Multibiometric Security in Wireless Communication Systems

A thesis submitted for the degree of Doctor of Philosophy

by

Mojtaba Sepasian

Brunel University
School of Engineering and Design

April 2010

THIS PAGE INTENTIONALLY LEFT BLANK

Abstract

This thesis has aimed to explore an application of Multibiometrics to secured wireless communications. The medium of study for this purpose included Wi-Fi, 3G, and WiMAX, over which simulations and experimental studies were carried out to assess the performance. In specific, restriction of access to authorized users only is provided by a technique referred to hereafter as multibiometric cryptosystem. In brief, the system is built upon a complete challenge/response methodology in order to obtain a high level of security on the basis of user identification by fingerprint and further confirmation by verification of the user through text-dependent speaker recognition.

First is the enrolment phase by which the database of watermarked fingerprints with memorable texts along with the voice features, based on the same texts, is created by sending them to the server through wireless channel.

Later is the verification stage at which claimed users, ones who claim are genuine, are verified against the database, and it consists of five steps. Initially faced by the identification level, one is asked to first present one's fingerprint and a memorable word, former is watermarked into latter, in order for system to authenticate the fingerprint and verify the validity of it by retrieving the challenge for accepted user. The following three steps then involve speaker recognition including the user responding to the challenge by text-dependent voice, server authenticating the response, and finally server accepting/rejecting the user.

In order to implement fingerprint watermarking, i.e. incorporating the memorable word as a watermark message into the fingerprint image, an algorithm of five steps has been developed. The first three novel steps having to do with the fingerprint image enhancement (CLAHE with 'Clip Limit', standard deviation analysis and sliding neighborhood) have been followed with further two steps for embedding, and extracting the watermark into the enhanced fingerprint image utilising Discrete Wavelet Transform (DWT).

In the speaker recognition stage, the limitations of this technique in wireless communication have been addressed by sending voice feature (cepstral coefficients) instead of raw sample. This scheme is to reap the advantages of reducing the transmission time and dependency of the data on communication channel, together with no loss of packet. Finally, the obtained results have verified the claims.

Dedication

To:

My Family

ACKNOWLEDGEMENTS

First and foremost, thank God the almighty for providing me with this opportunity and granting me the capability to proceed successfully.

The author wishes to express his thanks to the numerous individuals from whom he has received support. In particular, Professor Wamadeva Balachandran for his supervision, encouragement, and valuable contributions to the technical content of this thesis.

I am also thankful to Dr Bahmanyar, Dr Mares and Dr Azimi for giving me the opportunity to work with them and to be educated in the fields outside of my course, and supporting me with the all needed to succeed. I am sure that without their help, I would not have finished my research in the most appropriate way. I really appreciate their help and in this great occasion, I would like to convey my gratitude to them.

Many thanks to Dr Salihi for sparing his time in helping me investigate and test different technologies, and guide me in analyzing the results.

I would also like to thank Mr Khodabakhshi, and Dr Zolgharni who have been very supportive during the time of my studies at Brunel University.

I would like to thank my family and friends for their encouragement and inspiration which enabled me to work hard throughout my life. Without their ongoing support, I would not have been where I am now and, hence I give all the credit to my parents for all the achievements. They have been instilling in me the sense of integrity and a desire to do the right including education.

ABBREVIATIONS

AFIS	Automated Fingerprint Identification System
AHE	Adaptive Histogram Equalization
ASI	Automatic Speaker Identification
ASV	Automatic Speaker Verification
BKS	Behavior Knowledge Space
COTS	Commercial Off-The-Shelf
CLAHE	Contrast Limited Adaptive Histogram Equalization
CMS	Cepstral Mean Subtraction
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DoS	Denial of Service
DP	Decision Profile
DT	Decision Template
DTW	Dynamic Time Warping
DWT	Discrete Wavelet Transform
ECG	Electrocardiograph
E-Field	Electric Field
ERR	Equal Error Rate
FAR	False Acceptance Rate
FER	Failure to Enroll Rate
FOP	Fiber Optic Plate

FRR	False Rejection Rate
FrFT	Fractional Fourier Transform
FTIR	Frustrated Total Internal Reflection
GMMs	Gaussian Mixture Models
HE	Histogram Equalization
HMM	Hidden Markov Models
IBG	International Biometric Group
IDFT	Inverse Discrete Fourier Transform
IDWT	Inverse Discrete Wavelet Transformation
IFFT	Inverse Fast Fourier Transform
ITU	International Telecommunication Union
MAS	Max Score
MEMS	Micro-Electromechanical Systems
MFCCs	Mel Frequency Cepstral Coefficients
MIS	Min Score
MSI	Multi Spectral Imaging
MW	Matcher Weighting
OS	Order Statistics
SS	Simple Sum
RASTA	Real Active SpecTrAl
RDC	Relative Dielectric Constant
RF	Radio Frequency
ROI	Region of Interest
SVM	Support Vector Machine
TM	Template Matching
TIR	Total Internal Reflectance

UW	User Weighting
VQ	Vector Quantization
WSQ	Wavelet Scalar Quantization

Table of Contents:

CHAPTER 1 General Introduction

CHAPTER 2 Literature review

CHAPTER 3 Speaker Recognition in Wireless Application

CHAPTER 4 Liveness and Spoofing in Fingerprint Identification: Issues and Challenges

CHAPTER 5 Multibiometric Cryptosystem in Wireless Communication

CHAPTER 6 Watermarked Fingerprint (Tested Over Wireless Network)

CHAPTER 7 Conclusions and Recommendation for Future Work

List of Figures

List of Tables

Chapter 1

General Introduction

Enhancing the security in various scenarios such as used for national identification, network access and border pass, has resulted in an unprecedented growth in the use of biometrics. The ever-increasing application of biometrics extends also to wireless world for the obvious reason of important role security plays in this field. An example can be found in authorized mobile devices where an authorization based on biometric identification allows the user to gain access to data such as needed for bank transactions. In addition, the recent upgrading of the E-Health and E-Commerce to M-Health and M-Commerce [1-5] increased the contribution of biometric authentication in disparate wireless applications (e.g. [6, 7]) and this is expected to increase even more in the near future. Wireless networks have significant advantages over wired networks such as elimination of cables and freedom of mobility. Whereas the disadvantages are lower channel capacity (i.e. limited spectrum available, power restrictions, noise levels), Denial of Service (DoS), eavesdropping (signal is in the open air and data is not encrypted unless the protocol is encrypted), theft or loss of device (due to size and portability) and Masquerading (i.e. rogue clients pretend to be legitimate endpoint), etc. Currently the use of wireless networking is expanding way faster than before by the introduction of new technologies such as 4G, and WiMax. These networks regardless of whether they use WiMAX or Wi-Fi LANs as defined in the IEEE 802.11 standard are inherently less secure than wired counterparts due to the lack of physical infrastructure [8, 9].

The main issue here is making sure to have a control measure in place prior to establishing a connection, so that access is restricted to the authorized users only. Biometrics can deliver outstandingly here as compared to the traditional solutions for access control, taking into account the rare chances of data being lost or stolen. The only issue is that there is no single biometric technology, which suffices in terms of protecting from various types of threats. Unimodal biometrics in the context of security raises several design limitations such as noise in input data, intra-class variation, interoperability, vulnerability against spoof attacks and inter-class similarities [32].

Some of these restrictions can be alleviated through multimodal biometric approaches by providing multiple evidences of the same identity [35]. As with multimodal biometric, there are inherent problems with utilizing identification systems in open area such as wireless communications that seem likely to prevent further attempts at improving such approach. The main problems are deeply rooted starting first with the mobility of wireless systems and the availability in large numbers, making the system more intolerable against the spoofing and attack. The second issue is the incompatibility of some biometric technologies and algorithms to allow it be employed over wireless medium. There are other problems as well voting against using multibiometric, the biometric technology market is changing rapidly, standards are not widely supported, and performance is depending on the operation environment. In addition, life cycle cost of a biometric technology, i.e. enrollment, integration, and maintenance is a source of concern. Last but not least, parallel to improving the biometric technologies, various types of attacks and forges are being reintroduced and hence, suggested multibiometric system should be able to adapt and evolve. Therefore, once the compatible multibiometric algorithm is found, analysis of the wireless environment must be perfected to avoid any possibility of future attacks. While in a system based on one-to-one matching database can be decentralized, in wireless applications on the other hand it should take the opposite form. This means the database as well as data should be protected against the imposter attack during transmission and accessing database. In other words, the acquired sample must be transmitted securely to the location of template in order to perform at the decision level. Otherwise, incorrect storage or transmission in a biometric system can affect the overall performance of the system especially in wireless communication.

All in all, storing biometric features in a server is not an appropriate technique unless; some countermeasures are employed to make the data inaccessible for imposter (e.g. encryption or anonymous techniques). This thesis is about implementing an encrypted multiple biometric system over wireless networks.

1.1 Aim and Objectives of the Research

The main aim of this research is the development and investigation of the multibiometric cryptosystem based on combining the fingerprint authentication with that of speaker recognition as access control for secure wireless communication. In addition, this research investigates Wi-Fi, 3G, and WiMAX platforms as end-to-end communication channels. As a final point, it will carry out simulation studies of a number of typical scenarios. Such a system when fully developed could replace PIN or ID card as authentication in any feasible application (e.g. commercial and health care environments). Aside from the main purpose, this research also looks at various performance measurements of selected biometric devices and explains what each measurement means and how it can affect whether or not the user of the device is being accepted or rejected. As mentioned above, implementing biometric solutions comes with inherent problems, mainly the accuracy level and increased cost of maintenance. The final aim of this research is to recognize the base biometric identifications and to study the architectures and solutions for merging these biometric implementations and simulation of them to yield the highest level of accuracy and reliability. The conclusion and further work will highlight the process of this project from beginning to the end, indicating the ways to improve on. The following steps are taken in order to meet the main objectives of this research:

- To study and investigate the feasible biometric identification over wireless devices (e.g. laptop, PDA and, Mobile Phone);
- To develop and investigate the multibiometric cryptosystem based on fingerprint authentication combined with speaker recognition as access control for secure wireless communication. To do this, main requirements for either of the components are defined and addressed;
- To revise and investigate the existing weaknesses in the prevailing security of fingerprint and speaker recognition in wireless communication (e.g. 3G and WiMAX);
- To develop and investigate the performance of a three-step novel approach proposed for preprocessing the fingerprint identification, using CLAHE (Contrast Limited Adaptive Histogram Equalization) together with applying 'Clip Limit', standard deviation analysis and sliding neighborhood as fingerprint image enhancement algorithm;

- To design a method to embed and extract the watermark message into and from the enhanced fingerprint image by using the DWT (Discrete Wavelet Transform);
- To assess the performance of multibiometric security system to implement secure and real time wireless communication, this is studied over Wi-Fi, 3G, and WiMAX platforms as end-to-end communication channels.

1.2 Proposed Multibiometric Cryptosystem for Implementing Secure Wireless Communication

In brief, the system is built upon a complete challenge/response methodology in order to obtain a high level of security on the basis of user identification by fingerprint and further confirmation by verification of the user through text-dependent speaker recognition. This proposed system consists of two parts, enrolment, and verification, which are detailed, in Chapter 5. First, the enrolment phase by which the database of watermarked fingerprints with memorable texts along with the voice features, based on the same texts, is created by sending them to the server through wireless channel. Later in the verification stage, claimed users, ones who claims are genuine, are verified against the database, and it consists of five steps. Initially faced by the identification level, one is asked to first present one’s fingerprint and a memorable word, the former is watermarked into latter, in order for the system to authenticate the fingerprint and verify its validity by retrieving the challenge for accepted user. The following three steps then involve speaker recognition including the user responding to the challenge by text-dependent voice, server authenticating the response, and finally server accepting/rejecting the user. Figure 1.1 illustrates the different stages of this proposed system from beginning to the end.

In order to implement fingerprint watermarking, i.e. incorporating the memorable word as a watermark message into the fingerprint image, an algorithm of five steps is developed and explained in Chapter 6. The first three novel steps having to do with the fingerprint image enhancement (CLAHE with 'Clip Limit', standard deviation analysis and sliding neighborhood) are followed with two further steps for embedding, and extracting the watermark into the enhanced fingerprint image utilizing Discrete Wavelet Transform (DWT).

In the speaker recognition stage, the limitations of this technique in wireless communication are addressed by sending voice feature (cepstral coefficients) instead of raw sample in Chapter 3. This scheme is to reap the advantages of reducing the transmission time and dependency of the data on communication channel, together with no loss of packet. Finally, in order to assess the performance of proposed system in wireless communication, simulations and experimental studies have been carried out for each phase in Chapter 6. The medium of study for this purpose includes Wi-Fi, 3G, and WiMAX.

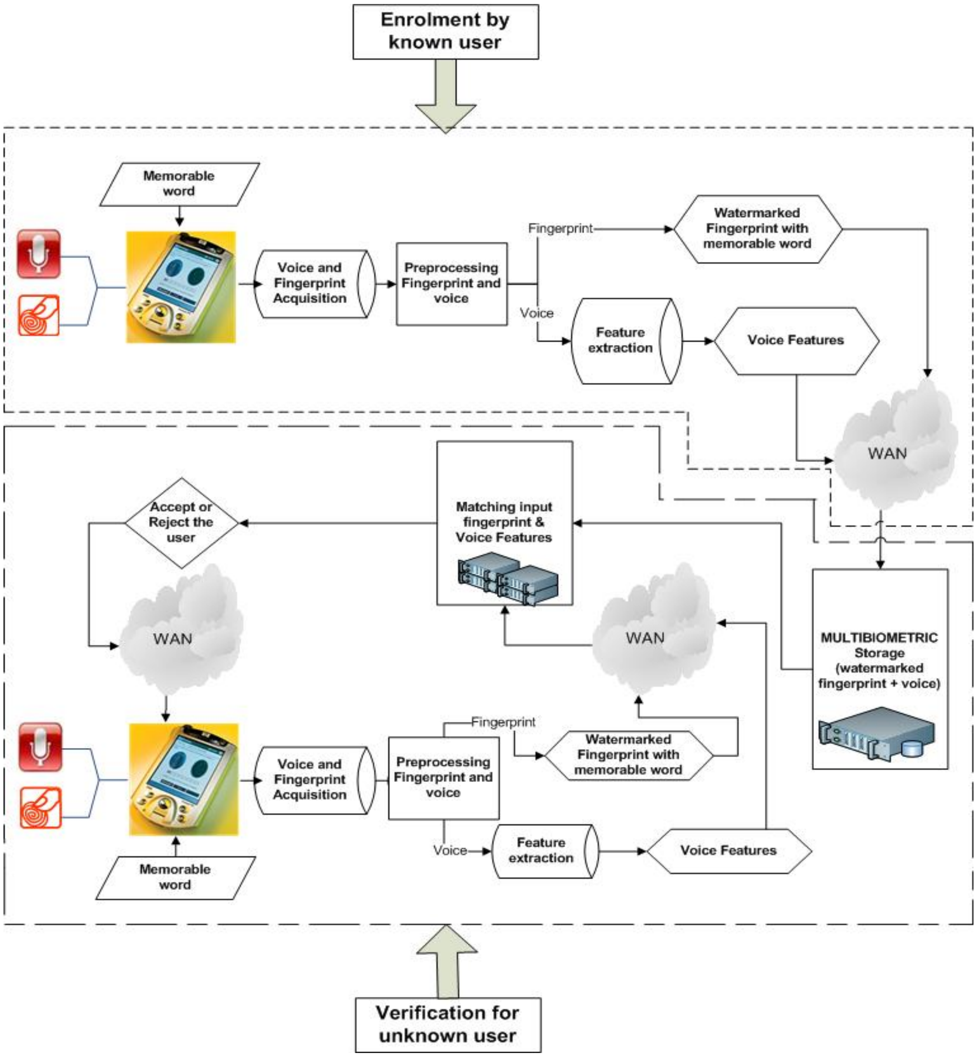

Enrolment by known user
Memorable word
Voice and Fingerprint Acquisition
Preprocessing Fingerprint and voice
Fingerprint
Watermarked Fingerprint with memorable word
Voice
Feature extraction
Voice Features
WAN
Accept or Reject the user
Matching input fingerprint & Voice Features
WAN
WAN
MULTIBIOMETRIC Storage (watermarked fingerprint + voice)
Fingerprint
Watermarked Fingerprint with memorable word
Voice and Fingerprint Acquisition
Preprocessing Fingerprint and voice
Voice
Feature extraction
Voice Features
Memorable word
Verification for unknown user

Figure 1.1: Block Diagram of Proposed Multibiometric System in Wireless Communication

1.3 Contribution to Knowledge

The following are the major claimed contributions to knowledge of this research:

- To improve the performance requirements of unimodal biometric and to cover its limitations, a compatible multibiometric system has been introduced based on combining the fingerprint authentication with that of voice recognition as access control for secure wireless communication system.

- The possible limitations of fingerprint and voice recognition in wireless communication have been investigated and multibiometric cryptosystem has been proposed and developed to address these limitations based on the watermarking the enhanced fingerprint image with the same text, which is used as text dependent speaker recognition (Figure 1.1).

- A novel three-step preprocessing for the fingerprint identification has been developed, using CLAHE (contrast limited adaptive histogram equalization) together with applying 'Clip Limit', standard deviation analysis and sliding neighborhood as image enhancement algorithm. The motivations for developing this method, its phases, and its possible advantages through a simulated investigation have been presented.

- To increase the security of fingerprint image in wireless communication, a new watermarking technique has been introduced and developed based on the embedding and extracting the watermark message in to enhanced fingerprint image by using the DWT (Discrete Wavelet Transform).

- The acceptable results have been achieved by applying and analyzing the effect of the proposed multibiometric cryptosystem and watermark algorithm to implement secure and real time wireless communication systems and Wi-Fi, 3G, and WiMAX platforms as end-to-end communication channels have been investigated.

In the following Chapters, a detailed description of each of these contributions is provided.

1.4 Structure of Thesis

The main body of the thesis comprises seven major Chapters, starting with the introduction in Chapter 1, and an Appendix containing the author list of publications. Chapter 2 presents an extensive review of literature on the application of biometrics and considers the implementation of these multiple biometric system over wireless communication system. This Chapter starts with a review of the advantages of biometrics and its requirements in section 2.1. In section 2.2, the various biometric techniques are compared in terms of weaknesses, strengths, cost, accuracy, distinctiveness perceived intrusiveness, and feasibility in wireless applications. Section 2.3 reviews the different types of biometric modules and processes. Section 2.4 indicates the difficulties and restrictions of unimodal biometric systems. Sections 2.5 propose appropriate biometrics over wireless application. Section 2.6 covers the rewards of unimodal biometric systems by multimodal biometric systems. Section 2.7 categorizes a fusion strategy for multibiometric in three categories, and the advantages and disadvantages of each fusion are discussed. Finally, section 2.8 is a conclusion of this Chapter.

With the main concern being how to provide access only to authorized users, Chapter 3 is devoted to investigating the limitations and merits of voice recognition as a way of securing wireless networks. First in section 3.1, speaker recognition as applied to wireless technology is investigated. In section 3.2, characteristics of this method are introduced. In section 3.3, a review of some of the well-known and popular features includes Mel Frequency Cepstral Coefficients (MFCCs), Cepstral Mean Subtraction (CMS), and RASTA filtering is presented. Section 3.4 describes some of the most famous classification and pattern-matching techniques that include Template Matching (TM), Dynamic Time Warping (DTW), Vector Quantization (VQ), Hidden Markov models (HMM), and Gaussian Mixture Models (GMMs). Section 3.5 summarizes these reviewed techniques from beginning to the end suggesting ways to improve. Finally, based on this analysis, the most suitable speaker recognition algorithm to apply over wireless communications is selected and presented in section 3.6.

Chapter 4 presents a review of possible techniques to detect liveness of fingerprint in patents and published literature. In this Chapter, an attempt has been made to assess and evaluate the performance of each technique and discuss their effectiveness and possible limitations. In Chapter 4, these methods are categorized into either voluntary or involuntary. Section 4.1 is devoted to critical review of various types of fingerprint scanning techniques. Section 4.2 reviews different kind of attack at sensor level and appropriate countermeasures are proposed. Finally, Section 4.3 is designated to summary and discussion.

Although, the fingerprint authentication system presents certain advantages from the protection viewpoint, it is from the enrolment to the verification level susceptible to various types of threats and attacks. Therefore, providing the software, hardware, and advanced algorithms to deal with this intolerability against spoofing and fraud, remains an issue of concern when employing fingerprint in wireless device. These specific aspects are investigated in Chapter 5. In Section 5.1, security challenges and requirements in wireless applications are explored. Section 5.2 describes different fingerprint image storage in wireless application. In Section 5.3, a review of the possible attacks at template and data communication level is carried out. Section 5.4 presents various countermeasures and protection methods against these possible attacks. Finally, limitations of using fingerprint techniques will be addressed through, the use of watermarked fingerprint with text dependent speaker recognition as proposed system in Section 5.5.

Chapter 6 is organized as follows: section 6.1 has introduced fingerprint characteristics. Section 6.2 provided a literature review with the aim of giving a full account of the technique resulting in desirable fingerprint identification with high performance. In section 6.3 performance of a novel three-step procedure for the fingerprint image enhancement are investigated, using CLAHE (contrast limited adaptive histogram equalization) together with applying 'Clip Limit', standard deviation analysis and sliding neighborhood as stages during processing of the fingerprint image. Section 6.4 is designated to develop and evaluate the two-step process for the fingerprint watermarking technique, embedding the watermark message and extraction this message from the watermarked fingerprint image. Section 6.5 described the methodology and the design of the five-step challenge/response process based on proposed method in Chapter 5. Section 6.6 is devoted to the simulation methods and environment of projected system. Subsection 6.6.1 and 6.6.2 present the simulation results for sending watermarked fingerprints and voice features over WiMAX, Wi-Fi and 3G. Subsection 6.6.3 is designated to the analysis of the presented results and section 6.7 is dedicated to summary of this chapter.

Finally, Chapter 7 is dedicated to conclusion of this research and suggestion for further research that may improve the accuracy and security of the proposed system.

Chapter 2

Literature Review

Introduction

The recent improvements and innovations in networking, communication, and mobility, particularly in wireless network such as Wi-Fi and WiMAX, have increased the demand for security and identification in these fields. In comparison to wired networks, wireless technologies are less robust against various types of threats and attacks, due primarily to mobility and the availability of data in open areas [9]. Inherent problems with utilizing identification systems in open applications like wireless communication seem likely to prevent further attempts to improve this approach. This limitation can be addressed by using biometrics as an access control, which has significant benefits when compared with traditional methods such as the inability to be lost or stolen. However, unimodal biometrics still has some significant limitations such as noise in the inputs data, which can be covered by using multiple biometric traits [35]. This Chapter presents an extensive review of literature on the application of biometrics and considers the implementation of these multiple biometric system over wireless communication system.

2.1 The Advantages and Requirements of Unimodal Biometrics

In the past, only passwords, ("what you know") and ID cards ("what you have") were known to restrict access to systems but these methods can be lost, stolen, or easily forged. The solution to this matter is biometrics, which cannot be borrowed, stolen, or forgotten. The word biometric comes from the Greek words bios (life) and metrikos (measure). Biometrics is based on individual biological (e.g. fingerprints, hand geometry, and facial recognition) or behavioral characteristics (e.g. voice and signature) of the human body (“what you are”).

In the case of a password-based system, the security of the entire system is only as safe as the weakest password and if the password is disclosed, there is no way for the system to distinguish between the genuine user and an imposter. Biometric based systems are significantly difficult to copy, share, and distribute. They also cannot be forgotten or disclosed, since biometrics data systems require the user to be present at the point of recognition. At the same time, increase in the demand of identification security in sensitive areas and communication devices have increased the contribution of biometric authentication in various applications such as E-Health and E-Commerce. Therefore, it is not complicated to understand the necessity of biometric traits as identification in various applications and scenarios.

2.1.1 List of Requirements

There are number of firm requirements for both physical and behavioural human characteristics, which should be satisfied in order to be an acceptable biometric technique [10, 26, 32]. These requirements for such characteristics comprise:

1. Permanence: characteristic should be invariant with time;
2. Universality: possessed and observable on all people;
3. Uniqueness: different across users;
4. Performance: achievable recognition accuracy and speed;
5. Unforgeable (circumvention): not defeated by disguise or counterfeit;
6. Acceptability: acceptance by user, not objectionable to display by users;
7. Collectability: the characteristic can be measured quantitatively.

In addition to the aforementioned requirements, there are a number of evaluation criteria in biometric techniques over wireless application that leads this research to design and implement successful security system.

8. Feasibility of the techniques on wireless device;
9. Failure to acquire rates (Reliability);
10. Scalability, especially for use with large data bases;
11. Accessibility: easily displayed to a sensor;

12. Enrollment time (Is the failure to enroll acceptable);
13. Environmental restrictions, limitations, hindrances;
14. Integration with other operations or policies;
15. Business process and policies requirements;
16. Management of enrollment;
17. Vulnerabilities and its consequence for each biometric technology;
18. Counter measures (Is the biometric system robust against spoofing);
19. Privacy issues.

2.2 A Comparison of Biometric Traits over Wireless Communication

As shown in the previous sub section (2.1.1), satisfying the following requirements is mandatory for all biometric identifiers. These requirements are universality, distinctiveness, permanence, collectability, performance, acceptability, and circumvention. Each biometric system should be harmless for the user, have acceptable recognition accuracy, and speed with reasonable resource requirements [10]. In fact, there is no best single biometric, because there is no set of criteria for all situations. Nevertheless, each biometric has its strengths and limitations and the choice typically depends on the application but being sufficiently robust to various fraudulent methods is a minimum requirement for the appropriate technology. In this section, several well known biometric techniques are described, analyzing limitations, robustness and the feasibility of these techniques on wireless devices, and evaluating authentic applications.

2.2.1 **Face**:

This technique is based on machine recognition of faces from still and video images and it has a high degree of acceptability due to the fact that method of obtaining face images is not disturbing. Currently the two techniques being used as identification based on face recognition comprise: (a) Transform approach [11, 59], in which the universe of the facial image domain is represented using a set of orthonormal basis vectors and the most popular basis vectors are eigenfaces. The approach transforms face images into a small set of characteristic feature images known as eigenfaces [56]. Two faces are identical if they are sufficiently “close” in the eigenface feature space that is resulting from the covariance analysis of the face image population. However, as it is shown experimentally by Belhumeur et al. [15], the proposed “Fisherface” method has error rates that are lower than Eigenface technique. (b) Attribute-based approach: facial attributes such as nose and eyes, are extracted from the face image and the invariance of geometric properties among the face landmark features is used for recognizing features [12]. However, this method is non-intrusive, it may suffer from facial masquerade, and research studies show that it is not easy to develop face recognition techniques, which do not suffer from problems with the effects of aging, facial expressions, slight variations in the imaging environment and variations in pose of face with respect to camera [50]. The main issues to utilize face recognition in wireless devices are possibility of face appearance change and imaging conditions. Despite this, recently cameras have been successfully integrated into mobile devices providing a novel possibility of using face recognition biometrics [14].

2.2.2 Hand and Finger Geometry:

This method scans some features related to a human hand such as length of fingers, width, thickness, and curvatures, which are relatively invariant for each person. In this technique, patterns can be extracts frontal and side view images of the palm flatly placed on a panel with outstretched fingers. However, finger geometry is not as mature as that for hand geometry, it is more compact and as it is claimed, more accurate than hand geometry. The main advantage of this system is its compact size and the requirements of the hand are very small (9 bytes) which is a valuable feature for bandwidth and memory limited systems (e.g. mobile phone). Several hand geometry technologies have developed such as electro-mechanical devices and solid-state electronic scanners. This technique can protects privacy of the user better than other biometrics such as fingerprint due to complexity of templates to be accurately “reverse engineered” to identify the users. In addition, hand geometry has a high level of acceptability as an identity authentication application and it could be used for blind persons. However, it suffers from limited distinctiveness and limited flexibility of the palm, e.g. those suffering from arthritis. Furthermore, it is not unique, permanent (the hands change due to natural, age and environmental changes), and it cannot be used as identification of an individual from a large population of identities [13, 50]. In order to limit the constraints usually posed on the environment and the placement of the hand, Malassiotis et al. [16] proposed a biometric authentication system based on measurements of the user's three-dimensional (3-D) hand geometry. This technique relies on a novel real-time and low-cost 3-D sensor that generates a dense range image of the scene and therefore, greatly contributes to the unobtrusiveness of the system. Furthermore, hand geometry is not affected by variations in illumination, obstructions, etc. In spite of the above advantages, it is not feasible to employ hand and finger geometry in majority of wireless devices due to the sensor size requirement [40].

2.2.3 **Iris**:

This technique is based on visual texture of the human iris, which can be determined by the chaotic morphogenetic processes during embryonic development and it is claimed to be distinctive for each person and each eye. The most unique phenotypic feature visible in a person's face is the detailed texture of each eye's iris [50, 57] and Iris recognition is one of the most powerful techniques for biometric identification ever developed [53]. An ordinary CCD camera with a resolution of 512 dpi captures images. The identification error rate in this technique is very small and the constant length position invariant code is a fast method of iris recognition. Acquiring an iris image requires the patience of the user in order for the image of iris to be registered in the inner imaging area and to ensure the iris is at a fixed distance from the focal plane of the camera [50]. In a different approach, Matey et al. [53], present Iris on the Move (IOM) system that is, enable to capture of iris images of sufficient quality for iris recognition while the subject is moving at a normal walking pace through a minimally confining portal. However, iris recognition is not generally employed in mobile devices, due to the imaging conditions, uncomfortable operation, and low acceptability [14].

2.2.4 **Keystroke Dynamics**:

This technique is based on the hypothesis that in typing a phrase or a string of characters, the typing dynamics or timing pattern can be measured and employed for identity verification. In addition, the authentication method based on keystroke dynamics can be used to verify the ongoing presence of the user at an input device (e.g. a user could be periodically prompted to type in the password) [17]. Although this behavioral biometric is not unique enough for each user as a sign of identity has, it can be used for the design of more robust authentication systems than traditional password when implemented in conjunction with traditional schemes [21]. However, this identifier suffers from various weaknesses. For instance, it is not unique enough to establish the identity of the user and it depends on the keyboard and person's emotions. In addition, it is less acceptable if the keyboard is continuously monitored [14].

2.2.5 Retinal Scan:

This technique is based on capturing the surface of the retina and comparing nerve patterns and blood vessels in the retina. The main advantage of this system is its accuracy since it is not easy to impersonate or replicate. However, it is not generally accepted, as the user must be trained to use it. The user is required to look into an eyepiece and focus on a specific spot in the visual field. In addition, retinal vasculature can be influenced by medical conditions (e.g., hypertension) and the required hardware is expensive compared to other methods [50]. Therefore, these issues reduce the public acceptability of retinal scan based biometrics and prevent the application of retina scans in wireless devices.

2.2.6 Signature:

This method comprises each user signing his/her name, known as a signature. As compared to an offline signature, an online signature is more robust as it stores dynamic features like azimuth, elevation, and pressure signals in addition to position trajectories [54]. Signature is a behavioral biometric and it is influenced by physical and emotional conditions of the signatories [18, 22]. Generally, there are two approaches to automatic online signature verification including parametric and functional. The parametric approach is based on comparing specific features of signatures that are typically global (e.g. total time taken). In the parametric approach, a signature is described compactly therefore; the enrolment data size is considerably small and constant. In addition, it is more reliable against the variations in local regions, which are common in signatures. While function-based approach relies on comparing specific functions such as position coordinates versus time, velocity, acceleration each versus time along the entire signature [54, 55]. The permanence in this technique is arguable and it is not secure enough due to the possibility of the change in the signature [14].

2.2.7 **Voice**:

Voice is a characteristic of an individual, which is not expected to be satisfactorily unique to permit identification of a person from a large database of identities [50]. Speaker recognition is the process of automatically recognizing the user by using speaker specific information included in speech waves. Speaker recognition can be classified into speaker identification (process of determining from which of the registered users a given utterance comes) and speaker verification (process of accepting or rejecting the identity claim of a user). In addition, speaker recognition can be categorized in two different ways include text-dependent and text-independent methods. Text-dependent is based on restricting utterances to predetermined words or sentences that are same for both training and recognition while Text-independent is not based on a specific text being spoken [23]. Although, it is more difficult to design a text-independent system than a text-dependent system, it is more robust against fraud. Despite, speaker recognition is an acceptable biometric in the majority of societies and of course over the phone, it is not sufficiently distinctive as an identifier in large databases and the quality of the voice signal can be degraded by the communication channel [32]. In addition, this technique is less acceptable in public places, due to the privacy issue, and also a person's voice can be changed unintentionally because of emotional, health conditions, stress, or even on purpose as some people can imitate others. This technique has already been applied to wireless devices, particularly mobile phones and majority of the wireless devices. Although, voice is not considered for all purposes and environment have a strong impact on the performance [14], sometimes it is the only possible biometric trait with sufficient security (as a verification method) to be used over the phones or wireless devices.

2.2.8 **Fingerprints:**

Fingerprinting is one of the more mature technologies used in criminal investigations and it can be captured either by scanning an inked impression of a finger or by using a live-scan fingerprint scanner. A fingerprint image is made of a spatial map of the friction ridges of the skin and the valleys between them. In order to find out if two images are a matching pair, an algorithm of identification is needed to compare two fingerprints by examining the "landmarks" of ridges and valleys. In the majority of the current fingerprint matching systems, the features employed in the matching process are the fingerprint minutiae, mainly ridge bifurcation and ridge ending. This is due to the following reason: (1) minutiae capture much of the individual information, (2) minutiae-based representations are storage efficient, and (3) minutiae detection is relatively robust to various sources of fingerprint degradation. Minutiae-based fingerprint matching transforms fingerprint image into a minutiae map and generally involves preprocessing, ridge direction and ridge width, enhancement, and minutiae detection [52, 60]. Using fingerprints as an identification system is very popular today and has almost become a synonym for biometric systems. Fingerprinting is suitable for a large number of recognition applications e.g. the FBI fingerprint database exceeded 200 million fingerprints and is growing continuously. In addition, fingerprints are very distinctive and fingerprint details are permanent even if there are temporary cuts or bruises on the skin [18].

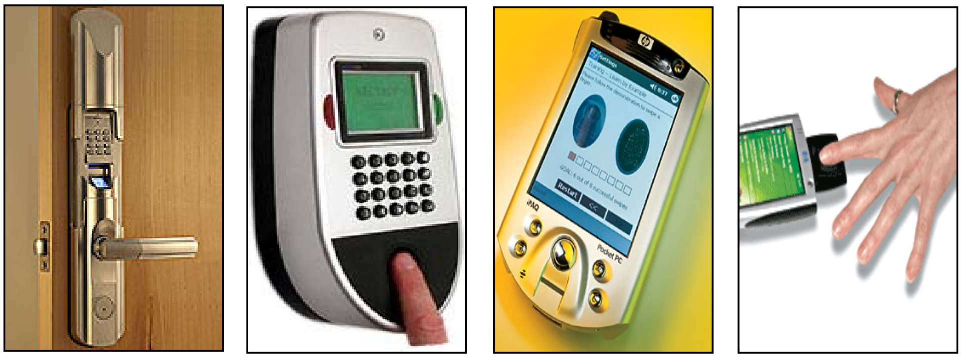


Figure 2.1: From left to right Lock, Corporate [27], PDA with fingerprint, and Fingerprint Cards provide in mobile phone [58]

Fingerprint sensors are one of the most accepted and developed biometric techniques in wireless device since it is quite small and relatively inexpensive with good performance. In addition, it is an appropriate technique for a large number of recognition applications. This technique is recognized by various mobile and handheld companies as an authentication method in their devices such as personal digital assistant or mobile phone that offers biometric security through a built-in fingerprint scanner (Figure 2.1) to restrict access to the devices. In addition, various wireless devices include fixed and mobile equipment with fingerprint recognition sensor such as Lock Secure, and Corporate Access Control Locks (Figure 2.1). Small size, inexpensive price, good performance of sensors, convenience, and user-friendliness are the key drivers for embedding fingerprint sensor in wireless devices such as notebooks and mobile phones. The major problem in utilizing fingerprints in mobile device is the varying image quality due to population characteristics and environmental factors [14]. Therefore, providing the software to deal with the alignment and quality of the image is an issue of concern when employing fingerprints in wireless devices. These issues will be further discussed in Chapter 6.

2.2.10 Biometrics Market and Revenue

Iris, DNA, retina and fingerprints are the most universal, unique and permanent biometrics. In addition, user acceptability is high when features can be obtained in a non-obtrusive way therefore; voice, face, and fingerprints are the best biometric identifiers in terms of acceptability. According to the biometric market report by the International Biometric Group (IBG) while fingerprints, iris, and alternative biometric technologies are still expanding, other biometric techniques, lack the potential to obtain market relevance [29]. Competition in biometric technologies pricing is very hard and therefore it is important to trade off between the benefits of new technologies and the costs associated with it.

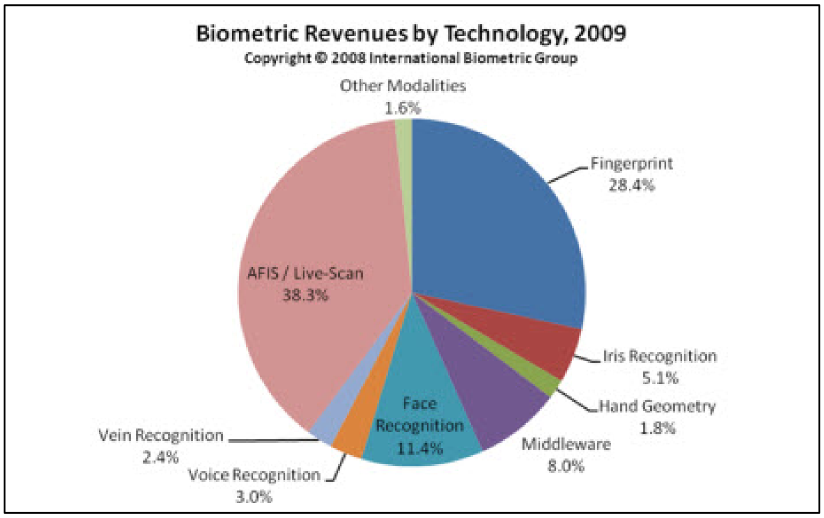


Figure 2.2: Biometric Market Report of International Biometric Group [29]

Figure 2.2 shows the Biometric market report of various biometric traits in the year 2009. Fingerprint-based biometric systems were the leading biometric technology in terms of market share with more than 60% (AFIS/live scan and fingerprint) of biometric revenue and face recognition was second with 11.4%. In addition, fingerprints with more than 50% and face scan with 12.9% were leading technologies in 2007 that is reported by International Biometric Group, so from 2007 until now using fingerprint technology is increasing. Figure 2.3 shows annual revenue projections from 2009 through 2014 for the eight leading biometric technologies as well as multimodal biometrics. Therefore, it is not difficult to predict the leadings biometric technologies for 2020. Every biometric technology is categorized based on the scores it attains in terms of ease-of-use, cost, accuracy, FAR, FRR, size, habituation, and distinctiveness perceived intrusiveness. In fact, the market for each biometric technology is directly dependent on the strengths and weaknesses of that technology.

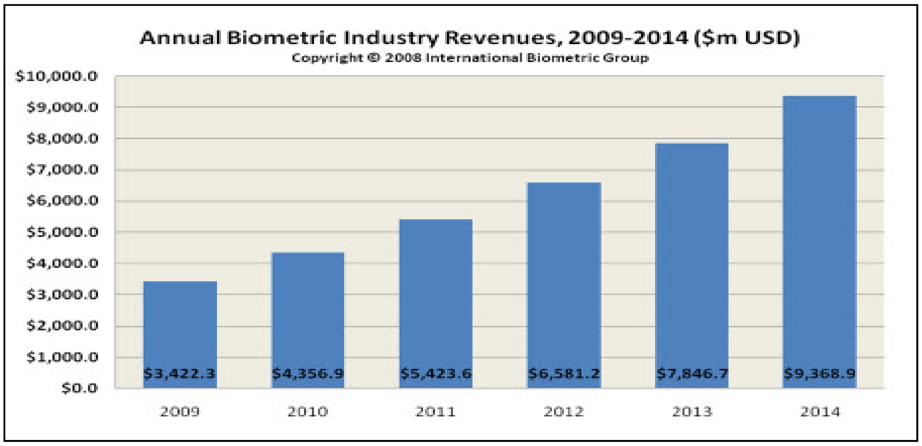


Figure 2.3: Annual revenue projections from 2009 through 2014[29]

2.3 Types of Biometric Modules and Processes

A biometric system is designed using the four main modules. These modules are sensor (captures the biometric data of an Individual), feature extraction (the acquired data is processed to extract a set of features), matcher (matching scores are generated by compare the extracted features against the stored templates), and system database module (which is used to store the biometric templates of the enrolled users). There are two distinct phases in the operation of biometric systems, enrolment, and verification/identification. The template is created during enrolment process; the enrolment process may require the individual to provide multiple instances of biometrics trait. Identification is commonly defined as the matching of a single biometric sample set against a database of samples. This entails that the user’s biometric trait is matched against all previously enrolled samples and generating the scores for each comparison. In general, the highest score exceeding the threshold results in a match. The verification or authentication means where a person's claimed identity must be confirmed or denied. This involves calculation of a similarity between a claimed biometric sample with an enrolled template. The verification mode is a "one-to-one" comparison while, identification means where a person's identity must be initially established and it is “one-to-many" comparison process [10, 26, 32].

2.4 Restrictions of Single Biometric Systems

It is important to note that some techniques, such as finger print recognition or retinal scanning, may offer high accuracy (especially retina scanning) while also having a high data collection error rate or low user acceptability. In both cases, their employment may not be appropriate for some applications due to the high level of co-operation required by the user or the social or psychological factors. Voice and face recognition are considered easy to use and normally acceptable by potential users, while their accuracy is currently less than some other biometric technologies, especially in unconstrained environments such as where background sound and illumination is variable. However, recently biometric authentication has experienced considerable improvements in reliability and accuracy, even the best biometrics to date are still facing numerous problems [30]. Zhang et al. [32] considered these vulnerabilities and limitations when such unimodal systems are deployed in real-world applications involving a large number of users. Their considerations are listed as follows:

1- **Intra-class variation:** it can be caused by a user who is incorrectly interacting with the sensor or changes in the biometric characteristics of a user over a period of time.

2- **Noise in the inputs data** (e.g. dirt on a fingerprint sensor) noisy data may not be successfully matched with corresponding templates and therefore incorrectly reject a genuine user.

