Novel Active Sweat Pores Based Liveness Detection Techniques for Fingerprint Biometrics

By

Shahzad Ahmed Memon

A thesis submitted for the degree

of

Doctor of Philosophy

Brunel University

School of Engineering and Design

April 2012

Abstract

Liveness detection in automatic fingerprint identification systems (AFIS) is an issue which still prevents its use in many un-supervised security applications. In the last decade, various hardware and software solutions for the detection of liveness from fingerprints have been proposed by academic research groups. However, the proposed methods have not yet been practically implemented with existing AFIS. A large amount of research is needed before commercial AFIS can be implemented.

In this research, novel active pore based liveness detection methods were proposed for AFIS. These novel methods are based on the detection of active pores on fingertip ridges, and the measurement of ionic activity in the sweat fluid that appears at the openings of active pores.

The literature is critically reviewed in terms of liveness detection issues. Existing fingerprint technology, and hardware and software solutions proposed for liveness detection are also examined. A comparative study has been completed on the commercially and specifically collected fingerprint databases, and it was concluded that images in these datasets do not contained any visible evidence of liveness. They were used to test various algorithms developed for liveness detection; however, to implement proper liveness detection in fingerprint systems a new database with fine details of fingertips is needed. Therefore a new high resolution Brunel Fingerprint Biometric Database (B-FBDB) was captured and collected for this novel liveness detection research.

The first proposed novel liveness detection method is a High Pass Correlation Filtering Algorithm (HCFA). This image processing algorithm has been developed in Matlab and tested on B-FBDB dataset images. The results of the HCFA algorithm have proved the idea behind the research, as they successfully demonstrated the clear possibility of liveness detection by active pore detection from high resolution images.

The second novel liveness detection method is based on the experimental evidence. This method explains liveness detection by measuring the ionic activities above the sample of ionic sweat fluid. A Micro Needle Electrode (MNE) based setup was used in this experiment to measure the ionic activities. In results, 5.9 pC to 6.5 pC charges were detected with ten NME positions (50µm to 360 µm) above the surface of ionic sweat fluid. These measurements are also a proof of liveness from active fingertip pores, and this technique can be used in the future to implement liveness detection solutions. The interaction of NME and ionic fluid was modelled in COMSOL multiphysics, and the effect of electric field variations on NME was recorded at 5µm -360µm positions above the ionic fluid.

Declaration

I declare that no part of the work referred to in this thesis has been submitted in support of an application for another degree or qualification in this or any other university or other institution of learning.

Shahzad Ahmed Memon

April 2012

.

Dedications

I would like to dedicate to ‘baba’ my late father who dreamed about my future and would have been proud to see me realise these ambitions. His care, training and the sacrifices he made to finance the education of all his children inspired me to achieve my goals.

To my mother, her love and prayers provide me with the strength to pass through difficult situations in my life.

To my sister baji Samina and brother Ashfaque, for their parental care after baba’s death and their trust and confidence in my decisions which have always provided me with support as I pursued my career.

For my brothers Imtiaz & Ishtiaque and their care and love for me.

My lovely niece Natalia, her angelic voice always made me relax and happy when I was stressed during my studies in the UK.

Acknowledgments

First of all, thanks to almighty Allah for providing me with the strength and capability to proceed successfully in the process of my research.

This thesis could not have been completed without the support I received from a number of people from inside and outside of the School of Engineering and Design. Perhaps it might be impossible to recall everyone, but there are a few people that stand out in the writer's memory to whom these acknowledgements are confirmed.

I would like to pay my gratitude to Professor Wamadeva Balachandran both for his encouragement of the research and his continued involvement and supervision throughout the process of my research. His critical suggestions always helped to improve my understanding of my research. I would also like to thank him for his continued guidance and help throughout my PhD.

I must also extend my thanks to Dr. Nadarajah Manivanan for his continued guidance and advice which provided me with immeasurable help in overcoming the difficulties I encountered during my research. His constant encouragement and recommendations during the process of my research helped to increase my confidence.

I am indebted to many of my colleagues for their help and support. I would like to thank Dr Jeremy C. Ahern for his valuable technical discussions and efforts in the development of an experimental rig for the research.

I am particularly grateful to Dr. Ruth Mackay for her valuable suggestions in the checking of my thesis structure and language.

I would also like to acknowledge Mr. Simon Lewis for his moral support, sincere efforts and taking the time to proof read my thesis.

Finally, I would like to pay my appreciation to the University of Sindh, Jamshoro, Pakistan and Higher Education Commission of Pakistan for providing the scholarship and other funds for my studies

Table of Contents

List of Figures

List of Tables

List of Acronyms

AFIS	Automatic Fingerprint Identification System
B-FBDB	Brunel-Fingerprint Biometric Database
CCD	Charge Coupled Deveice
CMOS	Complementary symmetry Metal Oxide Semiconductor
DA	Discrimination Ability
DE	Discrimination Efficiency
EGIF	Eccrine Gland Ionic Fluid
ESD	Electrostatic Discharge
FAR	False Acceptance Rate
Ffp	Fake fingerprint
FRR	False Rejection Rate
FTIR	Frustrated Total Internal Reflection
FOP	Fiber Optic Plate
FVC	Fingerprint Verification Competition
HCFA	High Pass Correlation Filtering Algorithm
LED	Light Emitting Diode
MEMS	Micro Electro-mechanical Systems
MNE	Micro Needle Electrode
NIST	National Institute of Standards and Technology
PolyU HRF	Polytechnic University-High resolution Fingerprint
RF	Radio Frequency
TFT	Thin Film Transistor

List of Publications

- **Memon, S**., Manivannan, N., Balachandran, W., and Boulgouris, N. 2012 "Fingerprint Sensors:Liveness Detection Issue and Hardware based Solutions" *Sensors & Transducers Journal*, vol. 136, issue 1, pp. 35-49.

- **Memon S**., Manivannan N., and Balachandran, W.,2011, "Active Pore Detection for Liveness in Fingerprint Identification System" *Proce. of the TELFOR 2011, IEEE 19th Telecommunications Forum* , 2011, pp. 619 – 622

- **Memon S**., Manivannan N., and Balachandran, W., "Liveness in Fingerprint Images by Active Pore Detection Technique" 2011, *Proce. of the ResCon'11, 4th Annual Research student Conference(20-22 June, SED, Brunel University)*, pp.75-77

- **Memon S**., Manivannan N., Boulgouris, N. and Balachandran, W.," Reference Patterns for Automatic Active Pore Detection in Fingertip Images", 2011, *Proc. of the World Academy of Science, Engineering and Technology (July 27-29, Paris, France),* Issue 79, pp. 707-710

- Manivannan N., **Memon S.**, Balachandran W. "Automatic detection of active sweat pores of fingerprint using High pass and correlation filtering" 2010, *IET Electronics Letters*, vol. 46 ,no.18, pp.1268-1269.

- Manivannan N., **Memon S.**, Balachandran W. "Security breaks a sweat" 2010, *IET Electronics Letters*, vol.46, no.18, pp.1241-1242.

- **Memon S.** , Balachandran W. "Low level ionic Current sensing Micro-tip", *Proc. of the Annual Meeting* of *IEEE Industry Applications Society (IAS) (Oct 3rd -7th, Houston, USA)*,pp.1-4

- **Memon S.** , Balachandran W. "Modelling of Current sensing Micro-tip", *Proce. of the NSTI,-Nanotech 2010 (June 21-24,CA, USA),* vol.2, pp.413-416.

- **Memon S.** , Balachandran W. (2009) " Fingerprint Sensing: Issues and Solutions" 2009, *Proce. of the ResCon'09, 2nd Annual Research student Conference (22-24 June, SED, Brunel University)*, pp 65-68.

- **Memon S.**, Sepasian M., Balachandran W. ,2008, "Review of Finger Print Sensing Technologies" *Proce. of the 12th IEEE International Multi-topic Conference (Dec23-24, Karachi, Pakistan)* pp.223-2226.

Chapter 1: Introduction

1.0 Background of biometrics

The term biometrics refers to the field of human identification. Individuals are identified using biological traits or behavioural characteristics as shown in Figure 1.1 [1]. Biological traits include fingerprint identification, facial recognition, iris recognition, palm prints and vein patterns. Examples of behavioural characteristics include vocal patterns, keystrokes, handwriting and gait recognition.

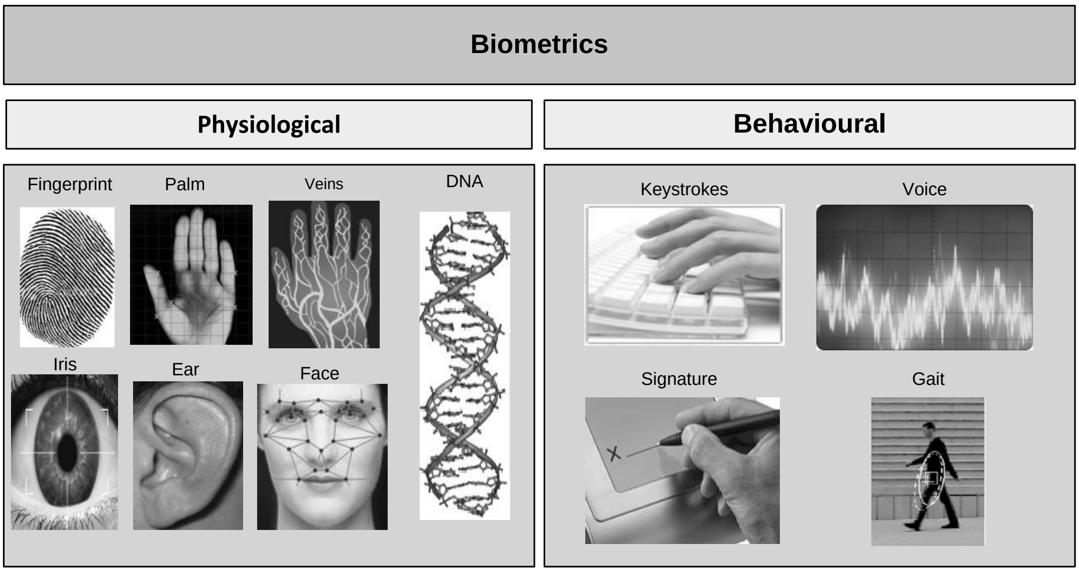


Figure 1.1 Types of biometrics

Biometric systems offer convenience and high level of security. Biometric identification based systems check identity rather than knowledge, for example a password or pin number or ownership of a key card [2]. People today regularly use passwords, however biometric identification offers a suitable and attractive option in order to validate a person’s identity. It has been shown that individual biometric characteristics are unique and cannot be transferred and information related to these traits cannot be lost, stolen or forgotten [3].

Within biometric technology the fingerprint is the most mature and trusted biometric identification method. It is one of the most developed biometric fields as a large amount of research and design already been undertaken [4, 5]. In addition, when compared to other biometric methods; it is relatively inexpensive and easily deployable with various systems. According to the report published by the International Biometric Group, in the next few years fingerprint technology will contribute to the generation of higher revenues as shown in Figure 1.2.

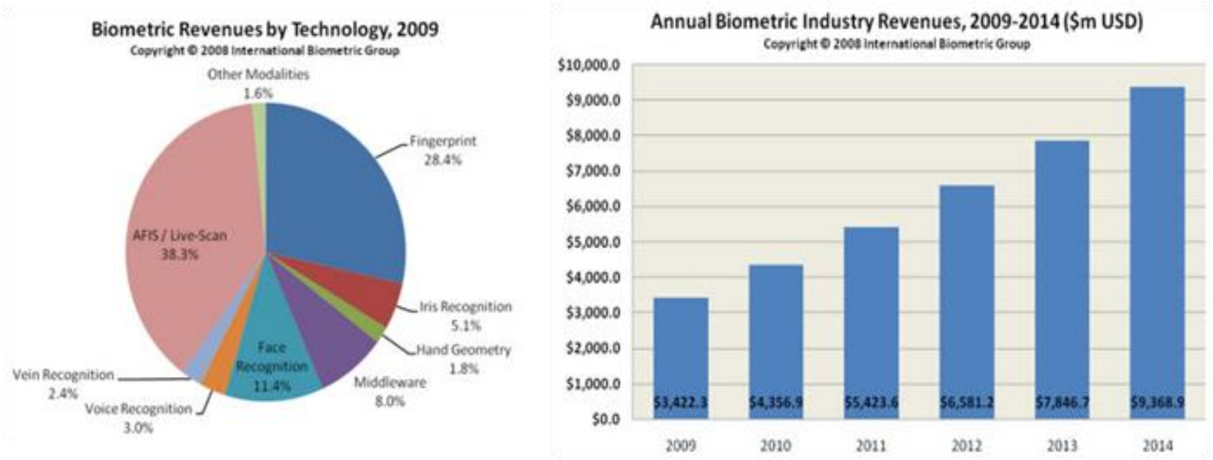


Figure 1.2: Market share for biometric technologies [6]

1.2 The fingerprint

The fingerprint is referred the image of finger tip (see figure 1.3), this is the visible pattern formed in the skin, and is absolutely unique to its own. Every person on earth has a different set of fingerprints. The details of these distinctive fingerprints are permanent even if they are damaged temporarily due to an injury such as cut to the skin. For this reason the fingerprint is accepted as secure, and is used for personal identification purposes around the world.

Fingerprints can be captured either by scanning an inked impression (on paper or card) of a fingertip and digitized with optical scanner or video camera or by using a live-scan fingerprint scanner which digitize the sensing tip of the finger directly. The fingerprint contains detailed pixel information from the friction ridges and valleys of the image (see Figure 1.3).

Figure 1.3: Fingerprint

1.3 Fingerprint spoofing

The fraudulent entry of an unauthorized person into a fingerprint recognition system by using a fake fingerprint sample is termed spoofing. The spoofing of fingerprint sensors was first revealed in a report published by Network Computing in 1998 [7]. The report addressed the vulnerability of fingerprint scanning devices in accepting fake fingers or lifted fingerprints. The test also found that four out of six devices were susceptible to fake finger attacks. To overcome this problem the fingerprint test must differentiate between a real and fake finger. Fingerprint spoofing is discussed further in Chapter 2.

1.4 Liveness detection

Liveness detection is a measure that determines whether or not the source of the image presented to a biometric sensor is from a living individual. The main reason for conducting liveness detection signs in fingerprint biometrics is to ensure that the sensor is capturing an image from real fingertip. It provides an extra level of security to the biometric system by working cooperatively with a matching algorithm that recognizes an enrolled user.

Although matching algorithms are highly successful in identifying the unique fingerprint biometric of an individual, they still lack the ability to determine whether the source of the image is coming from a live or a fake finger comprised of clay, silicon, gelatine or other materials.

1.5 Current liveness detection methods

The use of fake fingertips has shown that all fingerprint sensors based on different technologies were unable to distinguish artificial finger stamps from live fingertips. Commercially available automated fingertip identification systems (AFIS) should be able to detect when an artificial finger is placed on the sensor. In order to reject them, the system should take measurements to examine some other intrinsic features of live fingers than those of fingerprints. However, the manufacturers of fingerprint sensors typically do not mention whether or not these measures are actually implemented in emerging fingerprint sensors operational with AFIS.

In fingerprint liveness detection research several methods have been proposed in patents and published literature. Some are based on additional biomedical hardware to detect temperature, pulse, and heartbeat ,to the existing AFIS and other methods are based on software based fingerprint image processing for comparing the differences between images of spoof and real fingerprints captured with fingerprint scanners. The software based research is mainly tested on standard fingerprint databases such as NIST; however, the main disadvantage of these databases is that the fingerprint image does not contain clear signs of liveness that can differentiate it from a live or fake finger. According to the recently published reports and literature [7-10] it is clear that the issue of liveness detection still poses a big challenge to fingerprint biometrics.

1.6 Aims and objectives of research

The primary aim of this research was to investigate the features of the fingertip, and to develop a novel and implementable solution to liveness detection issue. In particular, attention has been devoted to the development of novel liveness detection techniques based on the activities of sweat pores on fingertip ridges. Many researchers have proposed liveness detection methods for fingerprint biometrics but according to published literature and patents, there has hitherto been no research carried out on the active sweat pore as a sign of liveness. Active pores are only available on live fingertips and they are extremely difficult to replicate. A critical literature review was completed on commercially available fingerprint sensing technologies in respect of their ability to detect liveness. The limitations of proposed additional hardware, and the software based liveness detection methods were also discussed. To support the theory of active pores and their role in liveness detection, a new high resolution live fingertip database was collected, with information on visible active sweat pores.

An image processing technique based on a high pass correlation filtering technique for detecting active pores from inactive pores as a sign of liveness. An experimental setup based on micro needle electrode was developed for the detection of ionic activities from a laboratory formulated sweat fluid for the detection of ionic activities as a means of discerning liveness.

1.7 The thesis structure

There now follows a brief description of the content and scope of the main chapters of the thesis.

Chapter 2 An in-depth critical literature review on the existing fingerprint sensor technologies, in terms of lack of liveness detection capability, is discussed. Hardware and software based solutions for liveness detection and their limits are also reviewed in this chapter.

Chapter 3: Commercially and specially collected fingerprint datasets are explained and features of each dataset are summarized in tables. Each dataset is critically reviewed and its usefulness in terms of liveness detection is discussed. A new high resolution fingertip database, Brunel Fingerprint Biometric Data Base (B-FBDB) which was specifically captured/collected and stored for this novel liveness detection research is also discussed in detail. Novel liveness detection algorithm known as High Pass Correlation Filtering Algorithm (HCFA) is explained in detail. The test results of HCFA on B-FBDB and other databases are presented in this chapter.

Chapter 4: This chapter contains the practical experimental results of the research. By using a Needle Microelectrode (NME) charges in sweat fluid, as a sign of liveness, are observed. This is achieved by using a prototype experimental setup. Details of the of the preparation of Eccrine Gland Ionic Fluid (EGIF), which was used as a substitute for actual sweat fluid, are explained in detail. Technical details of hardware used in the experimental setup and results of measurement are presented. Finite element modelling is conducted using COMSOL to understand the EGIF droplet and microelectrode interface.

Chapter 5: Concluding remarks are presented in this chapter, and further extensions that can be made with this project are also discussed.

1.8 Contribution in knowledge

As a result of this research the following main contributions are claimed:

- A critical literature review of :
    - commercially available fingerprint sensor hardware technologies with their liveness detection limitations;
    - Hardware and software solutions proposed for liveness detection;
    - Existing fingerprint datasets and their liveness detection limitations;
- Collection of a novel high resolution fingertip image dataset labelled Brunel Fingerprint Database (B-FBDB) with observable active sweat pores. It is claimed to be the first fingerprint dataset with information about active sweat pores.
- Development and testing of a novel High Pass Correlation Filtering based image processing algorithm to detect the active pores for fingerprint liveness detection. This technique effectively detects active pores in B-FBIG dataset images.
- A prototype experimental model, including a NME, to detect the charge in the surface of sweat fluid released from active pores on the fingertip. The experimental results also revealed that in future a micro/nano based electrode array can be add as a part of a liveness detection section with sensing elements. It is a novel idea to confirm and build the liveness detection at fingerprint sensor level.

Chapter 2: Literature Review

Within this chapter fingerprint characteristics and spoofing characteristics are discussed. A review of commercially available fingerprint sensing technologies follows and liveness detection issues are investigated. In addition, proposed hardware and software solutions for liveness detection are reviewed and practical limitations are discussed.

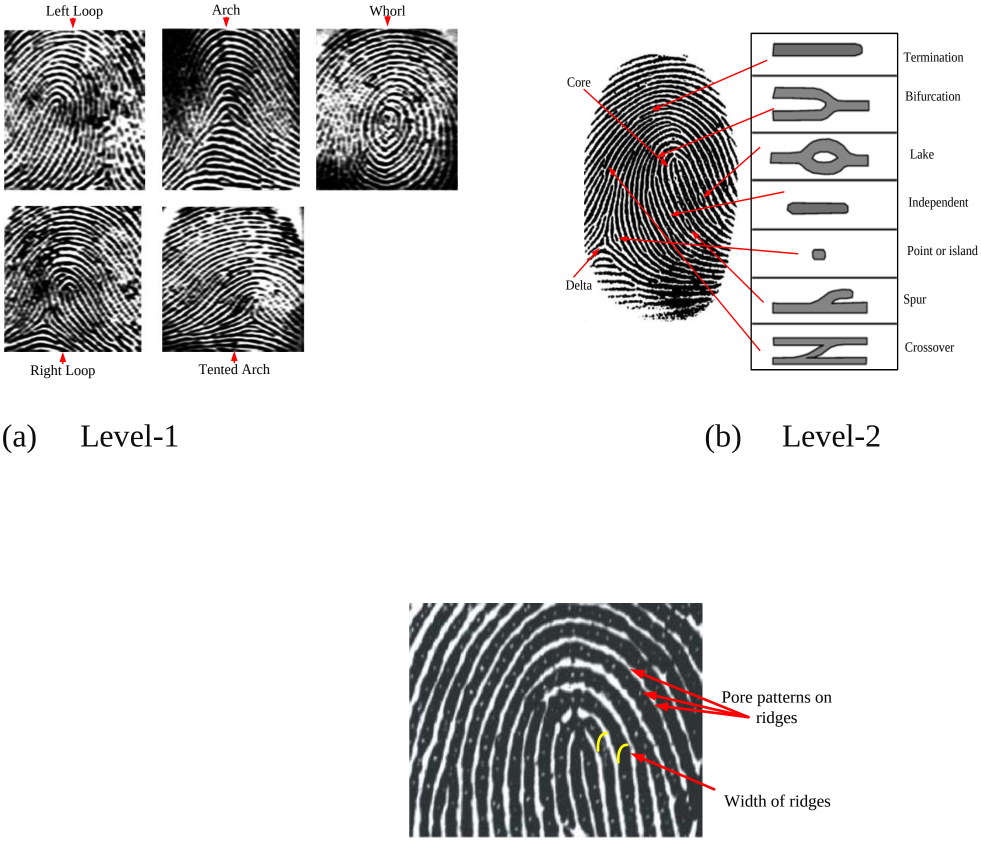
2.1 Fingerprint characteristics

These characteristics are categorized in three levels:

- Level-1 General ridge flow and patterns
- Level-2 Ridge ending, dots and bifurcation (known as minutiae)
- Level-3 Ridge contour points and pores

2.1.1 Level-1 characteristics

Level 1 includes the overall pattern formed by the flow of ridges, classification, ridge count, focal areas and orientation on the surface of the finger [5][11]. Level 1 characteristics are shown in Figure 2.1 (a)



(a) Level-1

(b) Level-2

(c) Level-3

Figure 2.1: Fingerprint characteristics

2.1.2 Level-2 characteristics

Level 2 refers to major ridge path variations, also known as minutiae. The location of the major changes in individual ridges such as ending, bifurcations, islands, dots, combinations, and their relationships [5]. These are the carriers of uniqueness because they follow a strong random path. Figure 2.1 (b), shows the minutiae on an actual fingerprint image. The flows of the black lines are called ridges. Spaces between the ridges are known as a valley. The flow of the ridges that continue or are divided constitute a particular fingerprint. An ending point is the point at which a ridge ends, and a bifurcation point is the point at which a ridge is divided into two ridges. The minutiae provide important information for the classification of an automatic fingerprinting system. There are other important points for bulk fingerprinting such as a core point at which the highest or lowest ridge occurs, Figure 2.1 b, or a delta where three ridges from three different directions converge.

2.1.3 Level-3 characteristics

Level 3 includes all dimensional attributes of a ridge such as ridge width, pore patterns (see Figure 2.1 (c) path deviation, edge counter, incipient ridges, breaks, creases and scars.

2.2 Automatic fingerprint identification system (AFIS)

The first live scan fingerprint system was introduced in 1988 [12]. The system was difficult to use and had many problems such as size and processing time. The declining cost of computing power and fingerprint sensors, along with the demand for security, efficiency, and convenience have made automatic fingerprint identification systems common, and they are frequently used in a large number of applications.

Automated fingerprint identification systems (AFIS) are primarily used by law enforcement agencies for criminal identification initiatives, the most important of which include identifying a person suspected of committing a crime or linking a suspect to other unsolved crimes [12]. AFIS captures, enrols and identifies a user in order to allow access to a specific system. The means by which a user may gain access to the specific system is based on four modules (See Figure 2.2):

- Fingerprint Sensor
- Signal processor
- Software interface
- Fingerprint Template database

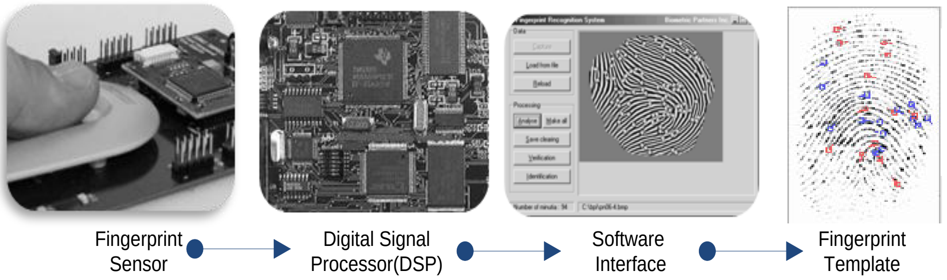


Figure 2.2: Functional modules of Automatic Fingerprint Identification Systems (AFIS)

The fingerprint sensor is an array of sensing elements based on optical, capacitive or radio frequency. The fingerprint sensor captures the image of a finger and then a fingerprint algorithm in a digital signal processor (DSP) unit runs image enhancement, template extraction and identification and/or authentication algorithms to match the captured image against stored templates.

2.3 Error rates in AFIS

Within the last decade, research and the practice of fingerprint matching and indexing has evolved the understanding of individuality, the information accessible in fingerprints and efficient ways of processing this information. Fingerprint matching is key to the system and affects the precision and efficiency of the whole system directly. Fingerprints are matched primarily on the fingerprint texture pattern. Two standard matching error rates are concerned with AFIS, these are the false acceptance rate (FAR) and fall rejection rate (FRR) [5, 13].

2.3.1 False Acceptance Rate (FAR)

The FAR is a measure of the possibility that the access system will mistakenly accept an access attempt; that is, will allow the access attempt from an unauthorized user.

$$(\%)FAR = \frac{fa}{n} \times 100\% \qquad (2.1)$$

fa = Number of incidents of false acceptance

n = Total number of samples

2.3.2 False Rejection Rate (FRR)

The FRR is a measure the percentage of authorized users that have not been able to enter the system

$$(\%)FRR = \frac{fr}{n} \times 100\% \qquad (2.2)$$

fr = Number of incidents of false rejection

n = Total number of samples

2.4 Fingerprint sensor spoofing techniques

Fingerprint spoofing methods were rigorously investigated by Matsumoto [7, 14]. In his research, Matsumoto explained in detail the process of making fake fingerprints using a mould of silicon, gum and gelatine (see Figure 2.3). The moulds were made in two distinct ways. In the first method, a mould was prepared by pressing a fingertip into a soft plastic, silicon or rubber. The indentation is then filled with liquid gelatine. After solidification it appears the same as the outer skin of the fingertip, with the same impression of ridges and valleys.

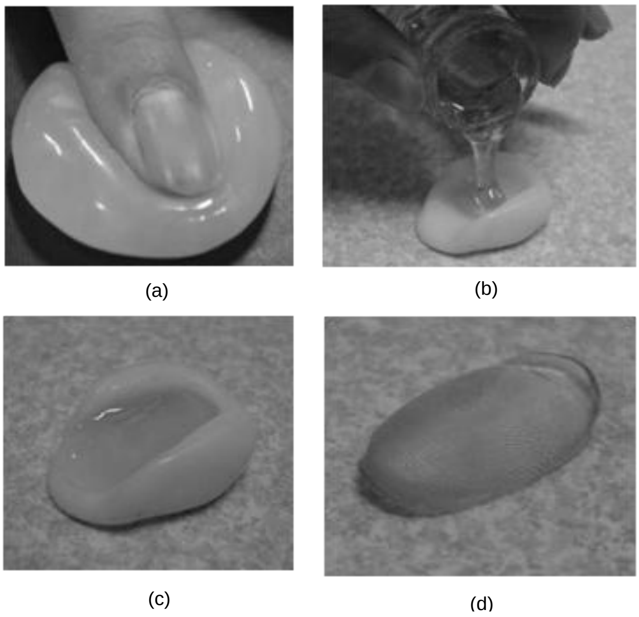


Figure 2.3: Process of making fake fingerprint from plastic/ silicon mould (a) Pressing of finger on soft plastic silicon/rubber mould (b) Dripping of liquid gelatine/rubber over mould c) Solidification d) Artificial fingerprint stamp [7, 14]

Matsumoto showed that 11 types of fingerprint sensors accepted gelatine fingers, which were easy to make with cheap, easily obtainable tools and materials. The images produced by these fake fingers can be accepted and processed by sensors as a real finger as shown in Figure 2.4.

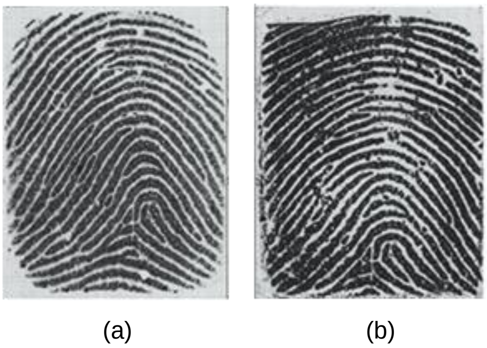


Figure 2.4. (a) Live finger (b) Fake/Gummy finger [15]

The second method for preparing fake finger stamps is illustrated in Figure 2.5 (a-d). This method captures an impression of a residual fingerprint on any surface. After imaging and processing, the fingerprint from the residue is used to create a mould on a plastic sheet.

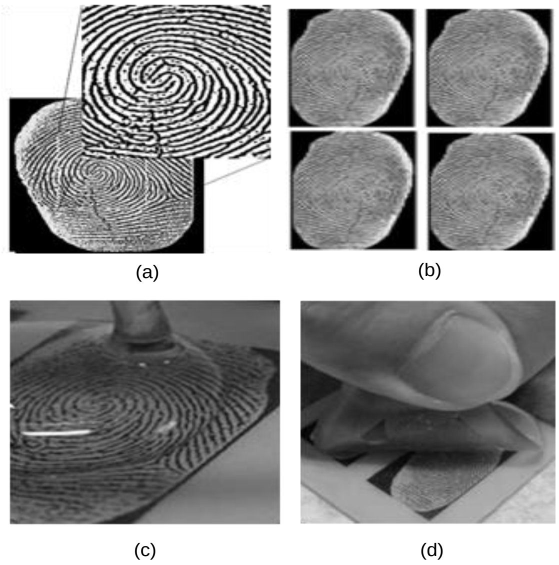


Figure 2.5 : (a) Imaging of fingerprint from residual fingerprint (b) Masking and printing of fingerprint (c) Masking and printing of fingerprint (d) Detaching of fake fingerprint stamp [14, 15]

In many tests, there was a high FAR with fingerprint readers using optical or capacitive sensors. In addition, fake fingers could be enrolled in the system (68–100% acceptance) [14, 15]. The test results on a variety of biometric devices demonstrated the vulnerability of these technologies [16, 17] .These fake finger stamps were tested on six capacitive, two optical, and one thermal fingerprint scanner device. For several capacitive based devices, they were able to retrieve the fingerprint from the scanner and create successful spoof fingerprints. Fake finger stamps can also be made with play-dough like materials, wood glue or latex. Some artificial fingerprints generated by wax casts and silicon moulds were able to deceive both the optical and thermal devices. In August 2003, two German hackers claimed to have developed a technique using latent prints on the scanner and converting them to a latex fingerprint [18]. They used graphite powder and adhesive tape to recover the latent prints that were digitally photographed, and then enhanced by using graphics software.

One recent publication [19] has shown new techniques of making 3D fake fingers (See Figure.2.6 a.) and fingerprints using materials such as glycerine supersede gelatine (See Figure.2.6 b). The glycerine based fake fingers have been tested on capacitive, optical and thermal sensors and they have been successfully enrolled and matched.

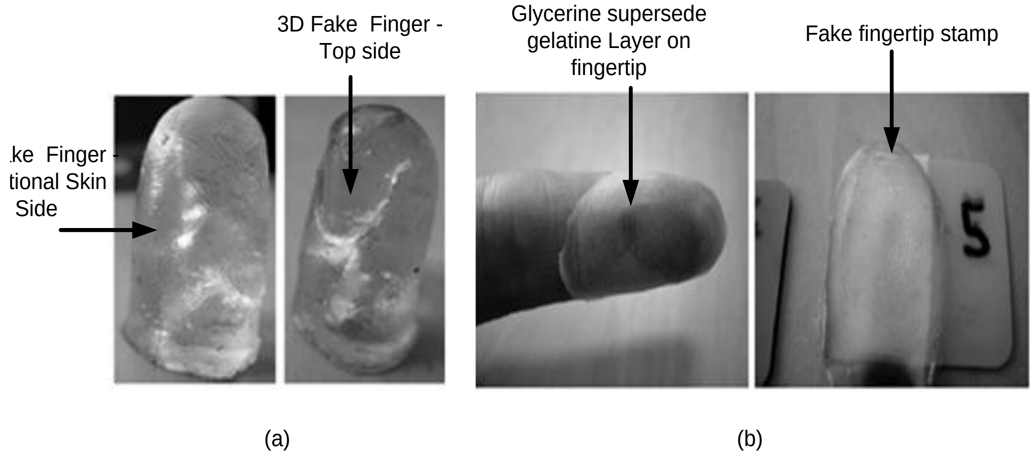
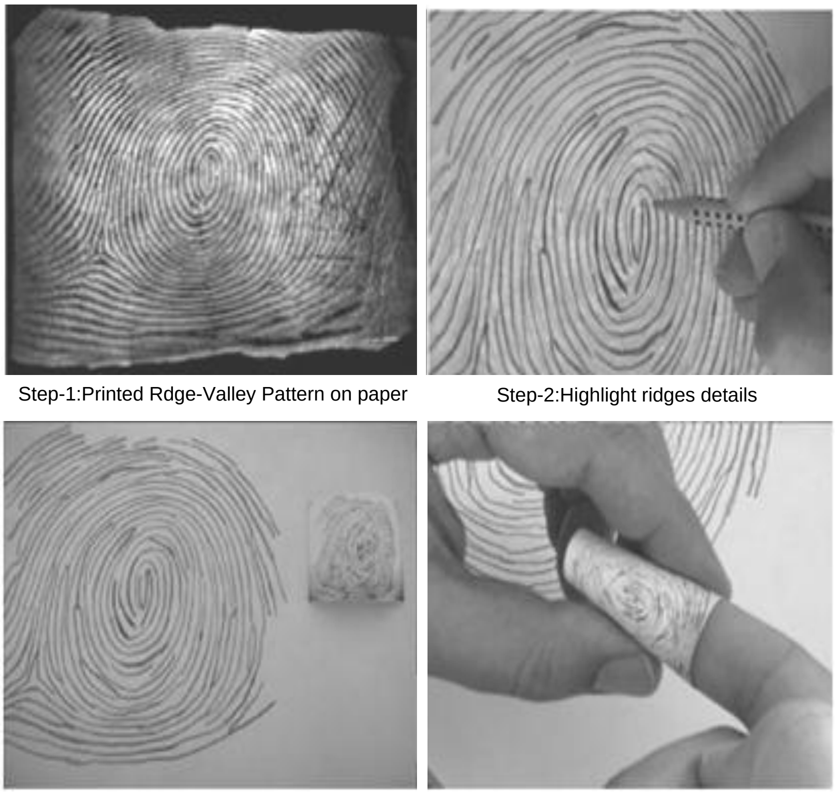

3D Fake Finger - Top side
.ke Finger - tional Skin Side
Glycerine supersede gelatine Layer on fingertip
Fake fingertip stamp
5
(a)
(b)

Figure 2.6. Glycerine supersede gelatine based fake finger and fingerprint (a) Glycerine based 3-D fake finger (b) Fingerprint samples [19]

Touchless surrounded imaging based fingerprint technique can be spoofed with a piece of paper containing prints of ridges and valley pattern of the finger [20]. The four step procedure of preparing fake fingerprint samples for touchless surrounded imaging is illustrated in Figure 2.7.



Step-1:Printed Rdge-Valley Pattern on paper

Step-2:Highlight ridges details

Step-3: Final pattern on paper

Step-3: Wrapping paper around finger

Figure 2.7. Four step process to prepare fake fingerprint to attack the touchless surrounded biometric system [20]

Much of the activity in spoofing biometric systems has, up until now, been confined to researchers. Moreover, as biometric systems become more widespread, the incentives to misuse or hack biometric systems will grow. Understanding the nature and risk of such attacks will become increasingly important to systems architects, administrators and security managers.

2.5 Fingerprint sensing technologies

The sensor is a key component of automatic fingerprint identification systems (AFIS). These sensors generally fall into two categories; area scan (touch) sensor and swipe sensor. When using a touch sensor, the user places and holds the finger on the sensor surface and an 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 .These square-shaped touch sensors are physically larger (in height and width) than swipe sensors. Touch sensors are found in places such as immigration access control applications. With a swipe sensor (a narrow row of sensors), the user slides a finger vertically over the surface [21]. These sensors are preferably used in portable consumer electronics because of their compact size and shape. However, swipe sensor technology inherently limits their suitability for some applications. These sensors require user training and practice to work reliably and they often fail to capture fingerprint images.

In both types of fingerprint sensors there are some common problems which still exist such as direct exposure to the environment, damage from mechanical effects, electrostatic discharge (ESD), thermal shock, and discrimination between a real or fake finger [22].

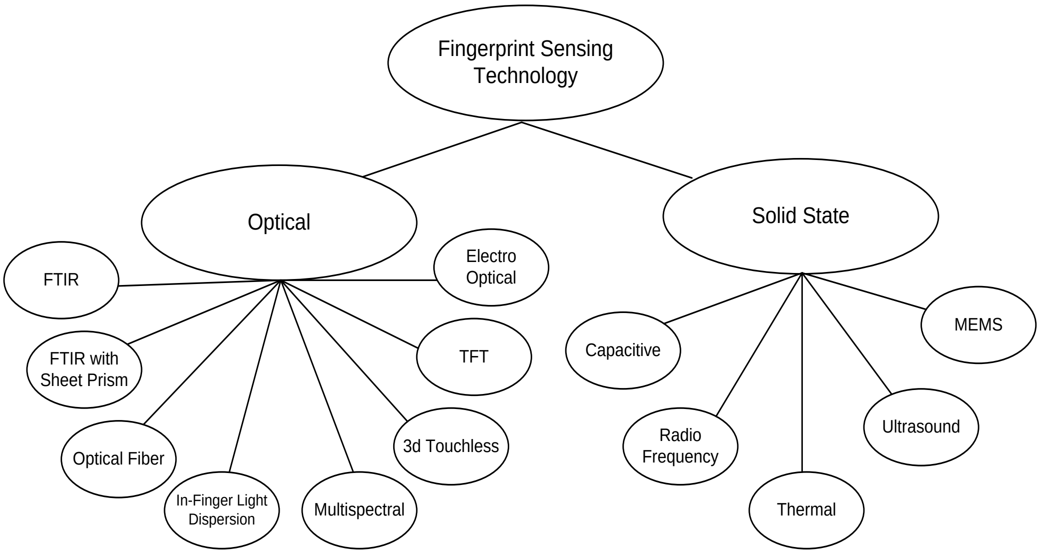


Figure 2.8: Fingerprint sensing technologies

Fingerprint sensing technologies are broadly divided in to two major categories, optical and solid state, as illustrated in Figure 2.8. The following section further explains each sensing technology with its advantages and disadvantages.

2.6 Optical sensors

Various fingerprint capture techniques, that use optical fingerprint sensors, have been introduced in last few years in a variety of security applications. In the following section major optical fingerprint sensing techniques are discussed in detail.

2.6.1 Frustrated Total Internal Reflection (FTIR)

FTIR is the oldest and most used live scan technique. The finger is placed on top of the prism as shown in Figure 2.9 (a) and is illuminated by a light source from one side. The light rays entering the prism are reflected at the valleys, and randomly scattered at the ridges of the finger as they are in contact with the prism surface. The lack of reflected light from the ridges (which appear dark in the image) can be distinguished from the valleys (which appear bright). The reflected rays are focused onto a CCD (charge coupled device) by an optical lens to form the image [23, 24]. Figure 2.9 (b) shows such an optical fingerprint sensor manufactuerd by MAXIS biometrics in 2009. The FAR of this optical sensors is <0.0001 and FRR is <0.01%. The image is captured with 500 DPI resolution

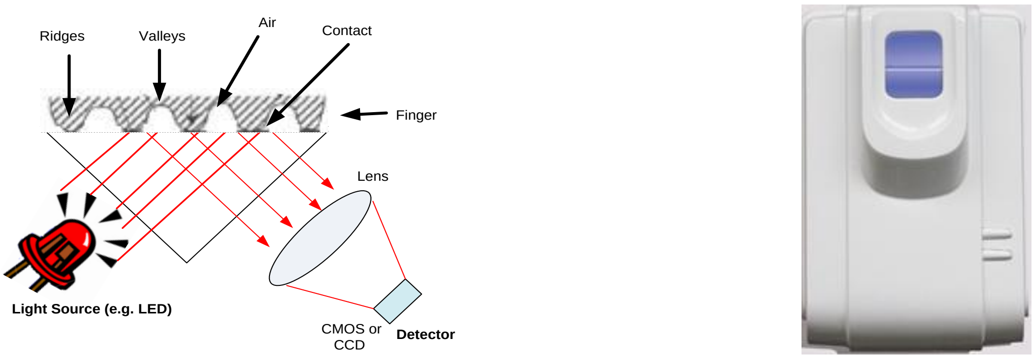


Figure 2.9: (a) FTIR mechanism [25] (b) MIAXIS FPR-620 optical fingerprint reader [26]

When compared to other fingerprint technologies, optical fingerprints sensors are robust and much less sensitive to adverse environmental effects such as mechanical shocks or electro-static discharge (ESD). However they are suscepectable to non-ideal skin conditions, and the image quality will be degraded, particularly if the skin is too dry or not in good contact with the sensor.

High resolution (500-1200 DPI) optical fingerprint sensors are commercially available [27] and they are used in various static access control systems. However; optical fingerprint sensors tend to be larger in size due to their sensing mechanisim, so they are not useful for mobile applications that require small sensors , such as in smart phones or tablet. Another drawback with these sensors is the latent fingerprints left by the previous user of the system. These can be copied and possibly used to prepare fake fingerprints to gain access to a system. In addition, FTIR based optical fingerprint sensors failed in many liveness detection tests [14]. This technology cannot distinguish between fake and original fingerprints because it only captures an image from the reflection of light from the surface of the finger skin without measuring the properties of the skin layer.

2.6.2 FTIR with a Sheet Prism

The sheet prism has a number of prisms adjacent to each other and each prism has a light entrance surface and an exit surface as shown in Figure 2.10. This sensor also operates on the same principle as FTIR. Although the prism size can be reduced the optical path remains the same [28]. However, this mechanism produces a poorer image quality than that of the traditional FTIR.

