2004

Contextual biometric watermarking of fingerprint images

Nikhil C. Tungala
West Virginia University

CONTEXTUAL BIOMETRIC WATERMARKING OF FINGERPRINT IMAGES

Nikhil C Tungala

Thesis submitted to the
College of Engineering and Mineral Resources
at West Virginia University
in partial fulfillment of the requirements
for the degree of

Master of Science
in
Electrical Engineering

Afzel Noore, Ph.D., Chairman
Roy Nutter, Ph.D.
Powsiri Klinkhachorn, Ph.D.

Lane Department of Computer Science and Electrical Engineering
Morgantown, West Virginia
2004

Keywords: Digital Watermarking, Biometrics, Fingerprint Images, MDCT, DWT

ABSTRACT

CONTEXTUAL BIOMETRIC WATERMARKING OF FINGERPRINT IMAGES

Nikhil C Tungala

This research presents contextual digital watermarking techniques using face and demographic text data as multiple watermarks for protecting the evidentiary integrity of fingerprint image. The proposed techniques embed the watermarks into selected regions of fingerprint image in MDCT and DWT domains. A general image watermarking algorithm is developed to investigate the application of MDCT in the elimination of blocking artifacts. The application of MDCT has improved the performance of the watermarking technique compared to DCT. Experimental results show that modifications to fingerprint image are visually imperceptible and maintain the minutiae detail. The integrity of the fingerprint image is verified through high matching score obtained from the AFIS system. There is also a high degree of correlation between the embedded and extracted watermarks. The degree of similarity is computed using pixel-based metrics and human visual system metrics. It is useful for personal identification and establishing digital chain of custody. The results also show that the proposed watermarking technique is resilient to common image modifications that occur during electronic fingerprint transmission.

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my advisor, Prof. Afzel Noore, for his guidance, nurturing, encouragement, and support in every stage of my graduate study. His knowledge, kindness, patience, and vision have provided me with lifetime benefits. I am grateful to Dr. Klinkhachorn Powsiri and Dr. Nutter Roy, in my research committee for their valuable comments and suggestions on the drafts. I would also like to thank all faculty members of the LCSEE Department at West Virginia University for their academic guidance and encouragement.

I would like to thank my two sisters for their constant encouragement, prayers, moral support and patience during the course of my studies. I am so grateful to Vasudha for her encouragement and support during the years at West Virginia University. Special thanks to Lok, Reddy, Srinath, Vamsi, Kanth and Phani for their friendship and for the enjoyable discussions on a wide range of topics.

I must mention two persons without whose love, nurturing, and support I could never accomplish all these. I thank my mom for her care and encouragement toward the pursuit of excellence. I also thank my dad, not only for his patience and sacrifice, but also for being such a great role model for his son. I dedicate this research to my parents.

This research (Award No. 2003-RC-CX-K001) was supported by the Office of Science and Technology, National Institute of Justice, Office of Justice Program, and U. S. Department of Justice. I thank Max Houck for serving as a project monitor and Sagem Morpho for donating the AFIS system used in performing this research.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AFIS	Automated Finger Identification System
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
HVS	Human Visual System
IDWT	Inverse Discrete Wavelet Transform
IMDCT	Inverse Modified Discrete Cosine Transform
JPEG	Joint Photographic Experts Group
LSB	Least Significant Bit
MSE	Mean Square Error
MDCT	Modified Discrete Cosine Transform
NIST	National Institute of Standards and Techniques
PSNR	Peak Signal to Noise Ratio
SSIM	Structural Similarity Measure
TDAC	Time Domain Aliasing Cancellation
UIQI	Universal Image Quality Index

CHAPTER 1. INTRODUCTION

The prolific use of Internet has increased the concern for copyright protection of digital data. Publishers, artists, and photographers are unwilling to distribute their intellectual property over the Internet due to lack of adequate security. One reliable solution for copyright protection and enforcement mechanism is achieved through digital watermarking. The process of watermarking embeds a unique digital data into the host image that is to be protected. This information called the digital watermark can only be removed by the rightful owner. Watermarking has several significant applications such as copyright protection, broadcast monitoring, owner identification, transaction tracking, authentication, copy control and device control.

A number of watermarking techniques are available [1] for embedding information securely in an image. These can be broadly classified as transform domain techniques [2, 3] and spatial domain techniques [4, 5]. Recently watermarking techniques have been used in conjunction with biometric identifiers [6-8]. Fingerprints are one of the reliable biometric identifiers that are extensively used for personal identification. Pankanti and Yeung proposed a fragile invisible watermarking method for fingerprint image verification in spatial domain [9]. In this technique a binary watermark image is inserted into the fingerprint image pixels using a verification key at the scanner. The server detects any tampering of the image by recalling the key. The verification does not require the original image. Ratha, Connel, and Bolle proposed a blind data hiding method [10], which is applicable to fingerprint images compressed with WSQ (Wavelet-packet Scalar Quantization) standard. The watermark message is assumed to be very small compared to the fingerprint image. The Quantizer integer indices are randomly selected

and each watermark bit replaces the LSB of the selected coefficient. At the decoder, the LSB's of these coefficients are collected in the same random order to construct the watermark. Jain, Uludag, and Hsu used the facial information as watermark to authenticate the fingerprint image [11]. A bit stream of eigen face coefficients is embedded into selected fingerprint image pixels using a randomly generated secret key. The embedding process is in spatial domain and does not require the original image for extracting the watermark.

This research aims at developing a novel contextual digital watermarking technique using facial image and demographic text data as multiple watermarks for protecting the evidentiary integrity of the fingerprint image. The watermarked fingerprint is resistant to tampering, saves storage space, and seamlessly obtains pertinent information of the subject without the need to access disparate databases.

1.1 Organization of the Report

A brief summary of the topics covered in each chapter is presented below.

Chapter 2 introduces the basic concepts of digital watermarking and its properties. It then provides a survey of the research in the field of image watermarking and identifies some common image watermarking attacks. The specific goals of this research are defined.

Chapter 3 develops a general image watermarking technique in Modified Discrete Cosine Transformation (MDCT) domain. The elimination of blocking artifacts using MDCT is illustrated. The performance of the technique is evaluated using image quality metrics and the robustness is studied under various attacks.

Chapter 4 describes the basic elements of fingerprint image in personal identification. Next, two fingerprint image watermarking techniques in MDCT and Discrete Wavelet Transform (DWT) domains are presented. The matching ability of the watermarked fingerprints and original fingerprints is verified using an AFIS system. The ability of the proposed watermarking techniques to withstand various transformations during electronic transmission is studied and the performance of DCT, MDCT and DWT based techniques are evaluated.

Chapter 5 summarizes the research and discusses the future work in the field of biometric image watermarking.

CHAPTER 2. BACKGROUND AND GOALS

This chapter introduces the basic concept of digital watermarking and the properties that characterize the watermarking system. It presents a brief review and work done by researchers in the field of image watermarking. The common image watermarking attacks are also studied.

2.1 Digital Watermarking Model

Fig. 2.1 illustrates the basic elements of a simple watermarking system. The process is divided into two phases, *Embedding* and *Extraction*. The watermark information is embedded into the host data in the encoding stage to produce watermarked data. In the decoding stage the watermark information is extracted from the watermarked data. The extracted watermark is compared with the original watermark for authentication.

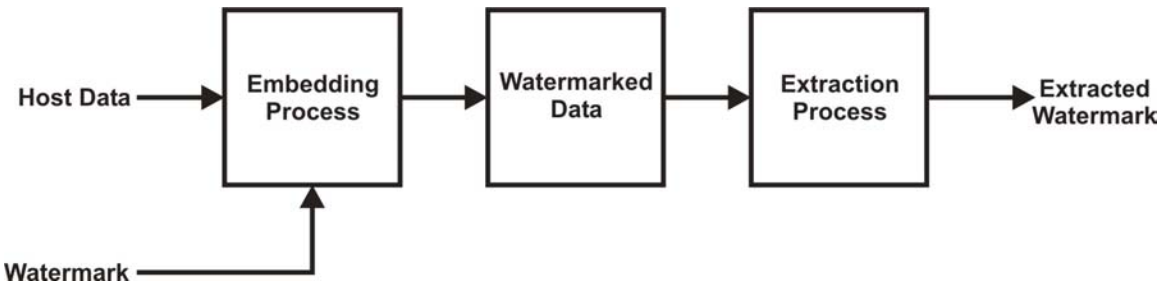


Fig. 2.1 General Watermarking Technique

A number of defining properties characterize the watermarking system depending on the application and purpose.

Imperceptibility: The degree of modification caused by embedding the watermark should be below the perceptible threshold, which is defined by the perceptibility criterion used.

Fidelity: The perceptual similarity measure between original and watermarked data.

Robustness: The ability to detect the watermarks after the watermarked data is subjected to various signal processing attacks is defined as robustness of the system.

Security: The embedded watermarks are said to be secure if they can resist the hostile attacks intended to thwart their purpose.

Blind or Informed Detection: Depending on the application, the original data is either required or not required for the recovery of watermark. The knowledge of original data makes the system more robust.

Data Payload: The number of bits a watermark encodes within a unit of time or within a work is called data payload.

Cipher and Watermark keys: Watermark keys are the secret keys used for embedding the message securely. In case of unauthorized detection without the secret key, the watermark information cannot be extracted

The relative importance of each property depends on the type of application environment. There are various types of watermarking based on the media content such as text watermarking, image watermarking, video watermarking and audio watermarking.

2.2 Literature Review

A significant progress in the watermarking research was made in mid-90's when several techniques were published in this area. In the early systems, the watermarking was modeled as a communication channel where the embedded data is treated as noise

[12]. In these systems the watermark is independent of the host data and the embedding process is known as blind embedding. Later on, the perceptual models [13, 14] were developed to maintain the trade-off between the fidelity and robustness. In these techniques, the watermark was modeled based on the content of the host data. These techniques are termed as informed embedding as the added information depends on the host data. With the introduction of communication with side information in watermarking [15, 16] watermarking techniques are more accurately modeled. Spread spectrum watermarking was introduced for the same purpose of maintaining the fidelity and robustness constraints [17]. The general spread spectrum communications spread the narrow band signal over wider frequency band. In case of spread spectrum watermarking even the weak watermark signals can be detected reliably. Cox *et al.* proposed the spread spectrum based watermarking algorithm [18] in which the host image is modulated with watermark data. The first 1000 largest magnitude DCT coefficients are treated as significant components to hide the information. The spread spectrum techniques are difficult to attack. To increase the data payload, the least significant bit (LSB) watermarking technique was introduced. These LSB based watermarking techniques [19] use grayscale images and logos as watermarks to enhance the authentication performance. Numerous techniques were introduced in recent years based on the application area and methodology. These watermarking techniques are traditionally classified into four main categories as shown in Fig 2.2 [17].

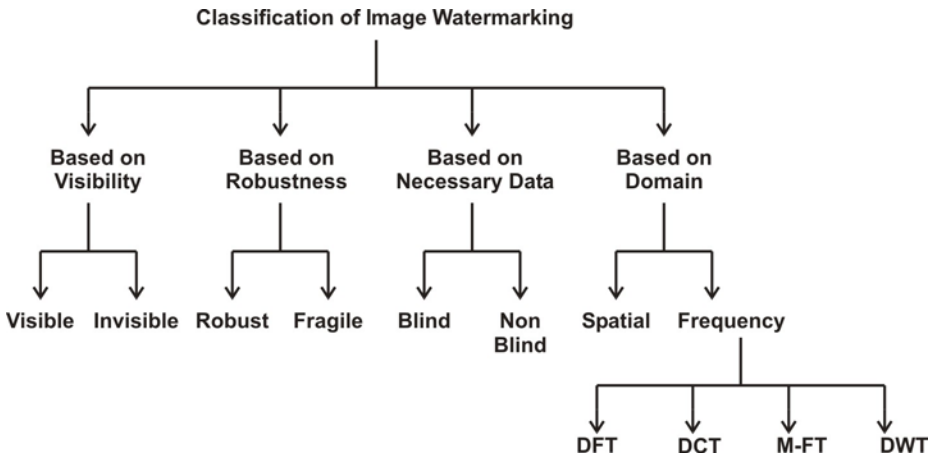


Fig. 2.2 Classification of Image Watermarking

2.2.1. Visible and invisible watermarking

In visible watermarking, the watermark (especially logo or trademark) is embedded in the host data by making it perceptible to the observer. Illicit removal of copyright information in visible watermarking is difficult and the embedding process is fast. The main drawback is degradation of original image quality. This technique is mainly used in logo and trademark applications. There are only few watermarking techniques in this field as the application area is limited. A wavelet domain visible watermarking technique based on the concepts of image fusion is presented in [20]. The modification of the host image wavelet coefficients is carried over by considering the global and local characteristics of both the host and watermark images. Another visible watermarking technique in DCT domain is proposed by Mohanty *et al.* [21].

In this method both the original and watermark images are transformed using 8 x 8 block Discrete Cosine Transformation (DCT). The computed signal to noise ratio proved that the watermarking technique preserved the integrity of the image. A human visual system based visible watermarking technique was presented in [22], which

modifies the host image DCT coefficients based on texture, edge and luminance information in each 8 x 8 block. Also the 8 x 8 blocks are classified into 8 different sensitivity classes based on robustness to attacks. Each class has its own watermarking strength factor for embedding information.

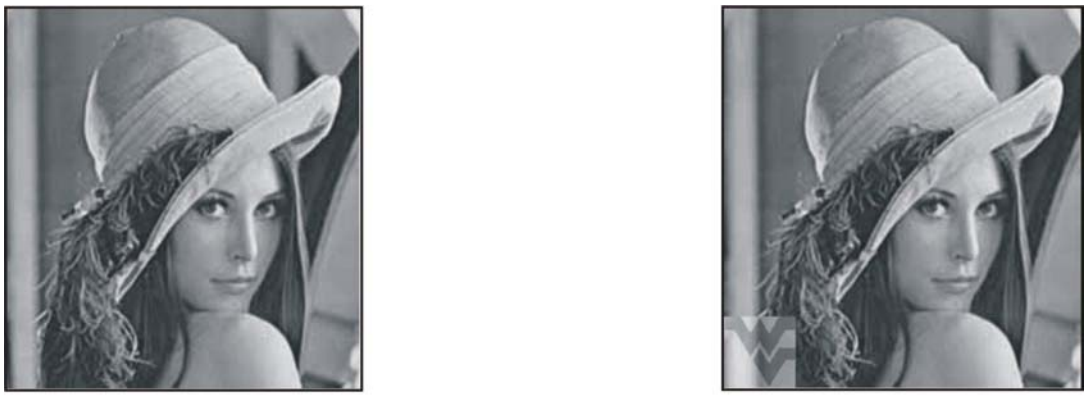


Fig. 2.3 (a) Invisible Watermarked and (b) Visible Watermarked images of Lena with West Virginia Logo

Invisible watermarking techniques aim at making the watermark imperceptible to human eye using mathematical techniques. They are used in most of the applications to preserve the quality of the original work. Human visual system characteristics are used in exploring the embedding features. A novel invisible data hiding technique in JPEG 2000 compressed domain was introduced in [23]. This steganographic technique employs a special mode of JPEG 2000 called *Lazy mode*. Data is embedded in selected magnitude refinement passes, except for the four most significant bit planes. This method of embedding is advantageous as the most significant bits act as a visual mask to make the modification of these subsequent bits less obvious. Higher data payload can be achieved using this technique.

The rest of the chapter concentrates only on the invisible watermarking systems and explores various embedding approaches.

2.2.2. Robust and fragile watermarking

In robust watermarking the embedded watermark should be resilient to various image processing manipulations. Any attempt to modify the embedded watermark should not hinder the detection process. A fragile watermark is characterized by its ability to detect the changes made to the original work. Modifications made to the original image will be reflected in the extracted watermark. The extracted watermark will render information regarding tampering and its location.