3- **Non-universality:** this is due to the inability of biometric system to acquire biometric trait or extract features from acquired data such as extract incorrect minutia features from poor quality of the ridges in fingerprint (e.g. HONG KONG (Reuters) –

"A Singapore cancer patient was held for four hours in the United States when they could not detect his fingerprints which had apparently disappeared because of a drug he was taking")

4- **Spoof attacks** caused by an impostor's attempt to spoof the biometric trait of a legally enrolled user in order to circumvent the system (especially when behavioral traits such as signature and voice are used).

5- **Inter-class similarities:** Overlap of feature spaces corresponding to multiple classes or individuals caused inter-class similarity. This can increase the false match rate of the system in unimodal identification systems comprising a large number of enrolled individuals and subsequently upper bound on the number of individuals that can be effectively discriminated by the biometric system.

6- **Interoperability issues:** This is another limitation in biometric systems caused by the theory of comparing biometric features from the same sensor. However, this theory is impractical due to difficulties in obtaining biometric data from different sensors and, hence, the ability of such systems are restricted when matching or comparing biometric data originating from different sensors. For instance, the challenge of comparing voiceprints originating from different handset or comparing fingerprints when the images are from different sensors. Ross and Jain [33] consider fingerprints obtained by using different multiple sensor technologies cannot be reliably compared due to variations in sensor technology, image resolution, sensing area, distortion effects, etc.

2.5 Proposed Biometric Traits for Wireless Applications

Since there is no set of criteria for all security system applications, there is no single best biometric trait for all applications. Figure 2.4 depicts the comparison of biometric technologies (in terms of ease-of-use, cost, accuracy, and distinctiveness perceived intrusiveness) and it shows that as one biometric, it may be possible to describe the most accurate, easiest to use, easiest to deploy, or cheapest biometric for that particular deployment, but no biometric technology is best for all situations [34]. Nevertheless, fingerprint has a high balance of the all-desirable properties in both type of biometrics and it is suitable for a large number of recognition applications. In addition, it is one of the most accepted and developed biometric techniques in wireless devices due to its small size, inexpensive price and good performance of sensors. There is also pragmatic evidence of fingerprints recognized in various wireless device and mobile handheld companies as an appropriate authentication method in their wireless devices.

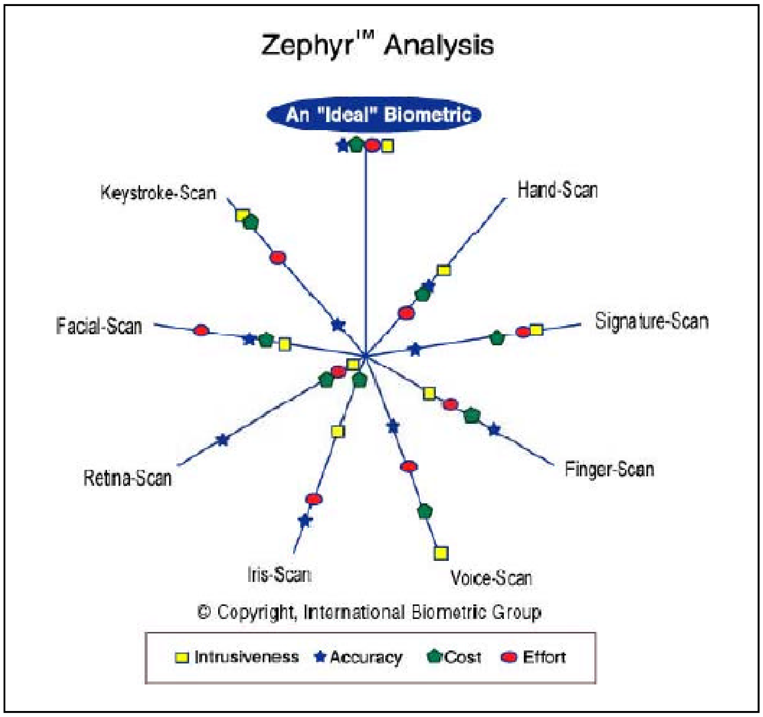


Figure 2.4: Biometric Market Report of International Biometric Group [34]

The main features of fingerprints to sum up briefly are:

1. Everyone has fingerprints even users with hand-related disabilities;

2. Fingerprints are very distinctive;

3. Fingerprint details are permanent even if there are temporary cuts or bruises on the skin;

4. Live-scan sensors can easily capture high-quality images without suffering from the problem of segmentation of the background like face recognition;

5. Currently, fingerprint sensors are becoming quite small and cheap with good performance;

6. Using Multibiometric systems with fingerprints recognition is quite difficult to circumvent;

7. It is suitable for a large number of recognition applications;

8. Fingerprint sensors are one of the most accepted and developed biometric technique in wireless device;

9. Fingerprinting technique is one of the mature technologies used in criminal investigations.

As it shown in table 2.1, fingerprinting has a high ranking in the majority of requirements and medium in some of them. Furthermore, using a person’s voice as a biometric is unobtrusive and it is an acceptable biometric in almost all societies. In addition, in wireless applications where identity authentication over the handheld device or telephone is desirable, sometimes voice is the only feasible biometric. The core weakness in voice recognition is affected by a person's condition (e.g., cold, stress, emotions, etc) and can be mimicked by others. However, there are a number of techniques to overcome impersonation such as prompting the subject to utter a different phrase each time (known as text dependent algorithms detailed in Chapter 3). However, in this thesis, such weaknesses are countered by the development and investigation of multibiometric based on combining the fingerprint authentication with that of voice recognition as an access control for secure wireless communication.

Biometric Identifier	**Universality**	**Uniqueness**	**Permanence**	**Collect ability**	**Performance**	**Acceptability**	**Mature**	**Size**	**Circumvention**
Face	High	Low	Medium	High	Low	High	High	Medium	Low
Fingerprint	Medium	High	High	Medium	High	Medium	High	High	High
Hand Geometry	Medium	Medium	Medium	High	Medium	Medium	Medium	Low	Medium
Iris	High	High	High	Medium	High	Low	Low	Medium	High
Retinal scan	High	High	Medium	Low	High	Low	Low	Medium	High
Signature	Low	Low	Low	High	Low	High	High	Low	Low
Voice	Medium	Low	Low	Medium	Low	High	High	High	Low
Facial thermo grams	High	High	Low	High	Medium	High	Low	Low	High

Table 2.1: Comparison of biometric technologies in wireless application **(**adapted from [26])

This section reviewed various kind of biometrics that are evaluated by several researchers to find an optimum solution for better throughput performance and accuracy as unimodal biometric security in wireless communication system. However, whilst unimodal biometric systems have advantages over traditional security system, such as the impossibility of being lost or stolen, they still have some considerable limitations. These limitations as detailed in section 2.4 and 2.5 can be addressed by using multimodal biometric technique. The next section considers implementing these multiple biometric system.

2.6 Multibiometric

In the previous section, an extensive literature review presented regarding unimodal biometrics in wireless communication system and its limitations. User verification system that is based on a single biometric in the context of security raises several design limitations such as interoperability issues, noise in input data, intra-class variation, non-universality, vulnerability against spoof attacks and inter-class similarities. Some of these restrictions can be alleviated through multimodal biometric approaches by providing multiple evidences of the same identity [35]. The integration of two or more types of biometric systems helps to improve the security and performance of unimodal system in different ways. Some of them are as follows:

1. Improving the accuracy of the overall system: The accuracy of the system can be improved by combining the information derived from multiple traits to reduce the FAR and FRR of the system;

2. Providing sufficient data if it is not successfully derived from a unimodal trait, for instance, this can cover cases where noisy data is an issue;

3. Furthermore, parallel to alleviate some of the drawbacks with individual matchers and increasing the performance which may not possible to obtain by a unimodal biometric system, multibiometric systems provide anti-spoofing measures by making it difficult for an impostor to spoof multiple biometric traits [35];

4. Multibiometric systems can address the issue of non-universality in a unimodal system if the user is not able to present a particular biometric trait by providing the additional biometric trait in order to enroll and authenticate (e.g. enrolling the user by his voice and fingerprint if the user’s face is not available).

This section starts with a review of the advantage of integration of two or more types of biometric verification systems, which is normally known as a “multibiometric” system, to improve the security performance requirements of unimodal biometrics and cover its limitations. However, designing an appropriate multibiometric system raises several issues such as cost/benefits, determining sources of biometric information, types of information and finally fusion methodology.

2.7 Fusion

Generally, information fusion is based on the combination of different sources of information either to produce one figurative format or to make a decision. This function can be executed in five categories including the information fusion acquired from multiple sensors, multimodal biometric, multiple units (multi-Instance), multi-sample and multiple algorithms for the same biometric [10, 32]. The main advantage of fusion is the increase in the reliability of biometric systems by either combining the information from separate biometric (e.g., fingerprints and voice or two fingers from the same person) or using a separate acquisition device (e.g. multiple cameras or microphone and camera). However, some researchers [32, 36] classify fusion levels into (i) fusion prior to matching and (ii) fusion after matching. Usually in literature, it is divided in to three possible fusion level based on the strategies of integration including, feature extraction level; the matching scores level; and the decision level [35]. In addition to these levels, there is another fusion level based on combining the digital output signal from more than one sensor at a sensor level. This level of fusion is very unusual in multimodal biometric systems due to the incompatibility of the obtained data from the various sensors [51]. In image processing literature, this sensor level fusion is referred to as image level or pixel level fusion [37]. However, fusion at a sensor level can be used over a unimodal system through the integration of obtained data from either using a single sensor or different compatible sensors to reduce the noise or cover the blind part of input data (e.g. mosaicing of multiple fingerprint impressions of a subject to make a more detailed fingerprint image) [32].

Although, integration of information, at the feature extraction level is more effective than the other two levels due to the availability of more information about the input data than in matching or decision levels. Appropriate care must be taken to check the relationship between the feature spaces that are combined to remove the highly correlated features [51]. Furthermore, developing efficient matching algorithms in many cases is the most challenging issue in the design of a biometric system and, therefore, fusion at the sensor or feature levels commences additional processing complexities. In addition, the majority of commercial biometric systems limit access to feature sets in their products. Therefore, the majority of researchers have focused on integration at match scores or decision levels [32]. Integration at the matching-score level is the most common level of fusion due to the ease in accessing and combining the scores generated by different matchers [190]. However, in the case of using the commercial off-the-shelf (COTS) matchers to build a multibiometric system, sometimes the only feasible level of fusion is decision level. This is due to restrict the access only to final recognition decision by many COTS biometric matchers [32].

Information fusion in biometrics can be accomplished at several levels and many fusion techniques documented in the literature regarding these levels. However, fusion is a compulsory phase of many multibiometric systems; the correlation between the sources has to be inspected before determining their suitability for fusion. In addition, correlation between sources is not the only driving factor behind fusion, the performance disparity between individual sources of information also impacts the matching accuracy of the fusion scheme. Hence, there is no clear criterion with regards to conditions, which depend on a great extent on correlation between sources and performance disparity between individual sources of information. “Defining a suitable diversity metric that would help predict the performance of a particular fusion scheme has been elusive thus far “[32].

2.8 Conclusion

This Chapter started with a review the advantages of the integration of two or more types of compatible biometric verification systems in wireless communication, which is normally known as a “multibiometric” system, to improve the security performance requirements of unimodal biometric and to cover its limitations. As indicated in this Chapter, finding the best fusion method, biometric trait, and transmission technique to fuse, and send secure data over the wireless channel is a challenging problem in multibiometric in term of types of information and fusion algorithms. This Chapter reviewed different biometric technologies in theory and experiments based on the evaluation of the output of several researchers to find the optimum type of biometric traits with better throughput performance and accuracy for multibiometric security in wireless communication systems. Finally, fingerprint and voice recognition were selected due to their feasibility, high balance of all the desirable properties, high performance, and accuracy. There are, many problems associated with fingerprint and voice technologies such as error rates, spoofing attacks, and interoperability. In the next Chapters (3 and 4) recent advances and limitations of these two biometric technologies are reviewed. In addition, this Chapter provided a literature review with the aim of giving a full account of the technique resulting in a desirable fusion technique and algorithms. Despite the fact that some of them proved efficient in improving the performance, it is not possible to predict the performance in every scenario. This is due to the using different environments and conditions, which depended on performance disparity between individual sources of information and correlation between the sources. For this reason, further investigation (in terms of performance and correlation imbalance) based on the suggested system in Chapter 5 and related expert of two selected biometric traits (voice and fingerprint) is essential. Nonetheless, accuracy of the whole system definitely can be improved using the appropriate fusion techniques to achieve results that are more reliable.

Chapter 3

Speaker Recognition in Wireless Application

Introduction

Wireless networks come with significant advantages over wired networks, including no cabling, freedom of mobility, scalability, and flexibility. Therefore, wireless networks are still gaining in popularity and are now becoming a viable alternative to traditional wired solutions. For instance, hospitals, universities, airports, hotels, and many retail shops are using wireless technologies to conduct their daily business operations [8]. Currently these networks are expanding much faster than ever with the introduction of 4G and WiMAX. The problem is however that wireless networks regardless of whether they are based on WiMAX or Wi-Fi LANs, as defined in the IEEE 802.11 standard, are inherently less secure than wired counterparts due to lack of physical infrastructure [9]. With the main concern being how to provide access only to authorized users, this Chapter is devoted to investigating the limitations and merits of voice recognition as a way of securing wireless applications.

3.1 Speaker Recognition in Wireless Technology and its Motivation

The use of speaker recognition technology as a biometric identification, as prevalent in commercial, civil, and forensic applications, is continually growing. These applications are access control to computer networks, transaction authentication (E and M-commerce), law enforcement (Home-parole and prison call monitoring), speech data management (Voice mail browsing and intelligent answering machines), and personalization (Voice-web or device customization) which are not an exhaustive list [62]. Despite, speaker recognition is an acceptable biometric in the majority of societies and of course over the phone, voice is not sufficiently distinctive as an identifier in large databases and the quality of the voice signal can be degraded by the communication channel [32]. In addition, a person's voice can be changed unintentionally because of emotional, health conditions, stress, or even on purpose as some people can imitate others. This technique has already been applied to wireless devices, particularly mobile phones and handheld devices. However, voice is not considered for all purposes, over the phone or wireless device sometimes it is the only possible biometric and secure enough as a verification method.

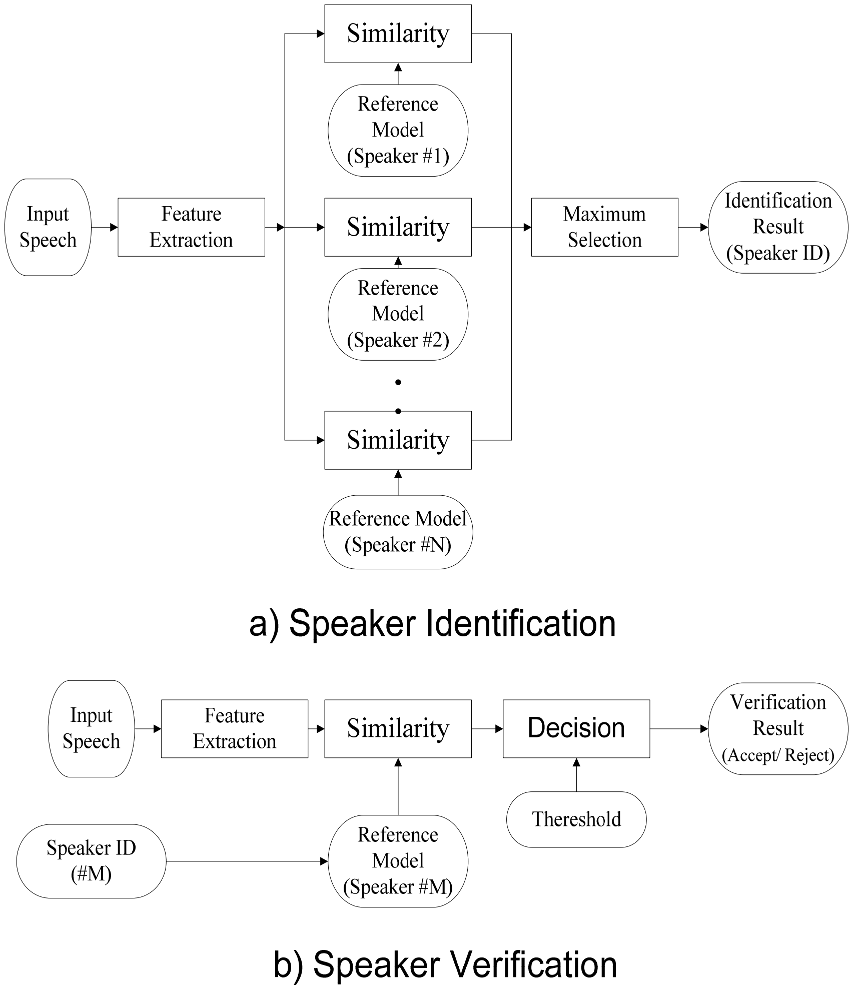
Speaker recognition over IP networks, wireless mobile devices, and through telephone channels has been widely studied in scientific literatures [66-73]. Problems arise in scenarios such as dependency of data on the quality of microphone and communication channel, transcoding, transmission errors (Lost data packets, delay and jitter), and possibility of hack by impostors [74]. There are many available publications in scientific domain, which address these limitations. For instance, Besacier et al. [66] and Mayorga et al. [67] cover the transcoding and transmission errors through reconstruction strategies. This is based on using the interleaving techniques to distribute the speech information among packets, and combined with interpolation methods, to estimate the lost acoustic features. Siau et al. [68] present investigations conducted into the transmission of data over network for the purpose of biometric-based recognitions. In spite of all, it is not still possible to transmit raw biometric data over Internet due to long delays. Based on experimental investigations, it is shown that the transmission of data models, or features, instead of raw material, will significantly reduce the transmission time. In addition, they have demonstrated that an increase in overall transmission time due to data encryption is relatively short. Evans et al. [69] have considered the adverse effects on speaker verification accuracy due to the two independent forms of signal degradation (packet loss in communications system and ambient noise at the wireless device). They have experimentally concluded that even without any form of recovery, packet loss is unlikely to be significant in speaker verification performance compared to the adverse effects of additive noise.

In addition, Reynolds [70] presents an empirical study of the effects of handset variability on text-independent speaker recognition performance. They have experimentally demonstrated that although many of the linear filter compensation techniques can improve performance under mismatched handset conditions, performance gap between matched and mismatched handset conditions persists to other uncompensated effects.

The main aim of this thesis is to provide a secure and robust authentication by implementing a multibiometric technique with high level of confidence. Furthermore, by using this technique, it might be possible to protect communication against denial of service, since the receiver has to establish the identification first before decrypting the message. The limitations of speaker recognition in wireless communication were identified and tackled in this section to make the system more effective. Some of the restrictions can be addressed through packet lost recovery (alternative is to send voice features rather than raw data). However, environmental noise and channel mismatch remain the main drawbacks for vocal biometric authentication. Therefore, in the following sections, the result of investigation that was called out to answer current possibility and limitation of voice recognition in wireless communication is presented. Finally, an overall evaluation of appropriate techniques to be applied to wireless devices is given.

3.2 Speaker Recognition Characteristics

Voice is a behavioral biometric and something that has been used since ages. The difference is that this technique is done nowadays automatically by machine. It is based on using the extracted features of voice to verify or identify the speaker. Therefore, it divides this into two main groups: Automatic Speaker Identification (ASI) and Automatic Speaker Verification (ASV) [23, 24, 75, 77]. In the former, the task is to validate a user's identity with no a-priori identity claim using feature extraction of the voice, while latter attempts to verify a claimed user identity (Figure 3.1). ASI determines the similarity between the two speakers, based on the calculation of similar features in known voice against the unknown in database. In the case of ASV, this is easier because one measures similarity by comparing the claimed with a known voice in the database. In addition, speaker recognition can be categorized in two different ways include text-dependent and text-independent methods. Text-dependent is based on restricting utterances to predetermined words or sentences that are same for both training and recognition while Text-independent is not based on a specific text being spoken [23]. Text-dependent is the commonly used method with lower error rates. It has short duration enabling system response, because user has to wait for authentication before system access [24].


Input Speech
Feature Extraction
Similarity
Reference Model (Speaker #1)
Similarity
Reference Model (Speaker #2)
Similarity
Reference Model (Speaker #N)
Maximum Selection
Identification Result (Speaker ID)
Input Speech
Feature Extraction
Similarity
Decision
Verification Result (Accept/ Reject)
Thereshold
Speaker ID (#M)
Reference Model (Speaker #M)

a) Speaker Identification

b) Speaker Verification

Figure 3.1: Speaker Verification and Identification Algorithms [80]

One should note that there is a difference between speaker recognition (subject who is speaking) and speech recognition (what is being said). Nevertheless, the bottom line is to note that the main aim is to identify who is speaking rather than recognizing precisely a random speech from a speaker. There are many factors and parameters, which can cause errors in speaker verification regardless of how good an algorithm is. Some of these factors are misreading (misspoken prompted phrases), extreme emotional states (stress or duress), time variation (intra or intersession), microphone placement, poor or inconsistent room acoustics (for instance multipath and noise), channel mismatch, sickness (example is flu that can alter the vocal tract), and aging (vocal tract drifts away from model with age) [81].

3.3 Feature Extraction Methods

The performance of a speaker recognition process is strongly dependent on appropriate set of feature extraction modules. Speaker pattern-recognition models are divided into three components: feature extraction and selection, pattern matching, and classification. The focus in speaker verification is to design a system that minimizes the probability of verification errors. It will therefore, discriminate between the given speaker and all the others [81]. In this section, some of the well-known and popular feature sets are reviewed briefly (for further information reader is referred to cited references). In addition, overview of the feature selection, extraction, and discriminate analysis can be obtained in [82, 83].

3.3.1 Mel Frequency Cepstral Coefficients (MFCC)

One of the popular speech based verification methods is to use the information from short-time Fourier spectrum represented by Mel Frequency Cepstral Coefficients (MFCC). Although MFCC features are quite effective for discriminating speakers, it can reduce the performance of a verification system due to mismatch between train and test conditions. This is because MFCC is affected by channel distortion and/or ambient noise. MFCC is based on frame-by-frame analysis of the speech signal, with 20ms as typical but also 10 ms as frame advance, (20 ms can represent stationary signal and allow for the computation of short-time Fourier spectrum) [88, 89]. The European Telecommunications Standards Institute defined a standard in order to employ MFCC algorithm in mobile phones [90]. MFCC can be obtained by initially performing a standard Fourier analysis, and consequently converting the power spectrum to a Mel frequency spectrum. Finally, obtained is MFCC by taking the logarithm of that spectrum and computing its inverse Fourier transform. In addition, just the first 8 to 16 coefficients are supplied to recognizer [73]. MFCC has generally obtained a better accuracy, and in terms of computational complexity, takes less processing resources as opposed to other feature extraction techniques [91]. It is for this reason that MFCC has taken the lead in speaker identification systems, speech recognition, and speaker recognition in general.

3.3.2 CMS and RASTA Filtering

There are two feature-based compensation techniques with the ability of providing robustness to channel effects: RASTA-PLP [92] and Cepstral Mean Subtraction

(CMS) [93]. Note though that the handset and channel mismatches can still be significant sources of error even after CMS or RASTA-PLP is applied [94]. CMS is the operation of subtracting the mean MFCC vector from each MFCC feature vector. CMS is often used in speaker verification systems for the removal of slowly varying convolutive noise due to the communication channel [95]. In this technique, it is assumed that the long-term average of the Cepstrum could be estimated from a few seconds of speech. This can remove the effects of the convolution distortion by subtracting this long-term average from the original Cepstral [73]. The main motivation for using CMS in reverberant environments lies in the modeling of room as a channel. However, CMS might not be as useful to reduce the effect of long-duration room impulse responses, which is often the case in room acoustics [94].

RASTA (Real Active SpecTrAl) is a generalization of CMS based on the fact that in many cases, rate of change of nonlinguistic components in speech lies outside the typical rate of change of the vocal tract shape. This suppresses the spectral components that change more slowly or quickly than the typical rate of change of speech. It is demonstrated by Hermansky et al. [96] that RASTA processing improves the performance of a recognizer in the presence of convolutional and additive noise. The main difference between the CMS and RASTA processing in the log spectral domain (Cepstral) is that CMS removes just the dc component of the short-term log spectrum, while RASTA makes the current output dependent on its past and enhances the spectral transitions. RASTA can be implemented in different filters and performed in various instances such as MFCC [73, 96].

3.4 Classification and Pattern Matching

Work on speaker recognition modeling has been going on for many years and varieties of techniques have been explored. Template matching is a popular method of pattern match in speaker verification. This approach is based on the comparison between the input utterance templates with the reference one by aligning the two at the same points in time. One of the widely used approaches in template matching is Dynamic Time Warping (DTW), which is based on dynamic programming that uses an optimum time expansion/compression function for nonlinear time alignment. This is due to the necessity of stretch/compress from invariable difference between the durations of reference and test templates. Another approach is based on probabilistic models of speech signal that describes its time-varying characteristics. This technique known as Hidden Markov Modeling (HMM) and can be employed in a number of speaker verification algorithms [97, 98]. Similar to the template matching, HMM-based speaker verification can utilize speaker models derived from a multiword sentence, a single word, or a phoneme [71, 100]. In addition, two popular methods in text independent speaker recognition described in this section include Vector Quantization (VQ) [101] and Gaussian Mixture Models (GMM) [102].

3.4.1 Template Matching

This method is based on using the reference templates as speaker models by composing a sequence of feature vectors derived from fixed sentences uttered by a registered user. Next step is to match scores that are obtained by measuring the similarity between the aligned utterance and templates. However using the fixed templates cannot model the wide variability present in the speech signals [103].

3.4.2 Dynamic Time Warping

DTW is the most popular method, which compensates for the speaking rate variability in template-based systems [104]. Doddigton [103] introduced DTW in 1971 and Booth [105] pointed out that the calculated warp path during the dynamic time warping process encodes time-independent information useful for speaker recognition. A text-dependent template model is a sequence of templates $\left(\overline{X}_1, \dots, \overline{X}_N\right)$ that must be matched to an input sequence, $(X_1, \dots, X_M)$ [105]. However, N is not equal to M due to the timing inconsistencies in human speech [82].

3.4.3 Vector Quantization

VQ source modeling is another form of template-based method that uses multiple templates to represent frames of speech [82]. Soong et al. [107] is first to introduce this but improvements in the standard VQ were made by Booth et al. [105]. VQ is a coding technique to transmit signals at low bit rates, and can be used in many applications such as image/voice compression. In speaker recognition, it is based on creating personalized codebook for each speaker, and unknown speaker will be identified by aligning the codebook that are closest to the input vectors usually based on reading a specific text. It is not essential to perform a time alignment in this scheme. Although lack of time warping greatly simplifies the system, it neglects speaker-dependent temporal information, which might be present in the prompted phrases [82]. In situations with large set of training data, VQ approach is more effective as it offers less computation, because it does not model classes separately and combine the separate models. In addition, it does not suffer from the problem of segmenting speech into phonetic units, and it is more computationally efficient than template matching. However, it is suffering from the complexity of codebook search during recognition [108].

3.4.4 Hidden Markov Models (HMM) and Gaussian Mixture Model (GMMs)

Hidden Markov Models (HMM) are possibly the most successful and established method of automatic speech recognition [97]. Although the basic theory of HMM was developed by Baum and Petrie [109], the first attempt to employ it in speech processing was made by Baker at CMU [110], and Jelinek et al. at IBM [111]. Over the course of time, several improvements have been reported by researchers such as mixture autoregressive HMM [112], subword HMM [86], and semi continuous HMM [114]. HMM is based on encoding both the temporal structure of feature sequences, and the statistical variation of the features. Therefore, it is an appropriate speaker model in text-dependent speaker recognition. HMM is a stochastic model that can be viewed as a finite state machine, with each state having an associated probability density function for feature vector. It is useful for modeling nonstationary signals whose time-varying characteristics may be described through a chain of statistical states. The main constituents of an HMM are the state observations and transition probabilities, which are defined by moving from one state to another. However, start states and last states have no income and output transitions respectively. These transition probabilities provide a mechanism for connection of the states and modeling variations, in speech duration and articulation rates. Finally, the observation densities model the statistical distribution of speech spectral features [115]. The HMM is called “hidden” since there is an invisible underlying stochastic process which affects the observed sequence of events [116]. HMM is suffering from the lack of an effective structure for modeling the correlation along the time axis of successive speech spectral (Or Cepstral) features. However Vaseghi et al. [115] have shown experimentally that the Cepstral-time features within an HMM result in an improved recognition (Hence HMM using Cepstral-time matrices are more robust to noise than HMM using Cepstral vectors).

The HMM technique is very similar to the VQ in action, and HMM states are found by a VQ-like procedures. However, in HMM probabilities of transition between states are encoded, and the order of presentation of speech data is important. It has to be noted though that HMM will cause problems in text-independent speaker recognition where no temporal correlation exists between the train and the test data. Therefore, single state HMMs known as Gaussian Mixture Models (GMM) can be used in text-independent speaker recognition [117, 102]. Although GMM provide a probabilistic model for each speaker, it is not similar to HMM, due to the fact that there is no Markov constraint among the sound classes, and hence order of presentation of speech data will not affect the recognition decisions. The secret of success with GMM is ability to deal with situations that there is no prior knowledge of what the speaker is going to say (In text-dependent applications, additional temporal knowledge can be incorporated by employing HMM as likelihood functions, because there is a strong prior knowledge of the spoken text) [95]. Applying GMM to speaker verification is based on firstly representing each registered speaker by a GMM, and secondly computing the ratio between the genuine likelihood and the imposter likelihood to enhance the discrimination between the two. The final matter is the issue of genuine GMM and background model [120]. Mostly background model is a GMM trained from the speech of a large number of speakers who should accurately represent the characteristics of all possible impostors. Alternatively, a set of background models is formed during verification by selecting the GMM of a small set of client speakers whose acoustic characteristics are close to those of the claimant [121].

3.5 Summary and Recommendation

This Chapter discovered a possible solution to address some of the limitations of speaker recognition in wireless communication system. Having reviewed different algorithms, the algorithm found most suitable and used in this thesis is that of Furui [93]. In addition, limitations of this technique in wireless communication are addressed by sending voice feature (cepstral coefficients) instead of raw sample. This scheme is to reap the advantages of reducing the transmission time and dependency of the data on communication channel, together with no loss of packet. Table 3.1 lists some of the works on speaker recognition and their error factors (results can loosely compare as they have not been applied under identical conditions for evaluation purposes, for instance different train and test paradigms, or dissimilar background speaker sets that were used). Obviously, finding the most reliable text-dependent speaker recognition technique depends on the specific scenario and the requirements of such scenario. Some of the general problems in wireless applications have been addressed earlier, and found that they can be resolved to a certain degree with packet lost recovery technique or sending encryption of voice features rather than the raw data. However, environmental noise and channel mismatch remain the main drawbacks for vocal biometric authentication. This is due to the acoustic mismatches or distortion of speech data gathered from different microphones, handsets, communication channels, and speech coder.

Source	Feature	Method	Text	Error
Atal 1974[122]	Cepstrum	Pattern Matching	Dependent	i:2%@0.5s v:2%@1s
Furui 1981 [93]	Normalized Cepstrum	Pattern Matching	Dependent	v:0.2%@3s
Li & Wrench 1983 [123]	LP,Cepstrum	Pattern Matching	Independent	i:21%@3s i:4%@10s
Higginsn & Wohlford 1986 [124]	Cepstrum	DTW Likelihood Scoring	Independent	i:10%@2.5s i:4.5%@10s
Higgins 1991 [120]	LAR, LP-Cepstrum	DTW Likelihood Scoring	Dependent	v:1.7@10s
Reynold 1995 [125]; Reynold et al. [102]	Mel- Cepstrum	HMM (GMM)	Dependent	i:0.8%@10s v:0.12%@10s
Che & Lin 1995 [126]	Cepstrum	HMM	Dependent	i:0.56%@2.5s i:0.14%@10s v:0.62%@2.5s
Reynold 1996 [127]	Mel- Cepstrum Mel-dCepstrum	HMM (GMM)	Independent	v:11%/16%@3s v: 6%/8%@10s v:3%/5%@30s Matched/Mis-Matched handset

Table 3.1: Selected Chronology of previous work include cestrum coefficients (i represents identification and v stands for verification) [81, 82**]**

3.6 Algorithm Description

Based on detailed requirements, normalized cepstral coefficients and dynamic time warping which is a text-dependent template model has been preferred as described by Furui [93] for automatic speaker verification using telephone speech. His results from experimental work indicate that the verification error rate of one percent or less can be obtained even if the reference and test utterances are subjected to different transmission conditions. Secondly, there is no significant increase in verification error with the increase of time interval (for further information reader is referred to cited reference). In addition, cepstrum coefficients have the other advantage that one can derive from them a set of parameters, which are invariant to any fixed frequency-response distortion introduced by the recording apparatus or the transmission system [93].

Chapter 4

Liveness and Spoofing in Fingerprint Identification: Issues and Challenges

Introduction

The fingerprint liveness detection refers to the inspection of the finger characteristics to ensure whether the input finger is live or artificial. A number of fingerprint identification systems are used widely and implemented at various important places such as border and immigration services. However, it is not declared by the manufacturers of these systems whether liveness detection is actually implemented. Possible measures to detect liveness are only proposed in patents and published literature. There are three major schemes, which are reported in fingerprint liveness literature. These are coupled with the additional hardware, software, or combination of fingerprint with other identifications is aimed to verify the liveness in submitted fingerprints. In this Chapter, various fingerprint liveness detection methods, which are categorized as voluntary and involuntary, are explored. The main objective of this Chapter is to critically review the voluntary and involuntary fingerprint liveness detection techniques proposed in the literature, and discuss their effectiveness and possible limitations.

4.1 Fingerprint Scanning Techniques

Fingerprint sensors come in various shapes and sizes however, they can be classified in two categories: area scan (or touch) sensor and swipe sensor. With a touch sensor, the user places and holds the finger on the sensor surface and impression transferred from the pad of the last joint of finger or thumb. Touch sensors are used mostly in fixed systems because of their size and shape [130]. On the other hand, in the swipe sensor (a narrow row of sensors), the users slides a finger vertically over the surface. These sensors are preferably used in portable consumer electronics because of their size and shape [130, 131]. However, user needs to be trained in order to work with these sensors and they are not always succeeding to capture fingerprint images. In addition, there are some common problems in both sensors, such as direct exposure to the environment, damage from mechanical effects, electrostatic discharge (ESD), thermal shock, and discrimination between liveness and spoofed finger.

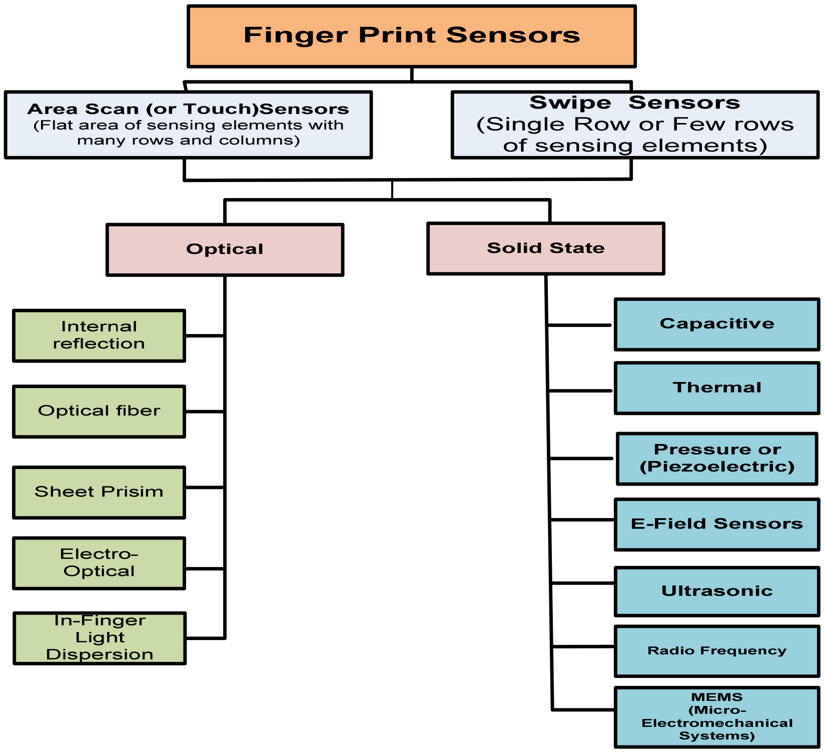

Finger Print Sensors
Area Scan (or Touch)Sensors
(Flat area of sensing elements with many rows and columns)
Swipe Sensors
(Single Row or Few rows of sensing elements)
Optical
Solid State
Internal reflection
Optical fiber
Sheet Prisim
Electro-Optical
In-Finger Light Dispersion
Capacitive
Thermal
Pressure or (Piezoelectric)
E-Field Sensors
Ultrasonic
Radio Frequency
MEMS (Micro-Electromechanical Systems)

Figure 4.1: Technologies of fingerprint Sensors

Fingerprint scanners using different technologies for capturing the image of a finger are divided into two categories optical and solid state. Figure 4.1 illustrates a general taxonomy of fingerprints sensors. In the following section, the different techniques used in optical fingerprint sensors are presented and critically reviewed.

4.1.1 Optical Sensors

The first generation of electronic fingerprint sensors was based on optical technology (Figure 4.2). A light source (usually LEDs) is pointed at one side of a prism and a finger is placed on one face of the prism. The ridges of the fingerprint absorb the light while the valleys of the fingerprint do not make contact with the prism, allowing the light to be reflected. A camera (CCD or CMOS) picks up the reflected light, which is the representation of the ridges and valleys. The optical path of light, S, is defined as the total optical length between the finger surface and sensor array.

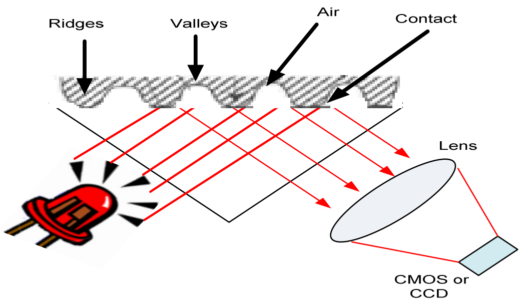


Figure 4.2: Optical Fingerprint sensor

Since the fingerprint size is fixed (a typical design has the finger 15 mm in width and 20 mm in height), S can be determined by the lens focus and camera array size. A smaller S means a more compact sensor [132].

$$S = U + V,$$

$$\frac{1}{u}+\frac{1}{v}=\frac{1}{f}\ \frac{u}{v}=\frac{d1}{d0} \tag{4.1}$$

Where u is the optical distance from the finger to the lens, v is the optical distance from the sensor array to the lens, f is the focal length of the lens, d1 is the finger width, and d0 is the camera array width. Initially, this technique was named as Frustrated Total Internal reflection (FTIR) [133]. The sensor based on FTIR have smaller size CMOS instead of CCD camera and it is difficult to fool them with a photograph or image of a fingerprint. Many of the proceeding technologies have replaced some mechanisms with smart components but still this has many drawbacks specially the size, focusing, and alignment components.

A. FTIR with a Sheet Prism

The sheet prism has a number of “prismlets” adjacent to each other [132]. Each prismlet has a light entrance surface and an exit surface, this sensor also operates on the principle as that of FTIR [134]. However, the prism size can be reduced; the optical path remains unchanged. On the other hand, this mechanism reduces the image quality than the traditional FTIR [18].

B. Optical Fiber Sensor

This technique employs a fiber-optic plate as a replacement for a prism and lens. The Fiber Optic Plate (FOP) consists of the array of optical fibers. A finger should be in contact with the upper side of FOP and illuminated from an angle by a light source by diffusing light on the top of the FOP. The ridges of the finger are in contact with the FOP, while the valleys are not .Therefore, only the ridges scatter light, and the scattered light does not reach the CCD/CMOS. Near the valleys, light is reflected totally at the FOP air boundaries and transmitted to the CCD/CMOS that is direct contact with the FOP [18]. This technique is better than prism sheet because it reduces the thickness of sensor and eliminates the additional mechanism required with sheet prism based fingerprint sensors. However, to build a high-resolution sensor using this technology increases the cost of the sensor because of the optical fibers.

C. Electro-optics Sensor

The top surface is a transparent layer upon which the finger is placed. On the inside there is a two-dimensional matrix of photoelectric elements (Imaging Layer) separated by strip-shaped gaps. The light emitting layer emits the light through the strip-shaped gaps, and this passes through the transparent layer to ridges or valleys of the fingerprint. Light is reflected back at the valleys to the imaging layer. Since the refractive index of a finger and the transparent layer are designed to be very close, the ridges will absorb light [33, 132]. The imaging layer is protected from light coming from the light emitting layer, hence it delivers an output signal only in response to light that has been reflected towards the imaging layer. As a result, the pattern of ridges and valleys will be generated to form a fingerprint image.

D. In-Finger Light Dispersion

In this relatively new sensing technique, a finger is placed directly on the sensor and is illuminated by ambient light (available or existing light), while the optical imager chip sense the strength of the dispersed light that reaches through the finger. The light eliminating form the valley part is dispersed in the air, and becomes weak leaving the corresponding pixels darker [136]. A proprietary, special surface glass over the imager chip ensures good imaging and protection. It is difficult to arrange the mechanism of theses sensors in compact form, since the focal length of small lenses can be very large and image distortion is possible when the reflected light is not focused properly. Because of their cost, size and sensing mechanism they are not suitable to become a part of many portable systems e.g. PDAs and Laptops.

4.1.2 Solid State Fingerprint sensors

Solid-state fingerprint sensors (aka silicon sensors) measure some physical properties of a finger and convert it to a digitized ridge valley pattern or image.

A. Capacitive

Although, solid-state sensors (also known as silicon or chip sensors) have been proposed in patent literature since the 1980s, it was not until the middle 1990s that these have been commercially available [137, 138]. Innovation in the field of integration and fabrication technologies makes possible to develop small and single chip solid-state sensors. These sensors designed to overcome the common problems related to optical sensors like image quality, calibration, size and cost [132].