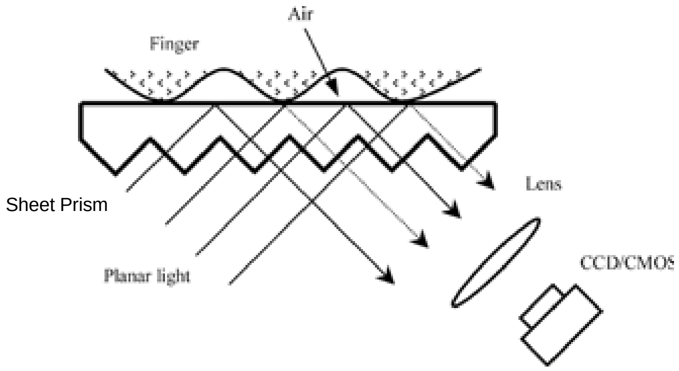


Figure 2.10 FTIR with sheet prism [28]

2.6.3 Optical Fiber Sensor

This technique employs a fibre-optic plate instead of a prism and lens. The fibre optic plate (FOP) consists of the array of optical fibres (See Figure 2.11).

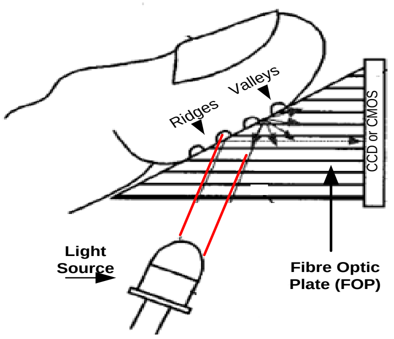


Figure 2.11 :Optical fibre based fingerprints sensor [29]

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 [29]. Therefore only the ridges scatter light, and the scattered light does not reach the Charge Coupled Deveice (CCD) or complementary symmetry metal oxide semiconductor (CMOS).

Near the valleys, light is reflected totally at the FOP air boundary and transmitted to the CCD/CMOS that is in direct contact with the FOP. 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 fibres. Furthermore, this technology is not fool proof from fake stamps.

2.6.4 In-Finger Light dispersion

In this relatively new sensing technique (see Figure 2.12). When a finger is placed directly onto the sensor it is illuminated by ambient light (available or existing light), and the optical imager chip senses the strength of the dispersed light that travels through the finger. The light from the valley part is dispersed in the air and becomes weak leaving the corresponding pixels darker [30]. A special proprietary glass surface over the imager chip ensures good imaging and protection.

It’s difficult to arrange the mechanisms of these sensors in compact form, since the focal length of small lenses can be very large, 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.

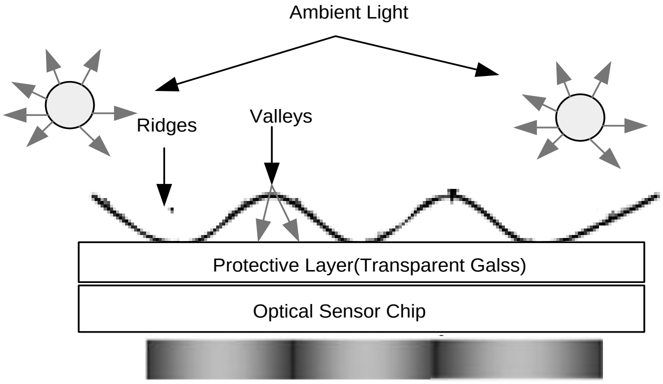


Figure 2.12: In-Finger light dispersion based fingerprint sensor [30]

2.6.5 Multispectral imaging

Multispectral imaging technology has been developed and introduced in optical fingerprints senosrs by Lumidigm Inc. USA. It is based upon the priciple that different wavelengths of light penetrates into the human skin to different depths and are absorbed differently by various chemical components of the skin [31]. Fingerprint sensors based on multispectral imaging technology collect multiple images of the surface and subsurface of the fingertip skin under a variety of optical conditions, and combine them to yield high-quality and complete fingerprint images [31, 32]. The group of raw images captured by this multispectral method is analyzed to ensure that the optical properties of the sample being measured match with those expected from a live finger [33].

The multispectral imaging system has two main modules: a multiple light source and an imaging system. These modules are designed and configured expressly to avoid the total internal reflection phenomena. The imaging mechanism of the multispectral technique is illustrated in Figure 2.13 (a). This technique utilizes multiple wavelength illumination sources rather than the monochromatic illumination commonly used in FTIR based fingerprint sensors. The orthogonal configuration of linear polarizers emphasise this multispectral light which penetrates the surface of the skin [34].

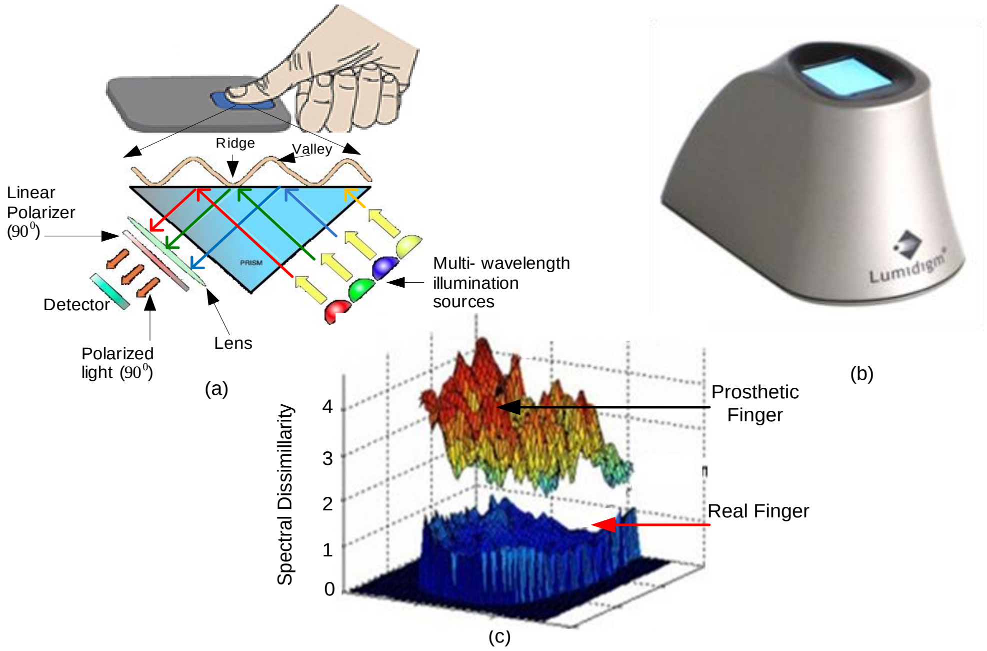


Figure 2.13 : (a) Principle of multispectral fingerprint imaging (b) Lumidigm Mercury Series M301multispectral imaging technology based fingerprint sensor [35] (c) Spectral dissimilarity test result [8, 36]

The light undergoes multiple scattering events before emerging from the skin towards the imaging array. In avoiding the optical phenomenon of FTIR, the multispectral imaging based fingerprint sensor is able to collect more identifying data from the finger than the FTIR based finegrprints sensor. Figure 2.13 (b) shows a commercially available multispectral imaging technology based fingerprint reader, Mercury Series M301 manufactured by Lumidigm inc USA in 2010.

The main advantage of this technique is that the combination of surface and subsurface imaging ensures that usable biometric data can be taken across a wide range of environmental and physiological conditions, such as wetness, bright ambient lighting, dry skin, various topical contaminants present on the surface of the finger, and poor contact between the finger and the sensor [32, 33]. In addition, they are very robust and relatively insensitive to adverse environmental effects, such as mechanical shocks or ESD, when compared to semiconductor fingerprint sensors. Moreover, this technique is claimed to be able to detect live tissues from non-living tissues or other organic or synthetic materials. An analysis of the surface and subsurface spectral charcterstics difference between a live finger and a prosthetic is illustrated in Figure 2.13 (c). These differences can be used to detetct prosthetics. However, this technology is deceieved by the use of fake fingers created with silicon and thermoplastic matirials [8].

2.6.6 3D touchless imaging

Compared to the flat touch-based fingerprint sensing systems, contactless or touchless fingerprinting is basically a remote sensing technique used to capture the ridge-valley patterns with no contact between the skin of the finger and the sensing area [20, 37]. The fingerprint representation using the touchless technology is different from the representation of the FTIR approach. While the latter method uses the optical principle of the reflection of the light (see Figure 2.14 (a)), the touchless approach produces mainly a photograph of the fingerprint [38]. Figure 2.14 (b) shows the touchless system with five cameras surrounding a finger. Knowing the position and orientation of each camera within a refence co-ordinate system, the five shapes or images are then projected into the 3D space and interpolated together to obtain the 3D shape of the finger [20, 38, 39]. The use of multiple views enables the capture of a full nail-to nail fingerprint that is faster than the traditional rolling procedures. Different views can be obtained by either different cameras surrounding the finger or one camera and a set of small mirrors.

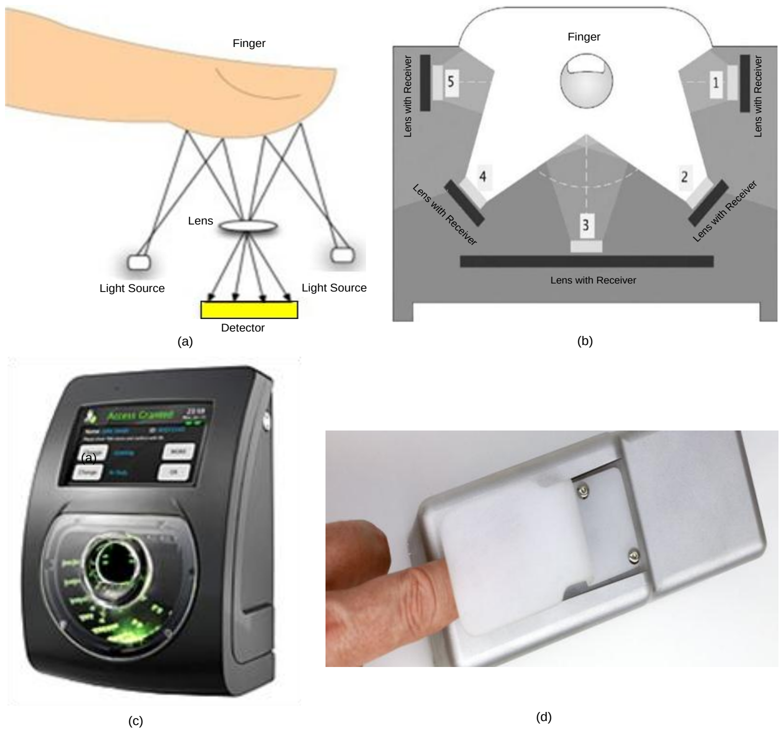


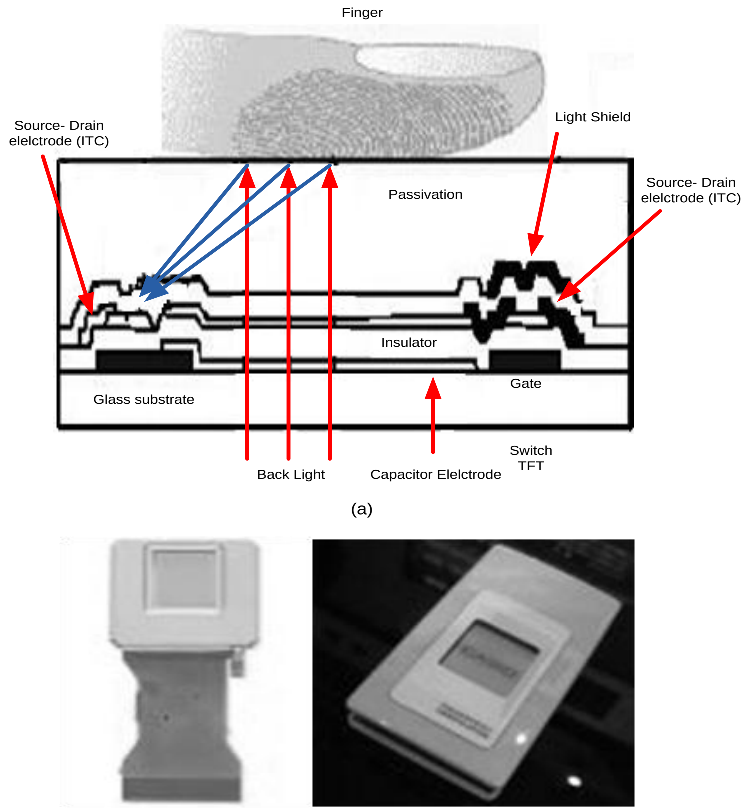
Figure 2.14: (a) Principle of toucless fingerprint imaging [40].
(b) Touchless finegrprint scanner with five optical sources and detect [20] (c) TBS 3DGuard Touchless fingerprint scanning Terminals [41, 53,46] (d) FlashScan 3D touchless fingerprint sensor [42]

Touchless fingerprint devices are already available on the market from Touchless Biometrics Systems (TBS) and FlashScan are shown in Figure.2.14 (c and d). However, due to their higher costs compared to other fingerprint sensing technologies, they did not generate sufficient interest in wide-spread use. This fingerprint technique tries to overcome the problem of the legacy optical capture technology, of the lack of contact between the finger and rigid surface [39, 42].The skin does not deform during the capture and the repeatablility of the measure is ensured. Nevertherless, in general, this new fingerprint scanning technology introduces some new challenges.The capture approach intrinsically provides system vulnerability and increases the risk of impostor intrusion, making it insecure and useless for access control or unattended applications. Also,lower image contrast, illumination, correct finger positioning and user convenience still need to be addressed.

Like the other optical imaging technologies, touchless fingerprint technology is not free from the liveness detction issue. In fact, it may be easier to fool this system than touch based optical fingerprint technology [20].

2.6.7 Thin Film Transistor (TFT) optical

Generally, TFT based optical detection techniques are used in facsimile and digital copying machines. In recent years, a TFT type optical detection sensor has been used as a fingerprint sensor. The TFT changes its electrical characteristics depending upon the presence of light incident on the device as illustrated in Figure 2.15(a) and two prototype sensors based on TFT are illustrated in Figure 2.15 (b).



(a)

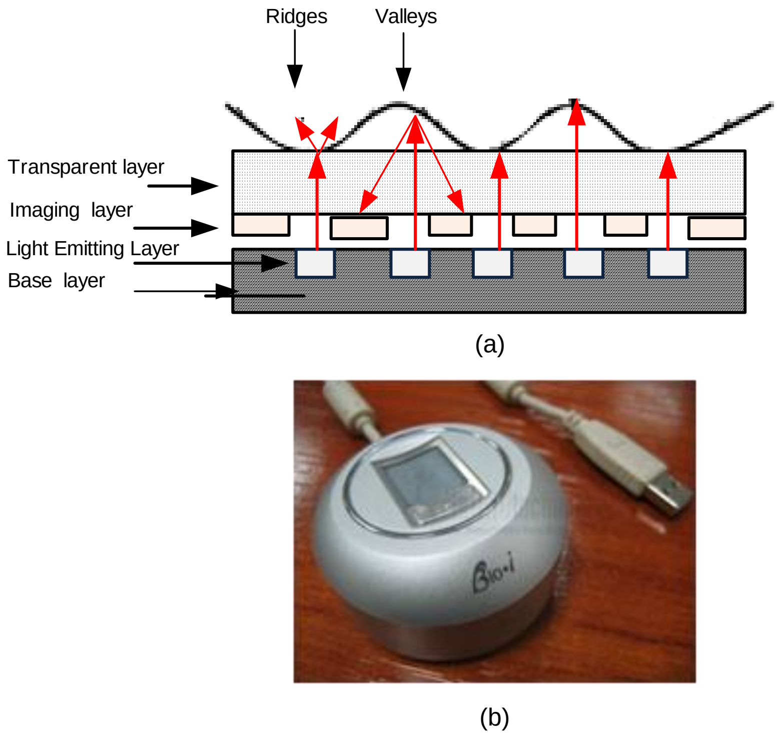
(b)

Figure 2.15: (a) Schemetic of TFT optical type fingerprint sensor [43] (b) Two optical TFT prototype from CASIO [25]

The optical detecting sensor comprises a window and a TFT sensor. Light which is generated by a light source passes through the window and reflects off the objects onto the TFT sensor. The TFT sensor generates optical current by detecting the reflected light [25]. The charges stored in the storage capacitor are transmitted by switching a TFT to an external driving circuit. In addition, a light-shielding layer for blocking light is formed over the semiconductor layer where the switching TFT is located.

TFT based fingerprint sensors could be a useful solution to integrate within touch display based applications because of their compactness and low power consumption; however, it is not possible to detect liveness from a finger placed on the TFT sensor. The reason for this is that the sensor just scans or copies the exterior layer of the fingertip, and this is not sufficient to detect liveness of the finger.

2.7 Electro-optical



(a)

(b)

Figure 2.16 : (a) Sensing principle of electro-optical fingerprint [43] (b) Bio-i CYTE fingerprint sensor manufactured by Testech, Inc[25].

In this system some polymers such as polyphenylene vinylene (PPV) and ploytiophene (PT) are able to emit light when properly excited with the proper voltage (usually a high voltage is required). This polymer is directly connected to a CMOS camera, which is a similar size to the finger (See Fig.2.16). Generally, the finger acts as the ground, and the polymer emits light where the ridges touch the polymer surface. As ridges touch the polymer, and the valleys do not, the potential is not even the same across the surface when a finger is placed on it, and the amount of light emitted varies, thus allowing a luminous representation of the fingerprint pattern to be generated and acquired by the imaging layer. This technology has not been tested, but as the basic principle of the technology is similar to that of TFT it can be assumed that it will not be of use liveness detection.

2.8 Capacitive

These sensors are made up of one or more semiconductor chips containing an array of tiny cells. Each cell includes two conductor plates covered with an insulating layer [44, 45]. The cells are slightly smaller than the width of one ridge on a finger, the average ridge width of a male is 0.48mm and a female 0.43mm [46]. The surface of the finger acts as a third capacitor plate, separated by the insulating layers in the cell structure and, in the case of the fingerprint valleys, a pocket of air. Varying the distance between the capacitor plates (by moving the finger closer or further away from the conducting plates) changes the total capacitance of the capacitor. It is because of this feature that the capacitor in a cell under a ridge will have a greater capacitance than the capacitor in a cell under a valley (See Figure 2.17) [47].

The array of pixels is used to map the fingerprint image based on the ridge and valley structure. The distance between the array of pixels and the finger should be very low i.e., the coating must be as thin as possible (a few microns), in order to provide enough sensitivity.

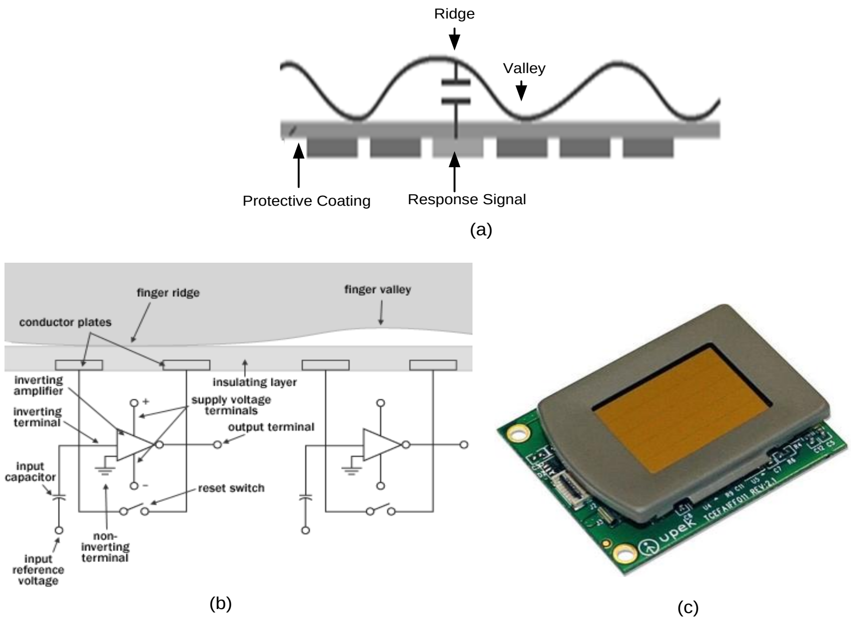


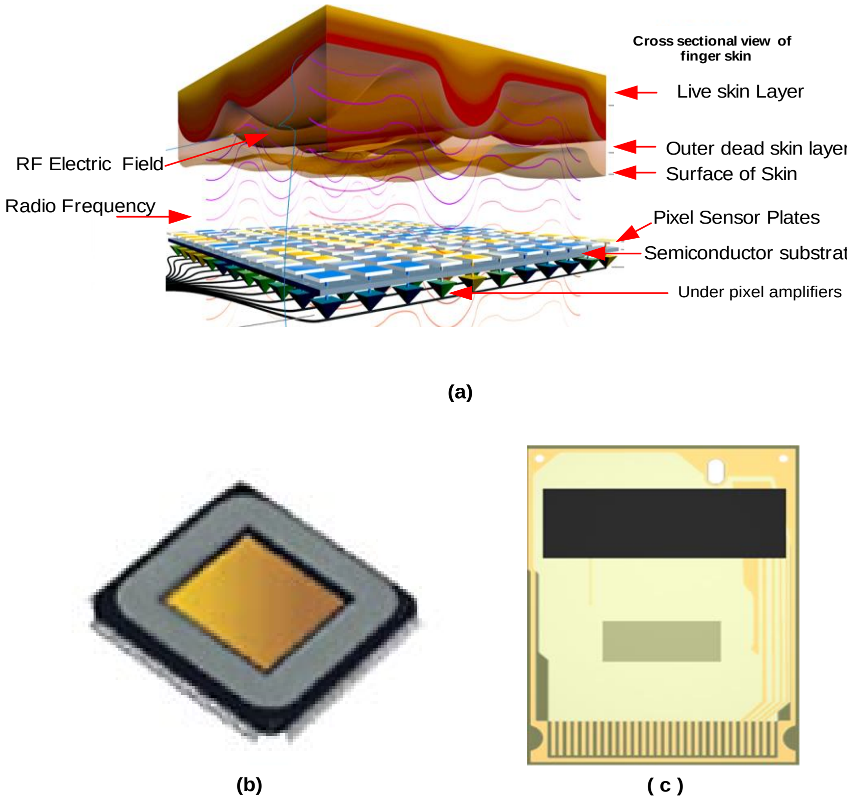
Figure 2.17: (a) Capacitive Fingerprint Sensing mechanism (b) Capacitance detection circuit [48] UPEK's TCS1 TouchChip Fingerprint Sensor [49]

The surface layer of the fingertip skin, which the capacitive fingerprint sensor detects is prone to damage and contamination in the course of everyday activities. Since, the dielectric constant of the surface layer is mainly due to moisture in the dead cells, ridges in dry fingers will have dielectric constants very close to air, resulting in very faded images. In addition, the capacitive sensing is vulnerable to strong external electrical fields, the most detrimental being ESD.

The simple measurement of the surface characteristics of the skin causes capacitive sensors to be most vulnerable to spoofing. They scan the surface of the fingerprint only, using dielectric measurements to distinguish between the ridges and valleys of the outer dead skin layer of the fingertip. Capacitive fields do not penetrate very far into the skin and can only image the surface of the finger tip, which is not sufficient to detect liveness. Capacitive fingerprint technology has failed in many liveness detection tests and can be easily spoofed with fake finger stamps [50]. The main advantages of capacitive sensors are their compact size and low cost. In market place Veridicom, Fujitsu, Infineon, Sony, Upek, Hitachi, LighTuning, Melfas, Atrua, NTT and Symwave, etc. are the major manufacturers of capacitive fingerprint sensors.

2. 9 Radio Frequency (RF)

In radio frequency based fingerprint sensing methods a radio frequency (RF) signal is injected into the finger from one side. A field will be created by RF signal between the finger and the adjacent semiconductor that mimics the shape of the ridges and valleys of the finger‘s epidemal layer, and the signal is received by a pixel array on silicon. These pixel arrays act like antennas (see Figure. 2.18 a) [51]. These antennas measure the skin’s subsurface (the live layer of skin) features by generating and detecting linear field geometries of the live layer of skin cells originated beneath the skins surface. This is in contrast to the spherical or tubular field geometries generated by a simple capacitive sensor, which only read the very top surface of the skin [52]. As a result, fingerprints that are difficult or impossible to acquire using capacitive sensors can be successfully acquired with RF Technology. The signal strength on the reciever pixel will depend on the capacitive/resistive connection between the source and the pixel reciever. An underpixel amplifier is used to measure the signals.



(a)

(b)

(c)

Figure 2.18: (a) Principal of operation of RF field sensing Fingerprint Sensor [43] (b) Authentic AES 4000 RF based finegrprint [52] (c) Valadity Liveflex VFS 201 Sensor [53]

Images obtined by RF technique, that accurately correspond to the pattern of the fingerprint, are clearer in quality compared with resulting images produced by optical or capacitive techniques. This technique is highly resistant to ESD, and it allows the sensor to acquire images from finger surfaces with dirt, oil, scars, cuts, or other impurities that can effect other technologies, thus improving the accuracy and reliability of the sensor. Despite being the newest form of fingerprint biometrics, it is also the most popular and more than 8 million RF fingerprint sensors are in use today[20]. Figure 2.18 (b) illustrates an authentic TruePrint® RF technology based AES 4000 fingerprint sensor. Validity‘s live flex® RF technology fingerprint sensor based on RF is depicted in Figure 2.18 (c), it uses 18-24 MHz frequency to capture image of fingertip. The FAR of live flex technology is <1:100,000, and lowest FRR < 1:500.

Despite the many advantages RF sensors fail when the sensor surface is wet. This is because they measure fingertip features very close to the surface of the skin (tens of microns), making the technology almost as susceptible as capacitive sensors to worn or missing skin features.

Manufacturers claim that RF based fingerprints sensors are very hard to spoof with fake fingerprints. Even though spoofing a RF fingerprint sensor takes a little more sophistication, spoofing is easy when proper materials are used [54]. RF fingerprint scanning technology utilizes conductive or live layer of skin beneath fingertip surface; however, a gummy finger can still successfully fool of the scanner because of the conductance. The properties of a properly made gummy finger are similar to that of a real and live finger.

2.10 Thermal

Thermal fingerprint sensors consist of an array of pyro-electric material based sensing elements. The pyro-electric materials (tourmaline, lithium sulphate monohydrate etc) generate voltages on the temperature differentials. Figure 2.19(a) illustrates the cross sectional view of a thermal fingerprint sensor. It scans only the surface skin of a fingertip by measuring the heat transferred from the sensor array to fingertip. When the sensor surface heats up, it creates a temperature difference between itself and the finger. The ridges of the fingertip touching the sensor draws heat away from the sensor faster than the valleys, which are separated from the sensor by insulating air (See Figure 2.19 (b)); therefore, the sensor detects the ridge-valley pattern or image of the fingertip [55].

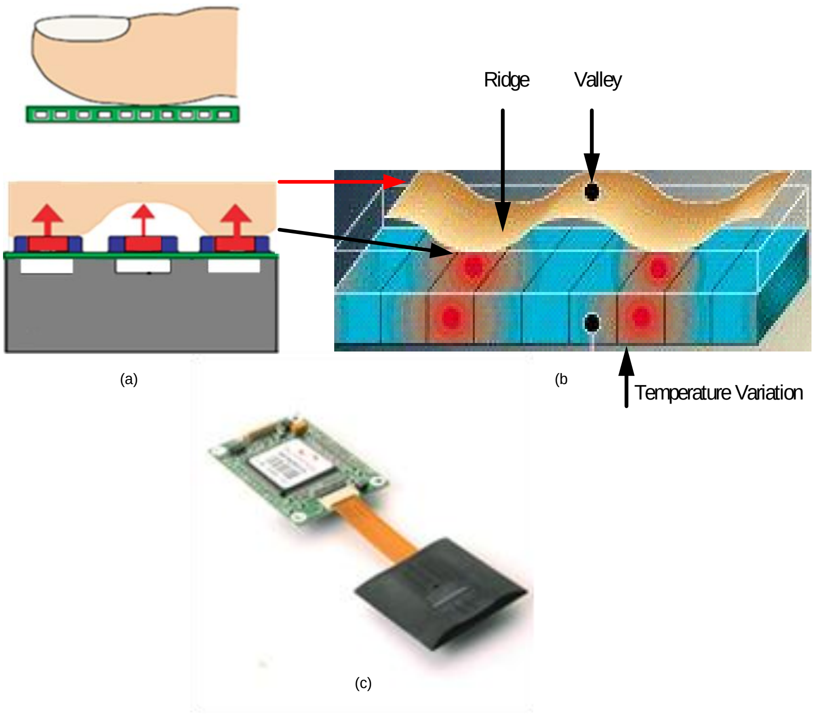


Figure 2.19:(a) Thermal Fingerprint Sensor [56](b) Sensing mechanism [25] (c) Atmel AT77C104B FingerChip™ Swipe fingerprint sensor[57]

When a finger is placed on the thermal fingerprint sensor, there is a significant change of temperature, and therefore signal, but after a short period (less than a tenth of a second), the image vanishes. Once the finger and the sensor chip have reached thermal equilibrium, there is no change in temperature, so there is no signal [55]. Therefore, it is necessary to avoid the possibility of a thermal equilibrium between the sensor and fingertip surface.

The main advantages of thermal sensing based fingerprint sensors is that they operate well under extreme environmental conditions, such as extreme temperatures, high humidity, oil and dirt. However, any heating of the sensor array increases the power consumption which, for portable devices, can significantly shorten battery life.

Thermal sensing methods are commercially less common and only one exists, the Atmel FingerChip™ thermal fingerprint sensor, which is illustrated in Figure 2.19 (c) It is based on the swiping method, which has the benefits of self-cleaning, and no latent fingerprint. However, the image quality depends on user’s skill in using the sensor, and they are currently the only reasonable option for portable consumer electronics such as cell phones and laptop computers.

Thermal fingerprint sensing technology is also incapable of differentiating between a fake and live fingertip because it can only scan the surface of the fingertip, and the variation between temperatures does not differentiate between live ridges-valleys or fake ridges-valleys. In liveness detection tests, the thermal sensor was easily spoofed by silicone rubber fingers [55, 58].

2.11 Ultrasound

Ultrasound sensors employ acoustic signals transmitted towards the fingertip surface. Acoustic waves travel at different speeds though ridges and air lodged under the skin. The reflected acoustic signal (echo) is captured by a receiver, which generates the fingerprint image [59] (See Figure. 2.20).

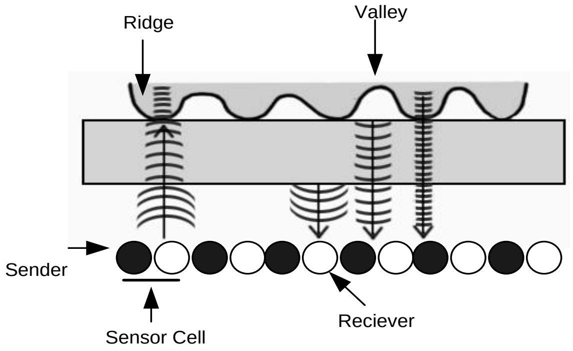


Figure 2.20: Principles of ultrasound fingerprint sensing [43]

The main advantage of this technology is that it can read the sub-surface of the skin rather than the surface only. Ultra-sound fingerprint sensing is not very common in the market place, because of its big size and high cost [5]. It includes mechanical parts and takes around two seconds to generate the image; therefore this technology is not suitable for large production. However, it has demonstrated that it is much more tolerant to external conditions that cause poor biometric image quality in optical or capacitive systems, such as ambient light, humidity, extreme temperatures and ESD.

There are still some issues with ultrasonic fingerprint scanning, such as poor image quality and susceptible to spoofing [59]. Ultrasonic fingerprint scanners can be compromised by soft artificial material such as gelatine that have the same echoing characteristics as fingers.

2.12 Micro-Electro-Mechanical Systems (MEMS)

Micro Electro-Mechanical System (MEMS) technology based devices in recent times shown interest in fingerprint acquisition systems as it is now possible to design and fabricate extremely small silicon switches [72, 73, 74]. Figure 2.21 (a) illustrates a 3D model of MEMS technology based fingerprint sensor and Figure 2.21 (b) depicts the SEM image of micro switches. The basic sensing principle is, when the ridge touches two adjacent tabs, the switch closes. It remains open when they are under a valley. The sensing method is illustrated in figure 2.21 (c) The ridge of a finger surface pushes the protrusion down, and the protrusion deflects the upper electrode. The deflection of the upper electrode increases the capacitance between itself and the lower electrode. The capacitance is detected by the sensing circuit just under the lower electrode [60].

On the other hand, the valley of a finger surface does not push the protrusion, and the capacitance is kept small. Therefore, the capacitance under a ridge Cr is larger than that under a valley Cv. This relationship Cr > Cv is translated into digitized signal levels. With this sensing, the detected signals from all the pixels generate one fingerprint image.

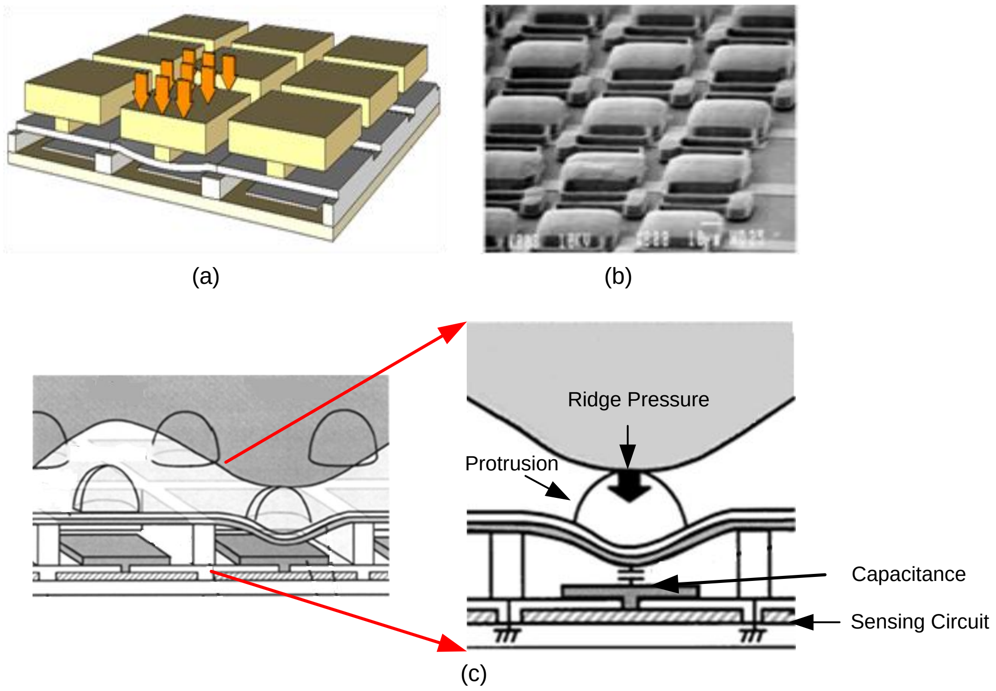


Figure 2.21: (a) 3D view of MEMS fingerprint sensor [61] (b) SEM Images of MEMS fingerprint sensor [25] (c) Principle of MEMS fingerprint sensors[60, 62]

Significant characteristics of this technology such as durability, low power consumption, being resistant to ESD, small in shape, and a direct binary output, lead to only minimal information of fingerprints [60]. However, one significant issue with this technology is the surface coatings, which protects the switches from dust or other environmental effects.

Although no liveness tests on MEMS based fingerprint sensors has been reported in literature, from their mechanism, they are not able to differentiate between fake and real fingertips placed on the sensor. This is because, it is possible to replicate ridges and valleys on fake silicon/gelatine based finger with same shape, size and weight and it is likely to apply the same pressure as of a real finger, therefore the sensor would not be able to differentiate between the pressure of a real and a gummy finger. No further development has been done with this technique beyond the laboratory. NTT Microsystem Integration Laboratories in Japan and Michigan University are currently working with this technology [61].

Among the commercial sensors available in the market, some vendors offer liveness detection features as an option, although no fingerprint system currently available is 100% fool proof. A false-accept occurs when a submitted template is incorrectly matched to a template enrolled by another user [5, 63]. This only refers to a zero effort attempt, i.e., an unauthorized user making an attempt with his/her own biometric to gain access to a system. If the false acceptance ratio is kept low, then the probability of a specific user with criminal intent matching another template is very low. The false acceptance ratio does not give information on the vulnerability of a system to spoof attack, beyond this probability.

The performance of many of the existing fingerprint sensors is subject to spoofing (fake and dummy), and identification and authentication is limited to 85%. As fingerprint sensors are basically an array of sensing elements and majority of sensing elements are made with solid state semiconductor materials with electrical and optical properties.

Many patents and proposals recommended in the last decade recommend the use of external hardware with fingerprint sensors for liveness detection. Also a vital amount of research has been done on the fingerprint algorithms to detect liveness from images. The following section reviews the proposed additional hardware and software based approaches to detect liveness.

2.13 Proposed Liveness Detection Techniques for Fingerprint Biometrics

Many patents and proposals recommended in the last decade recommend the use of external hardware with fingerprint sensors for liveness detection. Also a vital amount of research has been done on the fingerprint algorithms to detect liveness from images. The following section reviews the proposed additional hardware and software based approaches to detect liveness [22].

The reported hardware and software based liveness detection techniques are classified and illustrated in Figure 2.22.

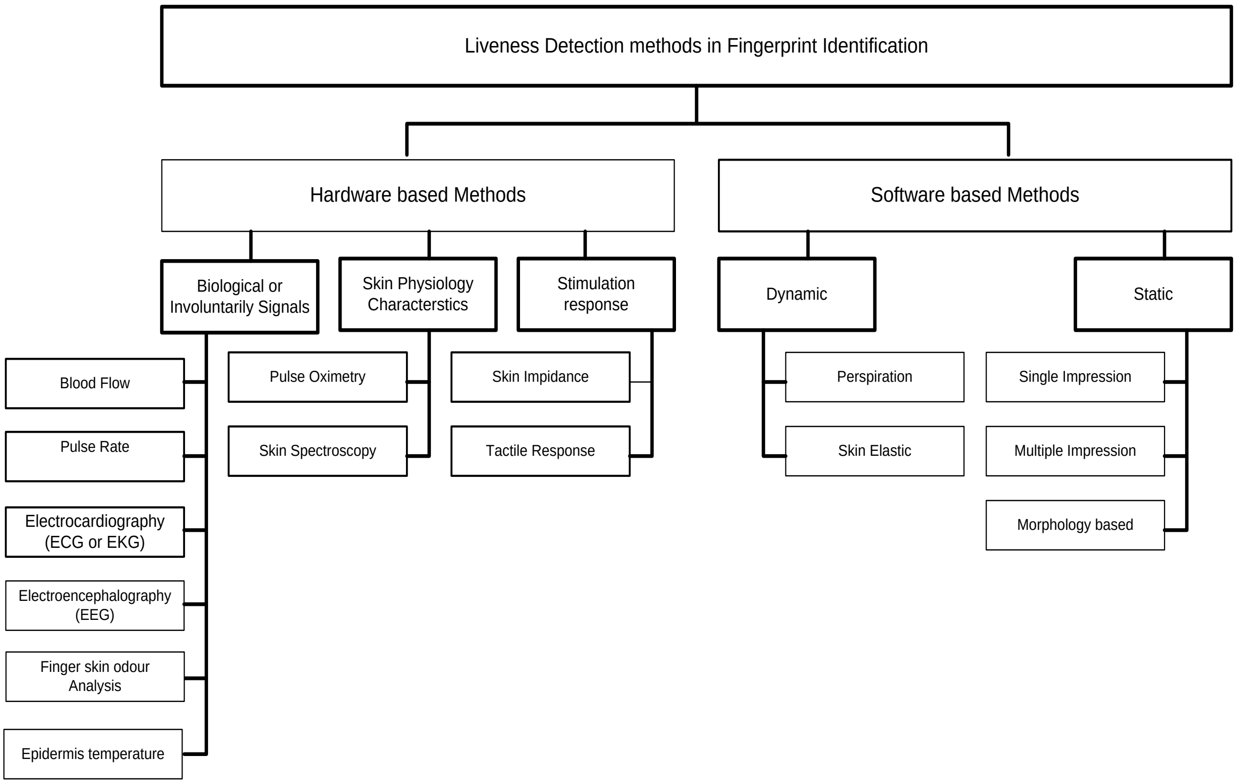


Figure 2.22:Proposed Liveness Detection Methods for fingerprint Biometrics

2.14 Hardware based Liveness Detection Methods

Detection of liveness patterns is one method in which physiological traits are identified in order to ensure that the image received by the biometric sensor is coming from a living source. It can be achieved by using extra hardware to acquire liveness signs.

A living human body generates many biological signals that can be measured at different points on the surface of the body. Some of the biological signals can be detected and measured from the finger tip of a person. Most of the hardware based liveness detection techniques recommended in literature use biomedical sensors to verify liveness. The following techniques were suggested from different researchers to overcome the liveness issue in fingerprint sensors.

2.14.1 Pulse oximetry

Pulse oximetry is used in the medical field to measure the oxygen saturation of haemoglobin in a patient's arterial blood [11, 27]. In this method the pulse and blood oxygenation are measured by shining the beams of light through the finger tissue (See Figure 2.23).

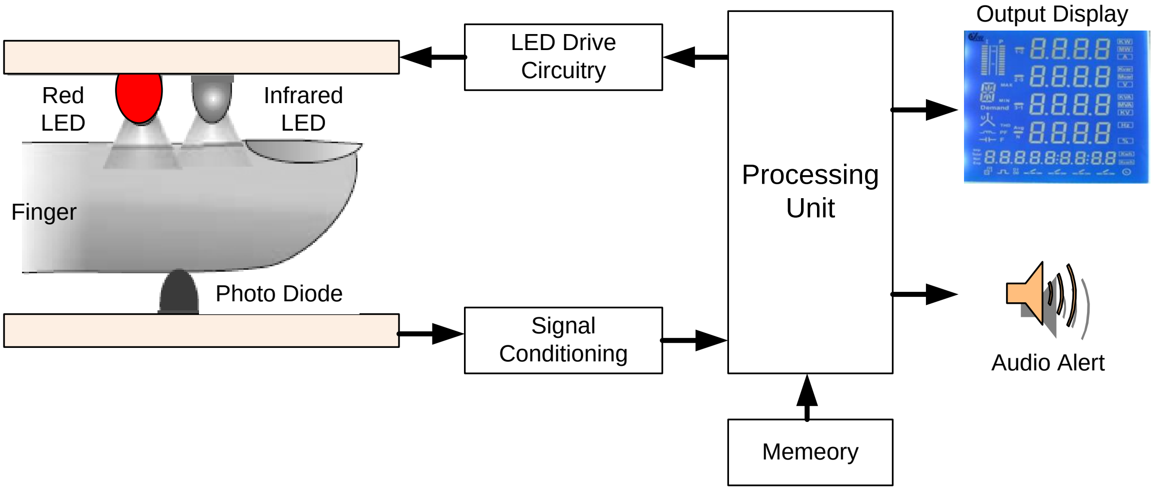


Figure 2.23: Pulse Oximatery Technique

The oxygenated haemoglobin allows red light to transmit through and absorbs more infrared light while the deoxygenated haemoglobin allows infrared to transmit through and absorbs more red light. Usually, a finger is placed between the source light emitting diode (LEDs) and the receiver (photodiode) acts as a translucent site with good blood flow. Once these absorption levels are detected from the finger, the ratio of absorption at different wavelengths can be obtained.

The advantage of this method, inherent in its origin, is the well known principle of pulse oximetry, which is especially used in medicine; however, it takes a long time for scanning pulses and possibly the measurements will fail in cold weather because of the lack of microcirculation in the fingertip. In addition, it can easily circumvent with the use of a thin fake finger layer made using gelatine.

