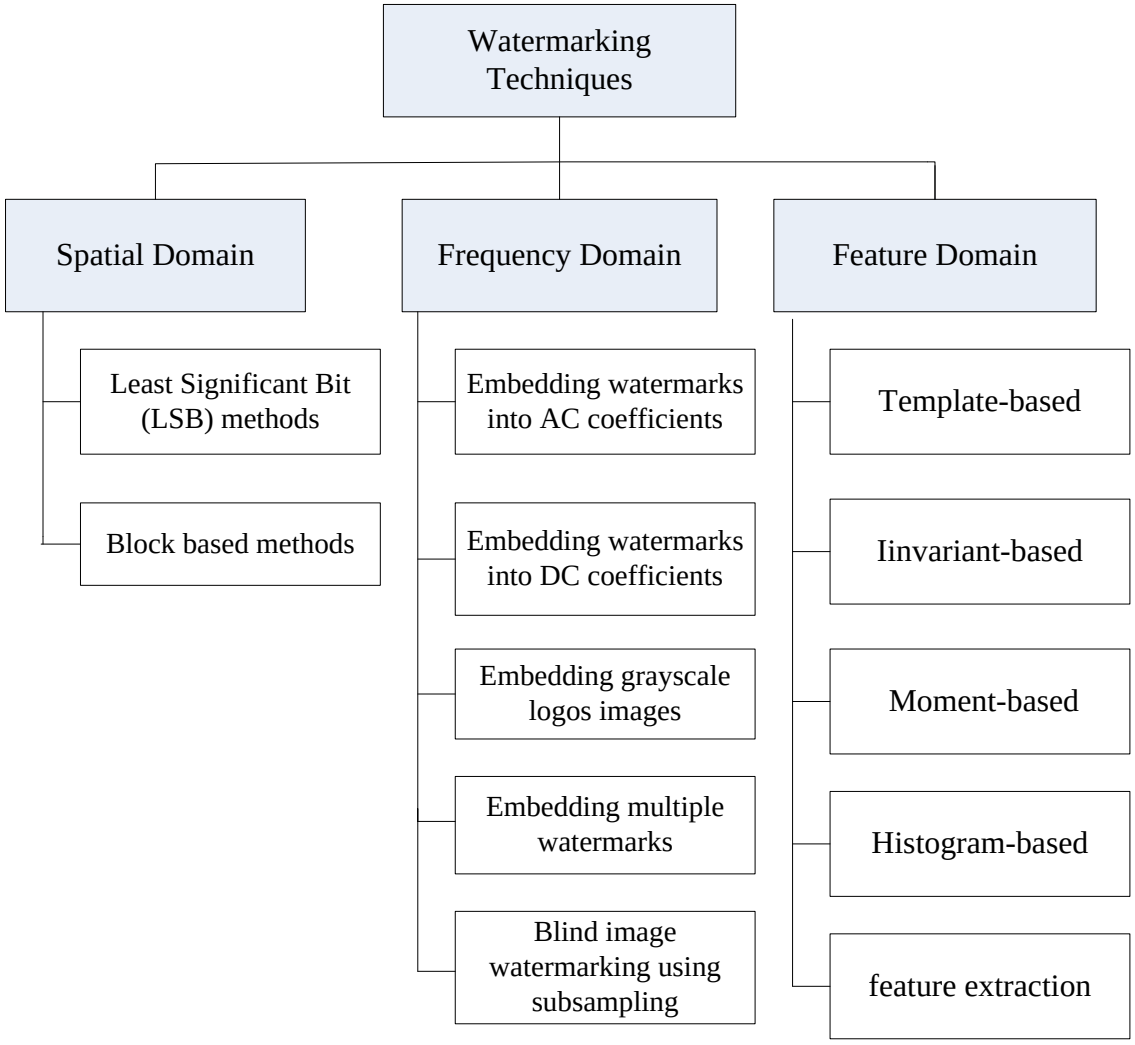


Figure 3.1 Classification of existing image watermarking techniques.

3.2 Spatial Domain Watermarking Techniques

In spatial domain watermarking techniques, watermarks are embedded directly in the pixel values of the host image. Therefore, pixel domain methods are conceptually simpler and have much lower computational complexities compared to frequency domain methods. The simplest spatial domain image watermarking technique is to embed a watermark in the least significant bits (LSBs) of the host image [30]. The imperceptible of the watermark relies on the assumption that the LSB bits of pixel values are visual insignificant. Many spatial image watermarking techniques are based

on adding fixed amplitude pseudo noise (PN) sequences to the host image. The PN sequences may be constructed according to a Gaussian distribution with mean μ and variance σ^2, generated with a user private key. The watermark extraction process requires knowledge of the PN sequence and the statistical properties of the embedding process.

Schyndel et al. [31] proposed two LSB techniques. The first replaces the LSB of the image pixel with a PN sequence, while the second utilizes linear addition of the PN sequence to the LSB of image pixels. The embedded PN sequence is extracted by comparing the LSB bit pattern with a stored counterpart. Bender et al. [32] proposed a statistical method called patchwork, which randomly chooses n pairs of pixels (a_i, b_j) in the host image and increases the brightness of a_i by one unit while simultaneously decreasing the brightness of a_j. Nikolaidis et al. [33] used a binary pattern as a watermark, which is embedded into the host image by slightly modifying the intensity level of randomly selected image pixels. In the embedding process, the pixels values are assigned into one of two sets. The intensity levels of pixels in one of the sets are altered while other intensity levels are not altered. The watermark is extracted by comparing the mean intensity value of the watermarked pixels with the unmarked pixels and using statistical hypothesis testing to determine the extracted bits. The results show that this method is not robust against geometric attacks.

To increase the security of the embedded watermark in the LSB, Matsui et al. [34] proposed a method, which uses a secret key to determine the embedding location of the watermark. Hwang et al. [35] suggested using a Hash function to improve the security of the watermarking algorithm. Voyatzis et al. [36] suggested using a chaotic transformation method called a toral automorphisms to securely scramble a binary watermark image into a pseudo-random bit sequence, which is embedded by modifying

the intensity values of selected host image pixels. The results show that this scheme is resistant to JPEG compression and filtering attacks only. Another method based on toral automorphisms is presented in [37]. This method used a mapping table in order to extract the watermark. However, the use of the mapping table increases the complexity of the algorithm. Similarly, in [38], Chin et al. used a toral automorphisms to scramble a watermark and retrieved the edge characteristic of the host image in order to generate a verification map to verify the copyright of a protected image. Wu et al. [39] used two chaotic maps to improve the security; one map is for encrypting the embedding position of the host image, and the second map is for determining the pixel bit to embed a watermark bit. A two dimensional Arnold cat map is used to shuffle the embedding position. As a result the watermark will spread in all regions of the host image chaotically. The watermark bits are embedded into the 4th, 5th, 6th or 7th bits of the corresponding shuffled pixels in the host image. The results show that this scheme is robust against JPEG and filtering attacks.

In general, methods, in which watermarks are embedded by modifying the LSB of image pixels, are not very secure and not very robust to signal processing attacks because the least significant bit plane can easily be replaced by random bits, effectively removing the watermark bits without inducing any noticeable degradation in the attacked image [30].

To improve the robustness of spatial domain watermarking techniques, some proposed methods used block based watermarking instead of pixel watermarking [40-42]. Darmstaedter et al. [40] proposed a block based spatial watermarking method, which alters the average luminance value of a block. Using this method, the host image is divided into a set of 8×8 blocks and each bit of the watermark is embedded in one block. This scheme is not robust against geometrical attacks. Chang et al. [41] proposed an adaptive image watermarking technique for copyright protection. It utilizes the

sensitivity of the human visual system to adaptively alter the intensities of some pixels in a block depending on the content of the block. In the embedding process, the original image is divided into blocks of size 4×4 and according to the content of the selected block, pixels values are altered to maximize robustness and guarantee invisibility. For example, if all the pixels have the same pixel intensity in the selected block, the pixel intensities will be altered by a small value. The results reported in [41] show that the proposed method is robust to some common image processing attacks such as low-pass and median filtering. A drawback of the method in [41] is the fixed block size assignment of 4×4 pixels. The block size is an important property of the watermark. The larger the block size the greater the robustness achieved. Kimpan et al. [42] proposed a method to overcome of drawback of the method proposed in [41] by using variable block size in order to increase the robustness of the scheme. In Kimpan's scheme, the original image is divided into several blocks of size 64×64, 32×32, 16×16 and 8×8 pixels. The block size depends on intensity level, which is determined by the mean value of the block. The experimental results show that this scheme is not robust to cropping attacks. To improve the security of a watermarking algorithm, Lin [43] used a unique serial number for converting a binary logo into a mark sequence, which is embedded by modifying pixel block intensities.

3.3 Frequency Domain Watermarking Techniques

Many watermarking schemes have been proposed in the frequency domain using transform methods, such as Discrete Fourier transform (DFT), full-frame discrete cosine transform (DCT), block based DCT, or Wavelet transform, etc. The discrete Fourier transform of an image is generally complex and this leads to a magnitude and phase representation of the image. The phase contains most of the image information, with DFT magnitude coefficients conveying comparatively little information. Therefore, the

watermark should be embedded into the phase of the DFT to be robust against attacks [44]. Using the DCT an image can be broken down into different frequency bands, and the watermark can be embedded into the significant band to be more robust against attacks [45]. The wavelet transform domain is used in digital watermarking because of a number of advantages, which include its compatibility with the image coding standard JPEG 2000, its excellent time-frequency features and its good match to the human visual system (HVS) characteristic [46].

In this section, work reported in the literature for watermarking algorithms based on the transform domain is presented. Existing work can be grouped into:

1. Embedding watermarks into AC coefficients of the transform domain
2. Embedding watermarks into DC coefficients of the transform domain
3. Embedding greyscale logo images
4. Embedding multiple watermarks
5. Blind image watermarking using sub-sampling

3.3.1 Embedding watermarks into AC coefficients of the transform domain

This section presents several types of image watermarking schemes, which use the DCT, or the wavelet domain for embedding watermarks into AC coefficients. In most existing image watermarking schemes, the low or middle frequency domain coefficients are used to embed watermarks because the high frequency coefficients may be discarded by lossy compression quantization or by low-pass filtering. However, the human eye is more sensitive to noise in the lower frequency coefficients than in the higher frequency coefficients [47].

Many proposed algorithms use the DCT transform domain. However, the Cox et al [45, 48, 49] and the Koch [50] algorithms are the most well known DCT based algorithms. Cox et al [45] proposed a non-blind method using the full-frame DCT, with an additive

white Gaussian noise (AWGN) sequence. This is embedded into the perceptually most significant DCT coefficients of the image in order to maximize the chance of detecting the watermark even after common signal processing attacks and geometric distortions. The weaknesses of this method are that the watermark detection process requires the original image, which is not available in many applications, the watermarking capacity is limited, since the watermark is embedded into only the significant coefficients of the transformed image, which mostly contains only few significant coefficients and applying the full-frame DCT is computationally expensive. Moreover; this method is weak against the invariability attack proposed by Craver [51]. Koch et al [50] uses a sequence of binary values as a watermark, which is embedded by modifying the difference between randomly selected mid-frequency coefficients in random 8×8 DCT blocks. Since the embedding of the watermark is achieved by modifying the difference between the AC coefficients of the DCT blocks without taken into account characteristics of the host image, visible artefacts may be induced in smooth regions in the watermarked image. In [52], the DCT coefficients of the middle frequency band are used to embed the watermark. The extraction process for this method requires the original image. In [53], a watermark is embedded into the DCT coefficients of the low frequency band by modifying the least significant bit (LSB) of the DCT coefficients. However, the embedded watermark can be easily removed by modifying the value of all DCT coefficients to ‘0’ or ‘1’ without inducing any visual degradation of the watermarked image. The authors in [54] used the DCT transform domain to embed the watermark in the host image by modifying the DCT coefficients of the middle frequency band with values corresponding to the quantization table for JPEG compression. The experimental results of this method show robustness to JPEG compression attacks only. Moreover the quality of the watermarked image is low. In [55], the authors proposed a method similar to that presented in [54], in which the

watermark bits are embedded into the low frequency coefficients of the DCT. Zhou et al [56] proposed an image watermarking scheme, in which the watermark is embedded into the low frequency coefficients of the 8×8 DCT blocks, which have smooth features. These blocks are selected according to the values of DC coefficients and the variances of AC coefficients. The selection process for the DCT blocks depends on the variance of AC coefficients, which may change due to the embedded watermark. Therefore, the detection process may fail to determine the right DCT blocks to extract the watermark. Wu et al. [57] suggested that more significant coefficients of a DCT block can be generated by breaking the local spatial similarity in an image using a block-based chaotic map. The results demonstrate that the watermark capacity can be increased. However, the robustness of this scheme is limited to JPEG and low-pass filtering attacks only.

Watermarks also have been embedded in wavelet domain coefficients [58-60]. Dugad et al. [59] proposed a spread spectrum image watermarking technique in the DWT domain. The watermark is embedded with a constant weighting factor into the perceptually significant coefficients in the high frequency sub-band in order to preserve invisibility of the embedded watermark. However, watermarks embedded into the high frequency band can be removed by compression or other common signal processing attacks, which reduces the robustness of this method. Two image watermarking methods using the wavelet transform domain are described in [60] . In these methods a zero tree wavelet algorithm is used to classify the wavelet coefficients as insignificant or significant. In the first method, a watermark is embedded in the insignificant coefficients, while in the second method significant coefficients are modified to embed a watermark. The watermark is detected by using the position of zero-tree roots and the threshold value. These methods have proved to be robust against JPEG compression. However, they may lose synchronization because it depends on insignificant coefficients. Dawei et al. [61]

proposed a new type of technique in which the wavelet transform is applied locally to sub-images. A chaotic watermark is embedded into selected sub-band coefficients and it is detected by computing the correlation between the watermarked coefficients and the watermark signal. This method shows robustness against geometric attacks such as, cropping and rotation but it is sensitive to common signal processing attacks such as, low-pass filtering.

In order to improve the security of the watermarking methods using the wavelet domain, authors in [62, 63] suggested using a key dependent wavelet transform. Wang et al. [62] used a randomly generated orthonormal filter bank as a major part of the private key. In Wang's method, a binary watermark is embedded into the middle frequency bands of the DWT of the host image to achieve both perceptual invisibility and robustness against signal processing attacks. The results for this method show that it is robust to JPEG compression attacks but it is weak under median and low-pass filtering attacks. Dietl et al. [63] suggested using wavelet filter parameterization as a secret transform domain to improve the security of wavelet-based watermarking methods.

The wavelet transform has been applied also in many other watermarking algorithms. The reader can refer for examples of these other wavelet techniques to references [64-67].

3.3.2 Embedding watermarks into DC coefficients of transform domain

Instead of using AC coefficients to embed a watermark, Huang et al. [68] suggested that greater robustness can be achieved if the watermark is embedded into the DC coefficients of the DCT. Because the magnitude of the DC coefficient is much larger than that of the AC coefficients, it can provide much greater perceptual capacity than the AC coefficients. Also, the DC coefficient is less affected than the AC coefficients if

the watermarked image is attacked by JPEG compression, low-pass filtering or sub-sampling operations. Using this suggestion, the authors of references [68-71] proposed methods to embed the watermark in the DC coefficients of the DCT transform domain and the fast Hadamard FHT transform domain. The main weakness of these methods is that the detection process requires the original image, which may not be available in some applications.

3.3.3 Embedding greyscale logo images

Some proposed schemes focus on embedding a greyscale image instead of embedding a binary image or a pseudo random sequence. At an early stage of the development of watermarking algorithms, the authors in [72, 73] suggested using greyscale logo images as a watermark, with as much as 25% of the host image size. Recently, Kundur et al [74] proposed a multi-resolution fusion based watermarking method for embedding greyscale logos into the host image in the wavelet transform domain. In this method, the greyscale logo image and the host image are decomposed into 1-level and each sub-band of the host image is divided into blocks. The sizes of those blocks are equal to the size of the sub-band of the logo image, which are embedded in the same orientation as blocks of the host image. A human visual model based on contrast sensitivity is used to maximize the robustness of the watermark. The weight factors of the human visual model are determined for the block of wavelet coefficients rather than individual wavelet coefficients. Therefore, the embedded watermark can cause visual degradation [75]. To overcome the weakness of the method reported in [74], authors in [75] proposed a method, in which a greyscale logo image is embedded into the significant coefficients of each subband selected by considering the human visual system (HVS), with its weight factors calculated for individual coefficients to maximize the strength of

embedded watermark and ensure there is no visual degradation of the watermarked image. Although the results reported in [75] show the robustness of this method against various attacks, the detection process requires the original image, which is not available to the detector in most applications.

3.3.4 Embedding multiple watermarks

Instead of embedding a single watermark into the host image, the authors in [76-79] embedded multiple watermarks into the same host image to achieve more robustness against various image processing attacks as follows: embedding watermarks into the low frequency band to achieve robustness against low-pass filtering or JPEG lossy compression attacks; embedding watermarks into high frequency band to achieve robustness against adding noise, or histogram equalization. In [76] two identical watermarks are embedded into low and high frequency components separately. Each watermark bit is embedded into a set of wavelet coefficients. The extraction process does not require the original image. In [77] two watermarks are embedded into low and high frequency bands of a two level wavelet decomposition. The extraction process requires the original image. A drawback of these methods is that the embedding process does not take into account the difference in magnitudes of lower and higher DWT coefficients. This leads to highly visible degradation of the watermarked image, especially in low frequency areas. In [78] three watermarks are embedded into low, middle and high frequency bands of the DCT in order to be robust against low-pass, median and high-pass filtering. The watermark is extracted by comparing the DCT coefficients of the original and watermarked images. In [79], two complementary watermarks are embedded into wavelet coefficients to make it difficult for attackers to

destroy both of them. The extraction process of this method requires the original image. Other multiple watermarks algorithms can be found in [80-84].

3.3.5 Blind image watermarking using sub-sampling

Recently, watermarking methods that do not require the original image at the watermark detection stage have become a topic of intense research [85]. Sub-sampling processes have been used recently in image watermarking techniques in order to recover the watermark without comparison with the original image. Chu [86] introduced a new blind DCT watermarking scheme based on a sub-sampling process. The weakness of Chu's scheme is that it is not robust under low-pass or JPEG compression attacks. Based on Chu's scheme, the authors of references [87, 88] proposed methods, in which the watermarks are embedded in wavelet and DFT transform domains. The method in [87] uses three-level wavelet decomposition and the watermark is embedded in pairs of coefficients in the HL3, LH3 and HH3 frequency bands. The embedding locations are determined by an order sequence. In [88] a randomly generated watermark sequence is embedded into the DFT domain of the four sub-images using Principal Component Analysis (PCA). The watermark is embedded into the amplitude spectrum coefficients at locations determined by a secret key. To overcome the weakness of the method presented in [86], Lu et al. [89, 90] proposed two schemes, which use the DCT of the full-frame image. The first of these is based on a sub-sampling and difference correlation detector. A random binary sequence is used as the watermark and embedded in the DCT domain of the subimages at locations determined by a secret key. The watermark is extracted by using coefficient difference correlation. The results show that this scheme is not robust against geometric attacks. The second scheme used a chaotic map to permute the binary watermark image, which is embedded using selected pairs of

AC coefficients of sub-images. The work described in references [86-90] showed that it is possible to extract the watermark without comparison with the original image using a sub-sampling process. However, these methods have the following weaknesses: (i) the human visual system is not taken into account when embedding the watermark and, as a result, the maximum-possible imperceptibility and robustness of the embedded watermark cannot be guaranteed; (ii) the full-frame DCT is used for the four sub-images. Therefore, it is not directly suitable for applications involving JPEG compressed images, requiring relatively high computing costs and low processing speeds.

3.4 Feature Domain Watermarking Techniques

As mentioned earlier, geometric attacks may induce synchronization errors between the encoder and the decoder of the watermark. As a result, the decoder is no longer able to detect the watermark. Several watermarking methods have been developed to overcome this problem. These methods can be roughly classified into template-based, invariant transform domain–based, moment-based, histogram-based, and feature extraction-based methods.

The template-based watermarking methods are based on embedding a template in addition to the watermark to assist the watermark synchronization in the detection process. This may be achieved using a structured template embedded in the DFT domain to estimate transformation factor to resynchronize the image [91-94] or by embedding the watermark several times at different locations [95]. However, there is an accuracy problem associated with log-polar mapping of the DFT since the inverse transformation requires image interpolation; moreover this technique has limitations in terms of robustness since the template can be easily deleted by eliminating peak values [96].

The most obvious way to achieve resilience against de-synchronization attack is to use an invariant-transform domain. In [97-100], watermarks are embedded in affine-invariant domains such as the Fourier-Mellin transform or log-polar domain to achieve robustness against affine transforms. However, watermarking methods involving invariant domains are usually vulnerable to cropping and they are difficult to implement due to the log-polar mapping [100].

In moment-based watermarking methods [101-103], watermarks are embedded into normalized-based moments robust against affine transforms. In [104] the watermark was embedded in an affine-invariant domain by using the Zernike moment. Moment–based methods are highly vulnerable to cropping due to the fact that the moments depend on all pixels. Indeed, removal of any part of an image will result in a significant distortion of the moment values.

Using the fact that image histograms are independent of the positions of pixels, the authors in [105-108] presented a histogram-based watermarking approach. However, these approaches suffer from robustness limitations under histogram enhancement and equalization attacks.

Another way to reduce or remove the synchronization issue caused by geometric attacks is to extract feature points, which represent invariant references to geometric transformations. These feature points can be used as reference points for both watermark embedding and detection. These techniques are called second generation watermarking [109]. The first second generation watermarking method was proposed by Kutter et al. [109], in which feature points and the Voronoi diagram are used to define regions of interest to be watermarked. The feature extraction process of Kutter's method is based on a decomposition of the image using Mexican-Hat wavelet.

Recently, image feature based watermarking methods have been widely exploited to overcome the watermark synchronization issue [110-114]. In [110], the Harris detector

is used to extract feature points, which are combined with a Delaunay Tessellation to define a number of triangular regions for embedding the watermark. The drawback of this method is that features points extracted from the original and attacked images are not matched. Therefore, the sets of triangles generated during watermark embedding and detection are different; moreover it is not robust to most signal processing attacks except JPEG compression [113]. In [111], a Mexican-Hat wavelet scale interaction method is used to extract feature points and then the watermark is embedded in normalized disks centred at the extracted feature points. In [112], the authors proposed a method in which the feature points are extracted using the scale-invariant feature transform (SIFT). The watermark is embedded into the circular patches generated using the SIFT. A drawback of this method is that polar mapping during the watermark pattern transformation produces interpolation error. In addition, due to the lengthy time needed to compute the SIFT descriptor and for compensation of alignment error, the applications of this method are limited. In [113], the authors proposed a method similar to that presented in [110], in which the adaptive Harris corner detector is used to extract feature points and the Delaunay-tessellation-based triangle matching method is used to reduce the watermark synchronization problem and resist geometric distortions. Experiments on this method show its weakness to flip attacks since the algorithm cannot match two triangles when one is flipped. Furthermore, the detection process requires the positions of the feature points from the original image to restore the probe image and reduce the synchronization errors. Therefore, extra memory is need for storage. In [114], the authors use the Harris detector to extract the feature points and embed the watermark in circular regions in the spatial domain. The results for this scheme show that its robustness against signal processing and geometric attacks is limited. For instance, the watermark cannot be detected when the watermarked image is attacked by JPEG compression with a quality factor as low as 60%.

The analysis of the existing work described above suggests that second generation watermarking methods [110-114] using local image feature points as references can provide solutions to resist geometric attacks. However, the feature point extraction techniques adopted by current feature-based approaches, for instance, the Harris detector or the Mexican hat wavelet detector are sensitive to image modification which makes their robustness to specific attacks limited .

3.5 Chapter Summary

In this chapter, digital image watermarking algorithms, which are classified based on the embedding domain into three main categories: spatial domain techniques, frequency domain techniques and feature domain techniques were reviewed. Spatial domain watermarking techniques are conceptually simpler and have much lower computational complexities compared to frequency domain methods. Block based watermarking methods achieved more robustness than pixel watermarking methods, in which watermarks were embedded by modifying the LSB of image pixels. The review of spatial watermarking methods shows that development of robust spatial domain watermarking methods is still a challenge research issue. For example robustness against cropping attacks. Many frequency domain methods, in which watermarks were embedded into the transform domain coefficients, were reviewed. These methods achieved more robustness than spatial domain methods because the watermarks were embedded into significant band. However, drawbacks in the existing frequency domain methods are that the detection processes require the original image; some existing methods used the full-frame DCT. Therefore, they require high computing cost and low processing speeds. Moreover, the conflicting requirements of watermarking scheme were not addressed directly in the frequency domain. Therefore, there is a challenge in designing a robust blind image watermarking scheme, which does not require the

original image in the detection process; address the conflicting requirements directly in frequency domain to reduce the computing cost and improve the processing speed and achieve more robustness against signal processing and geometric attacks. The review of the feature domain watermarking methods show that using image content image such as feature points as references can provide solutions for watermark synchronization. Feature points represent an invariant reference for geometric attacks. However, the feature point extraction techniques adopted by current feature-based approaches, for instance, the Harris detector or the Mexican hat wavelet detector are sensitive to image modification which makes their robustness to specific attacks limited. Moreover, the normalization technique was applied to the entire image. Therefore, robustness against cropping attack can not be achieved due to the fact the moments depend on all pixels. In the next chapter, a proposed multiple spatial watermarking technique in colour image is introduced.

CHAPTER FOUR

4 MULTIPLE SPATIAL WATERMARKING IN COLOUR IMAGES

4.1 Introduction

As mentioned in the Chapter 3, the main advantage of spatial watermarking schemes over alternative schemes is that they have lower computational cost. However, they are less robust against signal processing and geometric attacks. This chapter presents a robust colour image watermarking technique. It is based on embedding a binary watermark image into different regions of the blue channel of the host image to achieve more robustness against various attacks.

This chapter is organized as follows. Section 4.2 presents the overview of previous colour image watermarking techniques. Section 4.3 describes the proposed watermark encryption, embedding and detection processes for three watermarking schemes. Conclusions are drawn in Section 4.4.

4.2 Overview of Previous Colour Image Watermarking Techniques

As described in Chapter 3, a wide variety of image watermarking algorithms have been proposed to provide copyright protection of digital images. Most existing watermarking algorithms focus mainly on embedding watermarks into grey-scale images. The extension to colour images is usually accomplished by marking the image luminance

component or by processing each colour channel separately [115, 116]. Kutter et al. [117] proposed an alternative method for watermarking colour images. It is based on embedding a watermark by modifying a selected set of pixel values in the blue channel, since the human eye is less sensitive to changes in this band. To achieve robustness against JPEG compression attack, Lian et al. [118] suggested that the watermark should be embedded into the green component rather than the red or blue components of the colour image. This is because the loss of energy of the blue and red components is higher than the green component when the watermarked image is attacked by JPEG compression. However, the human eye is more sensitive to changes in the green band. In Lian's method, the watermark is embedded into the largest coefficients of the low-frequency subband of the DWT. The watermark capacity is limited, since the watermark is embedded into only the significant coefficient of transformed image, which mostly contains only a few significant coefficients. Fleet and Heeger [119] proposed a method, which takes into account the characteristics of the human visual system (HVS) with respect to colour perception. They suggested embedding the watermark into the yellow-blue channel of colour images and using the S-CIELAB space to measure the color reproduction error. However, their method can only resist printing and rescanning attacks. Barni et al. [120] introduced another colour image watermarking method based on the cross-correlation of RGB channels. However, it has relative high computing costs and low processing speed since the full-frame DCT is used for three colour channels. Tsai et al. [121] provided a solution of embedding the watermark on a quantized colour image. Kutter at al. [122] investigated watermarking of luminance and blue-channels using a perceptual model, which takes into account the sensitivity and the masking behaviour of the HVS. The results demonstrate that more robustness can be achieved when the watermark is embedded into the blue channel than the luminance channel of an image. Huang et al. [71] embedded the watermark into DC coefficients of a colour

image directly in the spatial domain, followed by a saturation adjustment technique performed in the RGB colour space. Verma et al. [123] suggested encoding the watermark by using convolution coding and then embedding the watermark bits into blocks of size 8×8 of the host image. The disadvantages of using the convolution coding are that it adds redundant information to the original watermark and it requires a constant large number of decoding operations, even if few or no errors occur [124]. This method is comparatively less robust to cropping attacks because the watermark bits are embedded into the whole image hence some data must be lost in cropping.

4.3 Proposed Multiple Watermarks Techniques Based on the Blue Channel and the Block Probability in the Spatial Domain

This section describes the proposed multiple watermarks techniques, which based on embedding a binary logo image into the blue channel of the host colour image. The blue channel is selected to embed the watermark because the human eye is least sensitive to modifications in the blue band [117]. Three watermarking schemes are presented. The embedding processes of these schemes are based on dividing the blue component of the host colour image into different regions and embedding watermark bits into 8×8 non-overlapping blocks. The differences between theses schemes are how to determine the regions to embed watermarks and how to extract and detect the watermark. The main contribution consists of embedding multiple watermarks into different regions of the blue component of the host image in the spatial domain. This is motivated by the following facts.

(i) Embedding watermarks into different regions of the host image can increase the robustness because if a watermarked region is destroyed, the watermark can still be extracted from other regions.

(ii) The human eye is less sensitive to noise and changes in the blue component of an image; this makes sense to select the blue component to for watermark embedding and ensures the imperceptibility of the embedded watermarks.

The following sections describe theses schemes.

4.3.1 Watermark Encryption process

In order to improve the security of the watermarking scheme, a watermark should be encrypted or permuted to obtain a pseudo random sequence, which is uncorrelated to the original watermark [90]. In the proposed schemes, a binary logo image is used as a watermark W, which represented by

$$\mathbf{W(i,\ j), O \leq i,\ j < M,\ W(i,\ j) \in (1, O)} \tag{4-1}$$

where (i, j) represents the pixel coordinates of the binary watermark image and M denotes the size of the watermark. Before embedding the watermark into the host colour image, the watermark is encrypted to produce pseudo random sequences, which are uncorrelated with the original watermark. The watermark encryption process can be defined as the function given by

$$W^{*} = E(W\ , C\ ) \tag{4-2}$$

where E (.) denotes the encryption function, W^{*} denotes the encrypted watermark, W is the original watermark, C is chaotic binary sequences, which are generated randomly by using a secret key. The number of bits used in chaotic binary sequences is 1024 bits. The encrypted watermark can be obtained by

$$\mathbf{W^{*} = W \oplus C} \tag{4-3}$$

where $\oplus$ denotes the XOR operation between the original watermark and the chaotic binary sequence. As an example, Figure 4.1 shows the original and the encrypted

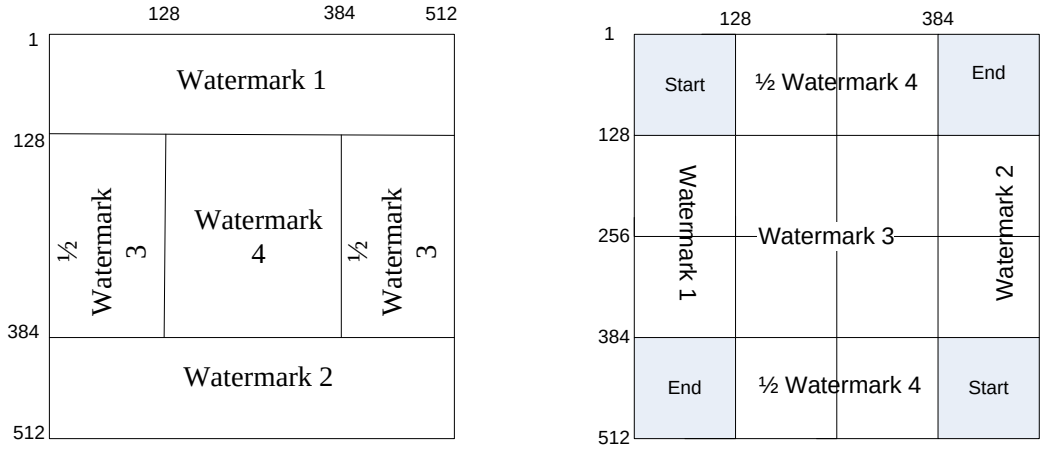
watermark, which is uncorrelated to the original watermark and difficult to obtain without knowing the secret key that was used in encryption process.

(a) (b)

Figure 4.1 (a) Original watermark, (b) Encrypted watermark.

4.3.2 Watermarking Procedure for the first and second schemes

In the first scheme, the blue channel of the host image is divided into different regions and into each embedded a watermark. The watermark is embedded four times in different regions in order to protect the watermarked image and make it harder for attackers to destroy all of them. These regions are defined as shown in Figure 4.2 (a). In the second scheme, the blue channel is divided into a different set of regions, each of size 128 ×128, in order to embed a part of the watermark as shown in Figure 4.2 (b). As can be seen, the first and the last part of the watermark1 and watermark2 are sharing with first and the last part of the watermark 4, respectively; therefore these parts of the watermarks are embedded once time. The limitation of these schemes is that in cropping attack, the watermark may not be extracted from a small portion of watermarked image, which may not contain the whole watermark. To overcome of this, a new embedding strategy is described in the third scheme (refer to Section 4.3.3).



(a) (b)

Figure 4.2 the watermark embedding regions, (a) first scheme, (b) second scheme .