Watermarking techniques that are robust against geometrical attacks are presented in [24-26]. A double watermarking technique for detecting and subsequent classification of tampering is presented in [27]. This is a complex watermarking technique used for tamper detection. One watermark is inserted at the embedder and the other at the detector. The second watermark acts as a reference for comparing with the first watermark, which helps in understanding the nature of the attack. A new robust watermarking technique based on triplet wavelet coefficients is proposed by Quan *et al.* [28]. Triplet wavelet coefficients are defined as three different detailed orientations of a certain decomposition level. These coefficients are categorized into different classes according to watermark bit. The extraction process does not require the original image and the algorithm is robust against various image processing and malicious attacks.

Several fragile watermarking techniques are presented for image authentication [29-32]. One example of fragile watermarking algorithm is introduced by Roger *et al.*

based on subband coding technique. The embedding process is carried out by simply changing the LSB's of higher subband regions. Any manipulation to the original work is reflected in the extracted watermark and the areas of tampering can be identified. A singular value decomposition (SVD) [33] based technique is proposed to differentiate the type of tampering from JPEG compression. Fan *et al*. [34] presented an artificial neural network based fragile watermarking technique that identifies even slight modifications to the cover image. This technique also has the ability to locate and characterize the alterations. A fragile watermarking scheme based on the genetic model is proposed by Lee *et al.* [35]. The edge information is used as a measure to determine the quality of degradation between the original and watermarked image.

2.2.3. Blind and Non-Blind watermarking

A watermarking technique is said to be non-blind if only authorized persons can read the watermark. This type of technique requires some information from the embedding stage for extracting the watermark. While, blind watermarking techniques allow anyone to read the watermark. These techniques do not require the original work for watermark extraction. Blind watermarking techniques are widely accepted, as the original work is not required for extraction of the watermark.

Many existing watermarking schemes are non-blind watermarking techniques as they allow precise extraction of the watermark information compared to the blind watermarking schemes. A non-blind watermarking scheme based on discrete wavelet transform (DWT) is proposed by Xia *et al.* [36]. The watermark is modeled as Gaussian noise and is embedded in the middle and high frequency bands of the host image. Kundur

et al. proposed a robust watermarking technique [37] similar to the one proposed by Xia *et al*. According to the algorithm two different watermarks are embedded orthogonal to one another. A binary sequence generated from a pseudorandom generator is used as the actual watermark called the robust watermark. A reference watermark is produced which has similar statistical properties as that of the robust watermark. The main advantage of this method lies in the repetition of watermark in the image, which helps to overcome a broad class of degradations.

Two simple blind watermarking schemes are presented in [38] based on the lattice principle and property of periodic function respectively. These schemes eliminate the host data interfaces and reduces the storage cost. Tay *et al.* proposed a blind watermarking technique using 2-D discrete wavelet transform [39]. The mid frequency bands of the source image are embedded using a scaled watermarked image. A blind watermarking scheme that can detect malicious attacks is presented by Joachim *et al.* and Bernd *et al* [40]. This technique is based on Scalar Costa Scheme (SCS) that helps in extracting watermark information from small image regions.

2.2.4. Spatial and transformation domain watermarking

The earlier methods of watermarking were implemented in spatial domain without performing any transformations to the original image. The pixel values are directly altered for information embedding. These techniques withstand cropping and translation attacks but are weak against noise and compression attacks. Later with the advent of sophisticated transformation techniques the embedding process was carried out in frequency domain. The transformation techniques take into account the perceptual

criteria and compression phenomenon in the embedding process. In order to achieve the requirement of imperceptibility and robustness, the watermark is embedded into the frequency domain of the original image instead of the spatial domain.

Early research in spatial domain watermarking was performed using spread spectrum technique [41, 42]. On the same lines a new communication based approach using block codes and turbo codes to provide error protection against the attacks is presented in [43]. It has been shown that the turbo codes and block codes enhanced the performance of spread spectrum based technique in attack characterization. Nikolaidis *et al*. [44] presented a robust spatial domain watermarking technique by segmenting the image and locating regions that are robust to several image manipulations. Adaptive clustering is used to derive the robust region from the segmented image. Chaotic watermark is embedded on the boundary region of these ellipsoidal robust regions.

A complex watermarking technique that embeds watermark both in spatial and frequency domains is proposed in [45], which focuses on the extraction of watermark without the use of original images. A digital seal image is used as watermark and embedded in spatial and frequency domains without changing the embedding algorithm. Experimental results showed that watermarking in spatial domain is robust against distortions like blurring, and frequency domain embedding is robust against JPEG compression. W. N. Cheung presented a similar spatial domain watermarking technique, which also works equally in transform domain [46]. A binary logo is used as watermark and is embedded into the edge detail of the source image. The buyer authentication watermarking technique in spatial domain is presented in [47]. This technique can recover the watermark even if the attacker possessing the knowledge of watermarking

algorithm tries to modify the watermarked data. It is capable of surviving attacks in both spatial and frequency domains.

The following section describes the various watermarking techniques in transform domain. Generally DCT, DFT and DWT are used as the transformation techniques for decomposing image data. Other type of transforms such as Orthogonal transforms and Kalman transforms are also widely used.

Discrete Fourier Transform

This transformation domain provides the possibility of controlling the frequencies of the host signal. DFT also helps in embedding sufficient information into the host data maintaining good trade-off between visibility and robustness of the watermark. This transform is commonly used for performing phase modulation between the host and the watermark. A robust watermarking algorithm using phase modulation is presented in [48]. The phase components of the image have more psychovisual impact than magnitude components [49] and have better robustness against noise. Phase watermarking also resists changes in image contrast. The DFT components are selected for embedding if their energy is greater than a predefined threshold to make a significant impact on the image. The other important application of this transform is to split the images into perceptual bands. A human visual system based image watermarking technique was proposed by Delaigle *et al.* [50]. DFT helps in deriving various visual components. The spatial frequency is computed from the amplitude of DFT and the orientation is computed from the phase. The derived forms of this transform are Discrete Cosine Transform and Mellin- Fourier Transform.

Discrete Cosine Transform

A highly robust watermarking system against JPEG or MPEG compression can be achieved by embedding information in DCT domain. Visibility studies conducted in the field of source coding can be easily adapted to DCT based embedding. The DCT transform categorizes the frequency coefficients into high frequency, low frequency and mid frequency bands. A particular frequency band can be chosen depending upon the application area. Embedding in the low frequency bands makes the watermark perceptual to some extent but the watermark is robust against compression attack. Most of information in the high frequency components is lost in compression. But the watermark is highly imperceptible in the high frequency regions.

There are two different spread spectrum based embedding algorithms with 8 x 8 block DCT coefficients [51] and DCT applied to the entire image [52]. A human visual system based watermarking in DCT domain is introduced in [53] that uses the modulation transfer function of the human visual system (HVS) model to increase the invisibility of the embedded watermark. To improve the robustness of the inserted watermark, the watermark is sometimes embedded in DC component of the DCT as they have larger perceptual capacity than AC components [54]. Luminance and texture masking features of HVS are incorporated in this algorithm. A similar watermarking technique of embedding in DC components of binary images is proposed by Lu *et al.* [55]. The pre-processing and post-processing of binary images using biasing threshold is including in this algorithm to improve the embedding performance. A more effective watermarking technique is presented exploiting the zerotree characteristics for the selection of significant DCT coefficients [56]. The zerotree structure is used to rearrange

the wavelet structure DCT coefficients. This method of embedding is highly robust to compression and other attacks.

Mellin-Fourier Transform

This transform alleviates the problems caused due to affine geometrical manipulations applied to watermarked image. The phase of the DFT transform is translated to obtain this transform. The watermarking technique based on Mellin-Fourier transform was introduced by Ruanaidh *et al.* [57]. Log-polar mapping is used to make the watermark insensitive to rotation and zoom. The rotation and zoom transformations in Cartesian coordinate system are referred to translation in logarithmic and polar coordinate systems respectively. The LPM of an element (x, y) is defined as

$$(x, y) = \begin{cases} x = \exp p \cos\theta \\ y = \exp p \cos\theta \end{cases} \quad \text{with } p \in R \text{ and } \theta \in [0, 2\pi] \tag{2.1}$$

Thus rotation and zoom transformations can be transformed into translation and the translation invariance property of Mellin-Fourier transform can be used to detect the watermark accurately.

Wavelet Transform

The wavelet transform is gaining more and more importance with its implementation in JPEG2000 compression standard. Similar usage of DCT to JPEG compressed images motivated the use of wavelets for JPEG2000 compressed images. On the other hand, wavelets provided multiscale spatial frequency decomposition of image,

which helps in straightforward implementation of various human visual studies. A good knowledge of wavelet transform and its applications can be obtained from [58. With this transformation we can achieve image information at different scale resolutions and orientations. The high frequency sub-bands contain fine detail at three different orientations, while the low frequency sub-band contains the low-resolution approximation image with coarse detail. Other than these a wide range of discriminate image characteristics such as texture, luminance, and contrast can be obtained which helps in designing a robust and highly imperceptible image adaptive algorithm. A variety of techniques have been proposed using various decomposition levels and various filters like Haar, Daubechies and Bi-Orthogonal filters.

Early work [59] in the wavelet domain watermarking used low-resolution approximation image for embedding watermarks. Corvi *et al.* proposed a spread spectrum based watermarking technique [60], which places the watermark in the approximation image. Another technique of using approximation image for watermarking is presented by Xie *et al.* [61], which quantizes the median coefficient of 3 x 1 sliding window. Kim *et al.* [62] used all the subband discrete wavelet transform (DWT) coefficients to place the Gaussian random watermark data in the entire image. Kundur *et al.* selects three wavelet coefficients from three different detail subbands for embedding information [63]. The middle coefficient among the sorted triple coefficients is quantized to encode either zero or one based on the watermark. Peter Meerwald developed a blind watermarking technique in wavelet based JPEG2000 coding pipeline [64]. Quantization Index Modulation (QIM) is used to embed the watermark in the independent code blocks. This scheme is robust to compression and other image processing attacks.

2.3 Discussion

The above section presents an overview of digital watermarking and discusses several existing digital image watermarking techniques and their limitations. Some of the observations include spatial watermarking techniques can easily be implemented on any image without any subsequent processing. But in the context of robustness and visual quality of the watermarked image, transform domain techniques are better compared to spatial domain techniques. In transform domain, DCT domain techniques introduce blocking artifacts as they employ block based transformation methods. They produce watermarked images with moderate robustness, good capacity and low visual impact. Embedding in wavelet domain proved to be highly robust to compression and also noise. Today, we have highly sophisticated techniques that embed the watermark in wavelet domain.

2.4 Goals of this Research

The objectives of this research are:

1. Investigate the performance of a digital watermarking system in eliminating the blocking artifacts using MDCT.
2. Develop two contextual digital watermarking techniques using facial image and demographic text data as multiple watermarks for protecting the evidentiary integrity of fingerprint images.
3. Verify the matching ability of the watermarked fingerprint and the original fingerprint using the AFIS system.

4. Measure the correlation between the original and extracted watermarks using pixel based and human visual system (HVS) based metrics.
5. Study the ability of the watermark to withstand several image manipulations during electronic transmission and evaluate the performance comparison between DCT, MDCT and DWT based watermarking techniques.

CHAPTER 3. ELIMINATION OF BLOCKING ARTIFACTS IN DIGITAL WATERMARKING

In this chapter a new digital watermarking technique for JPEG still images in modified discrete cosine transformation (MDCT) domain is proposed. Most of the existing image and video watermarking algorithms use block transformations that introduce blocking artifacts causing perceptible distortions. MDCT has better coding performance compared to DCT and also the computational complexity of MDCT is reduced compared to wavelets. In this chapter, we investigate the use of MDCT in the digital watermarking with well known JPEG still images [65]. The method embeds the watermark into perceptual significant image features (such as lines and edges) in modified discrete transformation domain. The image features are obtained by using Phase congruency technique [66]. Unauthorized tampering on the watermarked image intended to remove the watermark will visibly distort the image. Experimental results show that the proposed approach produces highly imperceptible watermarked images when compared to traditional watermarking techniques. Moreover, the watermark is robust to attacks such as compression, noise, filtering and geometric transformations.

3.1. Blocking Artifacts

Several studies determined that humans are more sensitive to active areas of images containing strong edges than to uniform and highly detailed regions [67]. Human visual system responds greatly to edges and orientation. Humans can detect image content from line drawing and edge maps, but the interior of the object does not excite

the cells in the brain. So the coding algorithm should consider the activity level of the image and distribute the compression artifacts around the visually unimportant areas.

In general, information embedding systems use block-transformation techniques for coding the images. The block transformation based watermarking of images using DCT is simple and effective. The basic approach divides the image into blocks, typically of size 8 x 8. DCT is applied to these blocks and the transform coefficients are individually quantized. The watermark is embedded into the host image in transformation domain and inverse transformation is computed. This block transform watermarking process introduces a number of undesirable artifacts into the images; two kinds of reconstruction artifacts are typical in transform coefficients, mainly at low bit rates: blocking (or tiling) and ringing. Blocking artifacts arise because the concatenation of the reconstructed blocks generates signal discontinuities across block boundaries. Ringing artifacts arise because the quantization errors on the transform coefficients generate signal reconstruction errors that last for the entire block duration.

We explain this problem quantitatively [68] for one-dimension and then extend for two dimension images. Let '*a'* be any discrete time signal of length *N*. In any linear orthogonal transform such as discrete cosine transform (DCT) of length *N,* a *signal block* is a single N-length block. The resulting transform matrix C, consists of coefficients $c(n)$ corresponding to each signal block $a(n)$. If D is the basis function column matrix, then the coefficients are defined as $c(n) = D^T a(n)$. Therefore each coefficient block is a function of only the signal block at that position (n), and so adjacent coefficients are independent of each other.

After the data has been decorrelated, information that is not considered important about the transform coefficients is discarded. This is called irrelevancy. Watermark is embedded into this coded image and resulting coefficients are reconstructed by the inverse transformation using only the coefficients provided and setting the rest to zero. This produces low quality images. More specifically, the most noticeable artifacts called blocking artifacts are introduced. These artifacts manifest itself as an artificial boundary among the pixels of the adjacent blocks and constitute a serious bottleneck for many important visual communication applications.

To improve the performance of such transformation techniques coefficient blocks that correspond to non-independent, but overlapping signal blocks are generated. This is achieved by using Modified Discrete Cosine Transform (MDCT), which is similar to modulated lapped transform (MLT). These transforms perform Time Domain Aliasing Cancellation (TDAC), which is a good tool to analyze and synthesis signals [69]. Figs. 3.1 (b), (c) and (d) shows the edge maps of Lena image in Fig. 3.1 (a) using Canny edge detector. The difference in the edge maps of the original image and the image reconstructed from DCT transformation and MDCT transformation are shown in Figs. 3.1 (e) and (f) respectively. From Figs. 3.1 (e) and (f) we conclude that the MDCT helps in natural degradation of the images compared to DCT. Using MDCT for transformation of images seems to be very practical solution to eliminate blocking artifacts. Even at high bit rate one can expect smoothing effect to produce very high quality images.