2.15 Blood flow

In 1998, a US patent entitled “Anti-Fraud Biometric Sensor” that accurately detects blood flow by Smart Touch LLC proposed the method of blood flow detection in finger [78]. This method uses two LEDs and a photo-detector to determine whether blood is flowing through the finger. Furthermore this patent declares to have solved these problems by checking if the background light level is above a threshold, and by detecting movement of the finger. However, it has been possible to fool similar solution by stimulating blood flow (Through the use of a flashing light or by moving the imposter’s finger).

2.16 Pulse rate

The pulse on the tip of the finger can be detected and used as a liveness detection method. In this method the underlying finger's pulse will be sensed; however, practical problems arise due to changes in the pulse. If person has a pulse of 60-80 beats per minute, then the finger must be held for at least a few seconds on the sensor for the pulse to be detectable. The pulse rate is also affected by physical and emotional states; therefore, the same person could have a pulse rate more than 80 beats per minute if he/she exercised immediately before the fingerprint scanning or becomes distressed or excited. An extra sensor and processing is required along with the fingerprint hardware and it will increase the processing time of fingerprint capturing and add an extra hardware cost in system.

2.17 Electrocardiography (ECG or EKG)

The contraction and relaxation of cardiac muscle result from the depolarisation and repolarisation of myocardial cells. These electrical changes are recorded via electrodes placed on the limbs and chest wall and are transcribed on to a graph paper to produce an electrocardiogram (commonly known as an ECG) [64, 65]. With access to only one fingertip the measurement of ECG pulses can be easily fooled by a small generator, and so this is an unrealistic choice of technology. The implementation of this system with fingerprint sensor requires expensive hardware and high processing costs.

2.18 Electroencephalography (EEG)

An electroencephalogram (EEG) is a painless test that records brain activity. When the brain cells send messages to each other they produce tiny electrical signals [66]. The EEG signals are recorded from the subject while being exposed to a stimulus, which consist of drawings of objects chosen from Snodgrass and Vanderwart picture set [67]. This technology has the same issues like ECG.

2.19 Finger skin odour analysis

This method is based on the acquisition of the odour by means of an electronic nose, the response of which in the presence of human skin differs from that obtained in the presence of other materials [68].

An odour sensor (electronic nose) is used to sample the odour signal and an algorithm allows discrimination of the finger skin odour from that of other materials, such as latex, silicone or gelatine, usually employed to forge fake fingerprints [68, 69].The acquisition of an odour pattern consists of sampling the data coming from an odour sensor during a given time interval, usually few seconds. The time necessary to restore the sensor response may vary depending on the sensor characteristic and environmental condition. This constitutes a limitation. In addition, experimental results confirm that the method, which is able to effectively discriminate real fingerprints from artificial reproductions, can be forged using a wide range of materials.

2.20 Temperature of Fingertip Epidermis

Temperature is an involuntarily generated signal under the finger tip. It is easy to measure, but it is not a sufficient indication of liveness. Average temperature on fingertips ranges between 26°C and 30°C [70, 71]. However, the temperature depends on the health condition of the user (fever or poor blood circulation could influence the result of the liveness detection). This could make an impostor with a thin artificial fingerprint attached on his real finger be accepted and, on the other hand, a user with poor blood circulation or cold be rejected. If a thin silicon artificial fingerprint is patched onto a real finger, the temperature can be decreased by a maximum of 2^0 C, which is well inside the working margins of the sensor. Sensors that are used outdoors often have a broader working margin, giving the intruder even more chance.

2.21 Skin Spectroscopy

In skin spectroscopy, an optical technique is used to measure the absorption of light by tissue, fat, blood and melanin pigment. Skin is a layered tissue structure and has a complex interaction with light. The spectroscopy measurement system is based on optical source that illuminates a small area of fingertip skin with multiple wavelengths of visible and infrared light. (See Figure. 2.24).

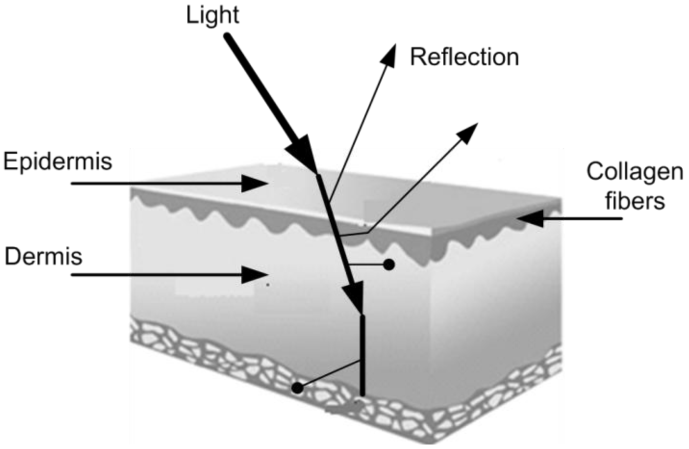


Figure 2.24: Skin Spectrometry

Light undergoes scattering and absorption at different layers of skin. Scattering is caused by the structural characteristics such as the arrangement of the collagen fibres. Absorption is caused by chromophores in the layers. The depth of light penetration depends on the wavelength of the light and the level of pigmentation. The light is reflected back after being scattered in the skin and is then measured for each of the wavelengths. The system analyzes the reflectance variability of the various wavelengths such as, 400–700 nm, they pass through the skin. Skin spectroscopy also provides a sensitive and relatively easy way to confirm that a sample is living tissue because the optical signal is affected by chemicals and other changes to the skin, [72]. Furthermore, the reflectance spectrum of skin provides information regarding the distribution and concentration of various chromophores present in the skin and is highly dependent on the person’s physical characteristics. Thus spectroscopic measurements can be successfully used as a biometric. However, the system needs moderate environmental conditions and might introduce delays in the access control process.

2.22 Stimulus response

The stimulus response of the skin can be obtained by applying small external electrical signals and measuring the variation [73, 74].

2.22.1 Skin impedance

The skin impedance method is based on simultaneous measurements of the electrical bio impedance of different skin layers. The measurements are sensitive to skin properties like stratum corneum impedance and viable skin impedance. Dispersive behaviour of these layers can be detected in the measured frequency range and anisotropy in the stratum corneum [73].

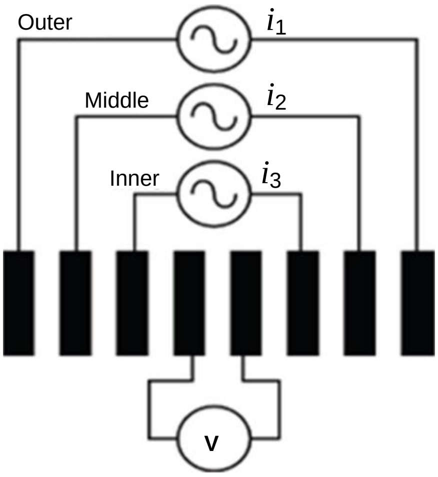


Figure 2.25: Electrical Impedance Measurement System [74]

The electrical impedance measurement system is illustrated in figure 2.25. This system uses electrode array with three alternative current injecting electrode sets and one set of voltage pick-up electrodes. The two middle electrodes are connected to the differential voltage input of the frequency response analyser, and the other three electrode pairs (denoted as i_1, i_2, i_3 in Figure 2.25) were in turn connected to the internal oscillator. The frequency response analyser consequently performed three successive four-electrode measurements, each time using the same voltage pick-up electrodes, but different current injecting electrode pairs (denoted as inner, middle and outer in Figure 2.25). In each measurement, a live or fake finger placed on the top of the electrode system with a light pressure and then a three frequencies scan was performed using an applied voltage on the current injecting electrodes with discrete frequencies.

The sensitivity field of a four-electrode system is found by taking the dot product of the current density vectors resulting from driving a unity current through the current injecting electrodes and voltage pick-up electrodes, respectively [74]. Up until now, this system has been tested at prototype level and proposed as a liveness detection solution for fingerprint sensor modules. However; it is not tested or implemented with actual fingerprint modules.

2.22.2 Electrotactile

The theory behind the electrotactile or elelctrocutaneous stimulation is the understanding of human touch sensation. The live skin is sensitive to temperature, vibrations, pressure, electrical voltage and current, with different receptors located at different depth of the skin for each sensation. Such tactile perception capability is absent in fake or dead skin. Electrotactile method uses electrical means to directly activate the nerve to stimulate the sense of touch. Such tactile system typically involves a matrix of surface electrodes that pervade very small, controlled electric currents into skin (See Figure 2.26).

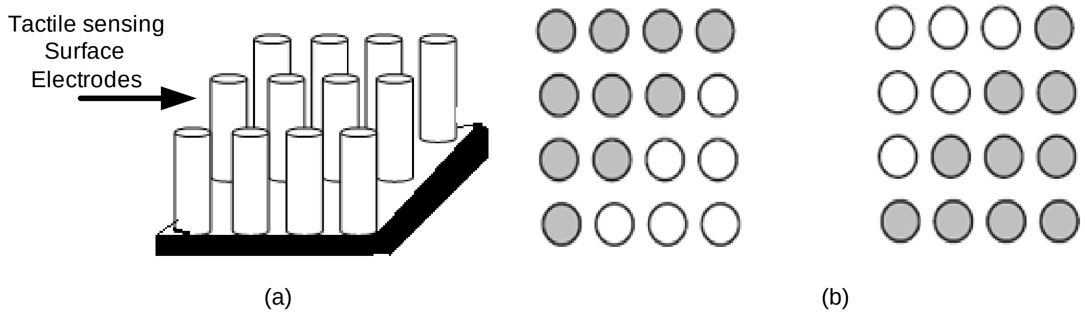


Figure 2.26: (a) 3D representation of Electrotactile Electrode Array (b) A 4-by-4 electrode pad showing an upper triangular (left) and lower triangular (right) tactile pattern. Each circle is an electrode. The dark circle represents an active electrode (having current flow) while the light circle represents a inactive electrode [75]

A liveness detection method, based on electrical based tactile sensation, is proposed in [75]. This system is capable of distinguishing between fake and live fingertip skin by use of a tactile pattern. The initial results from a prototype showed that the proposed approach is indeed able to detect gelatine fake fingers worn over live fingers, even when the gelatine is only 1mm thick.

Table 2.1 summarizes the requirements and limitations of hardware based liveness detection methods discussed in the above sections.

The design, cost, user acceptance and implementation are common issues with the proposed hardware based liveness detection solutions. It needs more research and investigation to find a suitable solution that can bring the balance between price, user-friendliness and the security of the system.

Methods	**Liveness Detection Technique**	**Requirements**	**Limitations**
Biological Signals	Epidermis Temperature	Additional Temperature sensing and signal processing hardware	• Timing of measurement and cost
	Blood Flow	Biomedical sensors and signal processing hardware	• Setup for measuring the noise free bio signals • Interface with fingerprint sensor • Cost and size issues
	Electrocardiogram (ECG)		
	Electroencephalogram (EEG)	Detection Electrodes	• Easily fooled (with a small signal generator) • Impractical with access to only one fingertip
	Pulse Rate Detection	Optical Sensors and measurement systems	• Environmental conditions • Size and cost of hardware • Integration with fingerprint scanners
	Odor Analysis	Sensors to detect different type of odor	• Extra sensors • Detection timing and Processing • Cost and system size
Skin Physiological Characteristics	Pulse oximetry	Optical sensors	• Biomedical hardware requirement • Complex signal processing
	Skin spectroscopy	• Different Optical sources and sensors • Additional measurement Systems	• Size of system • Additional signal processing and Software requirements • Not feasible in mobile applications
	Skin Impedance	• Electrodes Array • External Dc Voltage	• Skin condition can change resistance • Additional power
	Eleltrotactile	• Array of Electrodes with additional measurement system	• Deign of electrode array and size • Addition Signal processing hardware • Integration of fingerprint sensors

Table 2.1 Summary of Hardware based Liveness Detection Techniques

2.23 Software based liveness detection methods

The main focus of this section is to review the software based liveness detection approaches recommended in literature. There have been a number of attempts made at research level to detect fake fingerprints and establish the liveness of the finger. These methods exploit various type of features in the fingerprint such as optical properties of skin in relation to wavelength [76], skin coarseness [77], perspiration patterns (temporal and spatial) [78], wetness caused by sweat [79], elastic deformation of the skin of fingers [80], and signal of ridge patterns and noise of valley patterns [81]. In figure 2.22, an initial subdivision of the software based approach is adopted from [44]. The static category defines the methods which are based on features extracted from single fingerprint impression or the comparison of different impressions.

The second category, known as dynamic, involves the analysis of multiple frames of the same fingertip image. This method requires the subject to place his or her fingertip on a sensor for a certain length of time, in order to capture features such as perspiration process, and morphological approach such as intrinsic structure in these multiple frames.

Furthermore, a literature survey from year 2005-2011 is summarized in Table 2.2.The general motivation behind these approaches is that some peculiarities of live fingertips cannot be taken in artificial reproductions.

Pore detection and extraction has been researched by a number of groups to increase recognition accuracy. However, few researchers have used this to detect liveness. In the following section, five pore based methods for identification including liveness detection are discussed.

- Pore extraction algorithm was developed to extract the locations of sweat pores from the fingerprint images. This technique detects the positions of pores for unique identification [82] The results of pore extraction algorithm demonstrated using NIST 4 Database [83] contained live scan and inked prints.

- A level 3 (pores and ridge shape) propose the method of extracting the pores with ridge counters by using wavelet transform and Gabor filters to extract pores and ridge contours [27]. This technique was demonstrated on 1000 dpi fingerprint images.

Propose d Method	Publication Year	Technique for Liveness Detection	Summary
Based on Perspiration Check	2005	Time series detection of Perspiration [78]	In this research, a method is proposed based on detection of perspiration process through a time-series of fingerprint images measured directly from the scanner itself. Only a live finger can perspire and the perspiration can be detected by image analysis. This method is the most valuable and has been studied by many researchers. This method is susceptible to a number of factors including sensitivity to the pressure of the finger, the environment, user, and time interval.
	2006	Local Ridge Frequencies and Multi-resolution Texture Analysis Techniques [84]	
	2009	Wavelet based perspiration liveness check [85]	
	2009	Region Based [86]	
Based on Skin Deformation	2006	Skin Distortion Analysis [87]	This method is based on the difference of hardness (or elasticity). The difference of hardness will produce different deformations when pressing and rotating a finger on a sensor. Liveness can be detected by comparing these distortions. The key point of this method is the difference of the material hardness. Thus, the method performs poorly when the hardness of fake material is similar to live skin, and users need some training process.
	2006	Fine movement of fingertip Surface [88]	
	2007	Based on Skin Elasticity Analysis [89]	
Based on Image Quality	2007	Power Spectrum Based [90]	In fact, it is difficult to make a fake fingerprint image having the same or better image quality than that of live. In general, the quality of the fake fingerprint image is not good as live fingerprint image. Moon et. al.[13] detected the liveness of a fingerprint by calculating the standard deviation of the fingerprint image using the wavelet transform. The advantage of this method is that it is fast and convenient to use. Although Moon's work is only conceptual, it contributes an important hint that we can detect the liveness by checking the image quality.
	2007	Finger Colour Change Analysis [91]	
	2007	Band Selective Fourier Spectrum[92]	
	2008	Valley Noise Analysis [93]	
	2008	Curvet Energy and Co-Occurrence Signatures [94]	
	2008	Based on Papillary Lines [95]	
	2009	Fractional Fourier Transform [96]	
	2010	Curvelet Based Method [97]	
	2011	Multiple Image Quality Features [98]	

Table 2.2: Literature survey on proposed software based liveness detection techniques

- An adaptive anisotropic pore model was proposed in this research [27]. The parameters of this model are adjusted adaptively according to the fingerprint ridge direction and period. Fingerprint images are partitioned into blocks and a local pore model is determined for each block [99]. Experiments were performed on a 1200 dpi fingerprint dataset. This algorithm was proposed to improve the verification accuracy of pore based fingerprint recognition systems.

- An algorithm was proposed to detect liveness in fingerprint images by analysis of changes in the perspiration process. Perspiration patterns begin as changes of moisture levels in areas around the sweat pores spreading across the ridges over time [78]. This technique was based on a detection of perspiration pattern from two successive fingerprints captured at 0s and 2s. The algorithm was demonstrated with 58 live, 50 spoofed and 28 cadaver fingerprint images.

- To discriminate between fake and live fingerprint images by analysing the pore distribution on ridges was proposed in [100] . As pore size is less than 1mm, it was assumed that replication of pores on fake fingerprint is difficult. This technique demonstrated successfully on more than 14,000 images, including live and fake fingerprints captured with 569 dpi.

2.24 Summary

In the review of the existing fingerprint sensor technologies, it is concluded that no technology is present in the market which has an integrated capability for liveness detection. Simple spoofing techniques proved how easy it is to prepare an artificial fingertip stamp without having special expertise, and use it to deceive fingerprint based security systems. Liveness detection techniques proposed in literature are based on additional hardware, which adds extra costs, and increases the size and processing time of the system. Software techniques are still under research, and their detection methods are dependent upon checking the quality of fake and real fingerprint images. To discourage possible attempts at presenting a fake finger, it is important to ensure that the finger presented to the sensor is genuine, and is not fake/artificial or from a cadaver. Therefore, a live finger detection mechanism is a crucial part of AFIS used for security reasons. In AFIS, the live finger detection should be performed at the same time as the capture of the fingerprint. This would seem to be incompatible with currently available fingerprint technologies, without adding additional hardware.

To implement liveness detection, it is necessary to choose a property of the fingertip which is difficult or impossible to imitate. The only possibilities are to develop either a software based solution which can detect that property from a fingertip image, and which is embedded with the existing source codes used by AFIS, or a new sensing technology which will detect liveness in a placed finger without adding extra hardware, without adversely affecting the performance of AFIS, and that does not excessively increase the final cost of such a solution.

Pores on fingertip ridges are the potential features which require further investigation. Mainly pore based research described in above section was used for identification purposes only. No research is yet proposed or available on the liveness detection technique based on active pores. Chapter 3 introduces details of a novel active pore based image processing technique developed for liveness check in fingerprint images.

Chapter 3: Liveness using Active Sweat Pores

The most important feature that distinguishes a live finger from a non-live finger is the change of state of a sweat pore from inactive to active. Sweat pores become active in order to discharge sweat liquid to regulate finger temperature. In this chapter a technique based on detection of active sweat pores for liveness analysis in fingerprint biometrics is explained. Initially, the basic nature of an active sweat pore is introduced; a comparison between available fingerprint databases for fingerprint research is presented, alongside an examination of their limitations. In addition, details about a new high resolution (~800 dpi) fingertip database, referred to as the Brunel Fingerprint Biometric Data Base (B-FBDB), were collected for this research and are discussed. Finally the theory, development and results of a novel active pore detection algorithm based on high pass filtering and correlation technique is discussed.

3.0 Active sweat pores

In a live finger, to guarantee physiological thermo-regulation, there are many small openings named ‘sweat pores’. Figure 3.1 (a) illustrates the segment of a fingertip and a detailed view of the same segment where pores are clearly visible on the surface of finger ridges. These pores are opening end of eccrine glands, and the part of the physiology of the finger tip skin [101, 102].

The eccrine sweat glands is a long, coiled, hollow tube of cells located under the dermis (inner layer of finger tip skin), which terminates on the skin as an opening or pore [1, 4, 5]. (See Figure 3.1 b). The typical diameter of a pore is 88 to 200µm, and approximately 5 pores per mm ^{2} are on the ridges [103] .

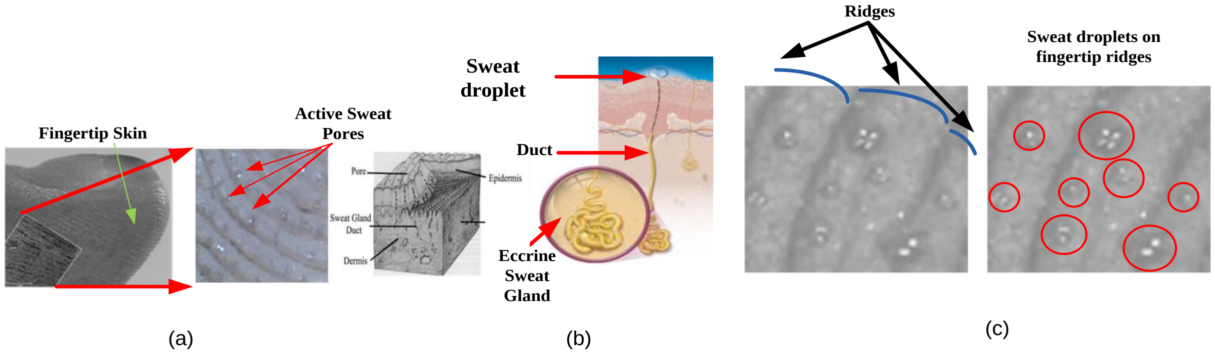


Figure 3.1: (a) Fingertip Segment [27]   (b) Eccrine Gland   c) Active pores

When they are active, they release a small amount of sweat fluid as encircled and illustrated in Figure 3.1 (c). This state of the pore is referred to here as an active pore and an active pore is a clear sign of liveness in fingertip.

3.1 Fingerprint databases

Reliable and accurate fingerprint recognition is a challenging problem in the field of pattern recognition. To test the robustness and performance of fingerprint algorithms, there are a number of standard fingerprint databases available. Nevertheless, to date, there are few benchmarks available for comparing developments in this area.

In practice common, usable and recommended fingerprint databases are:

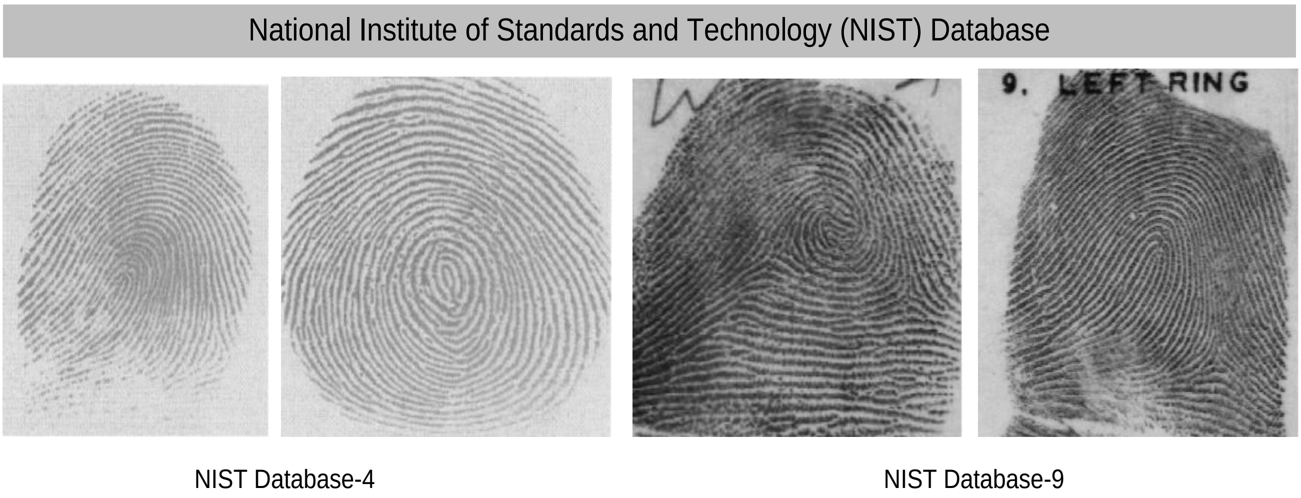
1. National Institute of Standards and Technology (NIST), USA
2. Fingerprint Verification Competition (FVC), USA & Italy
3. ATVS-FFp, Spain
4. Polytechnic University–High Resolution Fingerprints (PolyU-HRF), Hong Kong

The NIST database was purchased for this research while the other databases were obtained free of charge from ATVS (Universidad Autonoma de Madrid, Spain) and Biometric Research Centre (UGC/CRC) (Hong Kong Polytechnic University).

3.1.1 NIST database

These test fingerprint databases are produced by the Image Group, IT Laboratory, NIST, US. Nine databases of fingerprints were specifically developed for fingerprint classification and matching research in conjunction with the Federal Bureau of Investigation (FBI), the National Forensics Laboratory (NIJ), The Defence Computer Forensics Laboratory (DCFL) and U.S custom services [104]. It contains thousands of images scanned from paper cards where fingerprints were impressed by rolling “nail to nail” inked fingers. [104, 105].

Table 3.1 summarizes all available details about the NIST fingerprint databases, such as the method of capturing, image size, resolution, file format, total number of images and application. Out of the nine NIST fingerprint databases, eight databases are fingerprint images and one database contains live-sequences of 100 live fingertips from ten individuals. Some sample fingerprint images from NIST database-4 and databse-9 are illustrated in Figure 3.2.


National Institute of Standards and Technology (NIST) Database

NIST Database-4

NIST Database-9

Figure 3.2: NIST database sample images [83, 106]

These two databases are commonly used to evaluate the performance fingerprint matching algorithms. NIST database-4 contains 2000, 8bit gray scale fingerprint image pairs. Each image is 512X512 pixels. It was compressed using the JPEG lossless compression algorithm. In these images ridge and valley patters are clear and they are used for level 1 and 2 fingerprint matching. The NIST- database 9 contained 160 scanned card images with 832x768 and classified using National Crime Information Centre (NCIC) classes given by the FBI.

In both database images, the pattern of ridges and valley details are visible, but not with the high quality, seen in live scanned images. They can be useful for level 1 and 2 fingerprint research; however, the images do not show signs of active and inactive pores.

NIST special 24 Database is based on 100 video clips from live fingers and each clip size is 30 seconds. All clips compressed with MPEG-2 (Moving picture Expert Group). There were no details available about the NIST 28 special database so it is difficult to compare this with other NIST databases.

The majority of NIST databases are converted electronically by scanning ink impressed fingerprint cards. Due to the difference of resolution of the inked impression (which depends on the ink quality and pressure of finger on card) and scanning resolution, the final resultant image varies a little in clarity from those captured with fingerprint sensors. Although the NIST-30 special database scans fingertips with 500-1000 DPI, the final images are not good enough to locate active pores as a sign of liveness.

No	Database Name	Description	Method of Capturing	Size of Image (pixels)	Bit	Resolution Ppmm (Pixel per millimetre) Dpi (Dot Per Inch)	File format	No. Of fingerprints	Applications
1	NIST Special Database-4[83]	NIST 8-Bit Gray Scale Images of Fingerprint Image Groups (FIGS)	Live scan	512x512	8- Bit Gray scale	19.7 ppmm	JPEGL Compression	4000	Algorithm Development, Testing and Training
2	NIST Special Database -9[106]	Consists of five volumes have been released. Each volume is a 3 Disk set and each CD-ROM containing 90 mated card Pairs of segmented gray scale images.	Card prints and scanned	832X768	8- Bit Gray scale	500 dpi	JPEGL	13500	Automated fingerprint classification research, algorithm development and system training and testing. A valuable tool for evaluating fingerprint system using a statistical sample of fingerprints which approximate a natural horizontal slice of the NCIC classifications.
3	NIST Special Database -10[104]	NIST Supplemental Fingerprint Card Data (SFCD) (For special Database 9- 8-Bit Gray Scale Images	Card prints and scanned	832X768	N/A*	19.7 ppmm	JPEG (with lossless compression)	5520	Algorithm Development, system Testing and Training
4	NIST Special Database -14[107]	NIST Mated Fingerprint Card Pair (MFCP2)	Card prints and scanned- Live scan	832X768	8- Bit Gray scale	500 dpi	Wavelet Scalar Quantization (WSQ)Compression	27000 Pairs	Use in development and testing of automated fingerprint classification and matching systems on a set of images which approximate a natural horizontal distribution of the national Crime Information centre (NCIC) fingerprint classes
5	NIST Special Database -24[104]	NIST Digital Video of Live-Scan Fingerprint	Video camera	720X480 (300 frames)	5 million bits/sec		Compressed MPEG-2 video	100 videos Each 30 seconds	Developing and testing of fingerprint verification systems
6	NIST Special Database -27[104]	Developed in conjunction with FBI. It contains latent fingerprints from crime scenes and heir rolled fingerprint mates	Card prints and scanned	800X768	16-Bit gray scale	1000 dpi	ANSI/NIST-ITL 1-200 Standards	258	Development and test new algorithms, test commercial and research AFIS systems, train latent examiners and promote the ANSI/NISTI file format standards
7	NIST Special Database – 28 National Software Reference Library (NSRL)[104]	A collaboration of National Institute of Standards and Technology, The National Forensics Laboratory (NIJ), The Defence Computer Forensics Laboratory (DCFL), the U.S Customes services, software vendors, and state and local law enforcement organizations.	N/A*	N/A*	N/A*	N/A*	N/A*	N/A*	The NSRL is a tool to assist in fighting crime involving computers, such as child pornography, racketeering, cyber attacks, illegal gambling, internet fraud, and software piracy.
8	NIST Special Database – 29[108]	Plain and Rolled Images from Paired Fingerprint Cards	Card prints and scanned	N/A*	N/A*	19.7 ppmm	Wavelet Scalar Quantization (WSQ)Compression	2160	Development and testing fingerprint matching systems.
9	NIST Special Database -30[109]	Dual resolution Images from paired Fingerprint Cards	Card prints and scanned			500 and 1000 dpi	JPEGL	360	Developing and testing of fingerprint compression and fingerprint matching systems

*N/A (Not available)

Table 3.1 Summary of NIST databases

3.1.2 FVC database

The Fingerprint Verification Competition (FVC) attempted to establish the first common benchmark for testing an algorithm for fingerprint feature extraction and matching [110-113]. There were four FVC (FVC-2000 to FVC-2006) organized by following research groups.

- Biometric System Laboratory, University of Bologna, Italy
- Pattern Recognition and Image Processing Laboratory, Michigan State University, USA
- Biometric Test Centre, San Jose State University, USA
- Biometric Recognition Group - ATVS ,Universidad Autonoma de Madrid, Spain)

The FVC comprised four disjointed fingerprint databases, each collected with a different sensor technology. A total of four databases, DB1to DB4, are currently available for researchers. From these four databases, DB1 to DB3 are scanned live with optical, capacitive and thermal sensors; however, DB4 is created using the Synthetic Fingerprint Generator (SFinGe) [114]. Sample images from FVC databases are shown in Figure 3.3.

SFinGE is a software method of generating synthetic fingerprints. In all four FVC databases , the participant algorithms were performed on DB4 similarly to the other DBs. SFinGe is based on four steps [113,115]:

Step-A: Starting from the positions of pores and deltas, it exploits a mathematical flow model to generate a consistent directional map

Step-B: It creates a density map on the basis of some heuristic criteria

Step-C: The ridge-line pattern and the minutiae are created through space-variant linear filtering; the output is a near-binary very clear fingerprint image

Step-D: This step adds some specific noise and produces a realistic gray-scale representation of the fingerprint

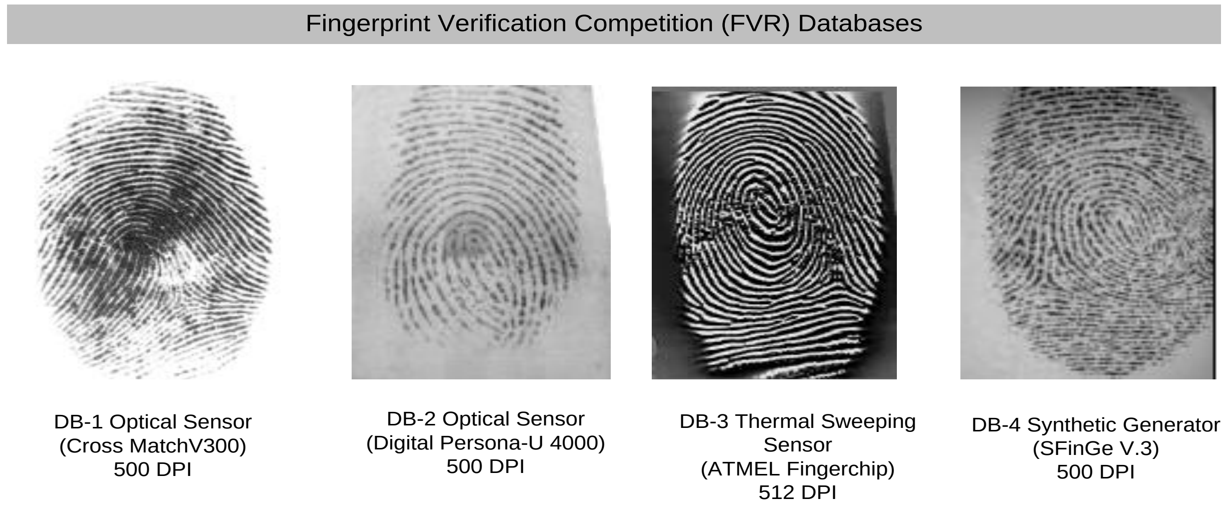

Fingerprint Verification Competition (FVR) Databases
DB-1 Optical Sensor (Cross MatchV300) 500 DPI
DB-2 Optical Sensor (Digital Persona-U 4000) 500 DPI
DB-3 Thermal Sweeping Sensor (ATMEL Fingerchip) 512 DPI
DB-4 Synthetic Generator (SFinGe V.3) 500 DPI

Figure 3.3: FVC database sample images

Unlike the to NIST fingerprint databases these are all captured using live scan. None are collected using the fingerprint card scanning method. The summary of FVC Databases is presented in Table 3.2.

The majority of these databases are used and recommended by fingerprint biometrics experts for testing various algorithms in fingerprint biometrics, however there are a few limitations [116-121]:

- All the images are captured with 500-569 DPI which is the same as NIST database
- The images in the database are not sufficient to locate the pores on the fingertip ridges
- These are only useful to evaluate the fingerprint feature extraction and matching algorithms

No	Database Name	Database No	Capturing Method	Size of Image (pixels)	Bit	Resolution (dpi)	File Format	No. Of fingerprints		Applications
								Set A (wxd)	Set B (wxd)	
1	**FCV 2000**[110]	DB1	Optical sensor "Secure Desktop Scanner" by KeyTronic	300x300	16 Gray Scale	500	Bit map image (BMP) Uncompressed	100x8	10x8	• Fingerprint algorithm performance evaluation • Testing the performance of algorithms in terms of feature extraction and matching.
		DB2	Capacitive sensor "TouchChip" by ST Microelectronics	256x364		500		100x8	10x8	
		DB3	Optical sensor "DF-90" by Identicator Technology	448x478		500		100x8	10x8	
		DB4	Synthetic fingerprint generation	240x320		~500		100x8	10x8	
2	**FCV 2002**[122]	DB1	Optical sensor "TouchView II" by Identix	388x374	16 Gray Scale	500	Bit map image (BMP) Uncompressed	100x8	10x8	
		DB2	Optical sensor "FX2000" by Biometrika	296x560		569		100x8	10x8	
		DB3	Capacitive sensor "100 SC" by Precise Biometrics	300x300		500		100x8	10x8	
		DB4	Synthetic fingerprint generation	288x384		~ 500		100x8	10x8	
3	**FCV 2004**[123]	DB1	Optical Sensor	640x480	16 Gray Scale	500	Bit map image (BMP) Uncompressed	100x8	10x8	
		DB2	Optical Sensor	328x364		500		100x8	10x8	
		DB3	Thermal sweeping Sensor	300x480		512		100x8	10x8	
		DB4	SFinGe v3.0	288x384		~ 500		100x8	10x8	
4	**FCV 2006**[112]	DB1	Electric Field sensor	96x96	16 Gray Scale	250	Bit map image (BMP) Uncompressed	140x12	10x12	
		DB2	Optical Sensor	400x560		569		140x12	10x12	
		DB3	Thermal sweeping Sensor	400x500		500		140x12	10x12	
		DB4	SFinGe v3.0	288x384		~ 500		140x12	10x12	

Table 3.2: Summary of FVC databases

3.1.3 ATVS-FFp database

For research purposes the ATVS-FFp database was obtained free from Biometric Recognition Group ATVS at Universidad Autonoma de Madrid, Spain [124]. This database contained fingerprints taken from real fingers and fake replicas of same finger. The previously discussed databases were captured with 500-569 dpi which is sufficient for the level-2 fingerprint research.

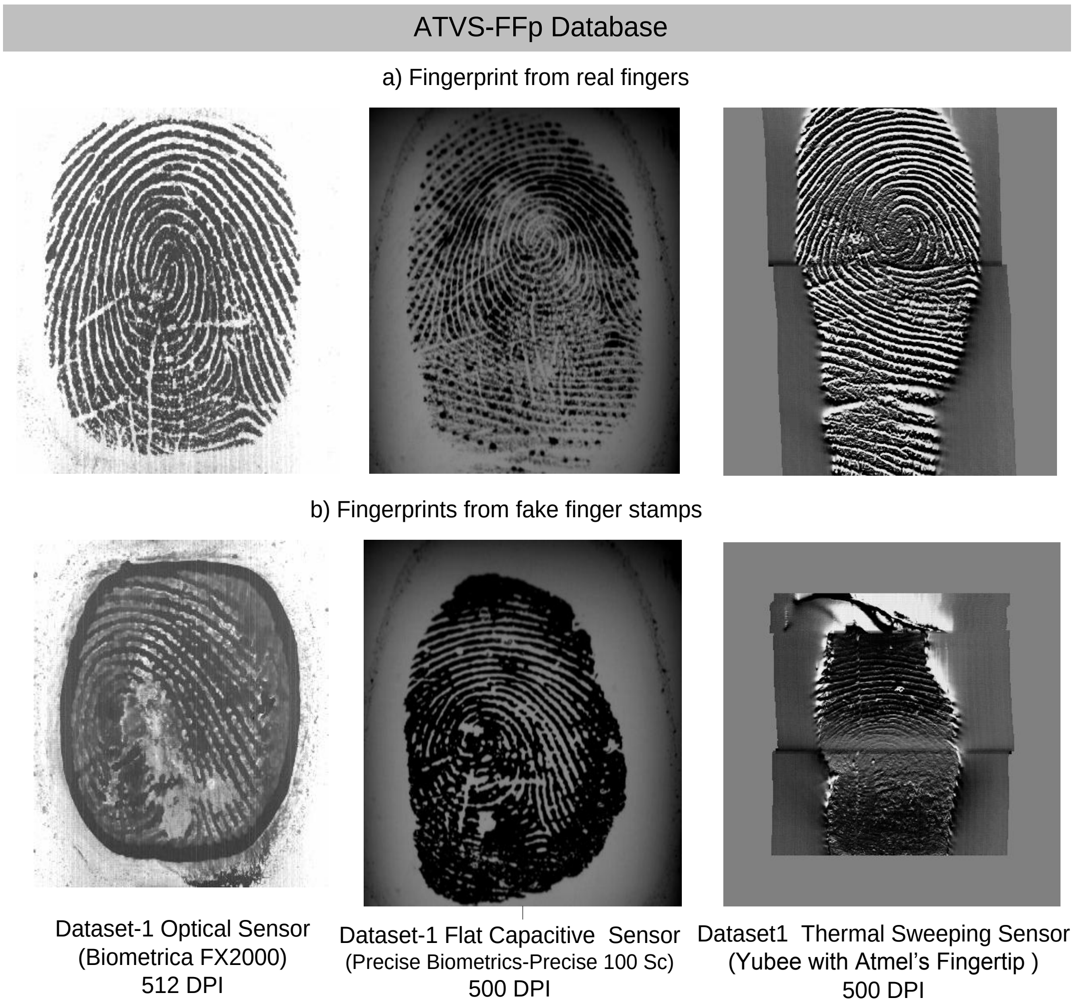

ATVS-FFp Database
a) Fingerprint from real fingers
b) Fingerprints from fake finger stamps
Dataset-1 Optical Sensor
(Biometrica FX2000)
512 DPI
Dataset-1 Flat Capacitive Sensor
(Precise Biometrics-Precise 100 Sc)
500 DPI
Dataset1 Thermal Sweeping Sensor
(Yubee with Atmel's Fingertip)
500 DPI

Figure 3.4: ATVS-FFp sample images [124] (a) Fingerprint taken from a real fingers b) Fingerprints captured from replica fingers

Database1 contained samples of the index and middle fingers (real and fake) from both hands of 17 users. Real fingerprints from database 1 are illustrated in Figure 3.4 (a) and fake fingerprints of same fingerprint images are illustrated in Figure 3.4(b). It comprises of 68 fingers, each with 4 samples that were captured with 3 sensors. In total 816 real images were collected and the same number of replica finger images.

In database 2, the replica fingers, from which fake fingerprint images were gained, were generated without the co-operation of the user. Fingerprint samples of the index and middle fingers from both hands of 16 users were collected. A total of 64 different fingers (real and fake) were collected for this database.

The main features of ATVS-FFp database are summarized in Table 3.3

Database Name	**Capturing Method**	**Size of Image (pixels)**	**Resolution (DPI)**	**File format**	**No. of Fingerprints**	**Applications**
DATABASE1 With co-operation	Biometrica FX2000 (Optical)	300x300	512	Bit map image (BMP) Uncompressed	816 real fingerprints and 816 fake fingerprints	Testing the performance of fingerprint liveness detection algorithms
	Yubee with ATMEL's fingerchip (Thermal)		500			
	Precise 100 SC (Capacitive)		500			
DATABASE 2 Without co-operation (Real and Fake)	Biometrica FX2000 (Optical)	300x300	512	Bit map image (BMP) Uncompressed	768 real fingerprints and 816 fake fingerprints	
	Yubee with ATMEL's fingerchip (Thermal)		500			
	Precise 100 SC (Capacitive)		500			

Table 3.3: Summary of ATVS- FFp database

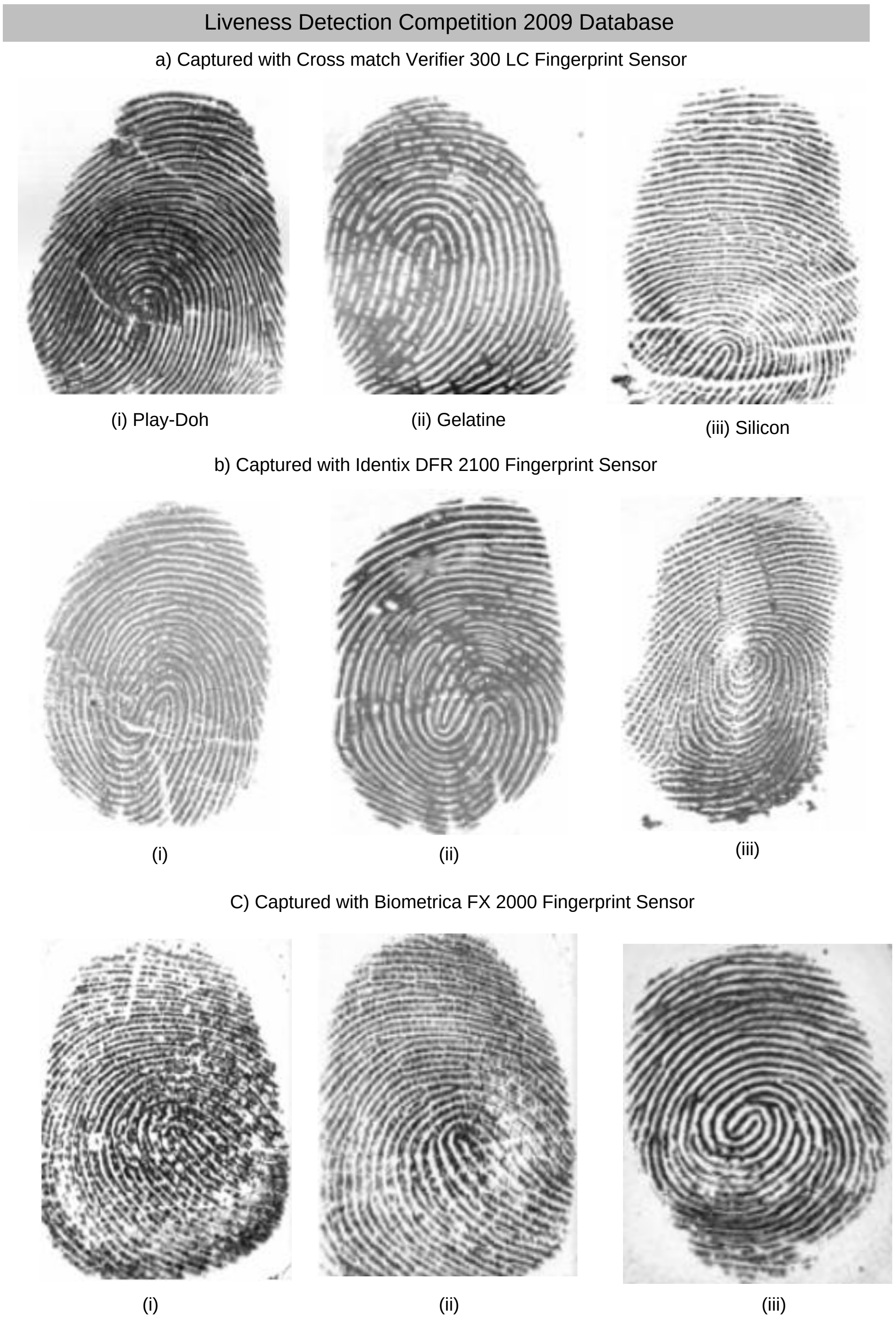
3.1.4 Liveness detection competition 2009 database

This was the first fingerprint liveness detection competition (LivDet 2009) which was organized by the University of Cagliari, Italy, in cooperation with Clarkson University, USA [125]. LivDet 2009 was organized for academic and industrial institutions that have a solution for software-based fingerprint liveness detection issues. The goal of the competition was to compare different methodologies for software based fingerprint liveness detection with a common experimental protocol and database [126, 127].