4.3.2.1 Watermark Embedding Process

The watermark embedding process of the first and second schemes is shown in Figure 4.3. Suppose I_b denotes the blue component of the original colour image to be protected by the binary image watermark W. The blue component of the original image I_b is represented by

$$I_b = (x(i, j), 0 \le i, j \le N) \tag{4-4}$$

where $x(i, j)$ represents the intensity pixel at location (i, j) and N represents the size of the original image. For convenience, we assume N = 512. Each bit of an encrypted watermark is embedded into an 8x8 block of the selected region. The total length of the watermark is defined as L, where

$$L = \frac{M \times N}{R \times T}, \tag{4-5}$$

T is the number of pixels that are used to embed the watermark in each block and R represents the number of watermarks embedded into regions. For example, the size of the host image is 512×512; a watermark bit is embedded in an 8×8 block and the

number of watermarks is 4. Therefore, the watermark length is 1024 bits. In the embedding process, each bit of an encrypted watermark is embedded into an 8x8 block of the selected regions. The watermark embedding algorithm can be described as follows:

$$x^*(i,j) = \begin{cases} x(i,j) + \alpha & 1 \le i,j \le 8 \quad \text{if } W^*(i,j) = 1 \\ x(i,j) - \alpha & 1 \le i,j \le 8 \quad \text{otherwise} \end{cases} \tag{4-6}$$

where $W^*(i,j)$ represents an encrypted watermark bit, $x^*(i,j)$ and $x(i,j)$ represent the watermarked intensity pixel and the original intensity pixel at location (i,j), respectively and α is the watermark embedding strength.

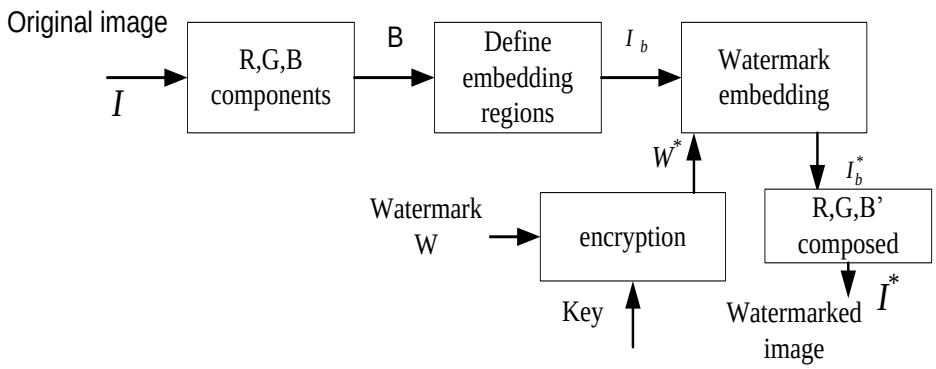


Figure 4.3 the watermark embedding process of the first and second schemes.

4.3.2.2 Watermark Extraction and detection Process

The watermarked image may be modified either intentionally or unintentionally. Under these circumstances it should still be possible to extract the watermark correctly. The watermark extraction and detection processes are shown in Figure 4.4. Suppose I^* is an image subjected to watermark detection. Firstly, the blue components of the original image and input image are decomposed into regions as shown in Figure 4.2. Secondly, the watermarks are extracted by comparing the intensity pixel of each region in the

original image with the corresponding region in the watermarked image and the probabilities of detecting bit ‘1’ or bit ‘0’ are computed for each small region of 8x8 as follows:

$$P_1 = P_1 + 1/64 \qquad \text{if} \quad x^*(i,j) > x(i,j), 1 \le i,j \le 8 \tag{4-7}$$

$$P_0 = P_0 + 1/64 \qquad \text{if} \quad x^*(i,j) \le x(i,j), \; 1 \le i,j \le 8, \tag{4-8}$$

where P_1 and P_0 are the probability of detecting bit ‘1’ and bit ‘0’ respectively, $x^*(i,j)$ and $x(i,j)$ represent the watermarked intensity pixel and the original intensity pixel at location (i,j), respectively. The extracted watermark bits can be obtained as follows:

$$W^*(i,j) = \begin{cases} 1 & \text{if } P_1 \ge P_0 \quad 1 \le (i,j) \le M \\ 0 & \text{if } P_1 < P_0 \quad 1 \le (i,j) \le M \end{cases}, \tag{4-9}$$

where W^* is extracted watermark, i,j represents the location of the extracted bit and M represents the size of the watermark.

Thirdly, the inverse encryption process is applied to all extracted watermarks using the same key that was used in the watermark embedding process. Normalized cross correlation is used to measure the similarity between the original and extracted watermarks. In the detection process of the first scheme, four watermarks are extracted and the watermark with highest value of NCC is chosen to be the extracted watermark. The detection process can be summarized as follows:

1- Five watermarks are extracted from the watermarked image.
2- Another watermark is built from extracted watermarks by dividing the extracted five watermarks into four parts as shown in Figure 4.5, and then the part with highest NCC value is selected to reconstruct the watermark.

3- The NCC values of the five extracted watermarks and the reconstructed watermark are computed

4- The watermark with highest value of NCC is chosen to be the extracted watermark.

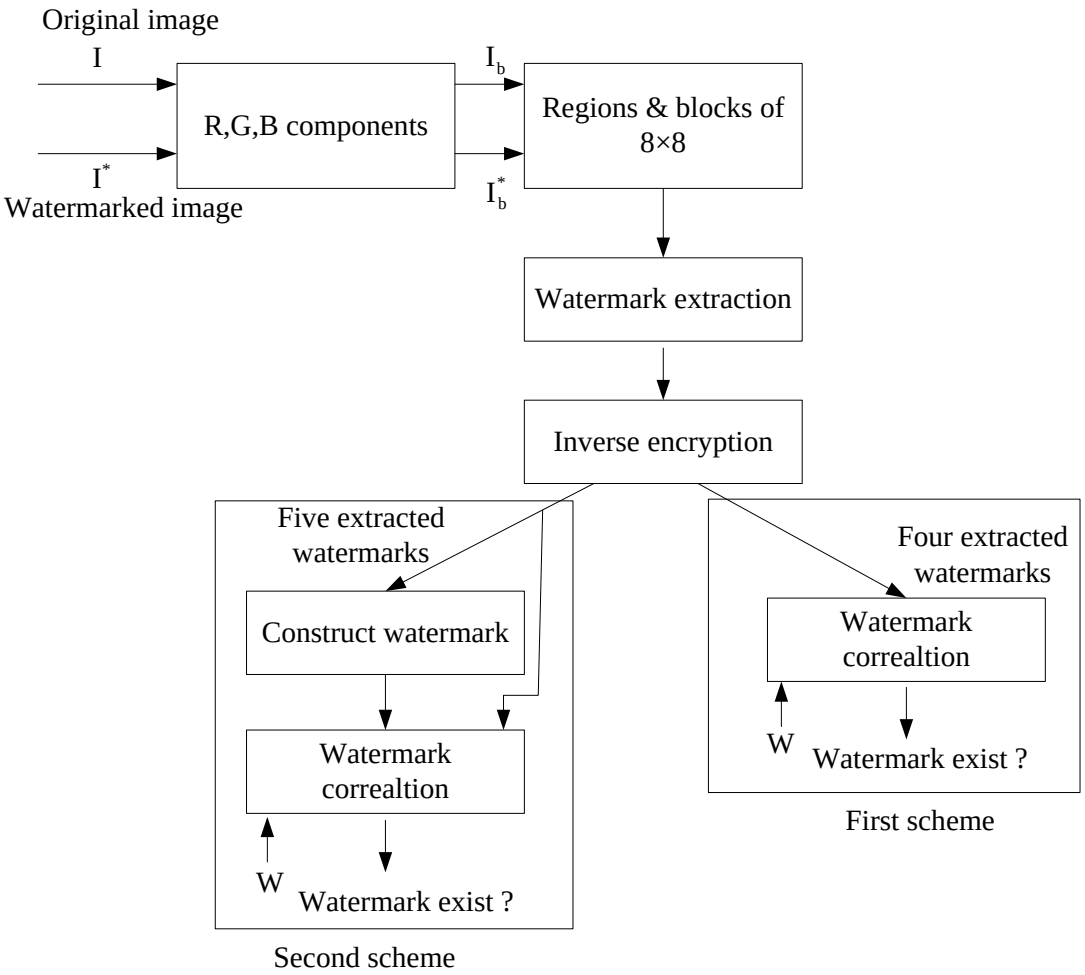


Figure 4.4 watermark detection process of the first and second schemes.

Figure 4.5 watermark parts.

4.3.2.3 Experimental Results for the First and Second Schemes

The performance of the proposed schemes was tested on several images commonly used for this purpose. Results are presented for the Lena, Peppers and Baboon colour images of size 512×512. A binary image of size 32×32 was used for the watermarking logo. The embedding strength (α) was determined as suggested in [123]. The un-watermarked 'Lena' and 'Peppers' images are shown in Figure 4.6. The watermarked 'Lena' and 'Peppers' images having PSNR values of 38.9239 and 39.0627 are shown in Figure 4.6 (b) and (d), respectively. The original and extracted watermark images are shown in parts (e) and (f) of Figure 4.6. It can be seen from inspection of Figure 4.6 that the differences between the corresponding watermarked and un-watermarked images are imperceptible, so the embedded watermarks are invisible to the human eye. Note that Lena image is watermarked by using first scheme and Peppers image is watermarked by using second scheme.

(a) (b)

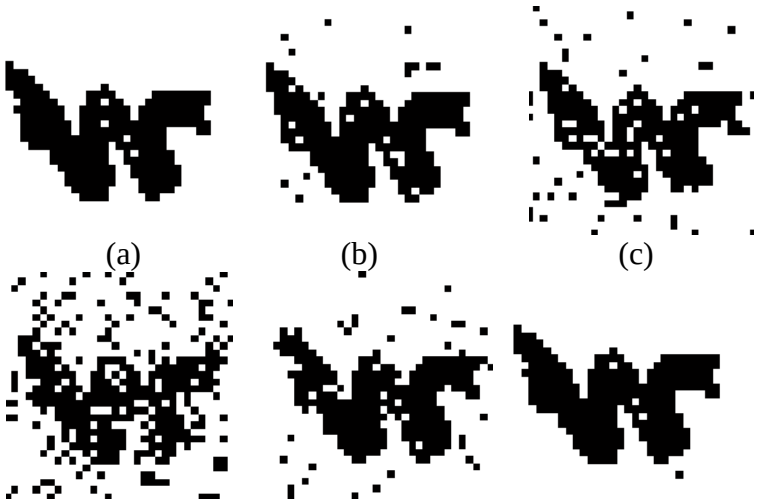
(c) (d)

(e) (f)

Figure 4.6 (a) Orginal Lena image, (b) Watermarked Lena image, (c) Original Pepper image, (d) Watermarked Pepper image, (e) Original watermark, (f) Extracted watermark.

The benchmark software StirMark 4.0 [6, 19] was used to test the robustness of the proposed schemes. This evaluates several attacking operations including median filtering, lowpass filter, JPEG-lossy compression, scaling, cropping, rotation-crop, rotation-scaling, rotation, removal of some rows and columns, and self–similarity attacks in different colour models, etc.

Figure 4.7 shows the extracted watermarks form the watermarked images 'Lena', 'Peppers', and 'Baboon' following several attacks including: 3×3 median filtering, 5×5 median filtering; 7×7 median filtering; JPEG compression with quality factors of 30% and 50%; self similarity attack (SS2); rotations by 0.5°, -0.75°; rotation-scaling by 0.25°, 1°; rotation-cropping by -1°,0.50°. All the extracted watermarks can be visually identified and the detector's response correctly declares the existence of the watermark.



(a) (b) (c)

(d) (e) (f)

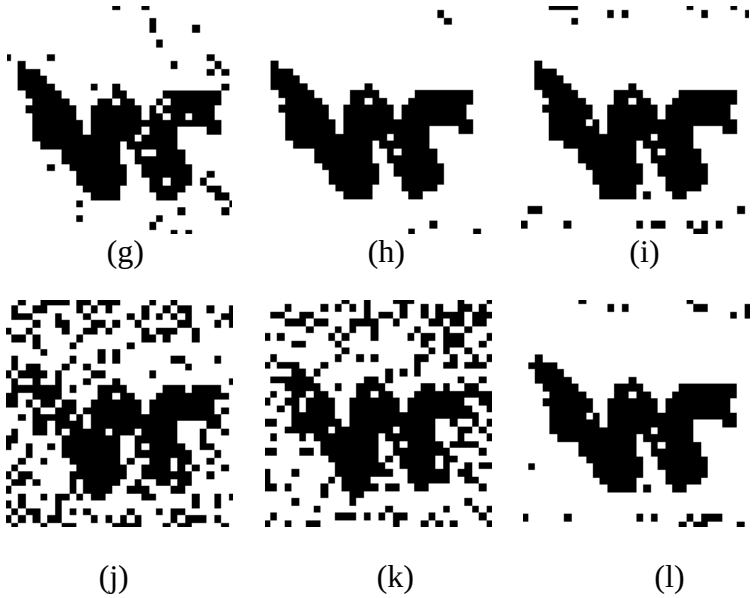
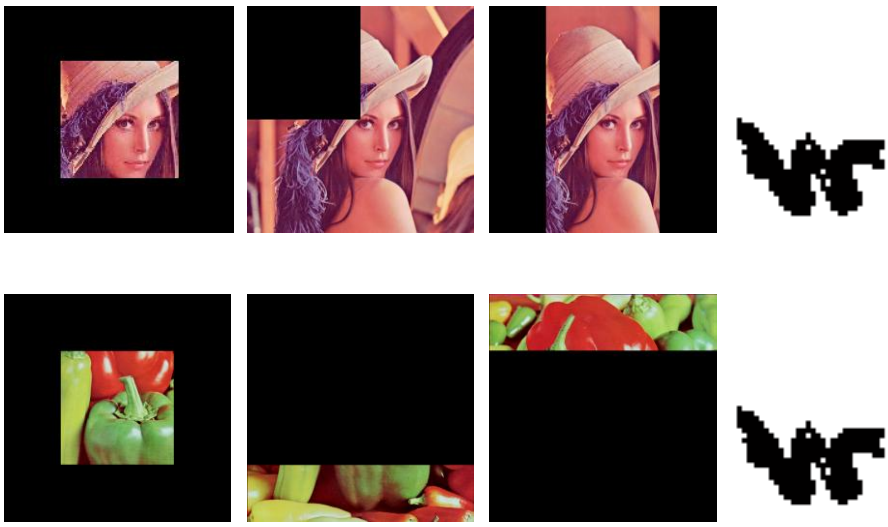


Figure 4.7 (a) Extarcted watermarks after (a), (b), (c) 3×3, 5×5 and 7×7 median filtering, respectively;(d) JPEG 30%; (e) JPEG 50%, (f) self similarty(ss2); (g), (h) rotations by 0.5°, -0.75°; (i), (j) rotation-scaling by 0.25°, 1°; (k), (l) rotation-cropping by -1°,0.50°

To test the robustness of the proposed schemes against cropping attacks, watermarked images were cropped as shown in Figure 4.8. The results demonstrate that the watermark can still be correctly extracted from the remaining portion of the watermarked images even when the watermarked image is cropped by 50%. This is because the watermark was embedded into different regions of the watermarked images so the watermark can still be extracted from the remaining regions, which contain the watermark.



(a) (b)

Figure 4.8 (a) Cropped watermarked images; (b) extracted watermarks.

Table 4.1 summarizes results from applying several common image processing and geometric attacks to the images 'Lena' and 'Peppers' watermarked using the proposed first and second schemes. It can be seen that the second scheme performs better than the first scheme. This is because in the second scheme, the watermark is reconstructed from all extracted watermarks, so if a part of the watermark is destroyed, this part can be recovered from other region.

The performance of the proposed schemes is due to following facts

(i) If a region destroyed by attacks such as cropping attacks, the detector can still extract the watermark from other regions.

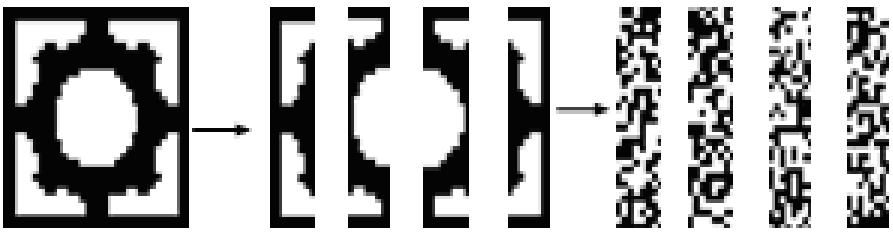
(ii) Each watermark bit is embedded into an 8×8 block. As a result, if some pixels in such block are destroyed, the watermark bit can still be detected from other pixels in the block.

Table 4.1 Expermental results with StirMark 4.0 for Lena and Pepper images (α=5) .

	First Scheme		Second Scheme	
	Lena	peppers	Lena	peppers
Attacks	NCC	NCC	NCC	NCC
JPEG 75%	0.82	0.72	0.99	0.99
JPEG 50%	0.55	0.50	0.95	0.93
Median filter 3*3	1.0	1.0	1.0	0.99
Median filter 5*5	1.0	1.0	1.0	0.99
Median filter 7*7	0.75	0.66	0.99	0.98
Rotation-scaling 0.25	0.57	0.54	0.96	0.97
Rotation-scaling-0.25	0.77	0.53	0.97	0.97
Rotation-crop 0.25	0.67	0.59	0.97	0.97
Rotation-crop -0.25	0.60	0.54	0.98	0.97
Rotation _0.25	0.98	0.72	0.97	0.85
Rotation _0.50	0.97	0.47	0.96	0.93
Rotation _2	1.0	1.0	1.0	0.97
Rotation _5	1.0	0.48	1.0	0.96
Rotation _30	1.0	0.87	0.99	0.82
Rotation _45	0.65	0.70	0.98	0.96
Rotation _90	0.72	0.56	0.99	0.98
Remov_lines_10	0.98	0.88	0.99	0.99
Remov_lines_50	0.84	0.82	0.99	0.98
Remov_lines_70	1.0	0.77	0.99	0.97
Remov_lines_100	0.85	0.53	0.99	0.98
Ss1	1.0	1.0	1.0	0.97
Ss2	0.69	0.66	0.98	0.81
Ss3	1.0	0.72	0.99	0.92

4.3.3 Watermarking Procedure for Third Scheme

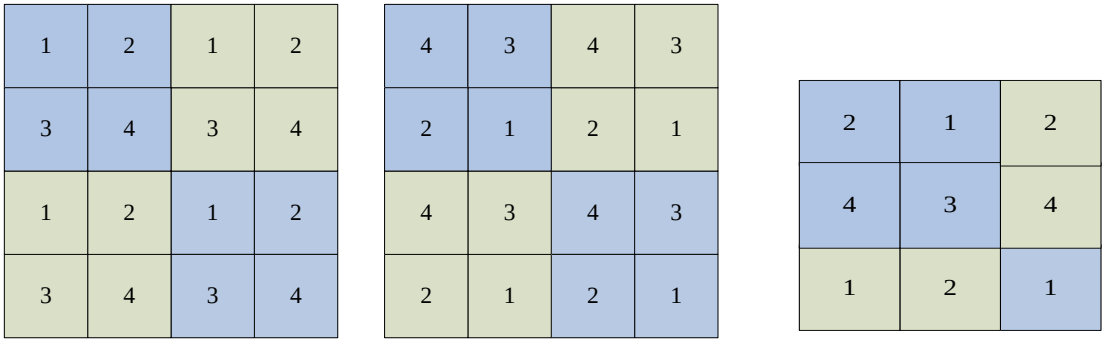
To improve robustness against cropping attacks, a new strategy for embedding multiple watermarks is presented. It is based on dividing a watermark into four parts; each encrypted using a secret key and embedded into different regions of the blue component of the colour host image. Figure 4.9 shows the original and the encrypted watermark parts.



(a) (b) (c)

Figure 4.9 (a) Original watermark; (b) watermark parts, (c) enceypted watermark parts.

In the embedding process, the blue component is divided into regions of size 128×128 and each is divided into non-overlapping blocks of size 8×8 in order to embed a watermark bit; therefore a watermark with size 32×32 requires four regions of size 128×128. Figure 4.10 illustrates the embedding regions for images of sizes 512×512 and 384×384. As shown in Figure 4.10, the numbers {1, 2, 3, and 4} represent the watermark parts, which are embedded in regions of size 128×128. The purpose of embedding each part into different regions is to protect the watermarked image from cropping attacks. For instance, the watermark can still be detected from any cropped image comprising 50% of the watermarked image. Also if only two regions remain, 50% of the watermark can still be detected. The watermark embedding algorithm uses equation (4-10).



(a) (b) (c)

Figure 4.10 Embedding regions.

4.3.3.1 Watermark Extraction and Detection Process

The watermark extraction and detection processes are shown in Figure 4.11. In the extraction process, the watermark parts are extracted from the watermarked image; in the detection process the watermark is reconstructed from the extracted watermark parts and detected using the Pearson's Correlation coefficient (CC) given in equation (2-10). Suppose I^* is an image subjected to watermark detection. Firstly, the blue components

of the original image and input image are decomposed into regions of size 128×128. Secondly, the watermark parts are extracted by comparing the intensity pixel of each region in the original image with the corresponding region in the watermarked image and the probability of detecting bit '1' or bit '0' are computed for each small region of 8×8 as given in equations (4-7) and (4-8), respectively. The extracted watermark bits can be obtained as follows:

$$W_i^*(m,n) = \begin{cases} 1 & \text{if } P_1 \geq P_0 \quad 1 \leq m \leq M,\ 1 \leq n \leq M/4 \\ 0 & \text{if } P_1 < P_0 \quad 1 \leq m \leq M,\ 1 \leq n \leq M/4 \end{cases}, \tag{4-11}$$

where W_i^* represents extracted watermark parts, $i \in \{1,2,3,4\}$; m, n represents the location of the extracted bit and M represents the size of the watermark. Each part of the watermark is extracted from four different regions. The inverse encryption process is applied to all extracted watermark parts using the same four secret keys that were used in the watermark encryption process. In the detection process, Pearson's Correlation coefficient (CC) given in equation (2-10) is used to select one part from each four identical extracted parts according to the highest value of CC of the extracted parts. The selected four parts are used to reconstruct the extracted watermark.

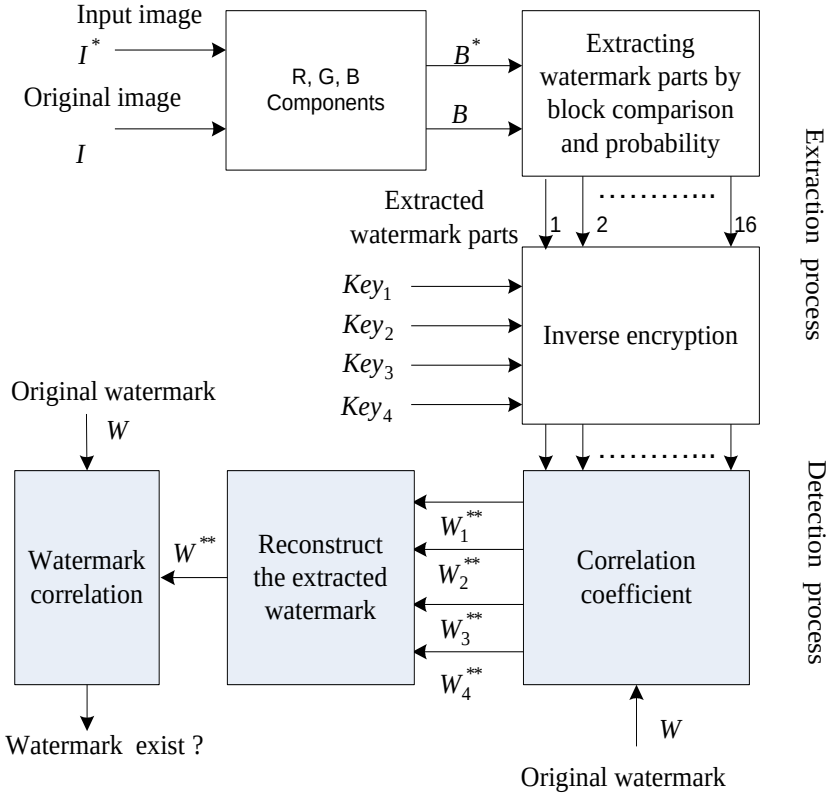


Figure 4.11 Watermark extraction and detection process.

4.3.3.2 Experimental Results

To evaluate the watermark imperceptibility, the Peak Signal-to-Noise Ratio (PSNR) given in equation (2-9) was adopted to measure the perceptual distortion of the proposed scheme. The Structural Similarity index Measure (SSIM) was also adopted for assessing the similarity between the original image and the watermarked one. Figure 4.12 shows the un-watermarked and the watermarked images 'Peppers' and 'Baboon'. The original watermark image and extracted watermarks are shown in Figure 4.13. It can be seen by inspection of Figure 4.12 that the differences between the corresponding watermarked and un-watermarked images are imperceptible and so the embedded watermarks are invisible to the human eye. The results in Table 4.2 show that PSNR values are greater than 30.00 dB, which is the empirically tested threshold value for an

image to have no perceivable degradation [113]. The SSIM results support this conclusion since the SSIM values are high after embedding the watermark. There is a relationship between the watermark strength and invisibility achieved by the proposed scheme.

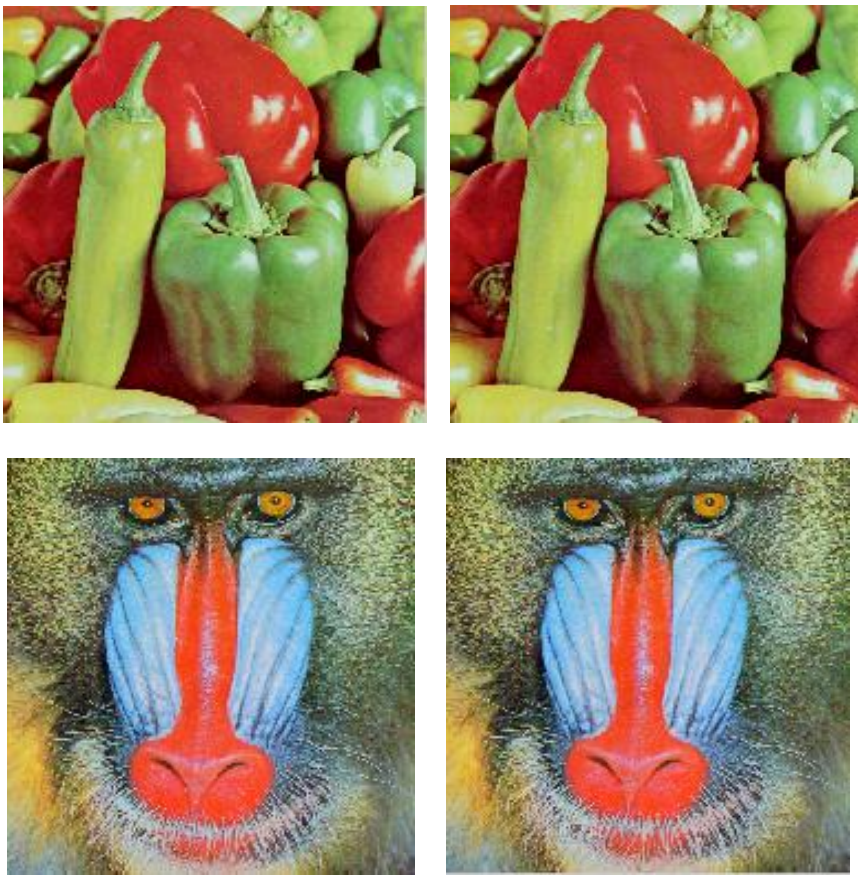
Table 4.3 shows the results of varying the watermark strength. As can be seen, increasing the value of the watermark strength introduces more distortion in the watermarked images.

Table 4.2 PSNR and SSIM of the watermarked images (α=4).

Images	PSNR	SSIM
F-16	40.863	0.9732
Lake	40.874	0.9815
Couple	41.104	0.9651
Opera	40.884	0.9816
Watch	40.901	0.9773
Water	40.862	0.9887
House	40.863	0.9829
Barbara	40.861	0.9879
Tiffany	40.870	0.9745
Arctic	41.312	0.9730

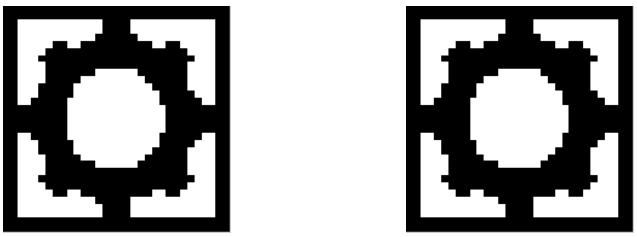
Table 4.3 Results of varying the watermark strenght (α).

	PSNR (dB)			SSIM		
α	Lena	Peppers	Baboon	Lena	Peppers	Baboon
1	52.90	52.99	52.91	0.9984	0.9984	0.9995
2	46.88	46.89	46.89	0.9938	0.9938	0.9982
3	43.36	43.47	43.37	0.9867	0.9867	0.9961
4	40.86	40.99	40.87	0.9775	0.9778	0.9932
5	38.92	38.96	38.93	0.9670	0.9676	0.9897



(a) (b)

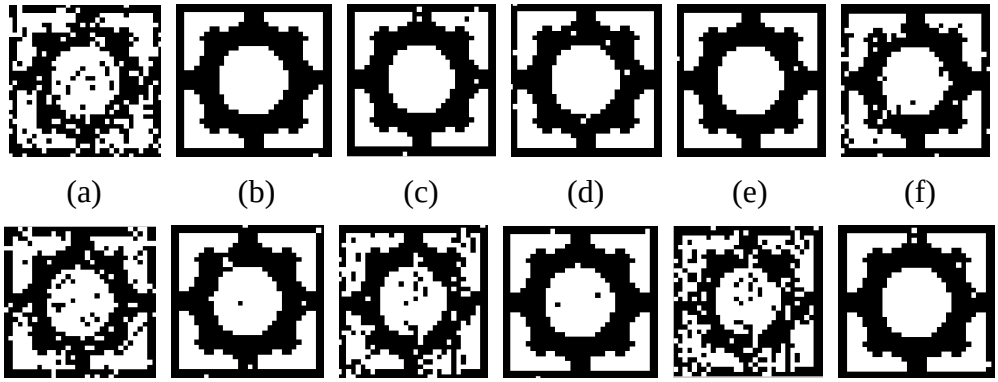
Figure 4.12 (a) Original images, (b) Watermarked images.



(a) (b)

Figure 4.13 (a) Original watermark, (b) Extracted watermark.

The benchmark software StirMark 4.0, mentioned earlier was used to test the robustness of the proposed scheme. Figure 4.14 shows the watermarks extracted from watermarked images 'Lena', 'Peppers', and 'Baboon' following several attacks including: JPEG compression with quality factors 30%, 5×5 median filtering; 7×7 Gaussian lowpass-filtering; scaling by 0.5; scaling by 2; rotation by 2°; rotation by 30°, rotation-scaling by 0.25°; rotation-scaling by 0.25°; rotation-cropping by 0.25°; rotation-cropping by 1°; self similarity attack (SS2). All the extracted watermarks can be visually identified and the detector's response correctly declares the existence of the watermark.



(a) (b) (c) (d) (e) (f)

(g) (h) (i) (j) (k) (l)

Figure 4.14 . Extracted watermarks after (a) JPEG compression with quality 30%, (b) 5×5 median filtering;(c) 7×7 Gaussian low-pass filtering; (d) scaling by 1/2; (e) scaling by 2; (f) rotation by2°; (g) rotation by 30°; (h) rotation-scaling by 0.25°; (i) rotation-scaling by 0.75; (j) rotation-crop by 0.25°; (k) rotation-crop by 1°; (l) self similarities (ss2).

The method described in [123] was implemented and used as a benchmark in order to evaluate the robustness of proposed scheme under the same environment. It was chosen to evaluate the proposed scheme because, like the proposed scheme, it is a block spatial domain method; it is non-blind method like the proposed scheme and it uses the blue channel for embedding a watermark. The method reported in [123] used convolution code for encoding the watermark. As a result, redundant information is added to the original watermark. As mentioned earlier, convolution code requires a constant large number of decoding operations, even if few or no errors occur.

Figure 4.15 shows examples of the watermarks extracted after JPEG attacks with quality factor of 80%, 50% and 30 % applied to watermarked 'Baboon' and 'Lena' images using the proposed scheme and the method reported in [123].

Figure 4.16 and Figure 4.17 show some experimental results from median, low-pass filtering, the combination of scaling with small angle rotation, the combination of small angle rotation with cropping attacks on the images 'Lena' and 'Baboon', watermarked using the proposed scheme and the method reported in [123].

It can be seen that the proposed scheme achieves more robustness to these attacks, in comparison with the benchmark. This is because in the proposed scheme the watermark is reconstructed from different parts of an image so if a part is destroyed the watermark can still be detected from other parts.