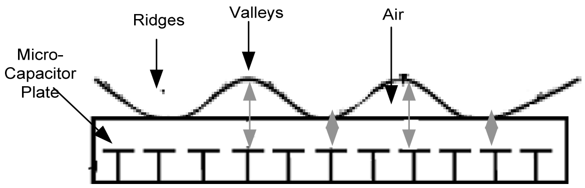


Figure 4.3: Capacitive Fingerprint Sensor [142]

Sensor is one chip includes two-dimensional array of micro-capacitor plate (Figure 4.3) and finger skin act as the other side of each micro-capacitor [139]. Small electrical charges are created between the surface of the finger and each of these plates when the finger is placed on the surface of the sensor [33]. These sensors have smaller imaging area, size, and resolution, however, because of cost of capacitive elements, such sensors are more expensive than same size, and quality images in optical sensors [141, 142]. The capacitance C is determined by [132]:

$$C = k\left(\frac{s}{d}\right) \tag{4.2}$$

Where C is the capacitance, k is the dielectric constant, s is the surface area of the capacitor, and d is the distance between the electrodes of capacitor.
In addition, it is known that:

$$\frac{dQ}{dt} = \mathbf{C}\,\frac{dV}{dt} \tag{4.3}$$

Where dQ / dt is the change of charge over time and dV/ dt is the voltage change over time. Since **k** and **s** are fixed, the capacitance **C** changes with **d**. In addition, **Q** can be set by charging the capacitor to a known value and therefore, the capacitor voltage V will change when **C** is changed due to the distance that each ridge (closer) or valley (further) is located from the capacitor plate. Thus, a fingerprint image can be determined by the measurement of the voltage output change over time at each capacitor of the sensor array [33, 143]. Many other issues are still with capacitive fingerprint sensors. These sensors corrode by frequent use and susceptible to electrostatic discharges (ESD) from the fingertip and can damage the device. These sensors just image the surface of the skin, which is susceptible to damage and contamination from daily activities. For the reason that the dielectric constant of the surface layer of finger skin is mainly due to moisture in the ridges and valleys, in dry fingers, the dielectric constants will be very close to air and this will result in faded images from the sensor. The performance of such sensors is nowadays being improved and most of the capacitive sensor makers are declaring that they have solved the ESD problem and show the corresponding value of ESD tolerance. However, the consistency has been questioned and the durability and mechanical strength are still an issue.

B. Thermal

Thermal technology based finger print sensors are made from the silicon die tiled by pixels of pyro-electric material that is sensitive to detect temperature differences. The transferred heat from sensor to the finger is measured by the sensor through scanning the surface of the finger [144]. The temperature difference between the ridge and valleys are translated to a fingerprint pattern. This is based on the fact that the heat is transferred from the sensor surface to the ridges of the fingerprint faster than valleys, which are insulated by an air-gap [145].

When the finger is placed over the sensor, there is a significant change of temperature, generating the corresponding t signal. However, after a short time, the image vanishes because the chip and finger have reached at thermal equilibrium, and as there is no change in temperature, there is no signal. This effect disappears when users sweep their finger over the sensor, due to the touch/no touch of ridge/valley. In order to obtain an acceptable data from the thermal sensor, the user must be sure to swipe the finger at a constant speed [18, 33]. These sensors tend to consume more power than competing technologies and can be less accurate in hot environments due to the low difference between the temperature of ridges and the valley. In addition, because of their high power consumption, they are inappropriate for portable systems.

C. Pressure

The principle of sensing is based on the piezoelectric effect. When a finger is placed over the surface (Non-Conducting dielectric material) of the sensor, only the ridges encounter the individual sensor cells and no other part of the finger. As a result, the pressure from finger generates a small amount of current [142]. The strength or weakness of the produced current depends on the pressure applied on the sensor surface. These sensors are almost same in size and resolution as capacitive sensors. They are less sensitive to condition (wet or dry), and other effects of the finger. However, the employed material in this technique is not sufficient sensitive to detect the differences between ridges and valleys [33]. Protective coating of non-conducting dielectric material over sensor cells blurs the resulting image.

D. Electric Field (E-Field)

The fingerprint sensor based on E-Field acquires the image by measuring the variations in conductive layer under the skins surface, due to the difference in thickness between the ridges and the valleys [18, 132]. The main advantage of this sensor is that it does not sufferer from dry skin conditions, calluses, or cuts as it creates a fingerprint image from the layer under the skin.

E. Radio Frequency (RF)

Radio frequency (RF) based finger print sensors uses RF electromagnetic field to create an image of a fingerprint. RF sensors are built on the principles of the capacitive sensor by using the finger itself as both the charge plate and the dielectric [142]. A signal can be produced by the finger ring around the periphery of the sensor area, travels through the finger. In addition, reduction level of the signal depends on the ridges and valleys and this attenuation is calculated by the sensor array to produce the fingerprint structure. The main approach of this technology is that it reads below the surface of finger, and cannot be affected by dirt, oil, scars, cuts, or other impurities.

Acoustic (Ultrasound)

The fact that there is noticeable difference between acoustic impedance of the skin (the ridges) and air (in the valleys) resulted in invention of an ultrasonic-based fingerprint sensor [132,149]. The ultrasonic sensors have two main elements comprising the sender and the receiver. The sender generates a short acoustic pulse, which can be detected by the receiver as the result of pulse-bounce-back from the surface of the finger [33].

Although, this is one of the most accurate fingerprint scanning techniques, it is not widely used due to the large size, high cost, and longer time requirement to acquire an image compared to other fingerprint sensors.

Technology	Outer Physic	Flexible Physical	Liveness Detection	resolution (R)	limitations
Optical	Solid	No	No	R ≤ 600dpi & 1000 dpi possible [136]	Optical Focusing and Alignment mechanism, Size
Capacitive	Solid	No	No	R < 600 dpi	ESD Protection, Poor performance for damaged and dry skin
Thermal	Solid	No	No	R < 600 dpi	Environment dependant, User need training , More power consumption, Not suitable for Mobile user
Pressure (Piezoelectric)	Solid	No	No	R < 600 dpi	Less sensitive, Protective layer reduces the quality of images
Radio Frequency	Solid	No	Possible	R < 600 dpi	Low accuracy with dry fingers
Ultrasonic	Solid	No	Possible	R < 600 dpi	large size, cost, more time to acquire image
Micro electro-mechanical (MEMS)	Solid	Possible	No	R < 600 dpi	Not particularly for Fingerprint Sensing

Table 4.1 Comparison of current fingerprint sensors with their physical state, liveness detection, and resolution

4.1.3 Limitations in Existing Fingerprint Sensors

In this section, a critical review of the technologies available in fingerprint sensors is presented. Although various improvements to the existing technologies are still taking place, still many problems exist. Apart from their size, cost, their physical state, and resolution, differentiation between real and gummy fingers is still a problem. Table 4.1, depicts and summarizes the comparison of existing fingerprint sensor technologies with their drawbacks. In future, it is essential to develop more sensitive and high-resolution fingerprint sensors that can acquire additional information from fingers with ridges and valleys including liveness detection. The physical state is also necessary to modify because the future electronics applications require the flexible, strong, and less environmentally sensitive fingerprint sensors.

In spite of the advantages of current fingerprint-sensing technologies, detecting liveness of a presented fingerprint sample has become a challenging research issue [149, 150], due to the possibility of defeating the fingerprint authentication. Although some biometric technologies such as facial thermogram and vein pattern may be considered stronger and more difficult to simulate artificially, these technologies are not widely implemented and will need to be validated as reliable biometric identifiers [151]. Next sections consider well-known attack and countermeasures to address the liveness limitations on the fingerprint sensor.

4.2 Sensor Attacks and Protection Schemes:

Liveness detection (vitality detection) in a biometric system means the capability of the system to detect if a presented biometric sample is alive or not. In addition, to checking that the sample belongs to the live enrolled and not just any live human beings, it is necessary to guard against artificial fingerprints [152]. Liveness detection can be executed either at the acquisition or at processing stage in two approaches, liveness detection, and non-liveness one (e.g. detecting bubbles in gelatin artificial fingerprints) [153]. The main concern in fingerprint techniques is at what level of security one can rely on fingerprint readers (e.g. travel authentication like passports or access to nuclear facilities). A fingerprint reader is the front end of a fingerprint authentication system. This unit captures the fingerprint image by a sensor, which is usually one of the optical or solid-state types. There are many techniques to recognize the liveness of presented data at sensor level.

In this section, various countermeasures to avoid spoof attacks at fingerprint sensor level are explored in voluntary and involuntary forms. These techniques are based on determining the presence of a user by different responses. This can be from either voluntary source such as passwords, smart cards, and multiple biometrics (which makes spoofing more difficult), or involuntary liveness detection such as pulse oximetry, blood pressure, and heartbeat. In the voluntary case, the required response is based on the reaction of the user to hearing, seeing or feeling something. Involuntary on the other hand is about the user automatically responding to a stimulus, such as muscles responding to electrical stimulation, or skin changing color when pressure is applied.

Although many fingerprint liveness countermeasures to avoid spoof attacks are presented in the literature, the majority lack proven results and additional hardware requirements, and do not operate efficiently in different environments (such as indoors, outdoors, summer and winter). For instance, 3M Blackstone liveness testing project (measured electrocardiograph signals (ECG), blood oxygen levels and pulse rate) was discontinued because of the disrupting effects caused by user movements during the ECG synchronizing stage. It was also quite difficult for the users to remain motionless and hold their fingerprints in the required position for six to eight seconds [151].

In addition, there are a number of other limitations with the required hardware such as price, size, and inconvenience for the user and in some cases, the possibility to fool the system by presenting an artificial fingerprint. The list of possible attacks is continuously growing and not all the extra hardware systems, which are needed to test and analyze the data, are available as COTS (Commercial, Off-The-Shelf) items.

In this section, first some of the well-known eminent threats and attacks on the fingerprint algorithms are explored. Secondly, some countermeasures and techniques to overcome such problems are discussed. Amongst the recommended solutions, an attempt is made to select the most effective one.

4.2.1 Sensor Attacks and Possible Tenability:

Parallel to improving the fingerprint based system technologies, the various types of attack and forging are improving. Due to the new software and hardware technologies for editing (e.g. Adobe Photoshop), making an artificial fingerprint has become easier than ever. For instance, by using high-resolution camera, one can get better photographs of the fingerprints; or by adding, a preservative to increase the usability of gelatin employed for storing fingerprints can last even longer than a week. The possibility of defeating a fingerprint biometric system due to its inability to ensure liveness through fake biometric samples, make fingerprint authentication systems vulnerable against various possible attacks. In this section, these possible attacks [150] are explored in different schemes as follows:

4.2.1.1 The Registered Finger:

- Stealing fingerprint of a user by casting it into a mould, or causing user to press against sensor either directly or indirectly by way of drugs;
- Separating finger from legitimate user's body ;

In this case, combining the fingerprint scanner with another authentication method such as password or ID card can be used as a countermeasure. Alternatively, a control measure to alarm when under duress, or have supervision in place as one control the other (two-person implementation where system requires fingerprint from two different people) are possible solutions. Obviously, this is not always feasible.

4.2.1.2 The Unregistered (illegitimate) Finger:

In this kind of attack, attackers try their own fingers to log in as another user. The probability of a successful attack is based either on the high FAR of the system, or in the case of categorized system as "loops", "whorls", or "arches", by presenting the similar unregistered pattern as registered finger. In this kind of attack, the countermeasures can be a) to reduce the FAR of the system; b) in the case of categorized systems, to evaluate both the categories of fingerprints and the fingers within each category [150].

4.2.1.3 A Genetic Clone of the Registered Finger:

Another type of the attack on the not robust system is genetic clone or using the similarity of identical twins fingerprints. Therefore, it raises the demand of carefully designed systems with capability to detect even slightly different fingerprints, since twin fingerprints are not identical. In the case of genetic cloned, this attack cannot be successful by employing a liveness detection mechanism in the system. Although, protection against the identical twin is not as easy as protection against a genetic clone, the combination with another authentication method can be a helpful countermeasure [150].

4.2.1.4 Artificial Fingerprint:

This attack is made by duplicating a real fingerprint with gelatin, silicone, copier, clay, or other materials. In this method, attacker should have the original fingerprint either by directly making a mould of user's finger, or by using a residual fingerprint to make an artificial one. The useful countermeasures are liveness detection or combination with other authentication methods [150].

4.2.1.5 The Others:

In addition to identified types of attack in fingerprint sensor level, there are various types of attacks such as flashing a light against scanner, heating up, cooling down, humidifying, impacting on, and vibrating the scanner outside its environmental tolerances. Moreover, using the residual fingerprint on the sensor surface by dusting graphite powder, pressing adhesive film on surface, and many other possible attacks in specific sensor type exist [150].

In addition to above identified attacks, Jain et al. [154] list a number of other types of attacks as follows:

1. **Denial of Service (DoS):** Damages the system by attacker while a legitimate user has no longer access to system;

2. **Circumvention:** Allows access to system and data by unauthorized user to get either access he may not be authorized to (privacy attack) or manipulate the system to be used for illegal activities (subversive attack);

3. **Repudiation:** Denies having accesses to system by authorized user to obtain double personal benefit;

4. **Contamination or Covert Acquisition:** Provides access to system by unauthorized user with compromised knowledge of a legitimate user (e.g. lifting the latent fingerprint of a user and making an artificial fingerprint by attacker, or recording the voice sample of legitimate user and playing it back);

5. **Collusion:** Access to the system by way of collusion between administrator (super user) and other users to overrule the decision made by system;

6. **Coercion:** Access to the system as genuine users by forcing the user to identify themselves to system.

Scenarios 2 and 4 can be classified as unregistered fingerprint, while 3 and 6 can be labeled as registered fingerprint attack as detailed above. In the case of denial of service (scenario 1), since every fingerprint sensor has individual acquisition technologies and related durability (e.g. surface of optical sensors can be easily broken), any offered solutions must depend on the especial investigation of each sensor. Furthermore, in scenario 5, the offer of any solution raises the demand of implementation details based on application requirements. Next subsection reviews various general protection schemes to find optimum solution to improve the security and accuracy of fingerprint systems at the sensor level.

4.2.2 Protection & Countermeasures

In the case of non-liveness detection fingerprint, the verification system is very vulnerable against artificial fingerprint attacks from user leaving behind fingerprints every day everywhere without noticing. As a result, with possible attacks either identified above or any other method, employment of such systems is inappropriate for any application unless a preliminary investigation is carried out in order to assess the capacity of the system to ensure liveness. Since every type of fingerprint sensor has individual acquisition and related tenability, the protection solutions must take into account the special characteristics of these sensors. Liveness detection in a fingerprint system ensures that only "genuine" fingerprints are capable of generating templates for enrollment, verification, and identification. In addition, in a live biometric system, it is difficult for an individual to repudiate the executed transaction or access a secure facility or data. However, design decisions are based on the specific needs of a biometric application. There are many techniques pointed out in literature to recognize the liveness of the presented data and hence, reduce vulnerability to spoof attacks at sensor level [149, 152, 153, 19, 156-167]. In this thesis, these techniques are explored in two different approaches as voluntary (acquisition of life signs by measuring the voluntary properties of users' body or users' response) and involuntary (acquisition of life signs by measuring the involuntary properties of users' body or users' response). Furthermore, some of the well-known techniques in both will be dealt with briefly.

4.2.3 Involuntary Captured Information by Biometric Reader

The main problem with fingerprint scanner is distinguishing between real fingerprints (i.e. silicone rubber) and, other not alive fake fingerprints, such as epidermis of a finger [149]. This subsection reviews the published literature on involuntary techniques based on automatic (without intention) acquisition of data from the user's body. Generally, the involuntary techniques can be divided into the acquisition of data with additional hardware, and use of existing information in fingerprint without any hardware requirements. The main concern with using additional hardware is adjusting the scanners to operate efficiently in different environments (such as indoors, outdoors, summer and winter), leading to problems with using a wafer-thin artificial fingerprint glued onto a live finger [149]. In addition, there are a number of other limitations with this scheme such as price, size, inconvenience for the user, and possibility to fool the system by using an artificial fingerprint [153]. Although not all of the extra hardware systems available at COTS (Commercial, off-the-shelf) have disclosed characteristics, some well-known methods in both categories evaluated by other researchers are described in this subsection.

1. Temperature:

This technique is based on extracting the temperature difference between the epidermis (about 26-30° C) and silicone artificial fingerprint (max 2°C). Lack of ability to detect the wafer-thin silicone rubbers is the main weakness of this technique [149].

2. Blood Pressure:

This method is not susceptible to a wafer-thin silicone rubber glued to a finger. Excluding single point sensors that must be entered directly into the vein, other available sensors at COTS require measurements at two different places on the body (e.g. both hands). In addition, it can be bypassed by using underlying finger's blood pressure [149].

3. Heartbeat:

This method is accomplished by sensing the finger pulse as liveness detection method. This technique has practical problems with diversity in the heart rhythm of a user, which makes it virtually impossible to use in order to consider a person's heart rhythm when scanning the fingerprint (e.g. different rhythms for same user). In addition, user's emotional condition and level of activity will affect the heartbeat [149].

4. Odor:

In this scheme, detecting the liveness of fingerprint is based on the acquisition of the odor by means of an electronic nose, and discriminating between humans skin with other material. In spite of the fact that this method is able to discriminate real fingerprints from artificial reproductions, creation of a single model of human skin, rather than a template, for each user is necessary [167].

5. Conductivity:

In this technique, liveness detection is made by checking the conductivity of the finger skin, which is from 200 KΩ (dependent on the type of sensor) to several MΩ respectively, depending on whether we are during dry freezing winter weather or summer. The simple attack in this system can fool the sensor by some saliva on the silicone artificial fingerprint to be accepted as live finger [149].

6. Detection under Epidermis:

This is based on detecting fingerprint patterns in the epidermis and between epidermis and dermis as a sign of liveness. There are two types of sensors: ultrasonic sensor and electric field one. Ultrasonic sensors focus on the fact that the underlying layer is softer and more flexible than the epidermis. While electric field alternative are focusing attention on the higher electric conductivity of the layer underneath the epidermis as compared to the epidermis itself. Two different layers of artificial fingerprints with the appropriate characteristics could fool the scanner when the characteristics of sensor are known. For instance, in the case of using ultrasonic sensors made of flexible and soft print, a second regular artificial print can be attached to the first while making sure that the two line patterns are in exact matching positions. This can be achieved very easily by a dental technician [149].

7. Relative Dielectric Constant:

The dielectric constant of a specific material reflects the extent to which it concentrates the electrostatic lines of flux [168]. Measuring the distinct values of relative dielectric constant (RDC) between a live and an artificial fingerprint is the foundation for this method. However, RDC is influenced by the humidity of finger in different conditions, and fooling such sensor is possible by wetting the silicone rubber using alcohol/water mixture before it is pressed on the fingerprint scanner. Since the RDCs of alcohol and water are 24 and 80 respectively, and the RDC of a normal finger is somewhere between the two [149], it is easy to fool the sensor.

8. Optical Properties:

These techniques are based on the different absorption, reflection or scattering between the human skins versus other materials under different lighting conditions. However, gelatin artificial fingerprint has optical properties very similar to human skin [152]. For instance, in color change approach, fake fingerprint can be detected by the property of color change exhibited by a real live finger when it touches a hard surface. This is due to interaction among the fingernail, bone, and tissue of the fingertip caused by applied force of real live finger when it is pressed on the hard surface of the scanner. This can modify the hemodynamic state of the finger, resulting in various patterns of blood volume or perfusion that is recognizable at the fingernail bed and at the surrounding skin region in contact with the scanner. A method to detect and quantify such color change is proposed in [169] and used to differentiate a real finger from the fakes. Although, this approach is privacy friendly and fast without any requirement or training from the user, it is not applicable with all available sensors but optical scanners [169].

9. Pulse Oximetry:

This technique is based on measuring the arterial oxygen saturation of hemoglobin in a pulse [19, 156]. It can be deterred by using translucent artificial fingerprint (e.g. gelatin) [156].

10. Fine Movements of the Fingertip Surface:

This method is based on the analysis of fine movements of fingertip surface, which is induced by volume changes due to the blood flow. Two optical solutions are proposed for measuring characteristic periodic changes of the fingertip volume. The first is based on a system composed of a CCD camera and a macro objective to acquire images and analyze that with respect to fine movements of the papillary lines to draw on the volume changes. The second is based on a triangulation of a distance laser sensor and variation of the distance to fingertip maps, to variation in fingertip volume with blood flow. In spite of the advantages, more investigation needs to be done to evaluate the effectiveness and feasibility of such methodology. In addition, matching techniques needs to be improved (for instance in the case of presenting similar patterns to real heart activity curve, measuring curves of camera and the laser is solution) [159].

11. Involuntary Challenge-Response:

This technique is based on determining the presence of a user by automatically (without intention) responding to the requested challenge. For instance, user's response to a stimulus such as muscles’ to electrical stimulation or change in the color of skin when pressure is applied [153]. An implemented instance of an involuntary challenge-response is found in the US patent detector, based on the finger's electrical reaction to the small impulse, which outranges response of predefined acceptable values assumed as fake [158].

Another approach has been proposed by [170] to detect fake finger using an Electro tactile display system. There are two kinds of limitations with this technique: first lack of acceptability because of using the uncomfortable stimulus such as shocking; second is the difficulty with distinguishing between the challenged person and the true owner of the fingerprint presented to sensor [153].

12. Surface Coarseness:

This new liveness detection approach is based on analyzing an intrinsic property of fingertips: surface coarseness (Figure 4.4). Firstly, a fingertip image is denoised using wavelet-based approach. In second step, noise residue (original image minus denoised image) is calculated and coarser surface texture tends to result in a stronger pixel value fluctuation in noise residue. Finally, standard deviation of the noise residue can be used as an indicator to the texture coarseness [160]. However, experimental results demonstrate the effectiveness of this technique on high-resolution fingertip images (~1000 dpi) [160]. Feasibility of such method is dependent on high-resolution fingerprint, which is not compatible with all current sensors.

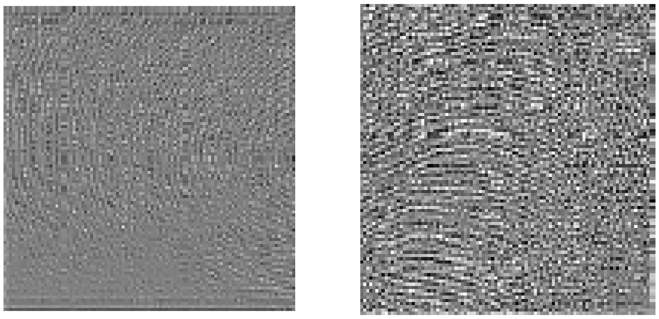


Figure 4.4: Using wavelet based denoising. For left image noise residue Standard Deviation = 11.5 while right image has noise residue Standard Deviation = 36.5 [160].

13. Underlying Texture and Density of the Fingerprint Images:

In this approach, detecting "liveness" associated with fingerprint scanners is based on the underlying texture and density of the fingerprint images (Figure 4.5). As first step, multiresolution texture analysis techniques are used to minimize the energy associated with phase and orientation maps. Subsequently, cross ridge frequency analysis of fingerprint images is performed by means of statistical measures and weighted mean phase is calculated. As a final point, these different features along with ridge reliability or ridge center frequency are given as inputs to a fuzzy c-means classifier. Although, the algorithm has 95.36% classification for the limited data, more investigation with multiple scanners and different underlying technologies are required to validate the ability of such a scheme [161].

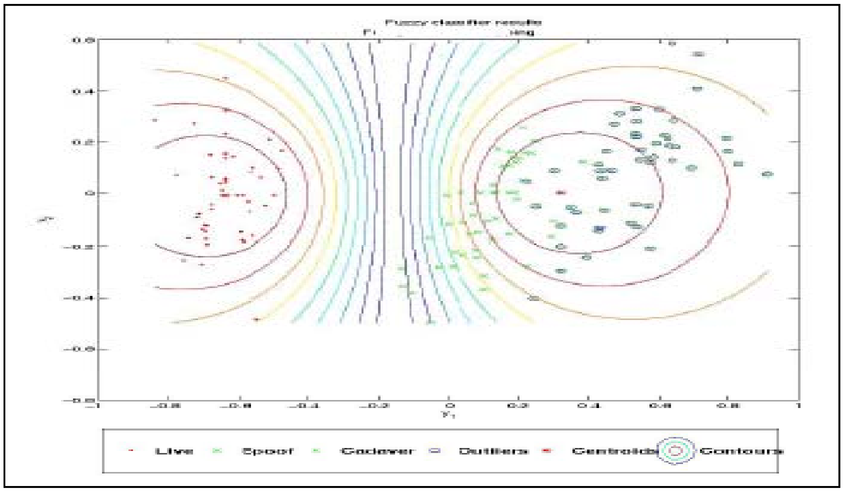


Figure 4.5: Result of the FCM classifier. The left centroid is for live fingerprints and right for not live [161].

14. Perspiration:

This is based on detecting the perspiration phenomenon between the human skin and other material under different conditions. In spite of the advantages, it is usually possible to deceive fingerprint systems by presenting a well-duplicated synthetic or dismembered finger. However, Derakhshani et al. [157] introduced one method to provide fingerprint vitality authentication in order to solve this problem. In their approach, vitality through fingerprint examination in conjunction with capacitive scanners (based on detection of the sweating pattern from two consecutive fingerprints), is captured during 5 seconds and a final decision about vitality is made by a trained neural network [158]. In addition, there are some other methods such as enhanced perspiration detection algorithm, which improves Derakhshani's work by including other fingerprint scanner technologies and use of larger, more diverse data sets along with shorter time windows [162]. Another technique is based on the statistics of wavelet signal processing to detect the perspiration phenomenon [163]. However, this technique has less ability for users with low moisture and highly perspiration-saturated fingers, and may not exhibit liveness due to the necessity of specific changes in moisture. Therefore, more investigations in terms of accuracy and environmental conditions are required to prove efficiency of such system [153].

15. Valley Noise Analysis:

This software-based method distinguishes between the live and artificial finger, using noise analysis along the valleys in the ridge-valley structure of the fingerprint images. The features are extracted in multiresolution scales using the wavelet decomposition technique, and liveness detection separation is performed using classification trees and neural networks. Dissimilar to live fingers, which have clear ridge-valley structures, artificial fingers, have a distinct noise distribution due to the material's properties when placed on a fingerprint scanner [164]. However, results show that this technique is very efficient (90.9–100%) for the capacitive, optical, and electro-optical scanners [164]. Efficiency of such method for all sensors though, needs especial investigation of each sensor specification.

16. Spectrographic Properties:

This technique is based on the analysis of the spectrographic properties of living human tissue (Figure 4.6 Left) for fingerprinting. In this method, multispectral imaging technology (MSI) uses multiple illumination wavelengths rather than the monochromatic illumination used in total internal reflectance (TIR) imaging.

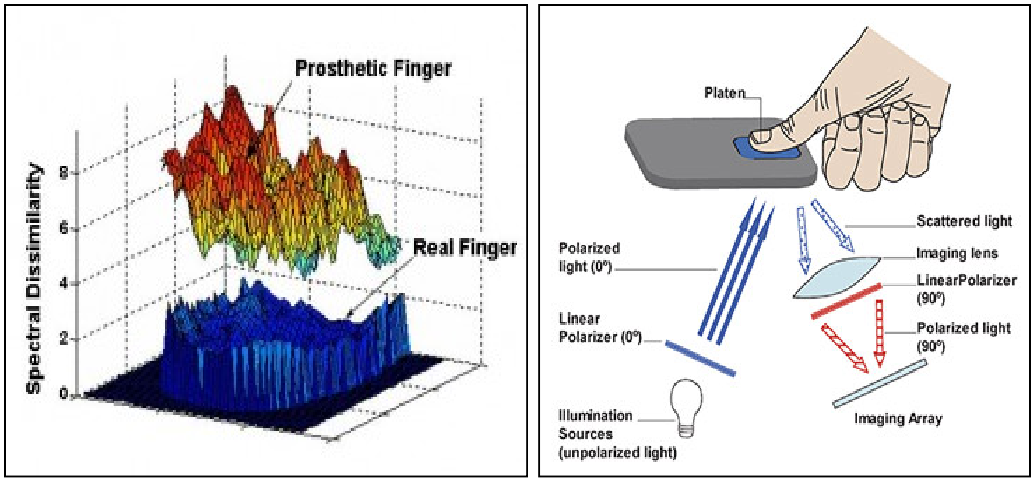


Figure 4.6: Left: Spectral-characteristics-of-spoofs and real fingerprint [165] and **Right**: Schematic of multispectral imaging elements [166]

In addition, polarizers can be utilized for the purpose of light penetrating surface that scatters several times by the time it leaves skin towards imaging array (Figure 4.6 Right). Inexpensive films and materials are proved inefficient against this method [165]. Although, TIR image quality is poor for people with dry skin, it has little or no effect on an MSI sensor. This ability to detect subsurface features of the fingerprint, based on the difference optical properties of human skin and synthetic material observed with the MSI sensor, enables this technology to detect spoof material [165, 166]. Therefore, more investigations need to be carried out in order to enhance usability and security for a fingerprint system that incorporates an MSI-based sensor [166].

17. Skin Deformation:

This technique is based on the information about how the fingertip's skin deforms when pressed against a surface. For instance, there are non-linear distortions between fingerprint impressions of the users, who are required to touch the sensor twice or move it once it has been in contact with the sensor surface. However, artificial fingerprint with the same type of requirements will only give a rigid transformation between the two fingerprint impressions and produce quite similar non-linear deformations as a live fingerprint [18].

18. Spatial Frequencies of Ridgelines:

In this scheme, band-selective Fourier spectrum has been proposed by [171] as fingerprint liveness detection. This is based on reflects the distribution and strength in spatial frequencies of ridgelines by 2D spectrum of a fingerprint image. In addition, the ridge-valley texture of the fingerprint produces a ring pattern around the center in the Fourier spectral image and a harmonic ring pattern in the subsequent ring. On the other hand, these rings can be produced by both live and fake fingerprints, with different amplitudes in different spatial frequency bands and stronger Fourier spectrum in the ring by live fingerprints. As an alternative approach, Lee et al. in [172] introduced a new method by using the fractional Fourier transform (FrFT). They have found out that the energy of live fingerprints is larger than the energy of fake fingerprints when it is transformed into the spectral domain. Firstly, fingerprint image has been transformed into the spatial frequency domain using 2D Fast Fourier transform and detected a specific line in the spectrum image. Secondly, this line has been transformed into the fractional Fourier domain using the fractional Fourier transform together with its standard deviation to discriminate between fake and live fingerprints. However, their experimental results demonstrate the possibility of their proposed method to detect fake fingers, further investigation in term of analysis of fingerprint image texture and studies on more data and sensors is necessary.

19. Pores:

This is based on using a very high-resolution sensor to acquire a fingerprint image, and therefore, fingerprint details (e.g. sweat pores) can be used for liveness detection since they are more difficult to copy in artificial fingerprints [18]. However, it is possible to coarse reproduction of intra-ridge pores with gelatin artificial fingerprints [150].

20. Other Claims:

In addition to aforementioned liveness detection methods, there are several other claimed methods and techniques, which are neither well known due to commercial confidentiality or not properly validated yet (e.g. electrocardiography) [149]. The possible classification of involuntary liveness detection methods is shown in Table 4.2.

Methods	Liveness Detection Technique	Limitations
Involuntary Measurements	Epidermis Temperature	Lack of ability to detect the Wafer-thin silicone rubbers
	Blood Pressure	Can be fooled by using underlying finger's blood pressure
	Electrocardiogram (EKG)	Disrupting the system by user movement during the EKG synchronizing
	Pulse Oximetry	Can be deterred by using translucent artificial fingerprint
	Odor	Creation of a single model of human skin, instead of a template for each user is necessary
	Heartbeat	Practical problems with diversity in heart rhythm of a user
	Detection under Epidermis	Can be fooled by two different layers of artificial fingerprints with the appropriate characteristics
	Relative Dielectric Constant	Influenced by the humidity of the finger in different conditions and can be fooled by wetting the silicone rubber
	Optical Properties	Gelatin artificial fingerprint has optical properties very similar to human skin
	Skin Conductivity	Can be fooled by some saliva on the silicone artificial fingerprint
	Skin Deformation	Can be fooled by artificial fingerprint with the same type of requirements for original fingerprint
	Pores	Possibility to produce coarse reproduction of intra-ridge pores with gelatin artificial finger
	Perspiration	Users with low moisture may not be able to use a fingerprint scanner, and highly perspiration-saturated fingers may not exhibit liveness
	Involuntary Challenge-response	Lack of acceptability and difficulty when distinguishing between challenged person and true owner of the fingerprint
	Underlying Texture and Density	Lack of relevant independent studies based on a very large number of users and effects of long-term experience on FRRs and FARs
	Surface coarseness	
	Fine Movements of the fingertip surface	
	Valley noise analysis	
	Spectrographic Properties	
	Spatial frequencies of ridgelines	

Table 4.2 Reported fingerprint involuntary liveness detection methods and limitations

4.2.4 Measuring the Voluntary Properties of User's Body or User's Response

As discussed above, involuntary liveness detections are suffering from a number of limitations such as low acceptability, lack of proven established results and additional hardware requirements, and cannot operate efficiently in different environments. Therefore, in this subsection voluntary techniques will be investigated in order to address some of these limitations of involuntary approach. However, it is clear that voluntary techniques have higher acceptability rate due to the detection of life signs from user (with intention) manually at the requested challenge. A possible classification of voluntary liveness detection methods, available in the literature, is presented in the following:

1. Using Multimodal Biometrics:

As discussed in Chapter 2, vulnerability against spoof attacks and liveness problems in unimodal biometrics can be addressed through multimodal biometric technique. Despite, some of these restrictions can be alleviated through multimodal biometric approaches by providing multiple evidences of the same identity. Implementing such system is currently much more difficult than it seems due to environmental, cost, or equipment limitations. Multimodal biometric systems can be designed to operate in five different scenarios [10, 32]:

a. Multi -Sensors:

In these systems, the information derived from multiple sensors for the same biometric trait are incorporated. For instance, the use of multiple sensors (ultrasonic and optical) in order to capture different fingerprint features of user.

b. Multimodal:

It is based on combining the evidence from more than one biometric trait such as fingerprint and voice. Therefore, it is more difficult for an attacker to create both an artificial fingerprint and another artificial biometric identifier such as iris, voice, or face. However, such system is cost effective due to employ more than one sensor in this scenario.

c. Multiple Units (Multi-Instance):

This is based on enrolling multiple instances of the same body trait, which can be used as identification/verification by either randomization of requested fingers (e.g. left and right index fingers), or requesting all fingers enrolled for identification/verification. This can reduce the likelihood of spoofed data being usable for verification [152].

d. Multi-sample:

This system is based on using a single sensor to acquire multiple samples of the same biometric trait (e.g. multiple impressions of the same finger).

e. Multiple Algorithms:

This system is based on processing the same biometric data by using multiple algorithms such as using different approaches to feature extraction or matching.

2. Retention of Identifiable Data:

Retaining image data (i.e. not destroyed data immediately after template generation) albeit posing substantial privacy and storage challenges may provide a means of resolving spoof claims [152].

3. Using Multi-Factor Authentication:

Although using biometrics with other authentication techniques such as password-protected smart cards reduces the probability of biometric systems being spoofed, it can be lost or stolen and reduces the convenience provided by biometrics [152]. In addition, it is not possible to employ such techniques in every application, especially in the case of availability of users in large numbers, which makes the template database much bigger than any allocated space in smart card.

4. Fingerprint with Password:

Using a password as identification is a very well known of the traditional methods. Besides, integration of password with fingerprint systems may reduce the associated security risk and possibility of forging with this traditional system. Such a system still suffers from lost or forgotten passwords. In addition, by using artificial fingerprint and stolen password, there is a high possibility to counterfeit such identification. However, this system is currently used in a number of applications such as wireless devices (e.g. laptop, mobile phone) due to affordability and high acceptability.

5. Supervision:

This technique is based on surveillance identification, verification, and enrolment to increase the security. Hence, it is more difficult to circumvent a system when being watched. However, this technique suffers from difficulty for a supervisor to detect transparent gelatin artificial print glued onto a live finger [19].

6. Voluntary Challenge-Response:

This technique is based on determining the presence of a user by a response to the requested challenge (e.g. place of birth). In voluntary case, the required response is based on the reaction of the user to hearing, seeing, or feeling something. Dissimilar to involuntary, voluntary techniques do not suffer from the lack of acceptability from using uncomfortable stimulus such as shocking (e.g. ask the user to enter the pin code). However, distinguishing between the challenge-response person and true owner of the fingerprint presented to the sensor is still a challenging issue in this technique [19, 153].

Table 4.3, illustrates the possible classification of voluntary liveness detection methods.

Methods	Voluntary Measurements	Limitations
Multimodal biometrics	Multiple sensors	Increases the timing, measurement and cost
	Multiple biometrics	
	Multiple units of the same biometric	
	Multiple representation and matching algorithms for the same biometric	Increases the timing, measurement and complex algorithms
	Multiple snapshots of the same biometric	Increases the timing, measurement and decrease acceptability
Retention of data	Retaining image data	Increases the timing, measurement and cost
Multifactor authentication	Fingerprint with password	Can be fooled by artificial fingerprint and stolen password
	Fingerprint with password-protected smart cards	Can be lost or stolen and reduces the convenience provided by biometrics
Challenge response	Reaction of the user to hearing, seeing, or feeling something	Difficulty of distinguishing between the challenge-response person and true owner
Supervision	Surveillance identification, verification, and enrolment	Difficulty for a supervisor to detect transparent gelatin artificial print glued onto a live finger

Table 4.3 Proposed fingerprint voluntary liveness detection methods and limitations

4.3 Summary and Discussion

Various methods in the public domain for artificial fingerprint attacks and countermeasures have been reviewed in this Chapter. Although these countermeasures have significant advantages for detecting artificial fingerprints, there are a number of limitations with them as:

a) The incompatibility of liveness techniques with some fingerprint sensors, which is increasing the measurement time, cost, and lack of proven results;

b) There is no clear criterion for all sensors and scenarios, and none of available methods in the literature has the ability to cover all requirements independently.

Therefore, any offered solutions for specific scenarios, and sensors, depend on special investigation of that scenario, individual acquisition, and related tenability of each sensor. Different environments and conditions used depend strongly on each sensor specification and each application requirement. Furthermore, more work needs to be done to verify these claims and evaluate security levels of each of them. Generally, the increase in the security of fingerprint system depends on the high recognition performance and liveness detection of user. However, many liveness detection techniques in the COTS (Commercial, Off-The-Shelf) and public domain claim to have had successful operations. Nevertheless, what is not clear is the proven efficient output (i.e. FRRs and FAR) in large number of users, and tenability experiences over long period of time. In this regard, using multibiometric have a number of advantages includes higher recognition, liveness detection, higher acceptability, and lower possibility of defeat due to difficulty for attacker to create both an artificial fingerprint and another artificial biometrics. However, it can increase the additional cost of sensors and authentication time, which can cause inconvenience for the user. From the above review, one can conclude that the security represents in fact, the prioritization of risks followed by coordinated and economical application of resources to minimize, monitor and control the negative effects (or even to accept some or all of the consequences of a particular risk), which is similar to other published works in the field [18]. Although the purpose of this Chapter was to present the particular liveness methods for use in fingerprint identification systems, a number of problems are preventing suggestions for perfect technique. The liveness technology market is changing rapidly, standards are not widely supported, and performance depends on the operational environment and life cycle cost of the technology. Furthermore, parallel to improving the liveness detection technologies, various types of attacks and forges are improving as well, and consequently the liveness detection systems should be one-step ahead in order to be efficient.

Chapter 5

Multibiometric Cryptosystem in Wireless Communication

Introduction

The recent improvement and innovation in networking, communication, and mobility especially in wireless networks such as GPRS and WiMAX, have increased the demand for enhanced security and identification in these fields. Regardless of the nature of the transmitting data with mobile devices, either involving the transfer of ownership or rights in M-Commerce or real-time monitoring of patient vital signs in M-Health, security of data and devices are the main issues. Many techniques have been proposed in the literature to employ biometric traits in wireless application such as Telemedicine, M-Health, and E-Commerce [6, 7]. Similarly, the embedding of fingerprint sensors in wireless devices such as notebook, PDA, and mobile phone has significantly increased during the last few years. Although, the fingerprint authentication system presents certain advantages from the protection viewpoint, like other unimodal biometric process, it is from the enrollment to the verification level susceptible to various types of threats and attacks. Therefore, providing the software, hardware, and advanced algorithms to deal with this intolerability against spoofing and fraud, remains an issue of concern when employing fingerprint in wireless device. These specific aspects are investigated in this Chapter.

5.1 Security Challenges in Wireless Applications

As discussed in previous chapters, wireless networks regardless of whether they use WiMAX or WLAN as defined in the IEEE 802.11 standard are inherently less secure than wired counterparts due to the lack of physical infrastructure [9]. There are a number of relevant publications that have addressed attacks and security issues of 3G, WiMAX, and WLAN [8, 9, 43, 44, 45, 47, 208]. These network security attacks have been explored by Karygiannis et al. [8] in two different approaches, including passive and active attacks as follows:

1) Passive Attack: This form of attack signifies that unauthorized party attempts to discover valuable information or listen to the channel instead of sending any message or disrupt the operation of a protocol. Generally, the passive attacks can be classified into the two subgroups as follows:

i) Eavesdropping*:* In passive eavesdropping, the attacker monitors transmissions for message content.

ii) Traffic analysis (traffic flow analysis): In this method, attacker attempts to gains intelligence by monitoring the transmissions for patterns of communication. In a wireless environment, it is very difficult to detect this attack due to not producing any new traffic.

2) Active Attack: This is another form of attack in which attacker inserts the information into the network. Although, there is a possibility to detect this kind of attack, it may not be feasible to prevent. This kind of attacks can be categorized as follows:

i) Masquerading (Impersonation): this is based on masquerading as trusted user by the attacker in order to achieve unauthorized privileges.

ii) Replay: this form of network attack is based on retransmitting the valid data by the attacker who intercepts transmissions.

iii) Message modification: this is based on altering a legitimate message by deleting, adding to, changing, or reordering it.

iv) Denial-of-service (DoS attack)**:** this is an attempt to prevent the normal use or management of communications facilities.

In order to make such networks more reliable, these vulnerability issues must be addressed first. Otherwise, consequences can be devastating, if such systems are not protected against these attacks, especially in sensitive application such as military. There are many available publications in scientific domain [8, 9, 45, 47, 208], which address this issue. Generally, wireless networks have to satisfy the following security requirement:

1. **Confidentiality**: this is to ensure that sensitive information is never disclosed to unauthorized third parties.
2. **Authentication**: verify the identity of the participants in a communication link which is known as authentication and hence, distinguishing legitimate users from impostors.
3. **Integrity**: integrity guaranties that transformed information could never be corrupted or altered in any unexpected way such as radio propagation impairment, or malicious attacks on the network.
4. **Availability**: since, DoS attacks could be launched at any layer of a wireless network and block a legitimate user's access to the network, availability can be a major security issue. This is to ensure the survivability or network services despite DoS attacks.
5. **Nonrepudiation:** this is to ensure that the originator of a message cannot deny having sent the message.