The LivDet 09 database for the final evaluation constituted of three sub-sets, which contained live and fake fingerprint images from three different optical sensors. Table 3.4 lists the details of such by sensor model, size of image, resolution and the number of fingerprints in the database. For this competition fingerprints were collected using different materials for the artificial reproduction of the fingerprint, such as gelatine, silicone and play-doh. Figure 3.5 shows examples of fake fingerprint images from the three optical scanners.

Database Name	**Capturing Method**	**Size of Image (pixels)**	**Resolution (DPI)**	**File format**	**No. of Fingerprints**		**Applications**
					Live Samples	**Fake Samples**	
Datset-01	Cross match Verifier 300LC Optical fingerprint sensor	480x640	500	N/A	2000	2000	For testing liveness detection algorithms
Datset-02	Identix DFR 2100 Optical fingerprint sensor	720x720	686	N/A	1500	1500	
Datset-03	Biometrica FX 2000 Optical fingerprint sensor	312x372	569	N/A	2000	2000	

Table 3.4: Summary of Liveness Detection Competition 2009 Database [127]



Liveness Detection Competition 2009 Database

a) Captured with Cross match Verifier 300 LC Fingerprint Sensor

(i) Play-Doh (ii) Gelatine (iii) Silicon

b) Captured with Identix DFR 2100 Fingerprint Sensor

(i) (ii) (iii)

C) Captured with Biometrica FX 2000 Fingerprint Sensor

(i) (ii) (iii)

Figure 3.5: Examples of fake fingerprint images from Liveness Detection Competition 2009 Databases [127]

This database was used only to check the liveness from the quality of fingerprints; however, there is no clear evidence of pores in any of the images from the database. Therefore, this database is not useful in an active pore based liveness detection algorithm.

3.1.5 PolyU-HRF database

This database has been developed by Biometric Research Centre (UGC/CRC) at Hong Kong Polytechnic University [128]. Currently, it is one of the largest, free of charge, high resolution fingerprint database available, that facilitates researchers for designing effective and efficient algorithms for extracting and matching fingerprint features. Fingerprint images were captured with a newly developed high resolution optical device created by the same team (see Figure. 3.6).

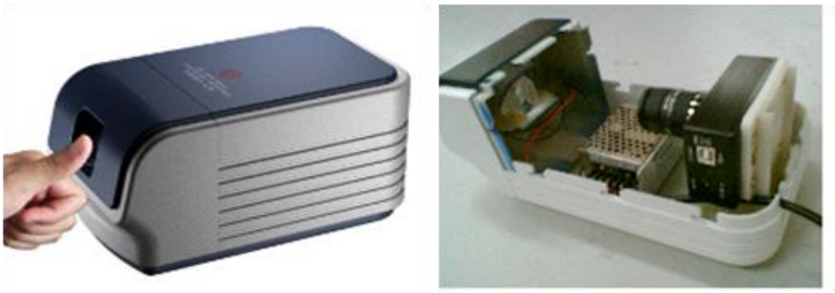
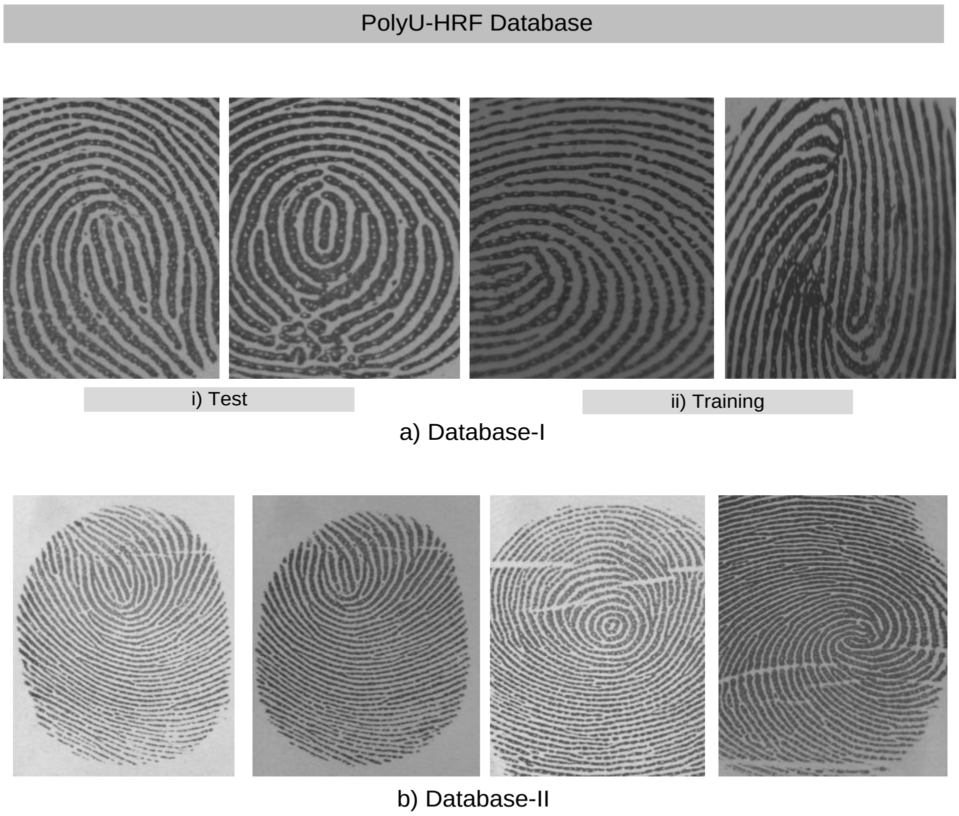


Figure 3.6: Optical Device for high resolution fingerprint imaging [128]



a) Database-I

b) Database-II

Figure 3.7: Sample Images form PolyU-HRF

Sample images from database I and II are illustrated in Figure 3.7. Pores are visible on ridges on the fingerprints in both databases (see Figure 3.6.(a)).

Database Name	Capturing Method	Size of Image (Pixels)	Resolution	File Format	No of Fingerprints	Application
DBI: Training	Specially designed High resolution optical scanner	320x240	~ 1200 DPI	JPEG	210	Designing effective and efficient algorithms for extracting and matching fingerprint additional features
DBI: Test		320x240	~ 1200 DPI		1,480	
DB-II		640x480	~ 1200 DPI	JPEG	1,480	

Table 3.5: Features of PolyU-HRF database

Features of PolyU-HRF database are presented in Table 3.5. All database were captured with 1200 DPI resolution in two different image sizes 320x240 and 640x480.

Currently, in fingerprint biometrics research, this high resolution database is available for research on pore patterns as a means of identification; however, it cannot be used to differentiate between active and inactive pores.

3.2 Common issues with fingerprint databases

From the literary review and by manual investigation of fingerprint database it has been shown that they have different features and limitations. Most of them cannot be used for detection of liveness .

LivDet09 was developed to investigate liveness detection algorithms based on detection of noise level differences in real and replica fingerprint images, or some other parameters to establish liveness. In ATVS FFp some pores are visible on fingertip ridges; however, there is no differentiation between active and inactive pores.

PolyU-HRF was the only database to contain fingerprint images captured at 1200 dpi, and pores can be clearly distinguish on the images. These images can be used for research involving the examination of pores on ridges, and pore patterns, for identification purposes. Fake fingerprints do not contain details about the status of pores on ridges, as has been demonstrated by P. Coli et. al [31]; however, these databases they cannot be useful in the detection of active or inactive pores.

Most fingerprint algorithm researchers usually perform tests conducted with self-collected databases due to the limitations of available fingerprint databases. It was in order to carry out further research on the theory of active pores that Brunel Fingerprint Biometric Data Base (B-FBDB) was produced. This is a high-resolution fingertip images databases using a non contact micro-capture camera with 100–400x magnification. database. Using the images from B-FBDB, the extraction and location of active sweat pores on ridges is achieved successfully using high pass and correlation filtering techniques (see section 3.5).

The following section further explains the process of B-FBDB database collection and comparison with other databases.

3.3 B-FBDB

B-FBDB database was collected with co-operation from province of Sindh, Pakistan. Images were captured using a USB micro-capture camera Model Veho VMS-004 deluxe with 2 megapixel CCD and 100–400X magnification (Figure 3.8 (a)). An approximately 25 mm area of each fingertip is captured (Figure 3.8 (b)) with 200-250 magnification settings. The size of each image in the database is 640x180 and stored in colour with JPEG compression. Micro capture software was provided within the camera, and was used to capture and store the all database images. Figure 3.8 (c) illustrates the complete data collection setup.

Samples in the database collection were taken from 45 volunteers of differing gender and age group. The purposes of this database collection and usage were clearly explained to each volunteer before capturing their fingers. Personal information such as name and gender of participants is kept anonymous to protect privacy.

The following fingerprint capture protocol was explained to volunteers.

- Wash hands carefully with soap to remove dirt or any other particles from fingertips;
- Dry hands in the air without rubbing with a cloth or tissue paper in order to avoid to avoid from any kind of particle contamination on fingertips;
- Fingertip images were captured by placing the right hand index finger, followed by the thumb over the top of the USB microscope. The same sequence of image capturing was followed for the left hand

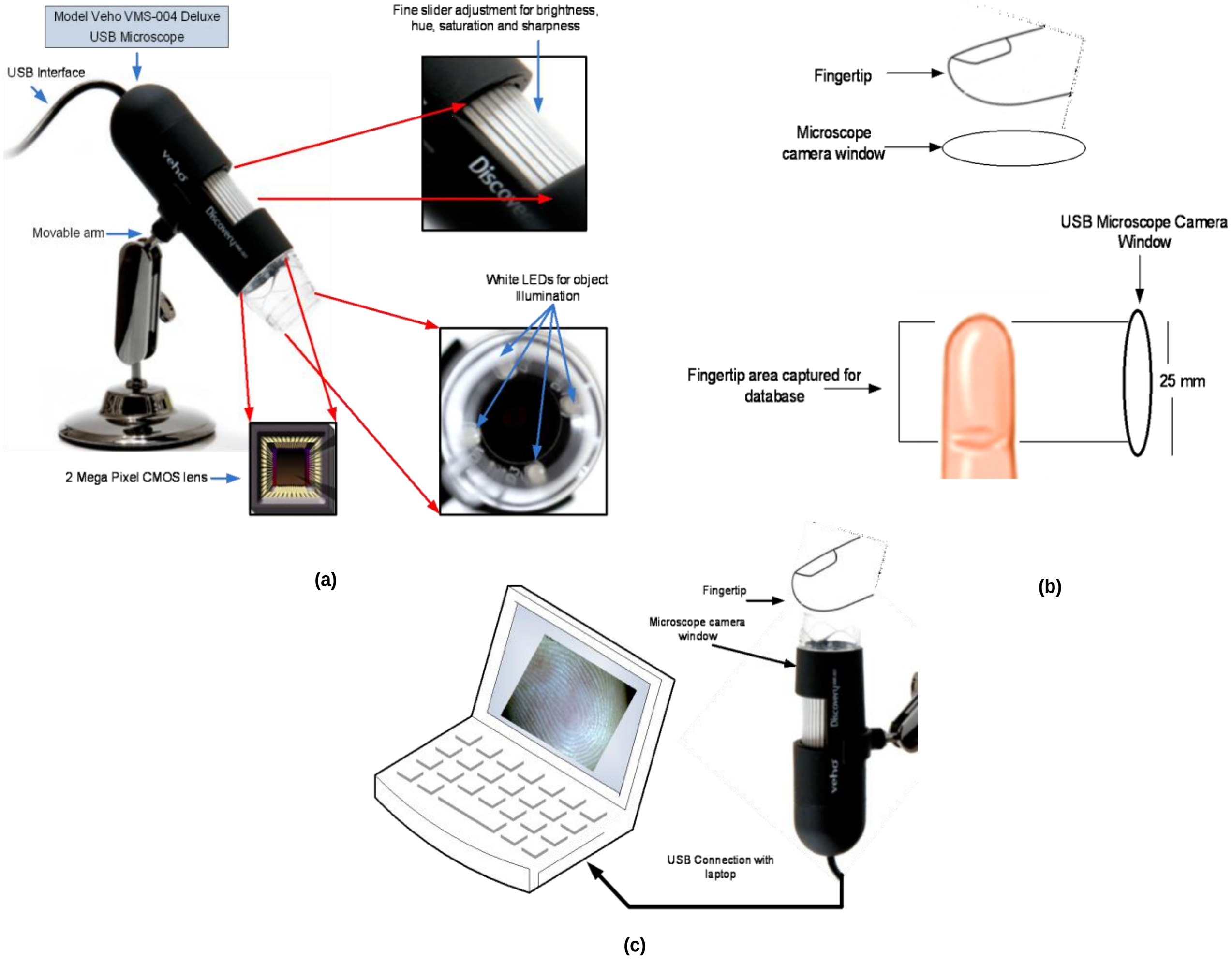

Model Veho VMS-004 Deluxe USB Microscope
USB Interface
Fine slider adjustment for brightness, hue, saturation and sharpness
Movable arm
White LEDs for object illumination
2 Mega Pixel CMOS lens
(a)
Fingertip
Microscope camera window
USB Microscope Camera Window
Fingertip area captured for database
25 mm
(b)
Fingertip
Microscope camera window
USB Connection with laptop
(c)

Figure 3.8: (a) Veho VMS-004 USB Microscope b) Fingertip region captured c) Database collection setup

A number of sample images from B-FBDB are illustrated in Figure 3.9. The images were randomly selected from the whole database, showing ridges and valley patterns. Active pores are visible on each ridge. Furthermore, segmented images from B-FBDB are also illustrated in Figure 3.9, which clearly show active pores on fingertip ridges.

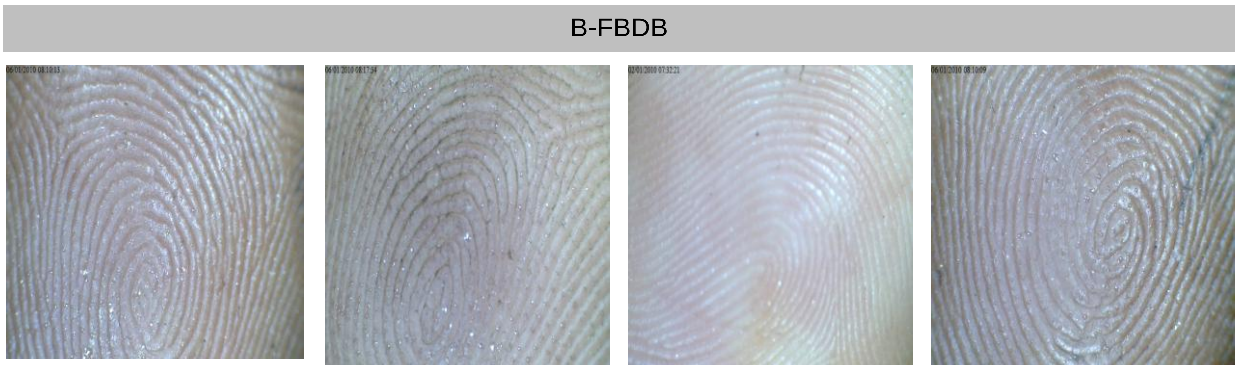


Figure 3.9: Sample images from Brunel Fingerprint Biometrics Database (B-FBDB)

B-FBDB was used to make close initial observation of the properties of sweat pores such as the opening and closing of pores, shape and size , position of pores on ridges, and the number of active and inactive pores in a specific region of fingertip. Features of B-FBDB are summarised in Table 3.6.

Database Name	**Capturing Method**	**Size of Image (Pixels)**	**Resolution (DPI)**	**File format**	**No of Images**	**Applications**
Brunel – FBIG	Veho VMS-004 Optical USB Microscope	640x180	~ 800	JPEG	210	Active pore research for liveness detection

Table 3.6: Summary of B-FBDB

Active pores are very distinctive from inactive pores in terms of its size and shape (see figure 3.10 (a)); i.e. active pores are generally larger by a factor 5 to10 than the inactive pores as can be seen in Figure 3.10. (b) Active pore images captured from different finger tips are illustrated in Figure 3.10 (c).

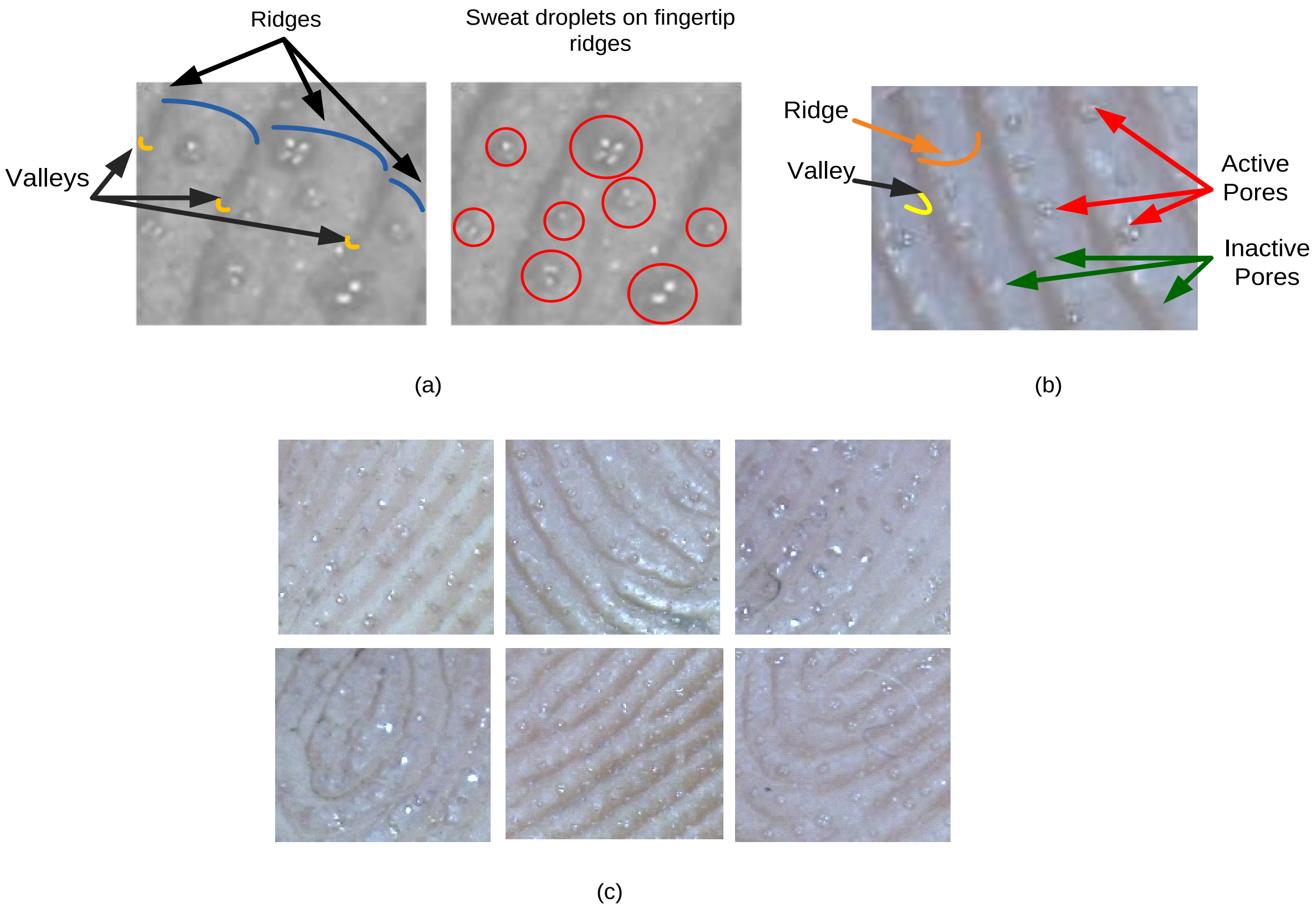


Figure 3.10 a) A segment of finger image from B-FBDB b) Active and Inactive pores on fingertip c) 150x150 size cropped images from B-FBDB showing active pores with different sizes and position

3.4 Pictorial comparison between databases

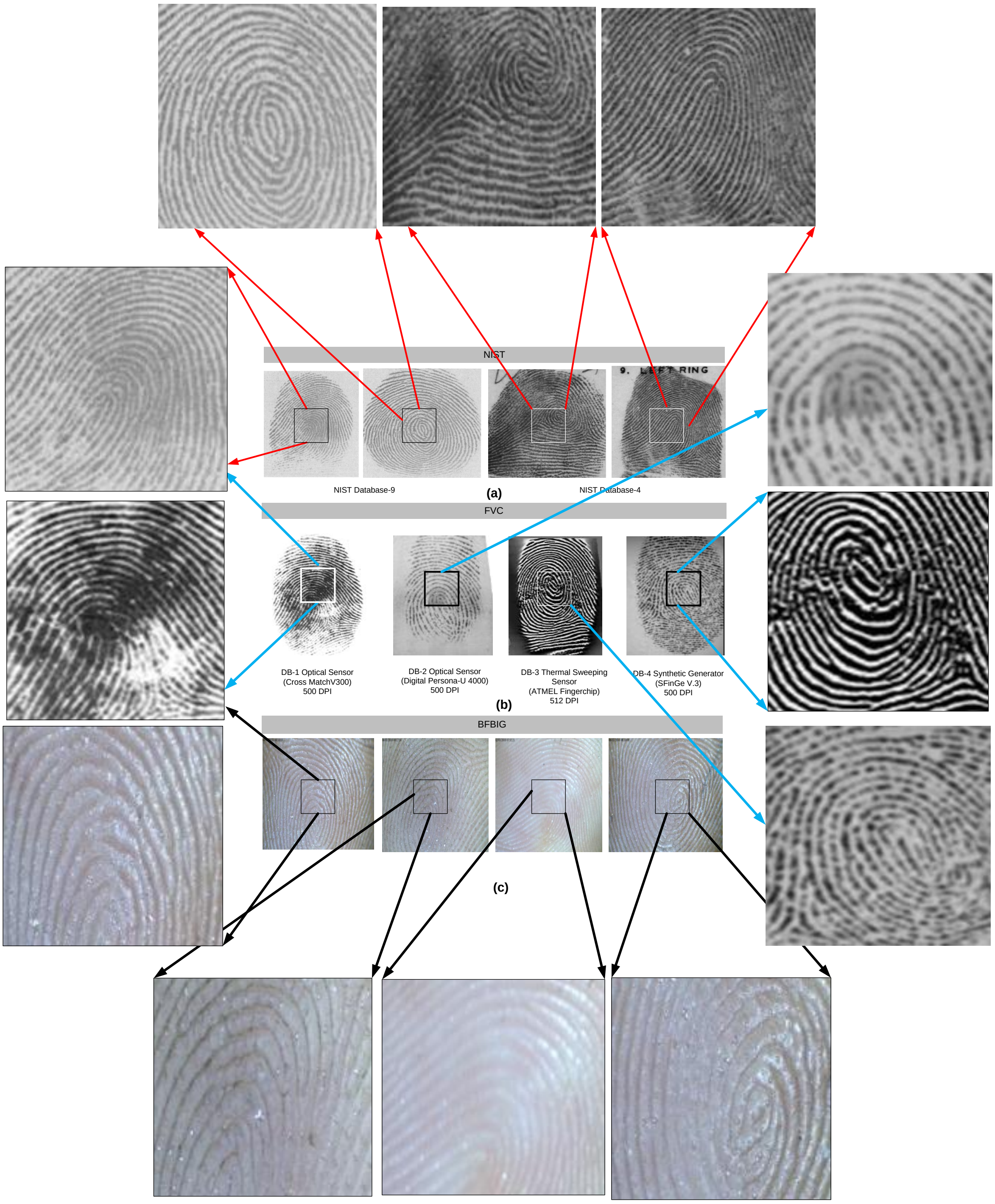


Figure 3.11 (a) 150x150 segment of fingerprint image from NIST-4 and 9 Database (b) 150x150 segment from FVC-2006 Database (c) 150x150 segment from B-FBDB

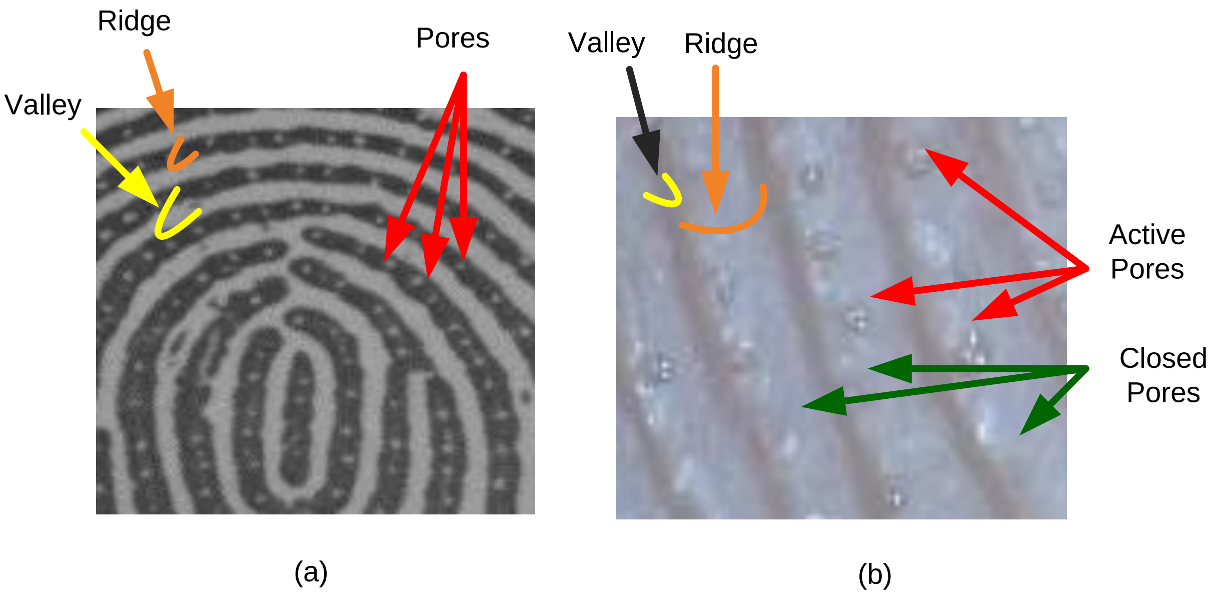


Figure 3.12 (a) 150x150 segment of fingerprint image from Poly-U HRF Database
(b) 150x 150 segments from B-FBDB Database

Limitations of B-FBDB:

- Created specifically to validate the theory of active pores for liveness check
- Not tested yet for other fingerprint applications such as matching

3.5 Algorithm for active sweat pore detection for liveness check

The research on B-FDB active pore database explored some new features that have hitherto not been reported in published literature on fingerprint liveness detection, namely the active status of pore. Various other software based liveness detection techniques proposed up to now were discussed in Chapter 2.

The distinction between active sweat pore and a corresponding inactive sweat pore was shown in terms of contrasting size and shape. An active sweat pore detected on fingertip is a clear sign of liveness. The preparation of fake fingerprints stamps with active pores is virtually impossible. These contrast variations can be extracted using frequency domain image processing. Using this theory, a novel image processing technique was developed using frequency domain high-pass filtering followed by correlation filtering. This technique is known as High-Pass and Correlation Filtering Algorithm (HCFA). By processing images from B-FBDB with HCFA, the extraction and position of active sweat pores on ridges was successfully obtained [129].

A brief background theory of the high pass and correlation filtering techniques and their demonstration is presented in the following section.

3.5.1 High-Pass filtering and correlation filtering

In this section the basic theory of high pass filtering and two dimensional correlations are explained. Additionally, example demonstrations are presented to support the theory of high-pass filtering and correlation filtering.

3.5.2 High pass filtering of frequency spectrum

Space domain images can be synthesised using the Fourier Transform and the resulting image consists of a spatial frequency spectrum of the image. Various structures of the image are made up of specific frequency spectrum components. It is therefore possible to manipulate the frequency spectrum to achieve a specific image processing technique in the space domain [130].

The frequency spectrum (G(X, Y)) of an image, g(x, y), can be evaluated using the following Fourier Transform integral.

$$G(X,Y) = \iint_{-\infty}^{\infty} g(x,y)e^{-j2\pi(xX+yY)}dxdy \qquad (3.1)$$

where (x, y) and (X, Y) denote the space plane co-ordinates and the frequency plane co-ordinates respectively.

Since digital images are considered in this work, Discrete Fourier Transform (DFT) will be used and is given as;

$$G_s(X,Y) = \frac{1}{N}\sum_{x,y=-N/2}^{N/2-1} g_s(x,y)e^{-j\frac{2\pi}{N}(xX+yY)} \qquad (3.2)$$

Where $g_s(x,y)$ and $G_s(X,Y)$ are sampled functions of an image and its frequency spectrum respectively and both functions are pixellated over a square grid of N × N square pixels. It should be noted that the Fast Fourier Transform (FFT) is used for evaluation in equation (3.2) for time efficient calculations. In the rest of these sections mathematical equations and the analysis presented will be based on continuous un-pixellated image and their frequency spectrums as it will not affect the pixellated versions.

In an image, the external boundary is high intensity, and shows darker than the lower intensity core. It is made up of high frequency components. Sharper transitions produce higher frequency components. Therefore, by applying high-pass filtering in the frequency domain, the edges of an image can be easily extracted. The two dimensional transfer function of the high pass filter (H(X, Y)) can be represented by;

$$H(X,Y) = \begin{cases} 1, & X \geq f_{xc}, \text{ and } Y \geq f_{yc} \\ 0, & otherwise \end{cases} \qquad (3.3)$$

where f_{xc} and f_{yc} are cut-off frequencies in X and Y directions respectively.

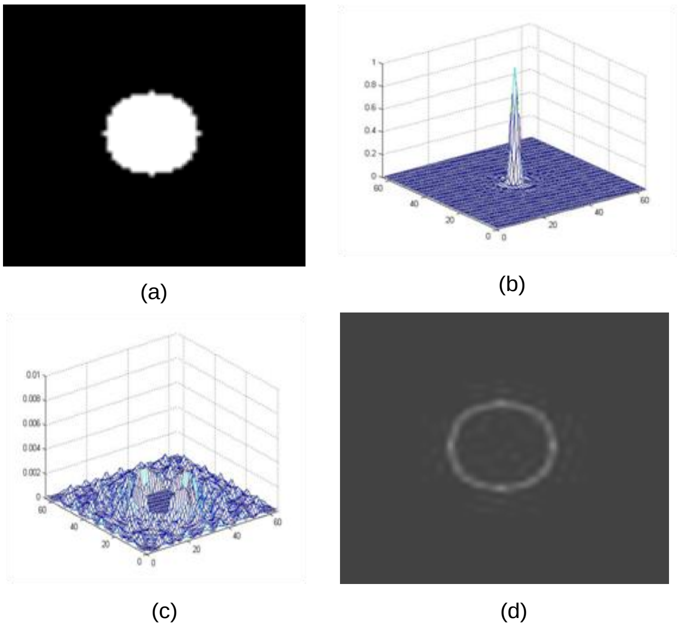
The following sections explain and demonstrate the effect of high pass filtering on an image.

3.6 Demonstration of high pass filtering

To demonstrate the effect of high pass filtering on a uniform circle with a radius of 10 pixel is selected. First, Fourier transform is applied to the circle as shown in Figure 3.13 (a) and its power spectrum is shown in Figure 3.13 (b). Then high pass filtering, with a cut-off frequency of 10 pixels, chosen empirically, is applied to the frequency spectrum, as illustrated in Figure 3.13 (c) .The resulting Fourier components are Inverse Fourier Transformed (IFT), as shown in Figure 3.13

(d), which clearly shows the edge of the circle and removes white space within the circle. This demonstration clearly shows that high frequency components make up the edges of the circle.

Another demonstration, which is similar to above, but a ring-type image, is also presented to explain the effect of a varying cut-off frequency in high-pass filtering. The original image is Figure 3.14 (a) and the rest of the images are passing through the high-pass filter with various cut-off frequencies. The cut-off frequencies in both directions have been chosen to be the same. The brightness of images (Figure 3.14(b) to Figure 3.14 (f)) is increased for clear illustration. These results visibly demonstrate the effect of the high pass filtering. Figure 3.14 (c) shows the best edge detection.



(a) (b)

(c) (d)

Figure 3.13: Edge detection of a uniform circle. (a) Circle with radius 10 in window size of 64 x 64 pixels (white represents 1 and black represents 0) (b) Power spectrum of the circle (a), (c) Power spectrum of the circle after DC components with aperture 10 x 10 pixels is removed and (d) Intensity distribution of the resulting Image (brightness increased for presentation purpose).

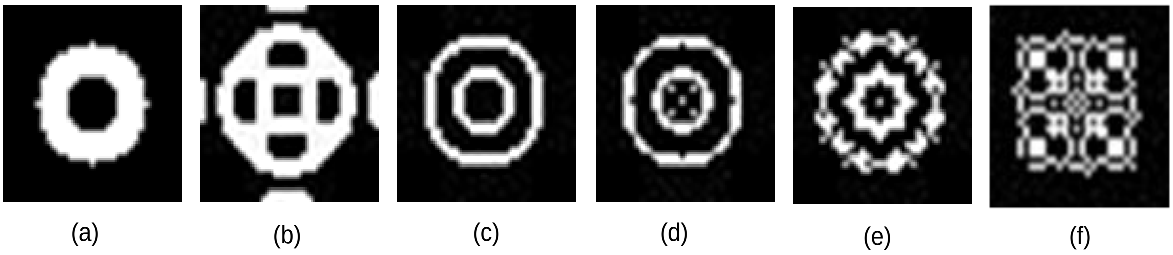


Figure 3.14: Effect of high pass filtering on a ring-circle (a) Original image (in 32x 32 pixels square), rest of the images are after passed through high pass filter of cut-off frequency in both X and Y directions (b) 5 pixels (c) 10 pixels (d) 15 pixels (e) 20 pixels and (f) 25 pixels. In all the images white represents intensity one and black represents zero.

This demonstration also suggests that a very high cut-off frequency can result in a completely different image. In these cases, very high frequency components are added constructively and destructively add to form a new set of images. It is therefore is very important to choose the appropriate cut-off frequency to get the right filtering frequencies. However, there is no analytical method available to determine the cut-off frequency to detect edges.

3.6.1 Theory of Correlation Filtering

Correlation techniques have been explored in many fields of engineering: optical pattern recognition [131], target tracking [131], face recognition [132], finger print feature matching [5], and spectrum sensing in communications [133].

Mathematical representation of the two dimensional correlation of two space varying 2D signals g(x,y) and h(x,y) can be given by equation (3.4).

$$v(x,y) = \iint_{-\infty}^{\infty} g(\xi,\eta)h(\ \xi - x,\ \eta - y)\ d\xi\ d\eta \qquad (3.4)$$

Where ξ and η are dummy variables used to evaluate the correlation integral. When g(x, y) and h(x, y) are identical then correlation will produce a peak value at the centre of the correlation plane (called the autocorrelation peak), otherwise a weak cross-correlation peak will be present at the centre of the correlation plane. The intensity value of the cross correlation peak is a measure of the similarities of the two signals.

The correlation plane field distribution can be evaluated using Fourier transform properties of the correlation integral [134] and can be given by the following equation:

$$\begin{aligned} \mathrm{v(x,y)} &= \mathrm{IFT[G(X,Y)\ H*(X,Y)]} \\ &= \mathrm{IFT[H(X,Y)FT[g(x,y)]]} \end{aligned} \qquad (3.5)$$

where G(X, Y) is FT of g(x, y) and H*(X, Y) is complex conjugate of FT of h(x, y). Equation (3.5) can be evaluated using FFT routines for both pixellated image and frequency spectrum functions.

Mathematical development of two properties of Fourier Transform (shift Invariant and Multiple correlations), which are relevant in this work, are described below followed by a demonstration.

a) Shift-Invariant

When one of the signals (g(x,y)) is translated (shifted) by a vector $\binom{x_s}{y_s}$, it can be denoted by g(x-x_s, y-y_s). Its frequency spectrum can be given by the equation (3.6) using FT properties [134]:

$$FT[g(x-x_s,y-y_s)] = e^{-j\,(Xx_s+Yy_s)}G(X,Y) \qquad (3.6)$$

The correlation plane amplitude distribution can be given by:

$$v(x,y) = IFT\left[e^{-j\,(Xx_s+Yy_s)}G(X,Y)H^*(X,Y)\right] = v(x-x_s,y-y_s\ ) \qquad (3.7)$$

Where $v(x-x_s,y-y_s\ )$ is a shifted version of v(x, y) by the same translation vector $\binom{x_s}{y_s}$ as it was at input. Thus the correlation peak follows the shift of the input image, allowing the input image to be tracked.

b) *Multiple Correlations*

When multiple shifted versions of g(x, y) are correlated with h(x, y) then multiple correlation peaks will be seen in the correlation plane with the same shift as that of at the input.

If an input scene consists of *n* multiple images (g(x, y)) with various shifts, $\binom{x_1}{y_2}, \binom{x_2}{y_2} \ldots \binom{x_n}{y_n}$, then input scene can be represented as:

$$g(x,y) = g(x - x_1, y - y_1) + g(x - x_2, y - y_2) \ldots \ldots + g(x - x_n, y - y_n) \qquad (3.8)$$

Frequency spectrum of the input scene will then be given by:

$$\begin{aligned} FT[g(x,y)] &= FT[g(x - x_1, y - y_1)] + FT[g(x - x_2, y - y_2)] \ldots \ldots + FT[g(x - x_n, y - y_n)] \\ &= e^{-j(Xx_1 + Yy_1)}G(X,Y) + e^{-j(Xx_2 + Yy_2)}G(X,Y) \ldots . + e^{-j(Xx_n + yY_n)}G(X,Y) \\ &= \left(e^{-j(Xx_1 + Yy_1)} + e^{-j(Xx_2 + Yy_2)} \ldots . + e^{-j(Xx_n + yY_n)}\right)G(X,Y) \end{aligned} \qquad (3.9)$$

Multiplying the frequency spectrum by the filter function (H(X, Y)) and inverse Fourier Transform will give the output plane distribution as given by:

$$\begin{aligned} v(x,y) &= IFT\left[\left(e^{-j(Xx_1 + Yy_1)} + e^{-j(Xx_2 + Yy_2)} \ldots . + e^{-j(Xx_n + yY_n)}\right)G(X,Y)H(X,Y)\right] \\ &= IFT\left[e^{-j(Xx_1 + Yy_1)}G(X,Y)H(X,Y)\right] + IFT\left[e^{-j(Xx_2 + Yy_2)}G(X,Y)H(X,Y)\right] \\ &\qquad \ldots + IFT\left[e^{-j(Xx_n + Yy_n)}G(X,Y)H(X,Y)\right] \\ v(x,y) &= v(x - x_1, y - y_1) + v(x - x_2, y - y_2) \ldots \ldots + v(x - x_n, y - y_n) \end{aligned} \qquad (3.10)$$

Thus the cross correlation peaks at the output would have multiple peaks at the same shift as the shifts in the input scene.

In the following section, two demonstrations are presented to illustrate the shift-invariant property of correlation filter and its ability to perform multiple correlations to detect the presence of the multiple reference images in the input scene.

3.6.2 Demonstration on Correlation Filtering

A uniform small circle (radius 3 pixels and origin as centre in 64x64 pixels square grid) is chosen as a reference image (r(x, y)) as shown in Figure 3.14 (a) r(x, y) can be described as

$$r(x,y) = \begin{cases} 1 & x^2 + y^2 \le 3 \\ 0 & otherwise \end{cases} \qquad (3.11)$$

Filter function {F(X, Y)} is then designed for the chosen reference image.

$$F(X,Y) \; = \; conj(FT[r(x,y)]) \qquad (3.12)$$

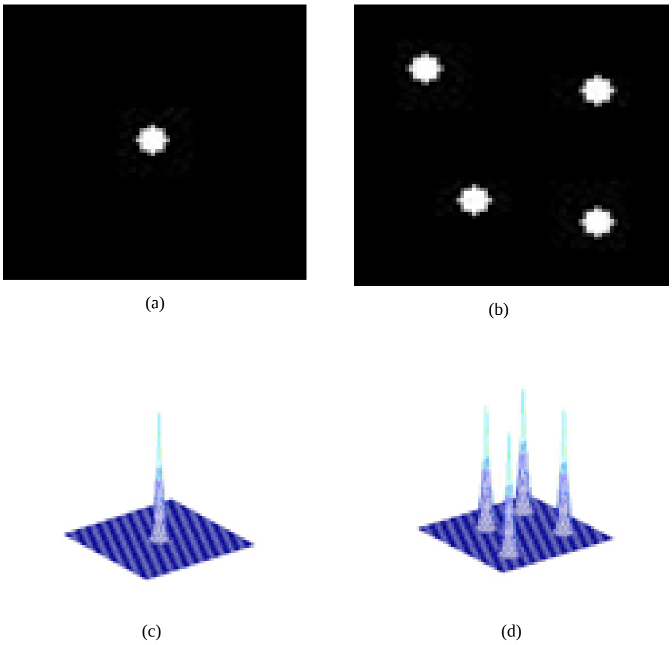


Figure 3.15: Demonstrating multiple correlations (a) a reference image (circle) with radius 3 pixels in a square of 64 × 64 pixels (white = 1 and black = 0) (b) an input scene with four randomly shifted reference images (c) Intensity distribution of autocorrelation output of the reference image (showing a single peak at the centre) and (d) Intensity distribution of cross-correlation of reference image (a) with input scene (b) (showing four peaks at the same location as in input scene)

Figure 3.15 (c) shows the intensity distribution of the autocorrelation output. As can be seen in this figure, the autocorrelation produces a sharp peak at the centre of the correlation plane. The reference image (see Figure 3.15 (a)) is then correlated with an input scene which consists of four randomly placed reference images, as shown in Figure 3.15(b). The intensity distribution of the output of this correlation is shown in Figure 3.15 (d). The results show four peaks at the same location as the input images in the input scene. The peaks are of the same height and the same width. This demonstration clearly shows the shift invariant property of the correlation operation and its ability to produce multiple correlations for each reference pattern at the input. These are the properties that were used to both detect and locate the active pores in the fingerprint images after they have passed through the high pass filter.