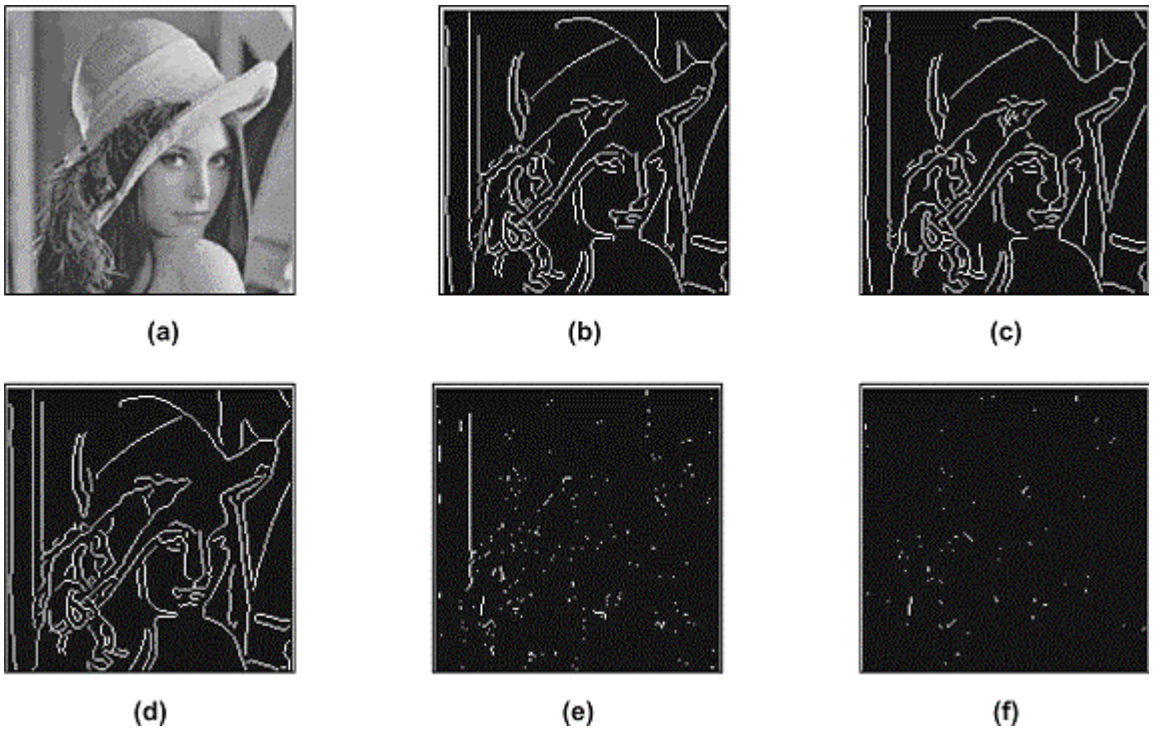


Fig. 3.1 (a) Original Lena Image, (b) Edge-map of Original Lena Image, (c) and (d) Edge-maps of Reconstructed Images using DCT and MDCT transformation respectively, (e) Difference between (b) and (c), and (f) Difference between (b) and (d)

3.2. Elimination of Blocking Artifacts

In this section, the properties of MDCT helpful in eliminating the blocking artifacts are studied. Let a be a one dimensional discrete time signal of length N that is segmented into n blocks denoted as a(n). Each block is assumed to consist of two parts, right and left half, denoted by a'(n) = [a_l'(n) a $_r'$(n)]. After the application of the MDCT transform, each signal block is left with l coefficients, where $l = 2n$. The adjacent blocks after the transformation overlap by l-n coefficients, which is equal to 50% overlap. There are n basis functions of length $2n$, so the transform operation does not produce any

increase in the data sample rate. The resulting transform matrix consists of coefficients that are given by $c(n) = B^T[a_r'(n-1)\ a_l'(n)\ a_r'(n)\ a_l'(n+1)]$, where B is the $2n$ x n matrix with basis functions as columns. Here the resulting coefficient blocks containing information not only about the $a(n)$ but also about $a_r(n-1)$ and $a_l(n+1)$, the corresponding adjacent signal blocks.

The implementation of MDCT on a sequence of data results in equal number of samples before and after the transformation. After performing inverse MDCT, no single block of data resembles the original data on which the transform is applied. When these blocks of data are concatenated after inverse transformation, the errors introduced by the transform cancel out due to the TDAC.

MDCT for a two dimensional array is defined as:

$$X(k,l) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} s(i,j)\ \cos\left[\frac{\pi}{N}(2k+1)(i+n)\right] \cos\left[\frac{\pi}{N}(2l+1)(j+1)\right] \tag{3.1}$$

where, $n = \frac{1}{2}\left(\frac{N}{2}+1\right)$

When it is implemented effectively with FFT algorithm and the coefficients are symmetrical,

$$\begin{aligned} x(k,l) &= x(N-k-1, N-l-1) \\ &= -x(k, N-l-1) \\ &= -x(N-k-1, l) \end{aligned} \tag{3.2}$$

This reduces the spectrum size from N^2 to $(n/2)^2$. The inverse MDCT is defined as

$$Y(k,l) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \frac{4}{N} s(i,j) \cos\left[\frac{\pi}{N}(2k+1)(i+n)\right] \cos\left[\frac{\pi}{N}(2l+1)(j+n)\right] \tag{3.3}$$

3.3. Proposed Watermarking Method

Phase congruency is a tool that helps in measuring the image features such as lines and edges and extracting them independent of the image intensity and contrast. In the proposed technique the image features of the host image are extracted using the phase congruency tool. The extracted line and edge features of the host image are transformed to MDCT domain. A binary image watermark is embedded into the MDCT coefficients of the host image features. The block diagram of the proposed method is shown in Fig. 3.2.

Let '*O*' be the original image and '*W*' be the watermark image.

$$O = \sum_{i=1}^{n} \sum_{j=1}^{m} \{O_{i,j}\} \tag{3.4}$$

where m and n are the length and width of the image coefficient matrix. Phase congruency of the host image is calculated and the image features are obtained.

$$P = Phase\{O\} \tag{3.5}$$

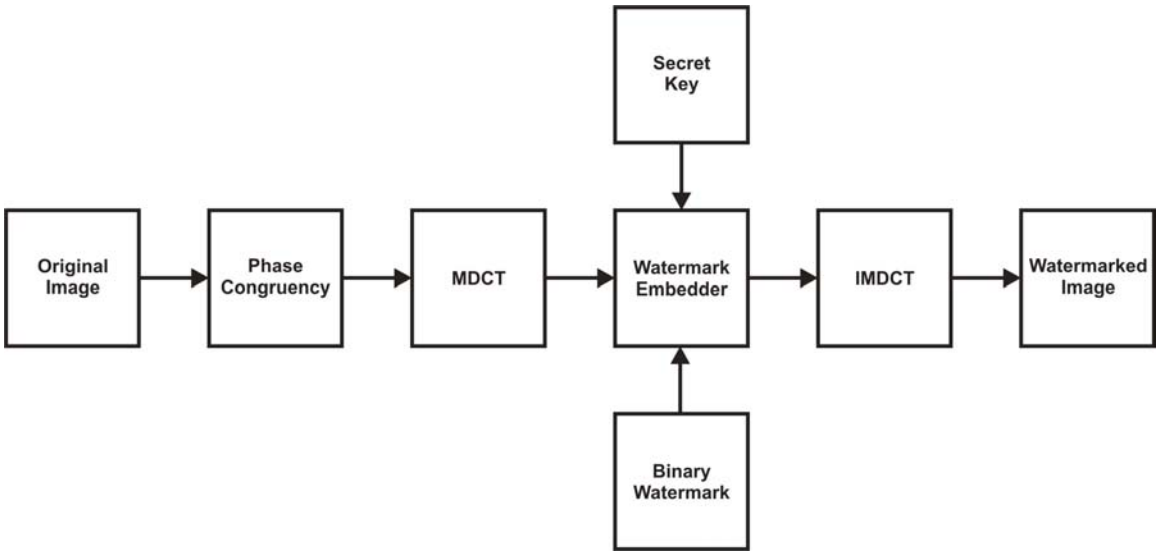


Fig. 3.2 Block Diagram of Proposed Embedding Algorithm

The coefficients corresponding to the image features are collected into a matrix F. This is obtained by selecting only the coefficients, which has a magnitude of 1.

$$F(r,s)=\sum_{i=1}^{n}\sum_{j=1}^{m} find\left\{P_{i,j}==1\right\} \tag{3.6}$$

The phase congruent image is then decomposed using the modified discrete cosine transform.

$$M = MDCT\left(F\right) \tag{3.7}$$

The size of the watermark image is adjusted to the size of the image feature matrix M, which is to be watermarked. The coefficients of the transformed matrix is

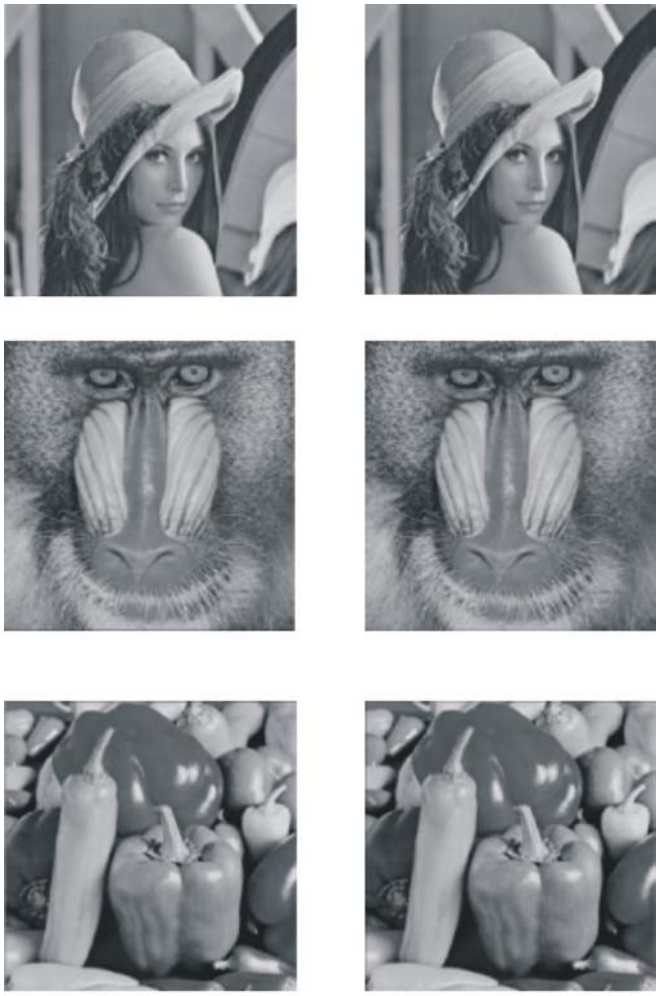
watermarked as shown in equation (3.8). A secret key is used for selecting the coefficients of the host image randomly.

$$S(r,s) = \sum_{i=1}^{r}\sum_{j=1}^{s} M(i,j) + \alpha * \sum_{i=1}^{r}\sum_{j=1}^{s} W(i,j) \tag{3.8}$$

α is the coefficient of watermarking strength. Coefficients i and j are randomly selected using a secret key. The watermarked coefficients (S) will replace the corresponding coefficients in the original image. Then inverse transform (IMDCT) is performed to obtain the watermarked image in spatial domain. This completes the embedding process. For extraction of the watermark, the reverse procedure of equation (3.8) is used. The secret key, α value, and the original image are needed for decoding the watermark. The extracted watermark is compared with the original watermark for verification.

3.4. Experimental Results

The proposed digital watermarking technique was tested on three JPEG test images Lena, Baboon and Peppers of size 512 x 512. Results in Fig. 3.3 show that the perceived quality of the watermarked images is very high. This is due to the significant reduction of the blocking artifacts. Also, the effect of the watermark on the images is hardly visible.



Original Image **Watermarked Image**

Fig. 3.3 Lena, Baboon and Pepper images watermarked using the proposed technique

The peak signal to noise ratio (PSNR) of the watermarked images test images is shown in Table 3.1. We can see that the watermark embedded by the proposed method is highly imperceptible compared to other known traditional watermarking techniques in different transformation domains [70-73].

Table 3.1 Performance comparison of invisibility

	Cox Method 1	Cox Method 2	Xia Method	Jong Method	Proposed Method
PSNR	51.36	42.43	50.12	52.46	56.01

The similarity between the original watermark and extracted watermark is calculated using the equation (3.9).

$$Sim\left(X, X'\right) = \frac{X \cdot X'}{\sqrt{X' \cdot X'}} / \frac{X \cdot X}{\sqrt{X \cdot X}} \times 100 \tag{3.9}$$

where X is original watermark and X' is the extracted watermark after the watermarked image has undergone different transformations.

The values obtained from the similarity equation is compared with those from the existing techniques. Fig. 3.4 shows that the proposed approach has high correlation between the original watermark and extracted watermark even after the watermarked image has undergone different transformations like JPEG compression at 70%, Gaussian noise, wavelet compression, cropping and salt and pepper noise and is superior compared to the traditional techniques.

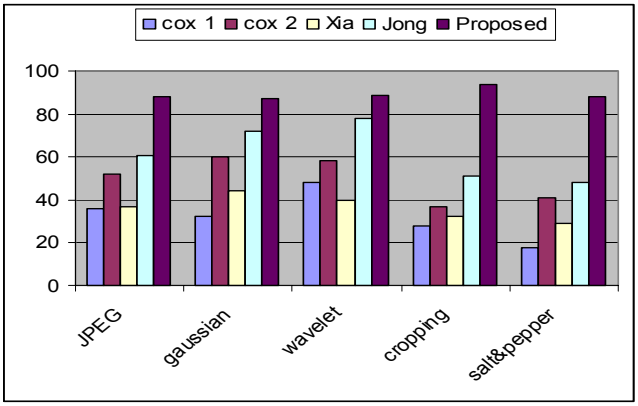


Fig. 3.4 Performance Comparison with existing techniques

The human visual system based (HVS) image quality metrics such as Structural Similarity Metric (SSIM) [74] and Universal Image Quality Index (UIQI) [75] are also used for measuring the similarity between original and watermarked images. Table 3.2 shows that there is no perceptible difference between the original and watermarked images and Table 3.3 shows that the extracted watermark from the attacked watermarked image closely resembles the original watermark image. The proposed method therefore produces imperceptible and robust watermark and the application of MDCT had improved the performance of the watermarking technique compared to DCT by eliminating the blocking artifacts.

Table 3.2 Visual Similarity of Original and Watermarked Images

Image	Structural Similarity Metric	Universal Image Quality Index
Lena	0.8760	0.9245
Baboon	0.8259	0.8411
Peppers	0.9031	0.9662

Table 3.3 Visual Similarity of Original and Extracted Watermark under Attacks

Attack	Structural Similarity Metric	Universal Image Quality Index
JPEG Compression	0.7432	0.7852
Wavelet Compression	0.8823	0.9144
Gaussian Noise	0.8594	0.9363
Salt & Pepper Noise	0.7920	0.8247
Cropping	0.5091	0.4680

CHAPTER 4. FINGERPRINT IMAGE WATERMARKING

This chapter proposes two watermarking techniques using Modified Discrete Cosine Transform (MDCT) and Discrete Wavelet Transform (DWT) for preserving the integrity of the fingerprint image. The demographic text and face images are used as contextual watermarks and are embedded into the fingerprint image. The MDCT based method embeds the watermarks into the ridge structures of the grayscale fingerprint image. The application of MDCT results in smooth edge decomposition so that the watermarked ridge structures do not degrade. MDCT has a better coding performance compared to DCT. In DWT based method the watermarks are embedded into selected texture regions of a fingerprint image. Experimental results for the proposed methods show that modifications in these locations are visually imperceptible and maintain the integrity of the fingerprint image as verified through the high matching scores on an AFIS system. There is a high level of visual correlation between the original and extracted watermark images. This is important for personal identification purposes and is quantitatively established using both pixel-based metrics and human visual system based metrics. The results also show that the proposed watermarking algorithms are resilient to common electronic image transmission transformations such as JPEG compression, filtering, and noise addition.

4.1. Fingerprints in Personal Identification

Biometric personal identification systems identify an individual based on physiological and behavioral characteristics. There are various biometric identifiers used

for personal identification and verification such as hand geometry, fingerprints, face, iris, speech, gait, and odor. Fingerprints are considered to be the most reliable identifiers next to iris. As fingerprint sensors continue to become less expensive and miniaturized, they are expected to lead the wide spread usage of biometrics in preventing fraud.

There are two types of fingerprint based biometric systems, Automated Fingerprint Authentication System (AFAS) [76] and Automated Fingerprint Identification System (AFIS) [77]. The authentication systems take the fingerprint image of the person and compares it with the templates stored in the database and the output is a binary decision, indicating whether the person's identity is verified or not. In the identification system, the input is a fingerprint image and the output is a list of likely candidates with associated scores indicating the similarity with the input fingerprint.