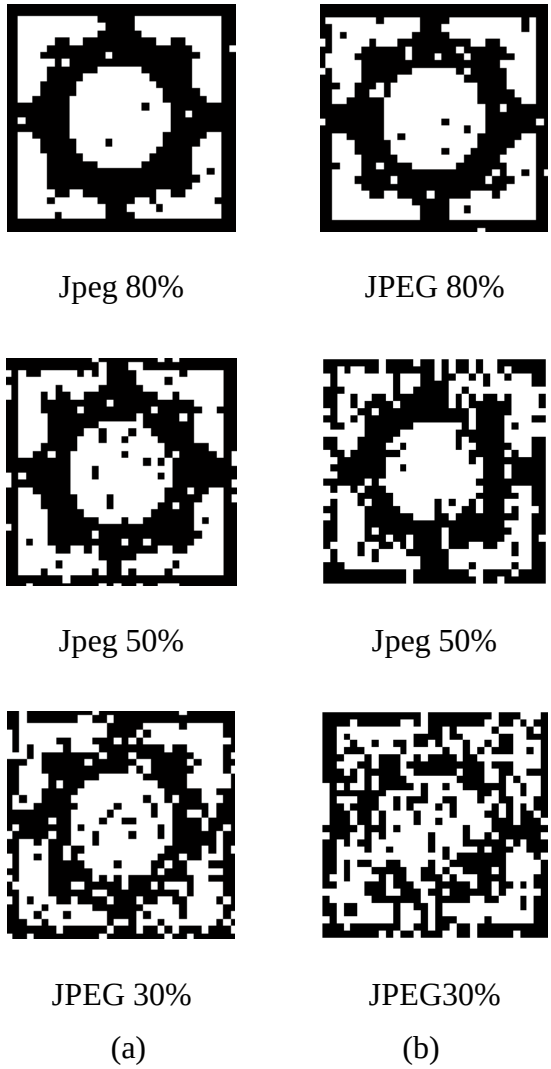
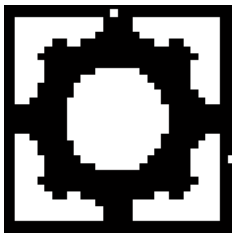


Figure 4.15 . Extracted watermarks after JPEG compression attacks, (a) proposed scheme, (b) scheme in [123].

Median filter 3×3
Baboon image

Median filter 3×3
Baboon image



Low-pass filter 3×3
Lena image

Low-pass filter 3×3
Lena image

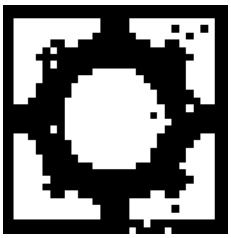
Low-pass filter 3×3
Baboon image
(a)

Low-pass filter 3×3
Baboon image
(b)

Figure 4.16 . Extracted watermarks after median and low-pass filtering attacks, (a) proposed scheme, (b) scheme in [123].

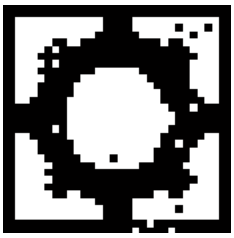
Rotation-scaling 0.25°
Baboon image

Rotation-scaling 0.25°
Baboon image



Rotation-scaling 0.25°
Baboon image

Rotation-scaling 0.25°
Baboon image



Rotation-crop 0.25°
Lena image

Rotation-crop 0.25°
Lena image

Rotation-crop 0.5°
Lena image
(a)

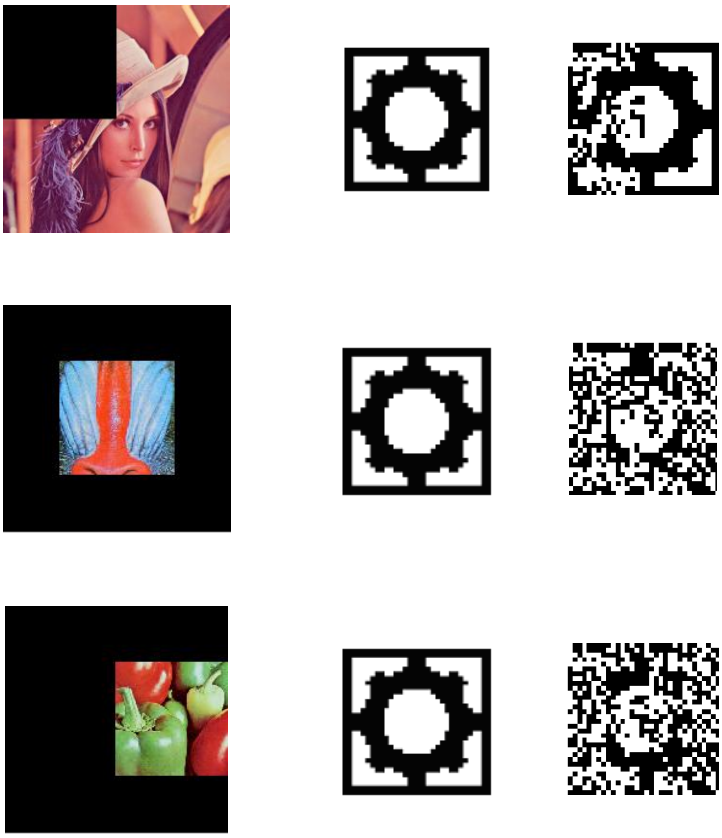
Rotation-crop 0.5°
Lena image
(b)

Figure 4.17 . Extracted watermarks after small rotation- scaling attacks and small rotation crop attack, (a) proposed scheme, (b) scheme in [123].

In order to test the robustness of the proposed scheme against cropping attacks, watermarked images were cropped in various ways as shown in Figure 4.18 and Figure

4.19. Results in Figure 4.18 show that watermarks can be extracted correctly with CC = 1 and results in Figure 4.19 show that watermarks can still be detected, even when the remaining area of the watermarked image Lena is 37 % of the whole image, or when only 12.5% of the whole watermarked image remains. It can be seen that the proposed scheme performs well against cropping attacks compared to the method reported in [123]. Because the watermark was embedded into different regions of the watermarked image, the proposed scheme is able to extract the watermark from the remaining regions of the watermarked image.

Table 4.4 summarizes the experimental results from applying common signal processing and some geometric attacks on Lena, Peppers and Baboon images watermarked using the proposed scheme and the method reported in [123].



(a) (b) (c)

Figure 4.18 (a) Cropped watermarked images, (b) Extracted watermarks using the proposed scheme, (c) Extracted watermarks using the method reported in [123].

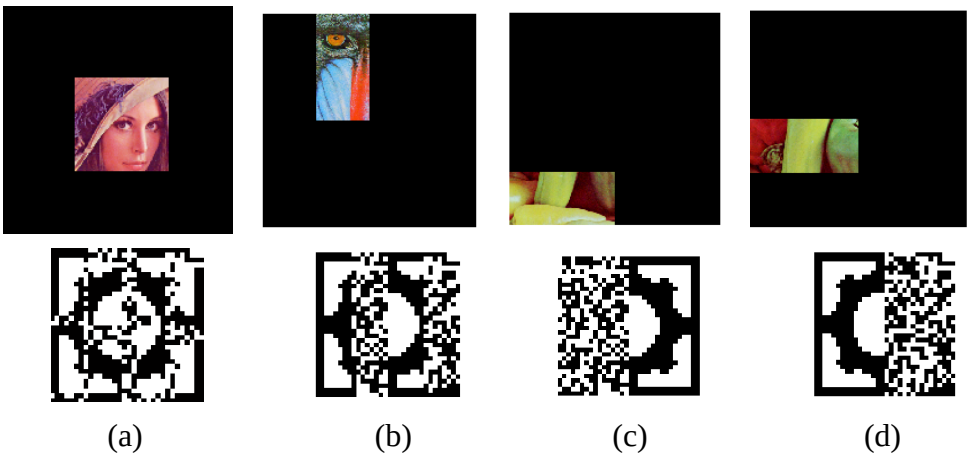


Figure 4.19 Watermarked cropped images and the extracted watermarks (a) 37%, (b), (c) and (d) 12% remaining area.

The improved performance of the proposed scheme compared to related work [123] is because in the proposed scheme, each part of the watermark is embedded into different regions of the host image. As a result, if some parts of the watermark are destroyed, the watermark can still be reconstructed from other parts. By contrast, the watermark is embedded into the whole image in the method reported in [123]. This leads to losing some data when the watermarked image is cropped.

Table 4.4 Comparison between the proposed scheme and the method reported in [123] under common signal processing and some gemometric attacks.

Attacks	Lena		Peppers		Baboon	
	Proposed scheme	scheme [123]	Proposed scheme	scheme [123]	Proposed scheme	scheme [123]
JPEG 80	0.99	1.0	0.98	0.97	0.96	0.96
JPEG 50	0.91	0.90	0.88	0.92	0.85	0.72
JPEG 30	0.69	0.48	0.68	0.46	0.64	0.41
Median filtering 3×3	0.99	0.98	1.0	0.90	0.83	0.61
Median filtering 7×7	0.99	0.96	0.95	0.94	0.77	0.62
Low-pass filter 3×3	1.0	0.85	0.65	0.31	0.97	0.65
SS1	1.0	1.0	1.0	1.0	0.95	0.92
SS2	0.99	0.99	0.97	0.98	0.63	0.47
SS3	1.0	1.0	0.98	0.98	0.88	0.82
Scaling 50%	1.0	0.98	0.98	0.99	0.92	0.98
Scaling 200%	1.0	1.0	0.99	0.99	0.99	0.99
Rotation scaling 0.25	0.97	0.95	0.96	0.84	0.88	0.58
Rotation scaling 0.50	0.84	0.72	0.88	0.62	0.69	0.23
Rotation scaling 1	0.60	0.17	0.66	0.19	0.46	0.16
Rotation scaling -0.25	0.99	0.90	0.95	0.84	0.88	0.73
Rotation scaling -0.50	0.87	0.64	0.82	0.59	0.73	0.30
Rotation scaling -1	0.61	0.14	0.61	0.21	0.53	0.01
Rotation crop 0.25	0.99	0.96	0.96	0.81	0.88	0.55
Rotation crop 0.50	0.87	0.75	0.78	0.56	0.72	0.19
Remov_lines_30	1.0	0.99	0.99	0.97	0.96	0.88
Remov_lines_50	1.0	0.98	0.98	0.97	0.95	0.94
Remov_lines_80	1.0	0.99	0.99	0.98	0.95	0.88

4.4 Conclusions

This chapter presents a new colour image watermarking technique. It is based on embedding a watermark into different regions of the blue channel of the host image in the spatial domain. It has been found that more robustness against various attacks can be achieved when a watermark is embedded into different regions of the host image. In order to increase the robustness of watermarking scheme against cropping attack, the regions into which a watermark is embedded should be carefully selected. To achieve more robustness against cropping attacks, a watermark should be divided into different parts and each part is embedded into different regions depending on the size of the host image. In the detection process, one watermark can be reconstructed from the extracted parts. It has been demonstrated that under most of the commonly used attacks, the proposed watermarking scheme can recover the embedded watermark.

CHAPTER FIVE

5 ADAPTIVE IMAGE WATERMARKING IN THE DCT DOMAIN

5.1 Introduction

This chapter presents an approach for adaptive image watermarking by exploiting DCT (discrete cosine transform) based image compression techniques to embed watermarks in an adaptive manner, where the watermarking strength is determined by content analysis and classification of DCT blocks and depends on the image characteristics. Moreover, the watermark is resilient to attack since it is embedded strongly in more salient components of the image. The host image is not required in the watermark extraction process. In addition, the performance of the proposed method is compared to existing image watermarking technique to demonstrate the success and potential of the method for image watermarking.

This chapter is organized as follows. Section 5.2 presents the limitation of existing work, an overview of the proposed method and the principle of using sub-sampling technique in the image watermarking process. Section 5.2.3 describes the proposed watermarking algorithm design, which consists of adaptive determination of watermarking strength, adaptive embedding of watermarks and proposed watermark extraction. Section 5.4 presents experimental results and discussion. Conclusions are drawn in Section5.5.

5.2 The Proposed Image Watermarking Problem

5.2.1 Limitation of Existing Work

Previously proposed watermarking methods [68-71] embed the watermark in the DC coefficients of the DCT, but the detection process of these methods requires the original image, which may not be available in some applications. Moreover, the features of the original image are not taken into account when embedding the watermark and, as a result, the maximum-possible imperceptibility and robustness of embedded watermark cannot be guaranteed [125] . Even though imperceptibility is important to ensure there is no visual degradation when the watermark is embedded in an image.

It is well known that there is a trade-off between the imperceptibility and robustness requirements of a digital watermarking system. To address this problem, the authors in [38, 70, 125-127] proposed methods which take into account the characteristics of the host image. In these methods, edges regions are determined by applying well known methods such as Canny, Sobel, Laplacian filter, or Prewitt on the host image in the spatial domain and then watermarks are embedded in the frequency domain. Therefore, extra cost is required using such these methods.

The analysis of the existing work described above show that there is still a challenging research problem in designing a robust image watermarking method, which can achieve a better trade-off between the imperceptibility and robustness requirements, require low computing cost and it does not require the original image in the detection process. The novel solution for such challenges is described in the next sections.

5.2.2 Sub-sampling-Based Image Watermarking

An image can be subsampled into four subimages through sub-sampling through the process that can be described as follows.

Suppose that V denotes the image of size $M \times N$, four sub-images can be obtained by

$$V_1(i, j) = V(2i, 2j),\ V_2(i, j) = V(2i, 2j+1),$$

$$V_3(i, j) = V(2i+1, 2j),\ V_4(i, j) = V(2i+1, 2j+1) \qquad (5\text{-}1)$$

where i = 0, 1, 2. . . M/2 - 1, j = 0, 1, 2. . . N/2 - 1, V_1, V_2, V_3 and V_4 denote the four sub-images. Since the four subimages are highly correlated, it is expected that $V_i \approx V_j$ for $i \neq j$. Figure 5.1 shows the Lena image of size 512×512 and the four sub-images of sizes 256×256 obtained by sub-sampling.

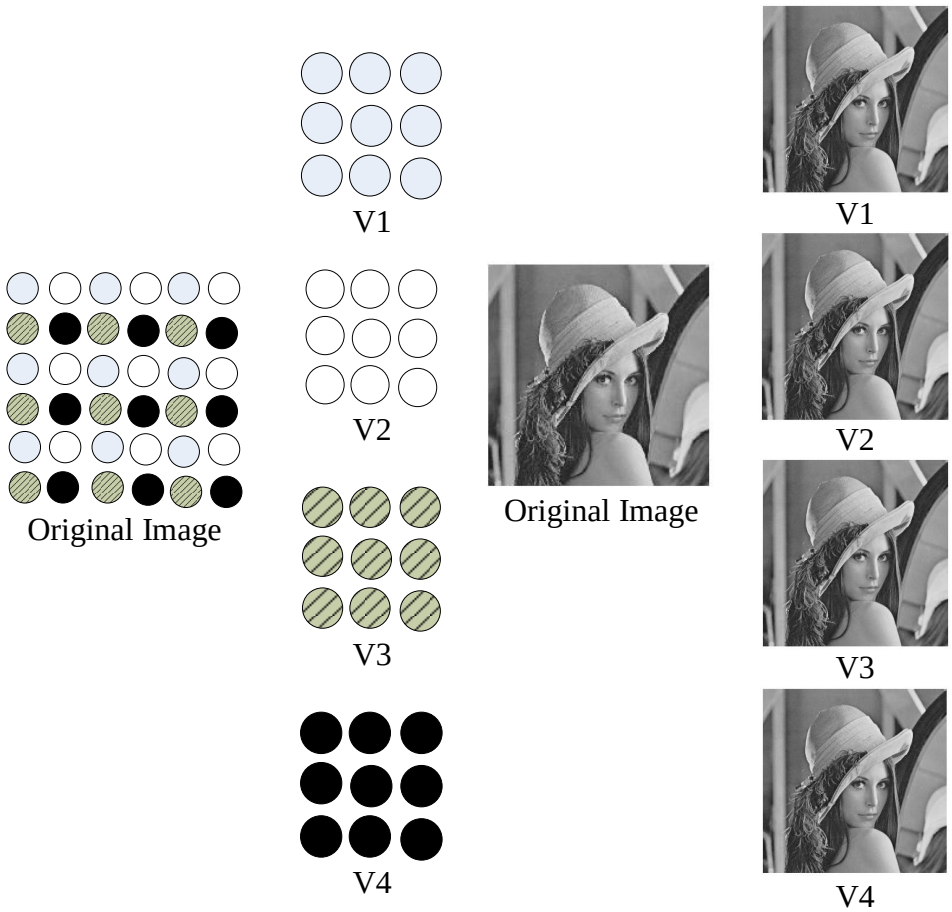


Figure 5.1: Sub-sampling of the Lena image into four sub-images

The sub-sampling process has been used recently in image watermarking techniques in order to recover the watermark without comparison with the original image. Chu [86] introduced a new blind DCT watermarking scheme based on the assumption that the DCT coefficients of different sub-images are approximately equal. In Chu's scheme,

two coefficients $D_i(u,v)$ and $D_j(u,v)$ are randomly chosen from the four DCT coefficients of the four sub-images in the same location to embed a watermark bit, and the embedding process is defined as follows

$$D_i^*(u,v) = D(1+\alpha W_n) \tag{5-2}$$

$$D_j^*(u,v) = D(1-\alpha W_n) \tag{5-3}$$

where W_n is a watermark bits, D is the average of the two selected coefficients, α is the watermark strength $i, j \in \{1,2,3,4\}$, and $i \neq j$. The watermarked sub-images can be formed by applying the inverse DCT into the sub-images, and the watermarked image is obtained by composing these watermarked sub-images. For watermark detection, the watermarked pairs of coefficients are selected as in the embedding process and the extraction of the watermark is defined as follows

$$W_n = \frac{D_i^*(u,v) - D_j^*(u,v)}{\alpha[D_i^*(u,v) + D_j^*(u,v)} \tag{5-4}$$

As mentioned in Section 3.3.5, the weaknesses of Chu's scheme are as follows: (i) It is not robust under low pass filtering or JPEG compression attack. (ii) The full-frame DCT is used for the four sub-images. Therefore, it has relatively high computing costs and low processing speeds. (iii) The embedding of the watermark is not reliable since the natural characteristics of the host image are not taken into account.

5.2.3 Overview of the Proposed Method

The sub-sampling process described in the precious section is used to obtain sub-images through sub-sampling the original image. The proposed method is based on the principle of embedding a watermark in the DC coefficients of sub-images in the DCT domain.

In comparison with existing approaches, the proposed algorithm possesses the following advantages:

1. The embedding process is adaptive and takes into account the natural characteristics of the host image and hence watermark embedding is reliable. By contrast methods in [86, 90] do not takes into account the natural characteristics of the host image.
2. Adaptability is achieved via classification of DCT blocks with three levels: smooth, edges and texture, yet such classification and analysis are implemented in the DCT domain by only analyzing the values of two AC coefficients rather than using methods such as Canny, Sobel or Prewitt. As a result, significant improvement of computing cost is achieved.
3. Stronger robustness is achieved when watermarks are embedded adaptively to the features of the host image in perceptually significant DC components. As a result of using adaptive embedding, the watermark strength can be as high as possible depending on image features in order to improve robustness. By contrast, methods in [86, 90] embedded the watermark in selected AC coefficients without taken into account the features of the image.
4. The algorithm is portable to other applications where the original image is not available in the detection process.
5. Due to its operation in DCT domain, the processing speed is high and the computing cost incurred is low.
6. The DCT and its inverse are applied only to the selected blocks, which are used to embed the watermark. By contrast, the method in [86, 90] applied the DCT to the full-frame image.

5.3 Proposed Watermarking Algorithm Design

The block diagram shown in Figure 5.2 provides an overview of the proposed watermark embedding process, which works by sub-sampling the host image into four sub-images and uses random generated sequences to select pairs of the four sub-images in order to determine the embedding positions of the watermark, which is encrypted to increase the security of the method. The DCT is applied to non overlapping selected blocks of 8×8 pixels and DC coefficients are used to embed the watermark. The watermark is embedded adaptively in order to achieve better trade-offs between the robustness and imperceptibility requirements. In general, the embedding strength of a watermark is preferred to be as high as possible in order to improve the robustness. However, this may affect the quality of the host image. Higher embedding strength results in lower quality of the watermarked image. It is obvious that the robustness and imperceptibility requirements are in conflict with each other. The best way to achieve better trade-offs among these requirements is to take the characteristics of the non-watermarked image into account when embedding the watermark. In this way, the embedding strength is determined adaptively to the image features such as, smoothness, edges and texture, aiming to minimize the perceptibility and maximize the robustness of the watermark. While most countermeasures reported in the literature [38, 70, 126, 128] usually focus on classifying edge patterns of the host image in the spatial domain using methods such as Canny, Sobel, or Prewitt and then embedding the watermark in the frequency domain, the proposed method completes the classification and the watermark embedding in the DCT domain by examination of only two DCT coefficients: X(1,0) and X(0,1).

The main contributions can be highlighted as : (i) the proposed technique embeds a watermark in an adaptive manner via classification of DCT blocks with three levels: smooth, edges, texture, implemented in the DCT domain by only analyzing the values

of two AC coefficients rather than by using methods such as Canny, Sobel or Prewitt for detecting the image edges. This adaptive technique is capable to achieve a better trade-off between watermark imperceptible and robustness requirements. This is motivated by the fact that the human eye is less sensitive to noise and changes in the texture regions; this makes sense to determine the watermark strength adaptively to the image content to ensure imperceptibility and robustness of the embedded watermarks; (ii) Blind watermark embedding and extraction in the DCT domain: embedding a watermark into DC components of the DCT makes the proposed method more robustness to common attacks. The blind watermarking method does not require the original image at the detection process, which makes the proposed method portable to many applications.

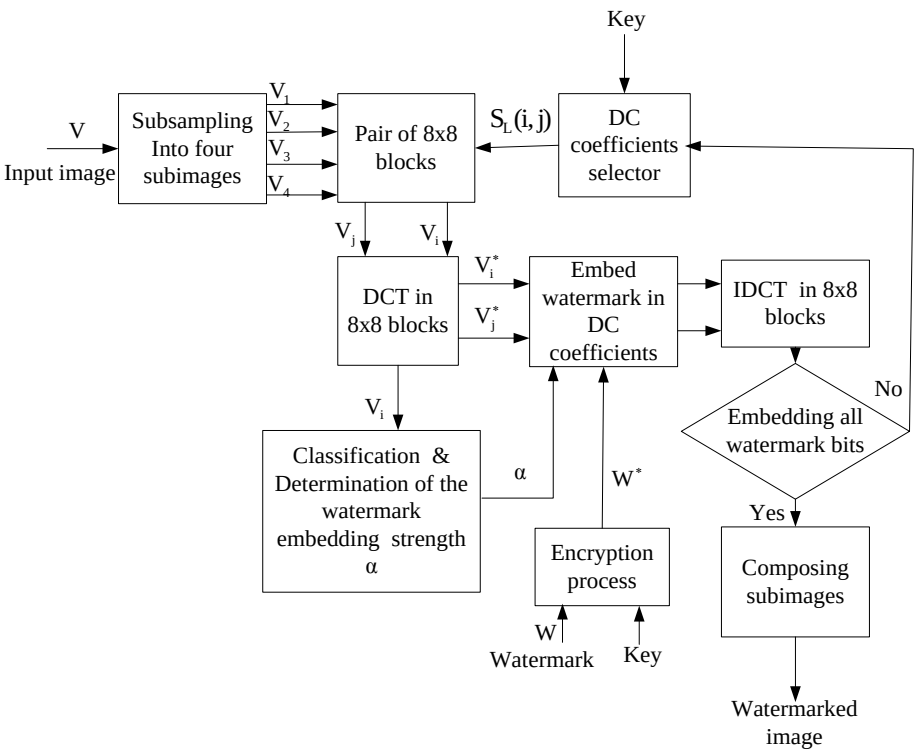


Figure 5.2 The proposed watermark embedding process.

5.3.1 Adaptive Determination of Watermarking Strength

There are two important issues when building a robust watermarking scheme: the structure of the watermark and the watermarking strategy [45]. In the proposed scheme, a binary logo image is used as a watermark *W*, which is represented by

$$\mathbf{W(i,\ j), 0 \leq i,\ j < M, W(i,\ j) \in (1,0)} \tag{5-5}$$

where (i, j) represent the pixel coordinates of the watermarked image and M denotes the size of the watermark. The watermark is encrypted to produce a pseudo random sequence, which is uncorrelated with the original watermark. The watermark encryption process can be given by

$$\mathbf{W^{*} = W \oplus C} \tag{5-6}$$

where W^{*} denotes the encrypted watermark, C is a chaotic binary sequence, which is generated randomly by a secret key and $\oplus$ denotes the XOR operation. An example watermark and its encrypted form are shown in Figure 5.3.

As mentioned earlier, a major challenge in designing a watermarking algorithm is to find a strategy that satisfies the conflicting objectives that, on one hand, the added watermark is imperceptible to the human eyes but, on the other, it should be robust to removal attacks. To achieve better trade-offs between requirements for imperceptibility and robustness, the characteristics of the non-watermarked image should be taken into account when embedding the watermark.

(a) (b)

Figure 5.3 (a) Original watermark, (b) Encrpted watermark

Given a block of 8×8 pixels, its texture can be classified as a certain type of edge pattern by dividing the block into four regions, as shown in Figure 5.4, and comparing their measure values as illustrated in

Table 5.1. While S_{ij} , $\mathrm{i, j} \in [0,3]$ given in Figure 5.4 represents the average pixel of the corresponding region, the measure values listed in

Table 5.1 indicate the strength of an edge pattern. For example, when $\delta_{\pi/2}$ is sufficiently large, the block can be classified as a vertical edge pattern. Chang et al [129] proposed a technique for extracting 5 edge patterns directly in the DCT domain, and proved that all the measure values given in

Table 5.1 can be directly obtained from the DCT coefficients X(0,1), X(1,0) and X(1,1). Jiang et al. [130] suggested that three edge patterns rather than five are sufficient to describe and characterize the visual content of the image in DCT domain. Therefore, the proposed method exploits this block classification scheme to analyze the visual content and hence determine the watermark embedding strength. The block classification is expressed as follows

$$\text{Block\_edge\_pattern} = \begin{cases} \text{no\_edge} & \text{if } \max(\delta_0, \delta_{\pi/2}) < \lambda \\ \text{vertical\_edge} & \text{if } (\delta_{\pi/2} \geq \delta_0) \\ \text{horizontal\_edge} & \text{otherwise} \end{cases} \tag{5-7}$$

where $\delta_0 = |X(1,0)|$ and $\delta_{\pi/2} = |X(0,1)|$ are the absolute values of the DCT coefficients X(1,0) and X(0,1), respectively, and λ is a pre-determined threshold.

S_{00}	S_{01}
S_{10}	S_{11}

Figure 5.4 Illustration of edge patterns in pixel domain.

Table 5.1 Measure of edges patterns in pixel domain

Edges	Measure values
No edge	δ_{NE} (set by user, where λ=50 in our design)
0	$\delta_0 = \left\| \frac{S_{00}+S_{01}}{2} - \frac{S_{10}+S_{11}}{2} \right\|$
$\pi/4$	$\delta_{\pi/4} = \max\left\{ \left\| S_{00} - \frac{S_{01}+S_{10}+S_{11}}{3} \right\|, \left\| S_{11} - \frac{S_{00}+S_{01}+S_{10}}{3} \right\| \right\}$
$\pi/2$	$\delta_{\pi/2} = \left\| \frac{S_{00}+S_{10}}{2} - \frac{S_{01}+S_{11}}{2} \right\|$
$3\pi/4$	$\delta_{3\pi/4} = \max\left\{ \left\| S_{01} - \frac{S_{00}+S_{10}+S_{11}}{3} \right\|, \left\| S_{10} - \frac{S_{00}+S_{01}+S_{11}}{3} \right\| \right\}$

Table 5.2 Measure of edges patterns in the DCT domain.

Edges	Measure values
No edge	δ_{NE} (set by user, λ=50 in our design)
0	$\delta_0 = \|x(1,0)\|$
π/4	$\delta_{\frac{\pi}{4}} = \frac{3}{4}\max\left\{ \left\| \frac{1}{2}(x(0,1)+x(1,0)+x(1,1) \right\|, \left\| \frac{1}{2}(x(0,1)+x(1,0)-x(1,1) \right\| \right\}$
π/2	$\delta_{\frac{\pi}{2}} = \|x(0,1)\|$
3π/4	$\delta_{\frac{3\pi}{4}} = \frac{3}{4}\max\left\{ \left\| \frac{1}{2}(x(0,1)-x(1,0)+x(1,1) \right\|, \left\| \frac{1}{2}(x(0,1)-x(1,0)-x(1,1) \right\| \right\}$

Via exploitation of the above classification scheme, all DCT blocks are further analyzed as smooth or non-smooth based on the specific values of the two DCT coefficients. Non-smooth blocks are then further classified to determine if they contain both vertical and horizontal edges or contain one of the edge patterns. The measurement of edge patterns is summarized in Table 5.2.

Table 5.2 The DCT blocks are classified as follows:

$$\gamma_i = \begin{cases} \text{smooth} & \text{if } \max(\delta_0, \delta_{\pi/2}) < \lambda_1 \\ \text{texture\_block} & \text{else if } \min(\delta_0, \delta_{\pi/2}) \geq \lambda_2 \\ \text{edge\_block} & \text{otherwise} \end{cases} \tag{5-8}$$

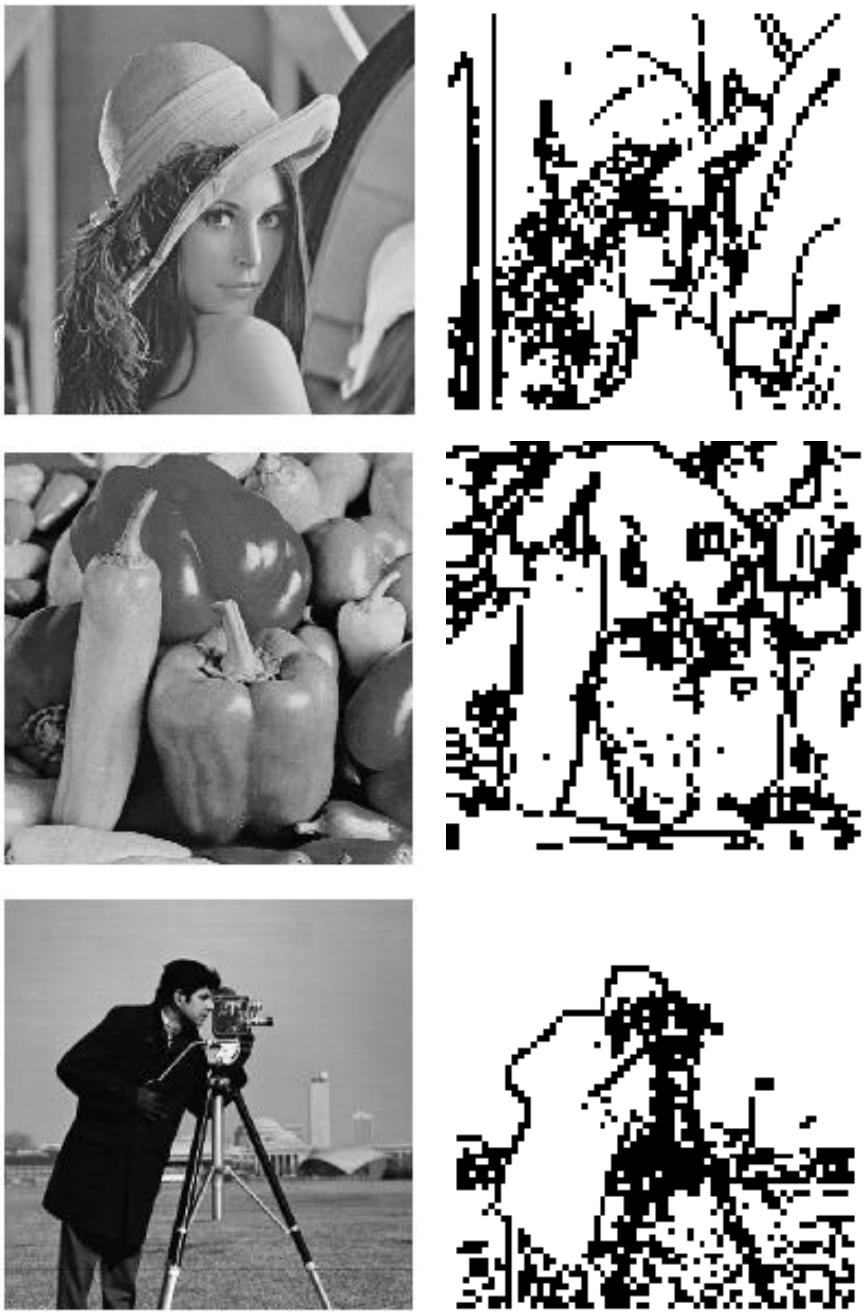
where γ_i stands for the classified blocks and $i \in [\text{smooth}, \text{texture}, \text{edge}]$, λ_1 and λ_2 are thresholds. As seen from Table 5.2, the determination of δ_0 and $\delta_{\pi/2}$ do not require any additions or multiplications and only two DCT coefficients are used to classify DCT blocks. Therefore, significant savings on computing cost can be achieved. Consequently, to determine the embedding strength, the following adaptive scheme is proposed

$$\alpha = \begin{cases} \alpha_{\text{smooth}} & \text{if } \max(\delta_0, \delta_{\pi/2}) < \lambda_1 \\ \alpha_{\text{texture}} & \text{else if } \min(\delta_0, \delta_{\pi/2}) \geq \lambda_2 \\ \alpha_{\text{edge}} & \text{otherwise} \end{cases} \tag{5-9}$$

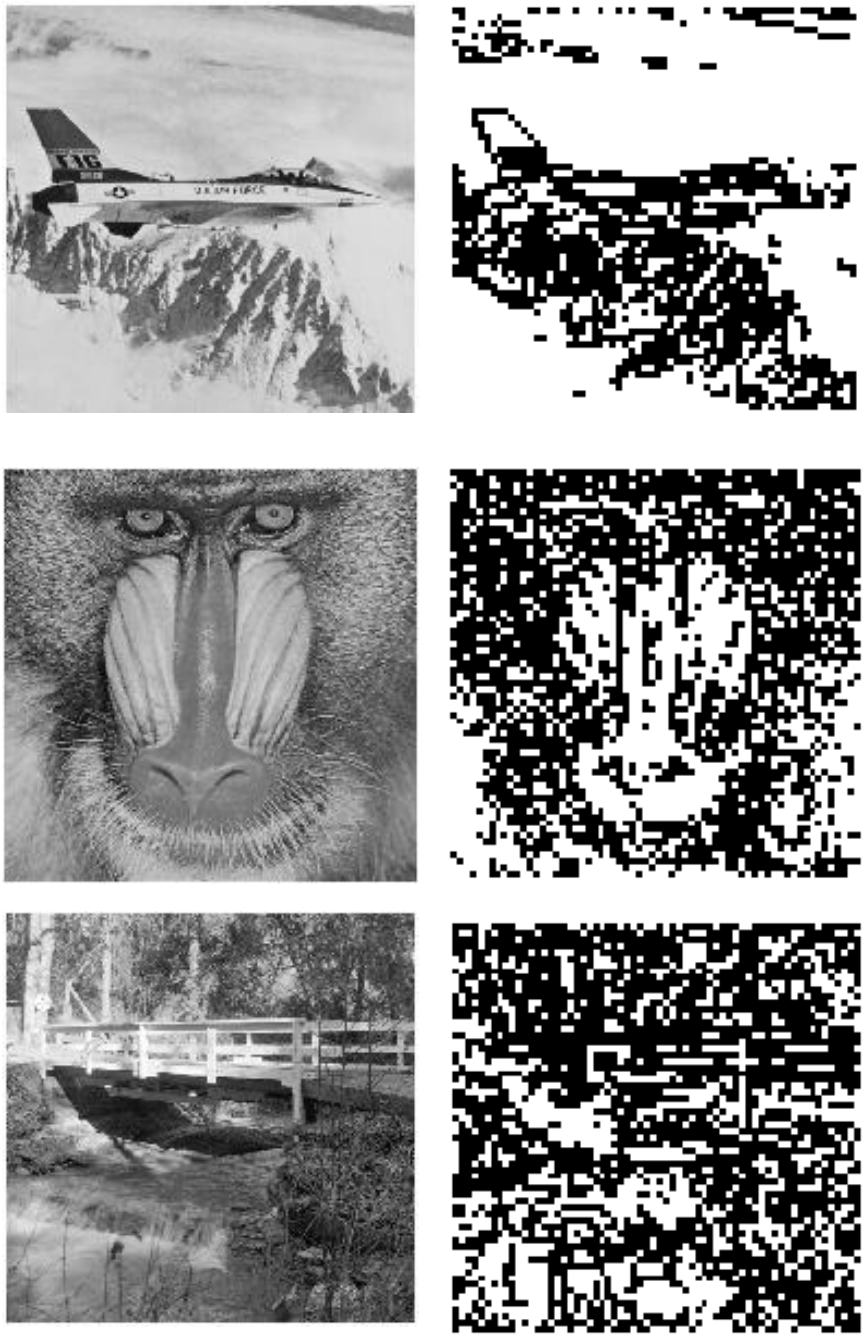
The proposed classification method enables a DCT block to be classified as a smooth, texture or edge block directly in the DCT domain using only two AC coefficients. Figure 5.5 demonstrates the classification results obtained by applying the proposed method to images with different textures including: 'Lena', 'Peppers', 'Cameraman', 'F16-plane', 'Baboon', and 'Walk-bridge'. For example, 'Lena' includes large smooth areas with sharp edges; 'Peppers' includes large smooth areas without sharp edges; 'Baboon' and 'Walk-bridge' include textured areas. The white areas shown in Figure 5.5

are classified as smooth, and thus any small change incurred by watermarking could be visible. As a result, the corresponding watermark should have a low embedding strength. Similarly, the black areas in Figure 5.5 are classified as edge or textured blocks, and hence changes incurred by watermarking would be less visible. Due to the fact that the human eye is less sensitive to noise and changes in the texture regions; the watermark strength in textured area should be higher than smooth and edges areas to ensure imperceptibility and robustness of the embedded watermarks. Therefore, the watermark embedding strength in texture area should be higher than smooth and edges area as described as follows

$$\alpha_{\text{smooth}} < \alpha_{\text{edge}} < \alpha_{\text{texture}} . \tag{5-10}$$



(a) (b)



(a) (b)

Figure 5.5 (a) Host images, (b) Classified images.