However, in certain applications there are other security concerns such as authorization and audit in E-Commerce application [46]. In addition, the mobility of wireless handsets and the possibility of these being lost or stolen is also a security concern. Wireless security is an end-to-end requirement, and as explained by Ravi et al. [44] can be sub-divided into various security domains including; appliance domain, network access domain, network domain and application domain security. The main concentration of this chapter is designated to have a control measure in place prior to establishing a network connection, so that access is restricted to the authorized users only. Biometrics can deliver outstandingly here as compared to the traditional solutions for access control, taking into account the rare chances of data being lost or stolen. As already discussed in previous chapters, there are inherent problems with utilizing multimodal biometric identification systems in wireless communications that seem likely to prevent further attempts at improving such an approach. The main problems are deeply rooted starting first with the mobility of wireless systems and the availability in large numbers, making the system more intolerable against spoofing and attack. The second issue is incompatibility of some biometric technologies and algorithms to allow it be employed over wireless medium. The latter has been alleviated by providing the incorporation of the fingerprint and voice recognition in previous chapters. Therefore, in order to limit the concentration to the scope of this thesis, providing the advanced algorithms to deal with former intolerability remains an issue of concern.

5.2 Fingerprint Image Storage

One of the main significant features in acceptability of any biometric system is directly dependent on where the data is stored and how it is protected. In a system based on one-to-one matching, the database can be decentralized (e.g. in smart card or on the local device) but in wireless applications due to the large numbers of users, it should be separated in a database center. Therefore, data and database should be protected against the imposter or attacker during transmission and in database. In such cases, the acquired sample must be transmitted securely to the location of template to perform the decision level. Otherwise, an incorrect storage or transmission strategy in a biometrics system can affect the overall biometrics system performance especially in wireless communications. As a result, storing biometric features in server is not an appropriate technique unless some countermeasures that can make the storage inaccessible for imposter such as encryption or anonymous techniques are employed.

In the next sections, well-known eminent threats and attacks on the fingerprint template database and data communication stream are explored. In addition, some countermeasures and techniques to overcome such a problem are discussed and amongst the recommended solutions, an attempt will be made to select the most appropriate one.

5.3 Protection and Attacks on the Data Communication & Template

As compared with wired networks, the wireless technologies are more intolerable against various types of threats and attacks, due to primarily mobility and availability of data in the open area. Therefore, data and database should be protected securely during transmission or in database. This section concentrates on the possibility of attacks at the fingerprint recognition systems during transmission or in database. Anderson [174] and Schneier [175] have documented a number of attacks and vulnerability points due to errors in design, implementation, and installation. These eight potential attack points (Figure 5.1) are classified in two categories called "Replay" and "Trojan horse" attacks [18].

5.3.1 Replay Attacks:

a. Attack on the channel between the acquisition device and the feature extractor by intercepting the data of a legitimate user which is replayed at a later time to the feature extractor;

b. Attack on the channel between the feature extractor and the matcher module by snooping a biometric feature of user, which is stored to be replayed later on the channel;

c. Attack on the channel between the system database and matcher module by snooping to steal the record of a user to replay later on the channel;

d. Attack on the channel between the matcher, and the application requesting verification by snooping to access the response of a previous verification that is stored to be replayed later in the channel.

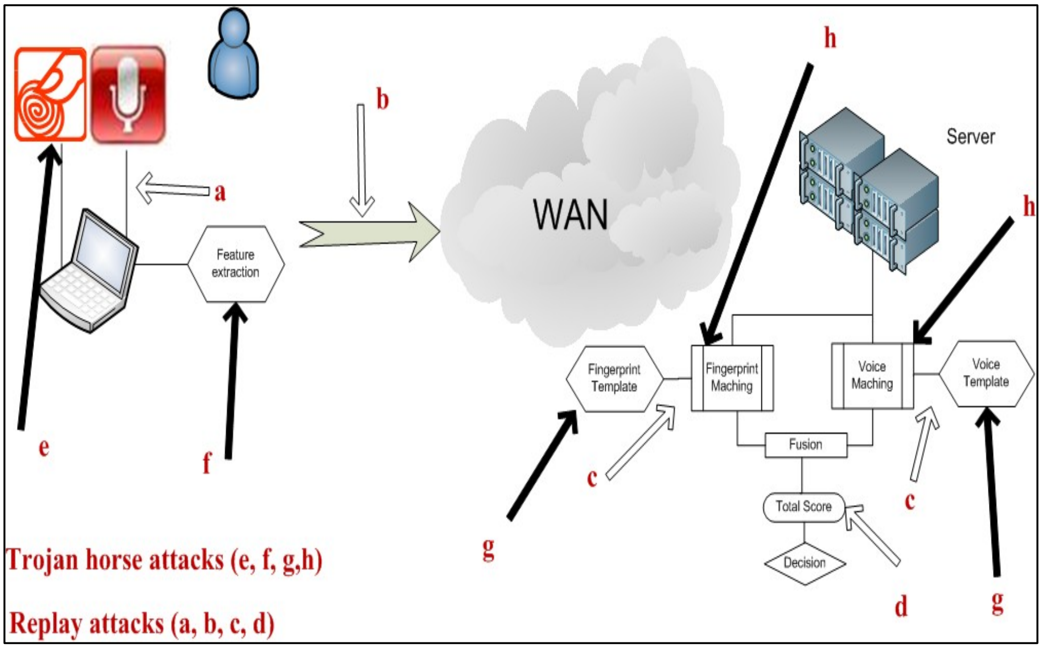


Figure 5.1: Possible security attack points **(**adapted from [179])

5.3.2 Trojan Horse Attacks:

e. Attack at the scanner by fooling the acquisition device (e.g. a fake fingerprint, such as a latent fingerprint lifted on a paper);

f. Attack on the feature extraction module by using a Trojan horse program to disguise as the feature extractor and submit artificially generated fingerprint features to the matcher;

g. Attack on the system database by employing Trojan horse program to disguise as the system database and submit an artificially generated database;

h. Attack on the matcher module by using Trojan horse program to disguise as a matcher and submit an artificially generated matching score, which can result a denial-of-service when generating a low matching score.

5.4 Protection & Countermeasures

As detailed above, the fingerprint authentication system from enrolling to the verification level is susceptible to Trojan horse attacks and Replay attacks. Various countermeasures proposed to thwart a fake fingerprint attack, therefore, providing the algorithms and techniques to deal with the intolerability against Trojan horse attacks and replay attacks are investigated in following paragraphs.

5.4.1 Trojan Horse Attacks:

The fingerprint authentication system processes from enroll to verification level (i.e. scanner, feature extraction, matcher, and system database) are susceptible to Trojan horse attack. Embedding a fingerprint recognition system (sensing, feature extraction, matching, and database) inside a smartcard is an effective way to prevent installing Trojan horses and to avoid intercepting the critical information [18]. However, smart card can be lost or stolen and it is not possible employ such techniques over wireless applications due to the existence of large numbers of users, which make the template database much bigger than any allocated space in smartcard. Therefore, these mentioned process levels should be located in a secure and confident position either by physical surveillance such as supervision or cryptography algorithms. The possibility to fool the scanner by fake fingerprint and the difficulty for a supervisor to detect, led to use the cryptography algorithms. Otherwise, it is very difficult to trust the scanner or feature extractor by server especially in the wireless application. In addition, it is impossible to use the supervision technique with a wide range of users such as large computer networks or wireless applications. As a result, storing biometric features in server is not an appropriate technique unless using some countermeasures that can make the storage inaccessible for imposter such as encryption or anonymous techniques.

5.4.2 Replay Attacks:

A reply attack can demolish the trust between the process levels (i.e. scanner, feature extractor, matcher, and database) by resubmission of intercepted data of a legitimate user. Embedding a fingerprint recognition system inside a smartcard is not an effective way to prevent a reply attack as well as Trojan horses in wireless applications due to the above-mentioned limitations. Therefore, protecting the fingerprint information during the communication process leads to use of the cryptography algorithms to increase the confidence in data in any authentication stages as a minimum requirement in wireless applications. The next subsections describe various cryptographic methods that are proposed by other researchers to find optimum solutions preventing such replay attacks at fingerprint system.

5.4.3 Cryptography Techniques:

A cryptographic system is as strong as the encryption algorithms, therefore by counterfeits encryption algorithms such as digital signature or one-way hash functions, whole the system can be forged. Generally, two kinds of key based encryption exist; Symmetric that refers to using a single secret key for both encrypting and decrypting a message and Public-key which is based on using a pair of keys, the first key (the private key) used to encrypt a message and the second one (the public key) used to decrypt the message. Key distribution is difficult in symmetric cryptography technique especially in a large network like wireless application, in which many key pairs should be managed. In addition, encrypted messages can easily be decrypted by compromised keys, which for a two-party communication will require the key to be changed frequently.

In comparison with the symmetric, the key management is easier in public-key cryptography because only the private key must be kept secret and the key may remain unchanged for considerable periods of time (even several years). Therefore, in a large network, the number necessary keys may be considerably smaller than in the symmetric-key scenario. Although this technique can be used to secure a communication link for data integrity, it is not able to solve the non-repudiation problem. In addition, no public-key scheme has been proven to be secure and throughput rates for the most popular public-key encryption methods are several orders of magnitude slower than the best-known symmetric-key schemes [176]. Digital signature is able to solve the problem of non-repudiation based on the ensuring the receiver that a message was sent by the claimed sender. There are various kinds of digital signature algorithms such as Full Domain Hash and RSA-PSS based on RSA, which similar to the traditional handwritten signatures can provide non-repudiation [177]. However, the use of public-key cryptography is computationally expensive for digital signatures [178] and still old stored image can be accepted as readily as a fresh one. In the same way, a hash or digital signature of a signal does not check for its liveliness but its integrity [179].

5.4.3.1 Challenge-Response:

Similar to the Challenge-response at the sensing level, this is based on determining the presence of a user by specific response from the receiver. The receiver who expects a fresh message from sender, first sends a nonce (challenge), requiring the subsequent message (response), and accepts the message as fresh only if the message contains the correct nonce value. For instance in fingerprint authentication, the server accepts the features as genuine only by receiving the secure response from the fingerprint scanner. The main limitation of this technique is the difficulty of distinguishing between the challenged responding person and the true owner of the fingerprint presented to the sensor [153].

Ratha et al. [179] proposed the method called Image based challenge/response that is based on the challenges to the sensor (assumed to have enough intelligence to respond to the challenges) instead of challenges to the user. Their approach to assure liveliness is providing the sensor with a dissimilar challenge each time and exploits the availability of a large number of image pixels to produce image-dependent response functions. Their proposed solution, initiated at the user terminal or system, then transaction server (assumed is secure) generates a pseudo-random challenge for the transaction and sends it to the intelligent sensor. Finally, the sensor acquires a signal at this point of time and computes a response to the challenge based on the new biometric signal. It is nearly impossible to inject a fake image by integrating the responder onto the same chip as the sensor [179].

5.4.3.2 Digitally Watermarking:

In this scheme, images or features can be protected by embedding information into itself. This technique can be explored with two approaches: either visible or invisible. In latter, data including picture or features are available visibly (for instance, when a logo is added to the corner of a TV broadcast). The invisible watermarking as its name suggests will not change the visual appearance of the image in any way and only a trained eye can spot the hidden incorporated data (example of this type is copyright protection). In addition, digital watermarking can be classified in different categories depending on robustness including fragile and semi fragile. Fragile watermarking is a scheme that any modification is detectable while as opposite in robust watermarking, modification to the watermarked content has not affect the watermark. The latter is normally used for copyright protection or fingerprinting applications. In addition, semi-fragile watermark is robust to legitimate changes such as image compression while fragile to severe tampering or malicious distortions such as content modification [173].

Generally, watermark insertion can be implemented in two common approaches encompasses spatial and transform domain. The transform domain watermarking methods are executed in the coefficients of transformed image, which is obtained by transform techniques such as DFT (Discrete Fourier Transform), DWT (Discrete Wavelet Transform), DCT (Discrete Cosine Transform), and many others. While in the spatial domain watermarking are directly implemented to the original image pixels. In addition, robust watermarks can also be performed by using a combination of domains as well. Usually, transform domain method is more robust to resist image attacks than spatial domain methods [155, 140]. However, in some cases, DCTs and DFTs outperform the basic solutions; the information hidden with DWTs represents the better surviving wavelet-based compression algorithms than information hidden with DCTs or DFTs [129, 135].

For instance, Yeung et al. [128] proposed the watermarking fingerprint image by apply some forms of chaotic mixing to transform a visually pleasant into indistinguishable forms. However, visual patterns can be recovered after inverse transformation in their method. Finally, they have shown that their invisible fragile watermarking technique does not affect the recognition and retrieval accuracy. They believe that "watermarking of images will provided value-added protection, as well as copyright notification capability, to the fingerprint data collection processes and subsequent usage”.

As another case in point, Ratha et al. [179] present a method to hide small messages in a wavelet compressed fingerprint image, called WSQ-based data hiding. Their method hides such messages with minimal impact on the decompressed appearance of the image. Their approach is characterized by random placement of the message bits in the compressed and quantized WSQ indices. The fingerprint image can be decompressed without any visible difference by any decoder while, only the right decoder can locate and extract the hidden message from the compressed image. The main advantage of the algorithm is the possibility of using different random number generators or seeding strategies to make each different implementation unique. In addition, breaking one version will not necessarily compromise another one due to the necessity of compatible outputs of one the encoder with another version of the decoder [179]. However, the main issue in fingerprint image-based techniques is the lack of proven established results in term of security and any advantage over standard cryptographic techniques [18].

5.4.3.3 Cancelable (Revocable) Biometrics:

As discussed by Schneier [180] in the case of stolen biometric information during the process, such as a template database dissimilar to the digital certificate, the biometric system is unable to issue another one. For instance, if the user’s thumb fingerprint information has been stolen during fingerprint authentication, the user does not have another thumb fingerprint as a different password and this remains stolen for life. In addition, the biometric traits are necessarily common across different functions and as one should never use the same password on different systems, the consequence of using the same encryption key in for two different applications is quite severe (e.g. fingerprint to start car, unlock medical records, and access to the laptop). However, as compared with PIN or signature, biometrics traits are powerful in term of uniqueness, universality, and impossibility of lost or stolen. Biometric lacks useful characteristics when used as key, such as secrecy, randomness, inability to update or destroy. These limitations can be addressed by designing the biometric systems with ability to reissue, update, or destroy the template if it is compromised (e.g. stolen digital data) which is called “Cancelable Biometrics”. The main advantage of such system is not losing the disclosed biometric information (e.g. fingerprint image or fingerprint template) forever and enhancing the security and privacy of the biometric system as a result. In addition, because of enrolling the intentionally distorted or some privileged information (e.g. an encryption key) in finger (or other biometric) instead of using the true finger, different applications are able to use a dissimilar template for which it becomes infeasible to change the database by using a fingerprint template [180]. Ratha et al. [181], have introduced cancelable biometric in order to alleviate the aforementioned problems with biometric systems. Their scheme consists of an intentional, repeatable distortion of a biometric signal based on a specific chosen transform. As a result, the biometric signal is distorted in the same fashion at each presentation for enrollment and for every authentication. Furthermore, using a different transform in every instance of enrollment is rendering the cross matching impossible. In the case of a compromised variant of the transformed biometric data, the transform function can simply be changed to create a new variant (transformed representation). When a noninvertible distortion transform is selected, even in the case of known transform function and transformed biometric data, the undistorted (original) biometric cannot be recovered [181]. Ratha et al. [182] loosely divide the alternate solutions emerged after defining the problem of cancelable biometrics:

1. **Biometric Salting**: In this technique similar to the password "salting" in cryptosystems, the database is created by hashing the password (P) and pseudorandom string (S) together (H (P + S)). As a result, the random sequence increases the entropy and finally the security of the password (biometric information) [182]. The main advantages of salting (e.g. Biohashing) scheme are low false accepted rates and possibility of generating multiple templates for the same user by using different keys (Since the key is user-specific). However, in the case of a compromised user-specific key, the template is no longer secure due to the usually invertible transformation. In addition, it is necessary to design the salting mechanism in such a way that the recognition performance does not degrade due to the matching in the transformed domain (especially in the presence of large intra-user variations) [183].

2. **Biometric Key Generation:** This scheme refers to generating a key directly from the biometric signal without requiring any user-specific keys or tokens like "biometric salting" methods. In this approach, instead of storing the actual biometric

itself, a calculated key K (B) from the biometric (B) is stored and during verification it is checked if K (B) = K (B'). However, the key generation is scalable when compared with the salting technique; the main problem remains achieving error tolerance in the key due to the inability to extract the same feature at different time [182].

3. **Fuzzy Schemes:** this is based on constructing cancelable templates by combining the biometric information with public auxiliary information P (also called helper data, shielding functions, or fuzzy extractors) to reduce the intra user variation. This scheme initiate by defining a metric d (B, B'), (e.g., Hamming, Euclidian, set distance, etc.) on noisy biometric data B and B'. In their notation, Gen and Rep represents generating and reproducing functions in this scheme. As next step, the generating function takes the biometric data along with user specific key/information K to produce a public string P and a secret string S, Gen(B, K) → < S, P >. Finally the reproducing function takes the public string along with another biometric measurement to reproduce the secret string Rep (B', P) → S. “In other words, fuzzy schemes extract some randomness S from B and then successfully reproduce S as long as d (B, B')≤ ε” [182].

4. **Noninvertible Transforms:** In this approach, the biometric is transformed using a one-way function stored instead of the original biometric. In addition, the transformation takes place in the same signal or feature space as the original biometric. One of the most popular non-invertible transform is a one-way hash function and when using it together with a verification function, can be used to hiding the biometric information due to the infeasibility to find x such that H(x)=h computationally for any given value h (information hiding). This feature can be used as collision avoidance due to the fact that for any given block x, it is computationally infeasible to find y≠ x such that H(y) = H(x). However, during different authentication attempts when passwords are the same, obtaining the same-hashed function it is not possible due to the impossibility of acquiring the same fingerprint image during various acquisitions [182].

The non-invertible transform provides increased security than the salting approach in the case of compromised keys due to the nature of this function, which makes very hard to recover the original biometric template. Such system provides also diversity and revocability by using application-specific and user-specific transformation functions, respectively. However, a trade-off between discriminability and noninvertibility of the transformation function remains the main drawback of this approach. This is caused by the necessity of preserving the discriminability (similarity structure) of the features transformation function and necessity of noninvertibility simultaneously in order to decrease the possibility to obtain the original feature set by the adversary [183].

Furthermore, Jain et al. [183] classified biometric cryptosystems as key binding and key generation systems depending on how the helper data is obtained. If this is obtained by a binding a key (independent of the biometric features) with the biometric template, it is referred as a key binding and if it is derived only from the biometric template and the cryptographic key is directly generated from the helper data, it is referred as key generation. The main advantage in the key binding system is that this is tolerant to intra-user variations in biometric data, due to the error correcting capability of the associated codeword. However, this can possibly reduce the matching accuracy due to the necessity of using error correction schemes by matching that prevents the use of sophisticated matchers developed specifically for matching the original biometric template. The other drawback is the necessity of carefully designing the helper data and not providing the diversity and revocability by biometric cryptosystems. As a recent trend, there are some attempts in the literature to introduce these two properties (diversity and revocability) into the biometric cryptosystems mainly by using them in conjunction with other approaches such as salting [184]. In contrast, the key generating cryptosystem remains an attractive template protection method especially in the cryptographic applications due to the direct generation of the key from biometrics. However, this key does not have a high stability and entropy due to the low stability of the biometric feature [183].

Ratha et al. [182] addressed the security and privacy issues with fingerprint databases by cancelable biometrics over other approaches. They present an analysis of the approximate strengths and merits for several alternatives, such as Cartesian, polar, and functional transformation. They showed experimentally that a surface folding transform achieves better results than the other two transforms. Finally, they conclude that a cancelable transform can be applied in the feature domain without much loss in performance.

As discussed by Thomas et al. [185], the main problem in using cancelable fingerprints is the requirement of an explicit registration step to align a fingerprint image to a pre-determined point of reference on some coordinate system. This means that in order to recover an alignment between two fingerprints in the feature space, it is easier to recover an alignment in the non-invertible transformed space and this is diminishing the verification performance of the fingerprint recognition system. One method to address this issue is the triangles technique described in [186] and extended in [187], which is using minutiae directly as features based on the computed higher-level Meta features (triangles). For any set of three minutiae, a triangle can be formed and the three sides of the triangles, the three angles of minutiae orientation, and the height of the largest triangle side are used as invariants [185]. In addition, Jain et al. [183] have discussed various aspects of attack against stored biometric templates and available techniques in the literature to counter these threats. They have classified template protection schemes into two categories namely the feature transformation and the biometric cryptosystem. In their analysis, they believe that there is no "best" approach yet for template protection and the choice of any protection scheme is directly dependent on the application scenario and requirements. They have presented the specific implementations of these approaches on a common fingerprint database. Finally, they conclude that available template protection schemes are not yet sufficiently mature for large-scale deployment and they do not meet the requirements of diversity, revocability, security, and high recognition performance. Therefore, they believed that the limitations of using a single template protection could be addressed either by hybrid schemes which take advantage of the different protection methods or by multibiometric and multifactor authentication systems [183].

For instance as a hybrid scheme, Bringer et al. [188] applied secure sketches to cancelable biometrics in order to use the security advantages of both schemes. They explained a specific algorithm that showed good performances on a fingerprint database by mixing several sketching techniques and a cancelable transformation. In addition, they proposed to add a physical layer of protection by embedding an enrolled template and the matching algorithm in a smart card [188].

In another multibiometric instance, Sutcu et al. [189] considered a fusion of a minutiae-based fingerprint authentication scheme with SVD values of face biometrics in the feature level, which was used to construct secure templates based on the "secure sketch" and a known geometric transformation on minutiae. However, the fusion at the feature level is difficult especially in the multi-modality biometrics due to the different feature representations and different similarity measures [190]. They have investigated different possible methods to combine the extracted features from different modalities, and construct secure templates to make it computationally infeasible to forge an “original” combination of fingerprint and face image that passes the authentication. Therefore, features of the transformation (minutiae to points on a circle) fingerprint minutiae [191] have been selected to be combined easily with SVD coefficients due to the same representations of features. They have shown the possibilities for much more complicated operations that can be performed over the combined biometric features before doing classification or authentication, although their fusion technique is based on the “and” of independent tests of fingerprint and face biometrics. However, the problems encountered are the precise measure of min-entropy of the original features, due to the high dimensional space and limited data and determine the exact information leakage due to the sketch.

5.5 Validation of Watermarked Fingerprint with Text Dependent Speaker Recognition

Although the fingerprint authentication system represents certain advantages from the protection viewpoint, like other unimodal biometric process, it is from the enrollment to the verification level susceptible to various types of threats and attacks. Therefore, various available attacks and countermeasures in the public domain for different level of fingerprint system (sensor, template, and communication level) have been reviewed in this Chapter. Despite the fact that these countermeasures are able to represent significant advantages against number of attacks, none of available methods in the literature has the ability to cover all fingerprint security requirements (e.g. diversity, revocability, liveness detection, and high recognition performance) independently.

Therefore, providing the software, hardware, and advanced algorithms to deal with this intolerability against spoofing and fraud, remains an issue of concern when employing fingerprint in wireless device. In this regard, using the hybrid schemes to take advantage of the different protection methods or multibiometric and multifactor authentication systems can alleviate some of the limitations of current fingerprint based system. As detailed in the previous chapter, multibiometric have a number of advantages includes higher recognition, liveness detection, higher acceptability, and lower possibility of defeat. Furthermore, in Chapter 3, possible solution to address the limitations of the speaker recognition in wireless communication has been recommended. It is based on sending voice features instead of raw sample through the proposed text dependent algorithm, therefore reducing the transmission time and dependency of the data on the quality of microphone or communication channel. Therefore, watermarked fingerprint with the same text, which is used as text dependent speaker recognition will be combined and embedded as cancelable multibiometric recognition (Figure 5.2).

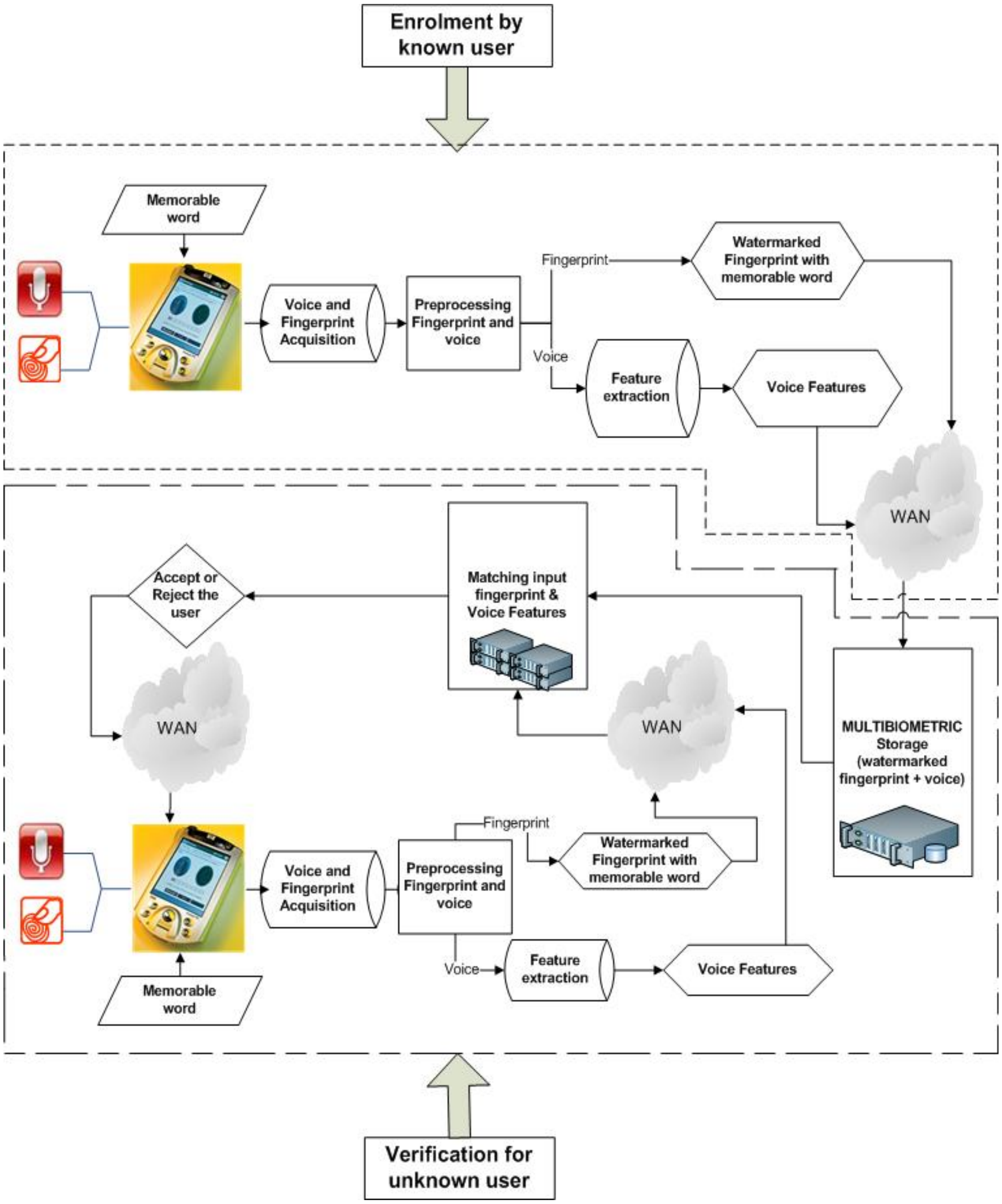

Enrolment by known user
Memorable word
Voice and Fingerprint Acquisition
Preprocessing Fingerprint and voice
Fingerprint
Watermarked Fingerprint with memorable word
Voice
Feature extraction
Voice Features
WAN
Accept or Reject the user
Matching input fingerprint & Voice Features
WAN
WAN
MULTIBIOMETRIC Storage (watermarked fingerprint + voice)
Voice and Fingerprint Acquisition
Preprocessing Fingerprint and voice
Fingerprint
Watermarked Fingerprint with memorable word
Voice
Feature extraction
Voice Features
Memorable word
Verification for unknown user

Figure 5.2: Block Diagram of Recommended System

In the enrolment scheme first, the fingerprint is watermarked with a memorable text and will be sent together with the voice feature based on the same text to the server over wireless channel. While in the verification stage, the claimed user will be asked to input fingerprint with a memorable text and utterance the text that is watermarked with the fingerprint during the enrolment stage. Finally, matching and accepting the claimed user will be based on the matched input fingerprint and text dependent voice feature of the claimed user with the one in the database. The Discrete Wavelet Transform technique has been used to embed and extract the text into the fingerprint image. This is due to the robustness of the transform domain as compare with spatial domain methods and DWT represents the better surviving wavelet-based compression algorithms than other. This wavelet technique will be explained in depth in the next Chapter.

This system has capability to take advantage of both cancelable biometric and multibiometric with less manipulation in wireless device, wireless communication and biometric system. In addition, this text dependent voice can be used as a challenge respond to determining the presence of a user by response to the requested challenge (e.g. place of birth). There are a number of other advantages for suggested system encompasses:

1. **Improving the accuracy of the overall system:** The accuracy of the system can be improved by combining the information derived from multiple traits to reduce the FAR and FRR of the system;
2. **Cover the limitation of non-universality and noisy data:** Provide sufficient data that is not derived from a fingerprint alone and cover the inadequate single trait as well (e.g. recognize the user by voice feature if fingerprint feature is not enough);
3. **Improving the security of system:** In consequence of integration of multiple traits, it is significantly difficult for an impostor to spoofing the identity of the legitimate user (i.e. it is more difficult to create both an artificial fingerprint and voiceprint). In addition, different applications are able to use the dissimilar templates and features.
4. **Ability to reissue, update, or destroy the template:** It has ability to reissue, update, or destroy the template if this is compromised (e.g. stolen digital data). In addition, such system is not losing disclosed biometric information (e.g. watermarked fingerprint or voice feature) forever which is enhancing the security and privacy.

5. **Cover the limitation of unacceptable challenge response:** Addressing the limitations of challenge response in this scheme by acceptability of voice in wireless device and simply distinguish between the challenge respond person and true owner if the fingerprint data contains the correct nonce (e.g. knowledge-based text dependent) value.

Some of the general techniques to build cancelable fingerprint and voiceprint have been discussed in this and previous Chapter; implementation details of the developed technique over wireless communication system will be investigated in the next Chapter.

Chapter 6

Watermarked Fingerprint
(Tested Over Wireless Network)

Introduction

In the previous Chapters (2, 3, 5), appropriate biometric traits (voice recognition and fingerprint identification) offered together with multibiometric system to provide a reliable authentication method with optimum performance and accuracy in wireless communication system. In addition, watermarking has been introduced and DWT (Discrete Wavelet Transform) was shown to be satisfying the need for the protection of fingerprint image. The purpose of this Chapter is to develop a simple and accurate method to obtain high level of confidence fingerprint identification and watermarking technique through a simulated investigation. Therefore, based on the proposed methodologies in the previous Chapter, embedding the watermark message into the fingerprint image has been design and developed. This scheme encompasses three-step procedure, fingerprint image enhancement, embedding the watermark message into the enhanced fingerprint image and verify the integrity of the claimed user by extracting this watermark from the watermarked fingerprint image. In addition, this Chapter presents the motivation for developing this method, its phases, and its possible advantages through the simulate investigation.

6.1 Fingerprint Characteristics

Each person has individual fingerprints, which consists of different patterns, which can be classified in different ways. The most recent standard used by experts after years of study is based on three different groups, called loop (left and right), arch (plain and tented) and whorl or whirl (Figure 6.1). In addition, these main pattern types can be divided into different subgroups such as right or left loops, plain or narrow arches, and combinations of them.

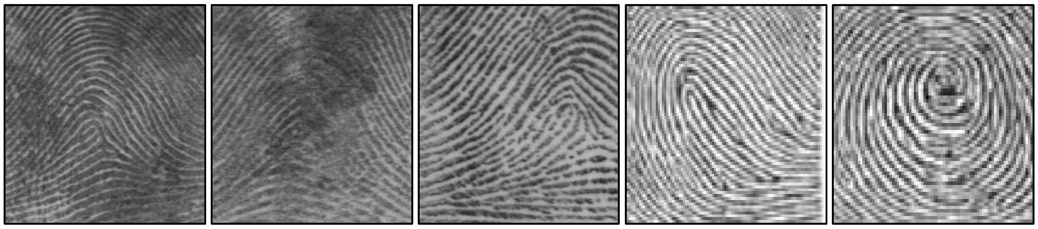


Figure 6.1: Tented arch, Arch, Left loop, Right loop, and Whorl

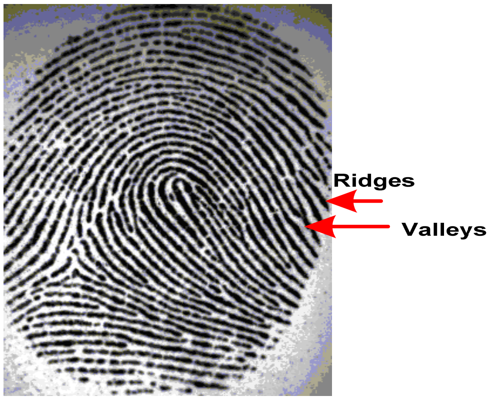


Figure 6.2: Fingerprint

6.2 Fingerprint Algorithm

The fingerprint contains detailed pixel information from the ridges and valleys of the image (Figure 6.2). Generally, fingerprint authentication techniques comprise the following five steps:

1. Fingerprint Acquisition

A fingerprint reader is the front end of a fingerprint authentication system. This unit captures the fingerprint image by a sensor, which is usually one of the two types: optical and solid state. These types of sensor have been detailed in Chapter 4.

2. Image Enhancement

Once the fingerprint image is captured, its quality is usually improved by enhancement techniques. This is particularly necessary if the image is damaged or not acquired very well.

3. Feature Extraction

In this stage, the characteristics or features of the ridge patterns are identified. Different features can be extracted from the ridges but the most prominent are called minutiae. These are alternatively known as endpoints (the point at which a ridge terminates) and bifurcations (the point at which a single ridge splits into two ridges).

4. Matching Level

This is the stage at which feature values are compared with similar feature values in a database, and a matching score is generated.

5. Decision Level

At this stage, a decision is made to either accept or reject the claimed identity based on the matching score obtained from the matching level.

Generally, fingerprint-matching techniques can be classified in three main groups namely; minutiae-based, correlation-based and ridge feature-based matching [18]:

(a) Correlation-Based Matching:

This method is based on superimposing an image from database with the fingerprint image captured during the enrollment and measuring the correlation of intensities between corresponding pixels for different alignments.

(b) Ridge Feature-Based Matching:

This technique is based on features (other than minutiae) extracted from the ridge pattern. Despite the fact that distinctiveness of these features is lower than minutiae, perhaps more reliable features may be extracted because of difficulty with extraction of minutiae in very low-quality fingerprint images.

(c) Minutiae-Based Matching:

In this matching technique, minutiae (ridge terminations and ridge bifurcations) are chosen as features. The position of minutiae are extracted from the fingerprint image and stored as sets of points in a plane. The two sets of points, one from the template and the other from the input image, are examined based on their alignment and the number of pairings is used for matching. Typically, in one fingerprint, endpoints and bifurcations combine to form up to 30 minutiae points on average.

In addition, there is another possibility by reaping the advantage of two matching systems. For instance, Ross et al. [49] proposed a hybrid-matching scheme based on employing both minutiae and ridge flow information in order to represent and match the fingerprints. In the correlation-based approach, decision is based on the measuring of the correlation of intensities between corresponding pixels for different alignments. The performance of these two methods relies on the effect of different parameters. These parameters are accurate detection of minutiae points and matching techniques in minutiae-based techniques. In the correlation-based approach, these parameters are non-linear distortions and image's noise. Nevertheless, generally minutiae-based presents better performance when compare with the correlation-based techniques [49].

In minutiae based matching, the attempt has been made to align two sets of minutiae points and make a decision based on the total number of matched minutiae [26, 49]. On the other hand, pre-processing of fingerprint images is a critical step before matching and feature extraction in order to improve the quality of the image, reduce computational time, and remove noise in the images. Hence, many efforts have been reported in the public domain to address this issue. For instance, Fourier transforms [76], Gabor filters [192], wavelets [193], histogram equalization [48, 64], and fuzzy algorithms [195] together with binarization, and thinning are a number of valuable steps for fingerprint image enhancement.

6.2.1 Justification of Using Fingerprint Enhancement before Watermarking

In order to address the lack of security issues in wireless communication, a novel multibiometric system has been proposed in previous Chapter. This was based on the combination of watermarked fingerprint with the same text, which is used as text dependent speaker recognition. The focus of this Chapter is on the minutiae-based matching and starts from the second step of fingerprint authentication (Enhancement) before embedding the watermark data. This is for the reasons that fingerprint image consist of worthless image area without valuable ridges and furrows which must be excluded before matching a pair of fingers. The valuable remaining area is sometimes known as ROI (Region of Interest). There are many publications in scientific literature on watermark schemes that are based on the enhancement of the fingerprint image [65, 79, 196 - 199]. For instance, Hsieh et al. [196] proposed a method based on the fingerprint image enhancement, discrete wavelet transform, and secret sharing scheme. They experimentally have shown that the retrieved enhanced fingerprint images are more recognizable than without enhancement.

In addition, there are several other advantages to embedding the watermarked data into the fingerprint image after enhancement algorithm. Firstly, watermark detection can be more robust against segmentation and other attacks such as filtering, due to degraded quality (even if the attacker concentrating his attack on the ROI). Secondly, there is the possibility of removing a part of watermark data during the enhancement process, which can be avoided by embedding this data into ROI, instead of whole image. Thirdly, it can provide more transparency to the embedded watermark since the region of interest is a highly textured area and the human eye is less sensitive to changes in that area. Finally, it can be used as countermeasures against changing the useless part of image by the attacker. This is because the useless part of fingerprint image is not processing in any fingerprint recognition algorithm, and hence it is not possible to detect any change in that portion of the image [65].

Therefore, some of the most common techniques used for the image enhancement step will be explained briefly together with proposing a novel method in the following section. This is to enable a discussion on the performance of the chosen method in comparison to other techniques in detecting artificial fingerprints or other attacks.

6.3 Fingerprint Images Enhancement Algorithms

The performance of feature extraction algorithms depend on the input fingerprint images and usually, fingerprint image enhancement is applied to obtain an enhanced output image through a set of intermediate steps. Various techniques, which are used to enhance the gray level of the fingerprint images, have been published in the scientific literature [106, 113, 119, and 202 –207]. The majority are based on the information about the local ridge structure in term of estimation of the local ridge orientation from input fingerprint images. However, such algorithms, which perform very well for good quality images suffer a drastic decrease of performance when low quality images are used, due to noise (creases, smudges, and holes). This section presents a novel enhancement algorithm based on the following methodology:

Methodology

Fingerprint images include unnecessary information such as scars, moist or areas without valuable ridges and furrows, and in order to eliminate the redundant information and filter the useful information, a specific process using the following four steps has been designed:

1. Normalization:

Generally, by normalizing an image, the colors of the image are spread evenly and all available values fills instead of just a part of the available gray scale. This technique used to reduce the variations in gray level values along ridge and furrows [25]. Histogram equalization, as normalization method, is a general process used to enhance the contrast of images by transforming its intensity values. As a secondary result, it can amplify the noise, producing worse results than the original image for certain fingerprints. Therefore, instead of using the histogram equalization, which affects the whole image, CLAHE (Contrast Limited Adaptive Histogram Equalization) is applied to enhance the contrast of small tiles and to combine the neighboring tiles in an image by using bilinear interpolation, which eliminates the artificially induced boundaries. In addition, the 'Clip Limit' factor is applied to avoid over-saturation of the image, specifically in homogeneous areas that present high peaks in the histogram of certain image tiles due to many pixels falling inside the same gray level range [99]. Additionally, a combination of filters in both domains, spatial and Fourier is used to obtain an appropriate enhanced image.

2. Binarization:

Its process to transforms the gray scale image into a binary image. Binary number (zero and one are represent by black and white) and then thinning process that reduces the ridges into one-pixel width. Finally, local minutiae are located on the binary thinned image. Various techniques are exist to binarizing the gray scale image such as: iterative application of a Laplacian operator and a dynamic thresholding algorithm [118] or fuzzy approach that uses an adaptive thresholding to preserve the same number of black and white pixels for each neighborhood [195] and etc.

In this section during this phase, the gray scale image is transformed into a binary image by computing the mean value of each input block matrix (16 × 16) and replacing all pixels with equal or greater than local mean with the value 1 and other pixels with the value 0 [48].

3. Quality markup:

In this phase, the unwanted data is removed, in order to separate the fingerprint image from the background or any unnecessary details before analysis. The algorithm is based on distinct block processing in which, the image is partitioned into blocks of 8 by 8 pixels, each represented by a matrix. The intensity of each pixel is used for the elements of these matrices. The standard deviation of each matrix (block) is calculated. All of the elements of each matrix are then replaced by its calculated standard deviation. Finally, in order to obtain the boundaries for the region of interest, the background image is removed by comparing the values of each matrix (elements) to a threshold value.

4. Thinning:

A good thinning method will reduce the width of the ridges down to a single-pixel while keeping connectivity and minimizing the number of false minutia as byproduct of this processing [26]. Generally, fingerprint images should often be filtered again to remove these false minutia structures. The proposed algorithm in this thesis eliminates most of these false minutia structures by sliding neighborhood processing in a first step followed by thinning without any additional filtering. Finally, the fingerprint image is separated from the background and local minutiae are located on the binary thinned image.

6.3.1 Histogram Equalization

In general, enhancement is the most used technique in medical image processing and biometric identification based on image. This will become the bottleneck when the image has very poor contrast. To improve the contrast of the image, a mapping can be used to transform the pixel intensities of the image. Histogram equalization is a well-known non-linear contrast enhancement technique to normalize cumulative histogram as the gray mapping function to obtain a new enhanced image with a uniform frequency distribution of image gray levels. Due to the flat distribution of the gray scale, basic form of the histogram can produce a worse result than the original image. In addition, by enhancing the contrast of an image through a transformation of its intensity values, the histogram equalization can amplify the visibility of image noise and eliminates the minor contrast differences of pixels falling in a small special region. Adaptive histogram equalization (AHE), which is an improved form of basic HE (Histogram Equalization), was invented independently by Ketcham et al. [211], Hummel [210] and Pizer [212] to enhance the contrast of medical images [216]. Basically, AHE uses pixelated form of the original image to apply the histogram equalization mapping to each individual pixel. In this method, the intensity of a pixel in a region is adapted by the surrounding pixels. Furthermore, bilinear interpolation scheme is applied to avoid visibility of region boundaries. Although, different size of the matrix set results in a different output, an 8 × 8 matrix commonly generates optimum result [213]. Whilst AHE largely improves the contrast of image in heterogeneous areas, the major drawback is amplification of background noise in homogeneous areas. To overcome this problem, a limited contrast enhancement is applied particularly in homogeneous areas. In the contextual histogram, these areas are distinguished as high peaks where many pixels fall inside the same gray level. Therefore, application of CLAHE permits only a specific number of pixels in each of the bins associated with local histograms. This result in a limited slope associated with the gray-level assignment scheme. To keep the total count of histogram identical, clipped pixels are then equally redistributed over the whole histogram. In this case, a multiple of the average histogram contents specifies the contrast factor (clip limit). To achieve limited contrast enhancement, low contrast factor is used as it lowers the slope of the local histogram. Whilst a very high contrast factor represents AHE technique, a very low factor (one) results in the original image (further information about CLAHE can be obtained from [213,216]).