Fingerprint Image Features

A fingerprint is composed of composite curve structures with light and dark regions called *ridges* and *valleys* respectively as shown in Fig. 4.1. The most important discriminating features of the fingerprints used in matching process are the *minutiae*, which are the local discontinuities in the ridge flow pattern. The automated fingerprint matching systems use two types of minutiae features, the *ridge ending* and *ridge bifurcation*. The minutiae location and angle of orientation are attributes used for representing the fingerprint and for matching. These attributes of the minutia points are invariant to light and dark polarity of the ridge structures, which ensures their consistent extraction under image degradation conditions such as noise and contrast variance. Two other special features of the fingerprint image called the *core* and *delta* points, also

referred as singularity points, are used as reference points in coding the minutia points. The core point is defined as the topmost point on the innermost recurving ridge and delta is the center point of the triangular region where three different directional flows meet.

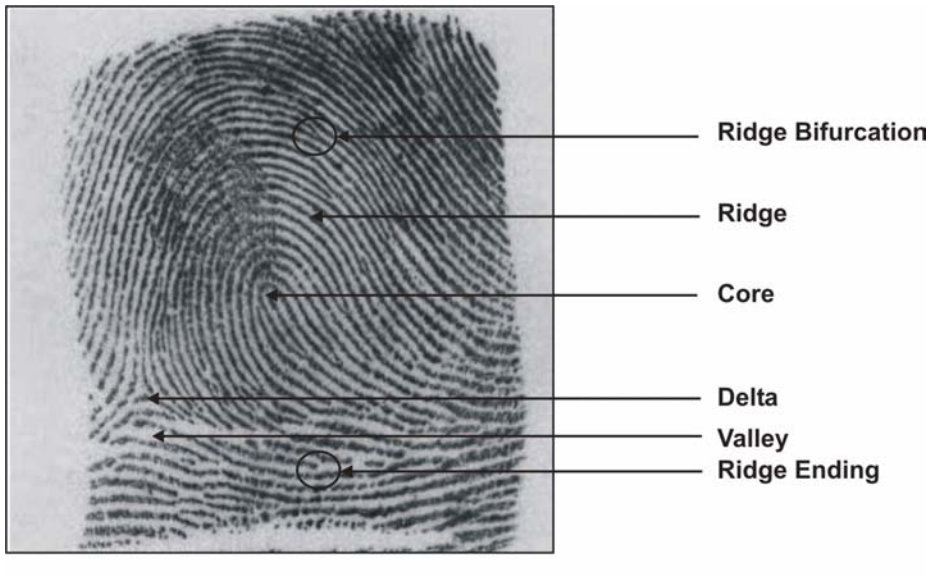


Fig. 4.1Fingerprint Image Features

The Cartesian coordinate system is used for minutia location [78] with its origin at top left corner and x-axis increasing towards right and y-axis increasing downwards. The angle is defined in degrees/radians, starting from zero on the right and increasing in counter-clockwise direction. While locating the minutia points the ridge structures are thinned to 1 pixel width and the end points and valley points are identified.

The pattern based [79] and image based [80] representations of the fingerprint image are the standard representations other than feature based using minutia points. All three representations are accepted by National Institute of Standards and Technology for fingerprint data interchange format. In contrast to feature based representation, pattern based representation relies upon global regions of the image. This type of representation

works very well in case of small-area and swipe sensors where extraction of features is not always possible. Usually, the images containing fewer pixels per inch and lesser number of grayscale levels are represented with image-based standard. A less commonly used fingerprint representation is based on the *pores* [81] that are located on the ridges. The pores are sometimes used as auxiliary features along with minutiae.

Fingerprint classification is another important aspect used in automated identification process for clustering the database. According to Henry *et al.* [82] fingerprints are classified into five different classes namely *arch, tented arch, right loop, left loop* and *whorl*. The most common type of representation used for classification of fingerprints is *direction map*, which is a matrix of directions indicating ridge and valley orientations at each location on the fingerprint image [83]. The number and location of core and delta points are used in building the directional map.

4.2. Proposed Watermarking Techniques

Fingerprint images collected by law enforcement agencies are stored in a database along with the demographic text data of the individual and a facial image. The different data types are usually stored under three different sub categories in a database. The collection, storage and analysis of disparate information introduces problems such as data mismatches and mishandling, high cost of storage, a longer time for retrieval, and unauthorized tampering of the files in the database. Furthermore, these images should be protected from possible network intrusion and manipulation. Maintaining the integrity of fingerprints and chain of custody is extremely important especially when it is used in

court as evidence. In this chapter, two watermarking techniques are proposed based on MDCT and DWT for fingerprint image authentication.

4.2.1. MDCT Based Watermarking Technique

The ridge structures are considered to be the significant features in automated fingerprint verification systems, which perform matching based on minutiae or ridge pattern. Embedding the watermarks into the ridges preserves the integrity of the fingerprint image. The ridge structures that are comprised of edges and lines are difficult to watermark. The characteristics of Modified Discrete Cosine Transform (MDCT) help in natural degradation of edges and line structures of the image. MDCT also has better coding performance compared to DCT.

A contextual watermarking scheme is proposed in this chapter that embeds a face and demographic text image watermarks into the host fingerprint image in MDCT domain. The application of MDCT results in smooth edge decomposition so that the watermarked ridge structures do not degrade. The watermarking scheme consists of two phases (1) watermark insertion and (2) watermark extraction. The extracted watermark is used to verify the authenticity of the fingerprint image. The fingerprint image is decomposed into transform domain using MDCT. The ridge structure locations are identified by converting the grayscale fingerprint image to binary using a global threshold and locating the dark regions.

$$R(i,j) = \sum_{i=1}^{M}\sum_{j=1}^{N} F(i,j) \leq G_T \tag{4.1}$$

$$R_T = MDCT(R) \tag{4.2}$$

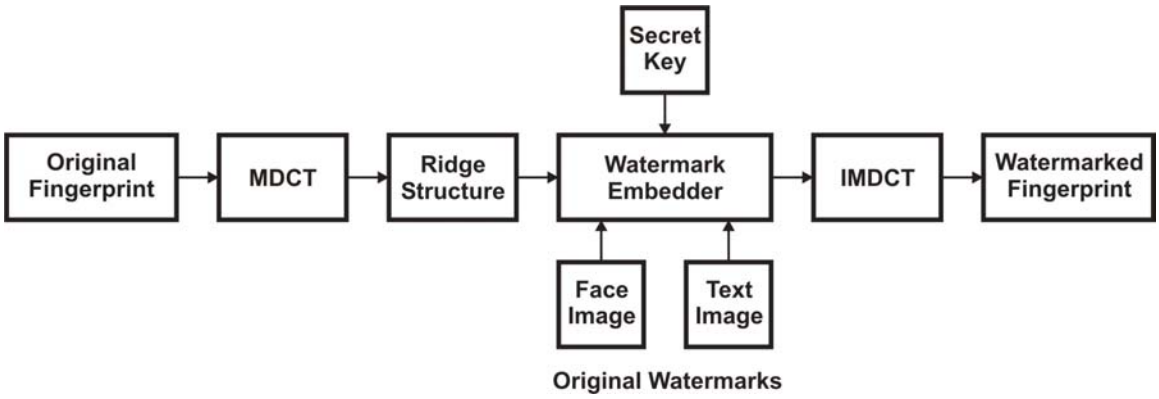


Fig. 4.2 Block Diagram of MDCT Based Fingerprint Image Watermarking Technique

where F is the grayscale fingerprint image of size M x N and G_T is the global threshold for binarization. The size of the ridge structure matrix is assumed to be greater than the combined image sizes of the watermarks. The MDCT coefficients corresponding to ridges are represented as R_T. The two watermarks are embedded at two different locations without overlap as shown in Fig. 4.2. The embedding process follows the equation (4.3) for the facial image W_f, which is of the size P x Q.

$$\dot{R}_T(i,j) = \sum_{i=1}^{P}\sum_{j=1}^{Q} R_T(i,j) + \alpha 1 * W_f(i,j) \tag{4.3}$$

where $\dot{R}_T$ is the ridge coefficient matrix embedded with the facial watermark. The embedding process for the text image W_t of size S x T is given in equation (4.4)

$$\ddot{R}_T(i,j) = \sum_{i=P}^{S}\sum_{j=Q}^{T} R_T(i,j) + \alpha 2 * W_t(i,j) \tag{4.4}$$

where $\ddot{R}_T$ is the ridge coefficient matrix embedded with both face and text watermarks. The watermarked fingerprint $\widehat{F}$ is obtained by reconstructing the embedded ridge coefficients with Inverse Modified Discrete Cosine Transform (IMDCT). A secret key is used to select the embedding locations randomly to secure the original fingerprint and the embedded face and text watermarks from tampering. The amplifying factors, α1 and α2, are computed from the perceptual model [84] that varies the watermarks such that maximum amount of information can be hidden in the host fingerprint image depending on luminance and contrast properties of the embedding region.

4.2.2. DWT Based Watermarking Technique

In this technique, the face and demographic text data are embedded into the texture features of the fingerprint image using DWT. The following sections explain the extraction of fingerprint texture features using DWT and the watermark embedding and extraction process.

4.2.2.1. Extraction of Fingerprint Texture Features

Texture is an important feature for the analysis of many types of images. Properties such as roughness, granulation and regularity, which do not have smooth varying intensities can be determined through a set of local neighborhood properties of the graylevels of an image region. Multi-scale processing, which humans apply for texture perception is modeled using wavelet analysis [85]. The image features that represent the scale-dependent properties can be extracted from each sub-image separately. A non-linear function that produces the energy of the image when summed

over a sub-image is widely used for texture computation. The feature set thus obtained consists of energies of different scales, which is an important characteristic for texture analysis. A signal f(x) when decomposed using a 1-dimensional wavelet transform into a basis of wavelet functions to obtain the transformed signal, $W_{p,q}$, is given by

$$W_{p,q}(f(x)) = \int f(x)\psi_{p,q}(x)\,dx \tag{4.5}$$

where p and q are scale and position parameters respectively. The basis vectors are obtained by translating and dilating the mother wavelet,

$$\psi_{p,q} = \frac{1}{p}\psi\left[\frac{x-q}{p}\right] \tag{4.6}$$

The mother wavelet ψ has to be localized in both spatial and frequency domains. A 2-dimensional wavelet transform is obtained by first applying a 1-dimensional transform along the rows and then along the columns. A Daubechies filter bank is used to implement the Discrete Wavelet Transform (DWT) resulting in a pyramid structure of sub-bands shown in Fig. 4.3. The 2-level decomposition consists of seven sub-bands. The sub-bands labeled HH, HL and LH contain the diagonal, horizontal and vertical details of the fingerprint image respectively, while the LL sub-band contains the coarse details of the image.

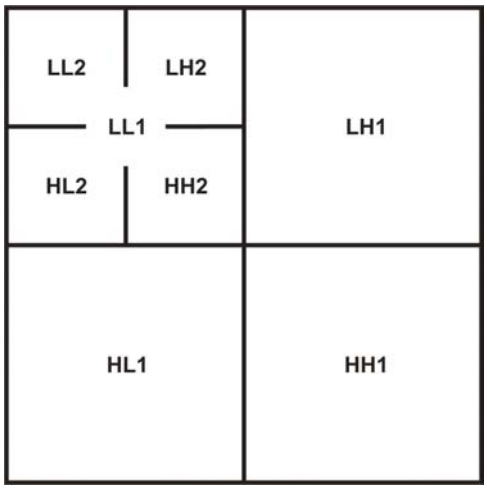


Fig. 4.3 Two-Level Decomposition Using DWT

The process of obtaining texture features from an image was adopted from [86]. Let I be an N x N input grayscale image in the spatial domain. This image is transformed to frequency domain (W) using DWT. The decomposed image consists of sub-images from which the texture information of the input image at different scale resolution is obtained. The resulting texture feature matrix is of dimension N/r x N/r, where r is the level of decomposition.

The texture map, t_{Wr}, is computed for each input sub-image W_r. The energy of the coefficient combined with the variance of the corresponding coefficients in the lowest LL sub-image represents the texture of that coefficient.

$$t_{W_r}(i,j) = W_r(i,j)^2 + \text{var}([LL2(i+1,j+1)\ \ LL2(i+2,j+2)]) \tag{4.7}$$

where var is the variance of the two coefficient block and $W_r \in$ (HH2, HL2, LH2, HH1, HL1 and LH1).

The background pixels in the texture map have a higher magnitude compared to the pixels representing the actual fingerprint image. The locations in the texture map whose magnitude is less than a predefined threshold, T_{W_r} , compared to its adjacent locations are selected. These selected locations containing higher texture details are used in our proposed watermarking algorithm. Modification of these coefficients is imperceptible since the most significant coefficients act as a visual mask. The selected texture regions of HH1, HL1 and LH1 sub-bands are denoted by ST_{HH1}, ST_{HL1} and ST_{LH1} and are defined in equation (4.8).

$$
\begin{aligned}
ST_{HH1} &= \min[t_{HH1}(i, j+1), t_{HH1}(i, j)] \quad \text{if} |t_{HH1}(i, j+1) - t_{HH1}(i, j)| > T_{HH1} \\
ST_{HL1} &= \min[t_{HL1}(i, j+1), t_{HL1}(i, j)] \quad \text{if} |t_{HL1}(i, j+1) - t_{HL1}(i, j)| > T_{HL1} \\
ST_{LH1} &= \min[t_{LH1}(i, j+1), t_{LH1}(i, j)] \quad \text{if} |t_{LH1}(i, j+1) - t_{LH1}(i, j)| > T_{LH1}
\end{aligned}
\tag{4.8}
$$

where,

$T_{HH1} = \max(t_{HH1}) - \text{avg}(t_{HH1})$

$T_{HL1} = \max(t_{HL1}) - \text{avg}(t_{HL1})$

$T_{LH1} = \max(t_{LH1}) - \text{avg}(t_{LH1})$

The texture maps and the corresponding selected texture regions of HH1, HL1 and LH1 are shown in Fig. 4. 4. The selection of texture regions in the remaining sub-bands is similarly computed.