5.3.2 Adaptive Embedding of Watermarks

Let V denote the host grey scale image to be watermarked using a binary watermark W. The host image of size M×N is subsampled into four sub-images as described in Section 5.2.2**.** The watermark embedding proceeds as follows:

(i) Four sub-images V_1, V_2, V_3, V_4 are obtained by sub-sampling the host image as defined in equation (5-1) . Each sub-image has size of $[M/2]\times[N/2]$;

(ii) The original watermark is encrypted as explained in Section 5.3.1 and converted into a vector $W^{*'}$;

(iii) A secret key is used to generate a random sequence $S_L = \{(i, j), i, j \in (1,2,3,4), i \neq j\}$, with the length equal to length of the watermark, which serves as a DC coefficient selector. *L*=1, 2, …, is the length of the watermark;

(iv) Two sub-images are selected according to random sequence S_L and the DCT is applied to non-overlapping blocks of size 8×8 of the selected sub-images;

(v) The DC coefficients of the pair of selected blocks of size 8×8 $\{(DC_i, DC_j), (i, j \in S_L)\}$ are used to embed a watermark bit leaving the AC coefficients unchanged. Two DC coefficients are used to embed a watermark bit in order to extract the embedded bit without use of the original image by comparing the value of these coefficients;

(vi) Determine the watermark embedding strength α according to the block pattern classification given in equation (5-9).

The procedure to embed the watermark bits in the DC coefficients of blocks with 8×8 pixels for the selected sub-images can be described as follows: If $W_L^{*'} = 0$ and $DC_i > DC_j$, then swapping i, j in S_L, and if $W_L^{*'} = 1$ and $DC_i < DC_j$, then swapping i, j in S_L. The swapping of the random selector is implemented to minimize the distortion of the watermarked image when the difference between the selected DC coefficients is too large and they do not satisfy the embedding conditions for watermark bits. Using the modified S_L, the watermark embedding algorithm is defined as follows

$$DC_{Avg} = \frac{DC_i + DC_j}{2} \tag{5-11}$$

$$DC_{Diff} = \frac{|DC_i - DC_j|}{2} \tag{5-12}$$

$$DC_{Ratio} = \frac{DC_{Diff}}{DC_{Avg}} \tag{5-13}$$

$$DC_i^* = \begin{cases} DC_i & \text{if } (DC_{Ratio} > \beta) \\ DC_i + \alpha.DC_{Avg} & \text{else if } (DC_{Ratio} \le \beta) \ \& \ (W_L^* = 1) \\ DC_i - \alpha.DC_{Avg} & \text{otherwise} \end{cases} \tag{5-14}$$

$$DC_j^* = \begin{cases} DC_j & \text{if } (DC_{Ratio} > \beta) \\ DC_j + \alpha.DC_{Avg} & \text{else if } (DC_{Ratio} \le \beta) \ \& \ (W_L^* = 0) \\ DC_j - \alpha.DC_{Avg} & \text{otherwise} \end{cases} \tag{5-15}$$

where α is the watermark embedding strength (refer to equation 5-9) and β is the threshold, DC_i and DC_j are the DC coefficients of the blocks inside the two selected sub-images, DC_i^* and DC_j^* are the watermarked DC coefficients. *L*=1, 2,…, is the length of the watermark. The values of the selected pairs of DC coefficients (DC_i, DC_j) are altered if they do not satisfy the embedding threshold β. The embedding procedure is dependent on the watermark bits as given in equations (5-14) and (5-15). In the case of embedding a watermark bit '1', the value of the DC_i will be increased and the value of the DC_j will be decreased. In the case of embedding a watermark bit '0', the value of the DC_i will be decreased and the value of the DC_j will be increased. The values of the increment and decrement are determined by the watermark embedding strength α in order to make the proposed method more robust.

5.3.3 Proposed Watermark Extraction process

While existing work [68-71] requires the original image (non-watermarked) for watermark extraction, the proposed algorithm extracts the watermark without use of the

un-watermarked image. Figure 5.6 shows a block diagram of the proposed watermark extraction process, Hence, the proposed method is able to meet the blindness requirement. Suppose V^* is an image subject to watermark extraction, the process can be summarized as follows:

(i) The input image V^* is subsampled into four sub-images as explained in the watermark embedding process;

(ii) The watermark embedding locations are determined by using the DC random coefficients selector S_L that was used in the embedding process;

(iii) The DCT is applied to 8×8 blocks of selected sub-images;

(iv) The extracted watermark bits are determined by comparing the DC values of selected sub-images as given below

$$W_L^* = \begin{cases} 1 & \text{if } DC_i^* \geq DC_j^* \\ 0 & \text{otherwise} \end{cases} \tag{5-16}$$

where W_L^* is the extracted bit, $L \in \{1,2,....,N\}$, N represents the length of the watermark, DC_i^* and DC_j^* are DC coefficient values of 8×8 blocks of the selected sub-images. After extraction of all the watermark bits, these are put into a matrix and the inverse encryption process using the original secret key is applied to produce an extracted binary watermark image. Normalized Cross Correlation (NCC) given below is used to measure the similarity between the original watermark and the extracted watermark

$$NCC = \frac{\sum_i \sum_j W(i,j).W^*(i,j)}{\sum_i \sum_j (W(i,j))^2} \tag{5-17}$$

where $W(i,j)$ and $W^*(i,j)$ represent the pixel values at the location (i, j) of the original and the extracted watermark, respectively. An appropriate threshold T is used to make

the binary decision as to whether a given watermark is present or not. Figure 5.7 shows the watermark detector response with 1000 watermark seeds, only one of which is the correct watermark. The threshold T was set as 0.6 and when the NCC value exceeded this, the existence of the watermark was declared.

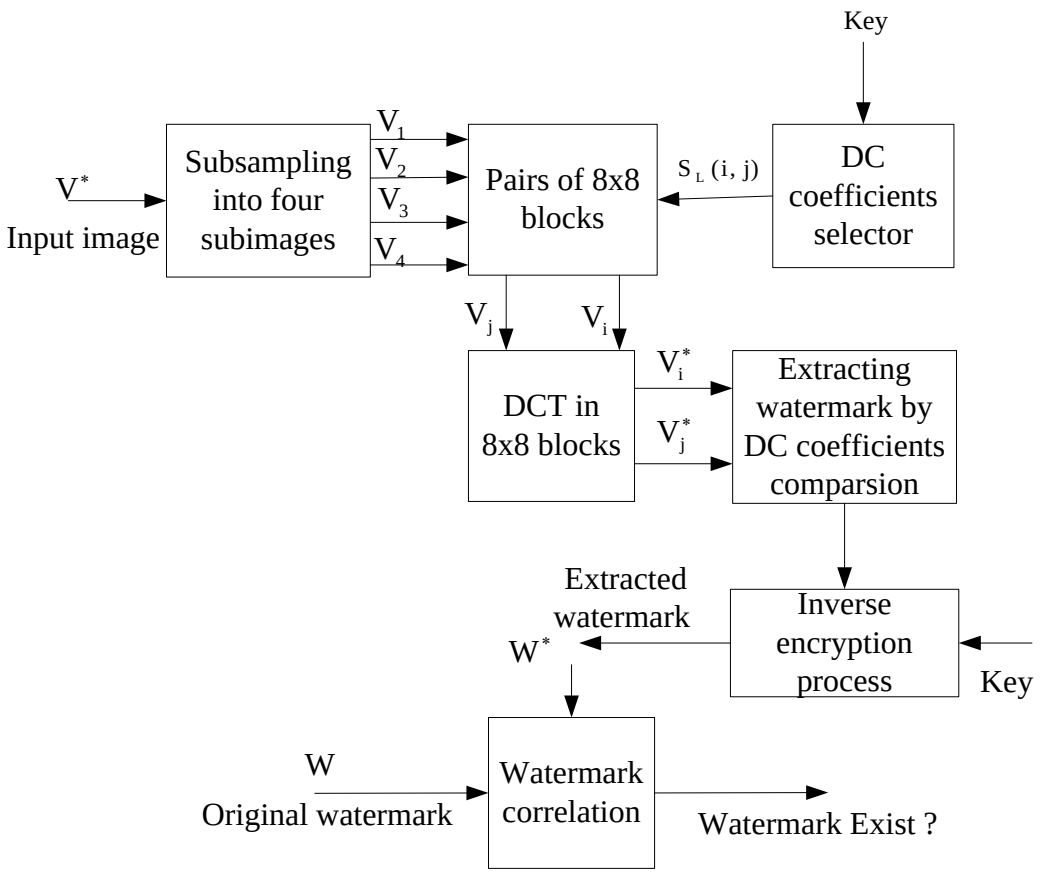


Figure 5.6 The proposed watermark extraxtion process.

To achieve the security requirement of the proposed method, the embedding positions of the watermark are determined by the random sequences generated a secret key. Therefore, it is impractical for an attacker to extract the watermark without knowing the sequences. To achieve the robustness requirement, DC coefficients are selected to embed the watermark because they can provide much greater perceptual capacity than the AC coefficients and they are less affected than any AC coefficient when the

watermarked image is attacked by JPEG compression, low-pass filtering or sub-sampling operations [68]. To achieve better trade-offs between the imperceptibility and robustness requirements, the watermark embedding strength is determined adaptively to the image features.

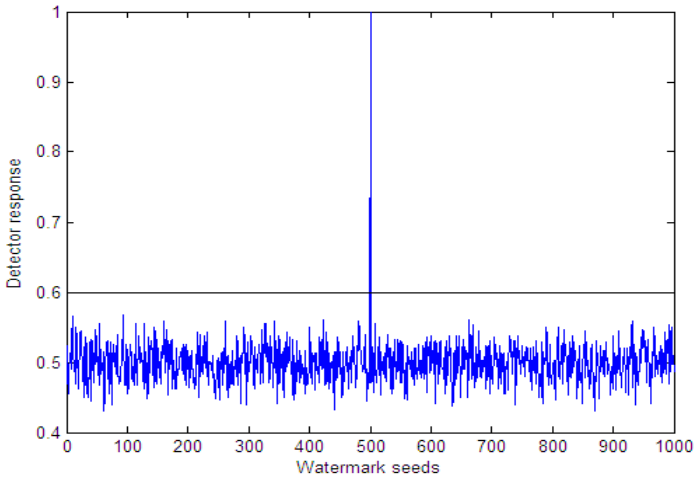


Figure 5.7 Detector responses for 1000 watermark seeds.

5.4 Experimental Results and Discussion

To evaluate the performance of the proposed algorithm, extensive experiments were carried out on a test database of 100 standard 8-bit greyscale images with 512×512 pixels. All these test images are publicly available and commonly used for this purpose. The experiments were organized in two phases. The first phase evaluated the watermark imperceptibility and the second phase evaluated the robustness of the watermark against various attacks including signal processing and geometric attacks. Moreover, the method described in [90] was implemented and used as a benchmark in order to evaluate the proposed method and compare the performance difference between embedding the watermark into DC coefficients and AC coefficients of the DCT under the same environment . It was chosen to evaluate the proposed scheme due to its similarity to the proposed technique in terms of using a sub-sampling process and

embedding a binary logo image as a watermark in the DCT domain, using blind detection for the watermark extraction process and its robustness against signal processing attacks. The method reported in [90] applies the DCT directly to the full-frame of the four sub-images obtained by using sub-sampling and embeds the watermark in selected AC coefficients without taken into account the features of the image. By contrast, the proposed algorithm applies the DCT only to the selected 8×8 blocks of two sub-images based on sub-sampling and uses the DC coefficients of those selected blocks to embed the watermark adaptively to the features of the image aiming to maximize both the robustness and imperceptibility of the embedded watermark. Regarding the applied DCT and its inverse, the total computing cost is $\left\lceil \frac{M/2}{8} \right\rceil \times \left\lceil \frac{N/2}{8} \right\rceil \times 4 \times 2$ for the benchmark, and $\left\lceil \frac{M/2}{8} \right\rceil \times \left\lceil \frac{N/2}{8} \right\rceil \times 2 \times 2$ for the proposed algorithm. Thus the proposed algorithm features low computing cost and high processing speed with 50% improvement over the representative existing algorithm.

5.4.1 The Impact of the Watermark Strength

In the embedding process, the distortion of an image depends on the threshold β, the watermark strength α, and the length of the watermark. The threshold β controls the difference between the watermarked DC coefficients. The greater β, the more embedding distortion is introduced in the watermarked image as given in equations (5-14) and (5-15). Meanwhile, the embedding of the watermark is controlled by the watermark strength α. The classification of the image determines where the watermark should be strong and where the watermark should be weak. The watermark strength α is lower in smooth regions and higher in textured regions. This is because smooth regions have less ability to cover the watermark than textured regions. There is a relationship

between the value of the watermark strength, and the visibility and robustness of the watermark. The higher α, the more distortion is introduced in the watermarked image. Hence, there is trade-off between robustness and imperceptibility. Table 5.3 shows the results of varying the watermark strength α. As can be seen, increasing the value of the watermark strength α induces more distortion in the watermarked image. In the experiments, the logo used for watermarking was a binary image with a size of 32×32 and the values of the other parameters used in the experiments were: λ_1=50, λ_2=65, β=0.05, $\alpha_{smooth} = 0.01$, $\alpha_{texture} = 0.04$, $\alpha_{edge} = 0.025$. These were empirically determined values, and found to be appropriate for the tested images. The values of β was determined as suggested in [90] and value of λ_1 was determined as suggested in [130].

Table 5.3 Results of varying the watermark strenght α.

No.	Watermark strength α			PSNR (dB)		
	α_{smooth}	α_{edge}	$\alpha_{texture}$	Lena	Peppers	Baboon
1	0.001	0.002	0.003	71.2441	71.0322	81.2441
2	0.005	0.007	0.01	53.693	54.1093	53.1358
3	0.007	0.01	0.02	49.7859	49.3479	48.2501
4	0.009	0.02	0.03	49.3031	48.8512	47.9879
5	**0.01**	**0.025**	**0.04**	**43.7894**	**44.8129**	**45.6381**
6	0.03	0.04	0.06	39.2229	38.2779	39.1369
7	0.07	0.09	0.1	33.5857	33.756	33.1069
8	0.1	0.15	0.2	31.2216	31.5904	30.8958
9	0.2	0.25	0.3	30.2677	30.5846	30.1356

5.4.2 Watermark Imperceptibility

To evaluate the watermark imperceptibility, 100 different images were tested including 'Lena', 'Peppers', 'Walk-bridge', 'Baboon', 'F16-plane' and 'Cameraman', etc. [41]. These images include high, medium and low texture categories. The Peak Signal to Noise Ratio (PSNR) was adopted to evaluate the perceptual distortion of the proposed scheme. As shown in Figure 5.8, the PSNR values of the 100 watermarked images are between 42 and 54. These values are all greater than 30.00 db, which is the empirically tested threshold value for an image to no perceivable degradation [113]. Since the watermark is embedded adaptively, the value of the PSNR depends on the characteristics of the host image. For instance, an image with large low-textured areas will have a bigger PSNR value than an image with large textured areas. Taking 'Peppers' and 'Walk-bridge' as examples, the un-watermarked and the watermarked images are shown in Figure 5.9. The PSNR values between the original and watermarked images are 44.81 for 'Peppers', 44.22 for 'Walk-bridge', 49.74 for 'Birds' and 45.56 for 'Butterfly'. It can be seen that the differences between the corresponding watermarked and un-watermarked images are imperceptible and the embedded watermarks are invisible to the human eye.

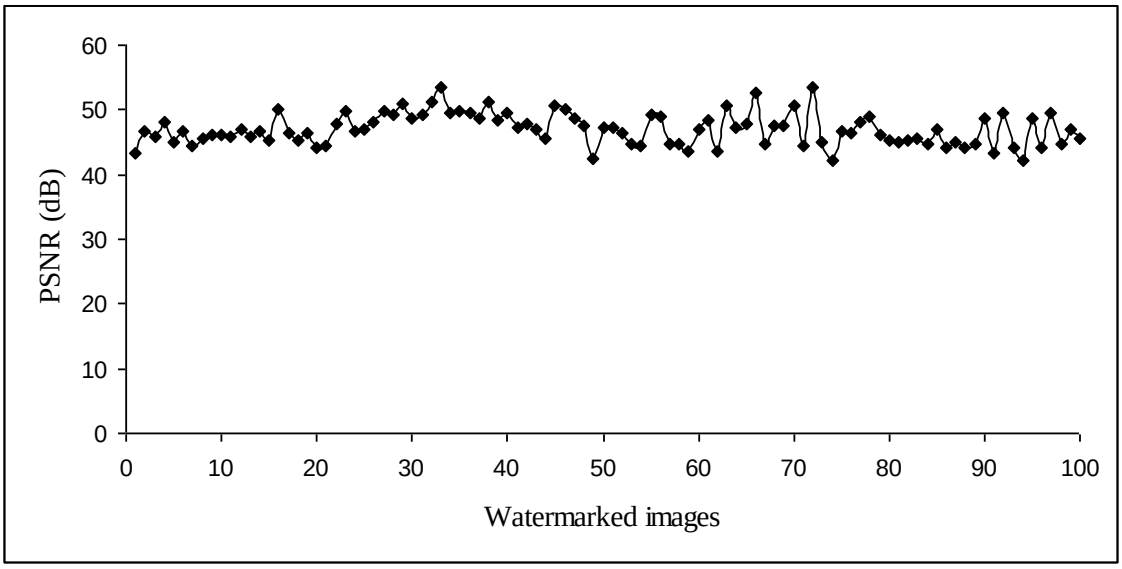
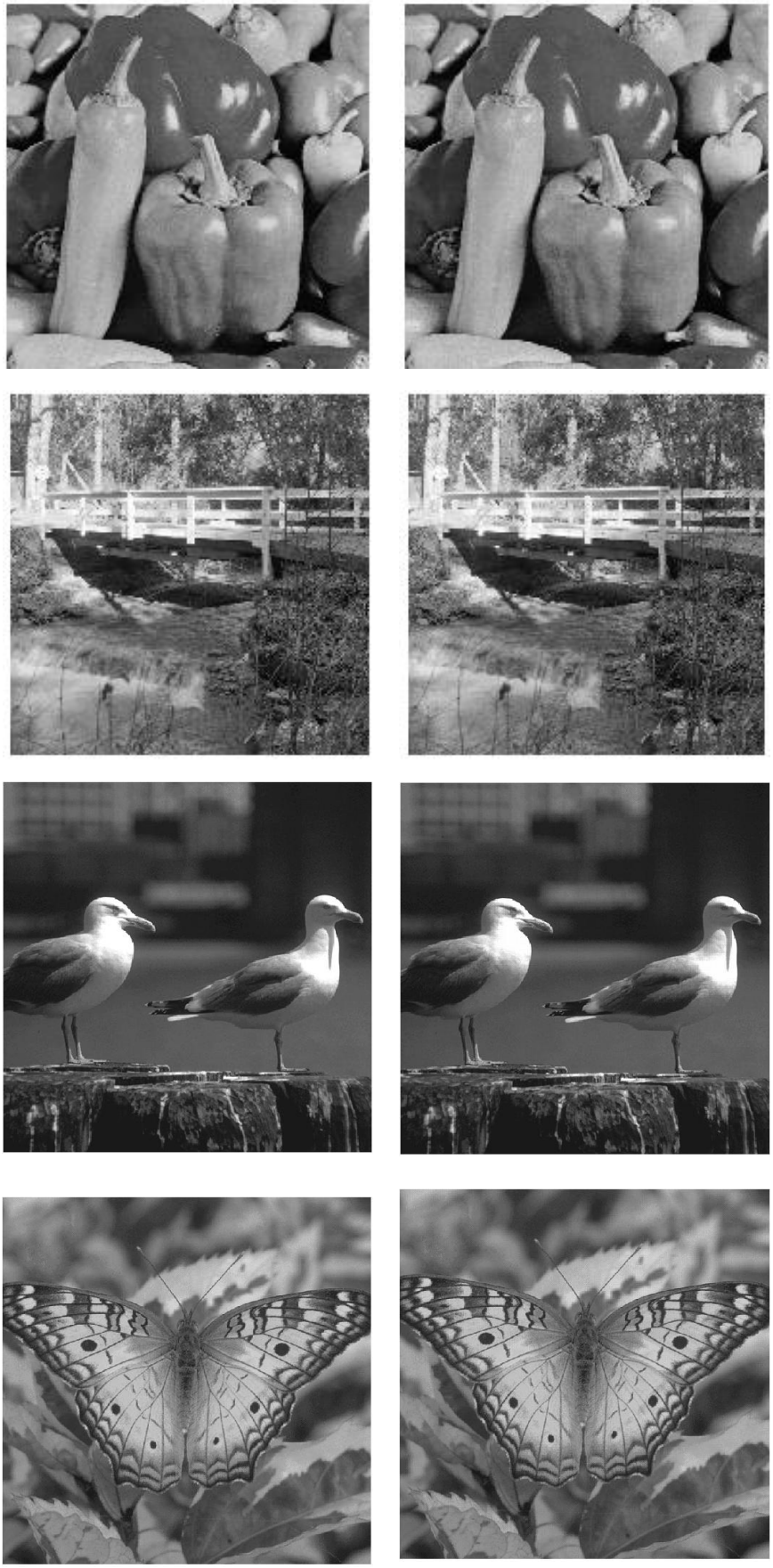


Figure 5.8 Watermark distortions (in PSNR).



(a) (b)

Figure 5.9 (a) Original images, (b) Watermarked images.

The structural similarity index (SSIM) was also adopted for assessing the similarity between the original image and the watermarked one. Figure 5.10 shows the SSIM values for 100 images watermarked using the proposed method and Lu's method [90]. As shown, the proposed method achieves better similarity between the original and watermarked images. This is because the watermark strength depends on the host image feature in the proposed method, while the watermark strength is kept constant for all images in Lu's method. For example, 'Cameraman' and 'Woman' images, which are represented by numbers 4 and 19 in Figure 5.10, respectively, have large low-textured areas; therefore, these low-textured areas have lower watermark strength than high-textured areas using the proposed method. However, in Lu's method the watermark strength has the same value for both low and high-textured areas of these images. As a result, the embedded watermark may be visible in low-textured areas and affect the quality of the watermarked images. For a high-textured image, as example, images, which are represented by numbers 2, 3,10,11,53 and 96 in Figure 5.10, respectively, the Lu's method achieves better similarity between the original and watermarked images. This is because the watermark strength in the proposed method is higher than in low-textured areas. However, high-textured areas of the host images are less sensitive to change than the low-textured areas and the changes in the high texture areas are unnoticeable to the human eyes [125]; this makes sense to use higher watermark strength in textured area aiming to ensure the imperceptibility and maximize the robustness of the embedded watermark.

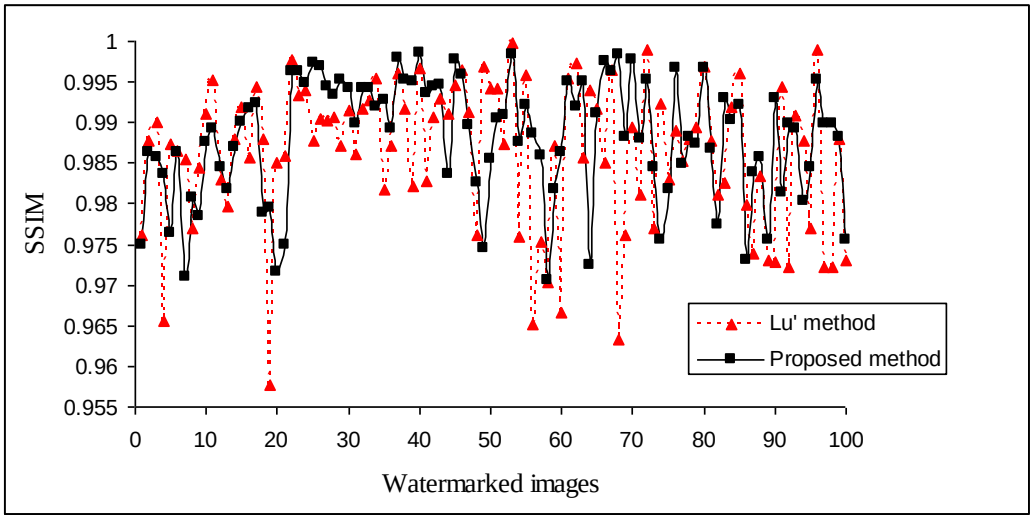


Figure 5.10 SSIM similarity measurement between original and watermarked images.

5.4.3 Watermark Robustness

To complete the second experimental phase, various common signal processing and geometric attacks were applied to the watermarked images. Most of these were performed using the benchmark software StirMark 4.0 [6, 19]. These attacks included: JPEG-lossy compression, median filtering, Gaussian filtering, low-pass filtering, mean filtering, addition of salt and pepper noise, addition of Gaussian noise, rescaling, cropping, rotation-scaling, rotation-cropping and removal of some rows and columns. Figure 5.11 shows some experimental results from JPEG attacks on the images 'Lena' and 'Peppers', watermarked using the proposed method and Lu's method in [90]. As shown, the proposed method performs better than Lu's method under JPEG compression attack and the watermark detector can even extract the correct watermark after JPEG compression with a quality factor of 10%.

Figure 5.12 shows the robustness to median and low pass filtering, from which it can be seen that the proposed method is more robust to these attacks with different filter sizes, in comparison with the benchmark [90].

The proposed method was also tested against additional noise attacks. In these experiments, Gaussian noise and salt and pepper noise were added to the watermarked images. For example, the results for the images 'Baboon' and 'Peppers' are shown in Figure 5.13. As can be seen, the proposed method performs better than the benchmark under both types of added noise.

Figure 5.14 shows the extracted watermarks from the watermarked images 'Lena', 'Peppers', and 'Baboon' following the image processing attacks, which include: JPEG compression with quality factors of 10%, 30%, 50%; 3×3 and 5×5 median filtering; 3×3 low-pass filtering; 3×3 Gaussian low-pass filtering; 3×3 mean filtering; 1% added Gaussian noise; 1% added salt and pepper noise; 1% salt and pepper noise and 3×3 median filtering; 5% Gaussian noise and 3×3 Gaussian filter. All the extracted watermarks can be visually identified and the detector's response correctly declares the existence of the watermark. The results illustrate the robustness of the proposed algorithm against a range of attacks as illustrated in Figure 5.14.

The watermark can also be extracted and correctly identified by the proposed algorithm under a variety of geometric attacks including: scaling; cropping; removal of some rows and some columns; the combination of scaling with small angle rotation; the combination of cropping with small angle rotation. Before watermark extraction, the scaled and cropped watermarked images are rescaled back to their original sizes. Figure 5.15 shows the detector responses for scaling attacks with different scale factors. As seen, the proposed algorithm still outperforms the benchmark under all these scaling attacks, and the watermark can be detected even when the watermarked images 'Lena' and 'Pepper' are scaled down to 25% or scaled up to 200%. Some results of cropping attacks are shown in Figure 5.16, from which it is seen that the watermark can be detected even when the watermarked images are cropped by 25 % or 50%.

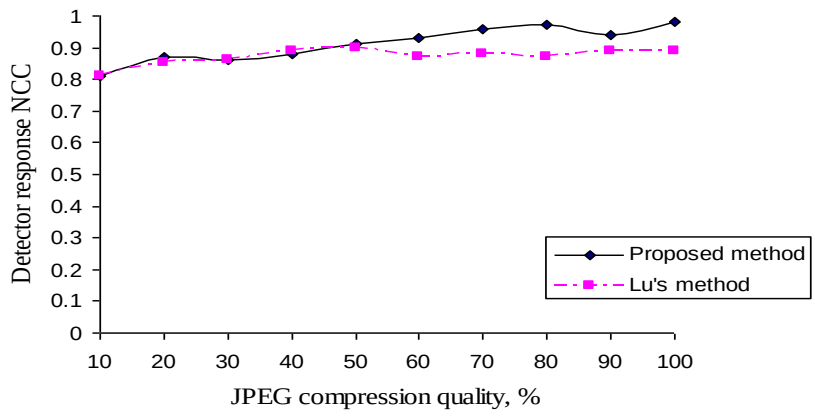
Table 5.4 summarizes the experimental results from applying several common image processing and geometric attacks on the images 'Lena', 'Peppers' and 'Baboon' watermarked using the proposed and Lu's methods. It can be seen that the proposed method performs better than Lu's under the common image processing attacks, median, low-pass, Gaussian filtering, JPEG compression, adding noise plus filtering and JPEG compression plus filtering. It also performs well under some geometric attacks including scaling, rows and columns removal attack, the combination of scaling with small angle rotation and the combination of cropping with small angle rotation.

A variety of attacks have also been performed on 100 different images watermarked using the proposed method and Lu's method. Table 5.5 summarizes the experimental results, by showing the lowest, the highest and the average NCC values of the extracted watermarks from the 100 watermarked images. As shown in Table 5.5, the proposed method achieves higher average NCC values than Lu's method. The improved performance of the proposed scheme compared to related work [90] is due to the following two factors:

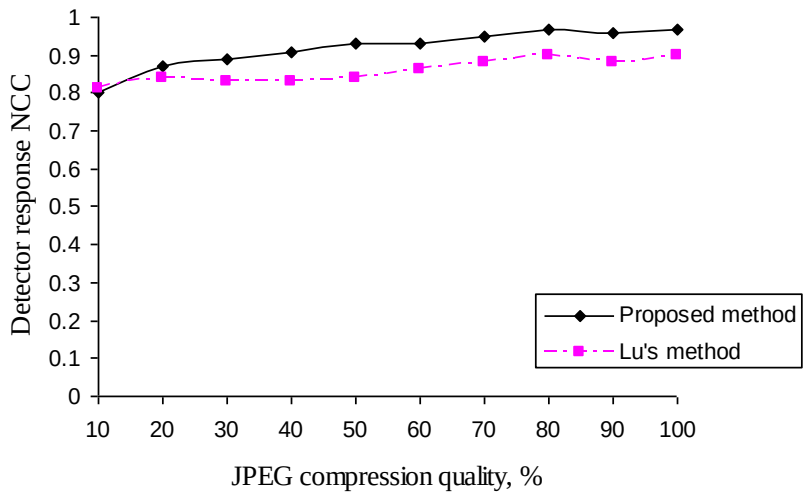
(i) Because the watermark is embedded adaptively to the host image features, the watermark embedding strength can be increased in high texture areas of the host images without inducing any perceivable degradation of the watermarked images. As a result, more robustness can be achieved. By contrast, in Lu's method, increasing the watermark strength will induce noticeable visual degradation in low-textured areas of the host images because features of host images are not taken into account in the embedding process.