3.7 High-Pass and Correlation Filtering Algorithm (HCFA)

HCFA takes high resolution images and process them through the following steps:

- High-pass filtering
- Correlation filtering
- Thresholding

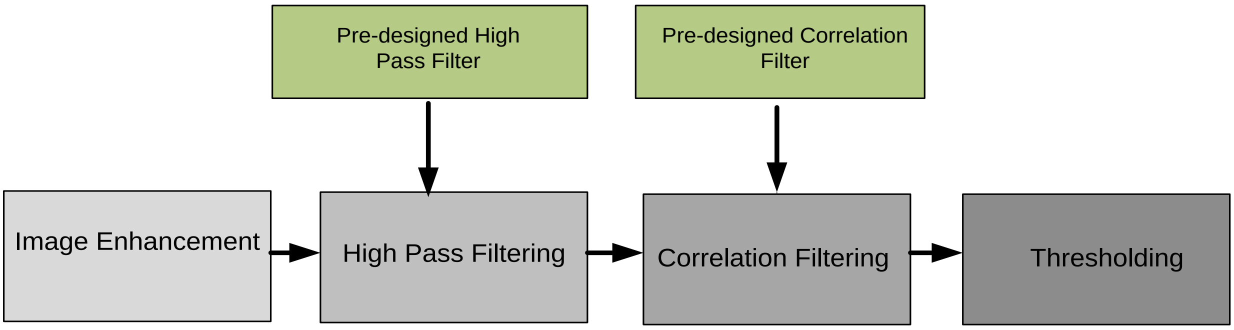


Figure 3.16 High Pass Correlation Filtering Algorithm (HCFA) processing steps

High-pass filtering removes the ridge-valley structure, while keeping the high frequency pore structures. Correlation filtering extracts and locates the pores as a set of correlation peaks. Hard thresholding is then applied to distinguish active sweat pores from inactive ones [129]. A sample of the resultant image, after going through the steps stated above is shown in Figure 3.16 the result of processing is illustrated in Figure 3.17.

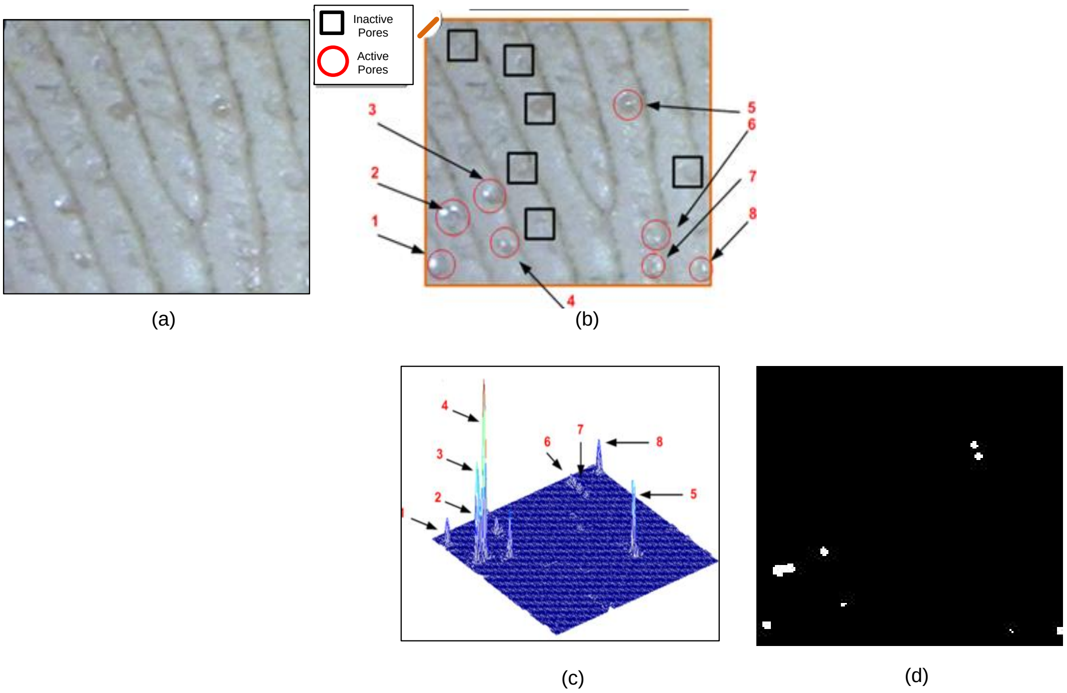
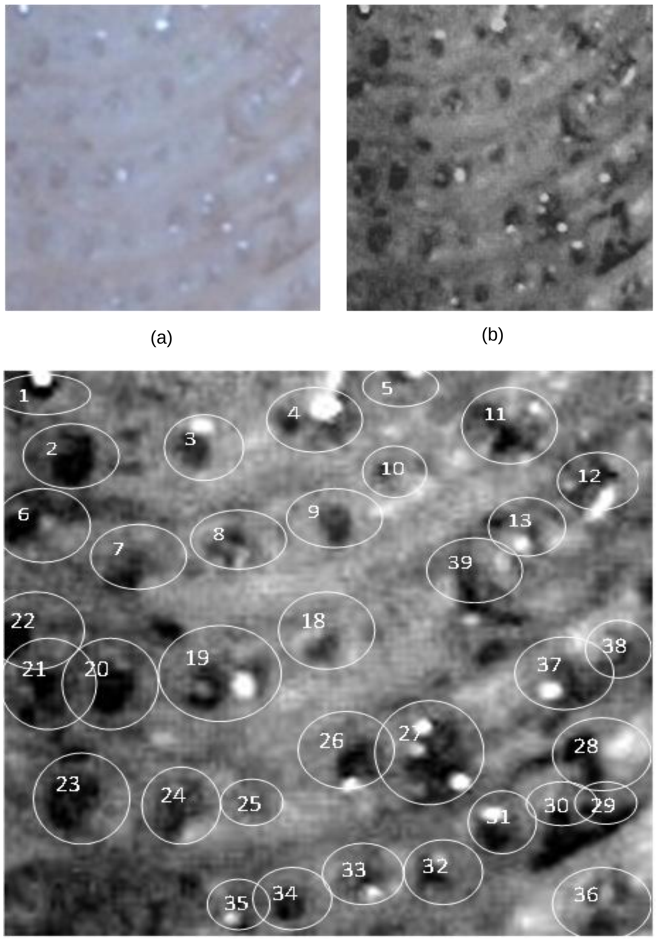


Figure 3.17 (a) Original 150x150 image from B-FBDB (b) manually marked active and inactive pores (c) Output correlation peaks represents position of active pores (d) binary output where white spots represents active pores

3.8 Manual Inspection of Pores

The history of the manual study of pores for identification goes back over a century. In its early stages, manual identification methods were used for the analysis of pore in terms of size, shape, density (number of pores in a cm^2), orientation in relation to ridges and inter-spacing (distance between adjacent pores) [101].

These studies were mainly performed in forensic applications and the images were usually microscopic ones, which have high resolution along with high magnification. These manual studies are expensive and time consuming, and definitely not appropriate for contemporary automated commercial applications. However, the work presented here invests in knowledge obtained through manual identification as it is important in validating the results obtained using HCFA.


(a) (b)

(c)

Figure 3.18 (a) B-FBDB Image (b) Gray scaled and contrast adjusted (c) Magnified image with pores circled and numbered.

Figure 3.18 shows the three images which were used to manually examine pores and their attributes. In Figure 3.18 (b) the variation in the level of gray colour indicates the depth of the structure, and the brighter section indicates sweat drops. Another fact used in this manual inspection is that pores are always on the ridges and therefore, any bright sections in valleys are discarded. The pores and pore-like features are circled and numbered for illustration and discussion.

From the manual inspection the following attributes of pores were identified:.

- **Active pores:** It is defined as those pores, which are discharging sweat liquid. In Figure 3.18 (c), this can be clearly seen as a very bright spot surrounded by very dark ring.(e.g.: 1, 3, 4, 5, 11, 12, 13, 19, 26, 27, 37, 35, 35, 32, 31 and 28).

- **Inactive pores:** The majority of pores are visible but not discharging sweat liquid. These are the pores ready to discharge sweat liquid or have just discharged liquid. Visible inactive pores can be those numbered as 2, 6, 7, 8, 9, 21, 22, 20, 18, 23, 24, 34, 36, 28, 30, and 29)

- **Scars:** It may sometimes be that scars (permanent or temporary) on the finger can be distinguished in the images used in this research (e.g. 14 is a scar).

- **Size of Pores:** The size of the pores varies, and in most cases it is difficult to come up with a single parameter to specify the size as the pores are generally irregular shapes. Two categories of pores are identified: small & medium, and large & very large. Small & medium sized pores are those numbered as 1, 3, 5, 8, 9, 13, 15, 18, 29, 30, 31, 32, 33, 34 and 35, and Large & very large are those numbered as 2, 6, 7, 11, 12, 17, 19, 20, 21, 22, 23, 24, 26, 27, 28, 32 and 34.

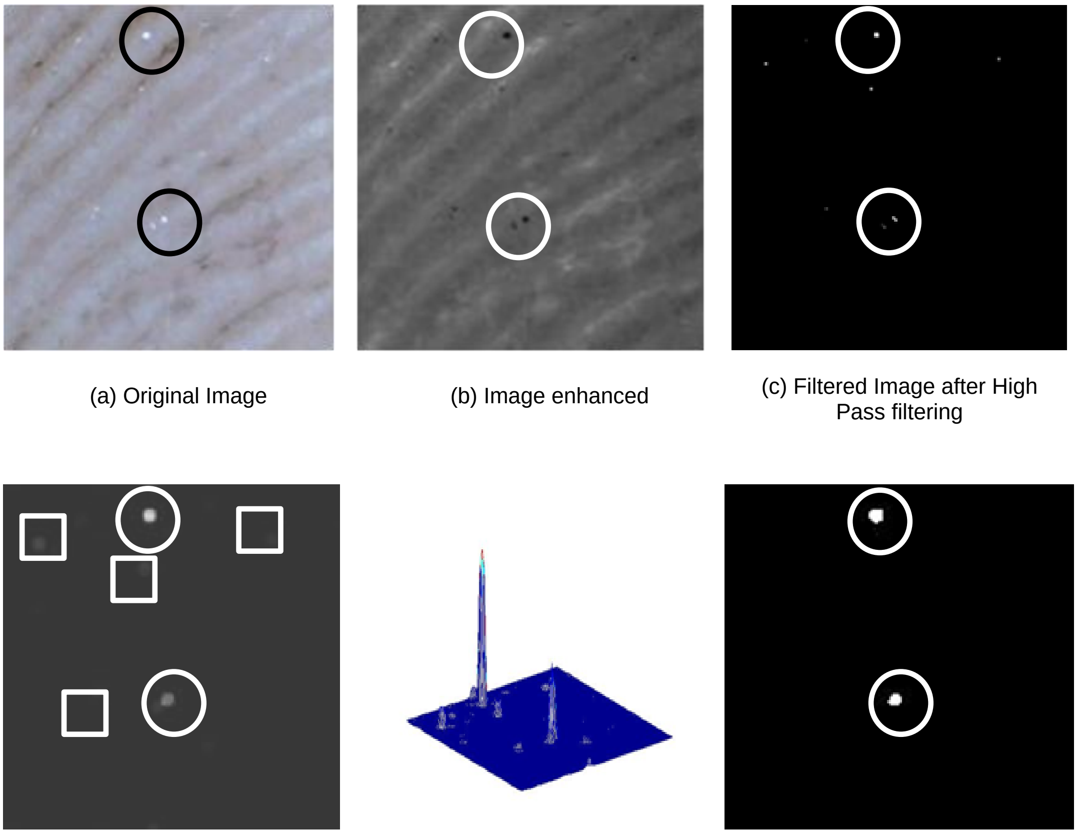
- **Multiple Pores:** There are instances where two or more pores are clustered together and these kinds of pores are called multiple pores (e.g. 19 & 27)

- **Shape:** A range of pore shapes can be identified in a typical fingerprint image, mostly being irregular shapes. The commonly identified shapes can be approximated to a circle, a rectangle or polygon.

Due to the varying attributes of the pores, the task of detecting of active pores is very challenging in both manual and computerised automated algorithms.

3.9 Demonstration on HCFA

A demonstration is presented in Figure 3.19 to illustrate the HCFA. It consists of six images, each with numbers in square bracket to cross reference with the output from each stage in the HCFA illustrated in Figure 3.19. The size of images is 150×150 pixels.



(a) Original Image

(b) Image enhanced

(c) Filtered Image after High Pass filtering

(d) Correlation Spots after correlation filtering

(e) Correlation Spots

(f) Binarized Output after thresholding

Figure 3.19 (a) is an original raw camera captured image and it shows two open pores as white openings. (b) Enhanced image shows opened pores as black openings (c) correlation spots on image after correlation step d) correlation peaks represent active pores (f), active pores and their processed versions are indicated by a set of circles.

The enhanced image is then passed through a rectangular high-pass filter (See Figure 3.19(a)) with a cut-off frequency of 37 pixels in both X and Y direction. This value of high-pass filtering is chosen empirically to get the best results at the output.

Figure 3.19 (c) is the image after high-pass filtering and it shows a number of white pixels in a black background. A careful examination reveals that most of the white pixels correspond to the open pores. The high-pass filter removed the ridge-valley pattern and the high frequency open pores remain, other high frequency structures, such as dirt and temporary marks in the fingerprint.

Figure 3.19 (d) and (e) are the outputs of the correlation stage. Figure 3.19 (d) is a gray scale intensity representation, and Figure 3.19 (e) is the respective 3D mesh representation. A small uniform circle with a diameter of four pixels is used as the reference pattern in the correlation operation. As can be seen in Figure 3.19 (d), a set of spots with a range of intensities can be seen. Careful examination reveals that these spots occur on opening pores. Bright spots result from larger open pores and dimmer spots result from of the small open pores that are almost closed.

Since the aim of this work is to identify fully opened pores, a threshold values were selected by the empirical method by applying different threshold values in HCFA. The small variation in threshold value has significant impact on the number of output white spots which represents active pores. Threshold value 0.2 was selected from the observations and applied to images in Figure 3.19 (d) to remove the spots relating to pores which are not fully dilated (these are indicated by squares in Figure 3.19 (d)). The results are presented in Figure 19 (f). This image shows two white spots in a black background. These white spots correspond to the active pores in the original image. In the rest of sections, the terms 'desired spots' and 'undesired spots' will be used to refer the spots which belong to the active or inactive spots respectively [135].

3.10 Results and discussion

Initially, twenty images from B-FBDB were used to validate the HCFA. The effect of the threshold in the algorithm performance was analysed based on two performance measures, Detection Efficiency (DE) and Discrimination Ability (DA), using standard statistical measures such as mean, median and inter-quartile range.

For further investigation in threshold levels, 0.05, 0.10, 0.15 and 0.20 levels were selected and applied for twenty images. The threshold values used to test and obtain the best threshold value for the algorithm. As already mentioned in section 3.9, these threshold values that gave a significant variation in the number of desired spots, and hence chosen for investigation. Furthermore these threshold levels were applied to process 120 Images. The following features were counted and recorded for all processed images:

1. Total number of white spots in the final output (t)
2. Number of desired spots in the final output and (d)
3. Number of active pores in the original image (u).

DE and DA were calculated for all twenty images using the results above.

3.10.1 Detection efficiency

DE is the ratio of the number of desired spots in the final output to total number of active pores in the input fingerprint image (eq. 3.13).This measure gives an indication how efficient the algorithm is in detecting active pores.100% means that all the pores detected were active and 0% means that all the pores detected were inactive.

$$\text{Detection Efficiency (DE)} = \frac{\text{Detected active pores}}{\text{Total active pores}} \times 100 \qquad (3.13)$$

3.10.2 Discrimination ability

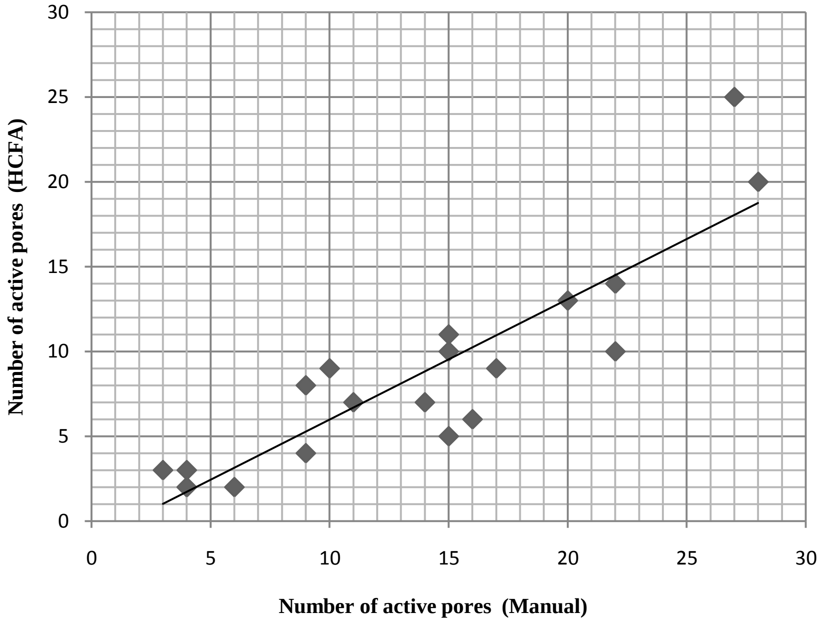
DA is the ratio of number of desired spots to total number of spots in the final output (eq. 3.14). This measure gives an indication of how good the algorithm is at discriminating active pores from other high frequency structures including inactive pores.

$$\text{Discrimination Ability (DA)} = \frac{\text{Detected active pores}}{\text{Total detetcted spots}} \times 100 \qquad (3.14)$$

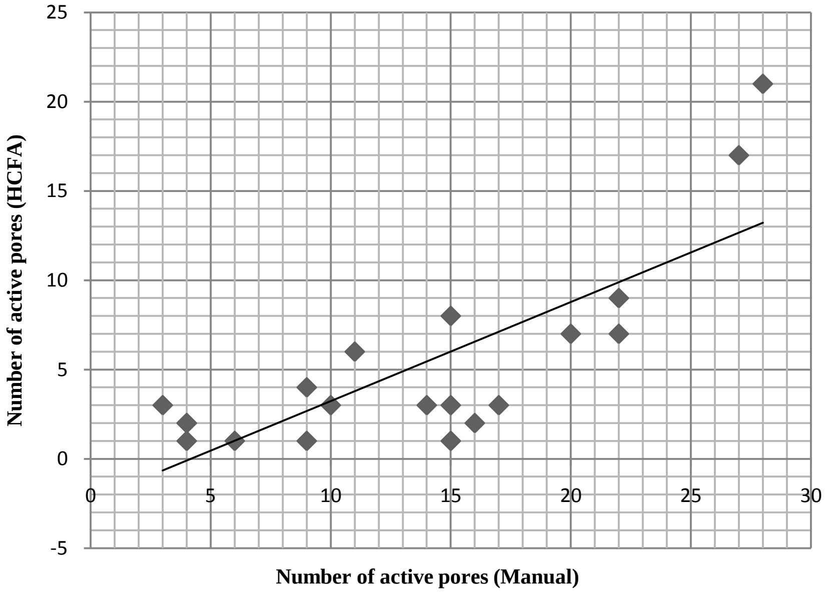
Furthermore, basic statistical analysis (mean, median and Inter Quartile Range (IQR)) was also performed on the results obtained to investigate the impact of the threshold values in the final performance.

This measure gives an indication of how good the algorithm to discriminate active pores from other high frequency structures including inactive pores. Again 100% means all of the spots detected, all are desired and 0% means all of the spots detected, none are desired.

DE and DA were calculated for all twenty images. Scatter graphs between active pores manual identification and results of HCFA on 20 B-FBDB are presented in Figure 3.20 (a) & (b) and results with 120 B-FBDB are presented in Figure 3.21 (a) and (b).

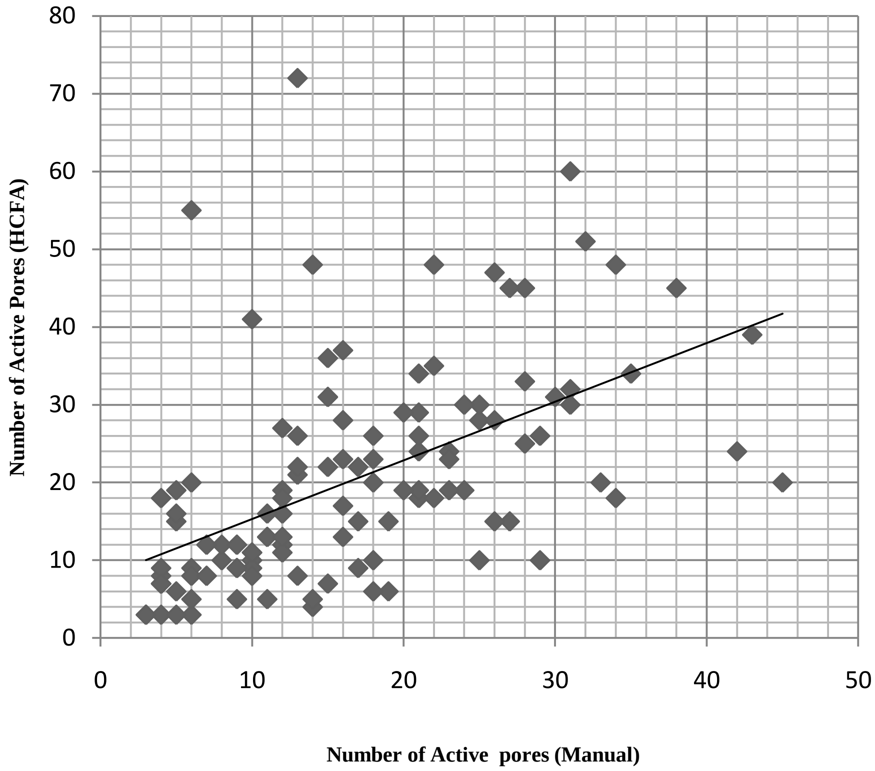


(a) Threshold - 0.05

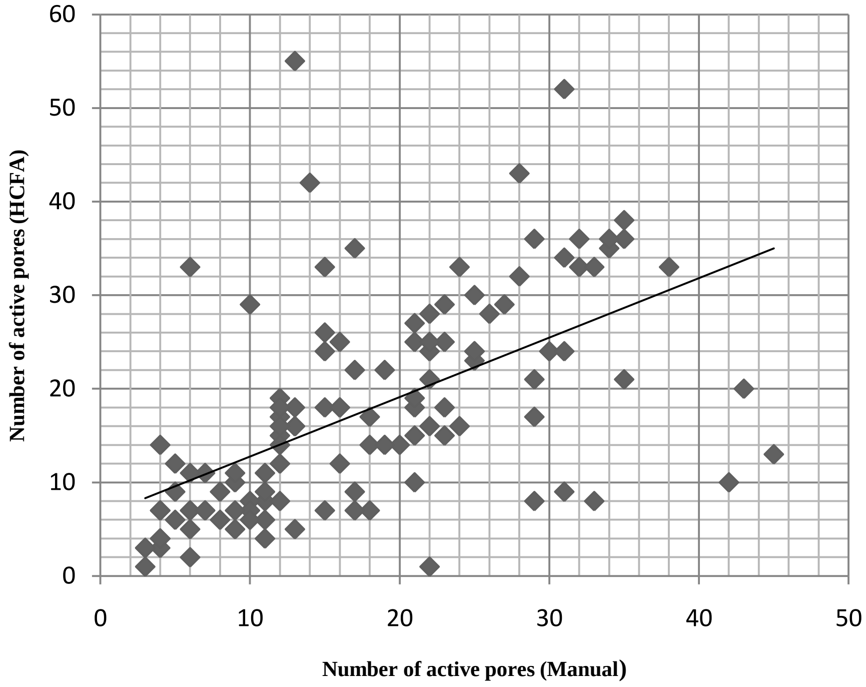


(b) Threshold - 0.10

Figure 3.20: Scatter Graph of identification of active pores in 20 B-FBDB images of both manual and HCFA (a) Threshold Value – 0.05and (b) Threshold - 0.10 (Diamond indicates the actual data and line indicates line of best fit



a) Threshold- 0.05



b) Threshold-0.10

Figure 3.21: Scatter Graph of identification of active pores 120 B-FBDB both manual and HCFA (a) Threshold Value – 0.05and (b) Threshold - 0.10

Resultant graphs clearly illustrate positive correlation between the manual identification and HCFA based identification. This means when there are more active pores in the fingertip, then there will be more desired spots in the output detected by HCFA [135].

The scatter graphs of other threshold values obtained showed similar tendency, therefore they are not presented here. However, a correlation coefficient between numbers of active pores obtained by manual identification and that from HCFA is calculated for all the four threshold values (0.05, 0.10, 0.15 and 0.2) and presented in Table 3.7.

Correlation coefficient 1 means there is a perfect match between the two data sets (meaning that the rate of increase is the same in both datasets) and -1 means there is negative perfect match (meaning that as one data set increases by an amount other data set decreases by the same amount) and 0 means no correlation between the two data sets.

The equation used for calculating the correlation coefficient (r) between two data sets of size 'n', say data set1- {x1, x2, x3 ……xn }and data set2- {y1, y2, y3, …….yn}, can be given by equation (3.15):

$$r = \frac{\sum_{i=1}^{n}\{(x_i - \overline{x})(y_i - \overline{y})\}}{\sqrt{\sum_{i=1}^{n}(x_i - \overline{x})^2 \ \sum_{i}^{n}(y_i - \overline{y})^2}} \qquad (3.15)$$

where $\overline{x}$ and $\overline{y}$ mean of data set 1 and data set 2 respectively.

The data shown in Figures 3.21 shows a positive correlation between manual and HCFA based active pore identification. However, as the threshold value decreases the correlation coefficient also decreases. This is because as the threshold value increases the more desired spots are discarded by HCFA. Another set of statistics are also calculated to understand the effect of the varying threshold in the HCFA. The results of Mean, Median and Inter Quartile Range (IQR) of DE and DA are tabulated in Table 3.7 IQR is the difference between Lower Quartile (LQ) {a cut-off value of the lower 25% of an ordered (ascending) data set} and Upper Quartile (UQ)) {a cut-off value of the upper 25% of an ordered (ascending) data set }.

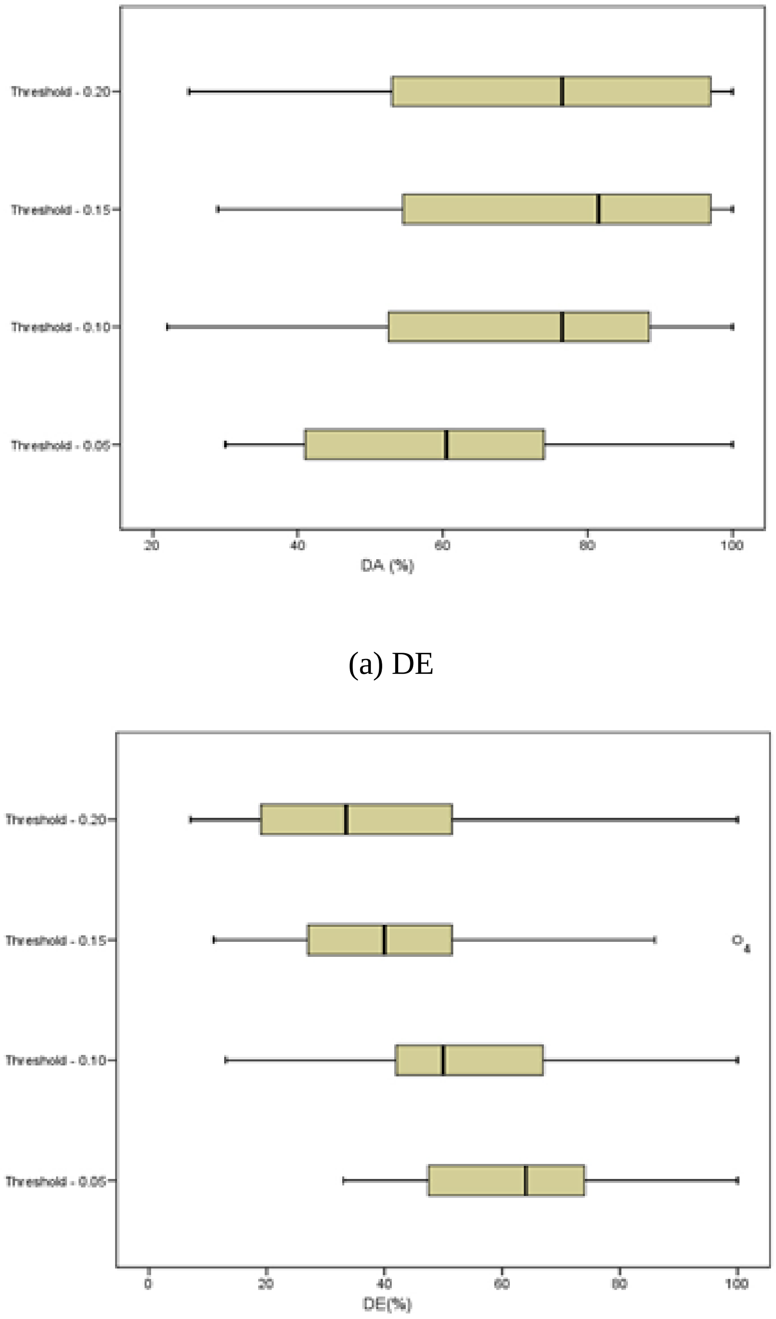
Type of Statistical Measure		**Threshold**			
		0.05	0.10	0.15	0.20
Correlation coefficient		0.90	0.83	0.81	0.79
DE	Mean	62.4	53.2	42.0	38.0
	Median	63.6	50.0	40.0	35.0
	LQ	48.9	42.4	28.3	19.4
	UQ	74.2	66.8	51.7	51.7
	IQR	25.3	24.4	23.4	32.3
DA	Mean	59.8	70.9	73.5	72.7
	Median	60.0	75.0	80.0	75.0
	LQ	41.3	52.8	54.9	54.2
	UQ	74.2	85.4	97.2	97.2
	IQR	32.9	32.6	42.3	42.5

Table 3.7: Statistical measures for four threshold values (0.05, 0.1, 0.15 and 0.2)

Figure 3.21 (a) shows how DE varies for various threshold values. As the threshold value decreases the box is moving towards the right and it implies that in general less DE is achieved for higher threshold values. This is because desired spots were detected for an increasing threshold value. However, no significant degradation is observed for the threshold value change from 0.15 to 0.20. From these results it can be concluded that a lower threshold value is required for a better DE. IQRs of Box plots shown in Figure 3.21 (a) are reasonably low (~20 to 25%), which means that the HCFA produces fairly consistent results in terms of DE.

The box plot in Figure 3.22 (b) show how DA varies as threshold values vary. In contrast to DE, DA increases as threshold values increase. Better discrimination between desired spots and undesired spots is achieved for increased threshold values. This is because more undesired spots are eliminated than that of desired spots as threshold value is increased, making the DA higher. Again no significant improvement is observed for the threshold values 0.15 and 0.20. IQR of DA is larger compared to the IQR of DE, though it is still less than 50%.

The positions of the box plots of DA are more to the left than that of DE. Thus, in general, the HCFA has a higher DA than that of DE. However, as already mentioned, it is desirable that both DE and DA should have higher values for better detection of active sweat pores.



(a) DE

(b) DA

Figure 3.22 (a) Box Plots for four threshold values (a) Detection Efficiency (DE) and (b) Discrimination Ability (DA).

None of the box plots shows 0% of DE or DA and this implies the HCFA always detects at least a few active pores. Even a few active pores can in fact determine the liveness of the finger. Therefore, HCFA algorithm has been 100% successful in terms of detection of liveness.

3.11 Reference pattern investigation

When two identical patterns are correlated the maximum peak intensity valued correlation spot (max peak) can be obtained. The fully opened pores are of various shapes and sizes and therefore, it is not possible to get a single pattern of the active pore to get the max peak. However, it is possible, but not straightforward, to find an optimum pattern so that when it is correlated with the extracted active pores, can give the best achievable maximum peak. To find out the optimum pattern for correlating open pores, a systematic investigation was carried out using two different types of shape as the reference pattern, a circle and a square in five different sizes (See Figure 3.23).

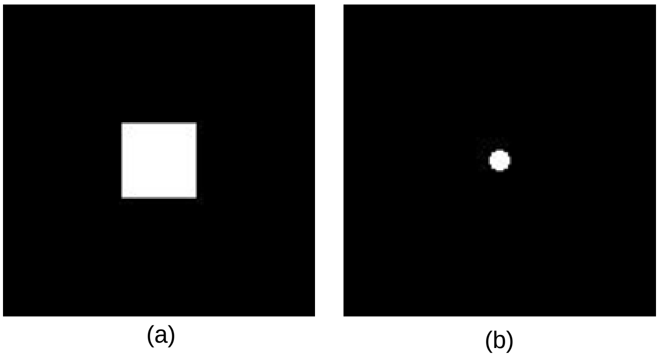


Figure 3.23 (a) Rectangular high-pass filter function and (b) Circular reference pattern

In this investigation, a fingerprint image is chosen with many active pores and many slightly visible inactive pores. Active pores are manually identified and indicated by small circular rings in Figure 3.24. Note the size of the image is 150 ×150 pixels.

The HCFA algorithm is applied to the image with a high-pass filter cut-off frequency of 36 pixels. The threshold value of the algorithm is tuned to get the optimum results and it is found, by trial and error, to be 0.01 for this image. The threshold is another area that needs investigation to get optimum results with the HCFA. The large brightness variation in the active pores, as can be seen in Figure 3.23, is the main indication of lower threshold values.

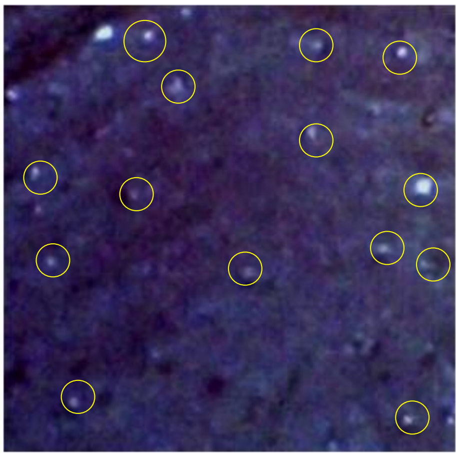


Figure 3.24: A Fingerprint Image with 14 active pores and indicated by ring circles.

Reference patterns of two shapes (circle and square) and five different sizes (2, 4, 6, 10 and 14 pixels) are used in this investigation. For a circle the size means diameter, and for a square it is the length of one side.

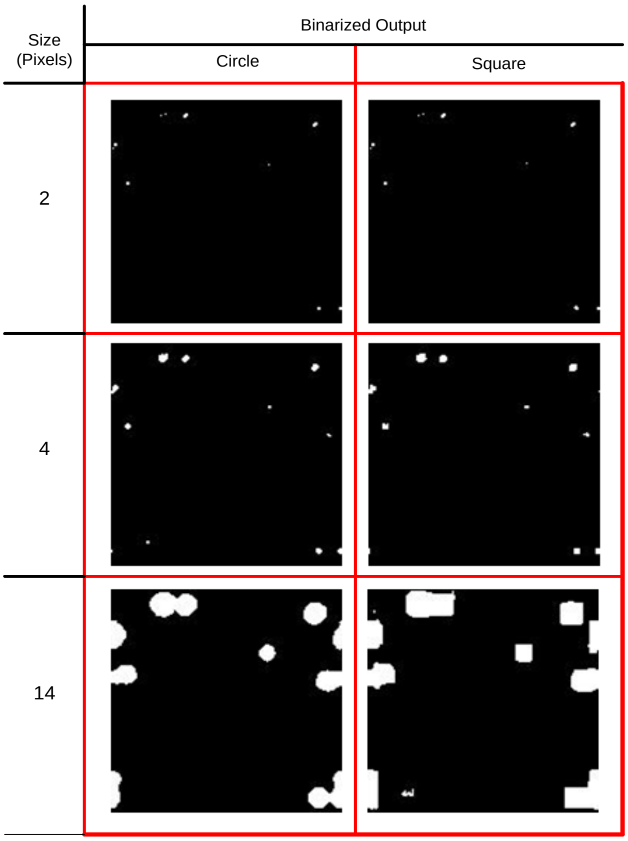


Figure 3.25 : Binarized output for three different sizes and two shapes of reference patterns (S- size of reference pattern in pixels)

Figure 3.25 shows the results obtained for this image for three sizes of the reference pattern (2, 4 and 14). This shows the binarized output image which should, in theory, belong to the active pores. The circular reference pattern produces circular white spots, and the square reference pattern produces square white spots. As the size of the reference patterns increases the white spots also increase in size, and for the sizes 10 and 14 some white spots start to merge with the adjacent white spots, which cause difficulties in calculating the performance measures. When a desired spot merge with an undesired spot, the problem arises as to determining whether the merged spot is desired or not desired. As it is important to have an accurate measure of performance, the following criterion was established.

Desired spot + desired spot = desired spot
Desired spot + undesired spot = undesired spot
Undesired spot + undesired spot = undesired spot

Using these criteria DE and DA are calculated and presented in Table 3.8.

Type of reference pattern	**Size (Pixels) (circle: diameter & Square: length)**	**DE (%)**	**DA(%)**
Circle	2	50	70
	4	64	82
	6	57	62
	10	50	64
	14	28	33
Square	2	50	70
	4	64	82
	6	57	62
	10	50	64
	14	28	44

Table 3.8 DE and DA of the HCFA algorithm for the fingerprint image given in figure 22 using circle and square as the reference patterns with three different sizes

As shown the best DE achieved was 64% for both circle and square reference pattern when the size is 4 pixels. The best DA was 82% for both circular and rectangular reference pattern when the size is 4 pixels. These results show that there is no significant difference between the shapes, but the size of the reference pattern can make a real difference in terms of clear and distinguishable spots so that spots can be easily countable.

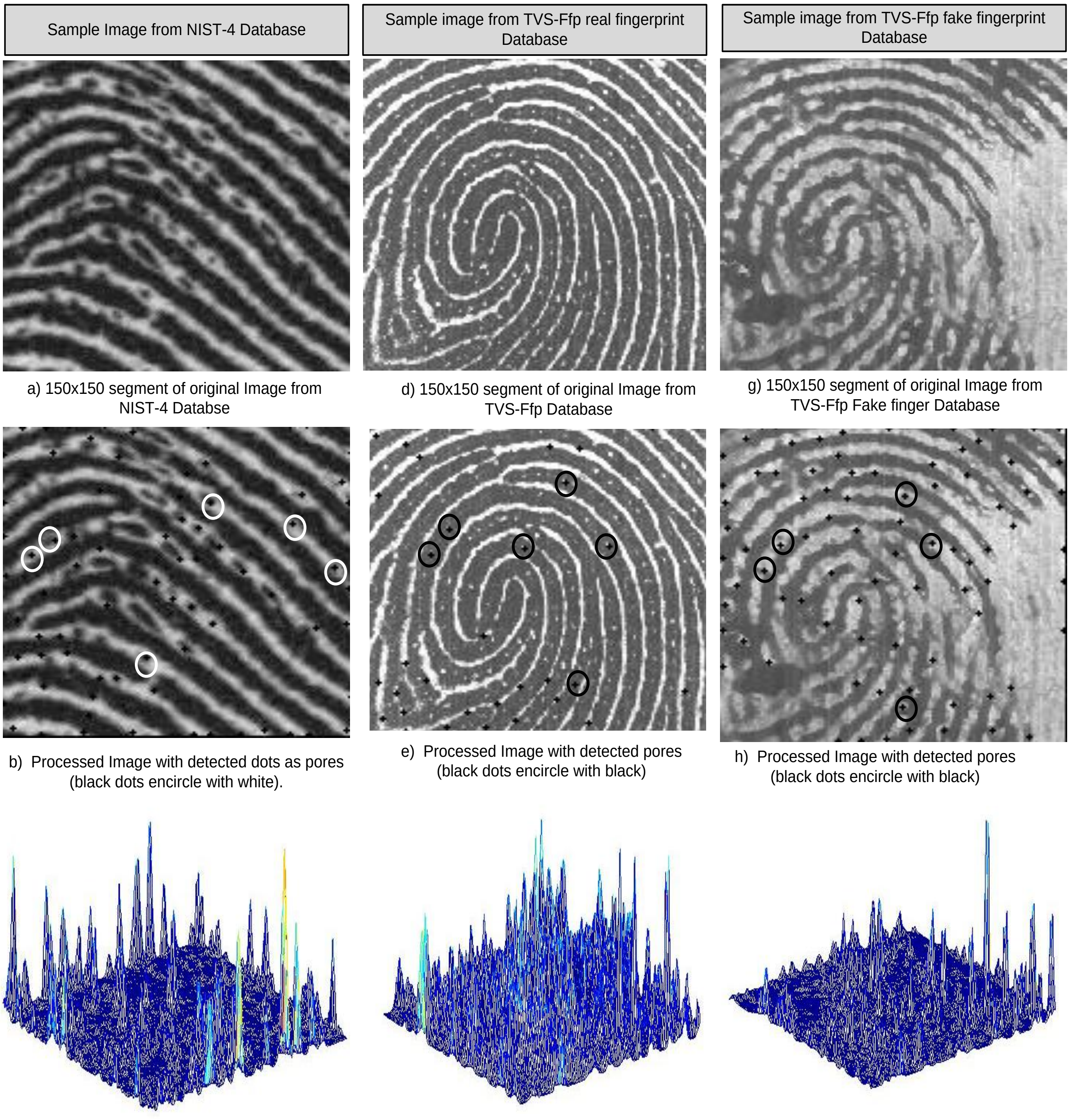
3.11 Testing of HCFA on other databases

HCFA was tested on other live scan Databases. The testing includes images from NIST-4 and three other Databases (TVS-Ffp Real finger, TVS-Ffp fake fingerprint Database and PolyU HRF) which we have obtained from other fingerprint biometrics research groups. All these sample image were captured by using optical methods. Initially, a random good quality image was selected from each Database and the centre segment of each image was cropped with 150 x150 dimensions. It is observed in the manual study of fingertips that the centre region of finger tips always contain more active pores than other regions of fingertips.

Figure 3.25 illustrates the step by step process on a NIST-Database 4 segmented image. In (a) the ridges (black), valleys (white) and minutia are very clear to see. However, there is no pore, either active or inactive, visible on the ridges. There are some scars or noise visible on the valleys and these were detected as pores in Figure 3.25 (b) showing as black dots; some are encircled with white to make it easily visible. The final result is presented as correlation peaks in Figure 3.25 (c). In the final result, the correlation peaks do not actually represent active or inactive pores, but rather the scars or noise present on the valleys in the image.