Although, selection of appropriate clip limit generates an excellent result on most images, output image intensity cannot be used for quantitative measurements, where physical meaning of image intensity is important. As a first step of the image enhancement process, histogram equalization is applied to enhance the image contrast by transforming the intensity values of the image (the values in the color map of an indexed image), which are given by the following equation for k= 1,2,3, ... L:

$$S_k = T(r_k) = \sum_{j=1}^{k} P_r(r_j) = \sum_{j=1}^{k} \frac{n_j}{n} \qquad (6.1)$$

Where S_k is the intensity value in the processed image, corresponding to r_k in the input image, and $P_r(r_j)$, $j = 1,2,3, \ldots L$, represents the histogram associated with the intensity level of input fingerprint image. In other words, the values in a normalized histogram approximate the probability of occurrence of each intensity level in the image. In the following Figures (Figure 6.3, 6.4, 6.5 and 6.6), the differences between the histogram of the normal fingerprint before and after histogram, equalization (implemented in the MATLAB Image processing toolbox by function "histeq") is depicted [214]. It should be pointed out that by enhancing the contrast of an image through a transformation of its pixel intensity values; the histogram equalization can amplify the noise and produce worse results than the original image for some fingerprints. This is due to the fact that many pixels fall inside the same gray level range. Therefore, instead of applying the histogram equalization, which works on the whole image, CLAHE is used to enhance the contrast of the small tiles of an image and to combine the neighboring tiles using a bilinear interpolation. This will eliminate the artificially induced boundaries. In addition, 'Clip Limit' factor (implemented in the Matlab Image Processing Toolbox by the function "adapthisteq (f,"clipLimit") is applied to avoid the over-saturation of the image, specifically in homogeneous areas, which display a high peak in the histogram at the particular image tile.

By using CLAHE with Clip Limit, the slope of the Cumulative Distribution Function determined for the contrast histogram equalization is limited and the histogram is redistributed across all recorded intensities, enhancing the contrast and reducing the noise effects. Finally, the pixels are mapped by linearly combining the results from the mapping of four nearest neighboring regions. One has to note that contrast enhancement methods are merely designed to enhance particular characteristics in order to improve the image contrast. They do not supplement the structural information of the image. CLAHE is based on adaptive histogram equalization (AHE), where the histogram is calculated for the contextual region of a pixel. The pixels intensity is thus transformed to a value within the display range proportional to the pixel intensity's rank in the local intensity histogram. CLAHE is a refinement of AHE where the enhancement calculation is modified by imposing a user-specified maximum, i.e., clip level, to the height of the local histogram, and thus on the maximum contrast enhancement factor. The enhancement is thereby reduced in uniform areas of the image, which prevents over enhancement of noise and reduces the edge-shadowing effect of unlimited AHE. The size of pixels contextual region and the clip level of the histogram are the parameters of CLAHE.

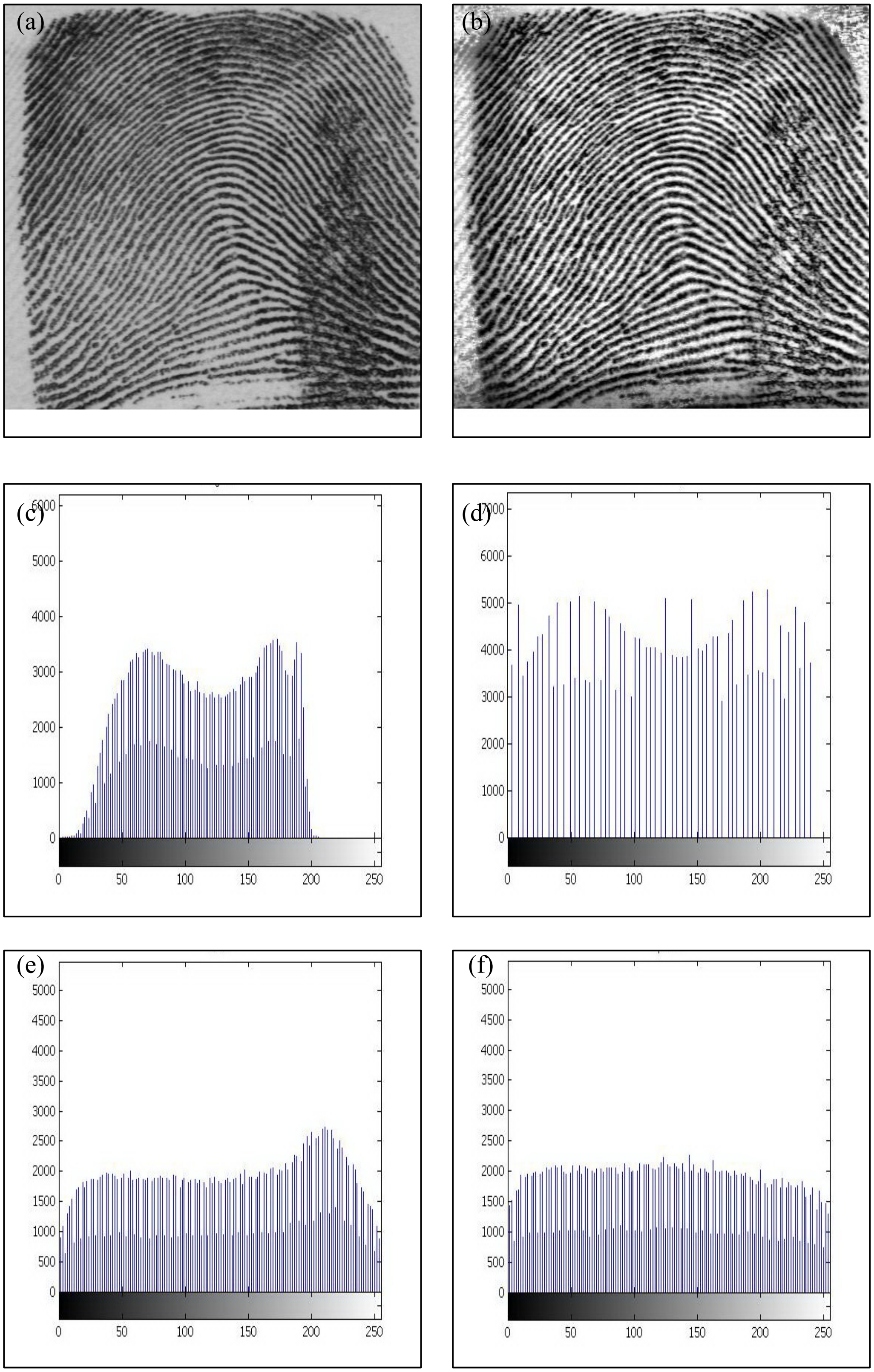


Figure 6.3: Original (sample1) fingerprint image (a), After CLAHE with Clip Limit (b), Histogram of original fingerprint (c), After Histogram equalization (d), After CLAHE (e), After CLAHE with Clip Limit (f).

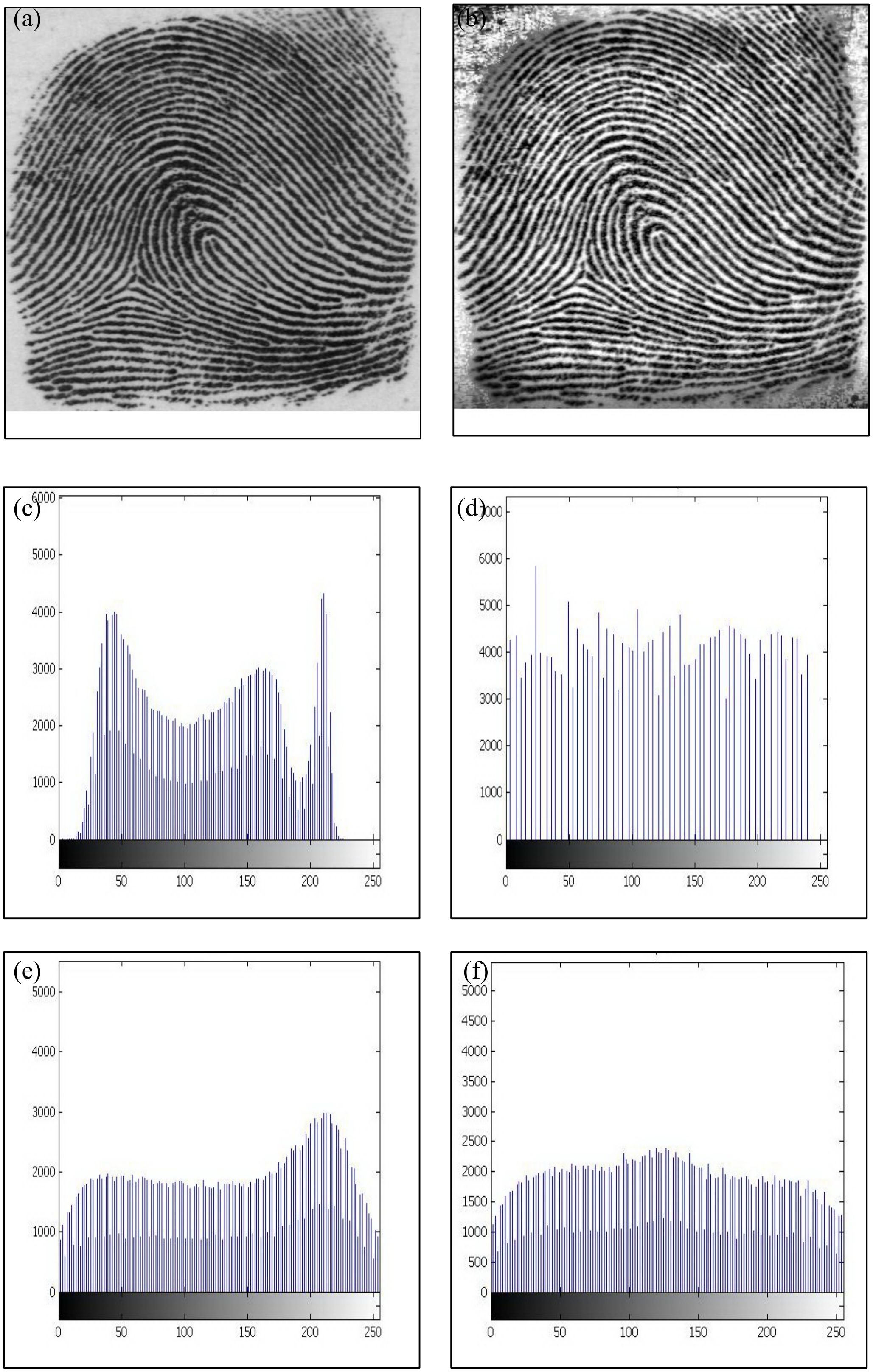


Figure 6.4: Original (sample2) fingerprint image (a), After CLAHE with Clip Limit (b), Histogram of original fingerprint (c), After Histogram equalization (d), After CLAHE (e), After CLAHE with Clip Limit (f).

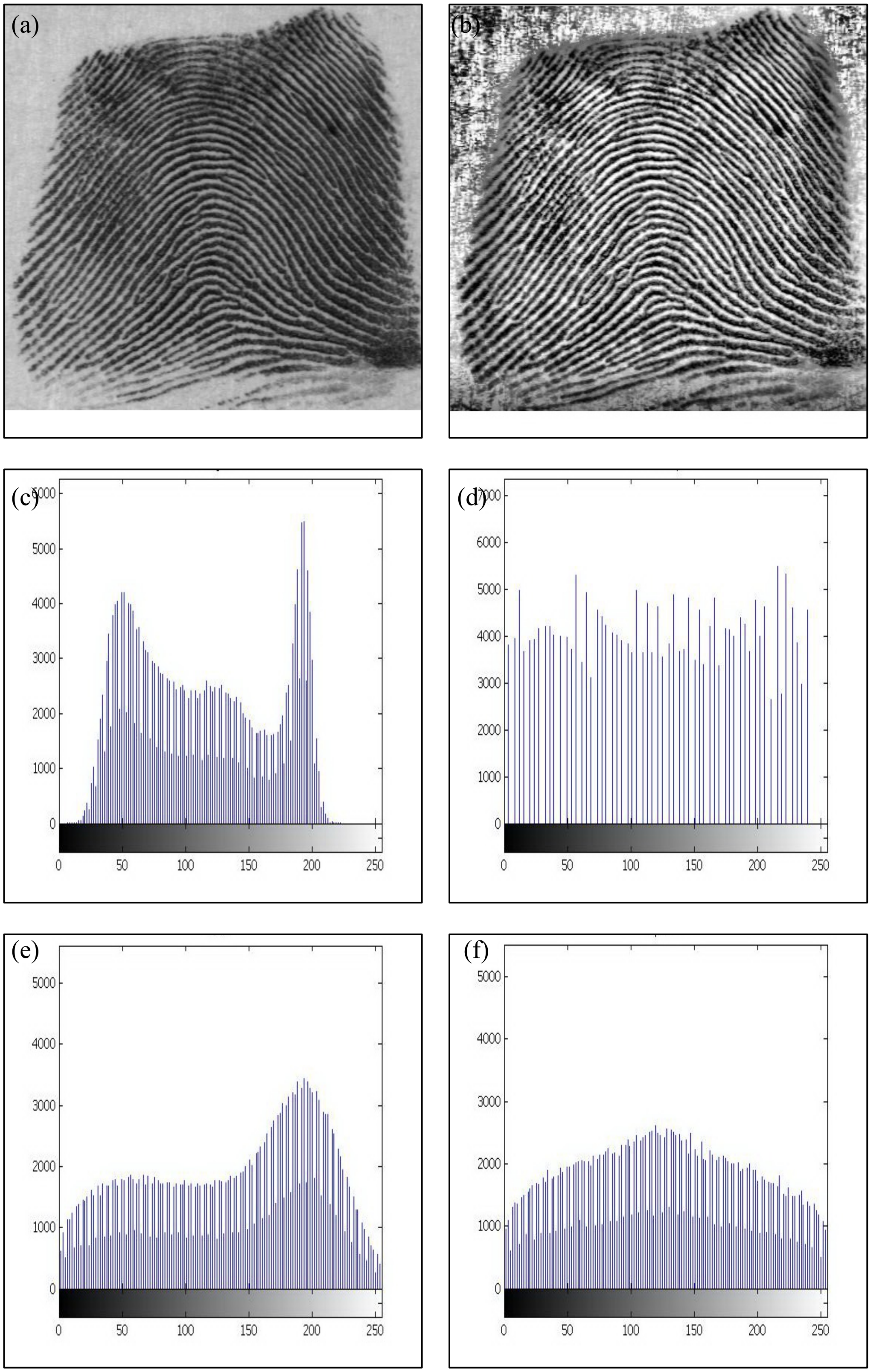


Figure 6.5: Original (sample3) fingerprint image (a), After CLAHE with Clip Limit (b), Histogram of original fingerprint (c), After Histogram equalization (d), After CLAHE (e), After CLAHE with Clip Limit (f).

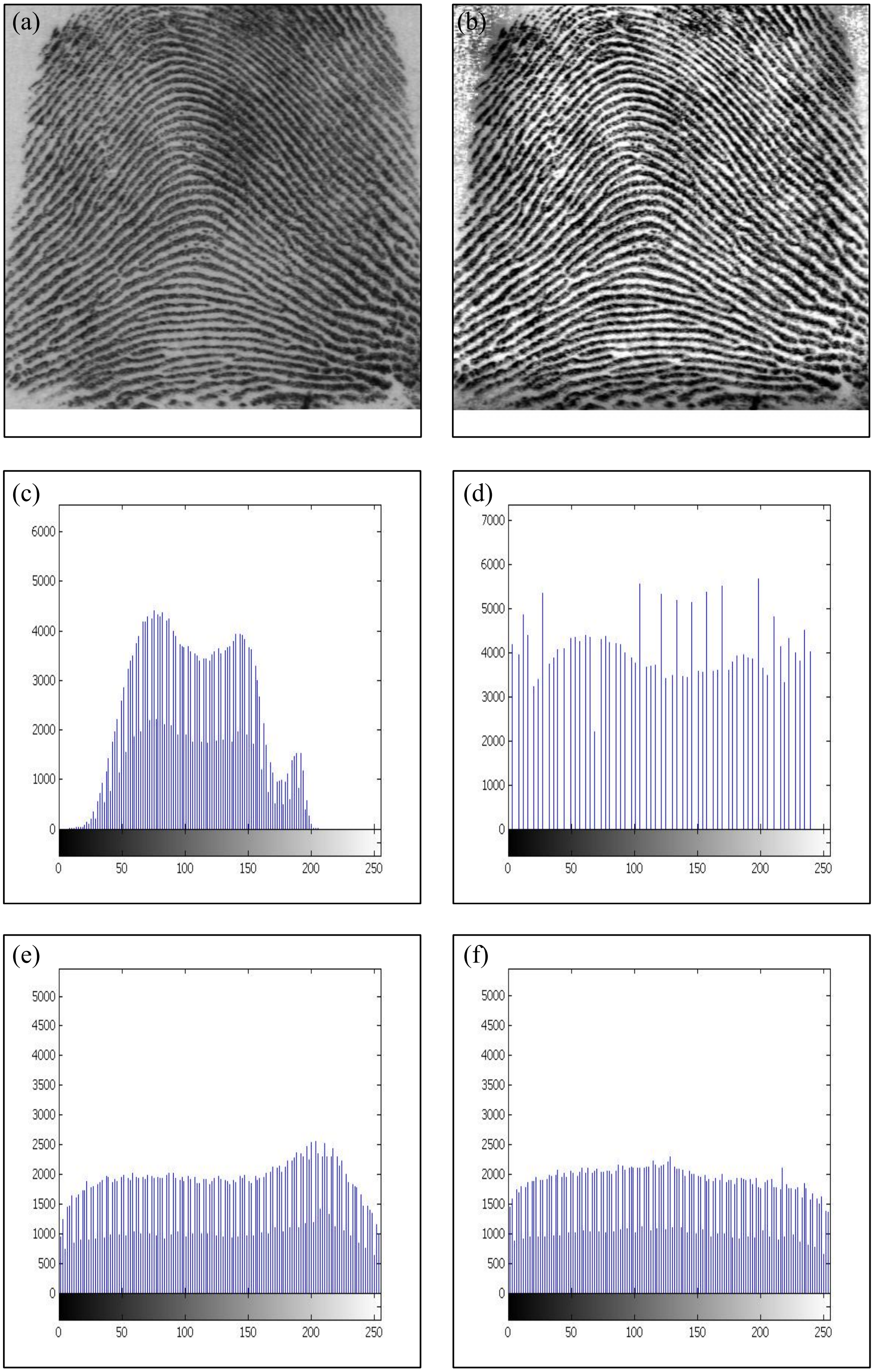


Figure 6.6: Original (sample4) fingerprint image (a), After CLAHE with Clip Limit (b), Histogram of original fingerprint (c), After Histogram equalization (d), After CLAHE (e), After CLAHE with Clip Limit (f).

The images in Figure 6.3, 6.4, 6.5 and 6.6 are the histogram-equalized results of the fingerprint images and improvements in average intensity and contrast are obvious. In addition, the spread of the histogram over the entire intensity increases the contrast and the average intensity level in the histogram of the equalized image. This level is higher (lighter) than the original level. The original fingerprint image and the corresponding processed images (after CLAHE with Clip Limit) are presented in Figure 6.3, 6.4, 6.5 and 6.6. The image in Figures 6.7 is the plot of transformation functions of CLAHE method with clip limit of 0.5. It is quite evident that the narrow range of intensity is transformed into full intensity scale in the output fingerprint image. In order to carry out the simulation of proposed enhancement algorithm, fingerprint samples from the database “DB 4 NIST” (National Institute of Standards and Technology) [220] have been employed. NIST Fingerprint database is comprised of 512 × 512 pixels in 8-bit gray scale images of randomly selected digitized inked fingerprints. However in practice, the NIST databases [220, 221] are only largely diffused datasets, they are not well suited to testing “on-line” fingerprint systems. This is due the fact that these images are considerably varying from those acquired by optical or solid state sensors, which are normally available in electronic devices [224]. Nevertheless, it was the attainable database during the simulation process. Therefore, experimental investigation of the other fingerprint databases such as FVC2004 or FVC 2006 [222,223] is necessary as future work of this research to evaluate the performance and to enable the unbiasedness of proposed algorithm. The experimental test has been carried out in Matlab environment under windows XP professional on PC Pentium 4.

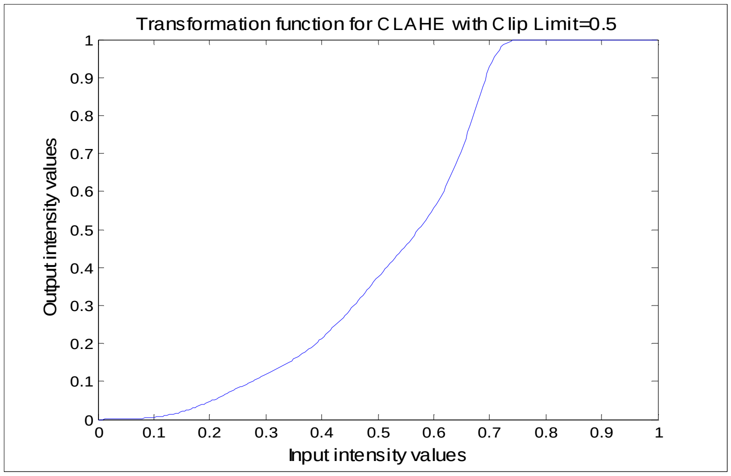


Figure 6.7: Plot of original image histogram, after CLAHE with Clip Limit

6.3.2 Spatial and Fourier Domain Filtering

Sherlock et al. [215] enhanced the fingerprint image in the Fourier domain, based on convoluting each image with pre-computed filters of the same size as the processed image. However, their algorithms do not use the full contextual information provided by the fingerprint image because of the assumptions that the ridge frequency is constant throughout the image, and decreases the number of pre-computed filters. Another approach has been proposed by enhancing the fingerprint image completely in the Fourier domain. This algorithm is based on dividing the fingerprint into overlapping blocks, and in each block, the image is obtained by [200]:

$$\mathrm{I_{enh}(x,y) = FFT^{-1}\{F(u,v)|F(u,v)|^{k}\}}$$

$$\mathrm{F(u,v) = FFT\big(I(x,y)\big)} \qquad (6.2)$$

This approach does not require the computation of intrinsic images for this operation, which has the effect of increasing the dominant spectral components while attenuating the weak components [200]. According to equation 6.2, a two-dimensional Inverse Fast Fourier Transform (IFFT) is applied as a second step, and computing the IFFT of each dimension of the input matrix is equivalent to calculating the two-dimensional inverse discrete Fourier transform (IDFT), defined by the following equation [99]:

$$\mathrm{f(x,y) = \frac{1}{MN}\sum_{n=0}^{M-1}\sum_{m=0}^{N-1} F(m,n)e^{j\frac{2\pi mx}{M}}e^{j\frac{2\pi ny}{N}}} \qquad (6.3)$$

$$\mathrm{0 \le x \le M-1,\quad 0 \le y \le N-1}$$

This technique was proposed by Watson et al. [87] and Willis et al. [39] to perform a sort of contextual filtering without requiring explicitly computing local ridge orientation and frequency. In their algorithm block size of 32 × 32 was found to be best and using a fast radix-2 FFT when the block size is a power of two, the FFT speed is optimum. Although , as it is considered by Willis et al. [39] requirements of patching in holes and smoothing, as well as separating incorrectly joined ridges is met in their algorithm, applying this technique raise two issues. The first is discontinuities at the edges of adjacent blocks and the second is at the edges and background of the image. In their algorithm, the former has been compensated by overlapping blocks and latter by summing the gray level pixels in each block and assigning the block to the background if this sum exceeds a threshold. However, a large amount of overlap between the neighboring blocks (e.g., overlap of 24 pixels) is necessary which can significantly increases the enhancement time [18].

Aguilar et al. [200], after analyzing various solutions used a combination of filters in both domains, spatial and Fourier to obtain an appropriate enhanced image. Their algorithm is based on algebraic sum of two enhanced images in which the resulting pixel will be white, if both images are white. As it is considered in their algorithm, Gabor filters have important signal properties such as optimal joint space frequency resolution. The even symmetric form of the Gabor function in their algorithm is given by:

$$G(x, y) = \exp\left\{-\frac{1}{2}\left[\frac{x^2}{\delta_x^2} + \frac{y^2}{\delta_y^2}\right]\right\}\cos(2\pi f x) \qquad (6.4)$$

Where f is the ridge frequency and the choice of δ_x^2 and δ_y^2 determines the shape of the filter envelope and the trade-off between enhancement and spurious artifacts [31, 200].

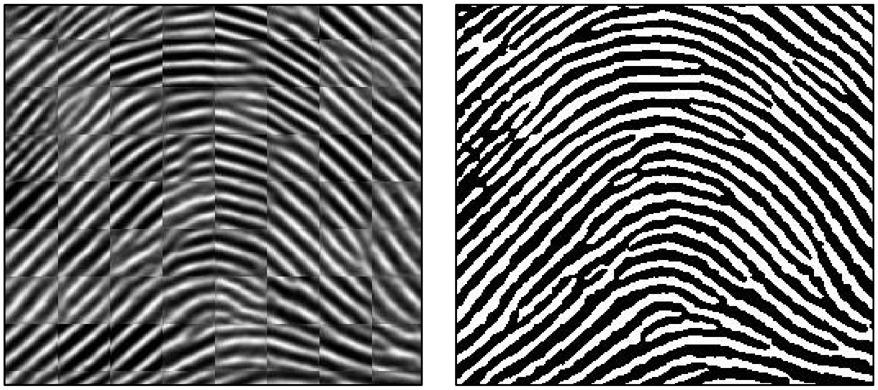


Figure 6.8: Left: After Fourier Transform **Right**: After Combination of Filters

6.3.3 Fingerprint Image Binarization

The fingerprint binarization is an algorithm that produces a 1-bit type image from 8-bit grayscale image. However, the adaptive binarization method is based on a threshold **t**, with gray-level pixels lower than **t** assigned to 0 and the others to 1. It is known that dissimilar fingerprint images have special contrast and intensity, and therefore, a unique threshold t is not the appropriate value for a general fingerprint image analysis. The local threshold technique changes **t** locally, by adapting its value to the average local intensity. However, in very poor quality fingerprint images, the local threshold method cannot guarantee acceptable results and a special threshold value, which has sufficient effect, is required [18, 26].

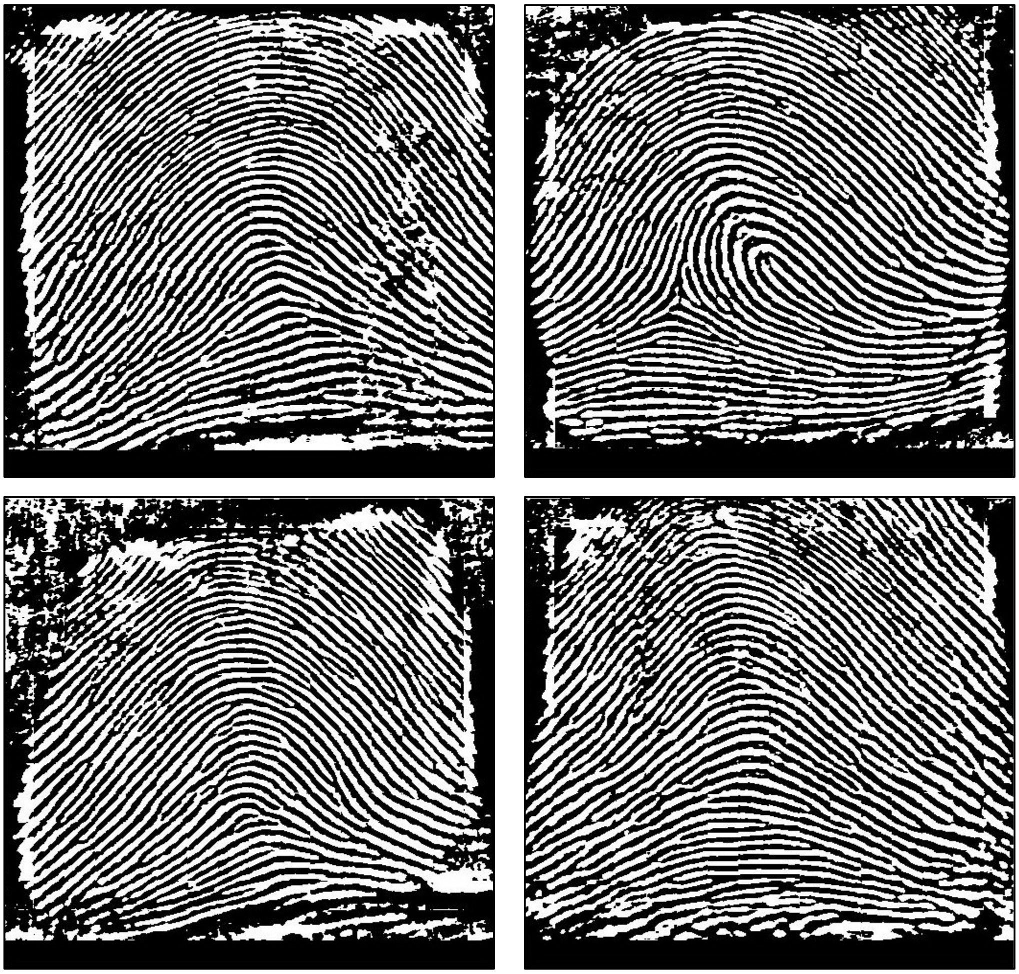


Figure 6.9: After Binarization

A wide range of evaluation study of locally adaptive binarization has been conducted by Trier et al. [41]. They have shown experimentally that Niblack's [147] method with post processing step appears to be the best. However, some improvement to this binarization method has been made by Sauvola et al. [148] and Wolf et al. [42] later. The fingerprint binarization based on the adaptive thresholding is a common image-processing tool [26] and has been previously utilized in number of the fingerprint enhancement methods [48, 78, 84, 85]. In this Chapter, Greenberg et al. [48] method is applied based on determining the mean value of each input matrix and replacing all pixels with equal or greater than local mean with the value 1 and other pixels with the value 0 (Figure 6.9). However, presented method in this thesis is able to reap the advantages of adaptive thresholding and Aguilar et al. [200] algorithm by summing the binarized images and assigning the resulting pixel to the background, if both belong to the background. From the experiment, this method is preferred due to the noticeable difference (more true minutiae) between this technique and summing the image after FFT and Gabor filter directly.

6.3.4 Foreground and Background Detection

In general, a fingerprint image contains ridges described by bright pixels and valleys by dark pixels plus some blank space near the edges. Normally the blank spaces are not valuable due to the noise of the image in this area. Therefore, the image area without valuable ridges and furrows must be excluded from the fingerprint image. The valuable remaining area is sometimes known as ROI (Region of Interest).

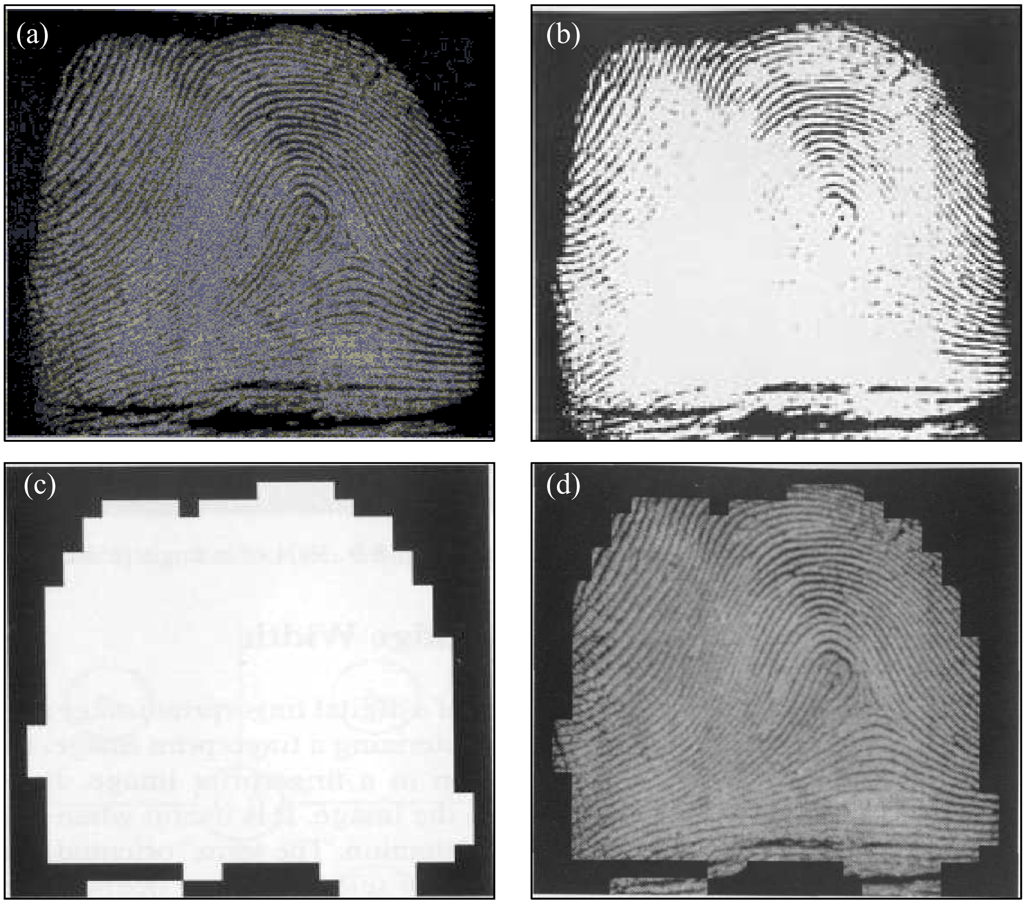


Figure 6.10: (a) Fingerprint image, (b) Thresholded fingerprint image (c) Region of interest (ROI) and (d) ROI of fingerprint [60]

Ratha et al. [60] in order to find the "interior" (aka ROI) of the fingerprint, have designed the algorithm based on partitioned fingerprint into 25 × 25 block and compute the percentage of white area (z) within each block and if z > t (threshold), set all pixels in the block to white. Otherwise, set all pixels in the block to black. In their algorithm, each block examined against a threshold t value obtained by the Otsu optimum threshold method [60]. In conclusion, each pixel is either an element of b (bright) or d (dark), as shown in Figure 6.10 (b). In their resulting image, the white region corresponds to the ROI (6.10 (c)) and by superimposing Figure 6.10 (c) on Figure 6.10 (a); they produce the regions of the fingerprint images, which is shown in Figure 6.10 (d) [60].

In order to find the ROI of a fingerprint, an algorithm based on distinct image block processing is presented in this Chapter. Suppose that the image is presented by an M×N matrix (corresponding to M×N pixels), whose elements define the gray scale intensities of the pixels. This matrix is partitioned into sub-matrices of size p × q. Here we assume that the numbers M and N are divisible by p and q respectively. If this is not the case, the image matrix is padded with zeros as necessary. As a result of partitioning, $\mathrm{n} = (\mathrm{M} \times \mathrm{N})/(\mathrm{p} \times \mathrm{q})$ sub-matrices B^{kl} are produced:

$$B^{kl} = \left(b_{ij}{}^{kl}\right)_{p\times q} \tag{6.5}$$

$$k = 1,2, \dots p, l = 1,2, \dots q$$
$$i = 1,2, \dots M/p\,, j = 1,2, \dots N/q$$

Where the values $\mathrm{b_{ij}}^{\mathrm{kl}}$ are the intensities of the pixels in the block. Next, the standard deviation of all elements is calculated for each sub-matrix and all of its elements are replaced by the standard deviation. This operation is shown mathematically as follows:

$$\sigma^{kl} = (\sigma^{kl})_{p\times q} \tag{6.6}$$

$$\sigma^{kl} = \sqrt{\frac{1}{p \times q}\sum_{i,j}\left(b_{ij}{}^{kl} - \overline{b^{kl}}\right)^2}$$

$$\overline{b^{kl}} = \frac{1}{p \times q} \sum_{i,j} {b_{ij}}^{kl} \qquad (6.7)$$

The transformed image consists of n blocks of different intensities. Figure 6.11 shows the result of this block processing for different block sizes. The reason behind using standard deviation will be explained as follows. Consider a block of the original image represented by the matrix B^{kl} . It is reasonable to assume that if the block is located in the region of interest its standard deviation will be higher than the case where it is located in the background. This is due to the fact that the variations in pixel intensities are higher in the ROI compared to the background. As a result, the blocks located inside the ROI are brighter as can be seen in Figure 6.11.