(ii) More robustness is achieved because the watermark is embedded in the DC coefficients rather than AC coefficients of the DCT. This is because DC coefficients are less affected than the AC coefficients when the

watermarked image is subjected to signal processing attacks, such as JPEG compression and low pass filtering [68].

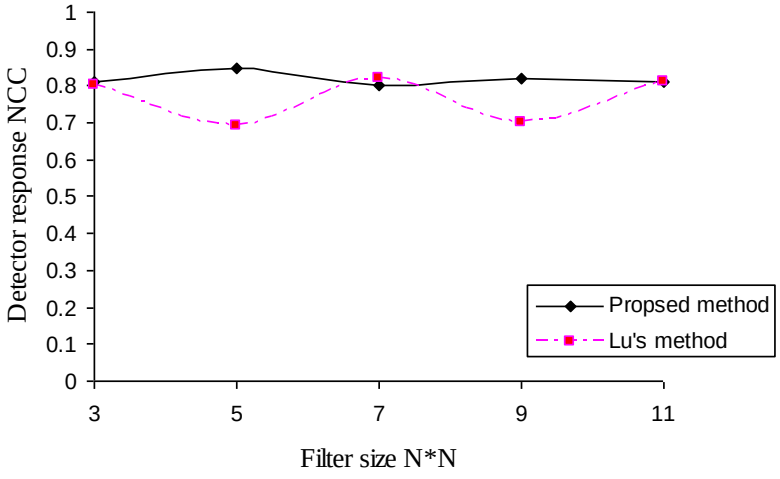


(a)

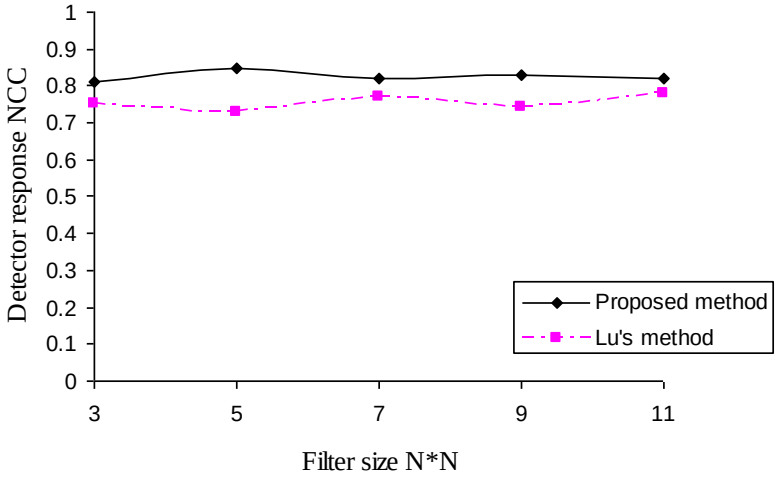


(b)

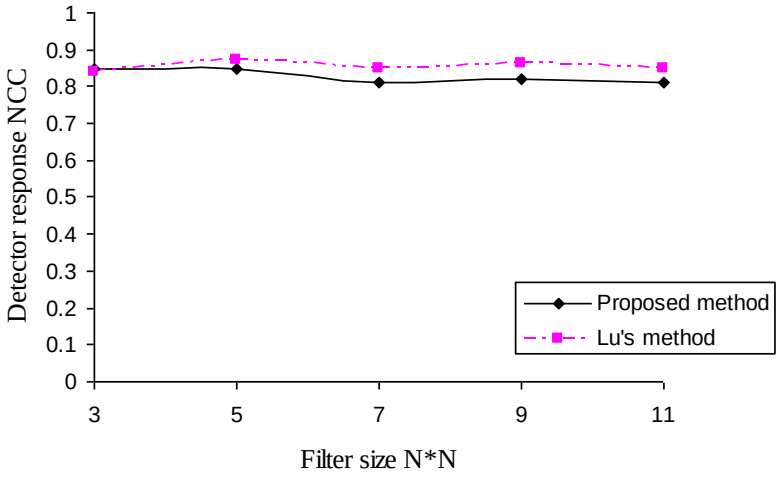
Figure 5.11 Results of attack by JPEG-loss compression with comparison between the proposed method and Lu's method, (a) and (b) Detector response NCC versus JPEG compression quality for images ' Lena' and Peppers', respectively.


Detector response NCC
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
3
5
7
9
11
Filter size N*N
Propsed method
Lu's method

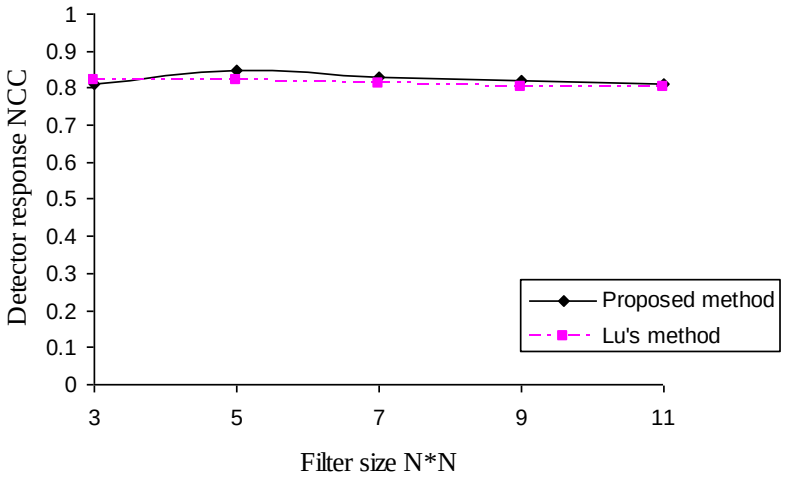
(a)


Detector response NCC
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
3
5
7
9
11
Filter size N*N
Proposed method
Lu's method

(b)

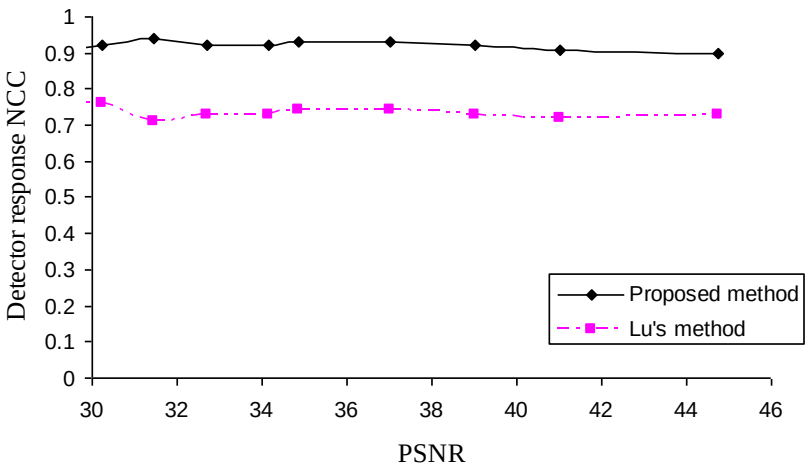

Detector response NCC
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
3
5
7
9
11
Filter size N*N
Proposed method
Lu's method

(c)

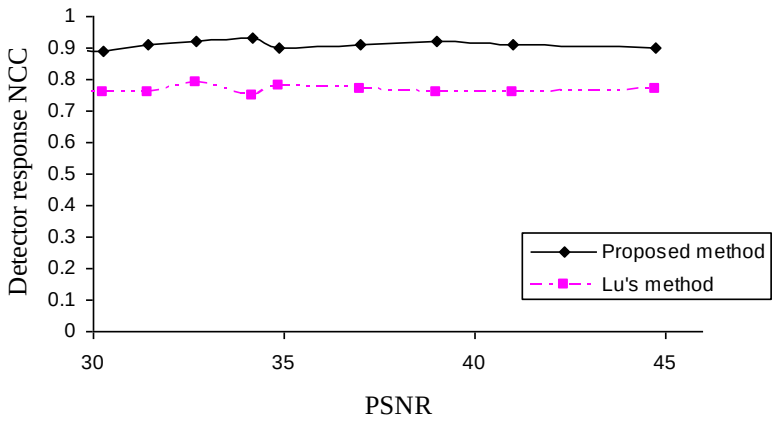


(d)

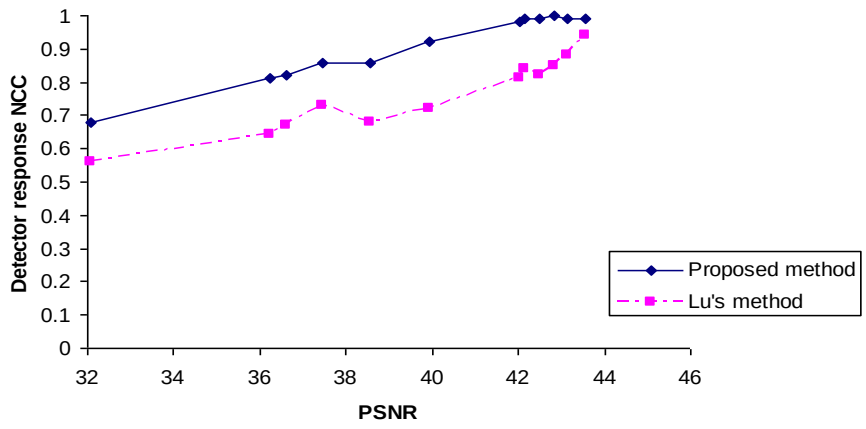
Figure 5.12 Results of attack by (a) Median filter to image 'Lena', (b) Median filtering to image 'Peppers', (c) Low pass filter to image 'Lena', (d) Low pass filtering to image 'Peppers' compared to Lu's method .



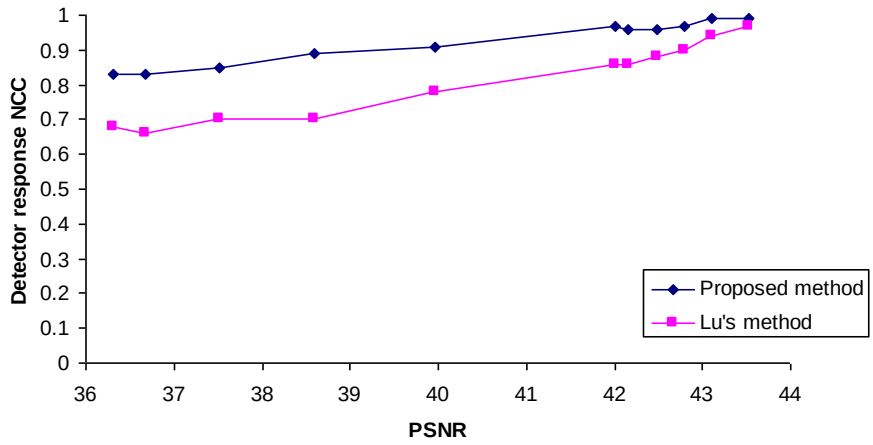
(a)



(b)



(c)



(d)

Figure 5.13 Results of attack by (a) Gaussian noise to image 'Peppers', (b)Gaussian noise to image 'Baboon', (c) Salt& pepper noise to image 'Peppers, (d) Salt& pepper noise to image 'Baboon' compared with Lu's method.

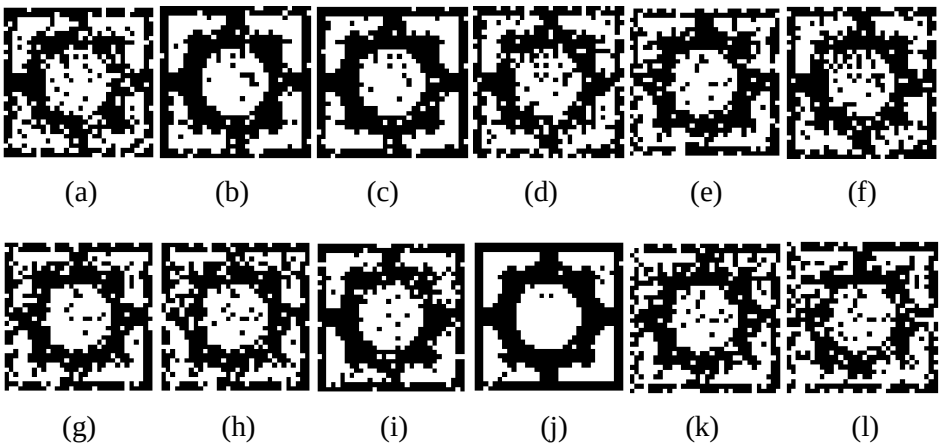
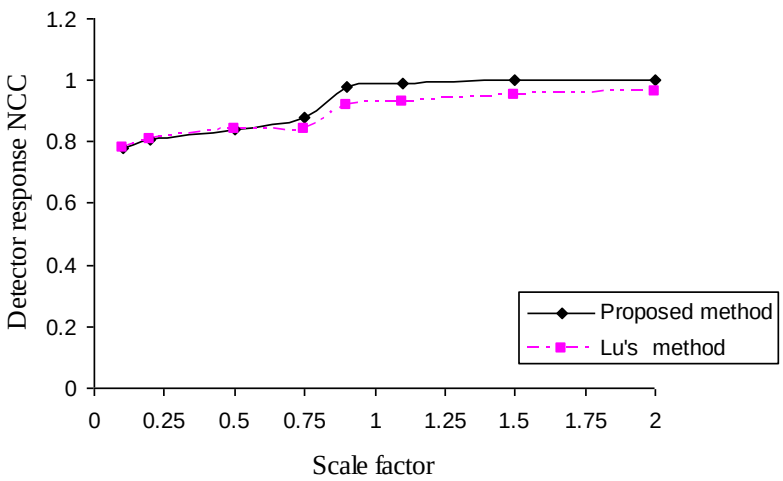
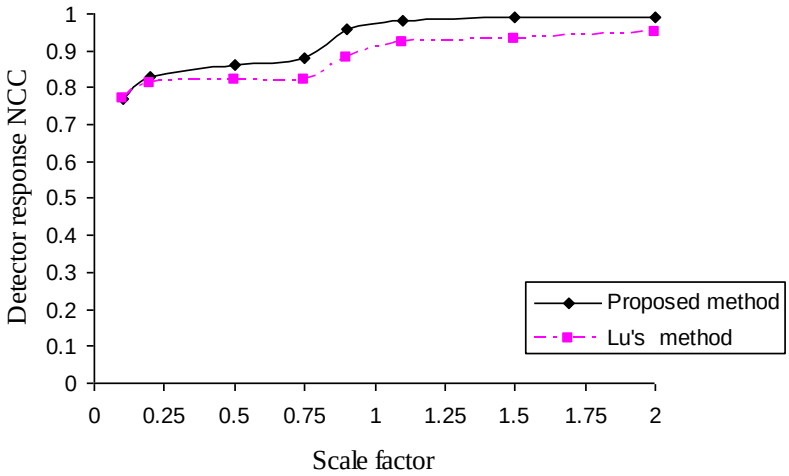


Figure 5.14 Extracted watermarks after (a), (b), (c) JPEG compression with quality factors 10, 30 50, respectively; (d) and (e) median filtering 3×3 and 5×5; (f) low pass filtering (3×3); (g) Gaussian low pass filtering (3×3); (h) mean filtering (3×3); (i) Gaussian noise 0.01; (j) salt & peppers noise 0.01;(k) salt & peppers noise 0.01+median filtering (3×3); (l) Gaussian noise 0.05+ Gaussian filter (3×3).



(a)



(b)

Figure 5.15 Results of scaling attack (a) image 'Peppers'; (b) image 'Baboon'.

(a) (b) (c) (d)

Figure 5.16 (a) Cropped image 'Baboon' by 25%; (b) extracted watermark with NCC=0.87; (c) cropped image 'Lena' by 50%; (d) extracted watermark with NCC= 0.74.

Table 5.4 Comparison between the proposed method and Lu's method under common image processing and geometric attacks.

Attack operation	Attack operation on images					
	Lu's method			Proposed method		
	Lena	Peppers	Baboon	Lena	Peppers	Baboon
	NCC	NCC	NCC	NCC	NCC	NCC
Jpeg 100	0.88	0.90	0.88	0.98	0.97	0.95
Jpeg 50	0.90	0.84	0.92	0.91	0.93	0.94
Jpeg 20	0.85	0.84	0.84	0.88	0.87	0.90
Scaling 2.0	0.95	0.94	0.98	1.0	0.99	1.0
Scaling 0.5	0.86	0.82	0.94	0.84	0.86	0.83
Scaling 0.25	0.88	0.81	0.94	0.81	0.83	0.79
Median filter 3×3	0.80	0.75	0.79	0.81	0.81	0.85
Median filtering 5×5	0.69	0.73	0.76	0.85	0.85	0.81
Mean filter 3	0.83	0.82	0.90	0.81	0.81	0.85
Low pass filter 3×3	0.84	0.82	0.91	0.85	0.81	0.82
Gaussian filter 3×3	0.85	0.82	0.91	0.86	0.86	0.88
Salt&pepper noise 0.07	0.82	0.87	0.81	0.99	0.97	0.84
Salt&pepper noise 0.1	0.64	0.67	0.61	0.81	0.83	0.79
Gaussian noise 0.001	0.77	0.74	0.67	0.92	0.88	0.87
Gaussian noise 0.1	0.73	0.78	0.68	0.93	0.90	0.88
Salt&pepper noise 0.07 +median filter 3×3	0.74	0.78	0.80	0.83	0.82	0.85
Gaussian noise 0.1 +Gaussian filter 5×5	0.73	0.77	0.79	0.83	0.84	0.84
Jpeg 40+ low pass filter	0.86	0.84	0.79	0.89	0.84	0.87
Jpeg 40+ median filter	0.79	0.84	0.77	0.81	0.85	0.87
Rotation-scaling 0.25	0.86	0.79	0.86	0.83	0.84	0.83
Rotation-scaling -0.25	0.81	0.80	0.87	0.83	0.84	0.82
Rotation-crop 0.25	0.87	0.82	0.87	0.84	0.86	0.83
Rotation-crop 0.75	0.79	0.76	0.78	0.77	0.77	0.75
Rotation-crop 1	0.80	0.72	0.76	0.76	0.76	0.69
Removal lines 10	0.91	0.84	0.92	0.93	0.98	0.98
Removal lines 50	0.89	0.84	0.93	0.90	0.94	0.94
Removal lines 100	0.87	0.82	0.92	0.93	0.96	0.97

Table 5.5 Comparison between the proposed method and Lu's method on 100 watermarked images.

Attacks	Lu's scheme [90]			Proposed scheme		
	NCC_{Low}	NCC_{Hig}	NCC_{Avg}	NCC_{Low}	NCC_{Hig}	NCC_{Avg}
JPEG 100	0.84	1.0	0.99	0.85	1.0	0.99
JPEG 80	0.80	0.88	0.91	0.83	0.99	0.95
JPEG 50	0.70	0.96	0.85	0.74	0.97	0.87
JPEG 30	0.64	0.94	0.82	0.67	0.95	0.87
JPEG 20	0.63	0.90	0.79	0.63	0.93	0.82
Scaling 0.5	0.59	0.98	0.78	0.60	0.92	0.78
Scaling 0.75	0.55	0.95	0.76	0.58	0.97	0.79
Scaling 2.0	0.79	0.99	0.91	0.79	1.0	0.96
Median 2×2	0.56	0.98	0.75	0.57	0.92	0.77
Median 5×5	0.69	0.94	0.83	0.67	0.95	0.83
Mean 2×2	0.58	0.89	0.74	0.59	0.94	0.78
Mean 5×5	0.73	0.96	0.85	0.70	0.94	0.85
Gaussian 3×3	0.90	0.99	0.96	0.81	0.99	0.96
Gaussian 5×5	0.91	0.99	0.96	0.82	0.99	0.95
Salt& Peppers noise 0.003	0.86	0.98	0.91	0.82	1.0	0.97
Salt& Peppers noise 0.007	0.64	0.96	0.86	0.83	0.99	0.94
Salt& Peppers noise 0.05	0.55	0.90	0.70	0.64	0.96	0.80
Salt& Peppers noise 0.1	0.50	0.85	0.65	0.58	0.89	0.73
Gaussian noise 0.001	0.60	0.89	0.75	0.67	0.97	0.84
Gaussian noise 0.005	0.55	0.94	0.75	0.68	0.96	0.84
Gaussian noise 0.1	0.60	0.96	0.76	0.72	0.97	0.84

5.5 Conclusions

This chapter presents a new embedding strategy for digital image watermarking. The proposed embedding algorithm can be divided into four stages, which include: (i) producing four sub-images by sub-sampling the host image with single pixel starting offsets; (ii) specifying the embedding positions of the watermark using a secret key; (iii) classifying DCT blocks as smooth, textured or edge blocks in order to embed the watermark adaptively according to the feature content of the host images; (iv) embedding the watermark in the perceptually least affected DC coefficients of the selected sub-images. In addition, the watermark extraction process is performed without using the un-watermarked image, which makes the proposed method applicable in a wider range of applications than those which require the un-watermarked image for detection. The main motivation is the development of a watermarking method, which can satisfies the conflicting objectives of achieving image content changes that are imperceptible to the human eyes whilst being extremely robust against unauthorized detection and intentional or unintentional removal attempts. The proposed method achieves this goal by embedding a watermark adaptively into DC coefficients of the DCT.

The experimental results show that the proposed scheme succeeds in making the watermark perceptually invisible and also robust against various signal processing operation and geometric attacks including JPEG compression, filtering, scaling, cropping, additive Gaussian noise, additive salt and pepper noise, combination of small rotation and cropping, combination of small rotation and scaling, cropping and rows and columns removal attacks. In addition, the embedded watermark can not be extracted without knowing the secret key that was used in the embedding process.

CHAPTER SIX

6 ROBUST IMAGE WATERMARKING VIA GEOMETRICALLY INVARIANT FEATURE POINTS AND IMAGE NORMALIZATION

6.1 Introduction

The robustness of watermarks to geometric attacks is considered to be an issue of great importance. Indeed, it constitutes one of the most challenging design requirements for watermarks. Geometric attacks can desynchronize the location of the watermark and hence causes incorrect watermark detection. Most countermeasures proposed in the literature focus on the problem of the global affine transform, which includes rotation, scaling and translation (RST). However, there is a challenge in designing a blind watermarking algorithm that is robust against both local geometric distortions such as cropping and global affine transforms as well as common signal processing attacks.

This chapter describes a robust image watermarking scheme using visually significant feature points and image normalization. A feature extraction method based on end-stopped wavelets has been adopted to extract significant geometry preserving feature points, which are shown to be robust against various types of common signal processing and geometric attacks. These feature points can be used as synchronization marks between the watermark embedding and detection processes. The watermark is embedded into non-overlapping normalized circular images, which are determined by

feature points. Rotation invariance is achieved via image normalization. The watermark embedding process is performed by modifying low-frequency coefficients of DCT blocks, which are randomly selected using a secret key. The proposed scheme is blind as the original image is not required for watermark detection.

This chapter is organized as follows. A short description of the feature extraction method used in the proposed scheme is provided in Section 6.2. The image normalization process developed for pattern recognition is briefly reviewed in Section 6.3. The watermark embedding and extraction processes are described in Section 6.4. Experimental results with comparison between the performances of our proposed scheme and related schemes are provided in Section 6.5. Finally, Section 06.6 draws conclusions from the work presented in this chapter.

6.2 Feature Extraction

Geometric attacks can induce synchronization errors between the watermark embedding and detection processes. As a result, the watermark might not be found during detection. To reduce synchronization errors during the detection process, we look for reference points for synchronization that are perceptually significant and can thus resist various types of common signal processing and geometric attacks.

6.2.1 Feature Detector Based on End-Stopped Wavelets

Monga *et al* [131] proposed an iterative feature detector to extract significant geometry preserving feature points. The detector determines the feature points by computing a wavelet transform based on end-stopped wavelets obtained by applying the first-derivative of Gaussian (FDoG) operator to the Morlet wavelet. Monga *et al* [131] evaluated the performance of this detector against three commonly used detectors namely the Harris corner detector, the maximally stable extremal region (MSER) detector and the Hessian Affine detector and concluded that the feature detector based

on end-stopped wavelets is the most stable and robust of these. Therefore, this detector has been adopted to extract the feature points in the present scheme. The feature detection process can be divided into the following steps:

(i) For each image location, the wavelet transform is computed as given in reference [131].

(ii) The significant features points are identified by looking for local maxima of the magnitude of the wavelet coefficients in a pre-selected neighborhood.

(iii) A threshold is applied to eliminate spurious local maxima in featureless regions of the image.

To determine the regions for each feature point for embedding the watermark, a search is carried out within a circular neighboring region whose radius is set to be R. If the detector response at the centre of the region achieves local maximum, the feature point is selected. Otherwise, it is discarded. To obtain non-overlapping regions, the most stable feature points are first selected. Then, any feature points whose corresponding region overlaps with the selected feature points are excluded. Figure 6.1 shows the final selected feature points with the corresponding non-overlapping circular regions for images ‘Lena’, ‘Baboon’, ‘Peppers’ and ‘City’. The number of feature points depends on the image texture. The more textured the image, the more feature points will be extracted. To illustrate the performance of the feature extraction detector, Figure 6.2 shows an example of extracted feature points from ‘Baboon’ image, which has been distorted by several signal processing and geometric distortions including: JPEG compression attacks with quality factor of 30%; 3×3 median filtering; 3×3 low pass filtering; translation in both directions by 20 pixels; shearing –x-5%, y-0%; histogram equalization; rotation by 30º; and affine transform. The correctly extracted feature points are marked with white circles, while the incorrect feature points are marked with red circles. In practice, there are always more than enough of extracted feature points,

which can be used as synchronization marks between watermark embedding and detection. The performance of the feature detector based on end-stopped wavelets was evaluated against various common signal processing and geometric attacks on images 'Lena', 'Peppers', 'Baboon', 'Woman' and 'Elaine'. Tables 6.1 depict the results of applying attacks include JPEG-lossy compression, median filtering, Gaussian filtering, Wiener filtering, translation, cropping and rotation attacks. As shown in Table 6.1, the overall a majority of feature points can still be correctly detected even when the images is compressed by jpeg compression with quality factor of 20%. It is worth to mention that the detection rate of correct feature points may be reduced when perceptually significant distortions are introduced in images. However, this is resulting in severe degradations of the quality of the image, thus, making it useless.

The success of the detector is due to facts that it is based on end-stopped wavelets cells, which respond strongly to extremely robust image feature such as corner and points of high curvature [131]; the selected feature points are selected to be largely invariant under perceptually insignificant distortions.

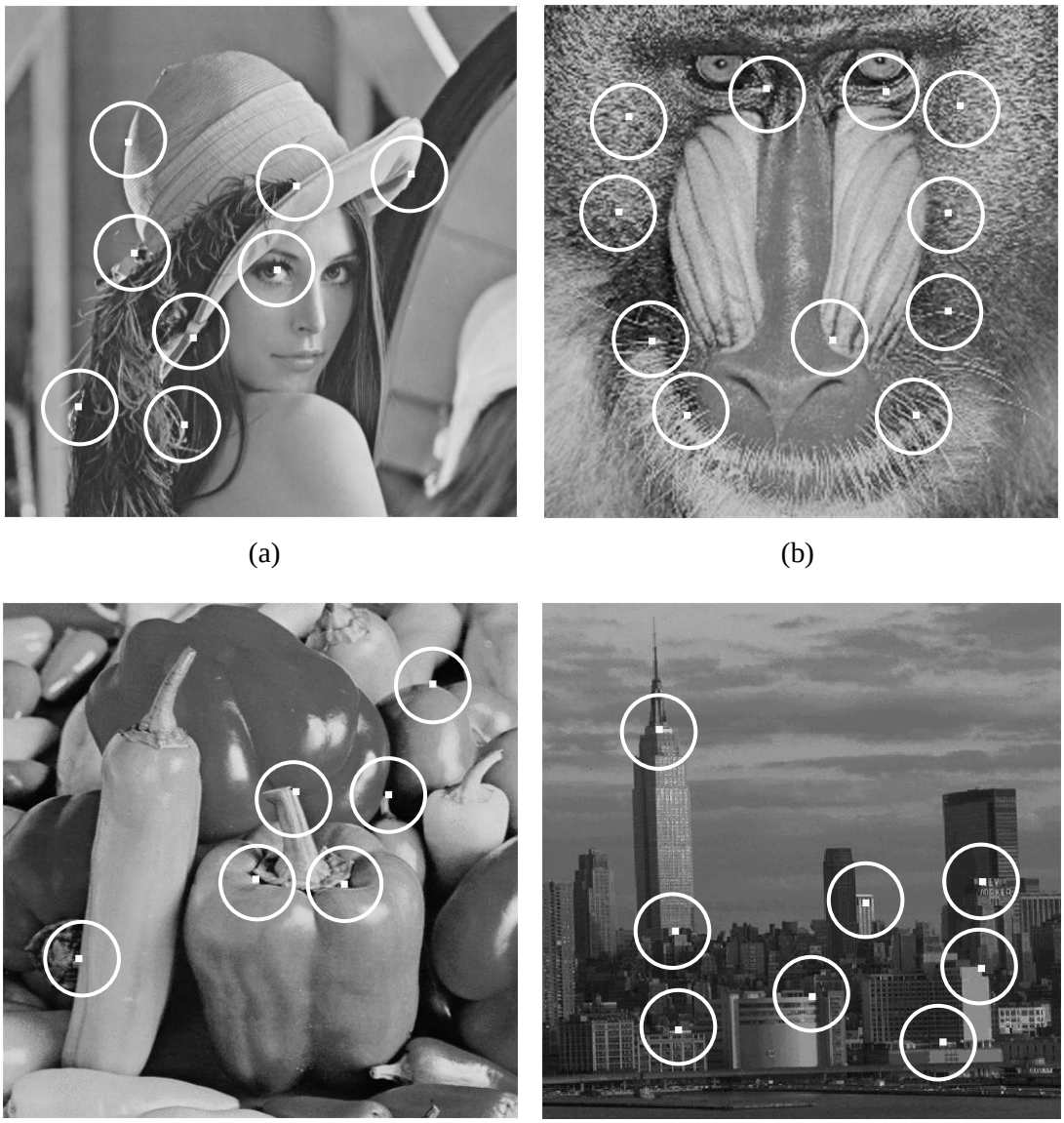
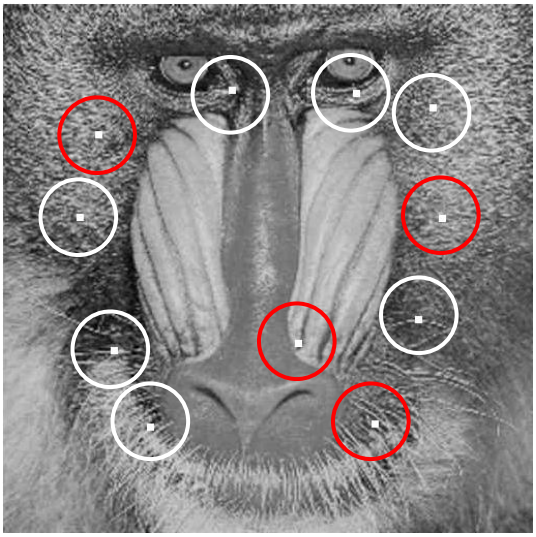
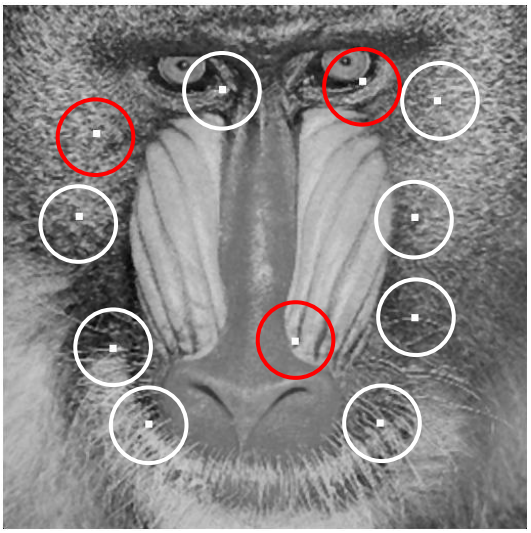


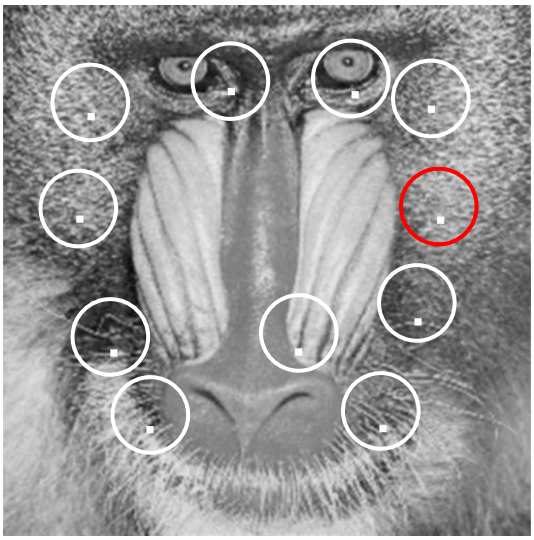
Figure 6.1 Final selected feature points and the non-overlapping regions.