In the next step, a segment of 150x150 from TVS-Ffp database, a real fingerprint image, was processed with HCFA. Figure 3.25 (d) illustrates an original fingerprint segment from TVS-Ffp real finger Database. This image was captured with Biometrica FX2000, optical technology based fingerprint sensor with 512 DPI resolution. The ridge, valley and minutia are clearly visible, as are pores on the ridges. Detected pores on ridges are on the image, detected pores on ridges are presented as black dots, some of which are encircled in black (See Figure 3.25 (e)).There are black dots are the valleys highlighted with a white circle but they are not actually pores.

After processing one TVS-Ffp real fingerprint segment with HCFA the final correlation peaks are shown in Figure 3.25 (f). The correlation peaks are complex and it is difficult to distinguish between the pores and other features detected by HCFA.



Sample Image from NIST-4 Database

Sample image from TVS-Ffp real fingerprint Database

Sample image from TVS-Ffp fake fingerprint Database

a) 150x150 segment of original Image from NIST-4 Databse

d) 150x150 segment of original Image from TVS-Ffp Database

g) 150x150 segment of original Image from TVS-Ffp Fake finger Database

b) Processed Image with detected dots as pores (black dots encircle with white).

e) Processed Image with detected pores (black dots encircle with black)

h) Processed Image with detected pores (black dots encircle with black)

c) Output correlation peaks of NIST-4 Database

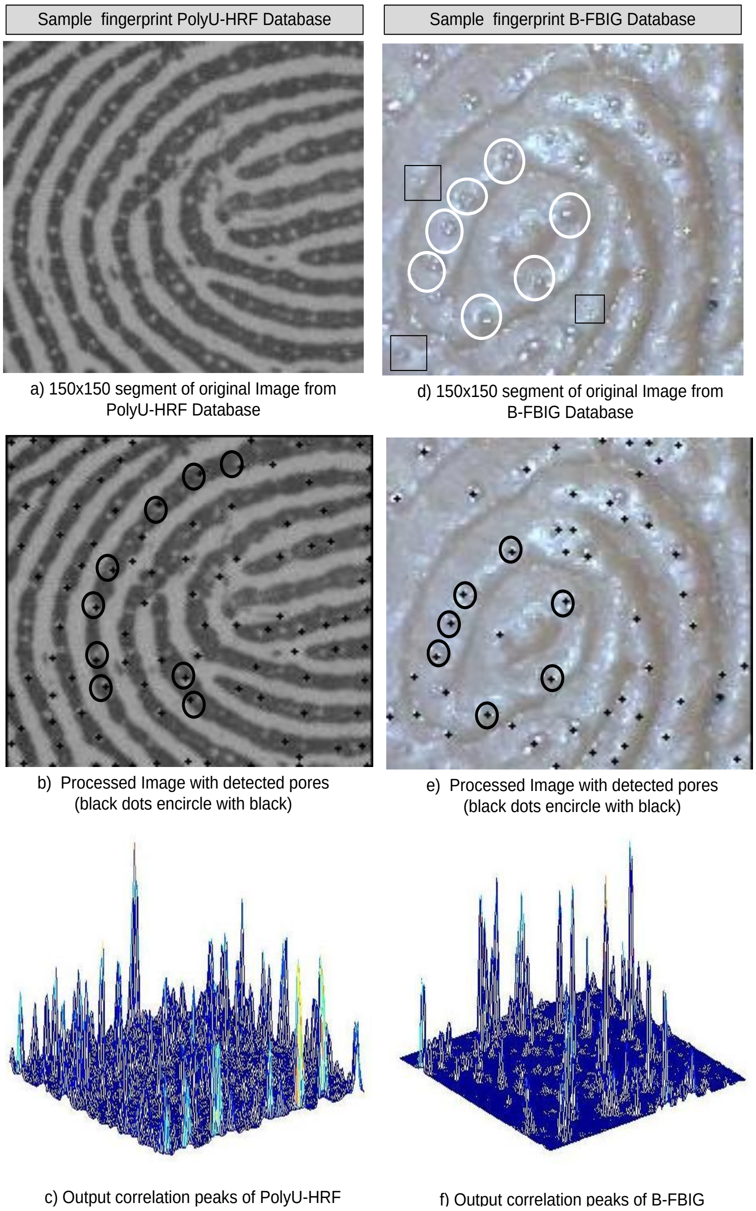
f) Output correlation peaks of TVS-Ffp real fingerprint Database

i) Output correlation peaks of TVS-Ffp fake fingerprint database

Figure 3.26: HCFA test on NIST-4, TVS-Ffp original and fake fingerprint

A sample image Figure 3.26 (g) from TVS-Ffp fake fingerprint was processed with HCFA. Figure 3.26 (e) is a scanned fake stamp of a fingerprint captured with the same Biometrica FX2000 optical fingerprint sensor. Clear differences of quality and features are visible in both images (Figure 3.26(e) & (g)).

In these fake finger images, the valleys are represented by white and the ridges are represented by black. In this image segment, there are only a few pores visible on the ridges. This is evidence that replicating pores, whether active or inactive on fingertip ridges is difficult in preparing fake finger stamps. However, ridges, valleys and minutiae points can be replicated easily. Some detected pores in the image in Figure 3.26 (h) are encircled in black and the same pores are encircled in the real fingertip image (See Figure 3.26 (e)). The output correlation peaks are also less than the original one and not exactly presenting the position of pores.


Sample fingerprint PolyU-HRF Database
Sample fingerprint B-FBIG Database

a) 150x150 segment of original Image from PolyU-HRF Database

d) 150x150 segment of original Image from B-FBIG Database

b) Processed Image with detected pores (black dots encircle with black)

e) Processed Image with detected pores (black dots encircle with black)

c) Output correlation peaks of PolyU-HRF

f) Output correlation peaks of B-FBIG

Figure 3.27 HCFA test on PolyU-HRF and B-FBDB original and fake fingerprint

The third test of HCFA was done on an image from the PolyU-HRF database. This database is one of the high resolution optical fingerprint databases used for research on pore pattern investigation. Images were captured with specifically designed optical scanner with 100 DPI resolution and pores are clearly visible on each fingerprint. A segment of a sample image from the database is illustrated in Figure 3.27 (a). The valleys are shown in white and the ridges are in black with white pores. HCF detected pores, circled in black, as shown in Figure 3.27(b); output correlation peaks in Figure 3.27(c) mostly relate to these detected pores. However, there is no difference is observable in active or inactive pores.

The final image segment is from B-FBDB (see figure 3.27 (d)), which was captured with a micro capture camera. Active pores (Active Pores = white circle and Inactive = Black rectangle) are clear to see in the image. The majority of active pores are detected by HCFA and shown as black spots in (e). Almost all correlation peaks represent the positions of active pores.

3.12 HCFA parameters

There are a number of parameters to be set in the algorithm in order to obtain the best set of results. It is not possible to determine these parameters analytically, and therefore an investigation should be carried out in order to understand the effect of these parameters empirically. Details of all three parameters which appear in the main stages of the algorithm are further explained here:

High-pass filtering: **Cut-off frequency** as shown in the demonstration (see Figure 3.14).
Various cut-off frequencies of the high-pass filter gave various sets of results. Through a number of experimental runs of the algorithm, for a set of images of 150 x 150 pixels, it was found that a cut-off frequency of 37 pixels in both X and Y directions give the optimum results to extract the pores and remove ridge-valley structure.

Correlation filtering: **Size and shape of reference pattern** It can be seen that size and shape of the reference pattern can make a significant difference in the height and width of the correlation peaks, due to variation in the shape and size of the active pores in a typical fingerprint image (see Figure 3.1). Higher, narrower, well-separated and uniform peaks are always desirable properties in correlation filtering. Through a number of experimental-runs, it was found that a reference pattern of circular shape with size of 4 pixels diameter can give optimum results, hence it was adapted in this work.

Thresholding: Threshold value This is the parameter which is used to differentiate between the peaks obtained for active pores and those of in-active pores. Again this value cannot be determined analytically, and therefore, a number of experimental runs are needed to find the best threshold value for the fingerprint images. It was found that threshold values between 0.05 and 0.2 make a significant variation in the algorithm performance. Low threshold value indicates that there is a great non-uniformity among the correlation peaks, which is due to varying brightness, shape and size of the active pores.

There are many image processing techniques such as wavelet was used to detect the noise level differences between real and fake fingerprint images as a sign of liveness (Table 2.2); however, HCFA was particularly developed to present and clarify the novel idea of detecting active pores as sign of liveness. At this level of research HCFA was not tested or compared with other techniques proposed in literature. The results obtained with HCFA are very positive; however, in the future further research is possible to use and test the wavelet or other image processing techniques to detect active pores in B-FBDB.

3.13 Summary

Liveness detection can be performed by detecting active sweat pores on fingertip ridges. The task of detecting active sweat pores is challenging due to the number of varying attributes of active sweat pores. The newly developed HCFA is a possible solution for liveness detection, in that it locates active sweat pores on the fingertip.

A validation of HCFA was performed using images from B-FBDB obtained from different subjects. The results were analysed using two newly defined performance measures, Detection Efficiency (DE) and Discrimination Ability (DA), along with a number of standard statistical measures. Four different threshold values were applied to these fingertip images in order to investigate the effect of the threshold value in the performance of the HCFA.

Tests of HCFA were compared with three other databases to further understand the ability of pore detection in each system. However, HCFA produced reasonably good results in the majority of the cases in terms of DE and DA. According to the results presented, HCFA was 100% successful in establishing liveness of fingertip. This highlights great potential for future research into liveness detection for fingerprint biometrics

Chapter 4: Measurement of Ionic Activity of specially Formulated Sweat

In chapter 3 the HCFA technique for the detection of active sweat pores from high resolution fingertip images was discussed and explained in detail. Further work in this research is extended to detect the ionic activity over the surface of sweat fluid that appears at the openings of active pores. Due to high conductivity in sweat fluid, ionic activity will appear at the surface, as can be detected by measuring the surface charge of the sweat fluid. Here, a prototype experimental set up was developed and used to measure the surface charge with an eccrine gland sweat fluid sample, which was prepared in the lab from chemicals with the same composition as natural sweat fluid secreted from the active sweat pores. The measurement setup was based on a micro needle electrode inside a Faraday cage with temperature and humidity sensors. The Micro Needle Electrode (MNE) was connected to an Electrometer for measuring the surface charge in small droplets of sample sweat fluid, mimicking the actual situation when a tiny amount of ionic fluid is secreted. In an actual scenario, to measure the surface charge in sweat fluid on active pores, the MNE should not touch the sweat fluid. There should be a gap between the MNE tip and the surface of sweat fluid droplets. That situation was replicated in the measurements taken during the experiment and in the modelling. The experiment measurements were taken from 10 different positions (50-360 µm) above the surface of the droplets; 6-10 nC of surface charge was measured in the 1-10 µl volume of sample sweat fluid droplets. Furthermore, a Finite Element (FE) model of MNE and ionic fluid interface was developed with COMSOL multi-physics to understand and visualize the electric field detected by the MNE. This experimental study and modelling was undertaken to explore the possibility of developing a nanotechnology based sensor for detecting ionic activity of active sweat pores.

4.1 Eccrine gland sweat fluid

The skin is the largest organ of the human body that protects us from external factors such as bacteria, chemicals, and heat. The average person has millions of sweat glands within the skin, and they are distributed over the entire body [70], Eccrine gland sweat is a type of ionic fluid which is composed of more than 95% water and some organic and inorganic substances [136]. It was observed in a study made by visual comparison, of high resolution fingertip images from the B-FBID images, the amount of sweat comes that comes out from a single pore is small (might be in µL quantities), and each sweat droplet appears different in size, with the common shape of an inverted bowl, or a cap of sphere like structure (Chapter 3, Figure 3.1 b & C).

Inorganic (Major)	**Quantity**	**Inorganic (Trace)**	
Calcium	3.4 mEq/l	Cobalt	
Iron	1- 70 mg/l	Copper	
Potassium	4.9 - 8.8 mEq/l	Lead	
Sodium	34 – 266 mEq/l	Manganese	
Bicarbonate	15-20 m*M*	Mercury	
Bromide	0.2 - 0.5 mg/l	Molybdenum	
Chloride	0.52 - 7 mg/l	Tin	
Fluoride	0.2 - 1.18 mg/l	Zinc	
Iodide	5-12 µg/l		
Phosphate	10-17 mg/l		
Sulphate	7-190 mg/l		
Ammonia	0.5-8 m*M*		
Organic (General)	**Quantity**	**Organic (lip**	**Quantity**
Amino Acids	0.3-2.59 mg/l	Fatty Acids	0.01-0.1 µg/ml
Creatine	N/A	Sterols	0.01-0.12 µg/ml
Creatinine	N/A	**Organic:** Chemical compounds that occur mainly outside of livi once living organisms, such as those in rocks, minerals, and ceran	
Glucose	0.2-0.5mg/dl		
Glycogen	N/A		
Lactate	30-40m*M*		
Proteins	15-25 mg/dl		
Pyruvate	0.2-1.6m*M*		
Urea	10-15 m*M*		
Uric Acid	N/A		
Vitamins	N/A		
Miscellaneous			
Enzymes			
Immunoglobulins			

mEq/L= Milliequivalent per litre
m*M*=Milli Mole
mg/L= Milligram per litre
µg/L= Microgram per litre
mg/dL= milligrams per decilitre

Table 4.1: Quality of compounds in standard eccrine gland sweat fluid [137]

		Inorganic (Major)	Quantity	Inorganic (Minor)	Quantity
1	+	Calcium	3.4mEq/l	Cobalt	Trace
2		Iron	1- 70mg/l	Copper	Trace
3		Potassium	4.9 - 8.8mEq/l	Lead	Trace
4		Sodium	34 - 266mEq/l	Manganese	Trace
5	-	Bicarbonate	15-20 m*M*	Mercury	Trace
6		Bromide	0.2 - 0.5 mg/l	Molybdenum	Trace
7		Chloride	0.52 - 7 mg/l	Tin	Trace
8		Fluoride	0.2 - 1.18mg/l	Zinc	Trace
9		Iodide	5-12µg/l		
10		Phosphate	10-17mg/l		
11		Sulphate	7-190 mg/l		
12		Ammonia	0.5-8m*M*		

Table 4.2 Quality of compounds used in preparation of EGIF (Using reference [137])

The quantity of sweat fluid from a pore depends on an individual's physiological characteristics and environmental conditions [136]. According to the reported literature [137], the organic and inorganic compounds and the amounts found in eccrine gland sweat is listed in Table 4.1

For purposes of this experiment a sweat sample was prepare using only inorganic compounds. Organic compounds were not added to the sample, as they do not have any effect on the increase or decrease of ions in the fluid. The quantity of inorganic compounds used in the sweat sample is listed in Table 4.2. This sample of ionic fluid is referred to as "Eccrine Gland Ionic Fluid" (EGIF) in the rest of the chapter. The conductivity of the EGIF, measured using a conductivity meter, was 15.17 ms.

4.2 Experimental setup

This experimental setup is based on six components and each component is described the in following section. The design of the experimental setup, and an illustrating photograph, can be seen in Figure 4.1 and 4.2, respectively.

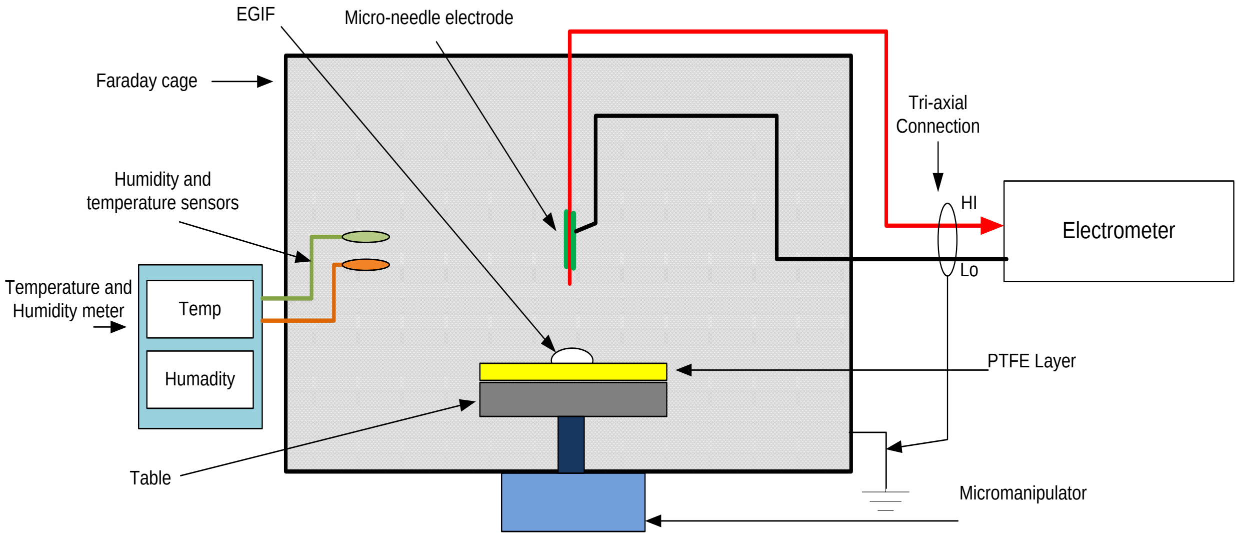


Figure 4.1: Design of experimental setup

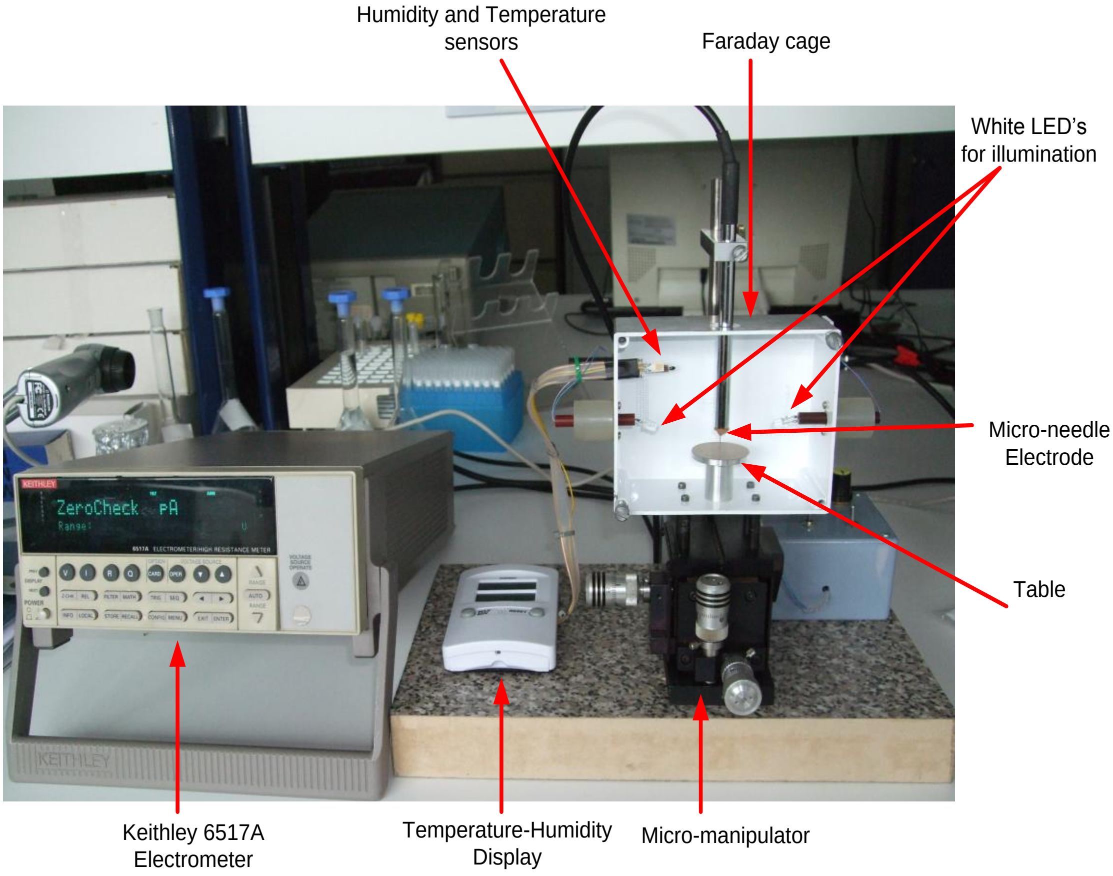

Humidity and Temperature sensors
Faraday cage
White LED's for illumination
ZeroCheck pA
Micro-needle Electrode
Table
Keithley 6517A Electrometer
Temperature-Humidity Display
Micro-manipulator

Figure 4.2: Photograph of experimental setup

This setup is developed for the measurement of charge in the EGIF . There are six main components of this experimental setup:

1) Micro needle electrode (MNE)
2) Table
3) Micromanipulator
4) Faraday Cage
5) USB Microscope Camera
6) Keithley 6517 A Electrometer

4.2.1 Micro Needle Electrode

For the measurements of charges from the surface of EGIF, a Micro-Needle Electrode (MNE) was developed from an acupuncture needle. The main shaft is of 220 µm diameter and it tapers down to a tip above 2.5mm of its length. The actual tip radius is around 8 – 10 µm.

MNE is insulated with a soft plastic tube with only 200 µm was exposed as the sensing surface to measure charges from the surface of EGIF droplet (See Figure 4.3).

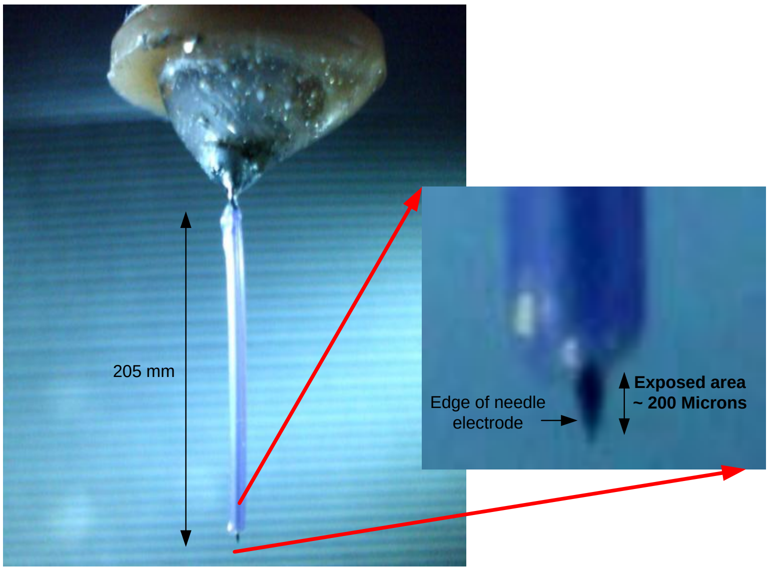


Figure 4.3 Micro Needle Electrode (MNE) used in experiment

The sensing MNE was connected to the electrometer via a triax cable as shown in Figure 4.2.

4.2.2 Table

A small rounded table was fitted inside the Faraday cage, and sweat droplets were placed over it for measurement (see Figure 4.5). The table is designed to represent the two physiological layers of fingertip skin. The table was made from free-machining aluminium material, and the top surface was covered with a layer of self-adhesive known as Polytetrafluoroethylene (PTFE), and an electrical insulator.

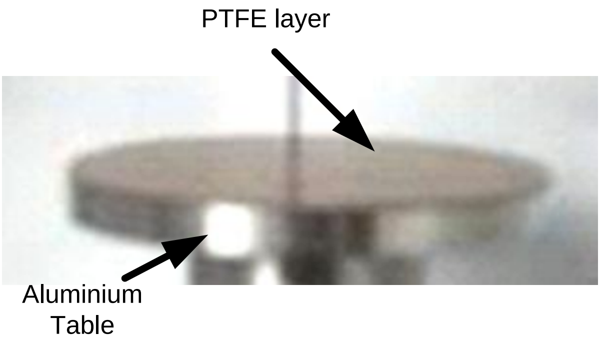


Figure 4.4 Table inside Faraday cage

The PTFE layer over the table represented the top surface layer of the fingertip, known as epidermis, which is usually considered to be a layer of dead skin (insulator). The thickness of the PTFE layer was 43µm. Underneath this layer was a stainless steel surface which represented the dermis layer of the fingertip, beneath the epidermis, and representing the live or conducting layer of skin. The actual thickness of this section (including the adhesive layer) is about 180 µm. This section of the experimental unit was fitted inside the faraday cage. Furthermore, the base of table was connected with a micromanipulator, to control the 3-axis movement of the whole Faraday cage unit.

4.2.3 Micromanipulator

It was used to control and set the different positions of sweat droplet for measurement.

4.2.4 Faraday Cage

The solid metallic body, surrounding the table was connected to the ground. This created the effect of a Faraday cage, to protect the measurements from any external Electromagnetic Interference (EMI). A white light LED was placed on each side, left and right, provide controlled illumination to observe the various positions of MNE and EGIF interface. Humidity and temperature sensors were also fixed on the left of the cage to record these measurements (see Figure 4.5). A removable glass plate was used to cover the front after placing the droplet over the table.

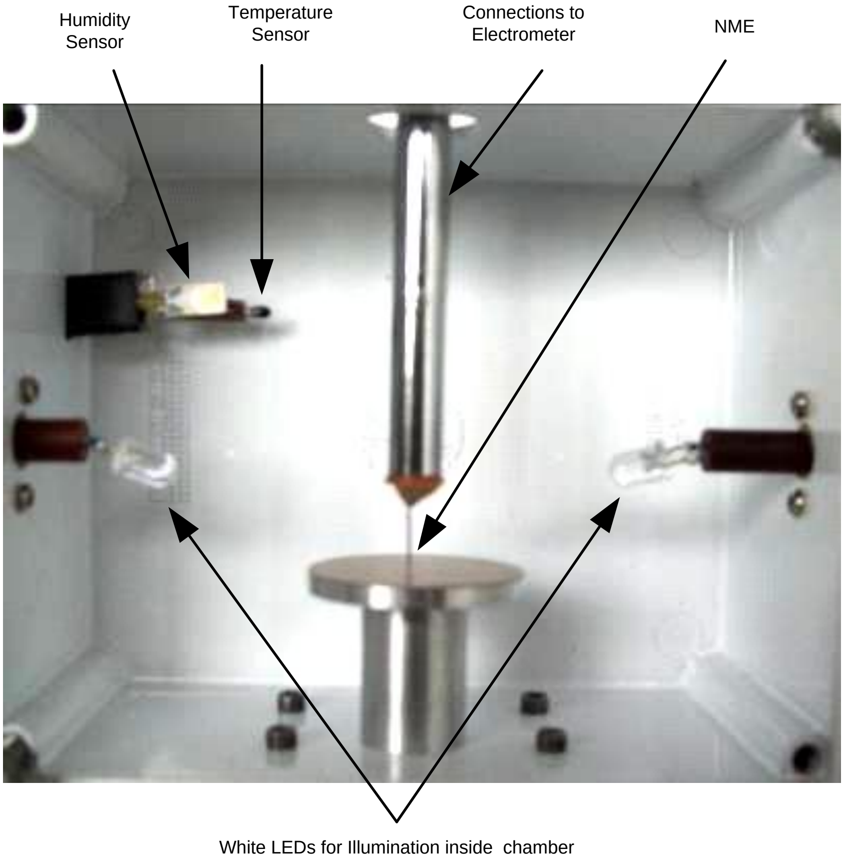

Humidity Sensor
Temperature Sensor
Connections to Electrometer
NME
White LEDs for Illumination inside chamber

Figure 4.5: Environment controlled chamber for charge/current measurement

4.2.5 USB microscope camera

To observe and capture the positions of the MNE over the EGIF droplet inside the Faraday cage, a High Resolution USB camera (model Pro Scope HR) with 50X lens was positioned at the front of the glass window. The camera was connected with a PC and Proscope software was used to capture images of the experiment.

4.2.6 Keithley 6517A Electrometer

A Keithley 6517A Electrometer was used for the measurement of low level charges. This electrometer was equipped with four different Coulomb ranges to resolve charge as low as 10 fC and measure as high as 2.1µC.

MNE was connected with electrometer with a co-axial cable. This cable used a BNC connector, but the Keithley 6517A electrometer could not be supported via connection. To overcome on this a Trix to BNC adopter connection (Model Keithley-7078-TRX-BNC) was used to connect the co-axial cable with the triax input.

4.3 EGIF droplets

Throughout the study and manual observation of B-FBDB images, the following points were observed:

- Sweat droplets which appeared over the surface of active pores are dynamic in nature;
- They appear over different pores at different times and evaporate in milliseconds;
- The droplet sizes tended to be small but varied, and depended on the sizes of the pores on the fingertip ridges of each individual.

It was difficult to find the appropriate amount and size of droplet to use for measurement for experimental purposes. A literature review of publications was conducted in this context, but no published research work was found which discusses, size and characteristics of eccrine gland sweat droplets.

Consequently, 10 different quantities from 1 to 10 µL of EGIF droplets were selected for charge measurement. These quantities were measured with pipettes. The 10 µL were used as a maximum quantity of EGIF sweat droplet, the 1 µL to 9µL were measured using micro syringe. Calculated size of droplets versus volume of EGIF is listed in Table 4.3

Volume **(**µL)	**Diameter of EGIF droplet** **(**µm)
1	~850
2	~900
3	~950
4	~1005
5	~1040
6	~1110
7	~1130
8	~1140
9	~1170
10	~1200

Table 4.3 Size of EGIF droplets used in experiments

4.4 Experiment settings

According to the manufacturer's instruction the Electrometer was turned on and allowed to warm up for an hour to achieve a rated accuracy. After an hour, the electrometer was connected to the MNE to begin the measurement process. The initial measurements were taken when there was no EGIF droplet present on the table, to ensure that no electrical interference was detected by electrometer.

It was assumed that in EGIF droplets, the signal generated by the ionic activity is low. For charge measurements the coulomb option was selected and set at 2-20 nC range.

To measure the approximate gap between the EGIF droplet surface and the MNE a paper printed with micro size was fixed behind the MNE and EGIF droplet interface. Each black and white printed line in the paper is equal to 200µm (See figure 4.6). This method does not provide an exact measurement of the gap between the MNE and EGIF; however, the appropriate spacing was deemed sufficient for these studies. Images were taken from all positions were analysed with ‘imageread’ function in Matlab R2010b. In that process, the numbers of pixels were counted in each printed line on the paper and the gaps were measured by counting the pixels between the MNE and EGIF surface.

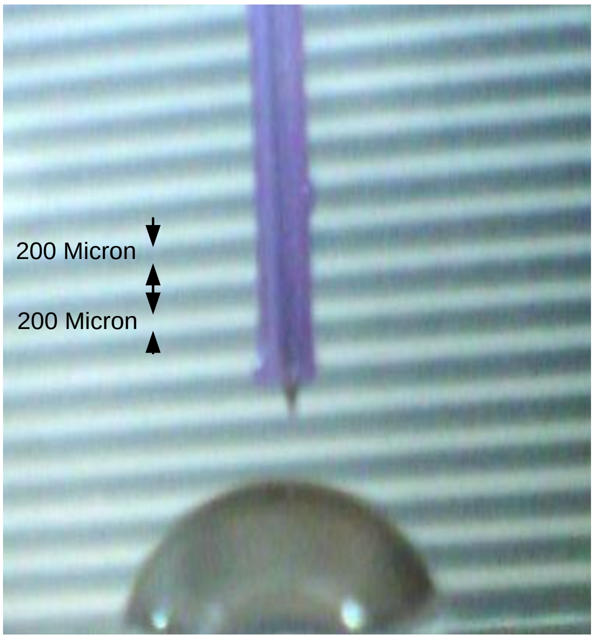


Figure 4.6 NME and EGIF interface

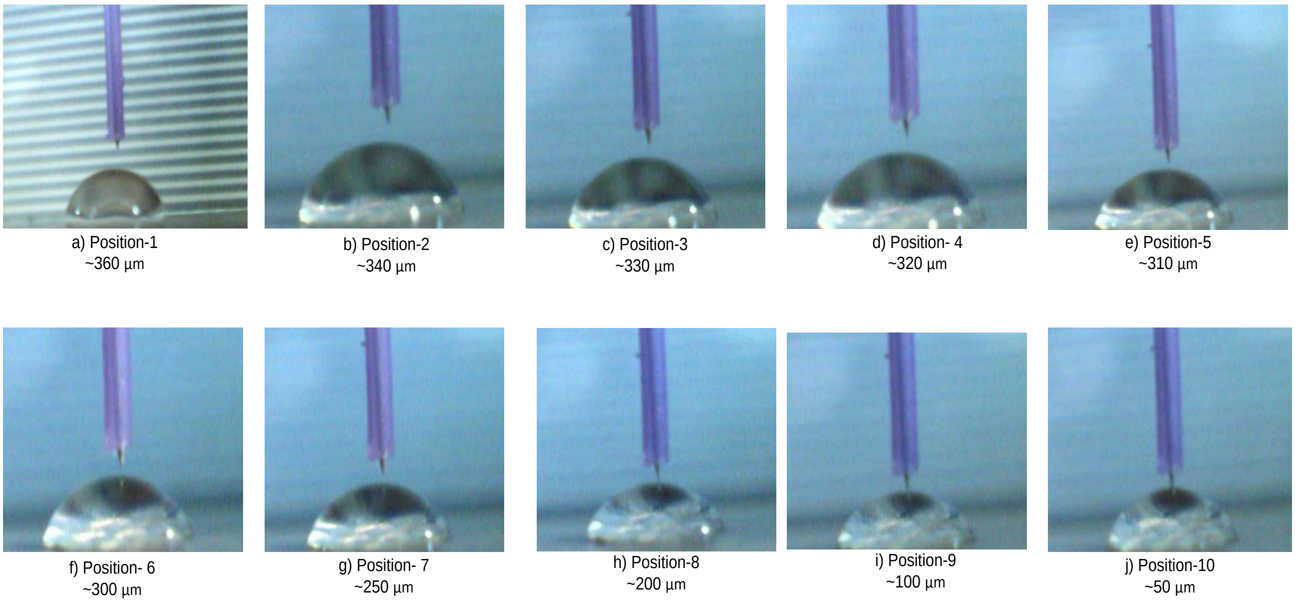


Figure 4.7 EGIF Droplets and NME interface with 10 different positions

To obtain the precise low level charge measurements, it is important to maintain a high signal to noise ratio (SNR). It is defined as the ratio of signal power to noise power.

$$\mathrm{SNR} = \frac{\mathrm{P}_{signal}}{\mathrm{P}_{noice}} \qquad (4.1)$$

Where P is the average power.

A high SNR indicates that the noise is less noticeable in the signal. There are several environmental factors that produce noise in the signal, such as temperature, humidity and electrical interferences. It is important to apply preliminary measures to protect the experiment environment in order to control any sources of noise before taking any measurements. The increase in the temperature to ranges above 25^0C, and the humidity to above 50%, can possibly produce a noise current which can interfere with the low level signal [138].

Moreover, any increase in humidity and temperature (above room temperature) can affect the size of EGIF droplet. An increase in temperature inside the cage can increase the evaporation process which would change the volume of the droplet. This process of evaporation will also cause of increase in the humidity (RH) level. The decrease in the volume of the EGI droplet will have a direct effect on the volume of surface charge.

Keeping these all factors in view, the temperature and humidity were constantly monitored inside the Faraday cage during measurement process. Temperature inside the Faraday cage varied between 22 and 24^0C, which is close to standard room temperature variations. The RH value recorded during the experiment varied between 38% to 53%.

The length of connection between the MNE and electrode can also be a cause of noise. Longer cables can produce capacitive noise, and signals can be affected by external electrical and mechanical interferences [138]. A 2 feet long shielded co-axial cable was used to connect the MNE to the electrometer. The aluminium shield in the co-axial cable, connected to the ground of electrometer, produces a Faraday cage effect, providing a shield from any external electrical interferences.

A complete set of temperature and humidity values measured with ten droplets are presented in table 4.4 with their mean and standard deviation.

Environment Factors	**Measured Values**										**Mean**	**Standard Deviation**
Temperature (^{0}C)	22	22	23	23	23	23	23	23	24	24	23	0.66667
Humidity (%)	38	39	43	44	46	48	50	51	52	53	46.4	5.31664

Table 4.4 Measured temperature and humidity

4.5 Charge measurement results

The charge measurements were taken from 10 different positions above the surface of the EGIF droplet, as illustrated in Figure 4.7. The distance of each position is listed in Table 4.5.

List of Positions	**Gap (µm)**
Postion-1	~360
Postion-2	~340
Postion-3	~330
Postion-4	~320
Postion-5	~310
Postion-6	~300
Postion-7	~250
Postion-8	~200
Postion-9	~100
Postion-10	~50

Table 4.5 Gap between NME and EGIF droplet

Charge measurements started with 10µL of EGIF droplet placed on the table and the position of MNE was fixed at a ~ 360 µm gap above the surface of the EGIF droplet. After measuring the charge at this point, the gap was reduced to 9 other positions of the MNE above the surface of the droplet (see Table 4.4). Same procedure repeated with 9, 8, 7, 6, 5, 4, 3, 2 and 1 µl EGIF droplets. The result of charge measurement in 10 EGIF droplets is illustrated in figure 4.8.

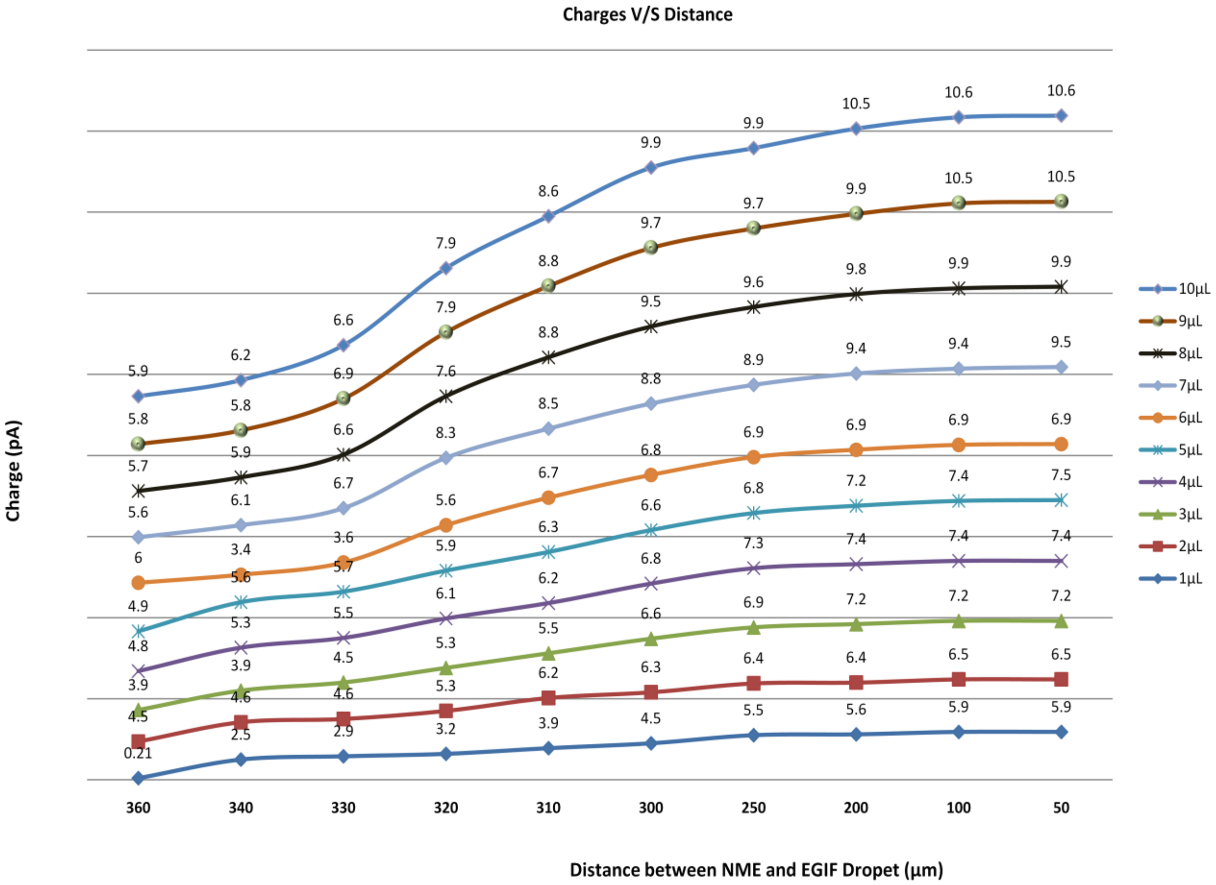


Figure 4.8 Charge measurements in ten EGIF droplets with 50-360 µm gap between EGIF droplet and MNE.

Results presented in figure 4.8 are further discussed in the following section:

The maximum 10.6 pC measured in 10 µl at 50 µm gap between EGIF surface and MNE. The major variation in charge observed between 300-360 µm and it was nearly remain constant between 50-200 µm. In 9 and 8 µl, the charge measurement started with 5.8 and 5.6 pC and up to the 300 µm it rapidly increased with changing the position closer to surface of EGIF surface. The 4-8% variation in surface charge is noticeable between 50-300µm in both droplets. There is no any major charge deviation measured between 50-200 µm distances; however, maximum charge level 10.5 pC and 9.9 pC were obtained at 50 µm position.

There was only 1% change in surface charge measured at 50 µm MNE position in 4 and 5 µl droplets, and 95% change is surface charge observed at 360 µm in both droplets. In 1µl at 360 µm position, 0.21 pC charge measured by electrometer and at 250 µm position a rapid increase in charge from 0.21-5.6 pC was observed. From 200-320 µm position the surface charge was steady with value of 5.9 pC. However, 5% increase in surface charge has been observed up to 50-200 µm.

Overall in measurements the maximum charge was observed at the 50 µm gap, because it was the closest gap used between the MNE and the EGIF. Also, in 10 µl, at all 10 different positions, the maximum charge levels were obtained. This is because of the quantity of EGIF, in which accumulated charge is higher than other quantities. The increase in the amount of EGIF showed an increase in the charge.

The reason for this is that surface charge is directly proportional to the surface area. Therefore a linear proportion was observed between the level of charge and the size of EGIF droplet. Furthermore, in each EGIF droplet, as the gap between surface and MNE diminished, the electric field induced in the MNE increased, resulting in an increase in the level of charge.

The exponential variation in the graph line in all measurement results shows the proportion between charges versus distance of MNE from the surface of the droplet. The major increase in charge was observed between 340-360µm, and there is a minor variation of charge value measured between 50-300 µm, and the maximum charge value measured at these positions in all EGIF droplets.