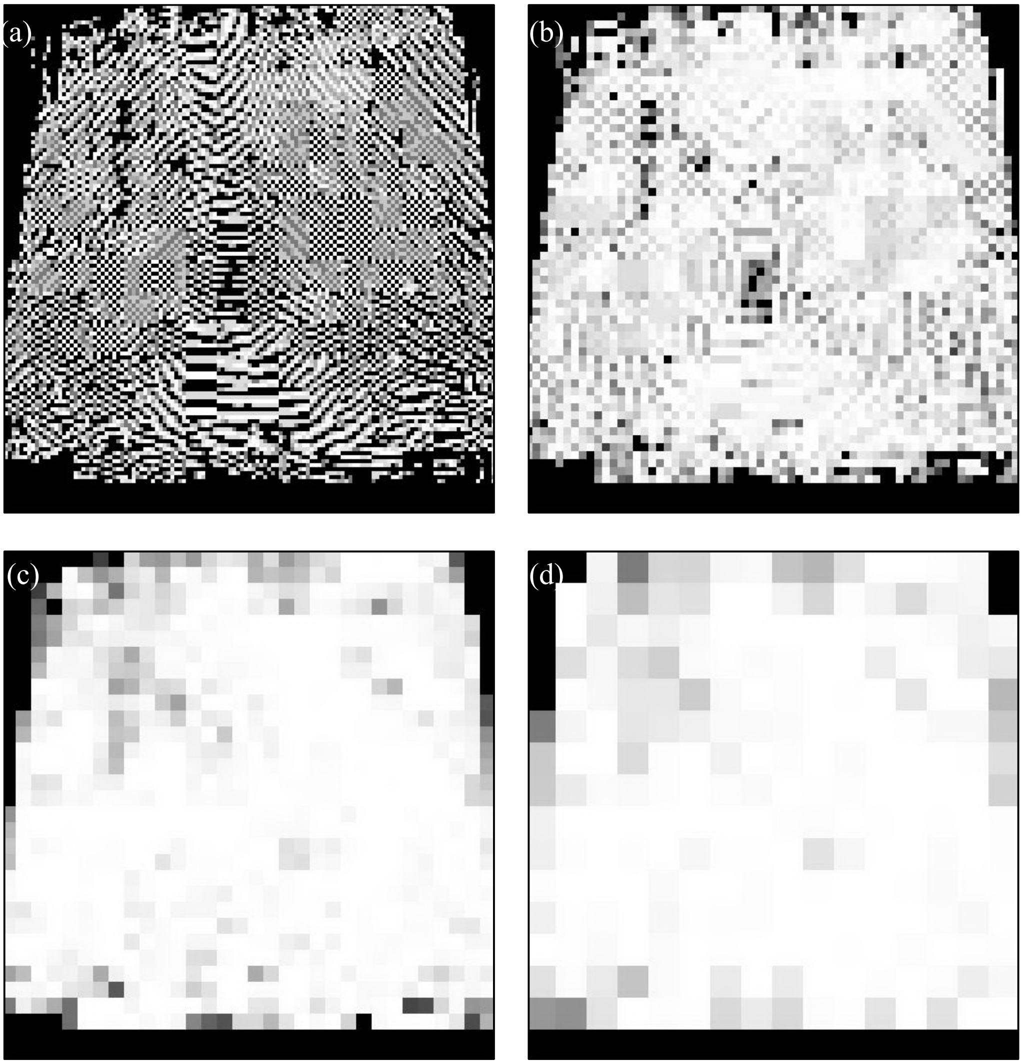


Figure 6.11: Transformed Fingerprint Image after Standard Deviation

a) 4×4 , (b) 8×8, (c) 16×16 and (d) 32×32

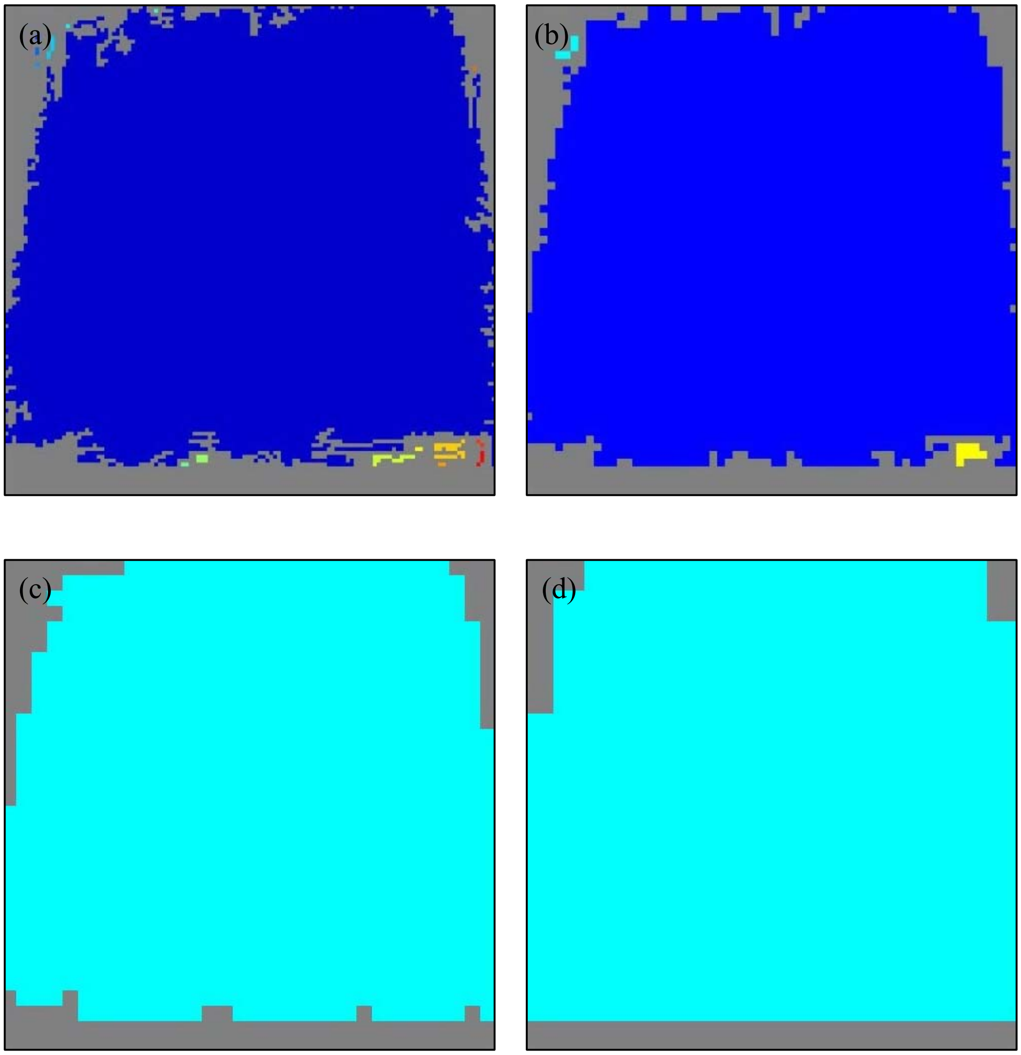


Figure 6.12: Boundaries after Standard Deviation
(a) 4×4 , (b) 8×8, (c) 16×16 (d) 32×32

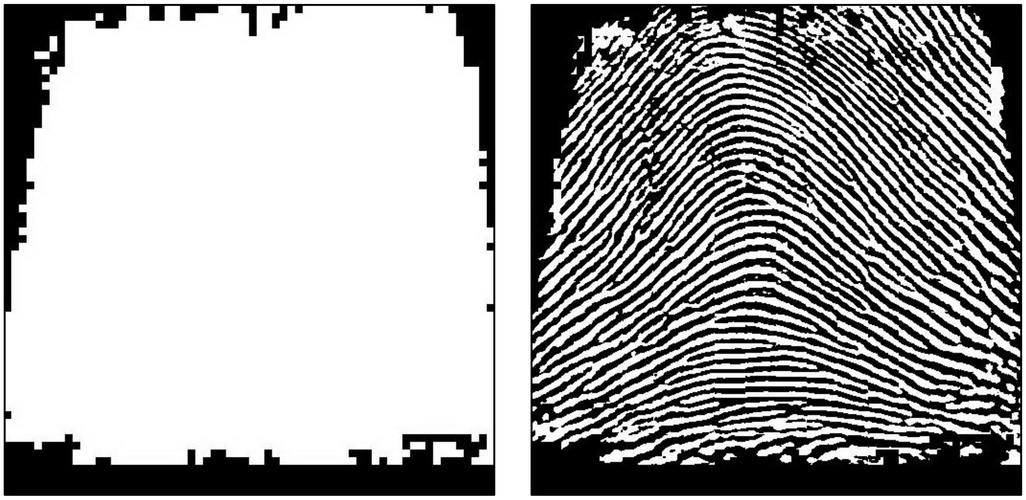


Figure 6.13: Left: Region of interest (ROI) and **Right**: ROI of fingerprint (sample4)

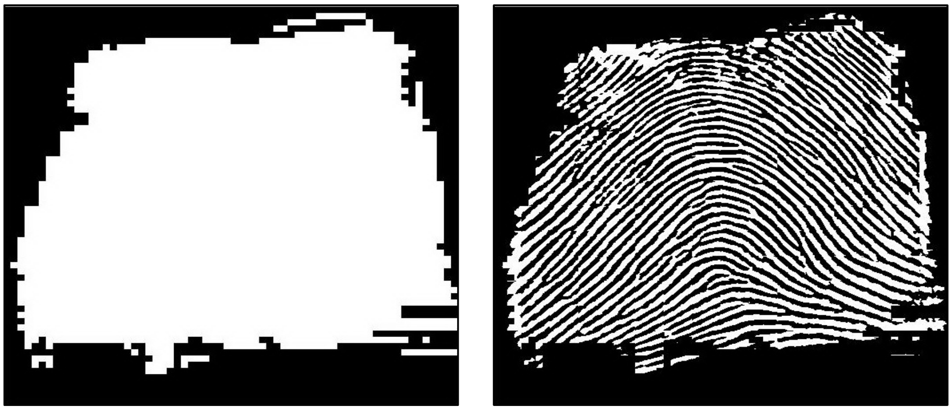


Figure 6.14: Left: Region of interest (ROI) and **Right**: ROI of fingerprint (sample3)

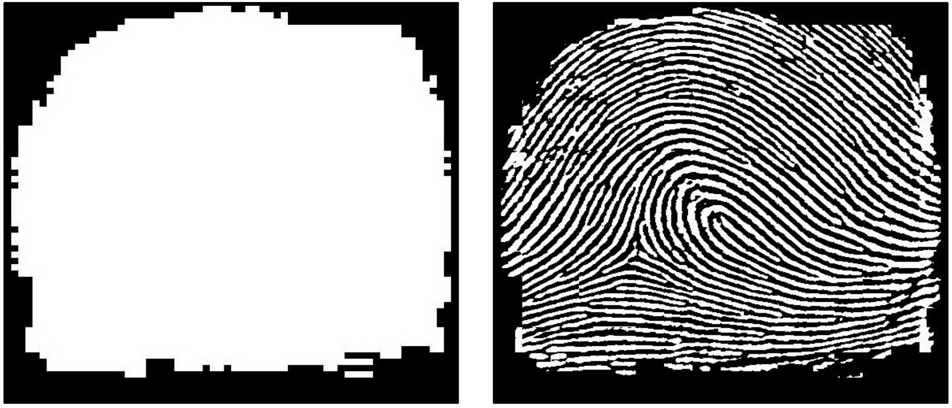


Figure 6.15: Left: Region of interest (ROI) and **Right**: ROI of fingerprint (sample2)

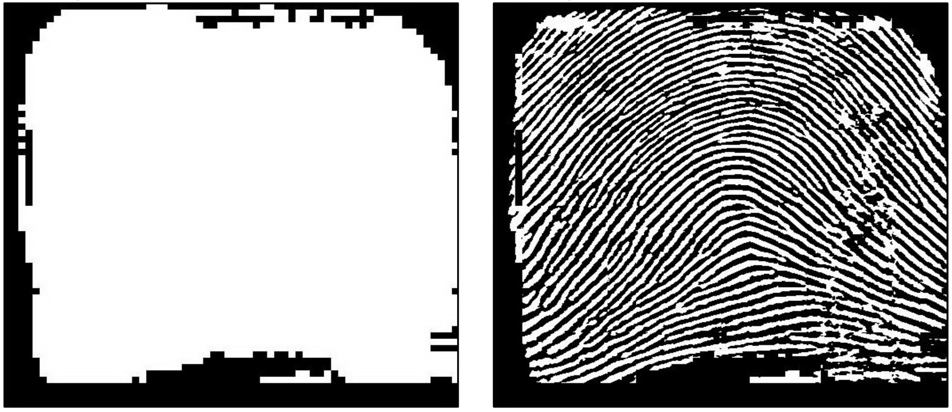


Figure 6.16: Left: Region of interest (ROI) and **Right**: ROI of fingerprint (sample1)

In order to remove the image background and obtain the ROI, each block σ^{kl} is examined against a threshold t value obtained by the Otsu optimum threshold method [217]. Elements of each matrix with higher value than the threshold are considered bright; otherwise, they are considered dark. In this way, the ROI is separated from the rest. As shown in Figure 6.12, matrices of different size result in different boundaries. As a result of numerical experiments, 8 × 8 matrices are selected and by superimposing this ROI on the binarized fingerprint, ROI of fingerprint images will be produced (Figure 6.13, 6.14, 6.15 and 6.16).

6.3.5 Thinning

Thinning is the last step of the fingerprint image enhancement before feature extraction, and it is used in order to clarify the endpoints and the bifurcations in each specific pixel, subject to the numbers of pixels belonging to these features in the original fingerprints. A good thinning method will reduce the width of the ridges down to a single-pixel while keeping connectivity and minimizing the number of false minutia as byproduct of this processing [26]. Generally, in order to eliminate the false minutia structures (e.g. bridges, holes, spurs, spikes and lonely points) that could appear when using thinning operation (Figure 6.17), the fingerprint images have to be filtered latter. For instance, in order to eliminate the spike that often appears on the thinned binary images, Ratha et al [146] implement an adaptive morphological "open" operator.

In this thesis an algorithm has been developed, which eliminates most of these false minutia structures in only one-step without any intermediate filtering. This is performed by using initially a sliding neighborhood processing and then thinning the result. Although, as it is considered by Ratha et al [146], the preprocessing stage does not eliminate all possible defects in the input gray scale fingerprint image (e.g. ridge breaks due to insufficient amount of ink and ridge cross connections due to over inking are not totally eliminated) and sometimes introduces some artifacts, which later lead to spurious features. Therefore, it might be necessary to employ post-processing stage in order to remove these artifacts (e.g. proposed heuristic rules by Ratha et al [146] to eliminate any remaining ridge breaks, spikes, and boundary effect).

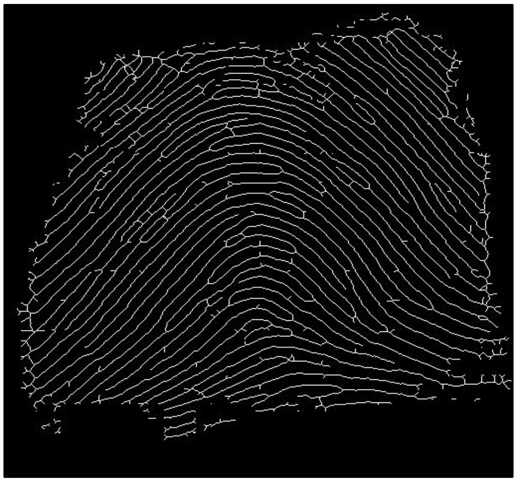


Figure 6.17: Affection of thinning without Sliding Neighborhood

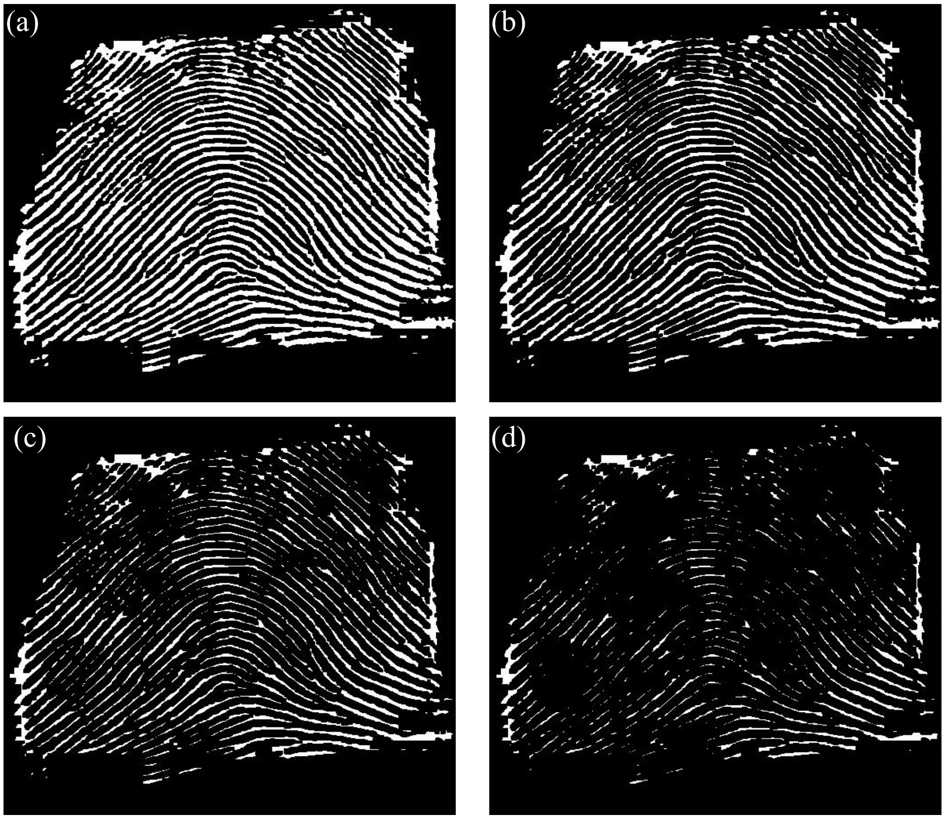


Figure 6.18: Fingerprint after sliding neighborhood a) 2×2, (b) 3×3, (c) 4×4and (d) 5×5

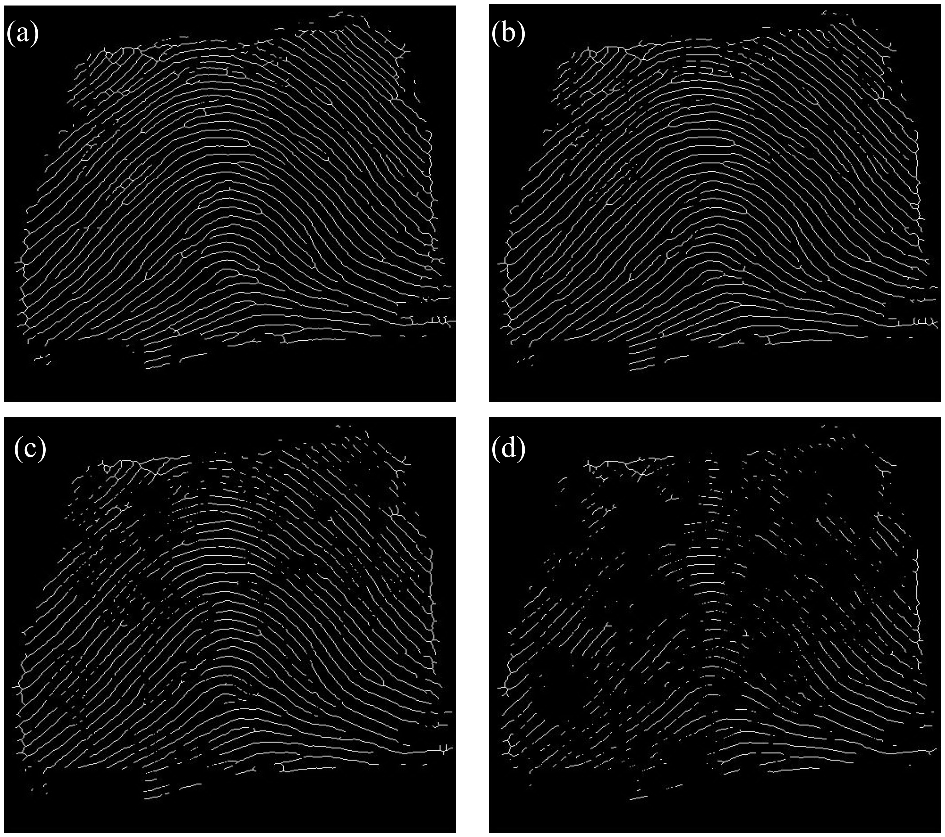


Figure 6.19: Fingerprint after thinning (a) 2×2, (b) 3×3, (c) 4×4 and (d) 5×5

A pixel's neighborhood is some set of pixels, defined by their locations relative to the center pixel and the analysis is performed on a pixel at a time. The value of any given pixel in the output image is determined by the application of an algorithm to the values of the corresponding input pixel's neighborhood. The neighborhood is a rectangular block that is slides in the same direction as you move from one element to the next in an image matrix.

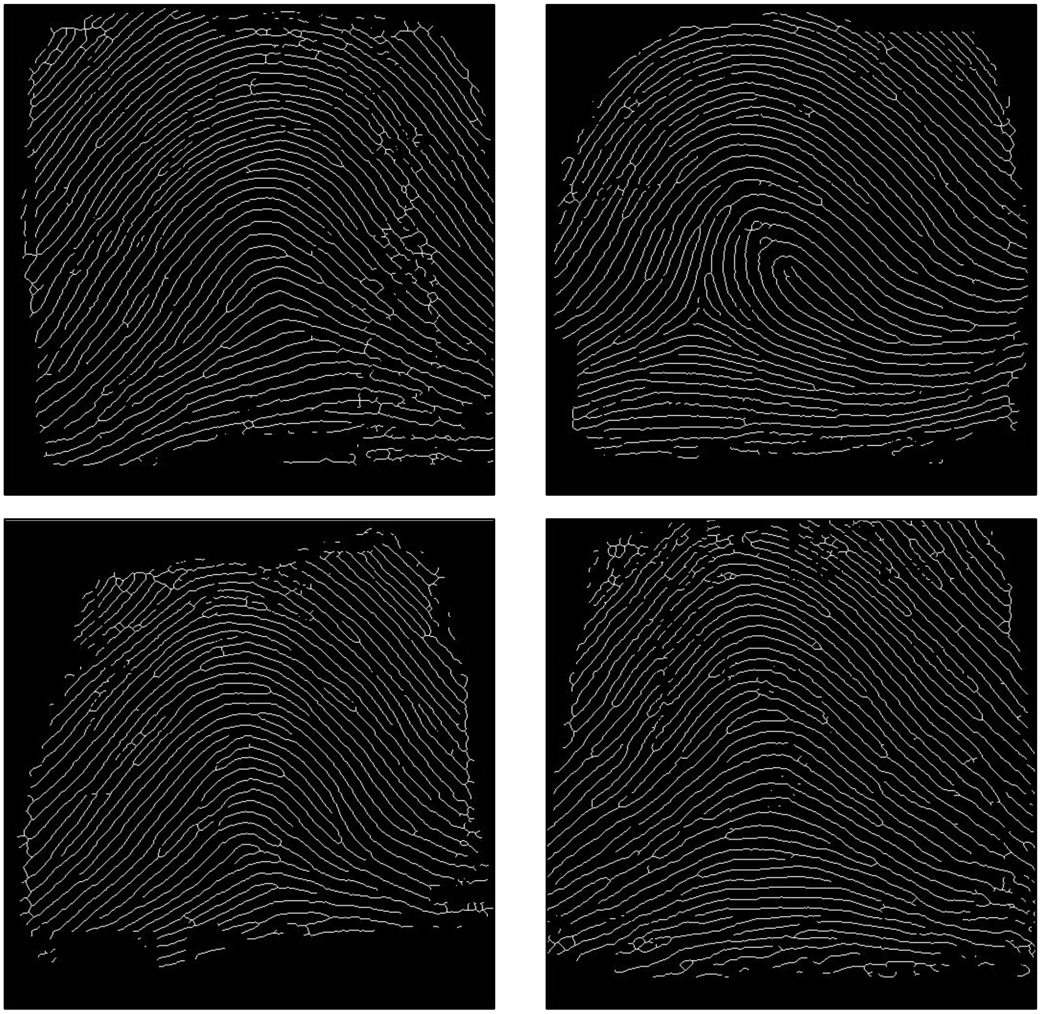


Figure 6.20: Fingerprint after thinning

Determining the Center Pixel is based on the odd or even number of rows and columns of neighborhood. If it both dimensions has an odd number, the center pixel is essentially in the center and if any of dimensions has an even number, the center pixel is just to the left or above center. For instance, the center pixel in a 2 × 2 neighborhood is the upper left one. Generally, the center pixel in any m × n neighborhood is mathematically shown by [99]:

$$\text{Floor}\ (([m\ n] + 1)/2) \tag{6.8}$$

As illustrated in Figure 6.18 and 6.19, the selection of different sets of blocks results in different outputs, and if the size of the block is bigger that 2×2, discontinuous ridges will be produced in the fingerprint image. Therefore, 2×2 set of matrices are applied in this step to avoid any discontinuous ridges (Figure 6.20). However, this algorithm has different effect on dissimilar fingerprint database depend on the width of the ridges and nature of the existing false minutia structures in the image. As it is explained earlier, the employed database in this thesis is considerably varying from those acquired by optical or solid state sensors, which are normally available in electronic devices.

6.3.6 Summary

Different methods in the public domain for fingerprint image enhancement have been reviewed, and a new methodology allowing superior performances is proposed. In order to avoid specific shortfalls of this process, the procedure follows first the application of CLAHE with Clip Limit in order to enhance the contrast of small tiles, to eliminate the artificially induced boundaries and to avoid over-saturation of the image specifically in homogeneous areas. In addition, a combination of filters in both domains, spatial and Fourier is used to obtain an appropriate enhanced image.

Some possible new developments have been carried out especially by applying the standard deviation analysis of the array to each distinct M × N blocks of image in order to remove the background and obtain the region of interest. The last phase of this new enhancement methodology is the application of the sliding neighborhood processing to obtain a thinned fingerprint image without any intermediate filtering and substantial reduction of the computational complexity. The analysis of its possible advantages is carried out through a simulated investigation.

6.4 Proposed Watermarking Algorithm:

In the previous Chapter, various watermarking techniques and possible domains in order to embed the watermark has been reviewed. As detailed, embedding the watermark in the transform domain is more robust as compared with spatial domain. Therefore, DWT, which is of latter type, is utilized to embed the watermark into the fingerprint image. This section focuses on the study of watermarking the fingerprint image as used in the proposed multibiometric cryptosystem in previous Chapter.

Methodology

Based on the proposed algorithm in Chapter 5, this section describes the methodology for performing the fingerprint watermarking with text. This algorithm is divided into two parts, watermark embedding and watermark extraction. In the watermark embedding stage, firstly, presented memorable word by the user is converted to the image. In a second step, a single-level two-dimensional wavelet (DWT2) is applied to the enhanced fingerprint image and transformed image of the text from prior step. This is to decompose both images into low-pass subband and high-pass subbands. Finally, after embedding watermark coefficients to the most significant coefficients at the low and high frequency bands of the discrete wavelet transform of an fingerprint image, watermarked fingerprint image has been reconstructed by using single-level inverse discrete two-dimensional wavelet transform (IDWT2). In the watermark extraction stage, the memorable word has been used to verify the integrity of the watermarked fingerprint image by the process of detection. Figures 6.21 and 6.22 illustrate the flowcharts of embedding and extraction respectively.

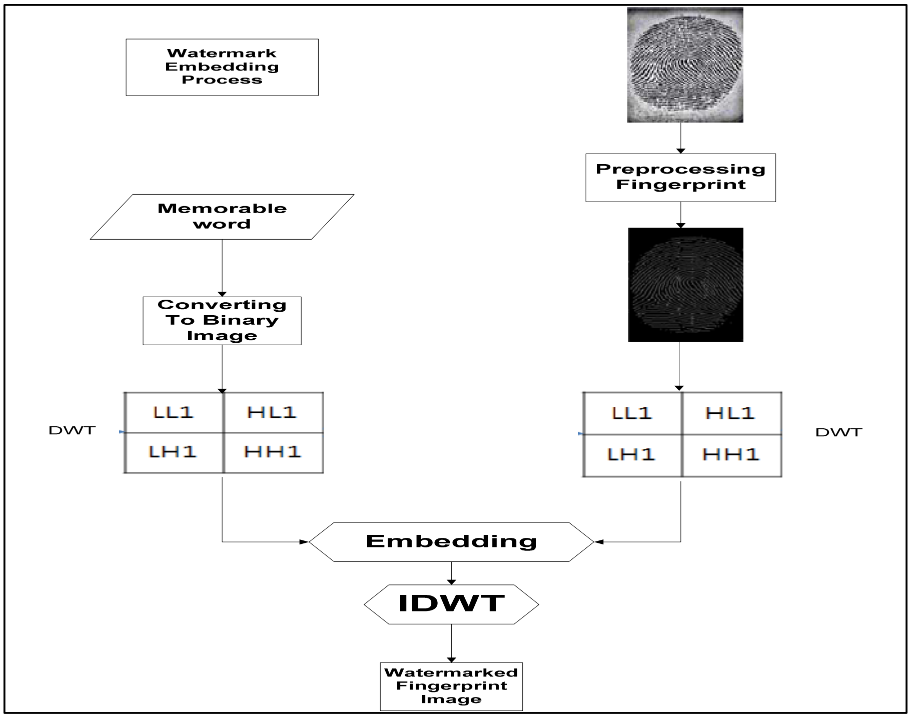

Watermark Embedding Process
Preprocessing Fingerprint
Memorable word
Converting To Binary Image
LL1
HL1
LH1
HH1
DWT
LL1
HL1
LH1
HH1
DWT
Embedding
IDWT
Watermarked Fingerprint Image

Figure 6.21: Watermark Embedding Process

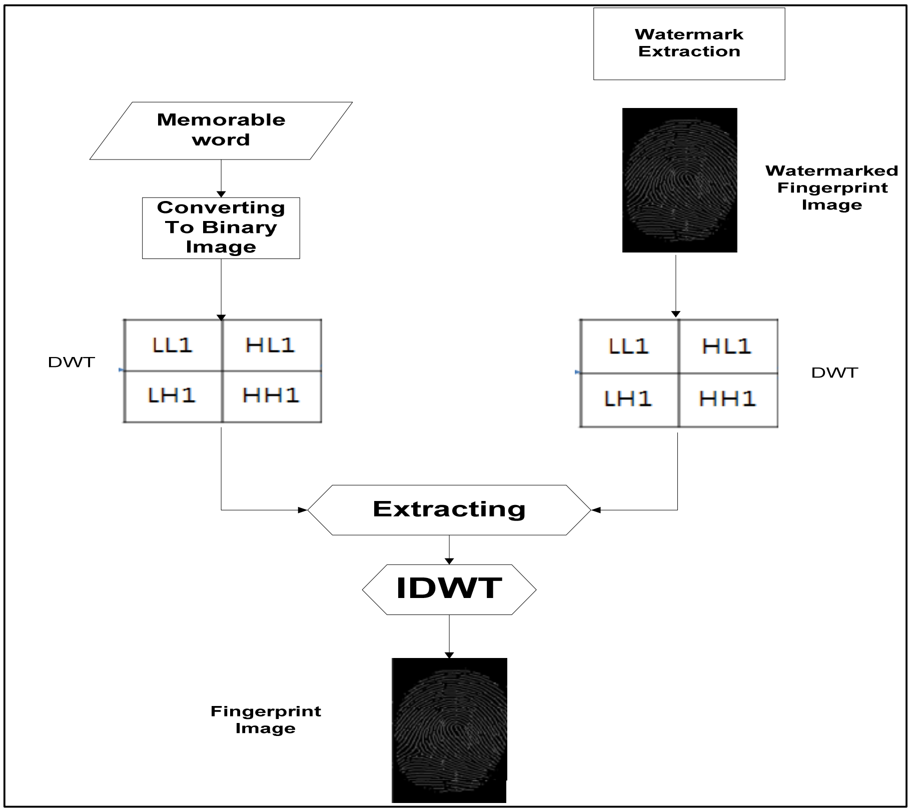


Figure 6.22: Watermark Extraction Process

The above approach is explained in more detail as follows:

A. Decomposition

As detailed in previous Chapter, watermark can be embedded in either the spatial domain or frequency. The watermark embedded in the frequency domain is more robust than in the spatial domain. As is explained by Mallat [218], a wavelet transform can be interpreted as decomposition into a set of frequency bands having the same bandwidth on a logarithmic scale. It comes with superior advantages and hence, discrete wavelet transform (DWT) is preferred in this work at decomposition stage. As is shown in Figure 6.23, firstly, input signal is computed by a successive low-pass decomposition (Lo_D) and high-pass (Hi_D). Two-dimensional DWT leads to a decomposition of approximation coefficients at level j in four components. This encompasses the approximation at level j + 1, which is produced from pure low-pass together with the decompositions produced from high-pass in three orientations (horizontal, vertical, and diagonal). The following chart describes the basic decomposition steps for fingerprint and watermark images:

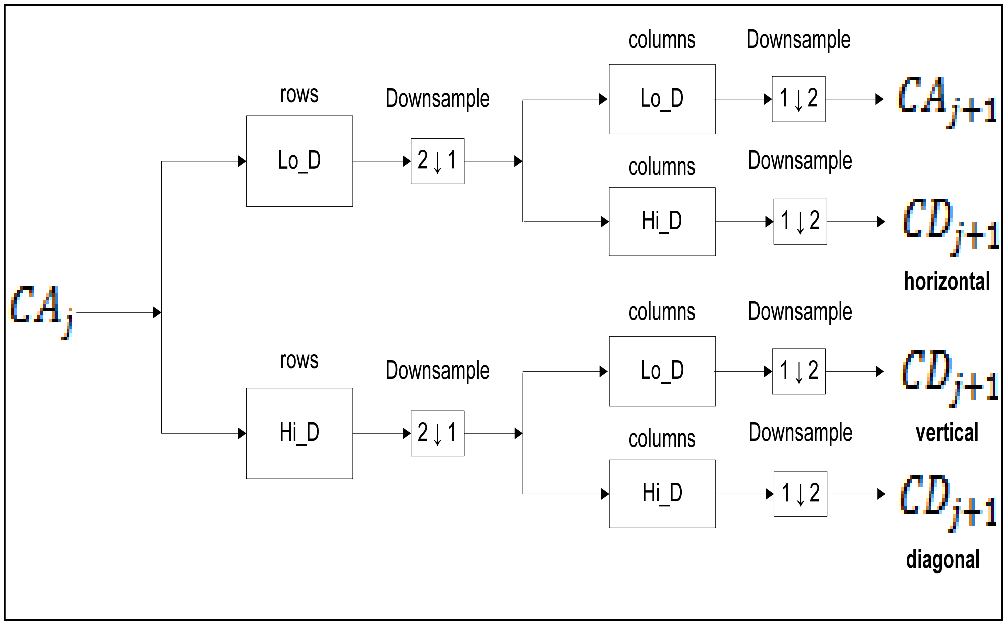


Figure 6.23: Decomposition steps of two-dimensional DWT [99]

Where downsample columns and rows keep the even indexed columns, and even indexed rows respectively. In addition, Lo_D and Hi_D convolve at rows with filter X, the rows of the entry, which is set to "Harr" filter in this experiment, and at columns, with filter x, the columns of the entry.

Computing the approximation coefficient (cA) of the watermarked fingerprint image is mathematically shown below [201, 219]:

$$I'_W = I_W\,(1+ \alpha\, W_W\,) \tag{6.9}$$

Where I'_W represents the cA of the watermarked fingerprint image I, I_W is the approximation coefficient (cA) of the fingerprint image and W_W is the (cA) of the watermark W. As expleained above these two coefficient (W_W and I_W) can be produced by using the DWT low-pass decomposition. In addition, there are three detailed information coefficients (cH, cV, and cD) of the watermarked fingerprint image I'_W that are embedded in the higher frequency components of the image. Computing these coefficients is based on the following equation:

$$I'_W = I_W + \beta\, W_W \tag{6.10}$$

Where, I_W is the coefficient (cH, cV, or cD) of the fingerprint image I and W_W is the corresponding coefficient of the watermark image W. As explained previously, these three coefficients can be produced from the DWT high-pass decompositions in three orientations (horizontal, vertical, and diagonal).

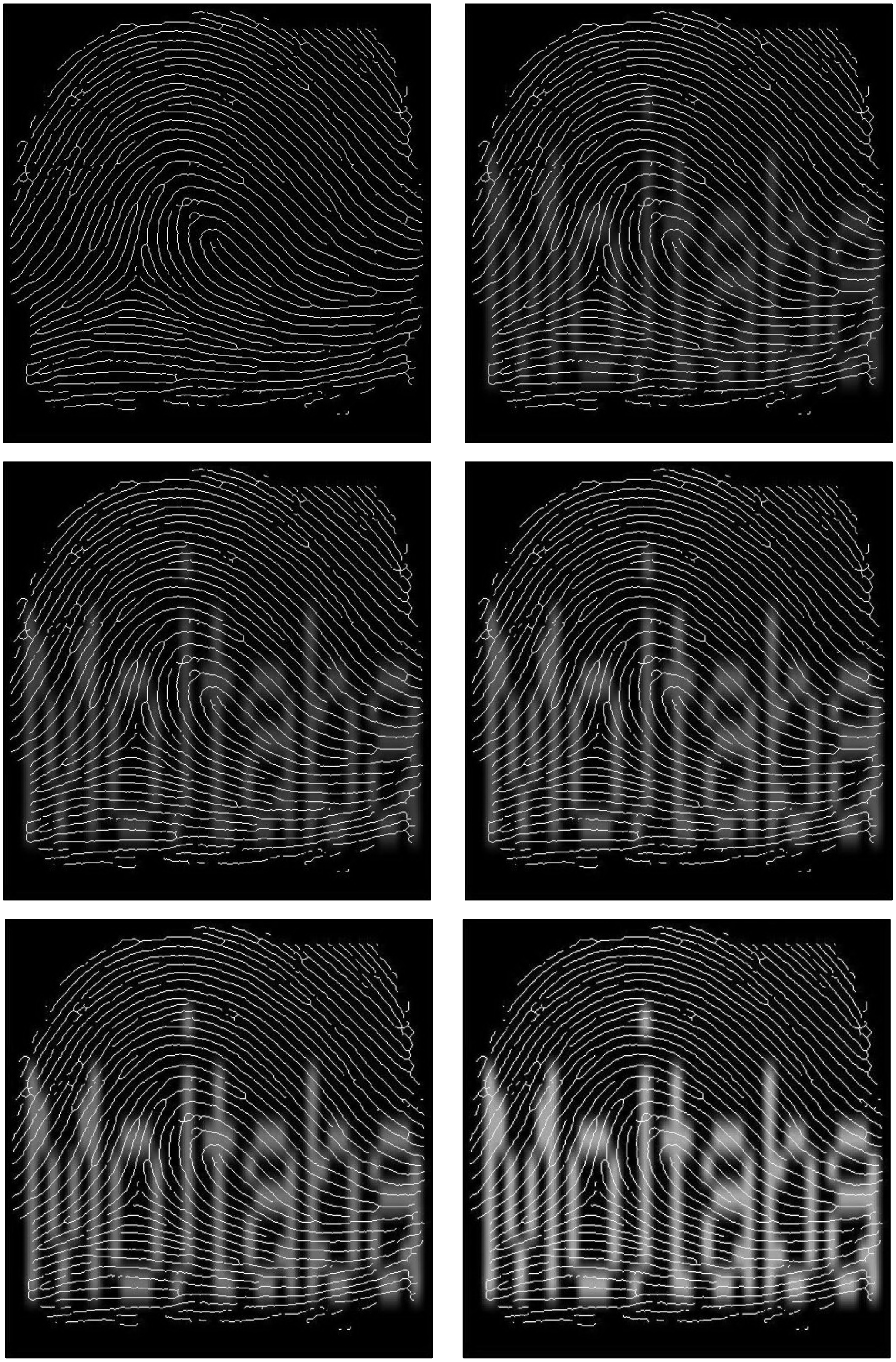


Figure 6.24: Invisibility of the watermark Image against Various value of α and β

As detailed by Taskovski et al. [219] and Lam et al. [201], human eyes are very sensitive to changes from low-pass decomposition but not sensitive to small changes in the edges and the textures which are embedded in the higher frequency components of the image. This is due to sensitivity of human eyes to small changes in smooth part of the image that is represented by low-resolution representation in which most of the information in image is located. Therefore, invisibility of the watermark is kept by selecting a smaller value of α, and a larger value of β. This invisibility is depicted in Figure 6.24.

B. Embedding a Watermark Image into the Fingerprint Image

Once these coefficients are obtained for both fingerprint and watermark images, the watermark image ones can be embedded into those of fingerprint. Firstly, fingerprint wavelet coefficients (I_W) and those from watermarked (W_W) are generated by a single-level two-dimensional wavelet transformation. Secondly, in order to obtain the approximation coefficient (cA) and three coefficients (cH, cV, and cD) for the watermarked fingerprint image, the equation 6.9 and 6.10 are being applied.

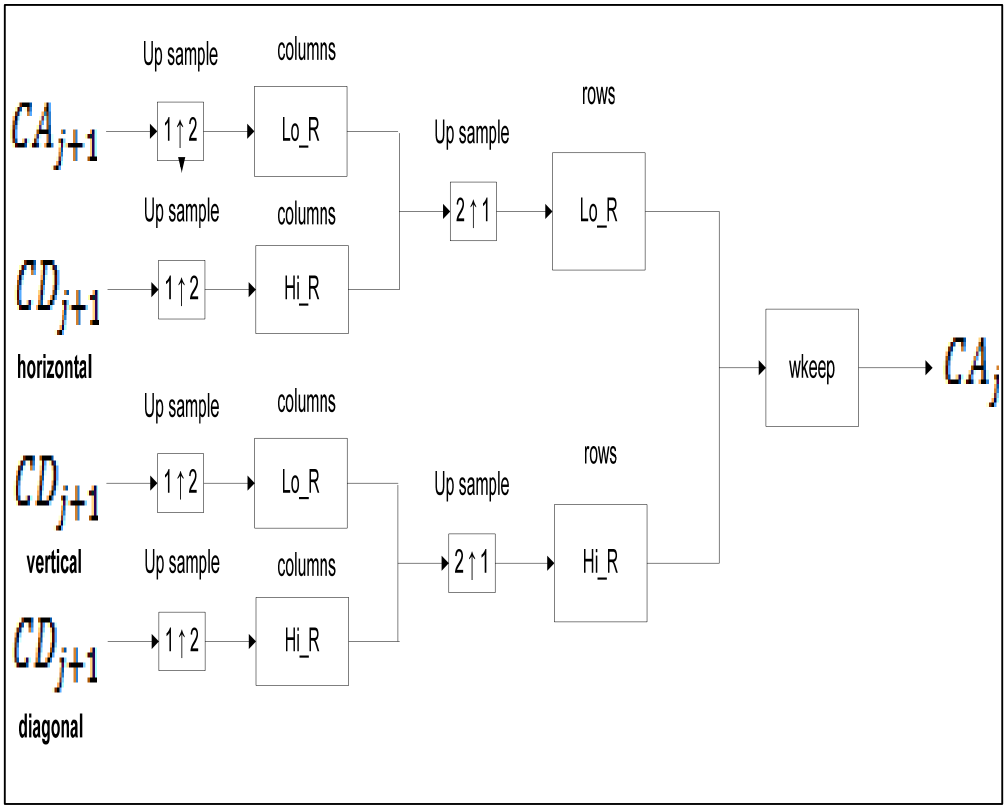


Figure 6.25: Reconstruction step of Two-Dimensional IDWT [99]

Furthermore, in order to reconstruct the watermarked fingerprint image, inverse Discrete Wavelet Transformation (IDWT) is applied to these coefficients, as is being discussed below.

C. Image Reconstruction

In this step, after embedding the watermark image coefficients, IDWT is applied to the watermarked fingerprint coefficients in order to achieve the final secure watermarked fingerprint image. Those decomposed components can then be assembled back into the original fingerprint image. This process is called reconstruction, or synthesis, and mathematical manipulation that affects synthesis is called the inverse discrete wavelet transform. Therefore, to reconstruct the watermarked fingerprint from the wavelet coefficients, IDWT2 has been performed. Figure 6.25 illustrates above, where upsample columns and rows insert zeros at odd-indexed columns and rows respectively. In addition, Lo_R and Hi_R at rows convolve with filter X, the rows of the entry, which is set to "Harr" filter in this experiment, while at columns; convolve with filter x the columns of the entry.

D. Retrieving an Embedded Watermark

In the previous steps, the discrete wavelet transform has been used to decompose images and then watermark image coefficients are embedded into the fingerprint image coefficients and assembled back into the original image by inverse discrete wavelet transform. Generally, the task of decoding the watermarked image is to verify the presence of the watermark image. However, because of using fingerprint image as host image, the fingerprint image should be unique; otherwise, it will cause the false acceptance for the imposter. This is due to the fact that fingerprint technology is unable to obtain the identical image and feature, each and every time scanning and analysis is done. Therefore, in order to address the problem of indistinctness in a fingerprint image when presented at different times, watermark image has been used to extract the fingerprint image. Finally, this extracted fingerprint image can be matched against the one that is stored in the database to verify the integrity of the claimed user. In addition, presence of the memorable word can be verified during this process. Figures 6.26 illustrates the original fingerprint and watermarked fingerprint images, extracted watermark and extracted fingerprint images.

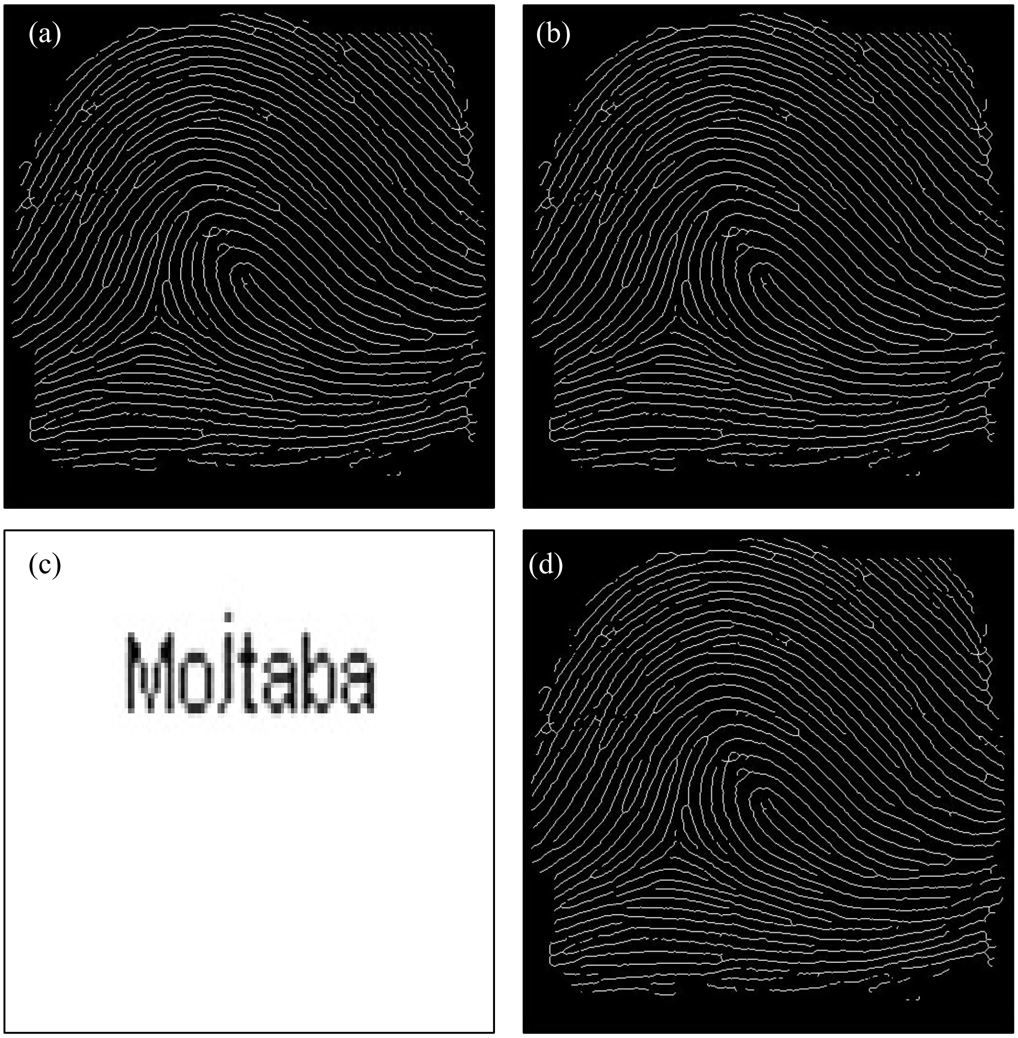


Figure 6.26: (a) Original Fingerprint (b) Watermarked Fingerprint image. (c) Watermark image and (d) Extracted Fingerprint image

6.4.1 Summary:

This section has been introduced and developed fingerprint watermarking technique based on the proposed multibiometric system in the previous Chapter. This scheme encompassed five-step procedure; novel three-step procedure for the fingerprint image enhancement together with two step embedding and extracting the watermark into the enhanced fingerprint image.