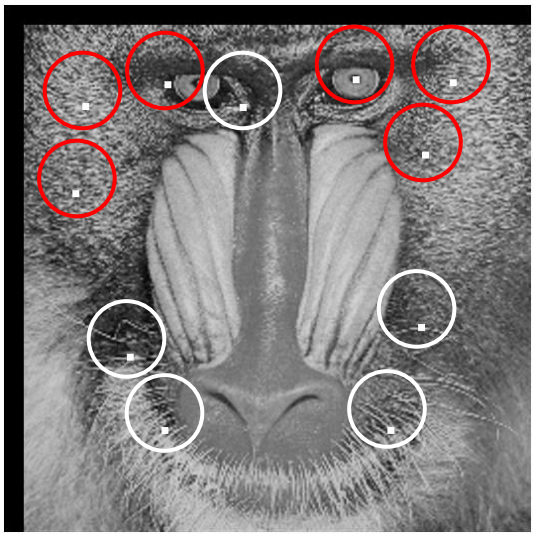
(a)



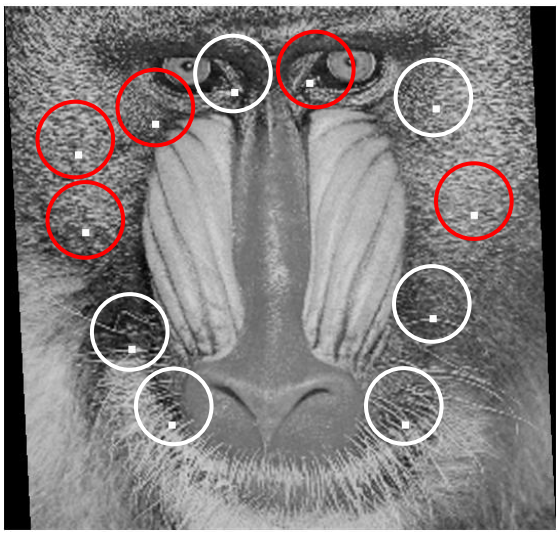
(b)



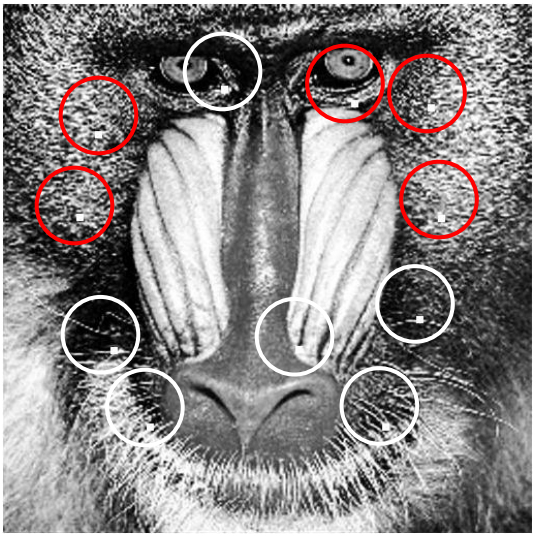
(c)



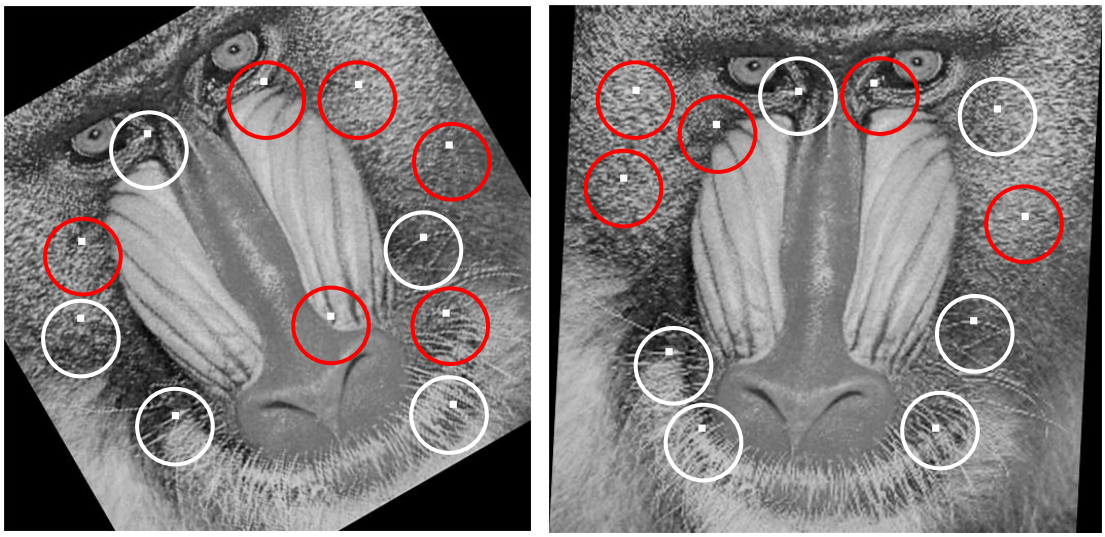
(d)



(e)



(f)



(g) **(h)**

Figure 6.2 The white feature points are extracted under different distortions: (a) JPEG 30 %, (b) median filtering 3×3, (c) low pass filtering 3×3, (d) translation x and y 20 pixels, (e) shearing –x-5%,y-0%, (f) histogram equalization, (g) rotation by 30º, (h) affine transform.

Table 6.1 Feature points detection results for common signal processing and geometric attacks (detection rates).

Attack	Lena	Peppers	Baboon	Elaine	Woman
Jpeg 80%	5/8	5/6	7/8	7/8	5/8
Jpeg 50%	4/8	4/6	8/11	5/8	4/8
Jpeg 30%	4/8	3/6	7/11	4/8	3/8
Jpeg 20%	3/8	1/6	6/11	3/8	2/8
Median filtering	5/8	3/6	8/11	5/8	5/8
Gaussian filtering	5/8	4/6	7/11	8/8	7/8
Winner filtering	5/8	4/6	7/11	7/8	5/8
Translation x & y 5	7/8	6/6	10/11	8/8	8/8
Translation x & y 10	7/8	6/6	8/11	7/8	8/8
Translation x & y 20	7/8	6/6	5/11	7/8	8/8
Centred cropping 5%	5/8	4/6	10/11	7/8	6/8
Centred cropping 20%	4/8	2/6	8/11	4/8	4/8
Rotation 1°	5/8	5/6	7/11	8/8	5/8
Rotation 2°	5/8	5/6	7/11	7/8	5/8
Rotation 5°	3/8	5/6	6/11	4/8	3/8
Rotation 15°	4/8	5/6	3/11	4/8	3/8

6.3 Image Normalization

As mentioned earlier, synchronization errors between the embedding and the detection of the watermark may be introduced by geometric attacks such as rotation, shearing and

translation and although the watermark is still present in the watermarked image, it can no longer be detected. Image normalization techniques developed for pattern recognition [132] can be used to overcome this problem as suggested in [103]. In the proposed scheme, an image normalization technique, which is invariant under rotation attacks, is performed on extracted circular images. The normalization process is defined as follows.

Geometric moments $m_{p,q}$ of a grayscale image are defined as

$$m_{p,q} = \iint_{\Gamma} x^p y^q \; f(x,y) \; dx \; dy \tag{6-1}$$

where Γ is the region of interest. The central moments are defined as

$$\mu_{p,q} = \iint_{\Gamma} (x-\bar{x})^p (y-\bar{y})^q \, f(x,y) \, dx \, dy \tag{6-2}$$

where $\bar{x}$ and $\bar{y}$ are the centroids of the image and are defined as

$$\bar{x} = \frac{m_{1,0}}{m_{0.0}}, \;\; \bar{y} = \frac{m_{0,1}}{m_{0,0}} \tag{6-3}$$

Central moments invariant under rotational transformations are defined as follows

$$\mu'_{30} = a_{11}^2 a_{12} \mu_{21} + 3a_{11} a_{12}^2 \mu_{03} \tag{6-4}$$

$$\begin{aligned} \mu'_{21} = {} & a_{11}^2 a_{21} \mu_{30} + (a_{11}^2 a_{22} + 2a_{11} a_{12} a_{21}) \mu_{21} \\ & + (2a_{12} a_{21} a_{22} + a_{22}^2 a_{21}) \mu_{12} + a_{12} a_{22}^2 \mu_{03} \end{aligned} \tag{6-5}$$

$$\begin{aligned} \mu'_{12} = {} & a_{11} a_{21}^2 \mu_{30} + (a_{21}^2 a_{12} + 2a_{11} a_{21} a_{22}) \mu_{21} \\ & + (2a_{12} a_{21} a_{22} + a_{22}^2 a_{21}) \mu_{12} + a_{12} a_{22}^2 \mu_{03} \end{aligned} \tag{6-6}$$

$$\mu'_{30} = a_{21}^3 \mu_{30} + 3a_{21}^2 a_{22} \mu_{21} + 3a_{21} a_{22}^2 \mu_{12} + a_{22}^3 \mu 03 \tag{6-7}$$

where $a_{11}, a_{12}, a_{21}, a_{22}$ are affine transformation coefficients calculated from the eigenvectors and eigenvalues of the covariant matrix of the image, as defined in [132]. To perform normalization against rotation attacks, two tensors are defined as follows:

$$t^1 = \mu'_{12} + \mu'_{30}, \qquad t^2 = \mu'_{03} + \mu'_{21} \tag{6-8}$$

Then the normalizing angle θ can be defined as

$$\theta = \arctan\left(-\frac{t^1}{t^2}\right) \tag{6-9}$$

To obtain a unique angle, another tensor t^3 is defined as:

$$t_3 = -t^1 \sin\Phi + t^2 \cos\Phi \tag{6-10}$$

As a result, angle ϕ can be obtained as follows:

$$\Phi = \begin{cases} \text{a unique } \Phi & t^3 > 0 \\ \Phi + \pi & t^3 < 0 \end{cases} \tag{6-11}$$

As an example, the normalization results for the original and the circular image rotated by 90º are shown in Figure 6.3. As can be seen, the equivalent normalized images can be obtained from the original and rotated circular images. Hence, the synchronization error during the detection process is eliminated.

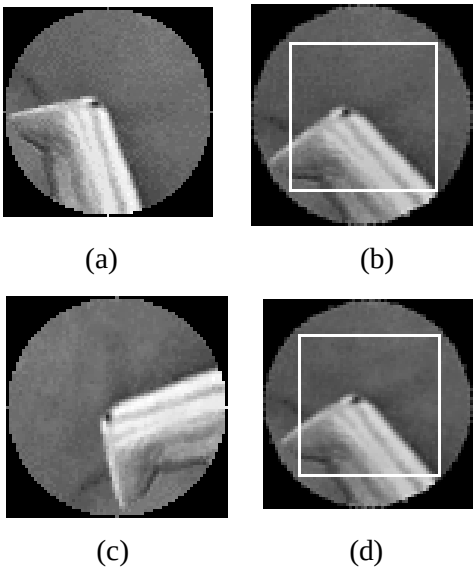


Figure 6.3 (a) Original circular image ,(b) Normalized circular image, (c) Rotated circular image by 90º, (d) Normalized circular image.

6.4 The Proposed Watermarking Scheme

The block diagram shown in Figure 6.4 provides an overview of the proposed watermarking scheme. First, a wavelet based feature detector is utilized to extract stable feature points from the original image; then circular regions are normalized by the process outlined in section 6.3. To enhance the robustness of the watermark, the watermark bits are embedded into all circular images. During the detection process, the existence of the watermark is claimed if a copy of the embedded watermark is detected in one embedded circular region.

The main contributions include:

(i) Combining the advantages of using image normalization and geometrically invariant feature points, which are extracted using an end-stopped wavelets detector.

(ii) In the proposed scheme the normalization is applied into sub-images rather than the entire image. This is motivated by fact that the moments depend on all pixels in the normalized image. Indeed, removal of any part of an image will result in significant distortion of the moment values.

(iii) Presenting a new reliable blind watermark embedding and extraction method based on quantization of DCT coefficients, which does not require the original image. Moreover, the detection process does not require the positions of the feature points from the original image.

(iv) Consideration of the local properties of feature points to detect the watermark even when some features are cropped.

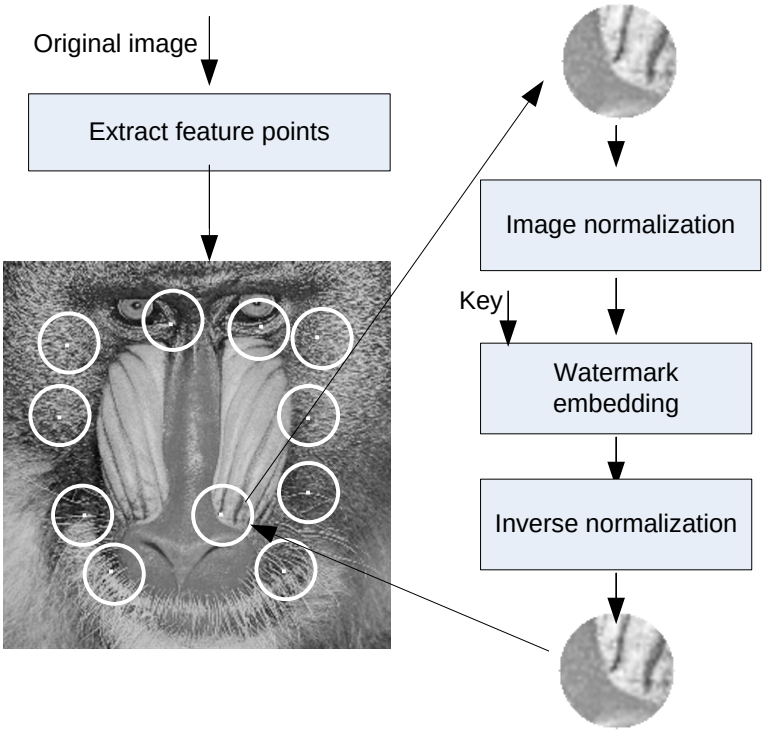


Figure 6.4 Watermark embedding Scheme.

6.4.1 Watermark Embedding Process

The watermark is assumed to be of length N_w in binary form. It is denoted by $W = \{w_i\ , i = 1,.....,N_w\ , w_i \in (0,1)\}$, which is a key-based PN sequence. The private key is shared with the detector to make the decision whether a given watermark is present or not. The watermark is embedded into low-frequency coefficients of 8×8 DCT blocks, which are randomly selected using a secret key. The proposed watermark embedding process is described as follows.

(i) A feature detector based on end-stopped wavelets is applied in order to determine feature points as described in Section 6.2. These feature points are used as the reference centres of circular sub-images for watermark embedding and detection.

(ii) For each determined feature points, search within a circular neighbouring region, whose radius is set equal to R to extract none overlapping circular images for embedding the watermark.

(iii) The normalization process is applied to each extracted circular image. As explained in Section 6.3. The normalized circular image cannot be transferred directly into the frequency domain. Therefore zero-padding operation could be performed on the normalized circular image or a sub-image could be extracted from the normalized circular image as illustrated in Figure 6.5. In the present method, sub-images are extracted from the normalized circular images because zero-padding operation will introduce error after applying the inverse DCT transform method.

(iv) The discrete cosine transform (DCT) is applied to a selected 8×8 blocks of the sub-images.

(v) To achieve robustness against common signal processing attacks, the low-frequency coefficient of the selected DCT block is used to embed the watermark. In the proposed scheme, the DC coefficients are kept unmodified and the first four AC coefficients in zigzag order are selected to embed the watermark. In order to reduce the visual degradation of the watermarked image, the number of AC coefficients for embedding a watermark bit in each selected DCT blocks is set to 4. This is because using more coefficients for embedding a watermark bit will cause more distortions of the watermarked image.

The watermark embedding process is carried out by quantizing the absolute value of the second largest DCT coefficients in the selected DCT blocks to the nearest values M_0 or M_1 as shown in Figure 6.6 by dashed vertical lines. The watermark embedding algorithm is defined as follows:

$$L_0 = L_1 = \frac{|AC_1|}{L} \qquad (6-12)$$

where L_0 and L_1 are the length of embedding intervals for bit 0 and bit 1, respectively. L represents the number of embedding intervals and $|AC_1|$ is the absolute value of the largest DCT coefficients selected from the first four AC coefficients in zigzag order. To

embed watermark bit 0 or bit 1, the absolute value of the second largest DCT coefficient $|AC_2|$ is quantized to the nearest M_0 to embed '0' or to the nearest M_1 to embed '1' as follows:

$$AC_2^* = \begin{cases} M_0 & \text{if } w = 0 \\ M_1 & \text{otherwise} \end{cases} \tag{6-13}$$

where AC_2^* is the watermarked coefficient, M_0 and M_1 are the centre values of the quantization interval '0' and interval '1', respectively. Figure 6.6 illustrates how the absolute value of the DCT coefficient AC_2 is quantized depending on the watermark bit. The absolute values of the DCT coefficients AC_3 and AC_4 are only quantized to the value of AC_2^* if they are greater than the watermarked coefficient AC_2^* as given in equations (6-14, 6-15).

$$AC_3^* = \begin{cases} AC_2^* & \text{if } AC_3 > AC_2^* \\ |AC_3| & \text{otherwise} \end{cases} \tag{6-14}$$

$$AC_4^* = \begin{cases} AC_2^* & \text{if } AC_4 > AC_2^* \\ |AC_4| & \text{otherwise} \end{cases} \tag{6-15}$$

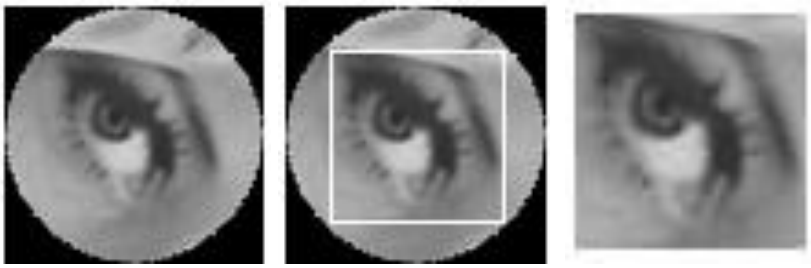
The signs of the watermarked coefficients are recovered as given below

$$AC_2^* = \begin{cases} -AC_2^* & \text{if } AC_2 < 0 \\ AC_2^* & \text{otherwise} \end{cases} \tag{6-16}$$

$$AC_3^* = \begin{cases} -AC_3^* & \text{if } AC_3 < 0 \\ AC_3^* & \text{otherwise} \end{cases} \tag{6-17}$$

$$AC_4^* = \begin{cases} -AC_4^* & \text{if } AC_4 < 0 \\ AC_4^* & \text{otherwise} \end{cases} \tag{6-18}$$

The watermarked sub-images are obtained by applying the inverse IDCT transform. Finally, the inverse normalized process is applied to each watermarked circular image.



(a) (b) (c)

Figure 6.5 (a) Zero-padded image, (b) selected sub-image, (c) extracted sub-image.

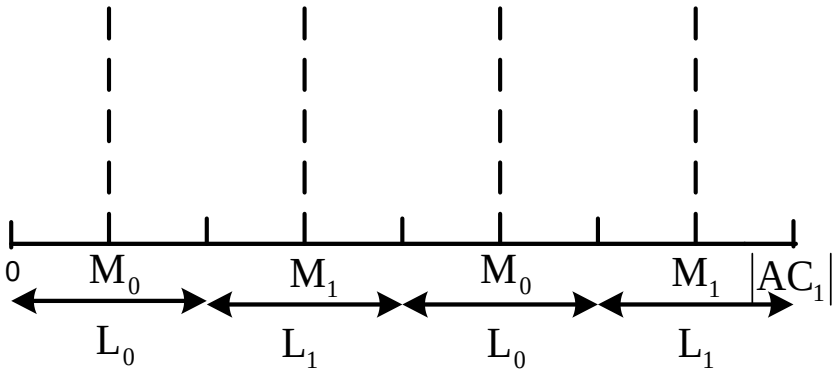


Figure 6.6 Quantization process for watermark embedding.

6.4.2 Watermark Extraction Process

Figure 6.7 illustrates the block diagram of the proposed watermark extraction process, which is performed without use of the original image (non-watermarked). Hence, the proposed scheme is able to meet the blindness requirements. In the extraction process, the first four steps are similar to that used in the watermark embedding process. A watermark bit is extracted as given below:

$$W_i^* = \begin{cases} 0 & \text{if } \left|AC_2^*\right| \in L_0 \\ 1 & \text{if } \left|AC_2^*\right| \in L_1 \end{cases} \qquad (6-19)$$

where $\left|AC_2^*\right|$ is the absolute value of the second largest DCT coefficient of the first four AC coefficients in the selected DCT blocks of size 8×8. The AC coefficients are selected in zigzag order, W_i^* is the extracted watermark bit and L_0 and L_1 are the

embedding intervals for bits 0 and 1, respectively. The extracted watermark sequence is then compared with the original embedded watermark to decide successful detection. Since the watermarked image may be modified intentionally, for example, by the embedded watermark or unintentionally by attacks, the locations of some extracted feature points may be shifted and not determined correctly. As mentioned earlier, the watermark is embedded into all circular images, which are related to extracted feature points. Therefore, ownership is proved if the watermark is detected from at least one circular image. The fact that the watermark is embedded into several circular images, rather than just one, makes it very likely to be detected, even after an image is attacked by signal processing or geometric attacks. In the detection process, an appropriate threshold T is used to make a binary decision whether a given watermark is present or not within the image. This threshold is defined based on the false-alarm probability, which may occur in the watermark detection. Since, the extracted watermark bits are independent random variables with the same 'success' probability, Binomial trials can be used to calculate the probability of extracted bits which match the embedded watermark bits as follows

$$P_k = \binom{n}{k} P^k (1-p)^{n-k} \qquad (6-20)$$

where p is success probability of a bit match between the extracted watermark and the embedded watermark bit sequences, n and k denote the number of watermark bits and the number of matched bits, respectively. Based on the assumption that the success probability is ½, the false-alarm error probability for each embedding sub-image is defined as given in equation (6-21).

$$P_{false\_alarm} = \sum_{k=T}^{n} \left(\frac{1}{2}\right) \left(\frac{n!}{k!(n-k)!}\right) \qquad (6-21)$$

This is the cumulative probability in the case where k ≥ T, where k represents the number of matched bits between the extracted and the original watermark bit sequences and T represents the threshold. The false-alarm probability against various threshold values is shown in Figure 6.8. As can be seen, the match between the extracted and embedded binary watermarks sequences in a sub-image corresponds to a false-alarm probability converging to extremely small values (as small as 15×10^{-6}) when the threshold T is set to 16.

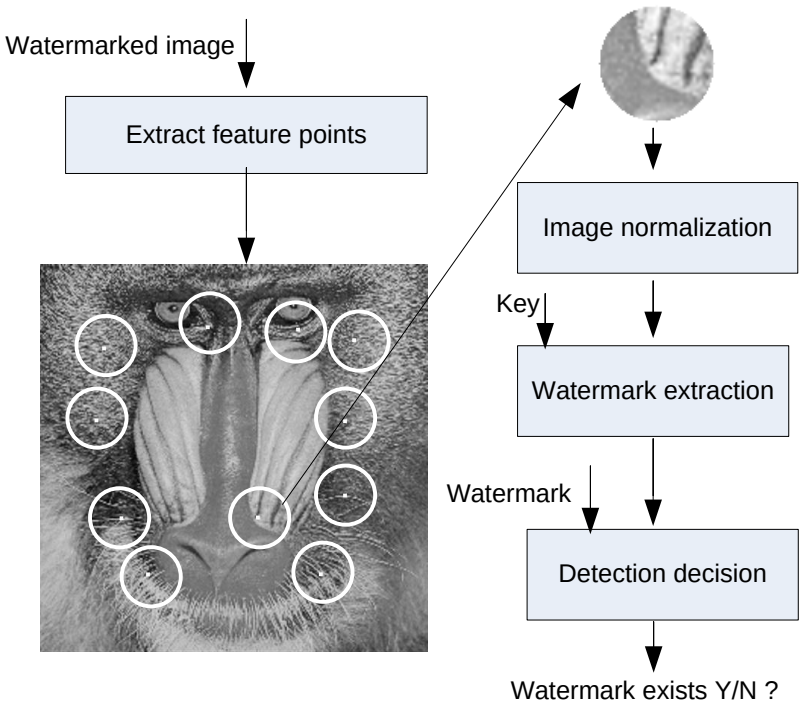


Figure 6.7 Watermark extraction process.

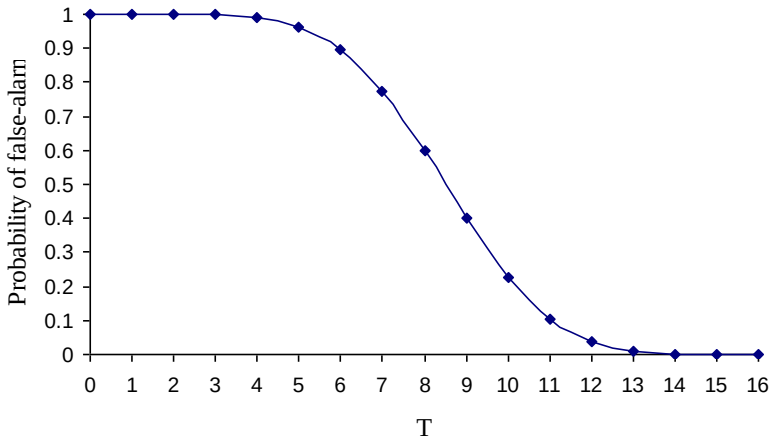


Figure 6.8 False-alarm probability of a sub-image .

6.5 Experimental Results and Discussion

The watermark imperceptibility and robustness were evaluated by using 100 different 8 bit grey scale images of size 512×512 including well known standard images such as Lena, Peppers, Baboon and Lake, etc. In all experiments, a pseudorandom sequence of size 16-bits was used as a watermark and the radius of each circular image was fixed at 71 pixels.

6.5.1 Watermark Imperceptibility

The degree of imperceptibility of the embedded watermark is important to ensure that there is no noticeable visual degradation due to the embedding process. The Peak Signal to Noise Ratio (PSNR) was adopted to measure the perceptual distortion of the proposed scheme. The Structural similarity index (SSIM) was also adopted for assessing the similarity between the original image and the watermarked one. A detailed description of SSIM can be found in [18]. Figure 6.9 shows the SSIM values for the 100 watermarked images. In the embedding process of the proposed scheme, the distortion of an image depends on the watermark length, the number of quantization levels for embedding the watermark, the number of extracted sub-images and the

number of AC coefficients for embedding a watermark bit in each 8×8 DCT block. The larger the number of AC coefficients used for embedding, the more significant the distortion. Also the more the quantization levels (L) for embedding watermark bits, the smaller the distortion. In the other words, increasing the number of quantization levels leads to a small change in the AC coefficients. Hence there is a trade off between robustness and imperceptivity. As shown in Figure 6.10, the PSNR values for 100 watermarked images are between 41.78 and 56.29 db. These values are all greater than 30 db, which is the empirically tested threshold value for an image without any perceptible degradation [113]. Table 6.2 shows the transparency results for the proposed scheme in comparison with those obtained in [111, 113, 114]. These schemes were chosen to evaluate the proposed scheme due to their similarity to the proposed technique in terms of using feature points and embedding the same watermark length. The results demonstrate that the proposed scheme offers high PSNR values. This is because the proposed scheme embeds a watermark bit in one AC coefficient and the other two AC coefficients are only altered if they do not satisfy the watermark embedding conditions; whereas, in [111, 113] a watermark bit is embedded into the magnitudes of two DFT coefficients while in [114], all pixels inside a circular region are altered to embed one watermark bit. As a result more distortions are introduced in the watermarked images. Taking ‘Elaine’, ‘Couple’, ‘Woman’ and ‘Lake’ images as examples, the original, watermarked images and circular sub-images are shown in Figure 6.11. It can be seen that the differences between the corresponding watermarked and un-watermarked images are imperceptible and the embedded watermark is invisible to human eye. The results in Figure 6.9 and Figure 6.10 also support this conclusion since the PSNR and SSIM are high after embedding the watermark.

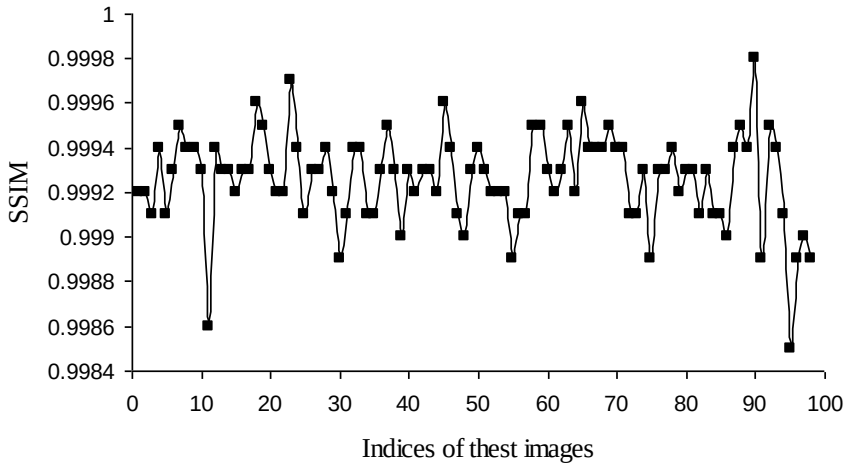


Figure 6.9 SSIM Similarity measurement between orginal and watermarked images.

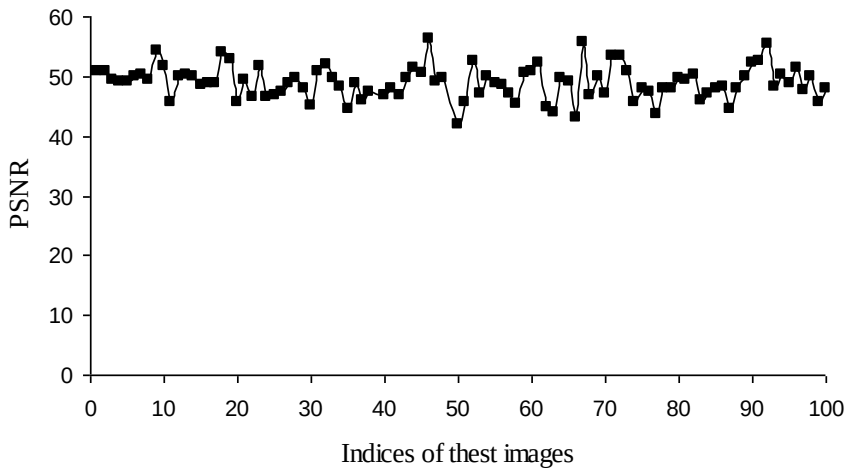
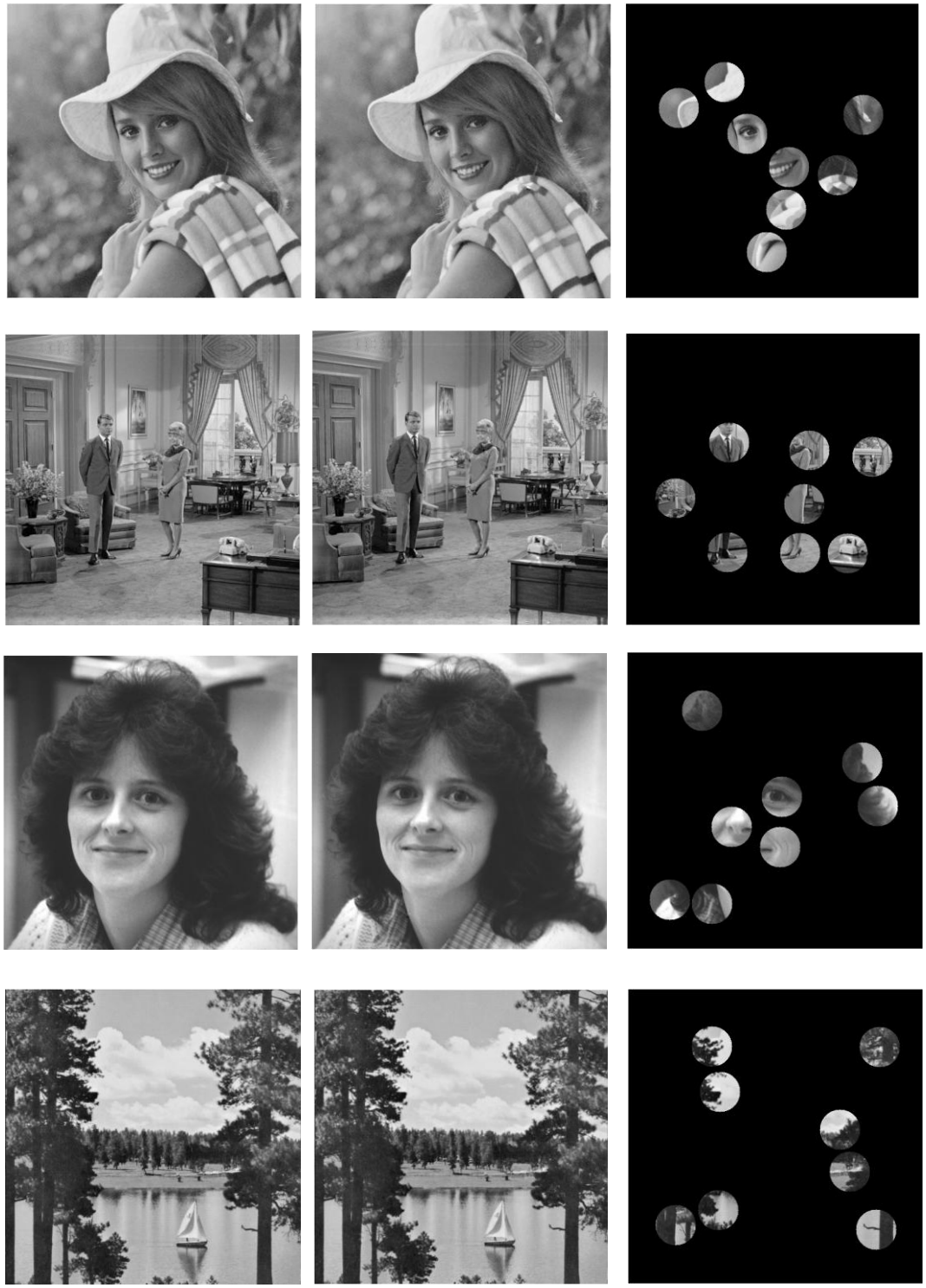


Figure 6.10 Watermark distortions (in PSNR).