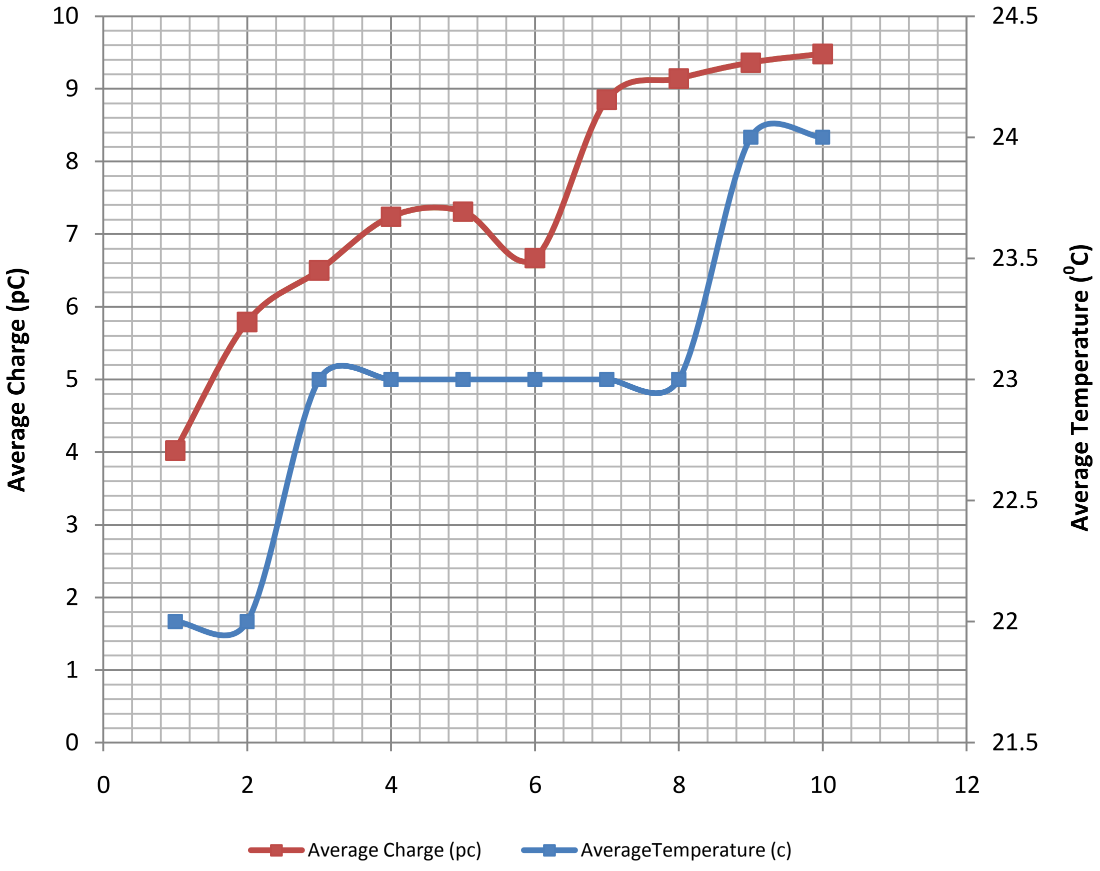


Figure 4.9 Variations of charge level with temperature

The temperature inside the faraday cage was measured throughout the charge measurement. The EGIF droplet could evaporate more rapidly if the temperature inside the measurement cage increases above room temperature. These temperature values were measured when an EGIF droplet was placed on the table inside the Faraday cage for measurement.

The average charge and average temperature values were used to plot this graph (See figure 4.9). There is no major variation in temperature and the plotted line is nearly stable and not exponential. This temperature variation did not have any major effect on the charge value.

In the next section, a Finite Element Model (FEM) of EGIF droplet and NME interface is explained. The FE model was developed in COMSOL Multiphysics software and details of modelling results are presented with illustrations.

4.6 EGIF and NME finite element model

After completion of experimental section, a Finite Element (FE) model has been developed using COMSOL Multiphysics 3.5 to observe the electric field variation around NME at different distances with EGIF. Stages in the development of FE model are discussed in the followings section.

4.6.1 COMSOL Multiphysics

The COMSOL Multiphysics is finite element analysis, solver and simulation software for many physics and engineering applications. It provides sophisticated and convenient tools for geometric modelling.

The COMSOL Multiphysics was selected for this research because:

- It has user friendly graphical interface for defining and creating geometries, sub domain settings, meshing and solver.
- Several application specific modules are available in this package such as, AC/DC and Micro Electro-mechanical Systems (MEMS) Module
- There are predefined application modes which act like templates in order to hide much of the complex details of modelling by equation

In COMSOL Multiphysics, design of the model began with the selection of appropriate model related to problem. General steps to develop a model in COMSOL Multiphysics are illustrated in Figure 4.10.

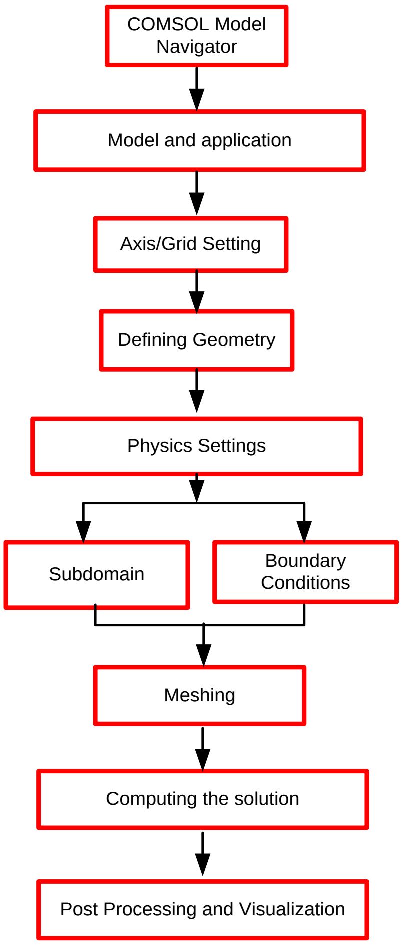


Figure 4.10 General steps of COMSOL modelling

4.6.2 COMSOL MEMS module

The MEMS module in COMSOL is a collection of application modes and models for the modelling of MEMS devices and applications. This module includes electrostatics, structural mechanics, piezoelectricity, film damping, and micro fluidics modes. These modes help in the modelling of actuators, sensors and microfluidic devices.

There is no predefined model available in the COMSOL library which supports modification for use in this research. The MEMS module was selected to develop the model because it was developed to support the design of micro dimension geometries with appropriate sub-domain and boundary conditions. Also, it has an electrostatics mode which is required in this design model.

4.6.1 FEM Modelling of experimental work

A 2D FE Model of the MNE and the EGIF Interface was developed by using the MEMS module with the electrostatics mode. This model was used to understand and visualize the effect of induced electric field and electric potential changes in the MNE at different distances above the EGIF. The process of modelling is illustrated in Figure 4.11.

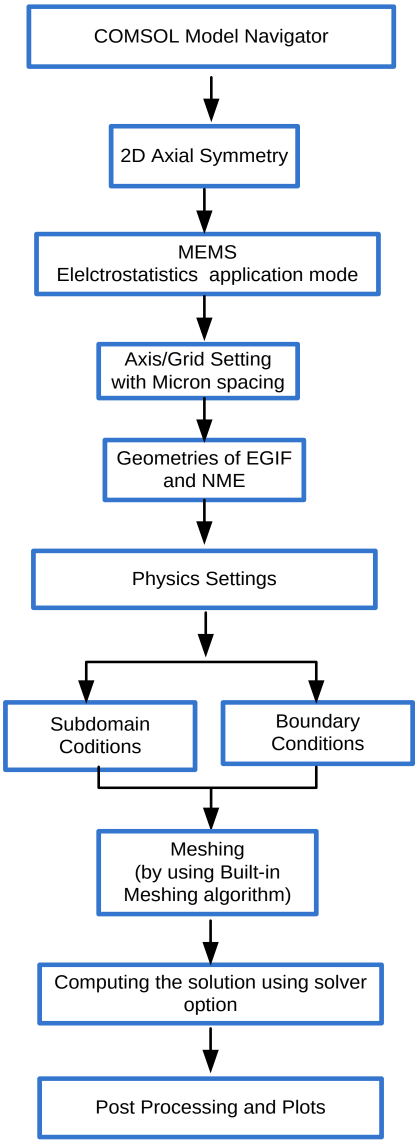


Figure 4.11 FE Modelling of NME and EGIF interface

4.6.1 Modelling of base for EGIF

In experiment, the EGIF droplet was laid on the PTFE surface of table (see Figure 4.12 a). A double layered rectangular shape created to represent the base and PTFE layer. The thickness of base shape is about 200 µm and the surface is about 50 µm. This geometry was created before the EGIF droplet. The detail of sub-domain and boundary condition for this layer is presented in Table 4.6 and 4.7.

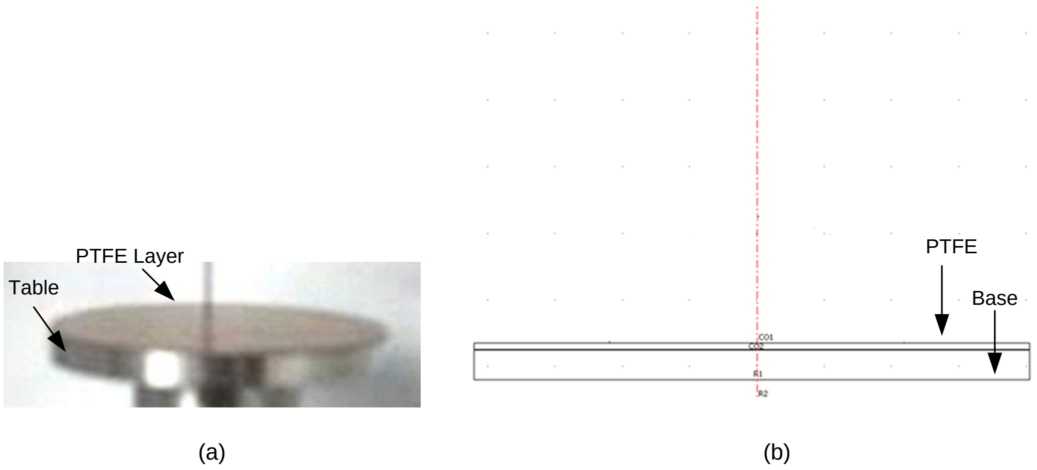


Figure 4.12 a) Shape of table in experimental setup b) Geometry of table in COMSOL

4.6.2 Modelling of FGIF

In COMSOL environment a predefined basic geometrical object tools such as, line, circle, square and ellipse are available to draw different shapes as required. The grid were set with 5 micron distance on X and Y axis. The EGIF droplet shape it looks like a semicircle (see Figure 4.13 a.), so keeping this view in mind, a semi-circle was created to represent the droplet geometry (see figure 4.13b.). The EGIF is not completely semicircle, but this is the only appropriate shape for making resemblance between experiment and simulation.

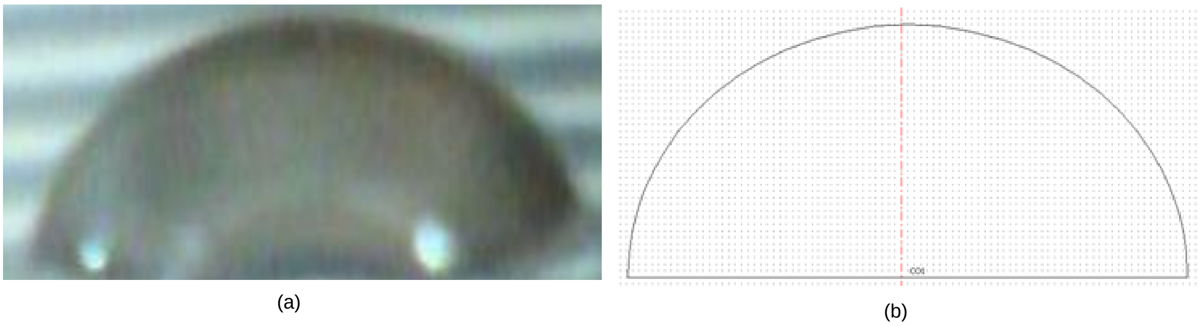


Figure 4.13 (a) Actual EGIF droplet b) COMSOL geometry of EGIF droplet

4.6.3 Modelling of MNE

Here, the geometry of sensing area of MNE is created only by using a line tool. Figure 4.14 shows the geometry and its similarity with actual MNE. The actual MNE was made up of stainless steel, so the same material properties were chosen from the material library and applied into the sub-domain property.

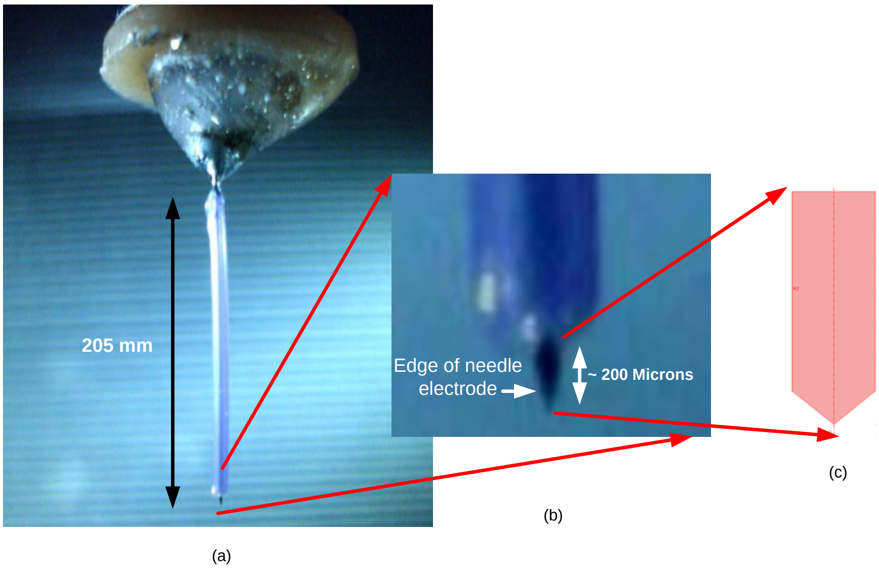


Figure 4. 14(a) Real MNE (b) Tip of MNE (c) COMSOL MNE model geometry

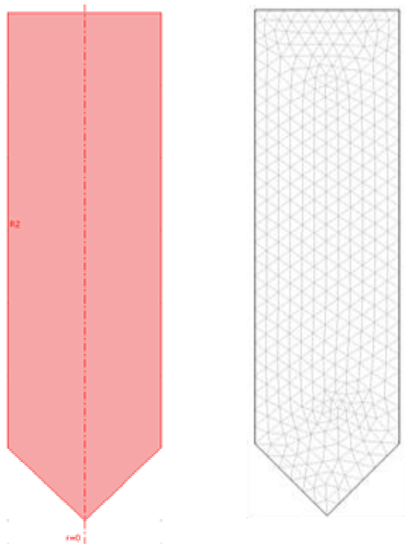
In the next step, a mesh was initialized for the MNE geometry. The meshing of the MNE model was performed by using the straightforward method given by the built-in meshing algorithms in COMSOL Multiphysics.

The following equation can be used to verify the FE model mesh element minimum quality (q):

$$\mathrm{q} = \frac{4\ \sqrt{3}\,\mathrm{A}}{h_1^2 + h_2^2 + h_3^2} \qquad (4.2)$$

Where A is the triangle area and h1, h2 and h3 are the side lengths of triangular element. If q> 0.3, the mesh quality should not effect on the solution quality [139, 140]. It was found from the (COMSOL Multiphysics manual 2008) [141] that in the fine mesh option, the value of q=0.46, and hence, this was considered to be an acceptable quality for the NME mesh elements.

For this reason a fine mesh option was selected in mesh settings and applied with triangular elements. This mesh quality provides precise results but it takes more time to process in solution compared with the coarse mesh. The final geometry of the MNE, with a fine mesh of 732 element, is illustrated in Figure 4.15(a) and (b).



(a) (b)

Figure 4.15 a) MNE geometry b) Meshed MNE model

4.6.4 NME with EGIF droplet interface

After designing the geometry for the Faraday cage electrically shielded condition was applied to all the boundaries. A complete interface model of MNE and EGIF within Faraday cage is illustrated in Figure 4.16.

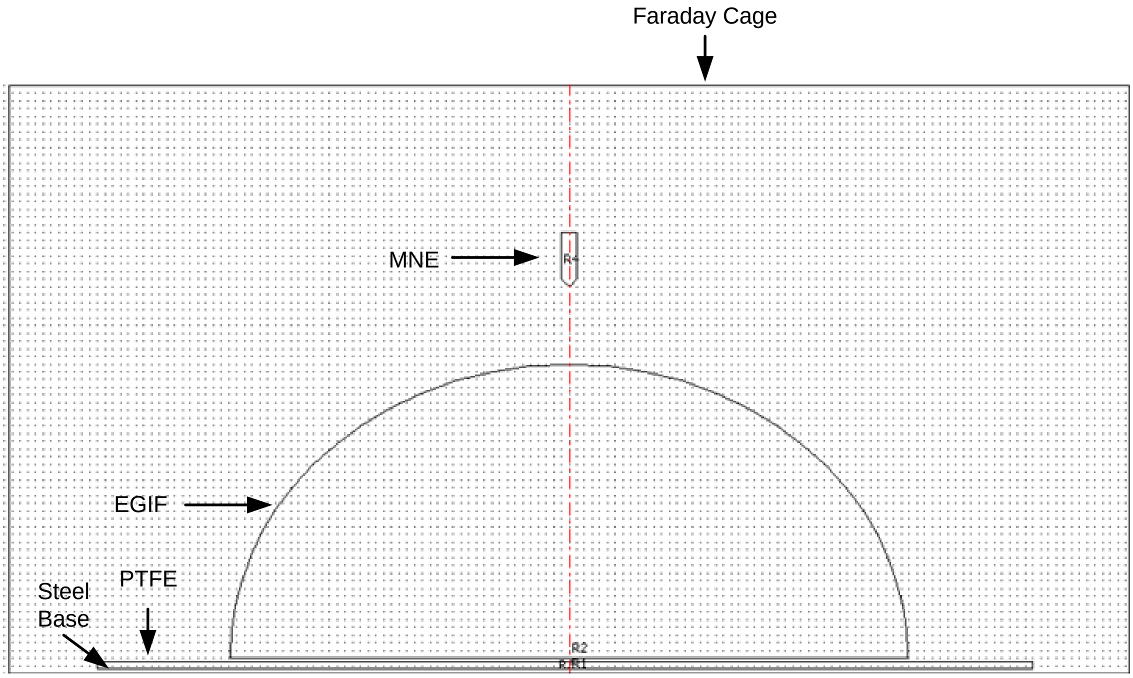


Figure 4.16 Complete MNE and EGIF Interface Model

This mode uses the differential form of Gauss's Law (equation 4.2) for sub-domains.

$$-\nabla.\,\varepsilon_0\varepsilon_r\nabla\mathrm{V} = \rho \qquad (4.3)$$

Where $\varepsilon_0$the permittivity of vacuum, ε_r is the relative permittivity is the potential and ρ is the total charge density.

The final model is based on four components EGIF, MNE, insulation layer, faraday cage and 16 boundaries. Each component is finalized by applying suitable boundary conditions and sub domain parameters. The details of each sub-domain and boundaries are illustrated in Table 4.6 & 4.7.

Component of Model	EGIF	MNE	Insulation Layer	Faraday cage
Surface charge Density (ρ) (c/m^3)	(See table 4.8.)	0	0	0
Relative Permittivity (ε_r)	80	1	2	1
Material Properties	Water	Steel	PTFE	....

Table 4.6 Sub-main Setting of Model

The relevant interface condition at interfaces between different media for this mode is

$$\boldsymbol{n_2}.(\mathrm{D}_{\mathbf{1}} - \mathrm{D}_{\mathbf{2}}) = \rho_s \qquad (4.4)$$

In the absence of electric charge, this condition is fulfilled by the natural boundary condition

$$n.[(\varepsilon_0 \nabla V - \mathbf{P})_1 - (\varepsilon_0.\nabla V - \mathbf{P})_2] = -\mathbf{n}.(\mathbf{D}_1 - \mathbf{D}_2) = 0 \quad (4.5)$$

Object	EGIF	MNE	Insulation Layer	Faraday cage
Boundary Number	7,16,17,18	8,9,10,11,12	4,5,6,13,14	1,2,3 and 15
Settings	Continuity	Continuity and boundaries 8-9= 1X10^{-6}volt	Continuity	Electrical shielding

Table 4.7 Boundary Conditions of Model

The continuity boundary

$$n_2.(\mathbf{D}_1 - \mathbf{D}_2) = 0 \quad (4.6)$$

It specifies that the normal component of the electric displacement is continuous across the boundary. The electric shielding boundary condition describes a thin layer of a dielectric medium that shields the electric field.

EGIF (µL)	**Diameter of EGIF droplet** (µm)	**Surface charge density (ρ) (c/m^3)**	**Relative Permittivity (ε_r)**
1	~425	4.89 $\times 10^{-6}$	80
2	~450	6.16 $\times 10^{-6}$	80
3	~475	6.78 $\times 10^{-6}$	80
4	~503	6.41 $\times 10^{-6}$	80
5	~520	7.31 $\times 10^{-6}$	80
6	~555	7.02 $\times 10^{-6}$	80
7	~565	7.33 $\times 10^{-6}$	80
8	~570	7.70 $\times 10^{-6}$	80
9	~585	7.75 $\times 10^{-6}$	80
10	~600	7.76 $\times 10^{-6}$	80

Table 4.8 Sub-domain settings of EGIF Droplet

Table 4.8 presents the 10 sub-domain conditions applied as surface charge density (ρ) in EGIF geometry. These values obtained by measuring charge in each EGIIF droplet and further surface charged density calculated for sub-domain condition. Surface charge density is proportional to the diameter of droplet, so the calculated value of surface charge density is higher in 10 µL droplets and decreased gradually with the radius of droplet (See Table 4.8). In next step, complete model meshed with the fine settings and resultant mesh consists of 17836 triangle elements (see Figure 4.17).

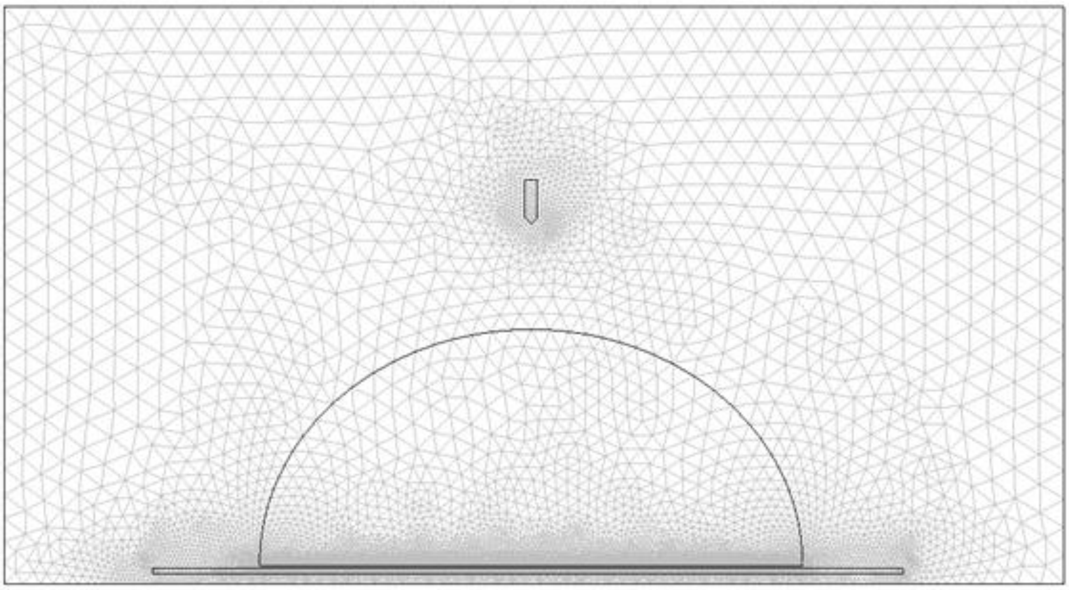
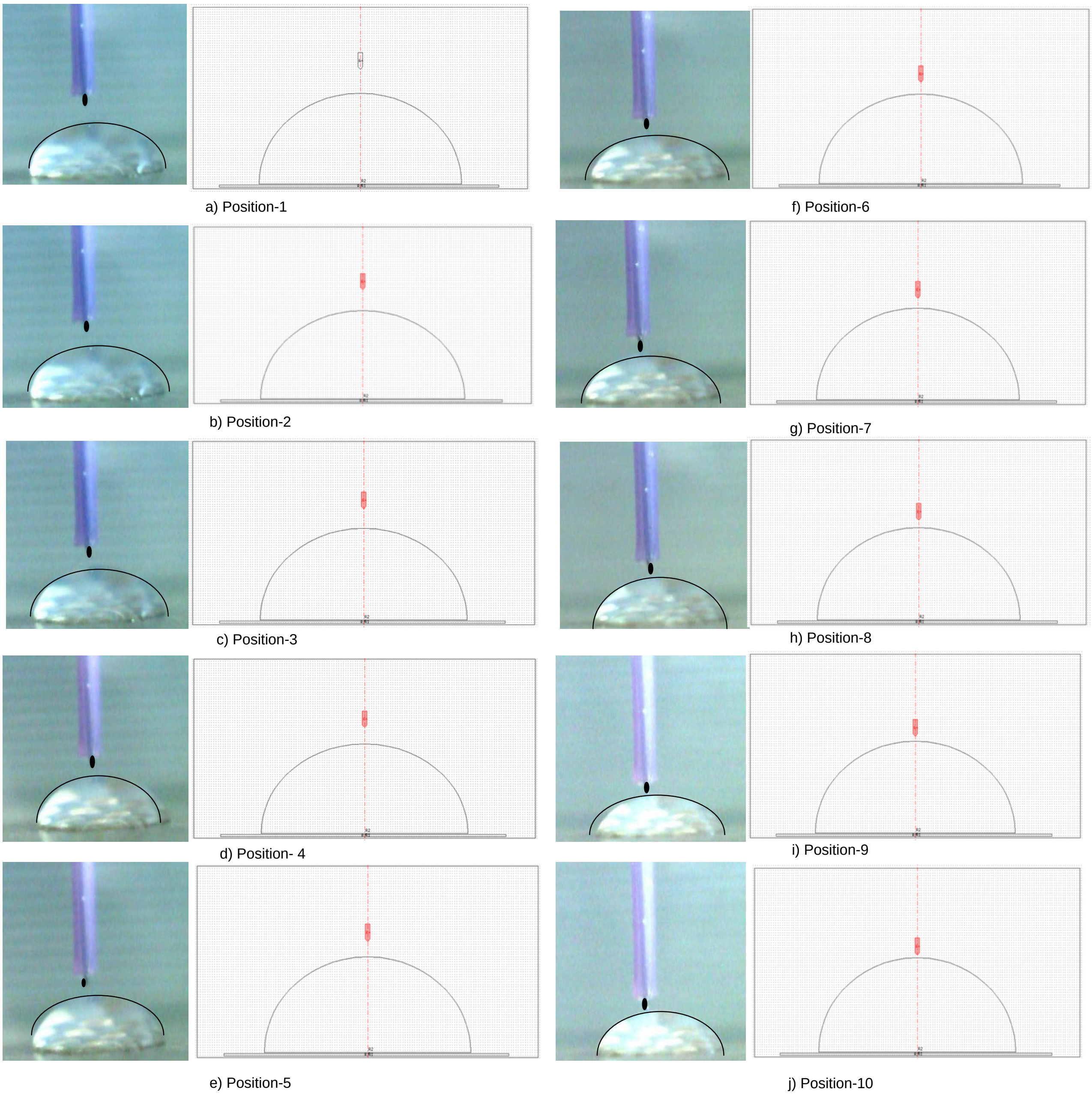


Figure 4.17 Final meshed NME –EGIF Interface

Position	Gap (µm)
1	360
2	340
3	320
4	310
5	300
6	250
7	200
8	100
9	50
10	25
11	15
12	5

Table 4.9 Gap between MNE and EGIF used in modelling

The results were obtained by applying 10 sub-domain conditions illustrated in table 4.9 In the model, the gap between MNE and EGIF is listed in Table 4.9 which is more precise and accurate than gap used in experiment. Also thee additional results were obtained with 25, 15 and 5 µm positions. Figure 4.18 illustrates positions used in experiment and modelling.



a) Position-1

f) Position-6

b) Position-2

g) Position-7

c) Position-3

h) Position-8

d) Position- 4

i) Position-9

e) Position-5

j) Position-10

Figure 4.18 Experimental and modelling positions of NME over EGIF surface

COMSOL Multiphysics normally select the appropriate solver for the FE model. For this model, the choice of the solver left to a default linear system solver called Direct (UMFPACK). This default solver usually used for solving 2D models. It not supports symmetrical matrix and always solve full system regardless of symmetry. It is faster but uses more memory compare to other solvers.

4.7 COMSOL simulation results

The results of simulation were obtained with 10 different gaps between NME and EGIF. The first simulation started with 380 µm which was the maximum gap and moved down to 5µm which is the minimum gap between NME and the surface of EGIF. In experiment, the EGIF surface position was moved towards the MNE but in simulation only MNE geometry moved from its maximum to minimum position towards EGIF. It imitates the same action used to obtain the required gaps for measurements in the experiment.

With each position, after meshing and solving the complete model, streamline plots for the electric field and surface plots for electric potential were obtained at 10 positions. The results were plots with surface charge density values (ρ) 4.89×10^{-6} c/m^3 to 7.76×10^{-6} c/m^3 in EGIF sub-domain settings. For each EGIF sub-domain setting, twelve sub-domain plots were obtained by using post processing option in COMSOL.

Only the resultant plots were obtained with higher value of charge density (ρ =7.76 $\times10^{-6}$ c/m^3) and demonstrated in Figures 4.19-30.

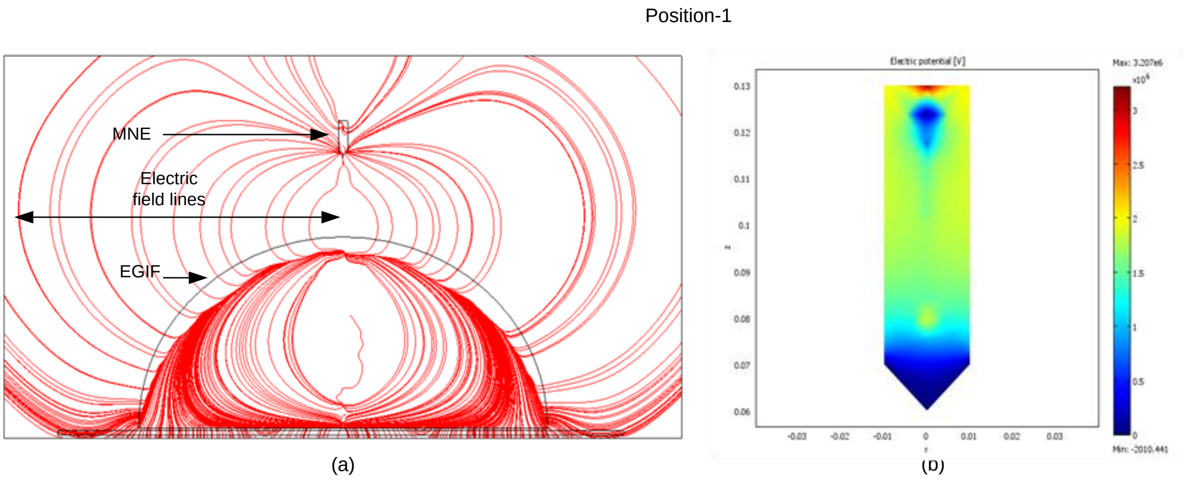


Figure 4.19 MNE at 360µm distance from Surface of EGIF (a) Stream plot of electric field (b) Surface plot of electric potential

In Figure 4.19 a, at 360 µm the electric field lines (in red colour) diverting from the surface of droplet towards MNE. At this position, the minimum electric potential is displaying at the edge of tip (Blue colour) and slightly higher electric potential at the rest region of MNE because of the more electric field induced at these points. In Figure 4.20 (a) the electric field lines are more intense at the tip of MNE and the edge of tip changed colour from blue to dark red confirms the maximum potential at this point (see Figure 4.20 b). At this position, distance between MNE tip and surface of EGIF is lower than the previous position so induced eclectic field is now high and it is demonstrated with high potential.

Position-2

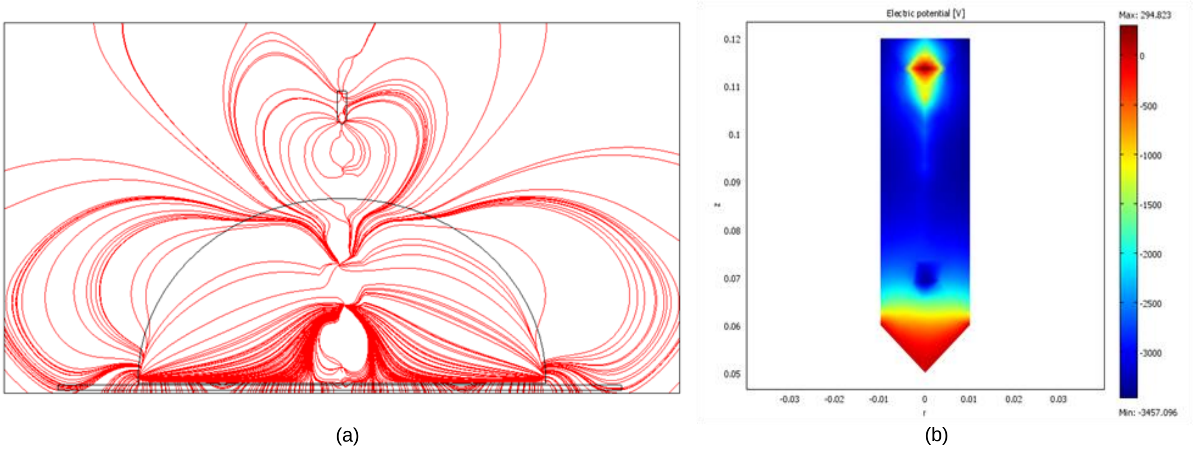


Figure 4.20 MNE at 340µm distance from Surface of EGIF (a) Stream Plot of Electric field (b) Surface Plot of Electric potential

Position-3

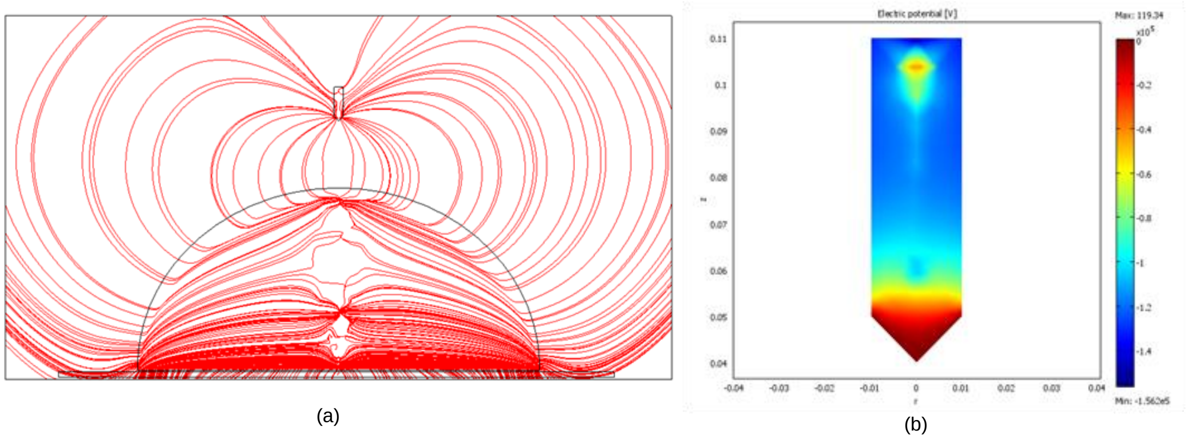
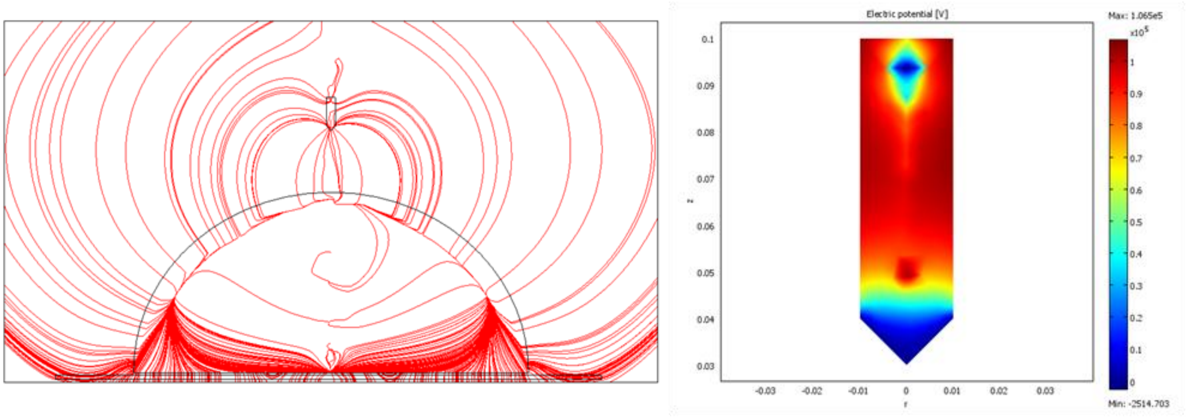


Figure 4.21 MNE at 330µm distance from Surface of EGIF (a) Stream Plot of Electric field (b) Surface Plot of Electric potential

At next two positions (330 and 320 µm), the electric field inducing more on the left and right sides of MNE tip (see Figures 4.21 & 4.22 a.) .At this distance the electric potential is dark red because of the intensity of the increase in the field lines that point. The variations of electric potential on the sides of NME tip are shown in surface plots in Figures 4.20 &4.21 b, where the deviation in red colour demonstrates the points of changes in electric potential.

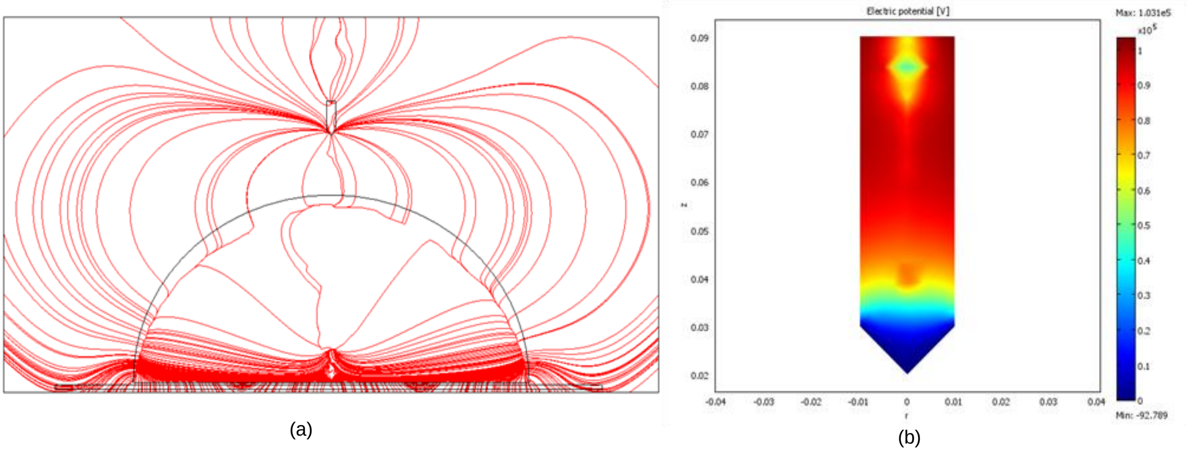
Position-4



(a) (b)

Figure 4.22 MNE at 320µm distance from Surface of EGIF with (a) Stream Plot of Electric field (b) Surface Plot of Electric potential

Position-5



(a) (b)

Figure 4.23 MNE at 300µm distance from Surface of EGIF (a) Stream Plot of Electric field (b) Surface Plot of Electric potential

At position 5, MNE set at 300µm distance from the surface of EGIF, the electric filed lines are around the whole MNE which is visible in Figure 4.23 a. Also, the intensity of electric potential is noticeable at the centre of MNE in figure 4.23 b. the results at 250 µm are illustrates in Figure 4.24 a and b. At 200 µm on the both sides of NME is high eclectic potential (dark red) because of intense electric field at these points (see Figure 4.25 b).