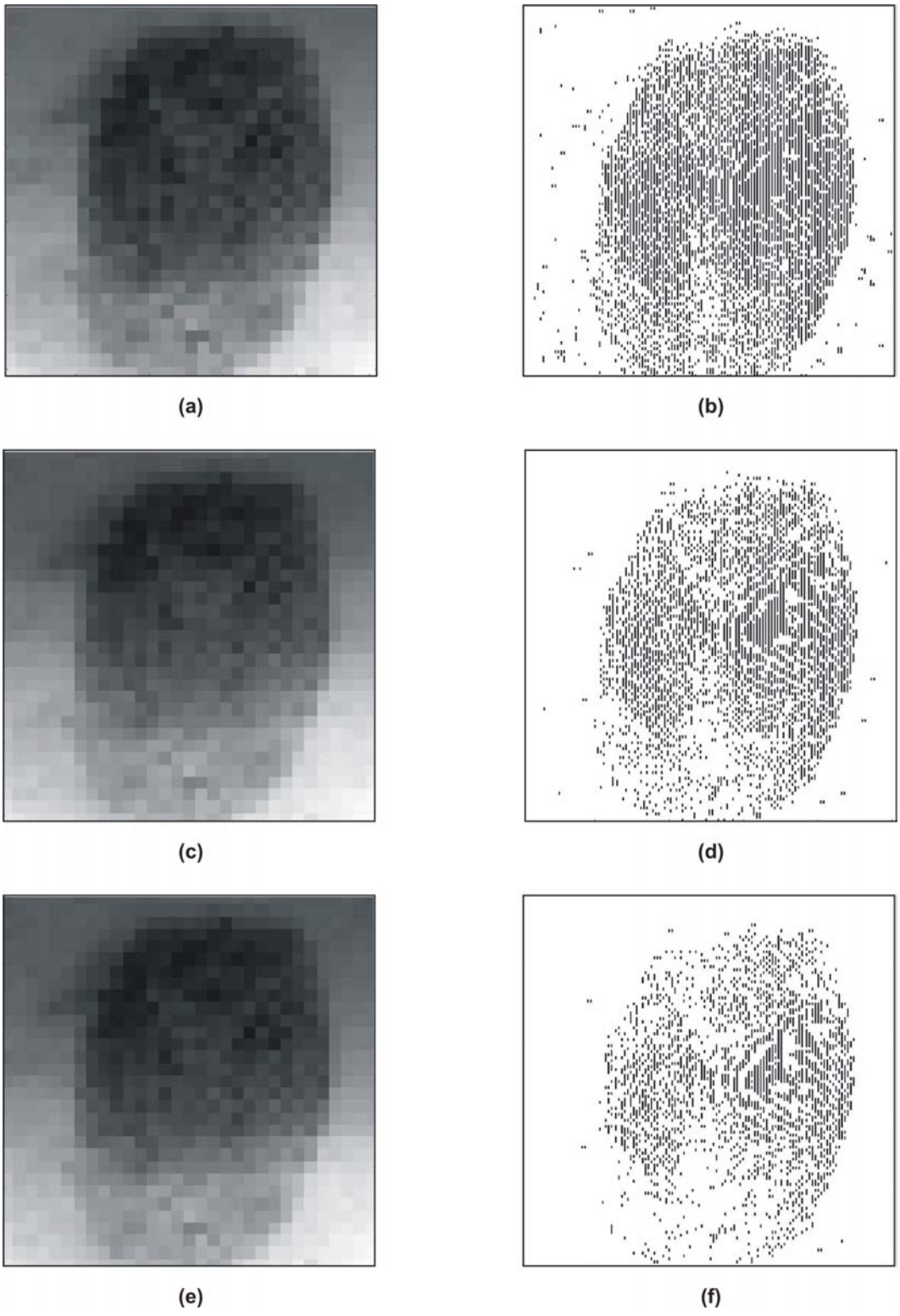


Fig. 4.4 (a), (b) and (c) are texture maps of LH1, HL1 and HH1 respectively; (d), (e) and (f) are corresponding texture representation

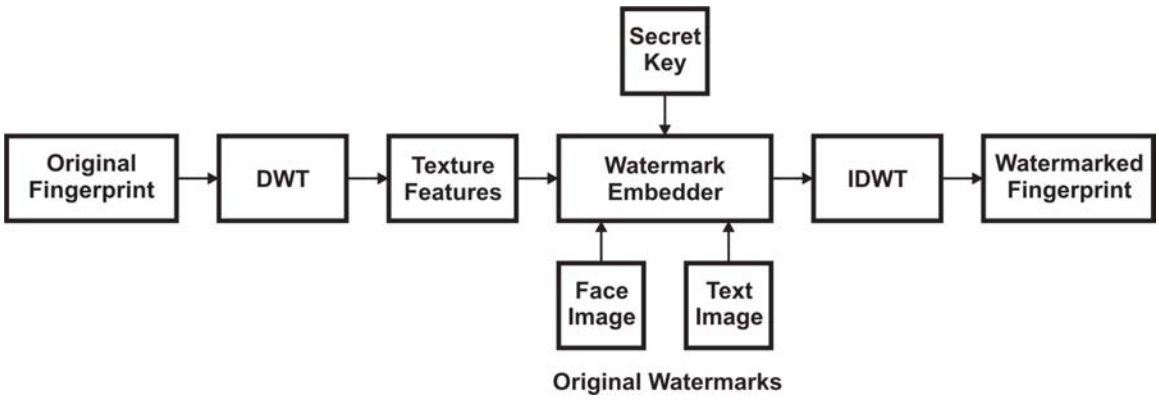


Fig. 4.5 Block Diagram of DWT Based Fingerprint Image Watermarking Technique

4.2.2.2. Watermarking Algorithm

The grayscale fingerprint image is decomposed using a 2-level Discrete Wavelet Transform to obtain seven sub-bands as shown in Fig. 4.3. The text and face watermark images are embedded into the wavelet coefficients of the fingerprint image that represent the locations of the selected texture regions. The facial image is in grayscale while the text image is in binary. The sub-image selection for watermarking depends on several factors. The modification of the low frequency sub-image LL2 will impose severe degradation of the reconstructed image as most of the energy is concentrated in this band. During filtering and compression some of the information will be lost in the high frequency bands. One way of overcoming this information loss is by redundantly embedding information in all the high frequency bands (LH1, HL1 and HH1). The three mid-frequency bands (LH2, HL2 and HH2) are good choices for embedding. We embed the grayscale face image into the mid-frequency bands and the binary text image is redundantly embedded into the high frequency bands.

Embedding the Face Image

The face image is embedded into the wavelet coefficients, Wav^{ST}_{LH2}, Wav^{ST}_{HL2} and Wav^{ST}_{HH2}, which represent the locations of the selected texture regions of LH2, HL2 and HH2 respectively. The size of the facial image is adjusted to be one third of the total number of available embedding locations. Let the face image watermark, w_f, be of size p x q. The grayscale values of the facial watermark image are divided into three bit-streams, L, I, and M, representing the least-significant, the intermediate, and the most-significant integer values respectively as described in equation (4.9).

$$W_f(i,j) = \sum_{i=1}^{p}\sum_{j=1}^{q}\left(100 * M(i,j) + 10 * I(i,j)\right\} + L(i,j)\right) \tag{4.9}$$

where, $0 \leq (L, I) \leq 9$ and $0 \leq M \leq 2$. The bit-streams L, I and M are inserted into the lowest order integer of Wav^{ST}_{LH2}, Wav^{ST}_{HL2} and Wav^{ST}_{HH2} respectively. The embedding of facial integer bit-streams into the wavelet coefficients is described in equation (4.10).

$$\begin{aligned} Lowest\_Order\_Integer(Wav^{ST}_{LH2}(i,j)) &= \sum_{i=1}^{p}\sum_{j=1}^{q} L(i,j) \\ Lowest\_Order\_Integer(Wav^{ST}_{HL2}(i,j)) &= \sum_{i=1}^{p}\sum_{j=1}^{q} I(i,j) \\ Lowest\_Order\_Integer(Wav^{ST}_{HH2}(i,j)) &= \sum_{i=1}^{p}\sum_{j=1}^{q} M(i,j) \end{aligned} \tag{4.10}$$

Embedding the Text Image

Next, the binary text image is embedded into the wavelet coefficients, Wav^{ST}_{LH1}, Wav^{ST}_{HL1} and Wav^{ST}_{HH1}, which represent the locations of the selected texture regions of LH1, HL1 and HH1 respectively. The size of the text watermark is made equal to the size of the smallest of three selected texture represented sub-images. The lowest order integers of Wav^{ST}_{LH1}, Wav^{ST}_{HL1} and Wav^{ST}_{HH1} are replaced by the text watermark bits. Let the size of the text watermark image, w_t, be r x s. The embedding of binary text image into the wavelet coefficients is given by equation (4.11),

$$\begin{aligned} Lowest\_Order\_Integer(Wav^{ST}_{LH1}(i,j)) &= \sum_{i=1}^{r}\sum_{j=1}^{s} W_t(i,j) \\ Lowest\_Order\_Integer(Wav^{ST}_{HL1}(i,j)) &= \sum_{i=1}^{r}\sum_{j=1}^{s} W_t(i,j) \\ Lowest\_Order\_Integer(Wav^{ST}_{HH1}(i,j)) &= \sum_{i=1}^{r}\sum_{j=1}^{s} W_t(i,j) \end{aligned} \qquad (4.11)$$

Generating the Watermarked Fingerprint

The final watermarked fingerprint image is obtained when the embedded sub-bands are reconstructed using a two-level Inverse Discrete Wavelet Transform (IDWT). A secret key is used to select the embedding locations randomly to secure the original fingerprint and the embedded face and text watermarks from tampering. As part of the implementation of the algorithm we use the perceptual model for varying the watermark images based on the fingerprint image content. An amplifying factor, α, is computed which varies the watermarks such that maximum amount of information can be hidden in the host fingerprint image depending on luminance and contrast properties of the

embedding region. In other words, the correlation between the original watermark, w_m, and the embedded watermark, w_a, is made maximum, while keeping the perceptual distance between the original fingerprint and watermarked fingerprint images constant. The best value of α is found by iteratively computing the just noticeable difference for the watermarked fingerprint and reducing this difference to a target value. The embedded watermark is finally obtained using the best value of α defined in equation (4.12).

$$w_a = \alpha\, w_m \tag{4.12}$$

4.3. Implementation of the Proposed Techniques

The proposed embedding algorithms are implemented using a 512 x 512 fingerprint image as the host image shown in Fig. 4.6a. Figs. 4.6b and 4.6c are the original face image of size 102 x 102, and the original text image of size 220 x 220 that are used as contextual watermarks. The proposed watermarking algorithms are used to embed the face and the text images in the fingerprint. The resulting watermarked fingerprint images from MDCT based method and DWT based methods are shown in Fig. 4.6d and 4.6e respectively. These fingerprint images are securely protected and can be used to verify if the chain of custody is maintained or the fingerprint has been compromised by external tampering. Any degradation in visual image quality between the original fingerprint image and the watermarked fingerprint image is very small and is hardly discernable.

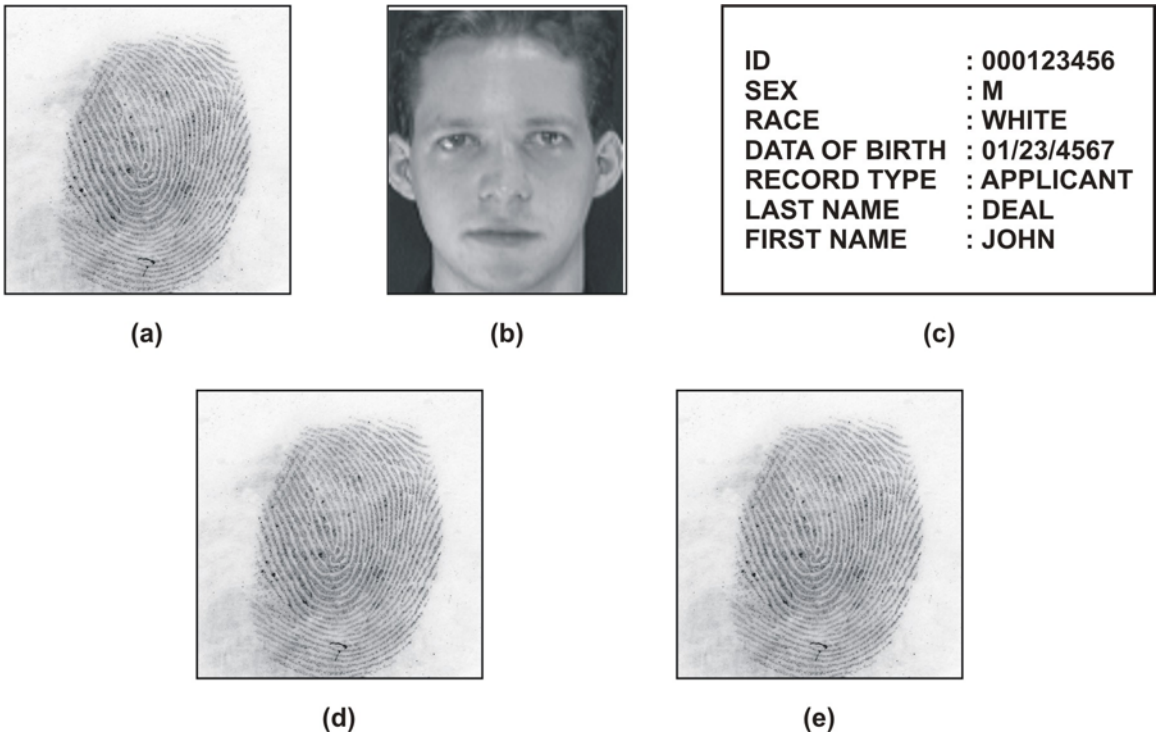


Fig. 4.6 (a) Original Fingerprint, (b) Original Face Image, (c) Original Text Image, (d) Watermarked Fingerprint Image Using DWT method, and (e) Watermarked Fingerprint Image Using MDCT method

4.4. Matching Performance of Watermarked Fingerprint

Embedding the facial and demographic text data into the individuals fingerprint image eliminates data mismatch, reduces the high cost of storage, speeds the retrieval of related data, establishes a digital chain of custody, and can detect tampering. It is important to ensure that the embedded text and face watermarks do not alter the functional integrity of the fingerprint and its ability to detect possible matches. To verify the effect of watermarking on matching fingerprint images, an AFIS system is used. A set of fingerprint images are watermarked using the proposed algorithms and are matched with other fingerprints stored in the database of the AFIS system. The results of the

matching scores are shown in Fig. 4.7 and 4.8 for MDCT and DWT methods respectively. The high matching scores of the original fingerprint image and the watermarked fingerprint image validate that the fingerprint features such as ridge bifurcations and ridge endings that are used for matching purposes have not been altered. The matching score of the next closest fingerprint or the second best fingerprint from the database is so low that it would not be classified as a possible match in the AFIS system.

4.5. Verifying the Integrity of the Watermarked Fingerprint

The watermarked fingerprint has several advantages. One of the main advantages is that the fingerprint, the demographic text information of the individual and the facial image need not be stored in separate databases. The contextual digital watermarking allows all related data to be stored and retrieved at the same time. From the extracted watermarks, the digital chain of custody and the integrity of the fingerprint can be verified against possible tampering. The retrieval of the facial image and the text data also helps with identification of an individual. The procedure to extract the text and face image is shown in Fig. 4.9a and 4.10a for MDCT and DWT techniques respectively. The extraction process is the reverse of the embedding process. The same secret key used during embedding is now used to determine the order of extracting the bits. The extraction process of the watermark images in the MDCT based technique includes the selection of ridge MDCT coefficients using the same global threshold for binarization, subtracting the magnitude of these coefficients from the corresponding original fingerprint image coefficients and scaling it with the amplification factor as given in equations (4.13) and (4.14).