Table 6.2 PSNR between watermarked images and the orginal images (db).

	Lena	Peppers	Baboon
Proposed	50.82	50.87	49.46
Scheme [111]	49.42	56.60	45.70
Scheme [113]	43.33	37.62	44.06
Scheme [114]	43.21	44.20	43.23



(a) (b) (c)

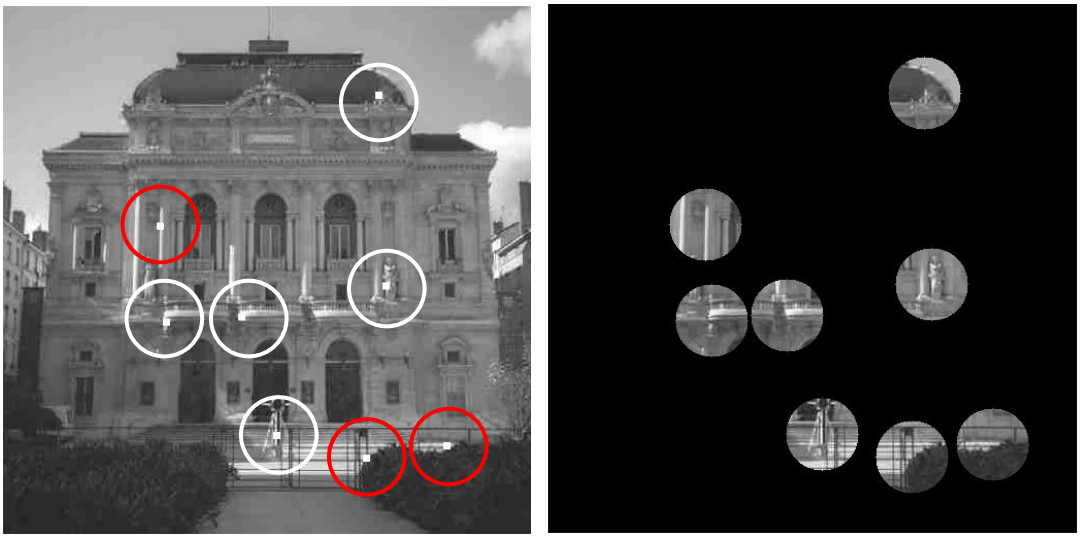
Figure 6.11 (a) Original images (b) Watermarked images (c) Circular feature regions for ‘ Elaine’, ‘Couple’ and ‘ Woman’ images.

6.5.2 Watermark Robustness

To evaluate the robustness of the proposed watermarking scheme, various common signal processing and geometric attacks were applied to the watermarked images. These signal processing attacks include JPEG-lossy compression, median filtering, Gaussian filtering and Wiener filtering and geometric attacks include rotation, scaling, shearing, linear geometric transformation, translation, row and column removal, cropping attacks. For the JPEG-lossy compression attacks, quality factor varied from 20% (high compression) to 100%. As examples, results for 'Elaine', 'Lena' and 'Opera' images under JPEG 50%, JPEG 30%, and JPEG 20% attacks, respectively are shown in Figure 6.12, in which the correctly extracted feature points are marked with white circles, while the incorrect feature points are marked with red circles. As can be seen, overall a majority of the watermarked regions can still be correctly detected even when the watermarked image is compressed by jpeg compression with quality factor of 20%. The robustness of the proposed scheme against JPEG compression attack is achieved by embedding the watermark into the low frequency coefficients of the DCT, which are less affected by JPEG compression attack.

(a)

(b)

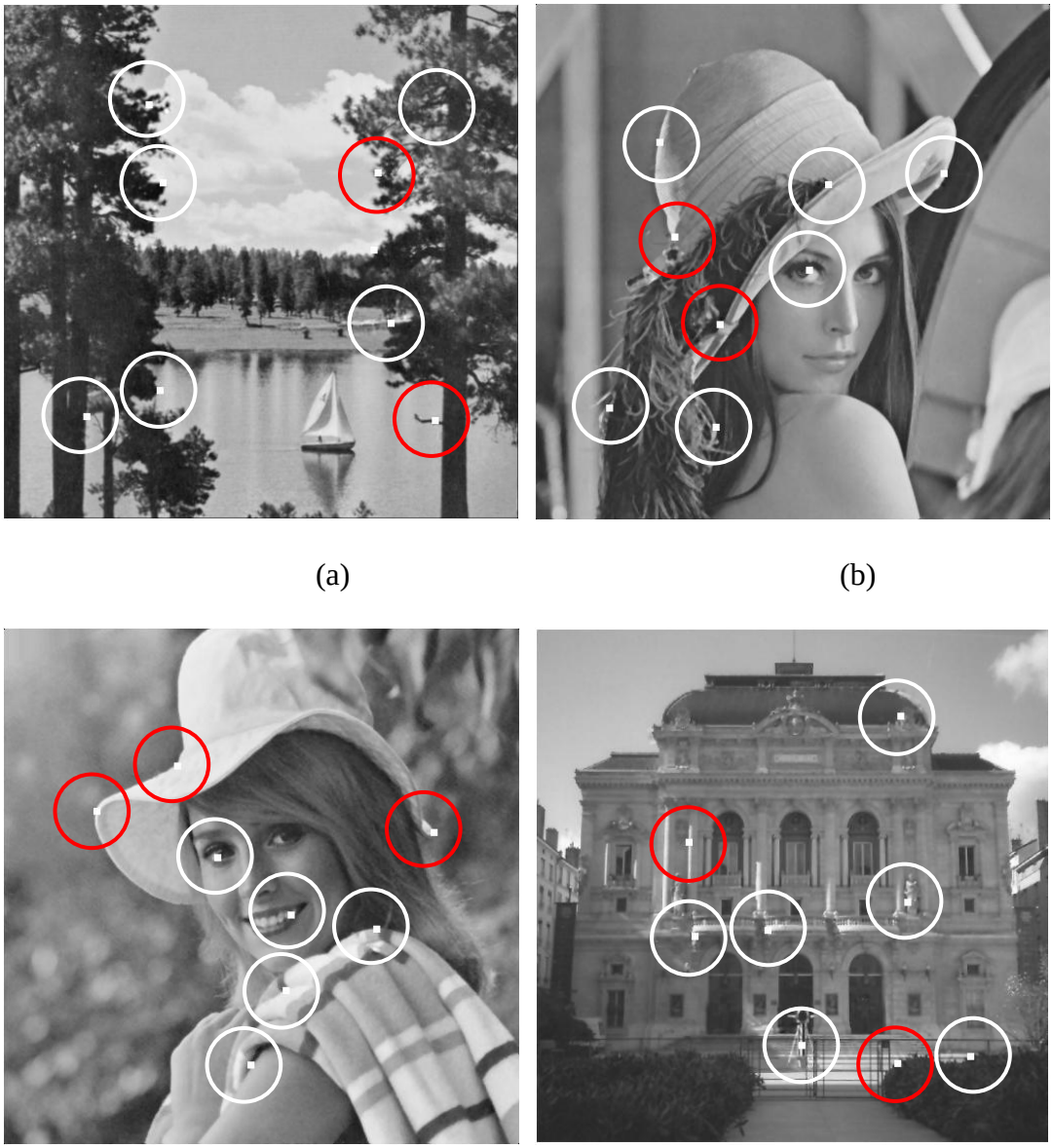


(c)

Figure 6.12 Results of JPEG compression attacks (a) watermarked 'Elaine' image with JPEG 50%, (b) watermarked 'Lena' image with JPEG 30%, (c) watermarked ' Opera' image with JPEG 20%.

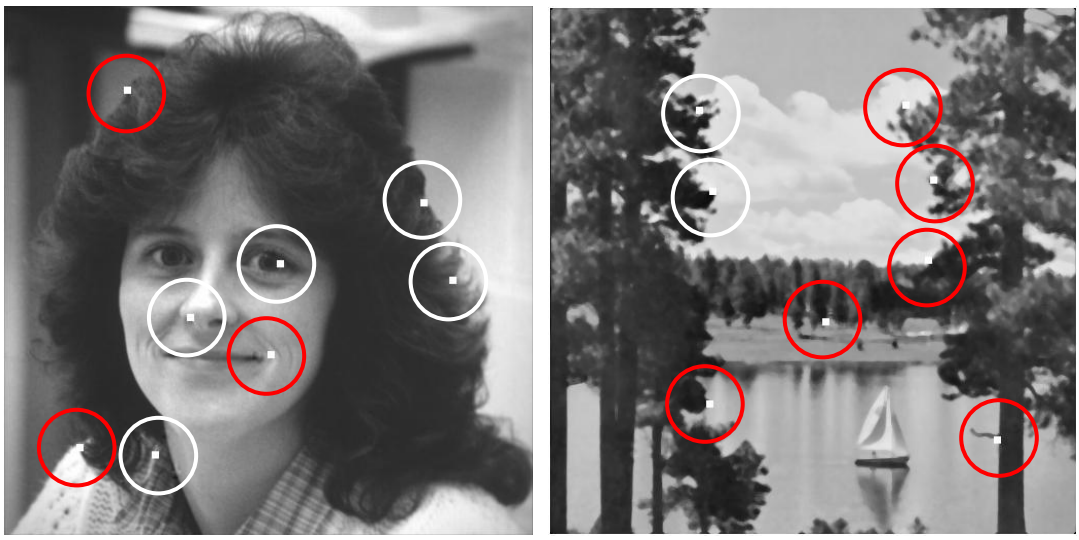
For filtering attacks, the watermarked images were subjected to median, Gaussian lowpass and Wiener filtering using different filter sizes and results are shown in Figure 6.13. The results show that the proposed scheme is robust against filtering attacks even with a filter size of 5×5. It can be seen that the larger the filter size, the lower the detector performance. However, using filter sizes greater than 5×5, the image content is

significantly degraded and this is not a practical attack because the resulting image quality is unacceptable.



(a) (b)

(c) (d)



(e) (f)

Figure 6.13 Results of filtering attacks applied to watermarked images (a) median filtering 2×2 , (b) median filtering 3×3, (c) median filtering 3×3, (d) Winer filtering 3×3, (e) Gaussian lowpass filtering 5×5, (f) median filtering 5×5

The robustness of the proposed scheme against geometric attacks was evaluated by applying common geometric attacks, which included rotation, scaling, shearing, linear geometric transformation, translation, row and column removal, cropping attacks. These types of attacks can be applied to watermarked images in order to make the detector lose synchronicity. For the rotation attacks, the watermarked images were rotated by up to 90º and before applying the detection process. Shearing distortion was applied to watermarked images using a factor up to 5% in x and y directions. For example, Figure 6.14 (a) shows the result of attacks on the 'Lena' and 'Woman' images rotated by 10º and 45º, respectively. Results of shearing attacks on the 'Lena' and 'Elaine' images are shown in Figure 6.14 (b). As can be seen, overall a majority of the watermarked regions can still be correctly detected. This is because the watermark was embedded into a number of local invariant regions of feature points, which are independent of the position of the pixels. Furthermore, the proposed scheme overcomes the synchronization problem caused by rotation and shearing attacks by normalizing the embedding local regions as explained in Section 6.3).

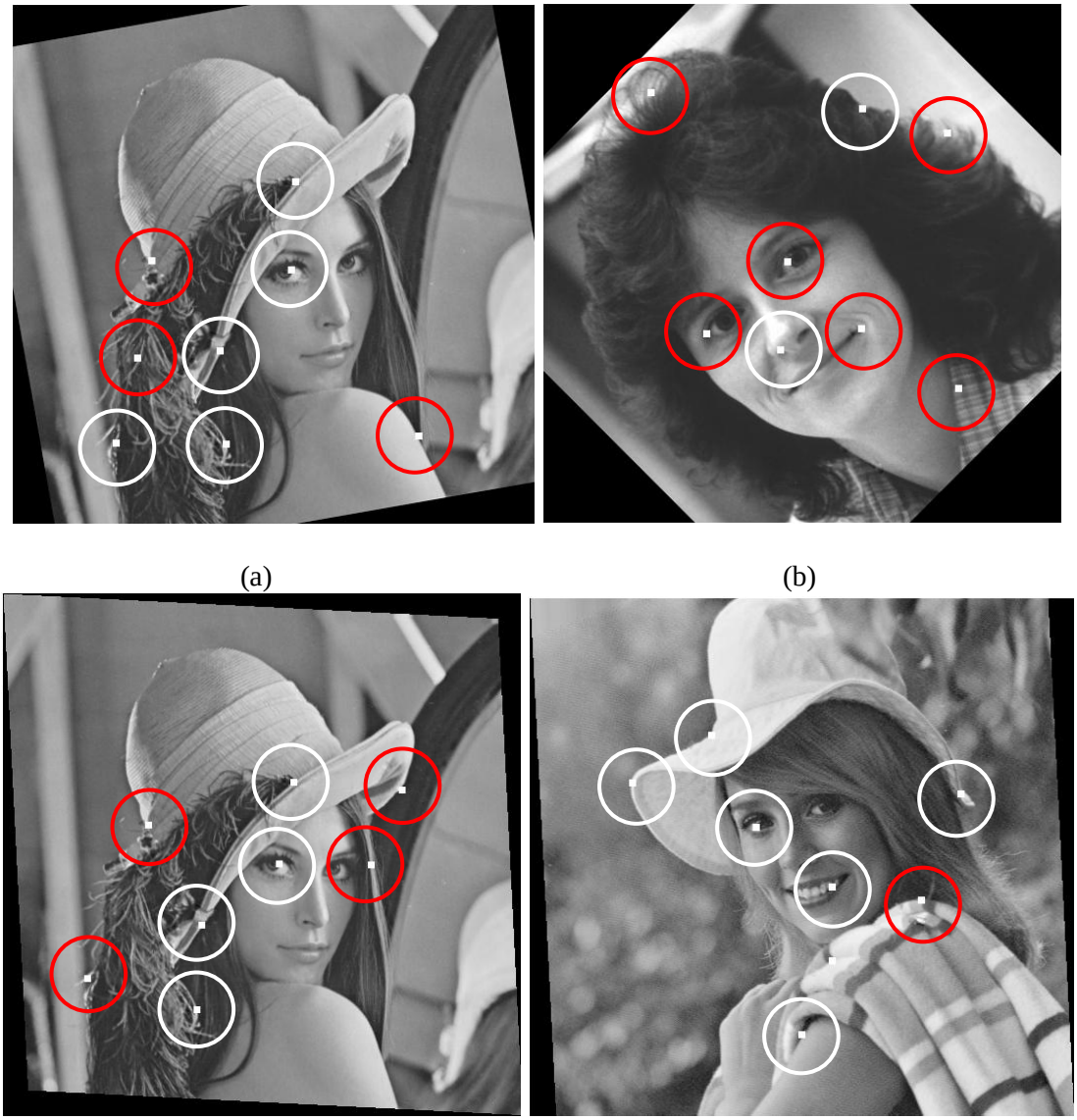


Figure 6.14 Results of geometric attacks; (a) Rotation by 10º, (b)) Rotation by 45º ,(c) Shearing x-5%, y-5%, (d) Shearing x-5%, y-0%.

The translation attack performs a geometric transformation which maps the position of each pixel in an input image into a new position in the output image. Under this attack, the pixels values remain unchanged except for the shift of location. As a result, synchronization error may be introduced at the detection process. As shown in Figure 6.15, the proposed scheme overcomes this problem and overall a majority of the watermarked regions can still be correctly detected. This is because the detector determines the location of watermarks independently of the position of the pixels.

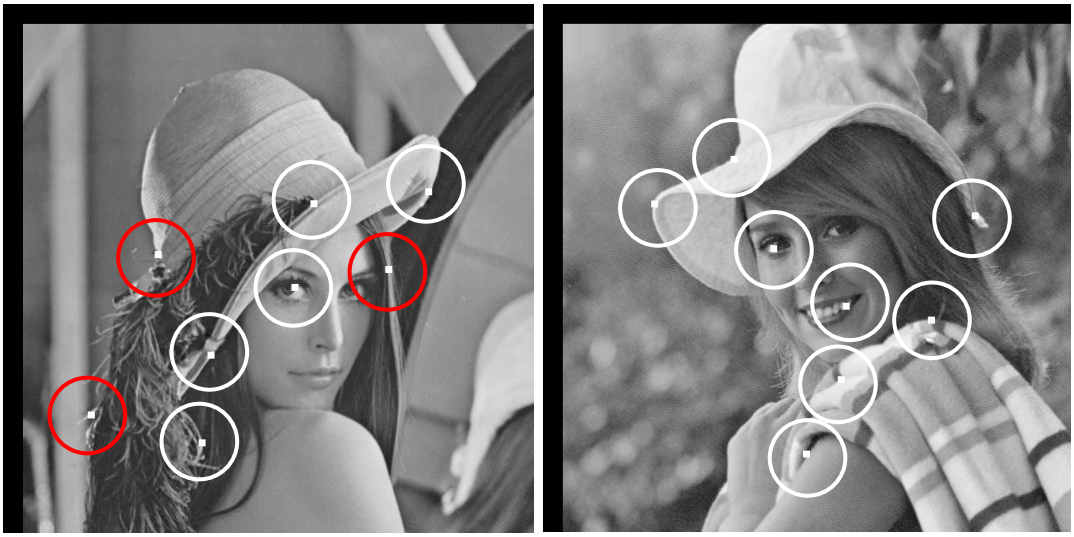


Figure 6.15 Results of tanslation attacks x-20 and y-20.

In a cropping attack, a portion of the watermarked image is removed. This leads to irretrievable loss of some data and can also introduce synchronization problem due to changing of pixels locations. Because the watermark was embedded into a number of local regions, which are determined independently of pixel locations, the proposed scheme is able to detect the watermark even when the watermarked image is cropped locally or by cropping 25% or 50% of the whole image. Under a cropping attack some regions that embedded the watermark may be destroyed, but others may remain unchanged. Figure 6.16 shows some results of cropping attacks applied to watermarked images.

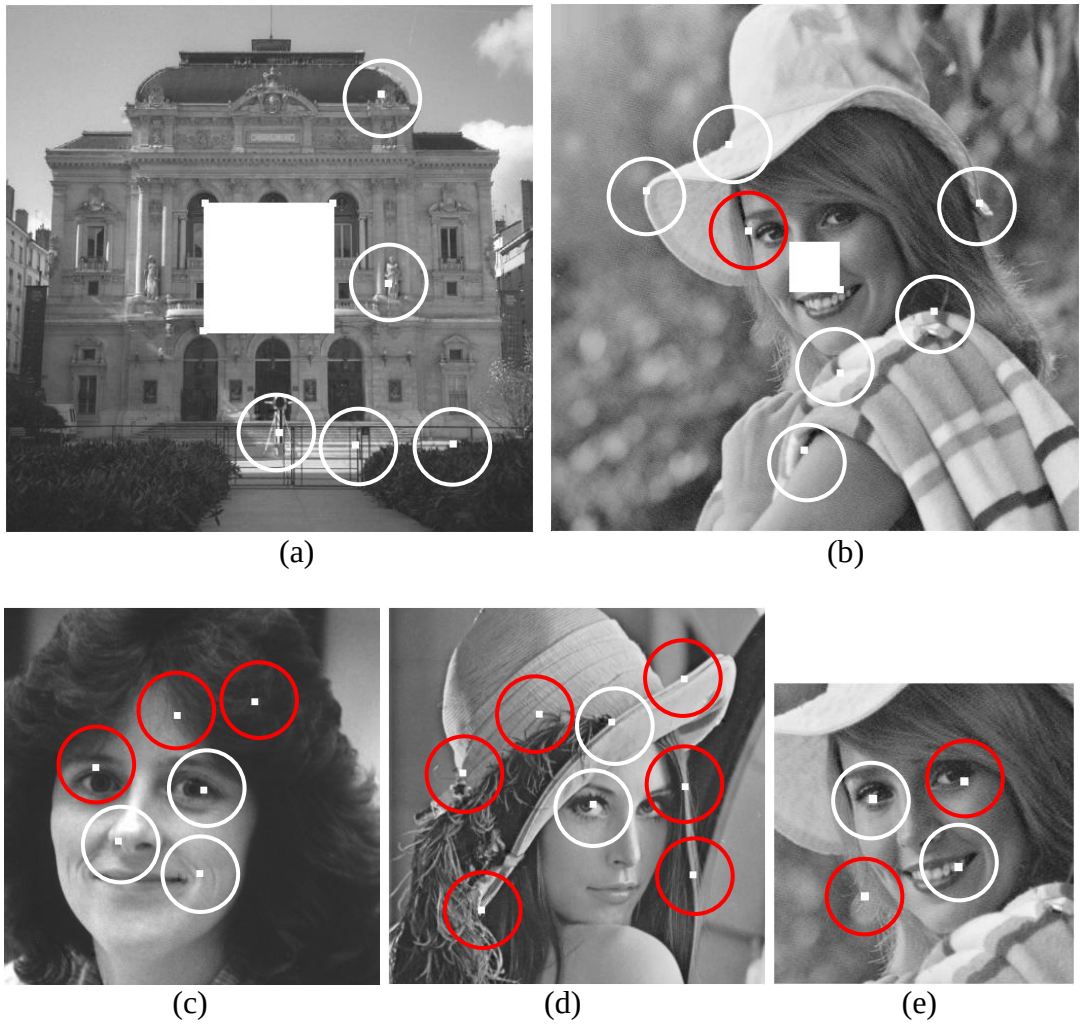


Figure 6.16 Results of cropping attacks; (a) centered cropping 20%, (b) centered cropping 10% (c) cropping 25% off, (d) cropping 25% off, (e) cropping 50% off.

The performance of the proposed scheme was also tested against random removal of some rows and columns from the watermarked image. This attack may also introduce synchronization problem due to changing of pixels locations. In this attack, the watermarked images were attacked by randomly removing 1 row and 5 columns, 5 rows and 1 column, 17 rows and 5 columns, 17 rows and 5 columns. The attack was implemented as described in [133]. For example, the watermarked images 'Opera' and 'Elaine' attacked by removing randomly 17 rows and 5 columns, and 5 rows and 17 columns, respectively are shown in Figure 6.17. It can be conclude from this figure that the proposed scheme is robust to rows and columns random removal attack.

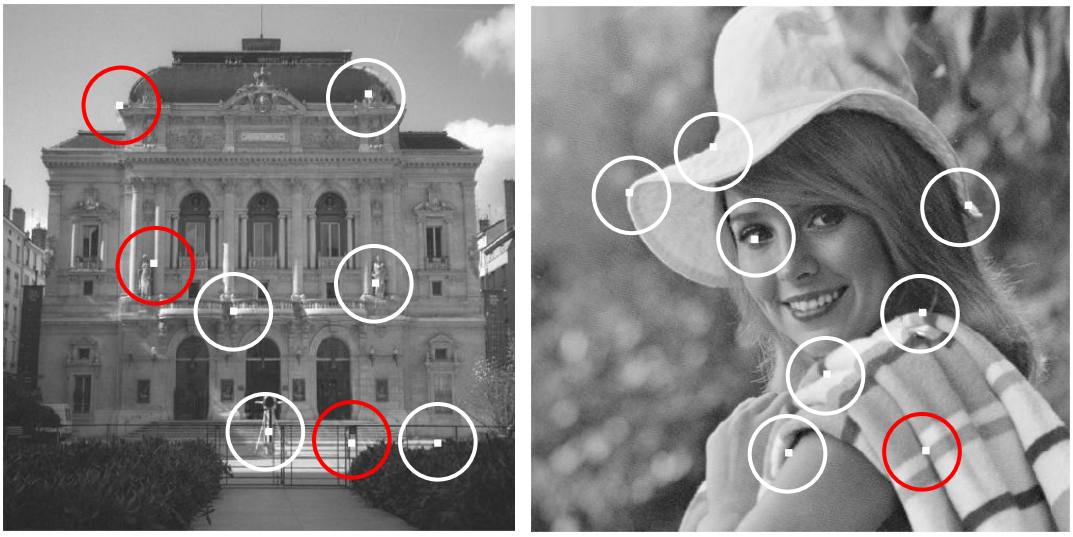


Figure 6.17 Results of row and column removel attacks; (a) 17 rows & 5 columns removel (b) 5 rows & 17 columns removel.

The performance of the proposed scheme is evaluated with the Tang's scheme [111]. Table 6.3 and Table 6-4 depict the results of various common signal processing and geometric attacks, in comparison with Tang's scheme [111] on images 'Lena', 'Peppers' and 'Baboon'. As shown in Table 6.3, the proposed scheme performs better than Tang's scheme under commonly used signal processing attacks, such as JPEG compression down to a quality factor of 30%, median filtering and combination of median filters with JPEG compression attacks.

The watermark can also be extracted correctly by the proposed scheme under a variety of geometric attacks, which Tang's scheme failed to handle as shown in Table 6-4. For example, rotation attacks with small rotation angles. It can be seen that the watermark can be correctly extracted by the proposed scheme under rotation, row and column removal, cropping, linear geometric transformation, up to 5% shearing in both horizontal and vertical directions and also translation in both directions.

The performance of the proposed scheme was also evaluated against Lei's scheme [114]. The robustness results are illustrated in terms of BER, which is defined as the ratio of the number of incorrectly extracted watermark bits to the length of the watermark sequence. The experimental results show that, the error bits are 1 bit

(BER=0.06) for different attacks, whereas, in the scheme presented in [114], the error bits are 6 bits (BER $\leq$ 0.35). As shown in Table 6.5, the watermark can be correctly extracted by the proposed scheme even under JPEG compression with a quality factor as low as 30%, while as reported by those authors, their watermark cannot survive under the scheme in [114] when the watermarked image is compressed with a quality factor of 40% or less.

The performance of the proposed scheme compared to related work [111, 114] can be justified by the following points:

(i) In the embedding process, the blocks that contain feature points are not used for embedding the watermark bits. As a result, the influence of the embedding process on the feature points is reduced in comparison to [111, 114].

(ii) As explained in Section 6.4, the proposed scheme embeds a watermark bit by changing one AC coefficient only which results in less distortion of the embedding circular images and hence more accurate normalization angles can be used at extraction.

(iii) Due to the use of low frequency coefficients of the DCT for embedding the watermark, better robustness against JPEG compression attack is achieved compared to [114], which embeds the watermark in the spatial domain.

(iv) Due to the more robust feature extraction method used in the proposed scheme, the local invariant regions of feature points can be determined correctly even when an image is attacked by common signal processing or geometric attacks.

Table 6.3 Watermark detection results for signal processing attacks (detection rates).

	Proposed method			Scheme in [111]		
	Lena	Peppers	Baboon	Lena	Peppers	Baboon
No attack	6/8	5/6	8/11	7/8	4/4	10/11
Jpeg 80%	5/8	5/6	7/11	6/8	3/4	9/11
Jpeg 70%	7/8	3/6	8/11	7/8	3/4	11/11
Jpeg 60%	4/8	4/6	7/11	6/8	1/4	7/11
Jpeg 50%	4/8	4/6	8/11	5/8	3/4	7/11
Jpeg 40%	4/8	4/6	7/11	3/8	1/4	5/11
Jpeg 30%	4/8	3/6	7/11	2/8	0/4	4/11
Median filtering2×2	2/8	2/6	5/11	1/8	1/4	6/11
Median filtering3×3	5/8	3/6	8/11	1/8	1/4	2/11
Gaussian filtering3×3	5/8	4/6	7/11	5/8	1/4	8/11
Median filtering 2×2+jpeg 90	2/8	2/6	5/11	2/8	0/4	6/11
Median filtering 3×3+jpeg 90	3/8	2/6	9/11	1/8	1/4	1/11
Gaussian filtering 3×3+jpeg 90	3/8	3/6	7/11	5/8	2/4	8/11

Table 6-4 Watermark detection results for geometric attacks (detection rates).

	Proposed method			Scheme in [111]		
	Lena	Peppers	Baboon	Lena	Peppers	Baboon
Rotation 1°	2/8	4/6	6/11	3/8	2/4	4/11
Rotation 2°	2/8	4/6	7/11	0/8	0/4	0/11
Rotation 5°	2/8	3/6	6/11	0/8	0/4	3/11
Centred Cropping 5% off	5/8	3/6	6/11	2/8	2/4	2/11
Centred Cropping 10% off	3/8	4/6	6/11	2/8	2/4	2/11
Remove 1 row and 5 Col.	4/8	4/6	7/11	3/8	3/4	6/11
Remove 5 rows and 17 Col.	4/8	3/6	5/11	0/8	1/4	3/11
Shearing-x-1%-y-1%	3/8	3/6	6/11	4/8	1/4	5/11
Shearing-x-0%-y-5%	2/8	4/6	5/11	2/8	1/4	3/11
Shearing-x-5%-y-5%	2/8	2/6	2/11	1/8	0/4	2/11
Linear geometric transform 1.007,0.01,0.01,1.012)	1/8	4/6	6/11	5/8	1/4	4/11
Linear geometric transform 1.010,0.013,0.009,1.011)	2/8	3/6	5/11	4/8	1/4	4/11
Linear geometric transform 1.013,0.008,0.011,1.008)	3/8	4/6	6/11	4/8	0/4	5/11
Translation-x and y 10	4/8	5/6	5/11	4/8	2/4	7/11
Translation-x and y 20	4/8	5/6	5/11	4/8	1/4	5/11
Centred Cropping 5% +JPEG70	4/8	2/6	6/11	2/8	2/4	2/11
Centred Cropping 10%+JPEG70	2/8	2/6	6/11	3/8	2/4	2/11

Table 6.5 Results of some signal processing and geometric attacks (BER).

	Proposed method			Scheme in [114]		
	Lena BER	Peppers BER	Baboon BER	Lena BER	Peppers BER	Baboon BER
No attack	0	0	0	0	0	0
Jpeg 80%	0	0	0	0	0	0.31
Jpeg 50%	0	0	0	0	0.18	0.35
Jpeg 30%	0	0	0	-	-	-
Median filtering	0	0	0	0	0	0
Rotation 5º	0.06	0	0	0	0	0
Rotation 20º	0	0	0.06	0	0	0
Rotation 45º	0.06	0.06	0.06	0	0.06	0.06
Rotation 90º	0	0	0	0	0	0.31
Translation x,y-5	0	0	0	0	0	0.06
Translation x, y -10	0	0	0	0	0	0
Scaling 0.70	0	0	0	0.06	0	0.35
Scaling 1.20	0	0	0	0	0	0

The results of testing 100 images against common signal processing and geometric attacks are shown in Table 6.6 and Table 6.7, respectively. A success rate is defined as the ratio between the number of watermarked images from which the watermark is extracted correctly and the number of test images. The results demonstrate that the proposed scheme is robust to common signal processing and geometric attacks.

Table 6.6 the success rates of the proposed scheme against common signal processing attacks.

Attack category	Detection rate (%)
No attacks	100
JPEG 100	100
JPEG 80	98
JPEG 50	98
JPEG 30	92
JPEG 20	88
Median filtering 2×2	90
Median filtering 3×3	95
Gaussian Filtering 3×3	99
Gaussian Filtering 5×5	99
Wiener filtering 3×3	97
Wiener filtering 5×5	96

Table 6.7 the success rates of the proposed scheme against geometric attacks.

Attack category	Detection rate (%)
Centered cropping 5%	99
Centered cropping 10%	99
Centered cropping 20%	94
Translation 5 pixels	100
Translation 10 pixels	100
Translation 20 pixels	100
Scaling 0.70	93
Scaling 0.90	98
Scaling 1.20	99
Scaling 1.50	99
1 row & 5 col. removal	94
5 row & 17 col. Removal	92
5 row & 1 col. removal	92
17 row & 5 col. removal	90
Shearing x 1% , y 1%	89
Shearing x 0% , y 1%	91
Shearing x 1% , y 0%	91
Shearing x 0% , y 5%	91
Shearing x 5% , y 0%	90
Rotation 1˚+cropping	99
Rotation 2˚+ cropping	97
Rotation 5˚+ cropping	94
Rotation 10˚+ cropping	96
Rotation 30˚+ cropping	82
Rotation 90˚	95
Linear geometric transform (1.007,0.01,0.01,1.012)	91
Linear geometric transform (1.010,0.013,0.009,1.011)	92
Linear geometric transform (1.013,0.008,0.011,1.008)	92

6.6 Conclusions

This chapter presents a robust image watermarking scheme, which is designed to be robust against both signal processing and geometric attacks. In order to resist geometric attacks, visually significant feature points were extracted using the end-stopped wavelets detector. This feature points are used as reference points to eliminate synchronization errors between watermark embedding and detection. According to the location of feature points, circular images were extracted, which were watermarked in the DCT domain. Rotation invariance was achieved using an image normalization technique. The reference image is not required at detection. The success of the watermarking scheme proposed here is due to the following factors:

(i) Using visually significant feature points, which are extracted by end-stopped wavelets detector and able to reduce synchronization errors between the watermark embedding and detection stages.