As indicated in this Chapter, feature extraction in fingerprint minutiae-based matching is performed by two-dimensional storage of sets of points extracted from two fingerprints. The performance of feature extraction algorithms highly depend on the quality of input fingerprint images and usually, to improve the quality of output image, an intermediate step of fingerprint image enhancement is required. In addition, there are several advantages to embedding the watermarked data into the enhanced fingerprint image, which is detailed in subsection 6.2.1. Therefore, section 6.3 introduces a novel method for enhancement of fingerprint image by means of eliminating the artificial induced boundaries, precise background omission; avoid oversaturation of the image in homogeneous areas, with no intermediate filtering and computational complexity. In order to eliminate the induced boundaries, CLAHE (contrast limited adaptive histogram equalization) technique is employed. 'Clip Limit' is then applied in order to avoid oversaturation of the image in homogeneous areas. Subsequently, the image is disintegrated into an array of distinct blocks and the discrimination of the blocks is obtained by computing the standard deviation of the matrix elements to remove the image background. Once the boundary for the region of interest is obtained, a new modified thinning method using slide neighborhood processing is applied to clarify the endpoints and the bifurcations in each specific pixel. In contrast to other thinning algorithm, proposed approach does not require any intermediate filtering and substantial reduction of the computational complexity. The analysis of proposed fingerprint image enhancement and its possible advantages is carried out through a simulated investigation in the section.

Finally, in section 6.4 watermarking technique has been introduced and DWT (Discrete Wavelet Transform) shown to be satisfying the need for the protection of fingerprint image. The purpose of this is to develop a simple and accurate method to obtain high level of confidence fingerprint identification and watermarking technique through a simulated investigation. Therefore, based on the proposed methodologies in previous Chapter embedding the watermark message into the fingerprint image has been design and developed. This scheme encompasses two-phases including converting the memorable word into image and embedding this watermark into the enhanced fingerprint image as first step and then verify the integrity of the claimed user by extracting this watermark from the watermarked fingerprint image. As it is shown in Figure 6.26, this image has been embedded into and extracted successfully from enhanced fingerprint image without any effect on appearance of the watermarked fingerprint and extracted fingerprint image. Furthermore, there is possibility of using different letter of the memorable word to make each different implementation unique. Therefore, breaking one version of the watermarked image will not necessarily compromise another one.

6.5 Applying Proposed Algorithm to Wireless Communication

In this thesis, unimodal and multimodal biometric were reviewed in theory and experiments in an attempt to find the optimum type of biometric traits with better throughput performance and accuracy in wireless communication systems. In Chapter 2, 3 and 5, literature review was provided with the aim of finding the biometric solution to protect wireless communication and finally linking appropriate biometric algorithms and techniques together. An algorithm to approach this goal is watermarking the fingerprint with the same text as a text-dependent voice recognition that in turn can be combined and embedded to form a cancelable multibiometric recognition. Such a method comes with the capability of taking advantage of both cancelable biometric and multibiometric. General techniques to build cancelable fingerprint and speaker verification have been discussed in Chapter 3 and 5. In addition, an appropriate fingerprint image enhancement and watermarking technique has been proposed and simulated in section 6.3 and 6.4 together with the voice recognition algorithm in Chapter 3. As discussed in previous Chapters, these biometric authentication techniques are able to cover the limitations of information security objectives in wireless communications. In spite of these advantages, providing the real-time authentication together with decreasing the bandwidth consumption in many wireless applications remains a challenging research issue. In this section, an attempt has been made to assess and evaluate the performance of proposed system. This encompasses the investigations and discussions on such fundamental issues, the implementation of this system and its effect on the relative performance over various wireless communication systems (WiMAX, Wi-Fi and 3G).

Methodology

The five-step challenge/response process (Figure 6.27) has been developed based on the described proposed methodologies in Chapter 3 and 5. As detailed in Chapter 5, in order to prove the validity of the presented fingerprint by the claimed user, the server should recognize the fingerprint and send a challenge in the form of a word or phrase to the user. Finally, the server accepts the user as genuine only by receiving the secure response, which is pronouncing the challenge (voiceprint). This form of implementing multibiometric in wireless communication can address the identified limitations of fingerprint identification by distinguishing the claimed person and true owner of the fingerprint though the user's voiceprint. There are two initial steps involved prior to engaging the user with challenge and awaiting user's response.

Establishing Security Capability

This phase is based on initiating the connection between user and server to have access to the service, device, or data. The user of a wireless device (e.g. PDA or Laptop) sends the request to server and asks for access to the data or facility.

Processing Request

The server begins this phase by sending User ID request (Fingerprint), in order to start authentication of the user.

Phase 1: Presenting the User Fingerprint and Memorable Word

Upon receipt of User ID requested by server, the user starts identification process by presenting his/her own fingerprint and memorable word as the User ID requested by server. The identification depends solely on fingerprints to authenticate the identity claimed by an individual who requires the access.

Phase 2: Authenticating the User and Retrieving the Challenge

Once the user's watermarked fingerprint is received, fingerprint identification will be implemented by the server. If the user is accepted by identification process, a related challenge in the form of word, or phrase will be retrieved from the watermarked fingerprint in database in order to verify the integrity of presented fingerprint.

Phase 3: Responding to the Challenge by Voiceprint

In this phase, the user responds to the requested challenge by pronouncing the phrase or word and sending it to sever as voiceprint. This response to the requested challenge can be used to verify either the claimed user is genuine or imposter, by verifying the liveness of presented fingerprint and avoiding any possible replay or Trojan horse attack. As it is detailed in Chapter 3, it is based on sending voice features (cepstral coefficients) instead of raw sample through the proposed system, therefore reducing the transmission time and dependency of the data on the quality of microphone or communication channel. In addition, this scheme has the benefit of the transcoding as well as no packet being lost. One point should be noted here is the high quality of acquired speech due to the controlled condition.

Phase 4: Authenticating the Response

Upon receipt of user response, the server will typically authenticate the received response from the user through the voice recognition algorithm. This is to validate the legitimacy of the user in order to have access to the service or data.

Phase 5: Accepting or Rejecting the User

This phase completes the setting up of a protected connection between the user of wireless device and remote server by either providing permission to have access or denying the user.

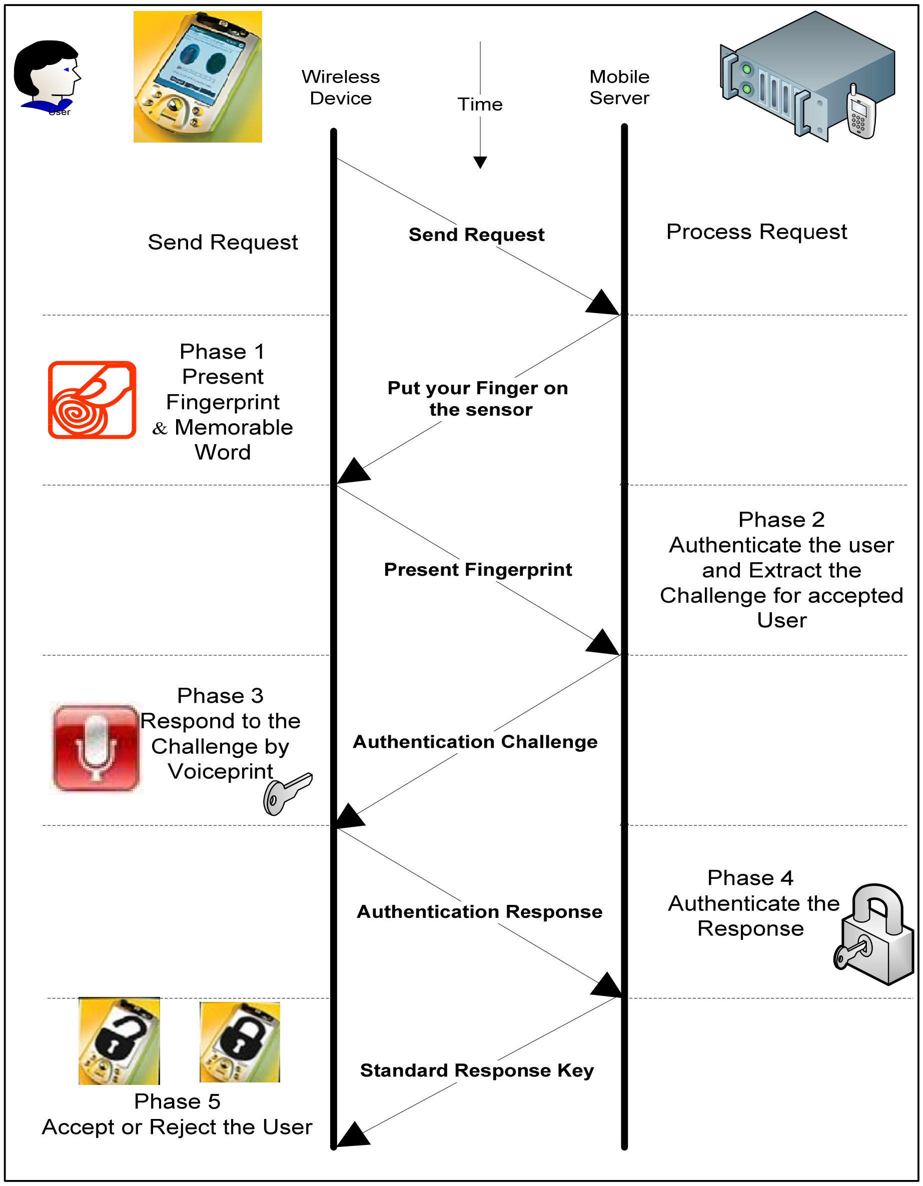

User
Wireless Device
Time
Mobile Server
Send Request
Send Request
Process Request
Phase 1 Present Fingerprint & Memorable Word
Put your Finger on the sensor
Phase 2 Authenticate the user and Extract the Challenge for accepted User
Present Fingerprint
Phase 3 Respond to the Challenge by Voiceprint
Authentication Challenge
Phase 4 Authenticate the Response
Authentication Response
Standard Response Key
Phase 5 Accept or Reject the User

Figure 6.27: Schematic Challenge/Response for Implementing Multibiometric in Wireless Communication

6.6 Simulation of Projected System in Wireless Communication

In the previous section, an appropriate architecture was offered to provide a multibiometric solution over wireless communication. This section simulates a projected model over three wireless technologies, WiMAX, Wi-Fi and 3G. After such a model is being simulated, the results will be presented to check the effect of these networks upon the performance of the proposed system in terms of speed, reliability, and the quality of service. Therefore, the five-step challenge/response process will be accomplished over WiMAX, Wi-Fi and 3G, and the most important parameters including corresponding delay, throughput, and jitter will be analyzed. Finally, these parameters can be further studied by investigating their effects on the proposed multibiometric applications in wireless communication. This is to clarify how wireless communication systems can benefit through this system.

Simulation Software and Environment:

In order to measure QoS (delay, throughput, and jitter), the Wireshark software [209] has been used which is a network packet analyzer. Wireshark will try to capture network packets and display packet data as detailed as possible. In addition, the experimental test has been carried out under Windows XP Professional on two Pentium (R) 4 notebooks, CPU 2.80 GHz as client and server. The delay (D) was monitored for every single packet and different sizes of watermarked fingerprints were tested using the PING utility tool based on the following equation:

$$\mathbf{D} = \frac{[(\mathbf{Rc}-\mathbf{Ts}) + (\mathbf{Rs}-\mathbf{Tc})]}{2} \qquad (6.13)$$

Where Ts is the time at which the packet was sent from the server. The time at which the packet was received by the client on the other hand is Rc. Similarly, Tc is the time at which the packet was sent from the client and the time at which the packet was received by the server is Rs. In addition, in order to experience the worst case of voice features in terms of size, maximum packet size of this feature has been utilized (126 KB). The tests for every packet size were performed four times, in different periods of a day. Every single packet size was tested 20 times in a single period of a day, and its average was calculated. The second parameter, jitter was monitored automatically on both client and server sides based on the following equations:

$$\text{Net Jitter} = 1/2 \sum_{n=0}^{N} \frac{\mathrm{Ts}_{\mathrm{n+1}} - \mathrm{Ts}_{\mathrm{n}}}{\mathrm{N}-1} + \frac{\mathrm{Tc}_{\mathrm{n+1}} - \mathrm{Tc}_{\mathrm{n}}}{\mathrm{N}-1} \qquad (6.14)$$

Where N and Ts_{n} are total number of packets and the time at which the packet (n) is received at the server respectively. As detailed in Chapter 5, watermark fingerprint and voice features will be sent instead of sending the raw voice file in order to avoid packets being lost. In spite of the fact that TCP can address the packet loss issue by retransmitting the missing packets, it can decrease the throughput of the connection. Therefore, these throughputs were measured automatically using Wireshark. The throughput at the client (uplink throughput) was measured when the server was sending and similarly, the throughput at the server (downlink throughput) was measured when the client was sending. The test was carried out around four to five times in order to calculate the average throughput for every individual file size. Simulation begins by sending the eight various sizes of fingerprint as phase one of proposed system in which the smallest, medium, and the largest sizes of data have been selected. The packets then are delivered through the three selected wireless technologies (WiMAX, Wi-Fi, and 3G) in order to measure QoS (delay, throughput, and jitter). The same process is carried out for the largest voice packet size. The Matlab codes employed in voice feature (cepstral coefficients) extraction have been provided for public use [61]. After the simulation, the results can be extracted from the measured parameters (delay, throughput, and jitter). The parameters here can be varied over the different wireless technologies. Finally, with the parameters being varied and under different technologies, the results can be evaluated.

6.6.1 Delay, Throughput, and Jitter for Fingerprint in Different Wireless Technologies:

The experiment was carried out by connecting the system to a hub and configuring its respective IPs. The substation was connected to a computer and was treated as a client. The base station was connected to another system and treated as a server. The readings for delay were noted initially at 5% bandwidth. To enable monitoring of delay over small packet sizes, the bandwidth was reduced to 1%. Ping application did not react to 1% bandwidth since the packets were damaged and hence the bandwidth was set to 3%. In addition, the Wi-Fi network at Brunel University and T-Mobile 3G-network card has been used for this simulation. The computer connected with the network card was treated as the server and another as client. Tables 6.1, 6.2, and 6.3 depict the average delay, throughput and jitter for every corresponding fingerprint packet respectively in WiMAX, Wi-Fi and 3G networks. The delay for every single network varies which shows the speed, external interference, and performances of every single network. As is shown in these three tables, the maximum delay, throughput, and jitter are 18.19, 507and 1.84 respectively in WiMAX, 82.44, 445 and 3.79 in Wi-Fi and 284.29, 129 and 12.64 in 3G networks.

FILE SIZE (KB)	WiMAX							
	54	59	72	150	256	364	482	570
Delay(ms)	14.4	14.52	18.12	16.11	17.19	12.65	18.19	17.54
Throughput (kbps)	502	502	501	507	504	501	502	504
Jitter(ms)	1.76	0.89	1.84	1.92	1.21	0.94	1.14	1.17

Table 6.1: Delay, Throughput, and Jitter for WiMAX

FILE SIZE (KB)	Wi-Fi							
	54	59	72	150	256	364	482	570
Delay(ms)	80.24	81.39	80.91	81.27	80.63	82.44	81.42	81.18
Throughput (kbps)	346	354	402	296	336	445	339	375
Jitter(ms)	2.17	3.79	3.25	2.36	2.76	1.92	1.21	2.25

Table 6.2: Delay, Throughput, and Jitter for Wi-Fi

FILE SIZE (KB)	3G							
	54	59	72	150	256	364	482	570
Delay(ms)	161.32	162.26	164.42	166.17	216.2	227.37	238.47	284.29
Throughput (kbps)	114	119	121	113	129	134	116	118
Jitter(ms)	10.54	9.65	10.73	12.64	10.31	11.54	12.52	11.86

Table 6.3: Delay, Throughput, and Jitter for 3G

6.6.2 Delay, Throughput, and Jitter for Voice Features in Different Wireless Technologies:

The table 6.4 shows the delay comparison for different sizes of voice features for all the three technologies WiMAX, Wi-Fi and 3G. The delay for all the three technologies clearly explains the performance of each technology. The delay was monitored for every single packet size and tabulated as shown below. In addition, table 6.5 illustrates the average delay, throughput, and jitter for the largest voice feature in WiMAX, Wi-Fi and 3G networks.

Wireless Technology	FILE SIZE (KB)							
	27	48	54	67	89	93	108	126
WiMAX (ms)	10.54	11.89	12.97	11.21	12.11	13.32	14.74	12.64
Wi-Fi (ms)	71.24	71.39	72.99	71.2	71.26	72.4	89.1	71.32
3G (ms)	101.1	108.3	118.9	119.6	124.43	129.3	135.41	141.17

Table 6.4: Delay Comparison for Voice Features in WiMAX, Wi-Fi and 3G

	Maximum voice feature size (126KB)		
	WiMAX	Wi-Fi	3G
Delay(ms)	12.64	71.32	141.17
Throughput (kbps)	596	342	146
Jitter(ms)	2.2	2.8	11.18

Table 6.5: Delay, Throughput, and Jitter of largest Voice Feature for Different Technologies

6.6.3 Analysis

As discussed in the literature review, WiMAX technology proved to be the quickest with high performance to transfer biometric data over the network due to the shortest delay as compared to the other networks (Wi-Fi and 3G). In addition, though different sizes of packets have been sent, the network delay always remains just about constant in WiMAX and Wi-Fi. However, the measured throughput varies for each technology and this is due to the experiments being carried out in different times, i.e. peak and off-peak. The jitters of all the three technologies did vary drastically from one another.

Obviously, specific requirements for any biometric system depend on the scenario and its requirements. To the best of our knowledge, there is no set standard for applying biometrics over internet or wireless communication, unless for voice and video. Latter addressed by ITU (International Telecommunication Union), Cisco[38] measures standard requirement for QoS parameter (150 ms is defined as acceptable delay, higher than 400ms is unacceptable and between these values user should be aware of quality issues, acceptable jitter is 30ms, and the guaranteed bandwidth for the video should be at least 1.2 times the actual throughput). Therefore, if guaranteed bandwidth is accepted for the voice and video, it is accepted in this algorithm (fingerprint and voice features) due to the less throughput requirement. There is however no restrictions on the proposed challenge/response algorithm in terms of delay, jitter, and throughput except in cases that requires verifying identities in real-time or near real-time delivery (no appreciable time delay). The Figures 6.28 and 6.29 show the delay comparison of different technologies with watermarked fingerprints and voice features differing sizably for WiMAX, Wi-Fi and 3G. The delays for all the three technologies clearly explain the performance of each technology. The delay does not increase proportionally as the file size increases in Wi-Fi and WiMAX, due to the background traffic in the network. However, maximum delay in the worst case, faced in 3G network, was 284.29 ms for fingerprint and 141.17 ms for voice feature, which is acceptable even in the real time communication. It should be noted that the main factors that were involved in delay encompass limited bandwidth of tested 3G network (150 kbps), signal variations, and background traffic. Therefore, in the case of real-time requirements and limited bandwidth in some environment (e.g. aircraft), either increasing the bandwidth or designating the special communication without any background traffic can be possible solutions. As an alternative solution to save the bandwidth in wireless channel, some effective compression techniques with small acceptable loss like Wavelet Scalar Quantization (WSQ) can be utilized for fingerprints. Although the jitters of all the three technologies vary drastically from each other, they are still all considered within the accepted range for every single network.

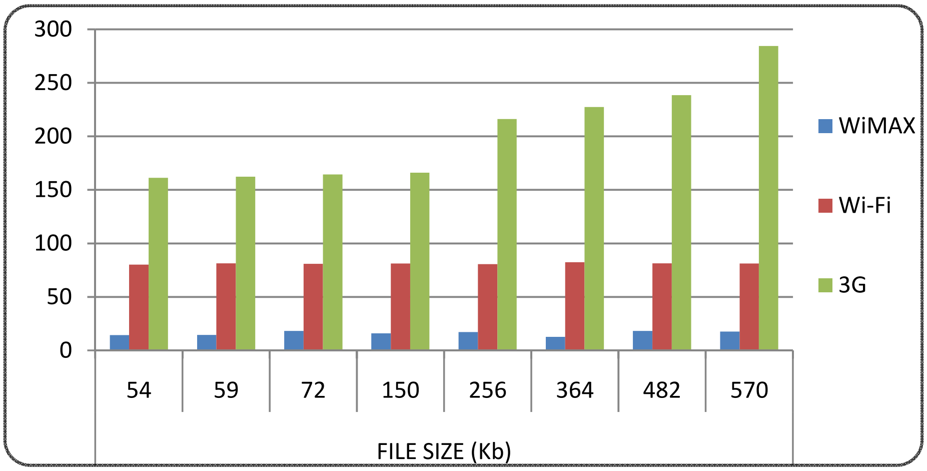


Figure 6.28: Delay Comparison for Different Size of Watermarked Fingerprint over Different Technologies

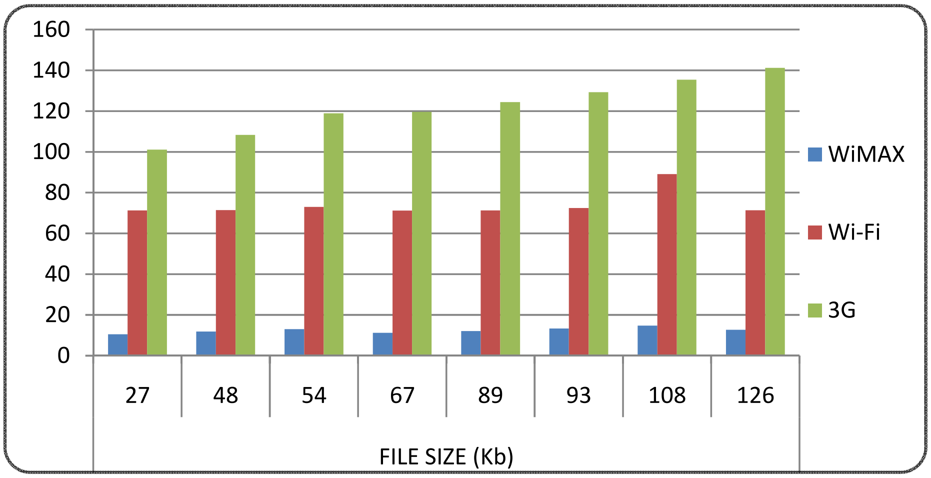


Figure 6.29: Delay Comparison for Different Size of Voice Features over Different Technologies

6.7 Summary:

In this thesis, a novel multibiometric system has been developed and proposed to achieve a fully automatic positive personal identification with high level of confidence over wireless applications. In previous Chapters, theoretical attempt has been made to assesses and evaluate the performance of proposed method over various wireless communication systems (WiMAX, Wi-Fi, and 3G). The review of the technological background on the multibiometric technologies has been performed with greater depth on why biometrics has been selected and what are the limitations of these biometric techniques in wireless applications. In this Chapter, an experimental study has been implemented to empirically evaluate the feasibility of such systems in wireless communications. Many network packet analyzers have been studied and finally Wireshark was found to be the best suited as it remains operable over many operating systems and definitely, it provides many advantages when compared with other available simulators. In this regard, experimental investigation of this system in wireless communications has been executed in two steps (phase one and three). This is due to the dependency of these two phases on QoS of communication channel. Therefore as a first step, various sizes of watermarked fingerprints have been selected and delivered through the three selected wireless technologies (WiMAX, Wi-Fi and 3G), in order to measure QoS (delay, throughput, and jitter). As second step, the same process was done for the largest voice packet sizes. Based on the experimental results, it is shown that such system is fully capable of being applied over these wireless communication channels (WiMAX, Wi-Fi and 3G). However, as it has been shown experimentally, the delays for WiMAX and Wi-Fi were shorter compared to 3G. In addition, as discussed in previous Chapters, the system provides an adequate security to prevent service theft, thus protecting the service provider's investments in wireless infrastructure through projected system. The performance comparison of WiMAX with Wi-Fi and 3G has provided a clear approach of implementing multibiometric in WiMAX for adequate security. Therefore, proposed multibiometric cryptosystem can be applied in real time for all types of mentioned wireless networks. Although, the developed integrated system has been simulated through wireless channel and simple test has been performed to validate its capability, the full evaluation based on the requirement of each specific application is necessary.

Chapter 7

Conclusions and Recommendation for Future Work

The main concentration of this thesis has been designated to having a control measure in place prior to establishing a wireless network connection, so that access is restricted to the authorized users only. In previous chapters (2 and 5), the limitations of using single biometric protection techniques and possible solutions to address them through the employment of multibiometric cryptosystem are presented together with a motivation for developing such methods. This system is built upon a complete challenge/response methodology in order to obtain a high level of security on the basis of user identification by fingerprint and further confirmation by verification of the user through text-dependent speaker recognition. First in the enrolment stage, fingerprint is watermarked with a memorable text and is sent together with the voice feature, constructed from the same text, to the server over wireless channel. Then in the verification stage, the claimed user will be asked to input the fingerprint plus memorable text, to be watermarked, and utter the same text for comparison with that of enrolment stage, for final acceptance or rejection. In addition, in chapters 3 and 6 appropriate fingerprint and speaker recognition algorithms have been described. In order to implement fingerprint watermarking, i.e. incorporating the memorable word as a watermark message into the fingerprint image, an algorithm of five steps has been developed. The first three novel steps having to do with the fingerprint image enhancement (CLAHE with 'Clip Limit', standard deviation analysis and sliding neighborhood) are followed with further two steps for embedding, and extracting the watermark into the enhanced fingerprint image utilizing Discrete Wavelet Transform (DWT). In the speaker recognition stage, the limitations of this technique in wireless communication are addressed by sending voice feature (cepstral coefficients) instead of raw sample. This scheme is to reap the advantages of reducing the transmission time and dependency of the data on communication channel, together with no loss of packet.

In Chapters 6, the performance of this multibiometric cryptosystem to implement secure and real time wireless communication has been assessed. The medium of study for this purpose included Wi-Fi, 3G, and WiMAX. Finally, as indicated by simulation study for each phase and experimental study of the whole system, this multibiometric cryptosystem can be applied in real time for all types of mentioned wireless networks.

7.1 Achievements

The main aim of this research was the development and investigation of the multibiometric cryptosystem as access control for secure wireless communication. In order to achieve this, related literature concerning feasible multibiometric application in wireless system that yield maximum security was reviewed in depth. The problem was however that wireless networks regardless of whether they are based on WiMAX or Wi-Fi, are inherently less secure than wired counterparts due to lack of physical infrastructure. With the main concern being how to provide access only to authorized users, this time literature concerning the limitations and merits of fingerprint and voice recognition has been reviewed as a way of securing wireless networks. It was concluded that there are two bottlenecks to employ these biometric traits in wireless application. First, there is the dependence of data on the quality of communication channel, transcoding, transmission errors, and possibility of impostors' hack in voice recognition. Second, although the fingerprint authentication system presents certain advantages from the protection viewpoint, it is from the enrolment to the verification level susceptible to various types of threats and attacks including fake finger attacks, Trojan horse attacks and replay attacks. Therefore providing the advanced algorithms to deal with this intolerability against spoofing and cover the limitations of these techniques in wireless application remains an issue of concern. In order to address these issues and improve the accuracy of the whole system, the following steps have been accomplished:

- A compatible multibiometric system based on combining the fingerprint authentication with that of voice recognition as access control for secure wireless communication system has been introduced. Fingerprint and voice recognition were selected due to their feasibility, high balance of all the desirable properties, high performance, and accuracy.

- The possible limitation of fingerprint and voice recognition in wireless communication has been investigated and multibiometric cryptosystem was proposed and developed to address these limitations based on the watermarking of the enhanced fingerprint with the same text, which is used as text-dependent speaker recognition.
- A novel method for enhancement of fingerprint image has been proposed by means of eliminating the artificial induced boundaries, precise background omission; avoid oversaturation of the image in homogeneous areas, with no intermediate filtering and computational complexity. In order to eliminate the induced boundaries, the CLAHE technique was employed. ‘Clip Limit’ was then applied in order to avoid oversaturation of the image in homogeneous areas. Subsequently, the image was disintegrated into an array of distinct blocks and the discrimination of the blocks has been obtained by computing the standard deviation of the matrix elements to remove the image background. Once the boundary for the region of interest was obtained, a new modified thinning method using sliding neighborhood processing is applied to clarify the endpoints and the bifurcations in each specific pixel. In contrast to other thinning algorithms, the proposed approach does not require any intermediate filtering and lead to a substantial reduction of the computational complexity. The analysis of the proposed fingerprint image enhancement and its possible advantages has been carried out through a simulated investigation.
- In order to implement fingerprint watermarking, i.e. incorporating the memorable word as a watermark message into fingerprint image, an algorithm was developed. In the watermark embedding stage, firstly, presented memorable world by the user was converted to the image. In a second step, two-dimensional wavelet (DWT2) was applied to the original fingerprint image and transformed image from the text. This was carried out in order to decompose both images into low-pass subband and high-pass subbands. Finally, after embedding watermark coefficients to the most significant coefficients at the low and high frequency bands, of the discrete wavelet transform of an enhanced fingerprint image, the watermarked fingerprint image has been reconstructed by using inverse discrete two-dimensional

wavelet transform (IDWT2). In the watermark extraction stage, the memorable word has been used to verify the integrity of the watermarked fingerprint image by the process of detection.

- The performance of multibiometric security and proposed system has been assessed in real time wireless communication systems and Wi-Fi, 3G, and WiMAX platforms were investigated as end-to-end communication channels.

The main goal of this thesis was to design a multibiometric system, which is capable of achieving a fully automatic positive personal identification with a high level of confidence over wireless channels. The author has developed a prototype multibiometric cryptosystem system as access control for secure wireless communication. Although, the main focus was designated to address the limitations of these two biometric traits in wireless communication, the whole system was developed and the performance proved to be acceptable. The reliability of this approach needs to be tested against a large database for any modifications to be made respectively. If proven commercially reliable, this system can be employed in wireless devices to provide access to authorized users. Such a system when fully commercialized could replace PIN or ID card as a way of authentication in any feasible application (e.g. commercial and health care environments). Nowadays various types of attacks at and interceptions into wireless communication in sensitive areas, such as airports and nuclear sites, have raised the necessity for such systems to protect the digital voice communications as well as access control. In addition, by using the authorized wireless devices such as mobile phones, many telephone calls, and delays could be eliminated.

7.2 Suggestions for Future Work

In this thesis, the author discussed the limitations of current fingerprint and voice recognition approaches in wireless communication and some possible solutions through the proposed challenge/response technique. Although, the presented results through the simulation and experimental study was able to assess an acceptable performance of this system over wireless channel, number of problems still need to be resolved to make this more effective. The possible improvements have been identified as follows:

- As detailed in Chapter 3, some of the speaker recognition limitations in wireless communication have been addressed by sending voice features (cepstrum coefficients) instead of raw sample. However, many approaches have been proposed in the literature for voice feature extraction and their results can only be loosely compared because of their evaluations not being performed under identical conditions. As a result, more evaluations, and comparison, are necessary to achieve more accurate voice features as future work.

- As alternative to the proposed watermarking algorithm, there is the possibility of using the voice feature as key to encrypt the fingerprint image. However, the vector should be unique, if not; it will cause the false acceptance for the imposter. On the other hand, re-extracting the vector is difficult in speaker recognition; therefore, these issues can be explored as the next challenge for this research.
- In general, the main goal in fingerprint feature extraction is extracting as many as possible, true minutiae and avoiding any possible false minutiae. This will become the bottleneck when the image has very poor quality. The author's enhancement algorithm based on a new methodology has allowed superior performances, and possible advantages were discussed in Chapter 6. Nevertheless, comparison with other enhancement algorithms can be implemented in order to enable a discussion of whether or not; these proposed techniques have better performances in terms of detecting minutiae points and elapsed time.
- The main concentration of this thesis was designated to address the security and feasibility of multibiometric technique over wireless communication. In this report, solutions to overcome such problems are offered and amongst the suggested solutions was tried to choose the best one. Performance improvement of the proposed system can be achieved by incorporating the accurate (proper) matching techniques for fingerprint and voice recognition. Although, to limit the concentration to the scope of this thesis, this scheme was not investigated, finding out the appropriate matching technique is ideal for further work.
- Despite the fact that some of the fusion techniques proved efficient in improving the classification performance, there is no consensus on the best fusion technique. For this reason, further investigation (in terms of

performance disparity and correlation between sources) based on the suggested multibiometric cryptosystem and related expert of two selected biometric traits (voice and fingerprint) is essential. Nonetheless, accuracy of the whole system definitely can be improved using the appropriate fusion techniques to achieve results that are more reliable.

- Although the main aim of this research was to develop and investigate the multibiometric (fingerprint and voice recognition) cryptosystem, such a proposed system has the capability to take advantage of integrating the password as well due to the already usage of the text as requested challenge. Therefore, this capability can be investigated as the next step of this research.
- It is imperative to study the engineering and legal aspects of the proposed system in real world applications (e.g. E-Commerce), before any deployment of such system.
- Although, the developed integrated system has been simulated through wireless channel and simple test has been performed to validate its capability, full evaluation based on the requirement of each specific application is necessary.
- Finally, more validation tests on the robustness of proposed watermarking technique are necessary against various kinds of attacks.

References:

[1] D. Wright, "**The Role of Wireless Access Interconnection in Mobile e-Commerce Industry Evolution**", Eighth World Congress on the Management of e-Business (WCMeB), Toronto, July 2007.

[2] M. Cocosila, N. Archer, "**Mobile healthcare initiatives for improving outpatient adherence: opportunities and barriers**", International Journal of Electronic Business, Volume 3, Issue 6, pp. 512 - 533, 2005.

[3] P. A. Vlachos, A. Pateli, A. Vrechopoulos, "**Drawing Emerging Business Models for the Mobile Music Industry",** Electronic Markets, Volume 16, Issue 2, pp. 154-168, May 2006.

[4] N.A. Mylonopoulos, I.A. Sideris, "**Growth of Value Added Mobile Services under Different Scenarios of Industry Evolution",** Electronic Markets, Volume 16, Issue 1; pp. 28 - 40, Feb 2006.

[5] C. Gabriel, X. Huagang, G. Qiang, G. Esteban, R. Ricardo, E. Jose, "**A Perspective of State-of-the-Art Wireless Technologies for E-Health Applications**", IEEE International Symposium on IT in Medicine & Education, pp. 76 – 81, Aug 2009.

[6] C.C.Y. Poon, Y.T. Zhang, S.D. Bao, "**A Novel Biometrics Method to Secure Wireless Body Area Sensor Networks for Telemedicine and M-Health**", IEEE Communications Magazine, Volume 44, Issue 4, pp. 73-81, April 2006.

[7] R. R. Vangala, S. Sasi, "**Biometric authentication for e-commerce transaction**", IEEE International Workshop on Imaging Systems and Techniques (IST 2004), pp. 113 – 116, 14 May 2004.

[8] T. Karygiannis, L. Owens, “**Wireless network security 802. 11, Bluetooth and Handheld Devices**”, NIST Special Publication 800-48, Recommendations of the National Institute of Standards and Technology (NIST), November 2002.

[9] C. T. Huang, J. M. Chang, “**Responding to security issues in WiMAX networks**”, IEEE Comp. Society IT Professional Magazine, Volume 10, Issue 5, pp. 15–21, 2008.

[10] A. K. Jain, A. Ross, S. Prabhakar, “**An introduction to biometric recognition**”, IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image-and- Video-based Biometrics, Volume 14, Issue 1, pp. 4 - 20, January 2004.

[11] M. Turk, A. Pentland, “**Eigenfaces for recognition**”, Journal of Cognitive Neuroscience, Volume 3, Issue 1, pp. 71-86, 1991.

[12] J. J. Atick, P. A. Griffin, A. N. Redlich, “**Statistical approach to shape from shading: Reconstruction of 3-dimensional face surfaces from single 2-dimensional images**”, Neural Computation, Volume 8 , Issue 6, pp. 1321-1340, August 1996.

[13] R. L. Zunkel, “**Hand geometry based verification**”, in Biometrics Personal Identification in Networked Society, Kluwer Academic Publishers, 4th edition, Chapter 4, A. Jain, R. Bolle, S. Pankanti, pp. 87–101, 2002.

[14] P. Tikkanen, S. Puolitaival, I. Känsälä, “**Capabilities of Biometrics for Authentication in Wireless Devices**”, Proceedings of the 4th international conference on Audio- and video-based biometric person authentication, pp. 796-804, Guildford, 2003.

[15] P. N. Belhumeur, J. P. Hespanha, D. J. Kriegman, “**Eigenfaces vs. Fisher faces: Recognition Using Class Specific Linear Projection**”, IEEE Transactions on Pattern Analysis and Machine Intelligence, Volume 19, Issue 7, pp. 711 – 720, 1997.

[16] S. Malassiotis, N. Aifanti, M.G. Strintzis, “**Personal authentication using 3-D finger geometry**”, IEEE Transactions on Information Forensics and Security, Volume 1, Issue 1, pp. 12 – 21, March 2006.

[17] E. Yu, S. Cho, “**Keystroke dynamics identity verification - Its problems and practical solutions**”, Journal of Computers and Security, Volume 23, Issue 5, Pages 428-440, July 2004.

[18] D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, “**Handbook of Fingerprint Recognition**”, New York, NY, USA, June 2003.

[19] M. SandstrÄom, “**Liveness Detection in Fingerprint Recognition Systems**”, Linkopings University, Master Thesis, Sweden, June 2004.

[20] J. Daugman, “**Recognizing persons by their iris patterns**”, in Biometrics Personal Identification in Networked Society, Chapter 5, A. Jain, R. Bolle, S. Pankanti, pp. 103–121, Kluwer Academic Publishers, 4th edition, 2002.

[21] F. Monrose, A. D. Rubin, “**Keystroke dynamics as a biometric for authentication**”, Future Generation Computer Systems, Special issue on security on the Web, Volume 16 , Issue 4, pp. 351 – 359, February 2000.

[22] V. Nalwa, “**Automatic on-line signature verification**”, Proceedings of the IEEE, Volume 85, Issue 2, pp. 213-239, February 1997.

[23] S. Furui, “**Recent advances in speaker recognition**”, Proceedings of the First International Conference on Audio- and Video-Based Biometric Person Authentication AVBPA’97, Lecture Notes in Computer Science; Volume 1206, pp. 237-252, Springer-Verlag, 1997.

[24] B. Toth, “**Biometric Security**”, version 1.1, February 2004, last visit September 2009, available at: https://www.deloitte.com/assets/Dcom-UnitedKingdom/Local%20Assets/Documents/UK_ERS_Bori_BiometricSecurity_April05.pdf

[25] J. Blomme, "**Evaluation of biometric security systems against artificial fingers**", Master's thesis, LinkÄoping University, Sweden, October 2003.

[26] A. Jain, R. Bolle, S. Pankanti, "**Biometrics, Personal Identification in Networked Society**", Kluwer Academic Publishers, 4th edition, 2002.

[27] Pictures Available at: http://www.fingerprintdoorlocks.com/, Last visit September 2009.

[28] P. Domingos, M. Pazzani, "**On the Optimality of the Simple Bayesian Classifier under Zero-One Loss**", Kluwer Academic Publishers Netherlands, Machine Learning, Special issue on learning with probabilistic representations ,Volume 29, Issue 2-3, pp. 103-130, Nov/Dec 1997.

[29] International Biometric Group, "**Biometrics Market and Industry Report 2009- 2014"**, available at http://www.biometricgroup.com/reports/public/market_report.html.

[30] U.M. Bubeck, "**Multibiometric authentication: An overview of recent developments**", Term Project CS574, San Diego State University, spring 2003.

[31] G. Aguilar, G. Sánchez, K. Toscano, H. Pérez, "**Frequency-Based Fingerprint Recognition**", in Handbook of Remote Biometrics, Advances in Pattern Recognition, pp. 363-374, ISBN: 978-1-84882-384-6, Springer London, June 2009.

[32] A. Ross, A. K. Jain, D. Zhang, "**Handbook Of Multibiometrics**", published by Springer-Verlag New York Inc, ISBN:0387222960, 2005.

[33] A. Ross, A. K. Jain, "**Biometric Sensor Interoperability**: **A Case Study in Fingerprints**", In Proceedings of ECCV International Workshop on Biometric Authentication (BioAW), Volume 3087, pp. 134-145, Prague, Czech Republic, Springer, May 2004.

[34] International Biometric Group, "**Biometrics Market and Industry Report**", 2002.

[35] A. Ross, A.K. Jain, “**Information Fusion in Biometrics**”, Pattern Recognition Letters, Special issue: Audio- and video-based biometric person authentication (AVBPA 2001), Volume 24 , Issue 13, pp. 2115-2125, September 2003.

[36] C. Sanderson, K. K. Paliwal, “**Information Fusion and Person Verification Using Speech and Face Information**”, Technical Report, IDIAP-RR 02-33, IDIAP, September 2002.

[37] R. S. Blum, Z. Liu, “**Multi-Sensor Image Fusion and Its Applications**”, CRC Press, Taylor and Francis Group, Florida, USA, 2006.

[38] T. Szigeti, C. Hattingh, "**End-to-End QoS Network Design: Quality of Service in LANs, WANs, and VPNs (Networking Technology)**". Cisco Press, USA, Nov 2004.

[39] A.J. Willis, L. Myers, “**A Cost-Effective Fingerprint Recognition System for Use with Low-Quality Prints and Damaged Fingertips**”, Pattern Recognition, Volume 34, Issue 2, pp. 255−270, February 2001.

[40] S. Giarmi, H. Magnusson, “**Investigation of user acceptance for biometric verification/identification methods in mobile units**”, Master thesis, Stockholm University, Royal Institute of Technology, Sweden 2002.

[41] O. D. Trier, A.K. Jain, “**Goal-Directed Evaluation of Binarization Methods**”, IEEE Transactions on Pattern Analysis and Machine Intelligence, Volume 17, Issue: 12, pp. 1191−1201, Dec 1995.