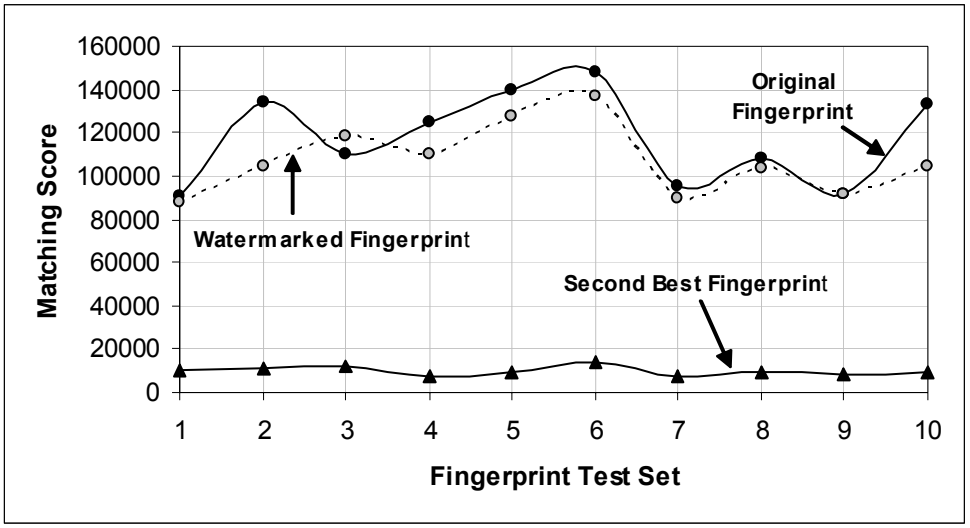


Fig. 4.7 Matching Watermarked Fingerprint Images Obtained from MDCT technique on AFIS System

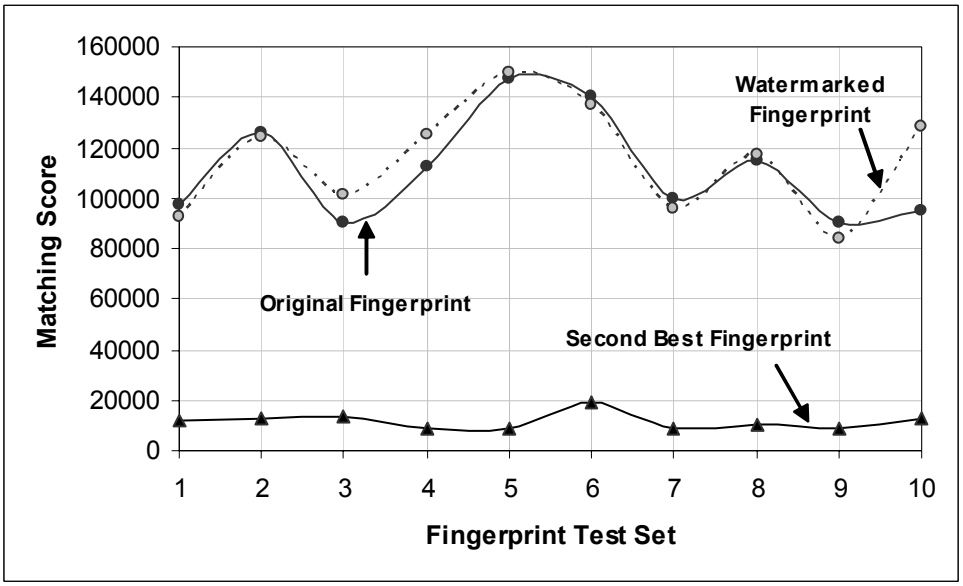


Fig. 4.8 Matching Watermarked Fingerprint Images Obtained from DWT technique on AFIS System

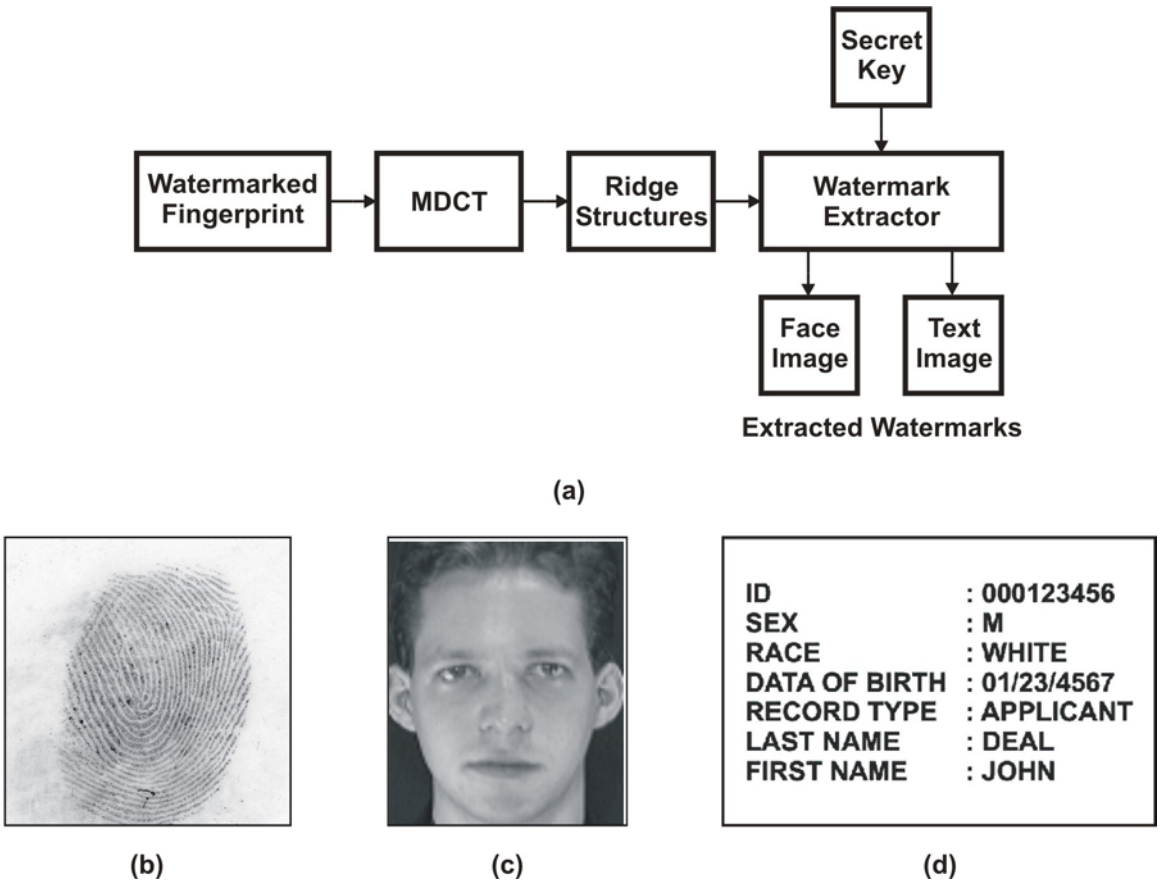


Fig. 4.9 (a) MDCT Based Extraction Process, (b) Watermarked Fingerprint (c) Extracted Facial Image, and (d) Extracted Text Image

$$E_f(i,j) = \frac{\sum_{i=1}^{P}\sum_{j=1}^{Q} R(i,j) - \ddot{R}(i,j)}{\alpha 1} \tag{4.13}$$

$$E_t(i,j) = \frac{\sum_{i=P}^{S}\sum_{j=Q}^{T} R(i,j) - \ddot{R}(i,j)}{\alpha 2} \tag{4.14}$$

E_f is the extracted facial image and E_t is the extracted text image. Figs. 4.9c and d show the extracted face and the extracted text images from the MDCT based watermarked

fingerprint image of Fig. 4.9b. The original fingerprint image is required for the extraction of watermarks.

In DWT based technique, the selected texture region is obtained for all six sub-images and the watermarks are extracted from the lowest order integer of the corresponding sub-images. The spatial redundancy introduced in the high frequency channel during embedding the text watermark ensures reliable extraction when at least two of the three values are the same. Using the same technique, the facial image is extracted from the lower frequency channel. Figs. 4.10c and d show the extracted face and the extracted text images from the watermarked fingerprint image of Fig. 4.10b. Neither the original fingerprint image nor the original watermark images are required for extraction. The extracted text and face image are of good quality and closely resemble the original images shown in Figs. 4.6b and c. This verifies that the chain of custody of the fingerprint is maintained.

We next quantitatively determine the degree of similarity between the original watermark images and the extracted watermark images using two different types of metrics. The peak signal to noise ratio (PSNR), mean square error (MSE), and correlation between the original and modified images give the pixel-based similarity between the images. The structural similarity measure (SSIM) and universal image quality index (UIQI) compare the images based on human visual system (HVS).

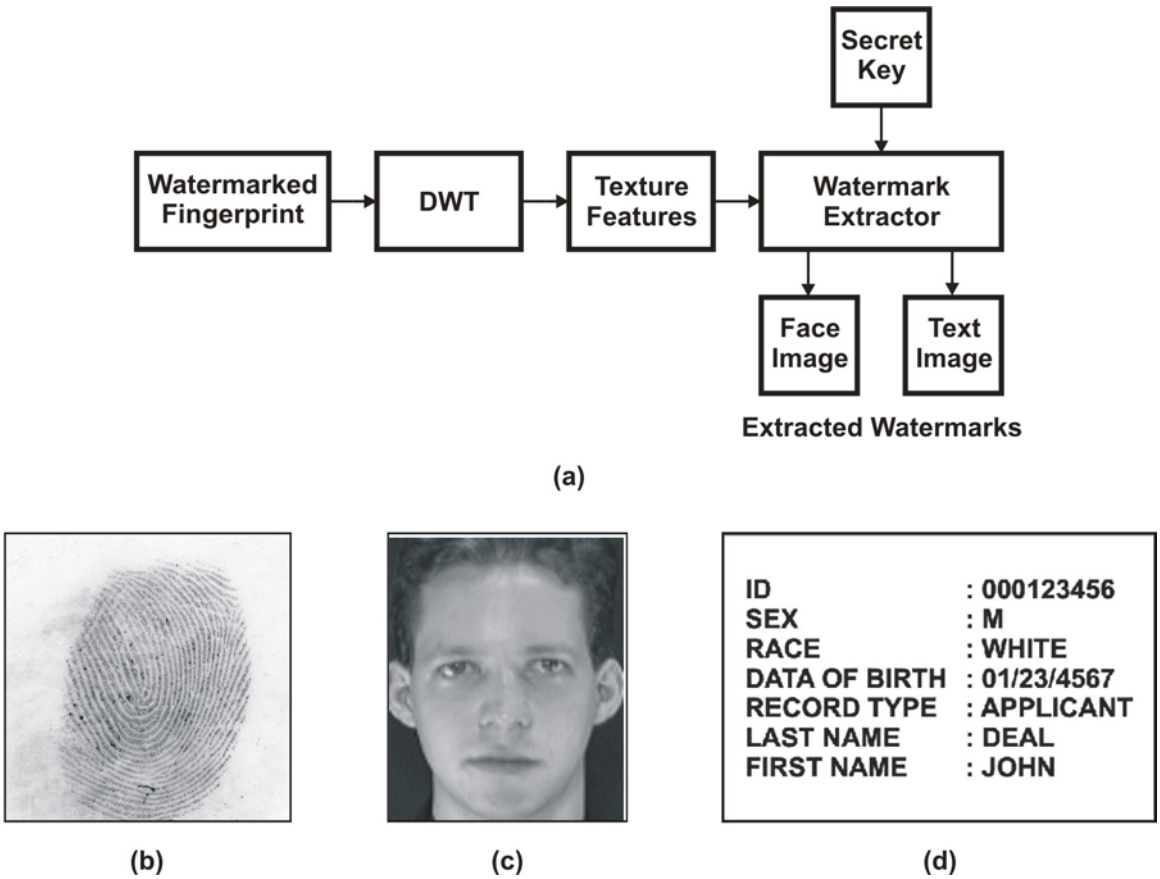


Fig. 4.10 DWT Based Extraction Process, (b) Watermarked Fingerprint (c) Extracted Facial Image, and (d) Extracted Text Image

Tables 4.1 and 4.2 show the degree of similarity between the original text and the face images, and the extracted images. The similarity values using both the pixel based approach and the human visual system approach show a high level of correlation between the images.

Table 4.1 Image Quality Metrics for DWT Based Method

	PNSR	MSE	Correlation	SSIM	UIQI
Face	70.45	58	0.9861	0.8568	0.9341
Text	88.99	40	0.8641	0.9994	0.8127

Table 4.2 Image Quality Metrics for MDCT Based Method

	PNSR	MSE	Correlation	SSIM	UIQI
Face	52.50	76	0.9230	0.8219	0.9341
Text	64.72	52	0.8439	0.9576	0.7780

Numerical results support that the image quality is high and is suitable for personal identification and verifying the chain of custody. The proposed contextual watermarking approach using face and text images to watermark a fingerprint is useful for authenticating the integrity of the fingerprint. The contextual watermarking is novel because the watermarked fingerprint image is compact and takes less memory space compared to the space occupied by individual images. Furthermore, the time taken to search different databases to obtain all pertinent information corresponding to an individual in greatly minimized since each fingerprint image has the demographic text and face image embedded as watermarks and can be easily extracted.

4.6. Electronic Transmission of Fingerprint Images

The electronic transmission of fingerprints over the communication channel introduces degradations in the image data. The basic block diagram of point-to-point communication link is shown in Fig. 4.11. The discrete information in the form of sequence of symbols is given as an input to the channel through source encoder. The encoding process reduces the redundant information from the symbol sequence and converts it to binary sequence. This includes compressing the image files using standard compression tools while transmitting large image files over low bandwidth channel. The

modulator converts the input binary sequence into waveform suitable for transmission over the available transmission channel. The transmission channel provides electrical connection between the source and the destination. The connecting media may be wires, telephone cable, an optical fiber or free space. Several types of impairments affect the transmitted signal in the communication channel such as noise. At the receiver, the demodulator converts the received waveform into binary sequence and the source decoder converts the binary sequence to symbol sequence and passes it to the user. In this process the image is filtered to remove noise and insignificant structures. Median filter is generally used to accomplish the filtering task.

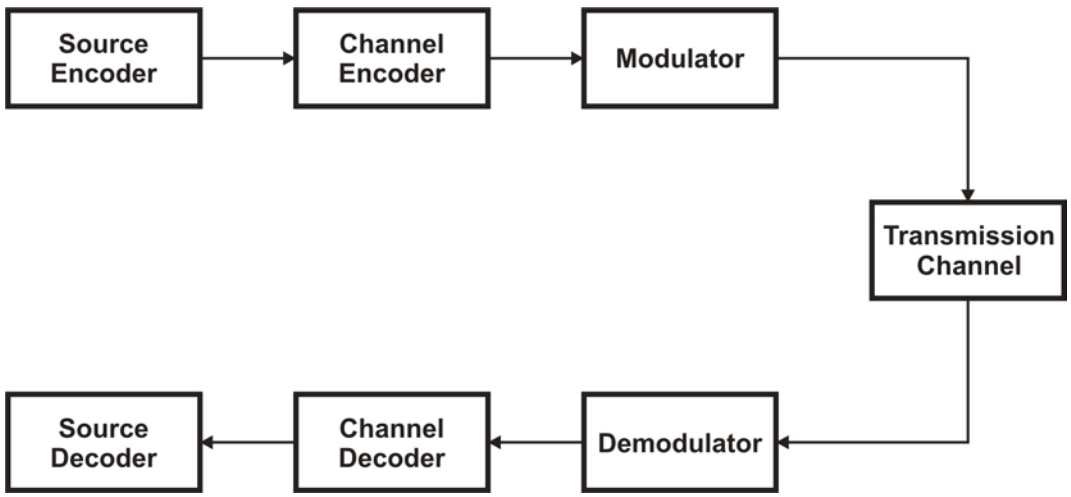


Fig. 4.11 Point-to-Point Communication Channel Model

These effects on the watermarked fingerprint are studied by using various image processing transformations such as JPEG compression, median filtering and the addition of Gaussian noise. For each type of transformation, the matching score of the

watermarked fingerprint image is compared with the matching score of the original fingerprint image and the remaining images in the AFIS database. Also, the watermarks are extracted from the transformed fingerprint images and quality scores are computed.

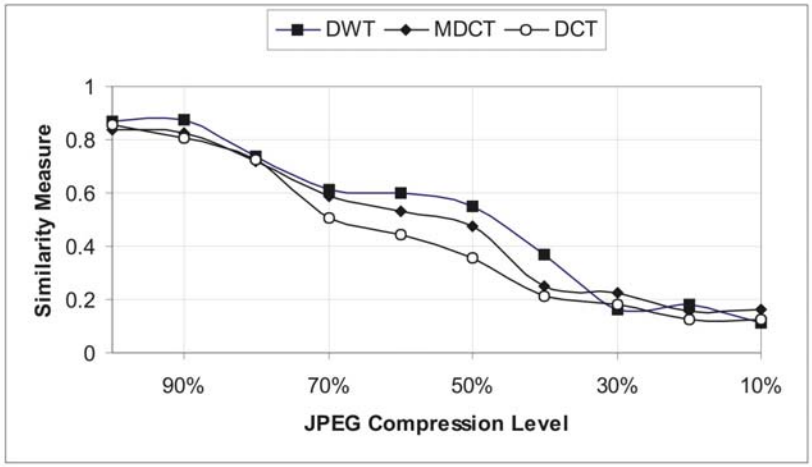
DCT Based Technique

The MDCT based fingerprint image watermarking technique introduced in Section 4.2.1 is implemented using DCT transform to investigate the performance improvement. In this technique the ridge detail obtained from the global threshold method is transformed into DCT coefficients and embedded with the watermarks using the equations (4.3) and (4.4).