(ii) Image normalization technique helps to achieve robustness against rotation attacks.

(iii) Since local properties of the features are considered, the proposed scheme is able to detect the watermark even when some feature points are cropped.

(iv) Robustness against common signal processing attacks is achieved by selecting low-frequency coefficients of the DCT for embedding the watermark.

It has been demonstrated that under most of the commonly used attacks, the proposed watermarking scheme can recover the embedded watermark from a considerable number of circular images. Experimentally, it is found that the more robust feature points an image has, the more robustness is achieved in watermarking.

CHAPTER SEVEN

7 CONCLUSIONS AND SUGGESTIONS FOR FURTHER WORK

7.1 Introduction

Digital watermarking techniques have been utilized to maintain the copyright of digital data by identifying the owner or distributor of digital data. Numerous methods have been proposed. However, digital watermarking still faces many challenges in both robustness and security requirements.

In this thesis, three novel image watermarking algorithms have been designed and implemented for copyright protection. The first algorithm is based on embedding multiple watermarks in the blue channel of the colour image in order to improve the robustness against attacks. The second proposed algorithm aims to achieve better trade-off between the imperceptibility and robustness requirements of a digital watermarking system. The third proposed algorithm aims to overcome the problem of synchronization errors caused by geometric attacks including global affine transform and local geometric distortions. In addition to the discussions in individual chapters, a summary of the results, the main contributions of this thesis and some suggestions for future investigation are provided in the following sections.

7.2 Summary of the results

The performances of the proposed algorithms were evaluated using a series of measures including the perceptual quality of the watermarked image, the similarity between the embedded and extracted watermarks and robustness to signal processing and geometric attacks. The Peak Signal-to-Noise Ratio (PSNR) and the Structural Similarity Index Measure (SSIM) were adopted to measure the perceptual distortion of the watermarked image. Experimental results show that the proposed algorithms succeed in making the watermark perceptually invisible. To evaluate the robustness of the proposed watermarking algorithms, various common signal processing and geometric attacks were applied to the watermarked images.

The results of the spatial image watermarking algorithm presented in Chapter 4 demonstrate that more robustness can be achieved by embedding multiple watermarks in the host image. The results of the second algorithm presented in Chapter 5 show that better trade-off between watermark imperceptibility and robustness requirements can be achieved. In addition, more robustness can be achieve when the watermarks are embedded adaptively to the feature content of the host image in perceptually significant DC components. The results of the third algorithm presented in Chapter 6 show that the synchronization errors between the watermark embedding and detection stages can be eliminated using invariant feature points and image normalization, which helps to achieve robustness against rotation attacks. The results show that the proposed algorithm is able to detect the watermark even when some feature points are cropped because the local properties of the features were considered.

7.3 Thesis Contributions

The main contributions in this thesis can be summarised as follows in terms of three research topics including watermarking of colour images in the spatial domain, adaptive watermarking of images in the DCT domain and image watermarking using local invariant feature points and image normalization.

Regarding watermarking of colour image in the spatial domain, the main contribution includes:

(i) Unlike previously proposed techniques, the proposed technique is based on dividing a binary watermark logo into parts and embedding each part into different regions of the blue component of colour images in order to improve the robustness against attacks. The experimental results demonstrate that the robustness of the spatial domain watermarking technique can be improved by embedding multiple watermarks.

Regarding the adaptive image watermarking technique in the DCT domain, the main contributions include:

(i) The proposed technique embeds a watermark in an adaptive manner via classification of DCT blocks with three levels: smooth, edges and texture, implemented in the DCT domain by only analyzing the values of two AC coefficients rather than by using methods such as Canny, Sobel or Prewitt for detecting image edges. As a result, significant improvement of computing cost is achieved. The experimental results support the claim that this adaptive technique is capable of achieving a better trade-off between watermark imperceptible and robustness requirements.

(ii) New blind watermark embedding and extraction processes implemented in the DCT domain: embedding a watermark into the DC components of the DCT makes the proposed method more robust to common attacks. The blind watermarking method does not require the original image at the detection process, which makes the proposed method portable to many applications. Furthermore, due to its operation in the DCT domain, the processing speed is high and the computing cost incurred is low.

Regarding the robust image watermarking via geometrically invariant feature points and image normalization techniques, the main contributions include:

(v) Combining the advantages of using image normalization and geometrically invariant feature points, which are extracted using an end-stopped wavelets detector. The experimental results demonstrate that using invariant feature points and image normalization reduces the synchronization errors caused by geometric attacks.

(vi) Presenting a new reliable blind watermark embedding and extraction method based on quantization of DCT coefficients, which does not require the original image. In comparison with existing methods, the proposed algorithm offers high PSNR values. This is because the proposed algorithm embeds a watermark bit in one AC coefficient and the other two AC coefficients are only altered if they do not satisfy the watermark embedding condition. As a result, less distortion is introduced into the watermarked images.

(vii) Consideration of the local properties of feature points to detect the watermark even when some features are cropped. Experimental results support the conclusion that the proposed algorithm improves over existing benchmarks in terms of watermark imperceptibility and robustness to common signal processing attacks and geometrical attacks including rotation, cropping translation, row and column removal, shearing, and linear geometric transformation attacks.

7.4 Further Work

The work presented in this thesis provides some ideas for further research, which are summarized as follows:

1. As presented in Chapter 5, to achieve a better trade-off between imperceptible and robustness requirements, the watermark strength is determined by content analysis and classification of DCT blocks. The scheme is able to determine where the watermark strength should be strong and where the watermark strength should be weak. The performance of this scheme could be improved if the scheme determines the value of the watermark strength. This may be achieved by using the noise visibility functions (NVF) to adjust the watermark strength [134]. The value of the watermark strength may be determined according to predefined threshold and SSIM value for each block. As a result of this suggestion, the scheme will be able to determine appropriate values of watermark strength for different images.

2. As mentioned in Chapter 6, a secret key is utilized for selecting the locations for embedding the watermark bits, which are embedded in the specified coefficients. The security of this scheme can be further improved. One suggestion is to use

chaotic maps to relocate the pixels in an image [36]. For each extracted sub-image, a chaotic map should be used to shuffle the locations of pixels. Then the embedding process is applied as described in Chapter 6. As a result, it would be impractical for an attacker to find the locations of the watermark.

3. The fact is that more robustness can be achieved if the watermark is embedded into significant coefficients. However, the number of theses coefficients is limited in transformed images. Therefore, a block-based chaotic map may be used as suggested in [57] to increase the number of these coefficients in the transformed image.

4. To increase to the watermark capacity of the proposed scheme in Chapter 6, the middle frequency may be used to embed more bits. However, a trade-off between the robustness and capacity requirement should be considered.

5. The work presented in Chapter 5 and 6 may be extended to video watermarking use.

6. The algorithm presented in Chapter 4 may be modified to be a blind algorithm, in which the original host image is not required in the extraction process.

7. The algorithms presented in chapters 5 and 6 can be extended to be used for colour images. The watermark may be embedded into the blue channel of the host image since the human eye is least sensitive to modification in this channel or in the luminance component Y in YIQ space.

REFERENCES

[1] L. M. Marvel, C. G. Boncelet, Jr., and C. T. Retter, "Spread spectrum image steganography," *IEEE Transactions on Image Processing* vol. 8 (8), pp. 1075-1083, 1999.

[2] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding-a survey," *Proceedings of the IEEE*, vol. 87(7), pp. 1062-1078, 1999.

[3] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proceedings of the IEEE*, vol. 87(7), pp. 1079-1107, 1999.

[4] I. J. Cox, M. L. Miller, and J. A. Bloom, "Watermarking applications and their properties," in *Int. Conf. On information Technology*, M. L. Miller, Ed., 2000, pp. 6-10.

[5] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data. A state-of-the-art overview," *Signal Processing Magazine, IEEE*, vol. 17, pp. 20-46, 2000.

[6] F. A. P. Petitcolas, "Watermarking schemes evaluation," *I.E.E.E. Signal Processing*, vol. 17(5), pp. 58–64, 2000.

[7] H. Guoa, Y. Lib, A. Liua, and S. Jajodia, "A fragile watermarking scheme for detecting malicious modifications of database relations " *Information Sciences (Elsevier)*, vol. 176(10), pp. 1350-1378, 2006.

[8] C. De Vleeschouwer, J. F. Delaigle, and B. Macq, "Invisibility and application functionalities in perceptual watermarking an overview," *Proceedings of the IEEE*, vol. 90, pp. 64-77, 2002.

[9] S. Craver, N. Memon, B.-L. Yeo, and M. Yeung, "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks, and Implications," *IEEE Journal on Selected Areas in Communications*, vol. 16(4), pp. 573-586, 1998.

[10] J. O. Ruanaidh, W. J. Dowling, and F. M. Boland, "Watermarking digital images for copyright protection," *IEE Proceedings on Vision, Signal and Image Processing*, vol. 143(4), pp. 250-256, 1996.

[11] K. Zebbiche, F. Khelifi, and A. Bouridane, "An Efficient Watermarking Technique for the Protection of Fingerprint Images," *EURASIP Journal on Information Security*, vol. 2008, Article ID 918601, 20 pages, 2008. doi:10.1155/2008/918601.

[12] Z. Wenwu, X. Zixiang, and Z. Ya-Qin, "Multiresolution watermarking for images and video," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 9(4), pp. 545-550, 1999.

[13] V. M. Potdar, S. Han, and E. Chang, "A survey of digital image watermarking techniques," in *3rd IEEE International Conference on Industrial Informatics, INDIN '05*, 2005, pp. 709-716.

[14] C. K. Chui, *Introduction to Wavelets*: Academic Press, San Diego, 1992.

[15] A. Oppenheim and R. Schafer, *Discrete-Time Signal Processing*: Prentice Hall, Englewood Cliffs, NJ, 1989.

[16] K. R. Rao and P. Yip, *Discrete cosine transform: algorithms, advantages, applications*: Academic Press, London, UK, 1990.

[17] R. Gonzalez and R. Woods, *Digital Image Processing*: Addison Wesley, Reading, MA, 1992.

[18] Z. Wang, A. C. Bovik, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13(4), pp. 600-612, 2004.

[19] F. Peticolas, R. Anderson, and M. Kuhn, "Attacks on copyright marking system," in *the second work shop information hiding, Portland.*, 1998, pp. 218-238.

[20] G. Voyatzis, N. Nikolaidis, and I. Pitas, "Digital Watermarking: An overview," in *IX European Signal Processing Conference (EUSIPCO'98)*, vol. I, 1998, pp. 9-12.

[21] H. Chiou-Ting and W. Ja-Ling, "Hidden signatures in images," in *International Conference on Image Processing ICIP'96*, vol. 3, 1996, pp. 223-226

[22] I. Cox and L. Miller, "A review of watermarking and importance of perceptual modelling," in *SPIE Conference on Human Vision and Electronic Imaging II*, vol. 3016, 1997, pp. 92-99.

[23] H. Yuan and X. P. Zhang, "Fragile watermark based on the Gaussian mixture model in the wavelet domain for image authentication," in *Proceedings International Conference on Image Processing, ICIP 2003*, vol. 1, 2003, pp. 505-508

[24] L. Ching-Yung and C. Shih-Fu, "A robust image authentication method distinguishing JPEG compression from malicious manipulation," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 11(2), pp. 153-168, 2001.

[25] M. M. I.J. Cox, J-P. Linnartz, and T. Kalker, "A Review of Watermarking Principles and Practices," *Digital Signal Processing for Multimedia Systems*, pp. 461-485, 1999.

[26] C.-T. L. a. F. M. Yang, "One-dimensional Neighbourhood Forming Strategy for Fragile Watermarking," *Journal of Electronic Imaging*, vol. 12, pp. 284-291, 2003.

[27] S. D. Servetto, C. I. Podilchuk, and K. Ramchandran, "Capacity issues in digital image watermarking," in *Proceedings International Conference on Image Processing, ICIP 98* vol. 1, 1998, pp. 445-449

[28] F. Zhang, X. Zhang, and H. b. Zhang, "Digital image watermarking capacity and detection rate," *Pattern Recognition Letters*, vol. 28(1), pp. 1-10, 2007.

[29] C. I. Podilchuk and E. J. Delp, "Digital watermarking: algorithms and applications," *Signal Processing Magazine, IEEE*, vol. 18, pp. 33-46, 2001.

[30] Y. K. Lee and L. H. Chen, "High capacity image steganographic model," in *IEE Proceedings - Vision, Image and Signal Processing*, vol. 147, 2000, pp. 288-294.

[31] R. Schyndel, A. Tirkel, and C. Osborne, "A Digital Watermark," in *Proc. IEEE Int. Conf. on Image Processing*, vol. 2, 1994, pp. 86-90.

[32] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for Data Hiding," *IBM System Journal*, vol. 35(3&4), pp. 313-336, 1996.

[33] N. Nikolaidis and I. Pitas, "Copyright protection of images using robust digital signatures," in *IEEE International Conference on Acoustics, Speech, and Signal Processing* vol. 4, 1996, pp. 2168-2171.

[34] K. Matsui and K. Tanaka, "Video-Steganography: How to Embed a Signature in a picture," in *Proceedings of IMA Intellectual Property*, vol. 1, 1994, pp. 187-206.

[35] H. Min-Shiang, C. Chin-Chen, and H. Kuo-Feng, "A watermarking technique based on one-way hash functions," *IEEE Transactions on Consumer Electronics*, vol. 45(2), pp. 286-294, 1999.

[36] G. Voyatzis and I. Pitas, "Applications of toral automorphisms in image watermarking," in *International Conference on Image Processing*, vol. 1, 1996, pp. 237-240

[37] C. Chang, J. Hsiao, and C. Chiang, "An Image Copyright Protection Scheme Based on Torus Automorphism," in *First International Symposium on Cyber Worlds* 2002, pp. 217.

[38] C.-C. Chang and P.-Y. Lin, "Adaptive watermark mechanism for rightful ownership protection," *Journal of Systems and Software*, vol. 81, pp. 1118-1129, 2008.

[39] X. Wu and Z.-H. Guan, "A novel digital watermark algorithm based on chaotic maps," in *Physics Letters A*, vol. 365, 2007, pp. 403-406.

[40] V.Darmstaedter, J.F.Delaigle, J. J. Quisquater, and B. B.Macq, "Low cost spatial watermarking," *Computer and Graphics*, vol. 22(4), pp. 417-424, 1998.

[41] L. Chang-Hsing and L. Yeuan-Kuen, "An adaptive digital image watermarking technique for copyright protection," *IEEE Transactions on Consumer Electronics*, vol. 45(4), pp. 1005-1015, 1999.

[42] S. Kimpan, A. Lasakul, and S. Chitwong, "Variable block size based adaptive watermarking in spatial domain," in *IEEE International Symposium on Communications and Information Technology*, vol. 1, 2004, pp. 374-377

[43] P.-L. Lin, "Robust transparent image watermarking system with spatial mechanisms," *Journal of Systems and Software* vol. 50(2), pp. 107-116, 2000.

[44] M. Ramkumar, A. N. Akansu, and A. A. Alatan, "A robust data hiding scheme for images using DFT," in *International Conference on Image Processing*, vol. 2, 1999, pp. 211-215

[45] I. J. Cox, J. Kilian, F. T. Leighton, and T. A. S. T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6(12), pp. 1673-1687, 1997.

[46] P. Meerwald and A. Uhl, "A survey of wavelet-domain watermarking algorithms," in *Proceedings of SPIE, Electronic Imaging, Conference on Security and Watermarking of Multimedia Contents III*, vol. 4314, 2001, pp. 505-516.

[47] H. Xi-Ping and Z. Qing-Sheng, "A Robust Wavelet-Domain Watermarking Algorithm for Color Image," in *International Conference on Machine Learning and Cybernetics*, 2006, pp. 3940-3943.

[48] I. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *Technical report 95-10, NEC Research Institute*, 1995.

[49] I. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for images, audio and video," in *International Conference on Image Processing*, vol. III, 1996, pp. 243-246.

[50] E. Koch and J. Zhao, "Towards robust and hidden image copyright labeling," in *IEEE Nonlinear Signal Processing Workshop*, 1995, pp. 452-455.

[51] S. Craver, N. Memon, B. Yeo, and M. Yeung, "On the invertibility of invisible watermarking techniques," in *International Conference on Image Processing ICIP* vol. 1, 1997, pp. 540-543.

[52] H. Chiou-Ting and W. Ja-Ling, "Hidden digital watermarks in images," *IEEE Transactions on Image Processing*, vol. 8(1), pp. 58-68, 1999.

[53] S. D. Lin and C.-F. Chen, "A robust DCT-based watermarking for copyright protection," in *International Conference on Consumer Electronics*, vol. 46, 2000, pp. 415-421.

[54] C. M. Kung, J. H. Jeng, and T. K. Truong, "Watermark technique using frequency domain," in *14th International Conference on Digital Signal Processing*, vol. 2, 2002, pp. 729-731

[55] S. D. Lin, S. Shih-Chieh, and G. Han Yi, "Improving the robustness of DCT-based image watermarking against JPEG compression," in. *International Conference on Consumer Electronics, ICCE*, 2005, pp. 343-344.

[56] H. Zhou, C. Qi, and X. Gao, "Low Luminance Smooth Blocks Based Watermarking Scheme in DCT Domain," in *International Conference on Communications, Circuits and Systems*, vol. 1, 2006, pp. 19-23.

[57] Y.-T. Wu and F. Y. Shih, "Digital watermarking based on chaotic map and reference register," *Pattern Recognition* vol. 40(12), pp. 3753-3736, 2007.

[58] H. Chion-Ting and W. Ja-Ling, "Multiresolution watermarking for digital images," *IEEE Transactions on Circuits and Systems II*, vol. 45 (8), pp. 1097-1101, 1998.

[59] R. Dugad, K. Ratakonda, and N. Ahuja, "A new wavelet-based scheme for watermarking images," in *International Conference on Image Processing*, vol. 2, 1998, pp. 419-423

[60] H. Inoue, A. Miyazaki, A. Yamamoto, and T. A. K. T. Katsura, "A digital watermark based on the wavelet transform and its robustness on image compression," in *International Conference on Image Processing*, vol. 2, 1998, pp. 391-395

[61] Z. Dawei, C. Guanrong, and L. Wenbo, "A chaos-based robust wavelet-domain watermarking algorithm," *Chaos, Solitons & Fractals*, vol. 22(1), pp. 47-54, 2004.

[62] Y. Wang, J. F. Doherty, and R. E. Van Dyck, "A wavelet-based watermarking algorithm for ownership verification of digital images," *IEEE Transactions on Image Processing*, vol. 11(2), pp. 77-88, 2002.

[63] W. Dietl, P. Meerwald, and A. Uhl, "Protection of wavelet-based watermarking systems using filter parametrization," *Signal Processing* vol. 83(10), pp. 2095-2116, 2003.

[64] C. Yueh-Hong, S. Jun-Min, H. C. Fu, H. Hsiang-Cheh, and P. Hsiao-Tien, "Adaptive watermarking using relationships between wavelet coefficients," in *IEEE International Symposium on Circuits and Systems*, vol. 5, 2005, pp. 4979-4982

[65] S. Agreste, G. Andaloro, D. Prestipino, and L. Puccio, "An image adaptive, wavelet-based watermarking of digital images," *Journal of Computational and Applied Mathematics* vol. 210(1&2), pp. 13-21, 2007.

[66] D. Kundur and D. Hatzinakos, "Digital watermarking using multiresolution wavelet decomposition," in *IEEE International Conference on Acoustics, Speech and Signal Processing*, vol. 5, 1998, pp. 2969-2972

[67] X. Gui and S. Hong, "Robust wavelet-based blind image watermarking against geometrical attacks," in *IEEE International Conference on Multimedia and Expo* vol. 3, 2004, pp. 2051-2054

[68] H. Jiwu, Y. Q. Shi, and S. Yi, "Embedding image watermarks in dc components," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 10(6), pp. 974-979, 2000.

[69] E. E. Abdallah, A. B. Hamza, and P. Bhattacharya, "A robust block-based image watermarking scheme using fast Hadamard transform and singular value decomposition," in *18th International Conference on Pattern Recognition* vol. 3, 2006, pp. 673-676.

[70] I. W. A. a. P. Sweeney, "Robust and transparent image watermarking resilient to random geometric attack," in *IASTED Int. Conf. on Signal processing, Pattern Recognition & Applications*, 2002, pp. 438-443.

[71] P. S. Huang, C. S. Chiang, C. P. Chang, and T. M. Tu, "Robust spatial watermarking technique for colour images via direct saturation adjustment," *IEE Proceedings -Vision, Image and Signal Processing*, vol. 152 (5), pp. 561-574, 2005.

[72] J. J. Chae, D. Mukherjee, and B. S. Manjunath, "A robust data hiding technique using multidimensional lattices," in *IEEE International Forum on Research and Technology Advanced in Digital Libraries,ADL98*, 1998, pp. 319-326.

[73] J. Chae, D. Mukherjee, and B. Manjunath, "A robust embedded data from wavelet coefficients," in *SPIE, Electronic Image, Storage and Retrieval for Image and video Database*, vol. 3312, 1998, pp. 308-317.

[74] D. Kundur and D. Hatzinakos, "Toward robust logo watermarking using multiresolution image fusion principles," *IEEE Transactions on Multimedia*, vol. 6(1), pp. 185-198, 2004.

[75] A. A. Reddy and B. N. Chatterji, "A new wavelet based logo-watermarking scheme," *Pattern Recognition Letters*, vol. 26(7), pp. 1019-1027, 2005.

[76] L.-H. Chen and J.-J. Lin, "Mean quantization based image watermarking," *Image and Vision Computing*, vol. 21(8), pp. 717-727, 2003.

[77] M. S. Raval and P. P. Rege, "Discrete wavelet transform based multiple watermarking scheme," in *Conference on Convergent Technologies for Asia-Pacific Region*, vol. 3, 2003, pp. 935-938

[78] L. M. Cheng, L. L. Cheng, C. K. Chan, and K. W. Ng, "Digital watermarking based on frequency random position insertion," in *Control, Automation, Robotics and Vision Conference* vol. 2, 2004, pp. 977-982

[79] L. Chun-Shien, H. Shih-Kun, S. Chwen-Jye, and L. Hong-Yuan Mark, "Cocktail watermarking for digital image protection," *IEEE Transactions on Multimedia*, vol. 2(4), pp. 209-224, 2000.

[80] E. Ganic, S. D. Dexter, and A. M. Eskicioglu, "Embedding multiple watermarks in the DFT domain using low- and high-frequency bands " in *Security, Steganography, and Watermarking of Multimedia Contents VII,SPIE*, vol. 5681, 2005, pp. 175-184.

[81] P. Tao and A. M. Eskicioglu, "A robust multiple watermarking scheme in the discrete wavelet transform domain," in *Conference on Internet Multimedia Management Systems V*, vol. 5601, 2004, pp. 133-144.

[82] C. Jin, T. Su, and L.-G. Pan, "Multiple Digital Watermarking Scheme Based on ICA," in *Eighth International Workshop on Image Analysis for Multimedia Interactive Services*, 2007, pp. 70-70.

[83] G. Fan, L. Zhe-Ming, and P. Jeng-Shyang, "Multipurpose image watermarking in DCT domain using subsampling," in *IEEE International Symposium on Circuits and Systems*, vol. 5, 2005, pp. 4417-4420

[84] R. Bangaleea and H. C. S. Rughooputh, "Performance improvement of spread spectrum spatial-domain watermarking scheme through diversity and attack characterisation," in *6th IEEE AFRICON*, vol. 1, 2002, pp. 293-298

[85] P. Campisi, M. Carli, G. Giunta, and A. Neri, "Blind quality assessment system for multimedia communication using tracing watermarking," *IEEE Transactions on Signal Processing*, vol. 51(4), pp. 996-1002, 2003.

[86] W. C. Chu, "DCT-based image watermarking using subsampling," in *IEEE Transactions on Multimedia*, vol. 5, 2003, pp. 34-38.

[87] T. Min-Jen and H. Hsiao-Ying, "DCT and DWT-based image watermarking by using subsampling," in *24th International Conference on Distributed Computing Systems Workshops*, vol. 7, 2004, pp. 184-189.

[88] F. Yonggang, S. Ruimin, and S. Liping, "Robust image watermarking scheme based on subsampling," in *Third International Conference on Information Technology and Applications* vol. 2, 2005, pp. 361-365

[89] W. Lu, H. Lu, and F.-L. Chung, "Novel robust image watermarking using difference correlation detector," *Computer Standards & Interfaces*, vol. 29, pp. 132-137, 2007.

[90] W. Lu, H. Lu, and F.-L. Chung, "Robust digital image watermarking based on subsampling," *Applied Mathematics and Computation*, vol. 181, pp. 886-893, 2006.

[91] S. Pereira, J. J. K. O. Ruanaidh, F. Deguillaume, G. Csurka, and T. Pun, "Template based recovery of Fourier-based watermarks using log-polar and log-log maps," in *IEEE Int. Conf. on Multimedia Computing Systems*, vol. 1, 1999, pp. 870-874

[92] S. Pereira and T. Pun, "Robust template matching for affine resistant image watermarks," *IEEE Transactions on Image Processing*, vol. 9(6), pp. 1123-1129, 2000.

[93] X. Kang, J. Huang, Y. Q. Shi, and Y. Lin, "A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13(8), pp. 776-786, 2003.

[94] J. L. Dugelay, S. Roche, C. Rey, and G. Doerr, "Still-image watermarking robust to local geometric distortions," *IEEE Transactions on Image Processing*, vol. 15(9), pp. 2831-2842, 2006.

[95] M. Kutter, "Watermarking Resisting to Translation, Rotation, and Scaling " in *Proc. SPIE Multimedia Systems. Applications*, vol. 3528, 1998, pp. 423-431.

[96] A. Herrigel, S. Voloshynovskiy, and Y. B. Rytsar, "Watermark template attack," in *Proc. Of SPIE Security and Watermarking of Multimedia Contents III*, vol. 4314, 2001, pp. 394-405.

[97] J.J.K. O'Ruanaidh and R. T. Pun, "Rotation, scale, and translation invariant digital image watermarking," in *Proc. IEEE Int. Conf. on Image Processing*, 1997, pp. 536-539.

[98] J.J.K. O'Ruanaidh and T. Pun, "Rotation, scale, and translation invariant spread spectrum digital image watermarking," *Signal Processing*, vol. 66(3), pp. 303-317, 1998.

[99] D. Zheng, J. Zhao, and A. E. Saddik, "RST-invariant digital correlation," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13(8), pp. 753-765, 2003.

[100] C.Y. Lin, M. Wu, J.A. Bloom, I.J. Cox, M. L. Miller, and Y. M. Lui, "Rotation, scale, and translation resilient watermarking for images," *IEEE Transactions on Image Processing*, vol. 10(5), pp. 767-782, 2001.

[101] M. Alghoniemy and A. H. Tewfik, "Geometric invariant in image watermarking," *IEEE Transactions on Image Processing*, vol. 13(2), pp. 145-153, 2004.

[102] P. Dong, J.G. Brankov, N.P. Galatsanos, Y. Y. Yang, and F. Davoine, "Affine transformation resistant watermarking based on image normalization," *IEEE Transactions on Image Processing*, vol. 14(12), 2005.

[103] M. Alghoniemy and A. H. Tewfik, "Geometric distortion correction through image normalization," in *Proc. Of IEEE Int. Conf. Multimedia Expo*, vol. 3, 2000, pp. 1291-1294

[104] H.S. Kim and H. K. Lee, "Invariant image watermarking using Zernike moments," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13(8), pp. 766-775, 2003.

[105] D. Coltuc and P. Bolon, "Watermarking by histogram specification," in *Proc. SPIE Security Watermarking of Multimedia Contents II*, vol. 3657, 1999, pp. 252-263.

[106] D. Coltuc, P. Bolon, and J. M. Chassery, "Fragile and robust watermarking by histogram specification," in *Proc. SPIE Security Watermarking of Multimedia Contents IV*, vol. 4675, 2002, pp. 701-710.

[107] S. Roy and E. C. Chang, "Watermarking color histograms," in *International Conf. on Image Process*, 2004, pp. 2191-2194.

[108] S. Xiang, H. Joong, and J. Huang, "Invariant Image Watermarking based on statistical features in low-frequency domain," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 18(6), pp. 777-789, 2008.

[109] M. Kutter, S. K. Bhattacharjee, and T. Ebrahimi, "Toward second generation watermarking schemes," in *IEEE Int. Conf. on Image Processing*, vol. 1, 1999, pp. 320-323.

[110] P. Bas, J.M. Chassery, and B. Macq, "Geometrically invariant watermarking using feature points," *IEEE Transactions on Image Processing*, vol. 11(9), pp. 1014-1028, 2002.

[111] C.W. Tang and H. M. Hang, "A feature-based robust digital image watermarking scheme," *IEEE Transactions on Signal Processing*, vol. 51(4), pp. 950-959, 2003.

[112] H.Y. Lee, H. Kim, and H. K. Lee, "Robust image watermarking using local invariant features," *Optical Engineering*, vol. 45(3), pp. 037002(1-11), 2006.

[113] X. Qi and J. Qi, "A robust content-based digital image watermarking scheme," *Signal Processing, Elsevier*, vol. 87(6), pp. 1264-1280, 2007.

[114] L.-D. Li and B.-L. Guo, "Localized image watermarking in spatial domain resistant to geometric attacks " *AEU - International Journal of Electronics and Communications, Elsevier.* , vol. 63(2), pp. 123-131 2009.

[115] K. I. Hashida and S. A., "A method of embedding robust watermarks into digital color images," *IEICE Transactions Fundamentals*, vol. E81-A(10), pp. 2133-2137, 1998.

[116] N. Nikolaidis and I. Pitas, "Robust image watermarking in spatial domain," *Signal Processing*, vol. 66(3), pp. 385-403, 1998.

[117] M. Kutter, F. Jordan, and F. Bossen, "Digital watermarking of color images using amplitude modulation," *Journal of Electronic Imaging*, vol. 7, pp. 326-332, 1998.

[118] L. Lian-Shan, L. Ren-Hou, and G. Qi, "A new watermarking method based on DWT green component of color image," in *International Conference on Machine Learning and Cybernetics*, vol. 6, 2004, pp. 3949-3954

[119] D. Fleet and D. Heeger, "Embedding invisible information in color images," in *IEEE Int. Conf. on Image Processing ICIP'97*, vol. 1, 1997, pp. 532-535.

[120] M. Barni, F. Bartolini, and A. Piva, "Multichannel watermarking of color images," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 12(3), pp. 142-156, 2002.

[121] P. Tsai, Y. C. Hu, and C. C. Chang, "A color image watermarking scheme based on color quantization," *Signal Processing*, pp. 95-105, 2004.

[122] M. Kutter and S. Winkler, "A vision-based masking model for spread-spectrum image watermarking," *IEEE Transactions on Image Processing*, vol. 11(1), pp. 16-25, 2002.

[123] B. Verma, S. Jain, D. P. Agarwal, and A. Phadikar, "A New color image watermarking scheme," *Infocomp, Journal of computer science*, vol. 5(2), pp. 37-42, 2006.

[124] K. Hueske, J. Geldmacher, and J. Gotz, "Adaptive decoding of convolutional codes," *Advanced in radio science*, vol. 5, pp. 209-214, 2007.

[125] H. Qi, D. Zheng, and J. Zhao, "Human visual system based adaptive digital image watermarking," *Signal Processing*, vol. 88(1), pp. 174-188, 2008.

[126] J. N. Ellinas, "A Robust Wavelet-Based Watermarking Algorithm Using Edge Detection," in *World Academy of Science, Engineering and Technology*, vol. 25, 2007.

[127] J. F. Delaigle, C. D. Vleeschouwer, and B. Macq, "Watermarking algorithm based on a human visul model," *Signal processing* vol. 66(3), pp. 319-335, 1998.

[128] H. Qi, D. Zheng, and J. Zhao, "Human visual system based adaptive digital image watermarking," *Signal Processing*, vol. 88, pp. 174-188, 2008.

[129] K. K. H.S. Chang, "A compressed domain scheme for classification block edge patterns," *IEEE Transactions on Image Processing.*, vol. 14(2), pp. 145-151, 2005.

[130] J. Jiang, K. Qiu, and G. Xiao, "A block-edge-pattern based content descriptor in DCT domain," *IEEE Transactions on Circuits, Systems and Video Technology* vol. 18(7), pp. 994-998, 2008.

[131] V. Monga and B. Evans, "Perceptual Image Hashing Via Feature Points: Performance Evaluation and Tradeoffs," *IEEE Transactions on Image Processing*, vol. 15 (11), pp. 3452-3465, 2006.

[132] S.-C. Pei and C.-N. Lin, "Image Normalization for Pattern Recognition " *Image Vision Computing, Elsevier*, vol. 13(10), pp. 711-723 1995.

[133] S. Pereira, S. Voloshynovskiy, M. Madueño, S. Marchand-Maille, and T. Pun, "Second generation benchmarking and application oriented evaluation," in *the 4th International Workshop on Information Hiding* 2001, pp. 340 - 353

[134] S. Voloshynovskiy, A. Herrigel, N. Baumgaertner, and T. Pun, "A Stochastic Approach to Content Adaptive Digital Image Watermarking " in *International Workshop on Information Hiding, Lecture Note in Computer Science*, vol. LNCS 1768, 1999, pp. 212-236.