[42] C. Wolf, J.M. Jolion, “**Extraction and recognition of artificial text in multimedia documents**”, Pattern Analysis & Applications, Volume 6, Issue 4, pp. 309–326, February 2003.

[43] I. Chlamtac, M. Conti, J. J.N. Liu, “**Mobile ad hoc networking: imperatives and challenges**”, Ad Hoc Networks Journal, Volume 1, Issue 1, pp. 13-64, July 2003.

[44] S. Ravi, A. Raghunathan, N. Potlapally, “**Securing wireless data: System architecture challenges**”, Proceedings of the 15th international symposium on System Synthesis, pp. 195-200, Kyoto, 2 - 4 October 2002.

[45] C. Xenakis, L. Merakos, “**Security in third Generation Mobile Networks**”, Journal of Computer Communications, Volume 27, Issue 7, pp. 638-6501, May 2004.

[46] P. Ashley, H. Hinton, M. Vandenwauver, “**Wired versus Wireless Security: The internet, WAP and iMode for E-Commerce**”, Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC), pp. 296 - 306, Dec 2001.

[47] K. Lu, Y. Qian, H, H, Chen” **WIRELESS BROADBAND ACCESS: WIMAX AND BEYOND - A Secure and Service-Oriented Network Control Framework for WiMAX Networks**”, IEEE Communications Magazine, Volume 45, Issue 5, pp. 124-130, May 2007.

[48] S. Greenberg, M. Aladjem, D. Kogan, I. Dimitrov, “**Fingerprint image enhancement using filtering techniques**”, 15th International Conference on Pattern Recognition (ICPR'00), Volume 3, pp. 322 - 325, Barcelona , Spain, 2000.

[49] A. Ross, A. Jain, J. Reisman, “**A hybrid fingerprint matcher**”, Proceedings of 16th International Conference on Pattern Recognition, Volume 3, pp. 795-798, August 11-15, 2002.

[50] A. Jain, R. Bolle, S. Pankanti, “**Introduction to Biometrics**”, in Biometrics Personal Identification in Networked Society, Chapter 1, A. Jain, R. Bolle, S. Pankanti, Eds. Norwell, MA: Kluwer, pp. 103–121, 2002.

[51] W. Zhao, R. Chellappa, “**Face Processing: Advanced Modeling and Methods**”, Academic Press, ISBN-13: 978-0-12-088452-0, Dec 2005.

[52] A. Bovik, “**Handbook of Image and Video Processing**”, Academic Press, ISBN 0-12-119790-5, USA, 2000.

[53] J. Matey, O. Naroditsky, K. Hanna, R. Kolczynski, D. LoIacono, S. Mangru, M. Tinker, T. Zappia, W. Zhao, "**Iris on the Move: Acquisition of Images for Iris Recognition in Less Constrained Environments**", Proceedings of the IEEE, Volume 94, Issue 11, pp.1936-1947, 2006.

[54] D.S. Guru, H.N. Prakash, "**Online Signature Verification and Recognition: An Approach Based on Symbolic Representation**", IEEE Transactions on Pattern Analysis and Machine Intelligence, Volume 31, Issue 6, pp. 1059 – 1073, 2009.

[55] M. Mingming, W.S. Wijesona, "**Automatic on-line signature verification based on multiple models**", Proceedings of the IEEE/IAFE/INFORMS Conference on Computational Intelligence for Financial Engineering (CIFEr), pp. 30 – 33, 2000.

[56] M.A. Turk, A.P. Pentland, "**Face recognition using eigenfaces**", Proceedings CVPR '91, IEEE Computer Society Conference on Computer Vision and Pattern Recognition, pp. 586 – 591, Jun 1991.

[57] J. G. Daugman, "**High confidence visual recognition of persons by a test of statistical independence**", IEEE Transactions on Pattern Analysis and Machine Intelligence, Volume 15, Issue 11, pp 148-1161, Nov 1993.

[58] Last visit June 2009, Y. Arar, Pictures Available at: http://pcworld.about.com/magazine/2102p034id108240.htm

[59] D. Swets, J. J. Weng, "**Using discriminant eigenfeatures for image retrieval**", IEEE Transactions on Pattern Analysis and Machine Intelligence, Volume 18, Issue 8, pp. 831-836, August 1996.

[60] N. Ratha, R. Bolle, "**Automatic Fingerprint Recognition Systems**", ISBN: 0387955933, Springer, October 2003.

[61] A. Mantravadi, R. K. Srinvasan, S. Chikkerur, "**EE 516 Term Project Speaker Recognition**", December 2003, last visit February 2010, Available at http://web.mit.edu/sharat/www/resources.html

[62] D.A. Reynolds, "**An Overview of Automatic Speaker Recognition technology**", IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '02), Volume 4, pp. IV 4072- IV4075, May 2002.

[63] A. K. Jain, L. Hong, R. Bolle, "**On-Line Fingerprint Verification**", IEEE Transactions on Pattern Analysis and Machine Intelligence, Volume 19, Issue 4, pp.302-314, April 1997.

[64] A. Wahab, S.H. Chin, E.C. Tan, "**Novel approach to automated fingerprint recognition**", IEE Proceedings on Vision, Image and Signal Processing, Volume 145, Issue 3, pp. 160-166, Jun 1998.

[65] K. Zebbiche, F. Khelifi, "**Region-Based Watermarking of Biometric Images: Case Study in Fingerprint Images**", International Journal of Digital Multimedia Broadcasting, Volume 2008, Article ID 492942, 2008.

[66] L. Besacier, P. Mayorga, J. F. Bonastre, C. Fredouille, "**METHODOLOGY FOR EVALUATING SPEAKER VERIFICATION ROBUSTNESS OVER IP NETWORKS**", Proceedings of the COST-275 Workshop (The advent of Biometrics on the Internet), Rome, Italy, November 7-8th, 2002.

[67] P. Mayorga-Ortiz, R. Lamy, L. Besacier, "**Recovering of packet loss for distributed speech recognition**", Proceedings of 11th European Signal Processing Conference, Toulouse, France, September 2002.

[68] J. Siau, A. Ariyaeeinia, "**DATA TRANSMISSION IN BIOMETRICS OVER THE INTERNET**", Proceedings of the COST-275 Workshop (The advent of Biometrics on the Internet), Rome, Italy, pp.51-54, November 7-8, 2002.

[69] N. W. D. Evan , J. S. Mason, R. Auckenthaler, R. Stapert, "**ASSESSMENT OF SPEAKER VERIFICATION DEGRADATION DUE TO PACKET LOSS IN THE CONTEXT OF WIRELESS MOBILE DEVICES**", Proceedings of the COST-275 Workshop (The advent of Biometrics on the Internet), Rome, Italy, November 7-8th, 2002.

[70] D. Reynolds, "**The effect of handset variability on speaker recognition performance: Experiments on the switchboard corpus**", Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, Volume 1, pp.113–116, May 1996.

[71] J.M. Naik, , L.P Netsch, G.R. Doddington, " **Speaker verification over long distance telephone lines**“, In International Conference on Acoustics, Speech, and Signal Processing, Volume 1, pp. 524 – 527, May 1989.

[72] M.W. Mak, S.Y. Kung, "**Combining stochastic feature transformation and handset Identification for telephone-based speaker verification**", IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '02), Volume 1, pp. I-701 - I-704, May 2002.

[73] A. Drygajlo, P. Boda, J.M. Boite, A.E. Cetin, K. Elenius, Z. Ka_ci_c, J.P. Martens, J. Nouza, F. Perdigao, H. Strik, J. de Veth, "**Feature extraction**", Final Report of COST Action 249, Continuous Speech Recognition over the Telephone, Chapter 2, University of Gent, May 2000.

[74] L. Besacier, A. M. Ariyaeeinia, J. S. Mason, J. F. Bonastre, P. Mayorga, C. Fredouille, S. Meignier, J. Siau, N . W. D. Evans, R. Auckenthaler, R. Stapert, "**Voice Biometrics over the Internet in the Framework of COST Action 275**", EURASIP Journal on Applied Signal Processing, Volume 2004, pp.466–479, 2004.

[75] D.R. Rodman, "**Computer Speech Technology"**, Artech House, Norwood, MA, USA, 1999.

[76] B.G. Sherlock, D. M. Monro, K. Millard, "**Fingerprint enhancement by directional Fourier filtering**", IEE Proceedings on Vision, Image and Signal Processing, Volume 141, Issue 2, pp. 87–94, Apr 1994.

[77] J. Ashbourn, "**Biometrics: Advanced Identity Verification**", Springer-Verlag, London, GB, ISBN 1-85233-243-3, 2000.

[78] A. Çavuşoğlu, S. Görgünoğlu, “**A fast fingerprint image enhancement algorithm using a parabolic mask**”, Computers & Electrical Engineering, Volume 34, Issue 3, pp. 250-256, May 2008.

[79] N. Nagamalleswara Rao, P. Thrimurthy, B. Raveendra Babu, “**An efficient copyright protection scheme for digital images using Biometrics and Watermarking**”, 2nd IEEE International Conference on Computer Science and Information Technology, Beijing, China, ISBN: 978-1-4244-4519-6, pp. 69 – 74, August 08-11, 2009.

[80] R. Cole, J. Mariani, H. Uszkoreit, A. Zaenen, V. Zue, ” **Survey of the State of the Art in Human Language Technology**”, Cambridge University Press, ISBN:0-521-59277-1, New York, NY, USA Ed. 1997.

[81] J. Campbell, ” **Speaker Recognition**”, Biometrics - Personal Identification in Networked Society, Chapter 8, Springer US, 2002.

[82] J. P. Campbell, “**Speaker Recognition: A Tutorial**”, Proceedings of the IEEE, Volume 85, Issue 9, pp. 1437-1462, Sep 1997.

[83] R. Gnanadesikan, J. R. Kettenring, “**Discriminant Analysis and Clustering**”, Statistical Science, Volume 4, pp. 34-69, 1989.

[84] C. Wu, Z. Shi, V. Govindaraju, “**Fingerprint image enhancement method using directional median filter**”, In Biometric Technology for Human Identification. Edited by A.K. Jain, N.K. Ratha, Proceedings of the SPIE, Volume 5404, pp. 66-75, 2004.

[85] L.C. Jain, U. Halici, I. Hayashi, S.B. Lee, S. Tsutsui, “**Intelligent Biometric Techniques in Fingerprint and Face Recognition**”, CRC Press, Boca Raton, FL, USA, 1999.

[86] D. A. Reynolds, "**Speaker Identification and Verification Using Gaussian Mixture Speaker Models**", Speech Communication, Volume 17, Issue 1-2, August 1995.

[87] C.I. Watson, G.I. Candela., P.J. Grother, “**Comparison of FFT Fingerprint Filtering Methods for Neural Network Classification**”, Tech. Report: NIST TR 5493, 1994.

[88] C. Sanderson, “**Speech processing & text-independent automatic person verification**”, Tech. Rep. 08, IDIAP, Martigny, Switzerland, 2002 (MINOR REVISION: JANUARY 2004).

[89] K. K. Paliwal, "**Speech Processing Techniques**", Advances in Speech, Hearing and Language Processing (editor: W. A. Ainsworth), Volume 1, pp. 1-78, 1990.

[90] European Telecommunications Standards Institute, “**Speech Processing, Transmission and Quality Aspects (STQ); Distributed speech recognition; Front-end feature extraction algorithm; Compression algorithms**” Technical standard ES 201 108, v1.1.3, (2000-04).

[91] S. B. Davis P. Mermelstein, “**Comparison of Parametric Representations for Monosyllabic Word Recognition in Continuously Spoken Sentences**”, IEEE Transactions on Acoustic, Speech, and Signal Processing (ASSP-28), Volume 28, Issue 4, pp. 357–366, Aug 1980.

[92] H. Hermansky, N. Morgan, A. Bayya, P. Kohn, “ **Compensation for the Effect of the Communication Channel in Auditory-Like Analysis of Speech (RASTA-PLP)**”, In Proceedings of “EUROSPEECH91” second European Conference on Speech Communication and Technology, Genova, Italy, pp. 1367-1370, September 24-26, 1991.

[93] S. Furui, “**Cepstral Analysis Technique for Automatic Speaker Verification**”, IEEE Transactions on Automatic Speech Signal Processing, Volume 29, Issue 2, pp. 254-272, April 1981.

[94] L. P. Heck, Y. Konig, M. K. Sonmez, M. Weintraub, “**Robustness to telephone handset distortion in speaker recognition by discriminative feature design**”, Speech Communication, Volume 31 , Issue 2-3, pp. 181-192, June 2000.

[95] F. Bimbot, J.F. Bonastre, C. Fredouille, G. Gravier, I. Magrin-Chagnolleau, S. Meignier, T. Merlin, J. Ortega-Garcia, D. Petrovska-Delacretaz, D. A. Reynolds, "**A tutorial on text-independent speaker verification**", EURASIP Journal on Applied Signal Processing, Volume 2004, Issue 4, pp. 430-451, 2004.

[96] H. Hermansky, N. Morgan, "**RASTA Processing of Speech**", IEEE Transactions on Speech and Audio Processing, Volume 2, Issue 4, pp. 578-589, Oct 1994.

[97] L. R. Rabiner, "**A tutorial on Hidden Markov Models and selected applications in speech recognition**", Proceedings of the IEEE, Volume 77, Issue 2, pp. 257-286, Feb 1989.

[98] J. Naik, "**Speaker verification: A tutorial**", IEEE Communications Magazine, Volume 28, Issue: 1, pp. 42–48, Jan. 1990.

[99] MATLAB help, version R2007b.rsion R2007b.

[100] J. Picone, G. R. Doddington, J. J. Godfrey, "**A Layered Grammar Approach to Speaker Independent Speech Recognition**", presented at the 1988 Speech Recognition Workshop, Harriman, NY, June 1988.

[101] A. Gresho, R. M. Gray, **"Vector Quantization and Signal Compression**", Kluwer Academic Publisher, Boston, 1992.

[102] D. A. Reynolds, R.C Rose, "**Robust Text-Independent Speaker Identification Using Gaussian Mixture Speaker Models**", IEEE Transactions on Speech and Audio Processing Volume 3, Issue 1, pp. 72–83, January 1995.

[103] G.R. Doddington, "**A computer method of speaker verification**", PhD thesis, Department of electrical engineering, university of Wisconsin, Madison, 1970.

[104] H. Sakoe, S. Chiba, "**Dynamic programming algorithm optimization for spoken word recognition**", IEEE Transactions on Acoustics, Speech and Signal Processing, Volume 26 , Issue 1 , no. 1, pp. 43–49, Feb 1978.

[105] I. booth, M. Barlow, B. Watson, “**Enhancements to DTW and VQ decision algorithms for speaker recognition**”, Speech science and technology: a selection from the papers presented at the Fourth International Conference in Speech Science and Technology (SST-92), Volume 13, Issue 3-4, pp. 427 - 433 December 1993.

[106] A. Sherstinsky, R.W. Picard, “**Restoration and enhancement of fingerprint images using M-lattice-a novel nonlinear dynamical system**”, Proceedings of the 12th IAPR International Conference on Pattern Recognition, Volume 2 - Conference B: Computer Vision & Image Processing, pp. 195 - 200, Oct 1994.

[107] F. K .Soong, A. E. Rosenberg, L.R. Rabiner, B. H. Juang, “`**A vector quantization approach to speaker recognition**", IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '85), Volume 10, pp. 387 - 390, Apr 1985.

[108] A. M. Ahmad, L. M. Yee, “**Vector Quantization Decision Function for Gaussian Mixture Model Based Speaker Identification**”, International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS2008), pp.1 – 4, Thailand, Feb 2008.

[109] L. E. Baum, T. Petrie, “**Statistical inference for probabilistic functions of finite state Markov chains**”, Annals of Mathematical Statistics, Volume 37, pp. 1554-1563, 1966.

[110] J. K. Baker, ” **The dragon system-An overview**”, IEEE Transactions on Acoustics, Speech and Signal Processing, Volume 23, Issue 1, pp. 24- 29, Feb 1975.

[111] F. Jelinek, “**A fast sequential decoding algorithm using a stack**”, IBM Journal of Research and Development, Volume 13, Issue 6, pp. 675-685, November 1969.

[112] N.Z. Tishby, "**On the Application of Mixture AR Hidden Markov Models to Text Independent Speaker Recognition**”, IEEE Transactions on Signal Processing, Volume 39, Issue 3, pp. 563 – 570, March 1991.

[113] D. C. Huang, “**Enhancement and feature purification of fingerprint images**”, Pattern Recognition, Volume 26, Issue 11, pp. 1661-1671, November 1993.

[114] Y. Gu, T. Thomas, “**Text Independent Speaker verification system using support vector machines classifier**”, Proceeding in European Conference on Speech Communication and Technology (Eurospeech'01), pp. 1765-1768, Aalborg, Denmark, September 2001.

[115] S. V. Vasegi, P. N. Connor, B. P. Milner, “**Speech modeling using cepstral-time feature matrices in hidden Markov models**”, IEE Proceedings I Communications, Speech and Vision, Volume 140, Issue 5, pp. 317–320, Oct 1993.

[116] M. A. Mohamed, P. Gader, “**Generalized Hidden Markov Models-Part I: Theoretical Frameworks**”, IEEE Transaction on Fuzzy Systems, Volume 8, Issue 1, pp. 67 – 81, February 2000.

[117] D. A. Reynolds, "**experimental evaluation of features for robust speaker Identification**", IEEE Transaction on Speech, and Audio Processing, Volume 2, Issue: 4, pp.639-643, 1994.

[118] B. Moayer, K.S. Fu, “**A tree system approach for fingerprint pattern recognition**”, IEEE Transaction on Pattern Analysis and Machine Intelligence, Volume 25 , Issue 3. pp. 262-274, 1976.

[119] D. Sherlock, D. M. Monro, K. Millard, “**Fingerprint enhancement by directional Fourier filtering**”, IEE Proceedings Image Signal Processing, Volume 141, Issue: 2, pp. 87 – 94, Apr 1994.

[120] A. Higgins, L. Bahler, J. Porter, “**Speaker verification using randomized phrase promoting**”, digital signal processing, pp. 89-106, 1991.

[121] A. E. Rosenberg, J. DeLong, C. H. Lee, B.H. Juang, K. Soong, “**The use of cohort normalized scores for speaker verification**”, In Proceedings of International Conference on Speech and Language Processing (ICSLP '92), pp. 599–602, Banff, Canada, Oct 1992.

[122] B. S. Atal, "**Effectiveness of linear prediction characteristics of the speech wave for automatic speaker identification and verification**", Journal of the Acoustical Society of America, Volume 55, Issue 6, pp. 1304-1312, June 1974.

[123] K. P. Li, E. H. Wrench, Jr., "**An approach to Text-independent speaker recognition with short utterances**", IEEE International Conference on Acoustics, Speech, and Signal Processing, Boston, MA, pp. 555–558, Apr 1983.

[124] S. Kullback, "**Information Theory, and Statistics**" New York: Dover, 1968.

[125] D. Reynolds, B. Carlson, "**Text-dependent speaker verification using decoupled and integrated speaker and speech recognizers**", in Proceedings of EUROSPEECH, Madrid, Spain, pp. 647–650, 1995.

[126] C. Che, Q. Lin, "**Speaker recognition using HMM with experiments on the YOHO database**", in Proceedings of EUROSPEECH, Madrid, Italy, pp. 625–628, 1995.

[127] D. Reynolds, "**M.I.T. Lincoln Laboratory site presentation**", in Speaker Recognition Workshop, A. Martin, Ed., sect.5, Maritime Institute of Technology, Linthicum Heights, MD, Mar. 27–28, 1996.

[128] M. Yeung, S. Pankanti, "**Verification watermarks on fingerprint recognition and retrieval**", Proceedings of SPIE Conf. Security and Watermarking of Multimedia Contents, Volume 3657, pp. 66–78, CA, USA, Jan 1999.

[129] P. Wayner, "**Disappearing Cryptography**", Morgan Kaufmann Publishers, Second Edition, by Elsevier Science (USA), 2002.

[130] J. Domingo, D. Chan, A. Watson, "**Smart card research and advanced applications**", Series: IFIP International Federation for Information Processing, Springer, Volume 52, 2000.

[131] N. Galy, B. Charlot, B. Courtois “**A Full Fingerprint Verification System for a Single-Line Sweep Sensor**”, IEEE Sensors Journal, Volume 7, Issue 7, pp 1054-1065, July 2007.

[132] X. Xia, L. O'Gorman, “**Innovations in fingerprint capture devices**”, Pattern Recognition, Volume 36, Issue 2, pp.361-369, February 2003.

[133] A. Ross, R. Nadgir, “**A calibration model for fingerprint sensor interoperability**”, in Prec. of SPIE conference on biometrics technology for Human identification III, Orlando USA , Volume 62020, April 2006.

[134] G. Zhou, Y. Qiao, F. Mok, ” **Fingerprint sensing system using a sheet prism**”, US Patent 5796858, 1998.

[135] X.G. Xia, C. Boncelet, G. Arce, “**A multiresolution watermark for digital images**”, Proceedings of the 1997 International Conference on Image Processing (ICIP ’97), Santa Barbara, CA, October 1997.

[136] J. Titus, “**Vendors make it easy to add biometric sensors to security systems**”, Design News, February 7, 2005 Available online. http://www.designnews.com/article/1453

[137] S. Shigematsu, H. Morimura, Y. Tanabe, K. Machida, “**A Single-chip fingerprint sensor and identifier**”, IEEE Journal of Solid-State Circuits, Volume 34 , Issue 12 , pp.1852–1859, Dec 1999.

[138] S. Jung, R. Thewes, T. Scheiter, K. F. Goser, W. Weber, “**A low-power and high-performance CMOS fingerprint sensing and encoding architecture**”, Proceedings of the 24th European Solid-State Circuits Conference (ESSCIRC '98), pp. 324 - 327, Sept 1998.

[139] N. Shimoyama, S. Shigematsu, H. Morimura, T. Shimamura, T. Kumazaki, M. Nakanishi, H. Ishii, K. Machida, "**Effect of scratch stress on the surface hardness and inner structures of a capacitive fingerprint sensor LSI**", Reliability physics symposium, Proceedings 45th annual IEEE International, pp. 412-416, April 2007.

[140] J. L. Liu, D. C. Lou, M. C. Chang, H. K. Tso, “**A robust watermarking scheme using self-reference image**”, Computer Standards & Interfaces, Volume 28, Issue 3, Validation of Software in Metrology, Volume 28, Issue 3, pp. 356-367, January 2006.

[141] J. Nam, S. Jung, M. Lee, “**Design and Implementation of a capacitive fingerprint sensor circuit in CMOS technology**”, Special Issue of The Micromechanics section of Sensors and Actuators (SAMM, based on contributions revised from the Technical Digest of the IEEE 19th International conference on Micro Electro Mechanical Systems (MEMS 2006), Volume 135, Issue 1, pp.283–291, 2007.

[142] F. Alonso-Fernandez, F. Roli, G. Marcialis, J. Fierrez, J. Ortega-Garcia, J. Gonzalez-Rodriguez, “**Performance of fingerprint quality measures depending on sensor technology**”, Journal of Electronic Imaging, SPIE Press, Volume 17, issue 1, January 2008.

[143] E. Kukula, S.Elliott, H. Kim; S. Martin, C, “**The impact of fingerprint force on image quality and the detection of minutiae**”, IEEE International Conference on Electro/Information Technology, pp. 432-437, May 2007.

[144] H. Kang, B. Lee, H. Kim, D. Shin, J. Kim “**A study on performance evaluation of fingerprint sensors**”, Proceedings of the 4th international conference on Audio- and video-based biometric person authentication, pp. 574-583, 2003.

[145] H. Han, Y. Koshimoto, “**Characteristics of thermal-type fingerprint sensor**”, Biometric Technology for Human Identification, Proceedings of SPIE, Volume 6944, March 2008.

[146] N.K. Ratha, S.Y. Chen, A.K. Jain, “**Adaptive Flow Orientation-Based Feature Extraction in Fingerprint Images**”, Pattern Recognition, Volume 28, Issue 11, pp. 1657−1672, 1995.

[147] W. Niblack, “An introduction to digital image processing”, Englewood, Prentice Hall, pp. 115–116, 1986.

[148] J. Sauvola, M. Pietikainen, “**Adaptive document image binarization**”, Pattern Recognition, Volume 33, Issue 2, pp. 225–236, February 2000.

[149] T. van der Putte, J. Keuning, “**Biometrical fingerprint recognition: don't get your fingers burned**”, In Proceedings of IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications, pp. 289–303, September 2000.

[150] T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, “**Impact of artificial gummy fingers on fingerprint systems**”, In Proceedings of SPIE Volume #4677, Optical Security and Counterfeit Deterrence Techniques IV, Yokohama National University, Japan, January 2002.

[151] J. Woodward, N. M. Orlans, P. T. Higgins, “**Biometrics**”, New York, McGraw Hill Osborne, ISBN: 0072230304, December 2002.

[152] International Biometric Group, “**Liveness detection in biometric systems**”, White paper, 2003, Last visit Dec 2009, Available at http://www.biometricgroup.com/reports/public/reports/liveness.html

[153] S. A. C. Schuckers, “**Spoofing and anti-spoofing measures**”, Information Security Technical Report, Volume 7, Issue 4, pages 56 – 62, December 2002.

[154] A. K. Jain, A. Ross, U. Uludag, "**Biometric template security: challenges and solutions**", Proceedings of the European Signal Processing Conference (EUSIPCO '05), Antalya, Turkey, September 2005.

[155] J. G. Ko, K. Y. Moon, “**Biometrics Security Scheme for Privacy Protection**”, Advanced Software Engineering and Its Applications, pp. 230 – 232, Dec 2008.

[156] E. Hill, M. D. Stoneham, “**Practical applications of pulse oximetry**”, Nuffield Department of Anaesthetics, Oxford Radcliffe NHS Hospitals Headington, 2000.

[157] R. Derakhshani, S. Schuckers, L. Hornak, L. O'Gorman, "**Determination of Vitality from A Non-Invasive Biomedical Measurement for Use in Fingerprint Scanners**", Pattern Recognition, Volume 36, Issue 2, pp. 383-396, February 2003.

[158] P. Kallo, I. Kiss, A. Podmaniczky, J. Talosi, "**Detector for recognizing the living character of a finger in a fingerprint recognizing apparatus**", Dermo Corporation, Ltd. US Patent, January 16, 2001.

[159] M. Drahansky, R. Notzel, W. Funk, "**Liveness Detection based on Fine Movements of the Fingertip Surface**", 2006 IEEE Information Assurance Workshop, pp. 42 - 47, June 2006.

[160] Y.S. Moon, J.S. Chen, K.C. Chan, K. So, K.C. Woo, "**Wavelet based fingerprint liveness detection**", Electronics Letters, Volume: 41, Issue 20, pp. 1112–1113, 29 Sept. 2005.

[161] A. Abhyankar, S. Schuckers, "**Fingerprint liveness detection using local ridge frequencies and multiresolution texture analysis techniques**", 2006 IEEE International Conference on Image Processing, pp. 321-324, Atlanta, October 2006.

[162] S. Parthasaradhi, R. Derakshani, L. Hornak, S. Schuckers, "**Time-series detection of perspiration as a liveness test in fingerprint devices**", IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, Volume 35, Issue 3, pp. 335–343, Aug. 2005.

[163] B. Tan, S. Schuckers, "**Liveness Detection for Fingerprint Scanners Based on the Statistics of Wavelet Signal Processing**", Proceedings of the 2006 Conference on Computer Vision and Pattern Recognition Workshop**,** June 2006.

[164] B. Tan, S. Schuckers, "**New Approach for Liveness Detection in Fingerprint Scanners Based on Valley Noise Analysis**", SPIE Journal of Electronic Imaging 17, January 2008.

[165] The page is available at "http://www.lumidigm.com/liveness-detection/", last visit January of 2010.

[166] R.K. Rowe, K.A. Nixon, S.P. Corcoran, "**Multispectral fingerprint biometrics**", Proceedings from the Sixth Annual IEEE SMC on Information Assurance Workshop, pp. 14 – 20, June 2005.

[167] D. Baldisserra, A. Franco, D. Maio, D. Maltoni, "**Fake Fingerprint Detection by Odor Analysis**", In D. Zhang, A.K. Jain (Eds.): ICB 2006, LNCS 3832, pp. 265-272, 2005.

[168] S.E. Braslavsky "**Glossary of terms used in photochemistry (IUPAC recommendations 2006)**", Pure, and Applied Chemistry, Volume 79, pp. 293–465, 2007.

[169] W.Y. Yau, H.T. Tran, E.K. Teoh, J.G. Wang, "**Fake Finger Detection by Finger Color Change Analysis**", Proceedings of International Conference on Biometrics (ICB'2007), pp. 888-896, Aug. 2007.

[170] W. Y. Yau, H. L. Tran, E. K. Teoh, "**Fake finger detection using an electro tactile display system**", 10th International Conference on Control, Automation, Robotics and Vision (ICARCV 2008), pp. 962 – 966, Hanoi, Vietnam, December 2008.

[171] C. Jin, H. Kim, S. Elliott, "**Liveness Detection of Fingerprint Based on Band-Selective Fourier Spectrum**", Proceedings of the 10th international conference on Information security and cryptology (ICISC 2007), pp. 168–179, Seoul, Korea, 2007.

[172] H. S. Lee, H. j. Maeng, Y. suk Bae, " **Fake Finger Detection Using the Fractional Fourier Transform**", Proceedings of the 2009 joint COST 2101 and 2102 international conference on Biometric ID management and multimodal communication, pp. 318-324, Madrid, Spain, September 29, 2009.

[173] C. S. WOO, "**Digital Image Watermarking Methods for Copyright Protection and Authentication**", PhD thesis, Information Security Institute, Faculty of Information Technology, Queensland University of Technology, March 2007.

[174] R.J. Anderson, "**Why Cryptosystems Fail**", Proceedings of the 1st ACM conference on Computer and communications security, pp. 215 - 227, Virginia, United States, 1993.

[175] B. Schneier "**Security Pitfalls in Cryptography**", Card Tech/Secure Tech Conference Proceedings, Volume 1: Technology, Card Tech/Secure Tech, Inc., pp. 621−626, 1998.

[176] A. Menezes, P. Van. Orschot, S. Vanstone, "**Handbook of Applied Cryptography**", CRC Press, 1996.

[177] W. Stallings, "**Cryptography and Network Security Principles and Practices, Fourth Edition**", Prentice Hall, November 2005.

[178] B. Schneier, "**Applied Cryptography**", 2nd edition, John Wiley & Sons, New York, 1996.

[179] N. Ratha, J. H. Connell, R. M. Bolle, "**An analysis of minutiae matching strength**", Proceedings of the Third International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA), Lecture Notes In Computer Science , Volume 2091 pp. 223–228, Sweden, June 2001.

[180] B. Schneier, "**Inside Risks: The Uses and Abuses of Biometrics**", Communications of the ACM, Volume 42, Issue 8, pp. 136, August 1999.

[181] N.K. Ratha, J.H. Connell, R. Bolle, "**Enhancing Security and Privacy in Biometrics-Based Authentication System**", IBM Systems Journal, Volume 40, Issue 3, pp. 614-634, March 2001.

[182] N. K. Ratha, S. Chikkerur, J. H. Connell, R. M. Bolle, "**Generating Cancelable Fingerprint Templates**", IEEE Transactions on Pattern Analysis and Machine Intelligence, Volume 29, Issue 4, pp. 561 - 572, April 2007.

[183] A. K. Jain, K. Nandakumar, A. Nagar, "**Biometric Template Security**" EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics, Volume 2008, January 2008.

[184] T. E. Boult, W. J. Scheirer, R. Woodworth, "**Fingerprint Revocable Biotokens: Accuracy and Security Analysis**", IEEE Conference on Computer Vision and Pattern Recognition (CVPR '07), pp. 1 – 8, June 2007.

[185] A. O. Thomas, N. K. Ratha, J. H. Connell, R. M. Bolle, " **Comparative analysis of registration based and registration free methods for cancelable fingerprint biometrics**", 19th International Conference on Pattern Recognition (ICPR 2008), pp. 1 – 4, Dec 2008.

[186] F. Farooq, R. Bolle, T. Jea, N. Ratha, "**Anonymous and Revocable Fingerprint Recognition**", IEEE Conference on Computer Vision and Pattern Recognition, 2007. CVPR '07, pp. 1 – 7, June 2007.

[187] F. Farooq, N. Ratha, T. Jea, R. Bolle, "**Security and Accuracy Trade-off in Anonymous Fingerprint Recognition**", First IEEE International Conference on Biometrics: Theory, Applications, and Systems (BTAS 2007), pp. 1 - 6, Sep 2007.

[188] J. Bringer , H. Chabanne , B. Kindarji, "**The best of both worlds: Applying secure sketches to cancelable biometrics**", Science of Computer Programming, Special Issue on Security and Trust, Volume 74, Issues 1-2, pp. 43-51, ISSN:0167-6423 , December 2008.

[189] Y. Sutcu, Q. Li, N. Memon, "**Secure Biometric Templates from Fingerprint-Face Features**", IEEE Conference on Computer Vision and Pattern Recognition (CVPR '07), pp. 1 - 6, Minnesota, USA, June 2007.

[190] A. K. Jain, K. Nandakumar, A. Ross, "**Score normalization in multimodal biometric systems**", Pattern Recognition, Volume 38, Issue 12, pp. 2270–2285, December 2005.

[191] Y. Sutcu, H. T. Sencar, N. Memon, "**A geometric transformation to protect minutiae-based fingerprint templates**", Biometric Technology for Human Identification IV (DS36), part of the SPIE International Defense and Security Symposium, Volume 6539, April 2007.

[192] E. Saatci, V. Tavsanoglu, "**Fingerprint image enhancement using CNN gabor-type filters**", Proceedings of the 2002 7th IEEE International Workshop on Cellular Neural Networks and Their Applications (CNNA 2002), pp. 377 - 382, July 2002.

[193] C. Hsieh, E. Lai, Y. Wang "**An effective algorithm for fingerprint image enhancement based on wavelet transform**" Pattern Recognition, Volume 36, Issue 2, pp. 303-312, February 2003.

[194] B. Moayer, K. Fu, "**A syntactic approach to fingerprint pattern recognition**", Pattern Recognition, Volume 7, Issues 1-2, pp. 1-23, June 1975.

[195] M.R. Verma, A.K. Majumdar, B. Chatterjee, "**Edge detection in fingerprints**" Pattern Recognition, Volume 20, Issue 5, pp. 513-523. ISSN: 0031-3203, 1987.

[196] S. L. Hsieh, H. C. Huang, I.J Tsai, "**A Copyright Protection Scheme for Gray-Level Images Using Human Fingerprint Images as Watermarks**", Third International Conference on Information Technology: New Generations (ITNG'06), Las Vegas, Nevada, pp. 482 – 489, ISBN: 0-7695-2497-4, April 2006.

[197] S. Jung, D. Lee, S. Lee, J. Paik, "**Fingerprint Watermarking for H.264 Streaming Media**", Frontiers in the Convergence of Bioscience and Information Technologies, Jeju Island, Korea, pp. 671 – 675, ISBN: 978-0-7695-2999-8, October 2007.

[198] S. Jung, D. Lee, S. Lee, J. Paik, "**Robust Watermarking for Compressed Video Using Fingerprints and Its Applications**", International Journal of Control, Automation, and Systems, Volume 6, no. 6, pp. 794-799, December 2008.

[199] S. Jung, D. Lee, S. Lee, and J. Paik, “**Biometric data-based robust watermarking scheme of video streams**”, Proceedings of 6th International Conference on Information, Communications and Singal Processing, pp. 1 - 5, Singapore, December 2007.

[200] G. Aguilar, G. Sánchez, K. scano, M.Salinas, M. Nakano, H. Perez “**Fingerprint Recognition**”, Proceedings of the Second International Conference on Internet Monitoring and Protection (ICIMP), P. 32, ISBN:0-7695-2911-9, California, USA, July 2007.

[201] I. T. Lam, C. M. Pun, “**Embedding Biometric Watermark on Document Image using Discrete Wavelet Transform**”, Proceedings of the 2009 IEEE International Conference on Information and Automation, pp. 583 – 588, Zhuhai/Macau, June 2009.

[202] L. Coetzee, E. Botha, “**Fingerprint recognition in low quality images**”, Pattern Recognition, Volume 26, Issue 10, pp. 1441-1460, October 1993.

[203] P. E. Danielsson, Q. Z. Ye, “**Rotation-invariant operators applied to enhancement of fingerprints**”, 9th International Conference on Pattern Recognition (ICPR), Volume 1, pp. 329 – 333, Rome, Nov 1988.

[204] R.P. Chiralo L. L. Berdan, “**Adaptive digital enhancement of latent fingerprints**”, In Proceedings Carnahan International Conference on Electronic Crime Countermeasures, pp. 131-135, 1978.

[205] L. O'Gorman, J. V. Nickerson, “**An approach to fingerprint filter design**”, Pattern Recognition, Volume 22 , Issue 1, pp.29-38, January 1989.

[206] T. Kamei, M. Mizoguchi, “**Image filter design for fingerprint enhancement**”, International Symposium on Computer Vision (ISCV 95), pp. 109-114, Coral Gables, FL, Nov 1995.

[207] K. Millard, D. Monro, B. Sherlock, “**Algorithm for enhancing fingerprint images**”, Electronics Letters, Volume: 28, Issue: 18, pp. 1720 - 1721, Aug. 1992.

[208] L. Zhou; Z.J. Haas, " **Securing Ad Hoc Networks",** Journal of IEEE Network ,Volume 13, Issue 6, pp. 24-30, Nov/Dec 1999.

[209] http://www.wireshark.org/, Last visit Sep 2009.

[210] R.A. Hummel, "**Image Enhancement by Histogram Transformation**", Comput. Graphics and Image Processing, Volume 6, Issue 2, pp. 184-195, 1997.

[211] D.J.Ketcham, R.W. Lowe, J.W.Weber, "**Real-time. Image enhancement techniques**", Proceedings of the Seminar on Image processing, pp. 120-125, Pacific Grove, California, February 1976.

[212] S. M. Pizer, "**Intensity Mappings for the Display of Medical Images"**', Functional Mapping of Organ Systems and other Computer Topics, Society of Nuclear Medicine, 1981.

[213] P. S. Heckbert, "**Graphics Gems IV**", Academic Press, 1994.

[214] R. Gonzalez, R. Woods, S. Eddins, "**Digital Image Processing Using MATLAB**", Pearson Prentice Hall, 2004.

[215] B.G. Sherlock, D.M.Monro, K.Millard, "**Fingerprint enhancement by directional Fourier filtering**", IEE Proceedings in visual image signal processing, Volume 141, Issue 2, pp. 87–94, Apr 1994.

[216] S.M. Pizer, E.P. Amburn, J.D Austin, R. Cromartie, A. Geselowitz, T. Greer, B. H. Romeny, J.B. Zimmerman, K. Zuiderveld, "**Adaptive Histogram Equalization and Its Variations**", Computer Vision, Graphics, and Image Processing, Volume 39, Issue 3, pp. 355-368, September 1987.

[217] N. Otsu, "**A Threshold Selection Method from Gray-Level Histograms**", IEEE Transactions on Systems, Man, and Cybernetics, Volume 9, Issue 1, pp. 62 – 66, Jan. 1979.

[218] S. G. Mallat, "**Multifrequency channel decompositions of images and wavelet models**", IEEE Transactions on Acoustics, Speech and Signal Processing, Volume 37, Issue 12, pp. 2091-2110, December 1989.

[219] D. Taskovski, S. Bogdanova, M. Bogdanov,"**Digital watermarking in wavelet domain**", University Sts.Cyril and Methodius, Faculty of Electrical Engineering,Karpos II b.b, Macedonia,1998.

[220] C.I. Watson, C. L. Wilson, "**NIST Special Database 4, Fingerprint database**", National Institute of Standard and technology, March 1992.

[221] C.I. Watson, "**NIST Special Database 14, Fingerprint database**", National Institute of Standard and technology, 1993.

[222] **FVC2004 : Third International Fingerprint Verification Competition**, 2004.

[223] **FVC2006 : The Fourth International Fingerprint Verification Competition**, 2006.

[224] D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman, A.K. Jain, "**FVC2000: Fingerprint Verification Competition**", IEEE Transactions on Pattern Analysis and Machine Intelligence**,** Volume 24 , Issue 3, pp. 402 – 412, March 2002.

Appendix

Publications

The following conferences papers, Chapter of the book and journal have been published containing the material based on the content of this thesis:

Preprints:

M. Sepasian, W. Balachandran, "Multibiometric cryptosystem for Wireless Application",

M. Sepasian, W. Balachandran, "Secure Fingerprint and Voice Transmission over Wireless Networks",

Published:

M. Sepasian, M. Bahmanyar, C. Mares, S. M. Azimi, W. Balachandran, "**Novel Fingerprint Image Enhancement Algorithm",** Chapter of the book in Advances in Electrical and Electronics Engineering - IAENG Transactions on Electrical and Electronics Engineering Volume I, Edited book published by IEEE Computer Society, pp. 243-251, ISBN: 978-0-7695-3555-5, 2009.

M. Sepasian, W. Balachandran and C. Mares, "**Image Enhancement for Fingerprint Minutiae-Based Algorithms Using CLAHE, Standard Deviation Analysis and Sliding Neighborhood**", World Congress on Engineering and Computer Science, ISBN: 978-988-98671-0-2, UC Berkeley, San Francisco, USA, 22-24 October, 2008.

M. Sepasian, W. Balachandran and C. Mares, "**Image Enhancement for Minutiae-Based Fingerprint Identification**", 37th IEEE Applied Imagery Pattern Recognition Workshop, pp. 1-4, ISBN: 978-1-4244-3125-0, ISSN: 1550-5219, Washington DC, USA, 15 October 2008.

S. Memon, **M. Sepasian**, W. Balachandran, “**Review of Finger Print Sensing Technologies**”, 12th IEEE International Multi topic Conference (IEEE INMIC 2008), Karachi, Pakistan, pp. 226 – 231, ISBN: 978-1-4244-2823-6, 23-24 December 2008.

M. Sepasian, C. Mares, W. Balachandran, “**Liveness and Spoofing in Fingerprint Identification: Issues and Challenges**”, Proceedings of the 4th WSEAS International Conference on Computer Engineering and Applications (CEA '10), ISBN ~ ISSN: 1790-5117, 978-960-474-151-9, pp. 150-158, Harvard University, Cambridge, USA, January 27-29, 2010.

M. Sepasian, C. Mares, W. Balachandran, “**Vitality Detection in Fingerprint Identification**”, International journal of WSEAS Transactions on information Science and Applications, Volume 7, Issue 4, pp. 498-507, ISSN: 1790-0832, World Scientific and Engineering Academy and Society (WSEAS) , Stevens Point, Wisconsin, USA, April 2010.