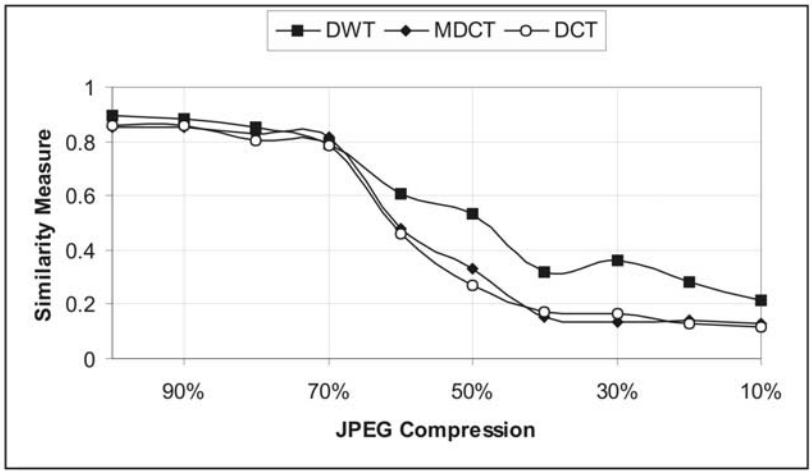
4.6.1. Experimental Results and Observations

The results of the attacks are shown in Figs. 4.12, 4.13, and 4.14 for DWT, MDCT and DCT based watermarking methods. The results of the tests show that the watermarked fingerprint is resilient to various distortions that commonly occur during image transmission process. Unauthorized tampering or substitution of the fingerprint data can be detected by extracting and examining the watermarks. Since the visual quality of the text and the face images are commonly used for personal identification, it is appropriate to use the human visual metrics for comparison purposes. The two HVS based metrics, SSIM and UIQI, used in Section 4.5 are averaged to obtain a single distance measurement. The average single distance measurement shows high similarity between the original and extracted watermarks up to 70% of JPEG compression level, median filter window size of 5 and gaussian noise variance of 0.05. Any attempt of tampering indicated by intensifying the transformation phenomenon to make the

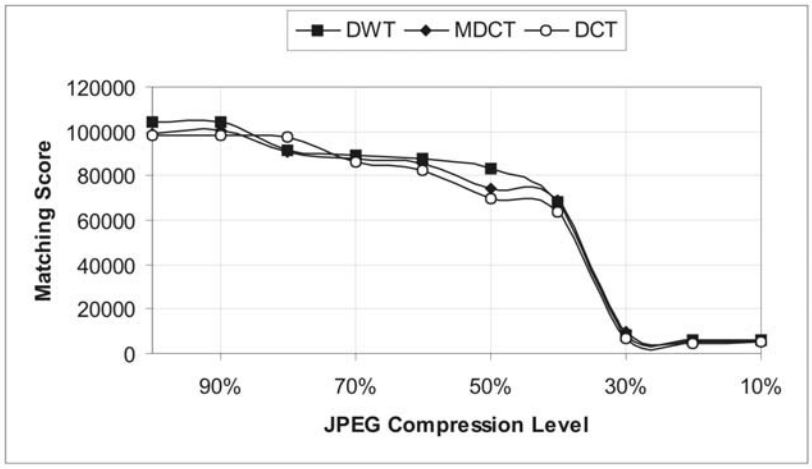
fingerprint unmatchable can be detected from the low matching score of the AFIS system. The results also validate that the proposed embedding technique does not alter the key fingerprint features used in level-2 matching when transmitted over the communication channel.



(a)

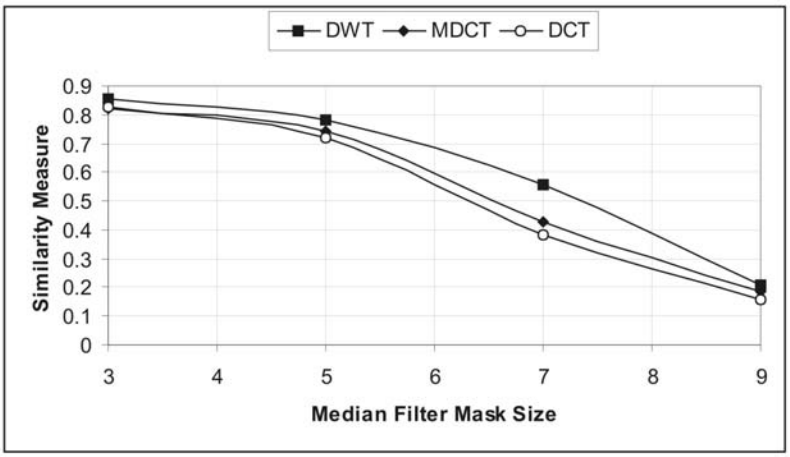


(b)

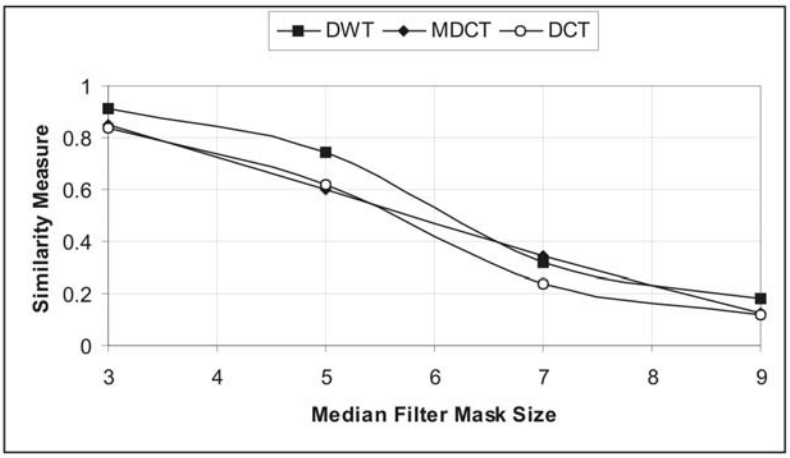


(c)

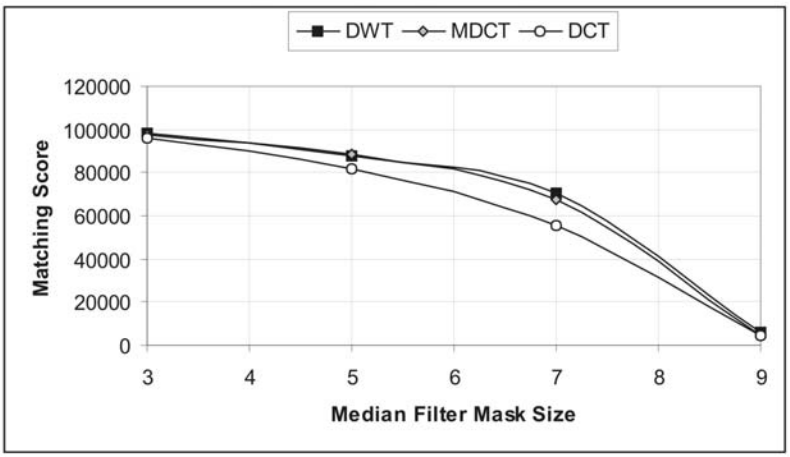
Fig. 4.12 (a) Similarity Measure of Extracted Face Image Under Compression, (b) Similarity Measure of Extracted Text Image Under Compression, and (c) AFIS Matching Score of Compressed Fingerprint



(a)

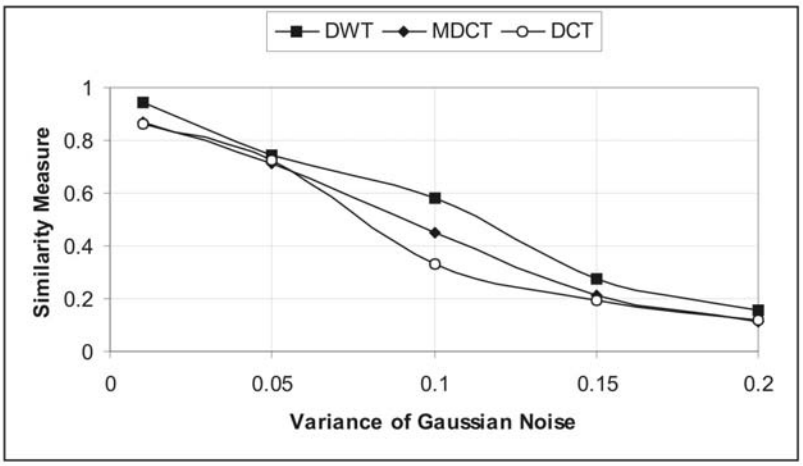


(b)

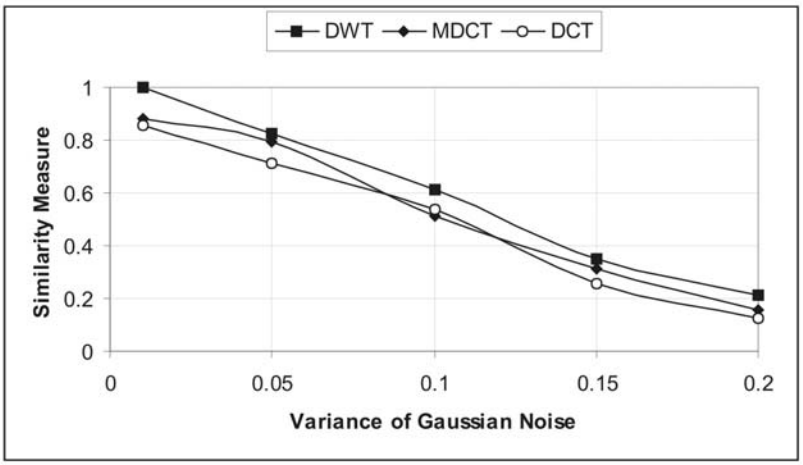


(c)

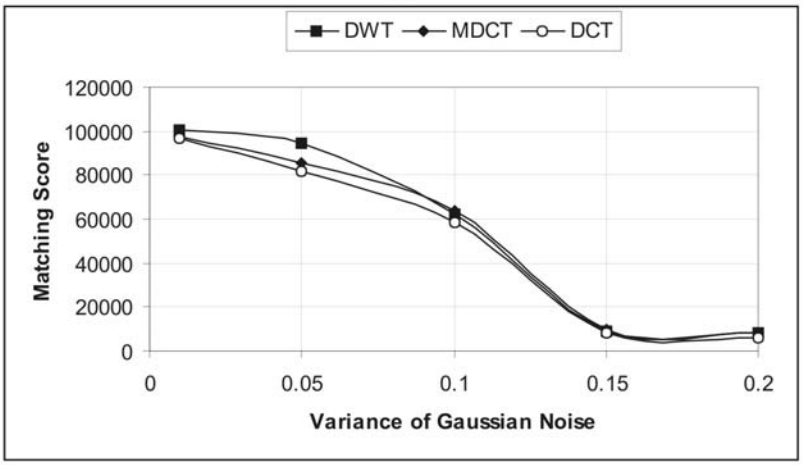
Fig. 4.13 (a) Similarity Measure of Extracted Face Image Under Filtering, (b) Similarity Measure of Extracted Text Image Under Filtering, and (c) AFIS Matching Score of Filtered Fingerprint



(a)



(b)



(c)

Fig. 4.14 (a) Similarity Measure of Extracted Face Image Under Gaussian Noise, (b) Similarity Measure of Extracted Text Image Under Gaussian Noise, and (c) AFIS Matching Score of Fingerprint with Added Noise

The proposed watermarking techniques are also robust to spatial domain attacks such as cropping and rotation as shown in Table 4.3 and 4.4. The 512 x 512 watermarked fingerprint image is cropped to 450 x 450 at the center and the angle of rotation is 10 degrees. The moderately high correlation between the original and extracted watermarks shows that the proposed techniques are robust to cropping and rotation.

Table 4.3 Resilience of MDCT Based Method to Spatial Domain Transformations

	Face Image			**Text Image**		
	PSNR	**SSIM**	**UIQI**	**PSNR**	**SSIM**	**UIQI**
Cropping	27.88	0.7302	0.6649	31.94	0.6851	0.6937
Rotation	25.06	0.7108	0.6285	28.65	0.6350	0.6748

Table 4.4 Resilience of DWT Based Method to Spatial Domain Transformations

	Face Image			**Text Image**		
	PSNR	**SSIM**	**UIQI**	**PSNR**	**SSIM**	**UIQI**
Cropping	29.17	0.7684	0.7179	35.62	0.7249	0.6930
Rotation	30.43	0.7290	0.6855	33.51	0.7485	0.6924

CHAPTER 5. CONCLUSIONS AND FUTURE WORK

This research presents multiple aspects of image watermarking with both analytic study and experimental results. We have illustrated that digital watermarking can be used for various applications, including copyright protection, personal identification, establishing chain of custody, tamper detection, and access or copy control. In addition to the design issues, we also discussed attacks on watermarking algorithms with a goal of identifying weaknesses and limitations of existing design as well as proposing improvements.

An improved digital watermarking algorithm using modified discrete cosine transform is presented. The binary logo is embedded into the image features of the host image so any attempt to tamper the watermark heavily deteriorates the host image. Using JPEG test images the experimental results show that the embedded watermark does not affect the quality of the image. The results also show that proposed technique using MDCT eliminates blocking artifacts and introduces a more natural degradation of the image at low bit rates and has better anti-aliasing properties. At higher bit rates the smoothing effect produces very high quality images. The proposed method is robust to various spatial and frequency domain attacks.

Besides the classic use in ownership protection, we have demonstrated that watermarking can be a useful tool for personal identification using biometrics. Two contextual fingerprint image watermarking algorithms are proposed in this thesis. A facial image and the corresponding demographic text data of an individual are embedded into selected regions of fingerprint image using Modified Discrete Cosine Transform and Discrete Wavelet Transform. The watermarked fingerprint provides added protection

from tampering and the fingerprint matching ability is not affected even when subjected to common attacks. Quantitative results show that the extracted face and text images are of high quality and provide additional information for identification purposes. Using the proposed approach, the absence of watermarks or visual distortions in the extracted watermarks would reveal if the integrity of the fingerprint image has been compromised.

Further research, related to the above work, can be conducted to determine the maximum information that can be embedded without compromising the functional integrity of the fingerprint image. This would be especially useful when color facial images are used instead of grayscale images as watermarks. Further research would also identify the appropriate metrics for comparing the original and extracted color face images. This would be appropriate in watermarking drivers' license to protect from external tampering.

REFERENCES

[1] T. Liu, Z.-D. Qiu, ”The survey of digital watermarking-based image authentication techniques,” *6th International Conference on Signal Processing*, vol.2, pp. 1556-1559, 2002.

[2] Y. Wang, J.F. Doherty, R.E. Van Dyck, ”A wavelet-based watermarking algorithm for ownership verification of digital images,” *IEEE Transactions on Image Processing*, vol. 11, no. 2, pp. 77-88, 2002.

[3] R. Tay, J.P. Havlicek, ”Image watermarking using wavelets,” *45th Midwest Symposium on Circuits and Systems*, vol. 3, pp. 258-261, 2002.

[4] R. Bangaleea, H.C.S. Rughooputh, ”Performance improvement of spread spectrum spatial-domain watermarking scheme through diversity and attack characterization,” *IEEE 6th Africon Conference*, vol.1, pp. 293-298, 2002.

[5] D.P. Mukherjee, S. Maitra, S.T. Acton, ”Spatial Domain Digital Watermarking of Multimedia Objects for Buyer Authentication,” *IEEE Transactions onMultimedia*, vol. 6, no. 1, pp. 1-15, 2004.

[6] A. K. Jain and U. Uludag, ”Hiding Fingerprint Minutiae in Images,” *Proc. of Third Workshop on Automatic Identification Advanced Technologies (AutoID)*, pp. 97-102, Tarrytown, New York, March 2002.

[7] V. Claus, S. Ralf, ”Approaches to biometric watermarks for owner authentification,” *Proc. of SPIE*, vol. 43, no. 14, pp. 209-219, 2001.

[8] A. K. Jain and U. Uludag, ”Hiding biometric data,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 11, pp. 1494-1498, 2003.

[9] S. Pankanti, M. Yeung, ”Verification Watermarks on Fingerprint Recognition and Retrieval,” *SPIE International Conf. on Security and Watermarking of Multimedia Contents*, vol. 3657, no. 7, pp. 66-78, Jan. 1999.

[10] N. K. Ratha, J. H. Connell, R. M. Bolle, ”Secure data hiding in wavelet compressed fingerprint images,” *International Multimedia Conference,Proceedings of the 2000 ACM workshops on Multimedia*, pp. 127-130, 2000.

[11] A. K. Jain, U. Uludag, R.-L. Hsu, ”Hiding a Face in a Fingerprint Image”, *Proceedings of International Conference on Pattern Recognition*, vol. 3, pp. 756-759, 2002.

[12] W. Bender, D. Gruhl, N. morimoto, A. Lu, “Techniques for Data Hiding,” *IBM Systems Journal*, vol. 35, pp. 313-336, 1996.

[13] R. D. Preuss, S. E. Roukos, A. W. F. Huggins, H. Gish, M. A. Bergamo, P. M. Peterson, A. G. Derr, “Embedded Signaling,” *United States Patent* 5, 319, 735, 1994.

[14] R. B. Wolfgang, C. I. Podilchuk, E. J. Delp, “Perceptual Watermarks for Digital Images and Video*,” Proceedings of the IEEE*, vol. 87, issue 7, pp. 1108 – 1126, 1999.

[15] I. J. Cox, M. L. Miller, and A. McKellips, “Watermarking as communications with side information,” *Proc. of IEEE*, vol. 87, issue 7, pp.1127–1141, 1999.

[16] Jim Chou, S. Sandeep Pradhan, Kannan Ramchandran, “On the duality between distributed source coding and data hiding,” *Thirty-third Asilomar conference on signals, systems, and computers,* vol. 2, pp.1503–1507, 1999.

[17] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia,” *Technical Report 95-128*, NEC Research Institute, 1995.

[18] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, ”A secure, robust watermark for multimedia,” *In R. Anderson, editor, First Int. Workshop on Information Hiding*, volume Lecture notes in Computer Science 1174, pages 185–206, Springer, 1996.

[19] R. G. van Schyndel, A. z. Tirkel, C. F. Osborne, “A Digital Watermark,” *Proceedings of IEEE International Conf. on Image Processing ICIP-94*, vol.2, pp. 86-90, November 1994.

[20] H Yongjian, S.Kwong, “An image fusion based visible watermarking algorithm,” *Proceedings of the 2003 International Symposium on Circuits and Systems*, vol. 3, pp. III-794 – III-797, May 2003.

[21] S. P. Mohanty, K. R. Ramakrishnan, M. S. Kankanhalli, ”A DCT Domain Visible Watermarking Techniques for Images,” *IEEE International Conference on Multimedia and Expo*, vol. 2, pp. 1029 – 1032, August 2000.

[22] M. S. Kankanhalli; Rajmohan, K. R. Ramakrishnan,”Adaptive visible watermarking of images,” IEEE International Conference on Multimedia Computing and Systems, vol. 1, pp. 568 – 573, June 1999.

[23] P.-C. Su and C. C. Jay Kuo, "Information Embedding in JPEG 2000 Compressed Images," *ISCAS 2003, Security and Data Hiding I*, Bangkok, Thailand, May 25-28, 2003.

[24] A. Tefas, I. Pitas, "Multi-bit image watermarking robust to geometric distortions," *International Conference on Image Processing*, vol. 3, pp. 710 – 713, September 2000.

[25] S. Pereira, T. Pun, "Robust template matching for affine resistant image watermarks," *IEEE Transactions on Image Processing*, vol. 9, issue 6, pp. 1123 – 1129, June 2000.

[26] A. Tefas, G. Louizis, I. Pitas, "3D image watermarking robust to geometric distortions," *IEEE International Conference on Acoustics, Speech, and Signal Processing*, vol. 4, pp. IV-3465 - IV-3468, May 2002.

[27] H. Knowles, D. Winne, N. Canagarajah, D. Bull, "Towards tamper detection and classification with robust watermarks," *Proceedings of the 2003 International Symposium on Circuits and Systems*, vol. 2, pp. II-959 - II-962, May 2003.

[28] H. Quan and S. Guangchuan, "A Semi-Blind Robust Watermarking for Digital Images," *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2003)*, vol. 3, pp. III – 541 – 544, April 2003.

[29] H. Lu, R. Shen, F.-L Chung, "Fragile watermarking scheme for image authentication," *Electronics Letters*, vol. 39, issue 12, pp. 898 – 900, June 2003.

[30] C.-T Li, F.-M Yang, C.-S Lee, "Oblivious fragile watermarking scheme for image authentication," *IEEE International Conference on Acoustics, Speech, and Signal Processing*, vol. 4, pp. IV-3445 - IV-3448, May 2002.

[31] J. Fridrich, M. Goljan, A. C. Baldoza, "New fragile authentication watermark for images," *International Conference on Image Processing*, vol. 1, pp. 446 – 449, September 2000.

[32] R. Swierczyński, "Fragile watermarking using subband coding," *Proceedings of International Conference on Computer Vision and Graphics (ICCVG 2002)*, pp.748 – 753, September 2002.

[33] R. Sun, H. Sun, T. Yao, "A SVD- and quantization based semi-fragile watermarking technique for image authentication," *6th International Conference on Signal Processing*, vol. 2, pp. 1592 – 1595, August 2002.

[34] Y.-C Fan, W.-L Mao, H.-W Tsao, "An artificial neural network-based scheme for fragile watermarking," *IEEE International Conference on Consumer Electronics*, pp. 210- 211, June 2003.

[35] S.-K Lee, Y.-S Ho, "Fragile watermarking scheme using a simple genetic algorithm," *International Conference on Consumer Electronics, 2002 Digest of Technical Papers*, pp. 190 -191, June 2002.

[36] X.-G Xia, C. G. Boncelet, G. R. Arce, "Wavelet transform based watermark for digital images," *Optics Express*, vol. 3, pp. 497, December 1998.

[37] D. Kundur and D. Hatzinakos, "Digital watermarking using multiresolution wavelet decomposition," *Proceedings of IEEE ICASSP '98*, vol. 5, pp. 2969 - 2972, May 1998.

[38] L. Yongliang, W. Gao, M. Cui, Y. Song, "General blind watermark schemes," *Proceedings of Second International Conference on Web Delivering of Music*, pp. 143 – 149, December 2002.

[39] R. Tay, J. P. Havlicek, "Image Watermarking Using Wavelets," *The 2002 45th Midwest Symposium on Circuits and Systems, 2002. MWSCAS-2002*, vol. 3, pp. III-258 - III-261, 4-7 August 2002.

[40] J. J. Eggers, B. Girod, "Blind watermarking applied to image authentication," *IEEE International Conference on Acoustics, Speech, and Signal Processing*, vol. 3, pp. 1977 – 1980, May 2001.

[41] M. Kutter, "Performance Improvement of Spread Spectrum Based Image Watermarking Schemes through M-ary Modulation," *Swiss Federal Institute of Technology*, Lausane, Switzerland, http://itswww.epfl.ch:1248/kutter

[42] F. Hartung, B. Girod, "Digital watermarking of Raw and Compressed Video," *In Digital Compression Technologies and Systems for Video Communication, SPIE Proceedings Series*, vol. 2952, pp. 205-213, October1996.

[43] H. C. S. Rughooputh, R. Bangaleea, "Effect of channel coding on the performance of spatial watermarking for copyright protection," *IEEE 6th African Conference in Africa*, vol. 1, pp. 149-153, October 2002.

[44] A. Nikolaidis, I. Pitas, "Region-based image watermarking," *IEEE Transactions on Image Processing*, vol. 10, issue 11, pp. 1726 – 1740, November 2001.

[45] W.-G. Kim, C.-W. Lee, Won Don Lee, "A watermarking scheme for both spatial and frequency domain to extract the seal image without the original image," *Proceedings of the Fifth International Symposium on Signal Processing and Its Applications*, vol. 1, pp. 293 – 296, August 1999.

[46] W. N. Cheung, "Digital image watermarking in spatial and transform domains," *Proceedings of TENCON 2000*, vol. 3, pp. 374 – 378, September 2000.

[47] D. P. Mukherjee, S. Maitra, S. T. Acton, "Spatial Domain Digital Watermarking of Multimedia Objects for Buyer Authentication," *IEEE Transactions on Multimedia*, vol.6, issue 1, pp. 1-15, February 2004.

[48] J. J. K. O'Ruanaidh, W. J. Dowling, F. M. Boland, "Phase watermarking of digital images," *International Conference on Image Processing*, vol. 3, pp. 239 – 242, September 1996.

[49] M. H. Hayes, "The Reconstruction of a Multidimensional Sequence," *IEEE Transactions on Acoustics, Speech and Signal Processing*, pp. 140 -154, April 1992.

[50] J. -F. Delaigle, C. De Vleeschouwer, B. Macq, "Watermarking using a Matching Model Based on the Human Visual System," *Ecole thematique CNRS GDR-PRC ISIS Information Signal Images*, Marly le Roi, 1997.

[51] E. Koch, J. Zhao, "Towards Robust and Hidden Image Copyright Labeling," *Proc. Of IEEE Workshop on Nonlinear Signal and Image Processing*, Neos Marmaras, Greece, 452 – 455, June 1995.

[52] I. J. Cox, J. Killian, T. Leighton, T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *NEC Research Institute*, Technical Report 95 - 10, 1995.

[53] O.-H Kwon, Y.-S Kim, R.-H Park, "Watermarking for still images using the human visual system in the DCT domain," *Proceedings of the 1999 IEEE International Symposium on Circuits and Systems*, vol. 4, pp. 76 – 79, June 1999.

[54] J. Huang, Y. Q. Shi, Y. Shi, "Embedding image watermarks in dc components," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 10, issue 6, pp. 974 -979, September 2000.

[55] H. Lu, X. Shi, Y. Q. Shi, A. C. Kot, L. Chen, "Watermark embedding in DC components of DCT for binary images," *IEEE Workshop on Multimedia Signal Processing*, pp. 300 – 303, December 2002.

[56] C.-F Wu, W.-S Hsieh, "Digital watermarking using zerotree of DCT," *IEEE Transactions on Consumer Electronics*, vol. 46, issue 1, pp. 87 – 94, February 2000.

[57] J. J. K. O'Ruanaidh, T. Pun, "Rotation Translation and Scale Invariant Digital Image Watermarking," *Proc. of International Conference on Image Processing*, vol. 1, pp. 536-539, October 1997.

[58] M. Antonini, "Image Coding using Wavelet transform," *IEEE Transaction on Image Processing*, vol. 1, no. 2, pp. 205 -220, 1992.

[59] F. M. Boland, J. J. K. O'Ruanaidh, C. Dautzenberg, " Watermarking Digital Images for Copyright Protection," *IEE Conference Proceedings on Image Processing and its Applications*, no. 410, pp. 326 – 330, July 1995.

[60] M. Corvi, G. Nicchiotti, "Wavelet-based image watermarking for copyright protection," *Scandinavian Conference on Image Analysis SCIA '97*, Finland, June 1997.

[61] L. Xie, G. R. Arce, "Joint Wavelet Compression and Authentication Watermarking," *Proceedings of IEEE International Conference on Image Processing ICIP '98*, Chicago, 1998.

[62] J. R. Kim, Y. S. Moon, "A Robust Wavelet-based Digital Watermark Using Level-Adaptive Thresholding," *Proc. of the 6th IEEE International Conference on Image Processing ICIP' 99,* Japan, October 1999.

[63] D. Kundur, "Improved digital watermarking through diversity and attack characterization*," Proc. of the ACM Workshop on Multimedia Security '99*, pp. 53 – 58, Florida, 1999.

[64] P. Meerwald, "Quantization Watermarking in JPEG 2000 Coding Pipeline," *IFIP TC6/TC11 Fifth Joint Working Conference on Communications and Multimedia Security*, CMS '01, May 2001.

[65] Test Images are acquired from www.petitcolas.net/fabien/watermarking/image_database/

[66] P. Kovesi, "Image Features From Phase Congruency". *Videre: A Journal of Computer Vision Research*. MIT Press., vol. 1, no. 3, Summer 1999.

[67] W. B. Jackson, M. R. Said, D. A. Jared, J. O. Larimer, J. L. Gille, J. Lubin, "Evaluation of Human Vision Models for Predicting Human-Observer Performance," *Proc. SPIE Medical Imaging,* vol. 3636, 1997.

[68] V. Vanhoucke, "Blocking Artifact Cancellation in DCT Based Image Compression," Project Report Stanford University, 2000.
http://www.ee.columbia.edu/~marios/courses/e6820y02/project/papers/Block%20Artifact%20Cancellation%20in%20DCT%20Based%20Image%20Compression.pdf
[69] S-W Lee, "Improved Algorithm for Efficient Computation of the Forward and Backward MDCT in MPEG Audio Coder," *IEEE Trans. on Circuits and Systems-2: Analog and Digital Signal Processing*, vol. 48, no. 10, Oct. 2001.
[70] I. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transaction on Image Processing*, vol. 6, no. 12, pp. 1673-1687, Dec.1997.
[71] HSU, C. T., and WU, J. L. "Hidden Digital Watermarks in Images," *IEEE Trans. on Image Proc*. vol. 8, pp. 58-68, 1999.
[72] X. Xia, C. Boncelet, and G. Arce, "Multiresolution Watermark for Digital Images," Proc. *IEEE Int. Conf. on Image Processing*, vol. 1, pp. 548-551, Oct. 1997.
[73] J. R. Kim and Y. S. Moon, "A Robust Wavelet-Based Digital Watermark Using Level-Adaptive Thresholding," *Proceedings of the 6th IEEE International Conference on Image Processing ICIP '99*, pp. 202, Kobe, Japan, Oct. 1999.
[74] Z. Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli, "Image quality assessment: From error measurement to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 1, 2004.
[75] Z. Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli, "A Universal Image Quality Index," *IEEE Signal Processing Letters*, vol. 9, no. 3, pp. 81-84, 2002.
[76] A. K. Jain, Lin Hong, S. Pankanti, and R. Bolle, " An identity-authentication system using fingerprints," *Proc. of IEEE*, vol. 85, issue 9, pp. 1365 – 1388, September 1997.
[77] R. Khanna, S. Weicheng, "Automated fingerprint identification system (AFIS) benchmarking using the National Institute of Standards and Technology (NIST) Special Database 4," *Proceedings of IEEE 28th Annual 1994 International Carnahan Conference on Security Technology*, pp. 188-194, October 1994.
[78] X. Jiang and W.-Y. Yau, "Fingerprint minutiae matching based on the local and global structures," *Proc. 15th International Conference on Pattern Recognition*, vol. 2, pp. 1038 –1041, September 2000.

[79] W. Zhang and Y. Wang, "Core-based structure matching algorithm of fingerprint verification," *Proc. 16th International Conference on Pattern Recognition*, vol. 1, pp. 70 – 74, August 2002.

[80] B. C. Seow, S. K. Yeoh, S. L. Lai, and N. A, Abu, "Image based fingerprint verification," *Student Conference on Research and Development, SCOReD 2002*, pp. 58 – 61, July 2002.

[81] A. R. Roddy, "Fingerprint Features-Statistical Analysis and System Performance Estimates," *Proc. of the IEEE*, vol.85, issue 9, pp. 1390-1420, 1997.

[82] E. R. Henry, *Classification and Uses of Finger Prints*, Routledge, London, 1900.

[83] S. M. Farani Costa, J. M. V. De Oliveira, F. J. R. Fernandez, "A new paradigm on fingerprint classification using directional image," *Proceedings of XV Brazilian Symposium on Computer Graphics and Image Processing*, pp. 405, October 2002.

[84] C. I. Podilchuk, W. Zeng, "Image-adaptive watermarking using visual models," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 525-539, 1998.

[85] M. Kociolek, A. Materka, M. Strzelecki, P. Szczypinski, "Discrete Wavelet transform - Derived Features for Digital Image Texture Analysis," *Proc. of International Conference on Signals and Electronic Systems*, pp. 163-168, Sept. 2001.

[86] A. S. Lewis, G. Knowles, "Image Compression using the 2-D Wavelet Transform," *IEEE Transaction on Image Processing*, vol. 1, no. 2, pp. 244-250, 1992.