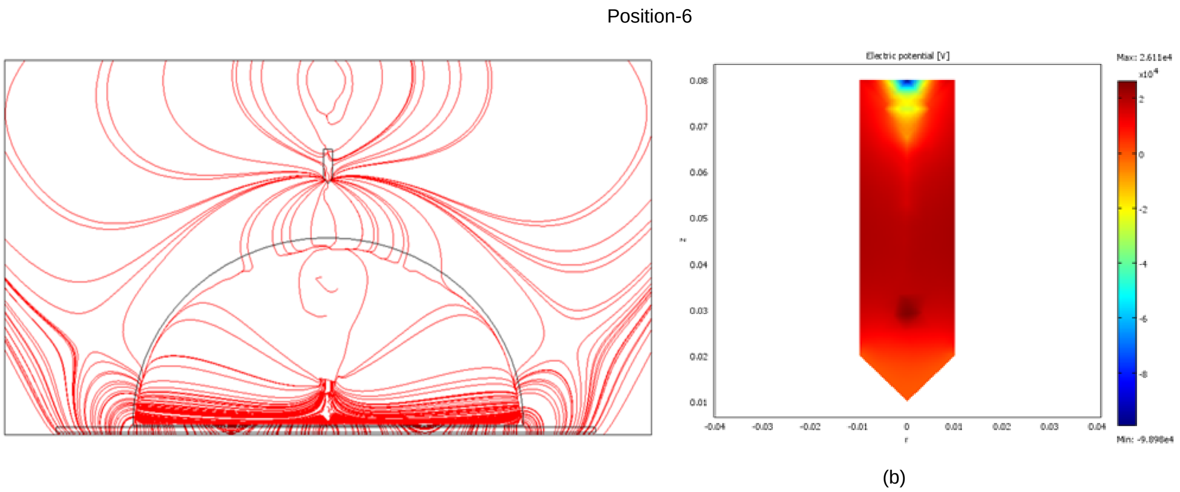


Figure 4.24 MNE at 250µm distance from Surface of EGIF (a) Stream Plot of Electric field (b) Surface Plot of Electric potential

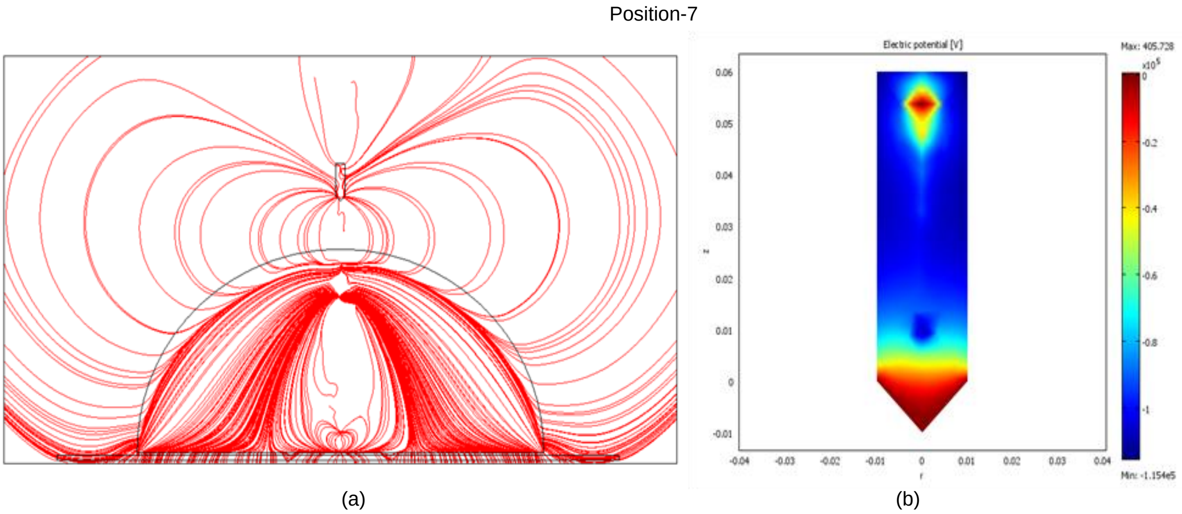
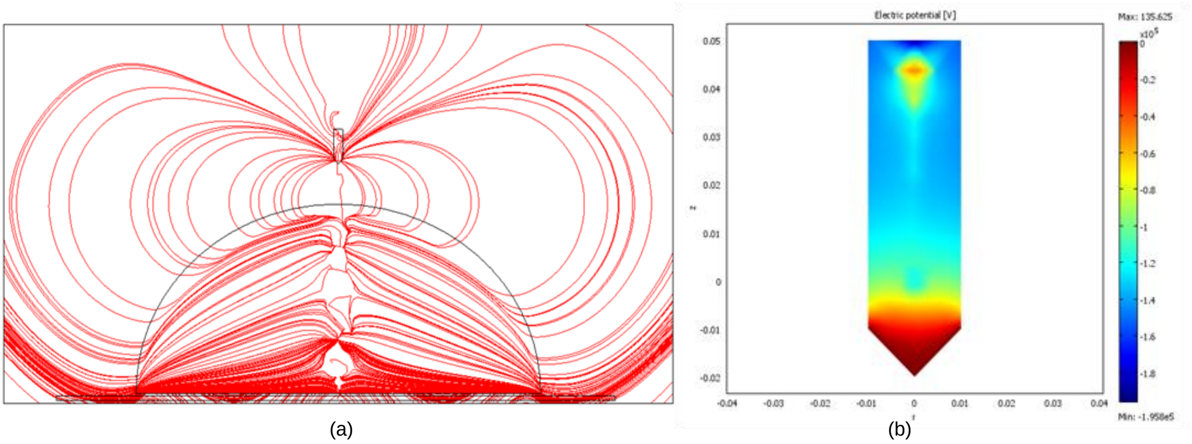


Figure 4.25 MNE at 200µm distance from Surface of EGIF (a) Stream Plot of Electric field (b) Surface Plot of Electric potential

Position-8



(a) (b)

Figure 4.26 MNE at 100μm distance from Surface of EGIF (a) Stream Plot of Electric field (b) Surface Plot of Electric potential

Position-9

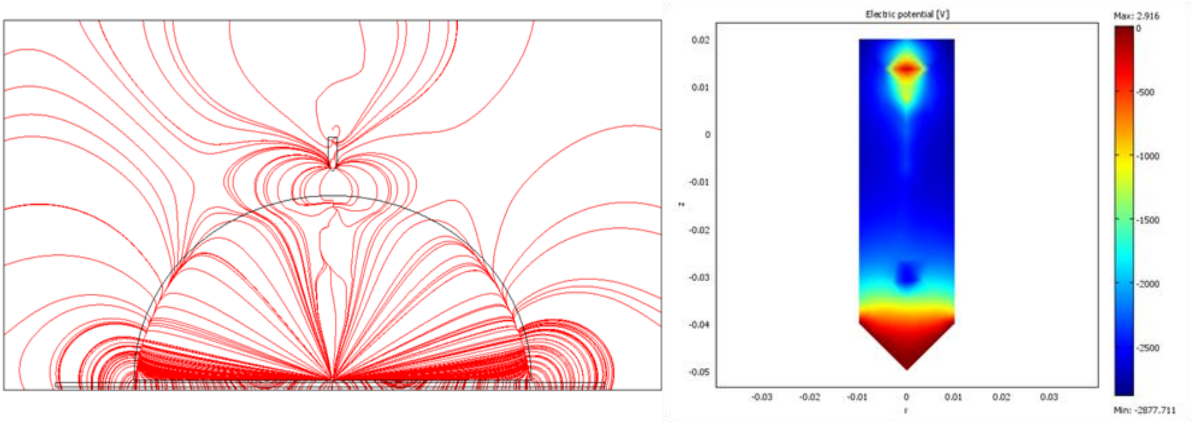
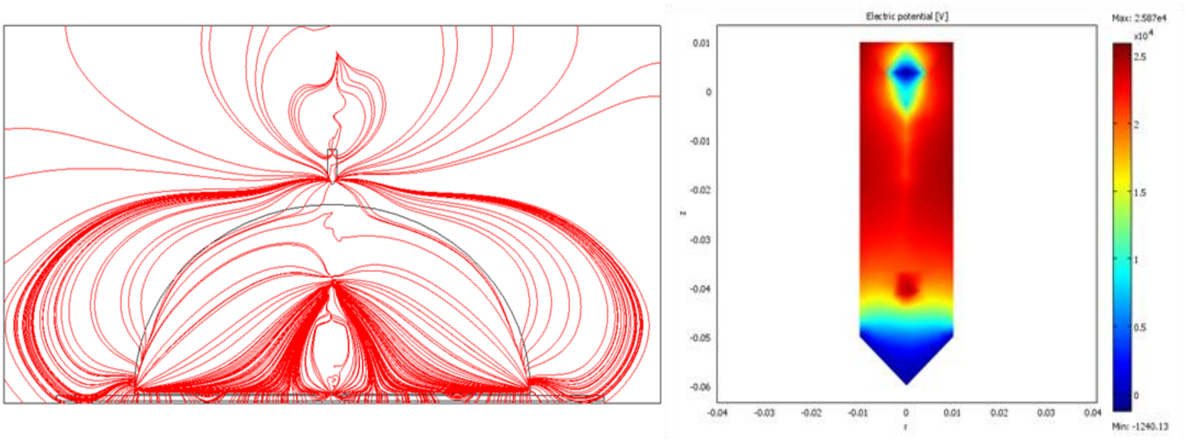


Figure 4.27 MNE at 50μm distance from Surface of EGIF (a) Stream Plot of Electric field (b) Surface Plot of Electric potential

In Figures 4.26 and 4.27(a) shows the results obtained with 100 and 50 µm. These positions are closer to the previous positions and because of this the electric field intensity is high at the centres of both sides of NME. The result of field intensity is observable in electric potential variation (dark red) in NME (see Figures 4.26 and 4.27b).

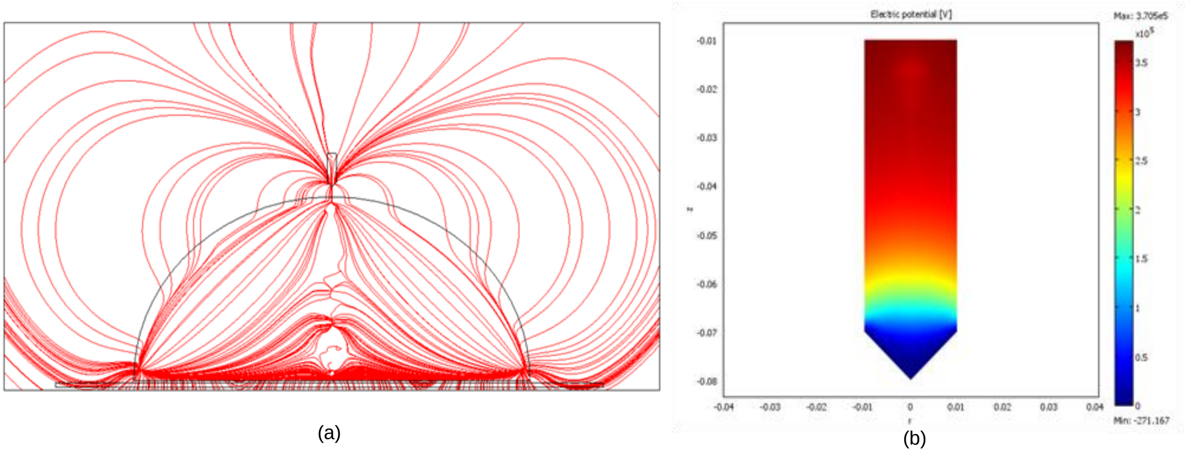
Position-10



(a) (b)

Figure 4.28 MNE at 25µm distance from Surface of EGIF (a) Stream Plot of Electric field (b) Surface Plot of Electric potential

Position-11



(a) (b)

Figure 4. 29 MNE at 15µm distance from Surface of EGIF (a) Stream Plot of Electric field (b) Surface Plot of Electric potential

At 25 & 15 µm position the maximum electric potential was seen above the area of MNE tip (see Figures 4.28 & 4.29 b.) as more intense electric field is visible in stream plot (see Figures 4.28 & 4.29 a).

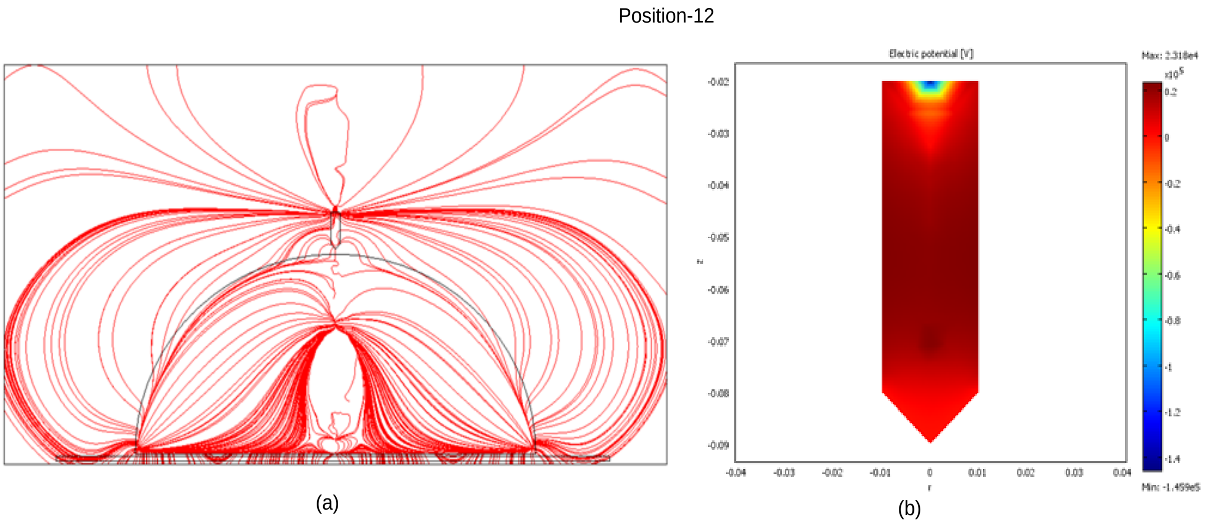


Figure 4.30 MNE at 5µm distance from Surface of EGIF (a) Stream Plot of Electric field (b) Surface Plot of Electric potential

In figure 4.30, the last result obtained with very close gap of 5 µm between MNE and EGIF droplet. At this point the NME is nearest the surface of EGIF where surface charges are stronger than the other positions. The maximum electric field lines are now around the MNE (see figure 4.30 a.).The surface plot in figure 4.30 b. obtained at this position where maximum potential (red colour) is observable in and surroundings of the MNE.

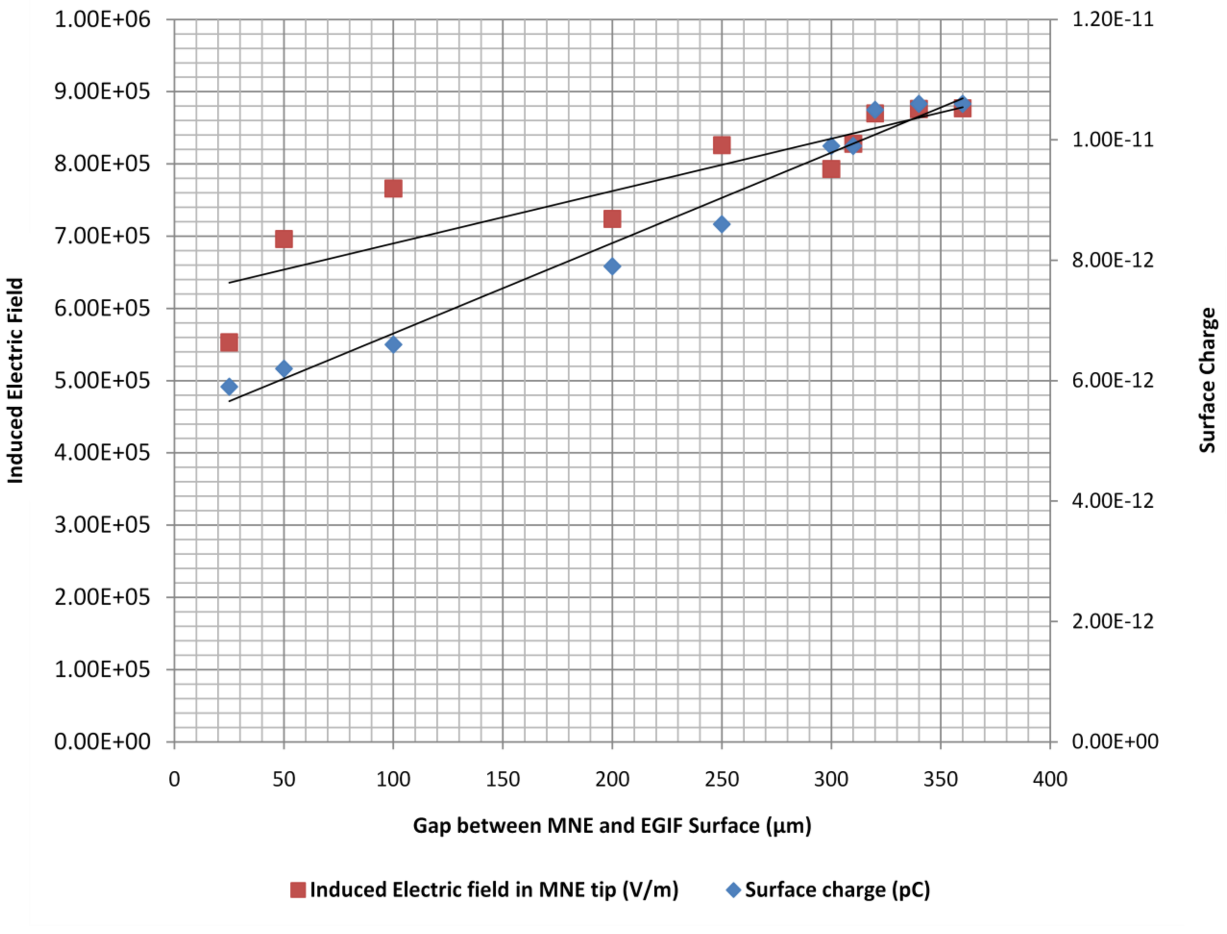


Figure 4.31 Induced electric field on MNE tip and surface charge

Relation between surface charge measured in experiment and induced electric field on MNE in simulation is illustrated in Figure 4.31, and trend lines shows a liner proportion between both parameters. As the MNE was reaching closer to the surface of EGIF droplet more field was induced in the tip of MNE. In Figure 4.30 (a) it is observable at 5µm position that 98% electric field was induced in the MNE and this is clearly visible in Figure 430 (b) as an increase in electric potential.

4.8 Summary

In this chapter the experimental setup, procedure and results of surface charge measurement in EGIF droplets was discussed. In this experiment, surface charge of 5.9 to 10.6 pC was measured in the EGIF droplets (1-10 µl), at ten positions (~50-~360 µm) of the NME. High levels of charge were measured at the 50µm position with all droplets, and the maximum charge was measured in the 10µl droplet. The size of the droplet shows linear proportion to the volume of surface charge. The measurement obtained with sample sweat fluid successfully proved the idea of non-contact ionic activity measurement in active pore sweat fluid as a proof of liveness. Actual sweat fluid droplets are different in shape and size, and because of that they formed different contact angles. In the future, it is necessary to study the effect of change in contact angle on the ionic activity.

The FE Model developed for this study showed a relationship between the induced electric field and measured surface charge. Surface plots obtained in the simulation explained the relationship between elelctric potential and the distance of the MNE. A small gap between the EGIF and the MNE produced a major increase in the electric potential. It would be possible to conduct further study on the shape, size and positions of the NME with this model in order to define the best positions for the electrodes.

The experimental setup can be modified in future by using micro/nano electrodes to develop an improved, highly sensitive, non-contact array to detect ionic activities from actual sweat droplets on fingertips.

Chapter 5: Conclusion and Future work

5.1 Conclusion

Liveness detection is a major issue in fingerprint identification biometrics. Many practical incidents have occurred and have been reported widely in the media. A large amount of published literature about the spoofing of commercial fingerprint sensors and systems with fake finger stamps is available. Various researchers proposed hardware and software based solutions for liveness detection for fingerprint systems. However, these have not yet been implemented in commercial AFIS because of many limitations that are still associated with the proposed techniques. These limitations were discussed with critical literature review of fingerprint sensing technologies, and proposed solutions in software and hardware for liveness detection, in Chapter 2. Fingerprint biometrics need a robust liveness detection solution which is not possible to replicate, and can be detected by a system efficiently before anyone is able to access the system illegitimately. The proposed solution should not be based on the detection or measurement of fingertip properties, which are easily replicable with little effort and skill. In addition, the liveness detection technique must be proficient to detect liveness from intrinsic properties of live fingertip skin, and should be a simple, fast and cost effective solution for liveness detection.

In this research, two novel active pore based liveness detection techniques for fingerprint biometrics have been developed, tested and proposed for fingerprint biometrics. The first technique, HCFA is an image processing technique based on high-pass filtering of frequency spectrum of the fingertip image, correlation filtering with a small uniform circular pattern followed by hard-thresholding. It detects and demonstrates the idea of detection and spot active pores on images of live fingertips. Novel HCFA algorithm was tested on more than 100 fingertip images from the B-FBIG Database. The task of detecting active sweat pores was very challenging due to a number of varying attributes of active sweat pores. A manual examination of active sweat pores were performed on the same images before processing them with HCFA. The results were analysed using the newly developed detection ability (DA) and detection efficiency (DE) parameters.

HCFA produced reasonably good results in most of cases in terms of DE and DA which shows great potential for future use in liveness detection. The results presented in Chapter 3 demonstrated that HCFA was 100% successful in establishing liveness of the fingertip.

A few limitations still exist in HCFA technique:

- The best results were obtained with only B-FBDB images. It should be capable to detecting active pores from other database images as well to increase its functionality with other commercially available database;
- The reference pattern and thresholding levels need additional research to obtain the shape and threshold level for achieving maximum detection efficiency (DE) and discrimination ability (DA).

5.2 Future Work

Future research work is needed to improve the HCFA with an innovative image enhancement technique for elimination of unwanted high-frequency structures, as well as enhancement of the specific active pore. Also, an investigation into the cut-off frequency of the high-pass filter for better edge detection of active pores; a self-tuning algorithm for choosing the optimum threshold value for binarizing the correlation peaks; and to decide on the desired spots by considering the spatial properties of the pores such as interspacing between the pores and average number of pores per cm^2.

The following are additional more future recommendations for the HCFA:

- Improvement in active pore detection by the use of various band pass filtering and various shapes of the correlation filters;
- HCFA can be modified to develop an automated technique for the detection of the distribution of sweat pores over fingertip ridges as a new method of human identification;
- It can also be further improved for the measurement of the degree of nervousness of the subject based on active pore count;

- At the moment HCFA can be only run from Matlab and in future specific model should be developed within a GUI environment to make it easier for use by any user without special training;

- Source code of HCFA should be platform independent so that should be compatible with any Mac, Windows or Android based machines. It should be compact, and must be able to installed on 3G mobile devices such as iPhones, tablet devices and net books with fingerprint security.

It was discovered whilst researching that the existing fingerprint databases were not appropriate for use in detect active sweat pore research, and were not able to be deployed in checking liveness by using HCFA.

Also, the fake fingertip images database (ATVS-FFp) was used to test HCFA. Manual inspection revealed that there was no active pores were available in the fake fingertip images. It was further evidence that active pores were not easy to replicate on fake finger stamps.

It was found from the critical review on fingerprint databases features that, the images are low resolution and do not show signs of active pores on ridges. It was even difficult in these images to manually identify pores as the distinguish attributes, that make clear the difference between active and inactive sweat pores, were not visible. Even in high resolution fingerprint database such as PolyU-HRF where pores were visible on fingertips, it was still difficult to distinguish between active and inactive pores.

B-FBDB database is a novel live fingertip database which contained the highest resolution images not only with ridges and valleys but also with visible active pores. This database can be very useful in the future to potential further in depth studies of active pores to build a liveness and pore distribution based identification method.

The second liveness detection technique presented in Chapter 4 was based on the detection of surface charge in sweat droplets which appear when the sweat pore is in an active state. The sweat fluid that appears at the openings of active pores possess an ionic charge. Sensing that ionic activity is a novel concept in the development of detecting evidence of liveness in a finger. This phenomenon only occurs in live fingertips. This liveness detection technique would help in

stopping the use of fake fingertips on systems; however, further research is needed to develop nanotechnology based sensor array to detect ionic activity on a finger sweat pores.
This technique was tested within a controlled experimental environment and specially formulated sample of sweat fluid used to represent actual sweat. This technique was not tested on real fingertips or real sweat droplets. However, an experimental setup was specifically developed for the measurement of sample ionic fluid prepared with the same composition of chemicals available in real sweat.

Following are the limitations with this technique:

- The measurements of surface charge were taken with sample ionic fluid droplets only and not tested with real sweat fluid from active pores;
- The present setup is not practical to measure in real-time the level of charge from actual sweat droplets because of its design limitations;
- The Experimental setup was based only a on a single microelectrode, and each measurement was obtained with only a single droplet

It is recommended that the experimental setup design can be altered to support the next level of research in the future by:

- Using a single or an array of micro/nano electrodes;
- Making the design suitable for the position of the finger;
- Controlling the precise position of the electrodes automatically;
- Simultaneous real time measurement of multiple sweat droplets of different sizes,
- The NME position is checked at the centre of droplet and therefore in future it is important to perform measurements at other positions of NME.

Here the main focus was to understand the phenomena of measurement of charge and current over the sweat droplets, which supported the best positions for the NME to fix it over the fingertip at appropriate distances to measure the charges from active sweat pores without making direct contact.

In future, using this idea, an integrated micro/nano array based sensor unit for liveness detection can be developed for real-time liveness detection using ionic activity of sweat pore. A conceptual image of such an envisaged sensor system is presented in Figure 5.1.

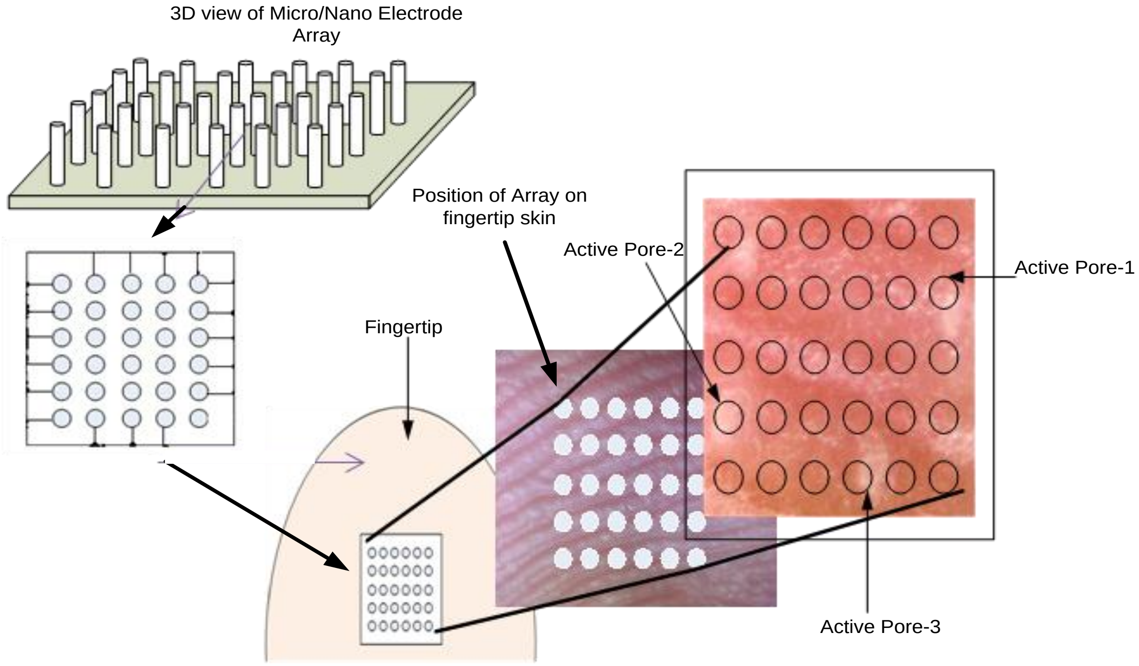

3D view of Micro/Nano Electrode Array
Position of Array on fingertip skin
Active Pore-2
Active Pore-1
Fingertip
Active Pore-3

Figure 5.1 Micro/Nano array for Liveness detection

A FEM of EGIF droplet and NME interaction was studied by in COMSOL multiphysics software. It was explained in chapter four with experimental results. In future, this model should be modified with different shapes and sizes of EGIF and electrode. The position of electrode(s) can be set at various points over the curve of EGIF droplet. Moreover, the same concept can be used to redesign with 3D geometries to show a more close to realistic view of the proposed idea.

References

[1] Anil K. Jain, "Biometric recognition," *NATURE*, vol. 449, pp. 38-40, September 2007, 2007.

[2] S. Prabhakar, J. Kittler, D. Maltoni, L. O'Gorman and T. Tan, "Introduction to the special issue on biometrics: Progress and directions," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 29, pp. 513-516, 2007.

[3] J. Fulton, "Fingerprint the point of sale," *Biometric Technology Today*, vol. 2011, pp. 7-9, 2011.

[4] A. Moore, "Biometric technologies — an introduction," *Biometric Technology Today*, vol. 15, pp. 6-7, 1, 2007.

[5] Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S. *Handbook of Fingerprint Recognition* 2009.

[6] International Biometrics Group. Biometrics revenues by technology 2009. *BMIR 2009-2014 2011(10/11)*, pp. 1. 2011.

[7] W. David , L. Mike. Six biometric devices point the finger at security. [Online]. *2011(10/11)*, pp. 2. 2010. Available: http://www.networkcomputing.com/910/910r1.html.

[8] M. Espinoza and C. Champod, "Risk evaluation for spoofing against a sensor supplied with liveness detection," *Forensic Sci. Int.*, vol. 204, pp. 162-168, 1/30, 2011.

[9] Y. Flink. Million dollar border security machines fooled with ten cent tape. *Find Biometrics-Global Identity Management* [Online]. *2010(03/13)*, 2009. Available: http://www.findbiometrics.com/articles/i/6090/.

[10] H. Kang, B. Lee, H. Kim, D. Shin and J. Kim, "A Study on Performance Evaluation of the Liveness Detection for Various Fingerprint Sensor Modules," *Knowledge-Based Intelligent Information and Engineering Systems*, pp. 1245-1253, 2003.

[11] R. Derakhshani, S. A. C. Schuckers, L. A. Hornak and L. O'Gorman, "Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners," *Pattern Recognit*, vol. 36, pp. 383-396, 2, 2003.

[12] P. Komarinski, *Automated Fingerprint Identification Systems (AFIS).* Academic Press, 2005.

[13] A. K. Jain, P. J. Flynn and A. A. Ross, *Handbook of Biometrics.* Springer, 2008.

[14] T. Matsumoto. Gummy and conductive silicone rubber fingers importance of vulnerability analysis. *Advances in Cryptology—ASIACRYPT 2002* pp. 59-65. 2002.

[15] T. Matsumoto, H. Matsumoto, K. Yamada and S. Hoshino, "Impact of artificial gummy fingers on fingerprint systems," in *Proceedings of SPIE*, 2002, pp. 275-289.

[16] Qinghan Xiao, "Security issues in biometric authentication," in *Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC*, 2005, pp. 8-13.

[17] U. Uludag and A. K. Jain, "Attacks on biometric systems: A case study in fingerprints," in *Proc. SPIE-EI 2004, Security, Seganography and Watermarking of Multimedia Contents VI*, 2004, pp. 622-633.

[18] C. Roberts, "Biometric attack vectors and defences," *Comput. Secur.*, vol. 26, pp. 14-25, 2, 2007.

[19] C. Barral and A. Tria, "Fake Fingers in Fingerprint Recognition: Glycerin Supersedes Gelatin," *Formal to Practical Security*, pp. 57-69, 2009.

[20] M. Tistarelli, S. Z. Li and R. Chellappa, "Handbook of Remote Biometrics: for Surveillance and Security," *Advances in Pattern Recognition*, pp. 382, 2009.

[21] S. Memon, M. Sepasian and W. Balachandran, "Review of finger print sensing technologies," in *Multitopic Conference, 2008. INMIC 2008. IEEE International*, 2008, pp. 226-231.

[22] S. Memon, N. Manivannan, A. Noor, W. Balachadran and V. N. Boulgouris, "Fingerprint Sensors: Liveness Detection Issue and Hardware based Solutions," *Sensors & Transducers Journal*, vol. 136, pp. 35-49, 2012.

[23] H. C. Lee, R. E. Gaensslen, H. Lee and R. Gaensslen, "Advances in fingerprint technology," *Boca Raton, Florida*, .

[24] C. Roberts. Biometric technologies - fingerprints. National Cyber Security Centre. New Zealand. 2006Available: www.ccip.govt.nz/notes/biometrics-technologies-fingerprints.pdf.

[25] Jean-François Mainguet. Fingerprint sensors. [Online]. *2011(08/12)*, 2009. Available: http://pagesperso-orange.fr/fingerchip/biometrics/types/fingerprint_sensors_productsi.htm.

[26] L. MIAXIS Biometrics Co, " FPR-620 Optical Fingerprint Reader," vol. 2010, 2009.

[27] A. K. Jain, Yi Chen and M. Demirkus, "Pores and Ridges: High-Resolution Fingerprint Matching Using Level 3 Features," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 29, pp. 15-27, 2007.

[28] Fernando Alonso-Fernandez, Fabio Roli, Gian Luca Marcialis, Julian Fierrez, Javier Ortega-Garcia and Joaquin Gonzalez-Rodriguez. Performance of fingerprint quality measures depending on sensor technology. *Journal of Electronic Imaging 17(1)*, pp. 11. 2008.

[29] I. Fujieda and H. Haga, "Fingerprint input based on scattered-light detection," *Appl. Opt.*, vol. 36, pp. 9152-9156, 1997.

[30] E. Sano, T. Maeda, M. Matsushita, M. Shikai, K. Sasakawa, M. Ohmi and M. Haruna, "Fingerprint sensor based on interior optical characteristics of the finger," *Electronics and Communications in Japan,* vol. 91, pp. 48-56, 2008.

[31] C. D. Tran, "Principles, instrumentation, and applications of infrared multispectral imaging, an overview," *Anal. Lett.,* vol. 38, pp. 735-752, 2005.

[32] M. Ennis, R. Rowe, S. Corcoran and K. Nixon, "Multispectral sensing for high-performance fingerprint biometric imaging," *Lumidigm, Inc.See: Http://www.Lumidigm.com/PDFs/Multispectral_Fingerprint_Imaging.Pdf,* 2005.

[33] R. Rowe, K. Nixon and P. Butler, "Multispectral Fingerprint Image Acquisition," *Advances in Biometrics,* pp. 3-23, 2008.

[34] R. K. Rowe, K. Nixon and S. Corcoran, "Multispectral fingerprint biometrics," in *Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC,* 2005, pp. 14-20.

[35] I. Lumidigm. Mercury desktop sensor. [Online]. *2011(8/10),* Available: http://www.lumidigm.com.

[36] K. Nixon and R. Rowe, "Spoof detection using multispectral fingerprint imaging without enrollment," in *Proceedings of Biometrics Symposium (BSYM2005), Arlington, VA,* 2005, .

[37] G. Parziale, "Touchless Fingerprinting Technology," *Advances in Biometrics,* pp. 25-48, 2008.

[38] C. Lee, S. Lee and J. Kim, "A study of touchless fingerprint recognition system," *Structural, Syntactic, and Statistical Pattern Recognition,* pp. 358-365, 2006.

[39] Y. Chen, G. Parziale, E. Diaz-Santana and A. K. Jain, "3D touchless fingerprints: Compatibility with legacy rolled images," in *Biometric Consortium Conference, 2006 Biometrics Symposium: Special Session on Research at the,* 2006, pp. 1-6.

[40] iFingersys, "Fingerprint Biometrics," vol. 2011, pp. 08, .

[41] TBS inc. Touchless terminals- the TBS 3D guard series. [Online]. *2011(9/13),* Available: http://www.tbsinc.com.

[42] Flash Scan3D, "3D Touchless Fingerprint Biometrics," vol. 2011, 2010.

[43] S. Memon, M. Sepasian and W. Balachandran, "Review of finger print sensing technologies," in *Multitopic Conference, 2008. INMIC 2008. IEEE International,* 2008, pp. 226-231.

[44] P. Coli, G. Marcialis and F. Roli, "Vitality detection from fingerprint images: a critical survey," *Advances in Biometrics,* pp. 722-731, 2007.

[45] S. Shigematsu, H. Morimura, Y. Tanabe, T. Adachi and K. Machida, "A single-chip fingerprint sensor and identifier," *Solid-State Circuits, IEEE Journal of,* vol. 34, pp. 1852-1859, 1999.

[46] M. A. Acree, "Is there a gender difference in fingerprint ridge density?" *Forensic Sci. Int.,* vol. 102, pp. 35-44, 5/31, 1999.

[47] M. L. Sheu, C. K. Lai, W. H. Hsu and H. M. Yang, "A novel capacitive sensing scheme for fingerprint acquisition," in *Electron Devices and Solid-State Circuits, 2005 IEEE Conference on,* 2005, pp. 627-630.

[48] T. Harris. Capacitive scanner

. [Online]. *2011(10/01),* pp. 01. 2010. Available: http://computer.howstuffworks.com/fingerprint-scanner3.htm.

[49] i. UPEK. TCS1 TouchChip fingerprint sensor. [Online]. *2011(8/20),* Available: http://www.upek.com.

[50] Hyosup Kang, Bongku Lee, Hakil Kim, Daecheol Shin and Jaesung Kim, "A study on performance evaluation of fingerprint sensors ," in *Audio- and Video-Based Biometric Person Authentication*Anonymous Berlin / Heidelberg: Springer, 2003, pp. 1055.

[51] D. R. Setlak, "Advances in fingerprint sensors using RF imaging techniques," *Automatic Fingerprint Recognition Systems, N.Ratha and R.Bolle, Springer-Verlag, New York,* 2004.

[52] Bergdata Biometrics GmbH. Fingerprint-E field sensors. [Online]. *2011(11/03),* pp. 01. 2010. Available: http://www.authentec.com/.

[53] Validity Inc., "VFS201 Fingerprint Sensor Product Brief," vol. 2010, pp. 02, 2010.

[54] K. M. Chan, A. Pop, S. Safarkhah and G. Virdi, "A Security Analysis of RF Biometric Fingerprint Scanners," .

[55] Hiro Han and Yasuhiro Koshimoto. Characteristics of thermal-type fingerprint sensor. *Biometric Technology for Human Identification,Proc. of SPIE 6944*pp. 1-12. 2008.

[56] J. Han, Z. Tan, K. Sato and M. Shikida, "Thermal characterization of micro heater arrays on a polyimide film substrate for fingerprint sensing applications," *J Micromech Microengineering,* vol. 15, pp. 282, 2005.

[57] G. MSC Vertriebs GmbH, "FingerChip™, Atmel‘s Biometric Sensor," vol. 2010, pp. 01, 2010.

[58] H. Kang, B. Lee, H. Kim, D. Shin and J. Kim, "A study on performance evaluation of the liveness detection for various fingerprint sensor modules," in *Knowledge-Based Intelligent Information and Engineering Systems,* 2003, pp. 1245-1253.

[59] Y. Saijo, K. Kobayashi, N. Okada, N. Hozumi, Y. Hagiwara, A. Tanaka and T. Iwamoto, "High frequency ultrasound imaging of surface and subsurface structures of fingerprints," in *Engineering in Medicine and Biology Society, 2008. EMBS 2008. 30th Annual International Conference of the IEEE,* 2008, pp. 2173-2176.

[60] M. Damghanian and B. Y. Majlis, "Novel Design and Fabrication of High Sensitivity MEMS Capacitive Sensor Array for Fingerprint Imaging," *Advanced Materials Research,* vol. 74, pp. 239-242, 2009.

[61] J. Scheibert12, G. Debrégeas and A. Prevost, "A MEMS-based tactile sensor to study human digital touch: mechanical transduction of the tactile information and role of fingerprints," 2010.

[62] N. Sato, S. Shigematsu, H. Morimura, M. Yano, K. Kudou, T. Kamei and K. Machida. Novel surface structure and its fabrication process for MEMS fingerprint sensor. *IEEE Transactions on Electron Devices 52(5),* pp. 1026-1032. 2005.

[63] D. Petrovska-Delacrétaz, G. Chollet, K. Anil and B. Dorizzi, *Guide to Biometric Reference Systems and Performance Evaluation.* Springer-Verlag New York Inc, 2009.

[64] Y. Wang, F. Agrafioti, D. Hatzinakos and K. N. Plataniotis, "Analysis of human electrocardiogram for biometric recognition," *EURASIP Journal on Advances in Signal Processing,* vol. 2008, pp. 19, 2008.

[65] K. N. Plataniotis, D. Hatzinakos and J. K. M. Lee, "ECG biometric recognition without fiducial detection," in *Biometric Consortium Conference, 2006 Biometrics Symposium: Special Session on Research at the,* 2006, pp. 1-6.

[66] S. Marcel and J. D. R. Millan, "Person Authentication Using Brainwaves (EEG) and Maximum A Posteriori Model Adaptation," *Pattern Analysis and Machine Intelligence, IEEE Transactions on,* vol. 29, pp. 743-752, 2007.

[67] R. Palaniappan and D. Mandic, "EEG Based Biometric Framework for Automatic Identity Verification," *The Journal of VLSI Signal Processing,* vol. 49, pp. 243-250, 11/01/, 2007.

[68] P. E. Keller, "Electronic noses and their applications," in *Northcon 95. I EEE Technical Applications Conference and Workshops Northcon95,* 1995, pp. 116.

[69] D. Baldisserra, A. Franco, D. Maio and D. Maltoni, "Fake Fingerprint Detection by Odor Analysis ," *Advances in Biometrics,* pp. 265-272, 2005.

[70] Jim Edmond Riviere, "Structure and function of skin," in Anonymous CRC Press, 2005, pp. 1-18.

[71] M. Chaberski, "Level 3 friction ridge research," *Biometric Technology Today,* vol. 16, pp. 9-12, 12, 2008.

[72] Ryan R. Emerging biometric technologies. *Secuity infoWatch* [Online]. *2010(03/12),* 2009. Available: http://www.securityinfowatch.com/Access+Control/emerging-biometric-technologies.

[73] O. Martinsen, S. Clausen, J. B. Nysæther and S. Grimnes, "Utilizing Characteristic Electrical Properties of the Epidermal Skin Layers to Detect Fake Fingers in Biometric Fingerprint Systems—A Pilot Study," *IEEE Transactions on Biomedical Engineering,* vol. 54, pp. 891–894, 2007.

[74] T. Shimamura, H. Morimura, N. Shimoyama, T. Sakata, S. Shigematsu, K. Machida and M. Nakanishi, "A fingerprint sensor with impedance sensing for fraud detection," in *Solid-State Circuits Conference, 2008. ISSCC 2008. Digest of Technical Papers. IEEE International,* 2008, pp. 170-604.

[75] Wei-Yun Yau, Hai-Linh Tran and Eam-Khwang Teoh, "Fake finger detection using an electrotactile display system," in *Control, Automation, Robotics and Vision, 2008. ICARCV 2008. 10th International Conference on,* 2008, pp. 962-966.

[76] K. Nixon, V. Aimale and R. Rowe, "Spoof detection schemes," *Handbook of Biometrics,* pp. 403-423, 2008.

[77] Y. S. Moon, J. Chen, K. Chan, K. So and K. Woo, "Wavelet based fingerprint liveness detection," *Electron. Lett.*, vol. 41, pp. 1112-1113, 2005.

[78] S.T.V. Parthasaradhi, R. Derakhshani, L.A. Hornak and S.A.C. Schuckers, "Time-series detection of perspiration as a liveness test in fingerprint devices," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on,* vol. 35, pp. 335-343, 2005.

[79] R. Derakhshani, S. A. C. Schuckers, L. A. Hornak and L. O'Gorman, "Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners," *Pattern Recognit,* vol. 36, pp. 383-396, 2003.

[80] A. Antonelli, R. Cappelli, D. Maio and D. Maltoni, "A new approach to fake finger detection based on skin distortion," *Advances in Biometrics,* pp. 221-228, 2005.

[81] B. Tan and S. Schuckers, "Spoofing protection for fingerprint scanner by fusing ridge signal and valley noise," *Pattern Recognit,* vol. 43, pp. 2845-2857, 2010.

[82] M. Ray, P. Meenen and R. Adhami, "A novel approach to fingerprint pore extraction," 2005.

[83] C. Watson and C. L. Wilson, "NIST special database 4, fingerprint database," National Institute of Standards and Technology, USA, 2008.

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

[85] A. Abhyankar and S. Schuckers, "Integrating a wavelet based perspiration liveness check with fingerprint recognition," *Pattern Recognit,* vol. 42, pp. 452-464, 3, 2009.

[86] B. DeCann, B. Tan and S. Schuckers, "A novel region based liveness detection approach for fingerprint scanners," *Advances in Biometrics,* pp. 627-636, 2009.

[87] A. Antonelli, R. Cappelli, D. Maio and D. Maltoni, "Fake finger detection by skin distortion analysis," *Information Forensics and Security, IEEE Transactions on,* vol. 1, pp. 360-373, 2006.

[88] M. Drahansky, R. Notzel and W. Funk, "Liveness detection based on fine movements of the fingertip surface," in *Information Assurance Workshop, 2006 IEEE,* 2006, pp. 42-47.

[89] J. Jia, L. Cai, K. Zhang and D. Chen, "A new approach to fake finger detection based on skin elasticity analysis," *Advances in Biometrics,* pp. 309-318, 2007.

[90] P. Coli, G. L. Marcialis and F. Roli, "Power spectrum-based fingerprint vitality detection," in *Automatic Identification Advanced Technologies, 2007 IEEE Workshop on,* 2007, pp. 169-173.

[91] W. Y. Yau, H. T. Tran, E. K. Teoh and J. G. Wang, "Fake finger detection by finger color change analysis," *Advances in Biometrics,* pp. 888-896, 2007.

[92] C. Jin, H. Kim and S. Elliott, "Liveness Detection of Fingerprint Based on Band-Selective Fourier Spectrum," *Information Security and Cryptology - ICISC 2007,* pp. 168-179, 2007.

[93] S. S. Tan B. New approach for liveness detection in fingerprint scanners based on valley noise analysis. *SPIE Journal of Electronic Imaging 17(1),* 2008.

[94] S. B. Nikam and S. Agarwal, "Fingerprint liveness detection using curvelet energy and co-occurrence signatures," in *Computer Graphics, Imaging and Visualisation, 2008. CGIV'08. Fifth International Conference on,* 2008, pp. 217-222.

[95] M. Drahansky and D. Lodrova, "Liveness detection for biometric systems based on papillary lines," in *Information Security and Assurance, 2008. ISA 2008. International Conference on,* 2008, pp. 439-444.

[96] H. Choi, R. Kang, K. Choi, A. T. B. Jin and J. Kim, "Fake-fingerprint detection using multiple static features," *Optical Engineering,* vol. 48, pp. 047202, 2009.

[97] S. B. Nikam and S. Agarwal, "Curvelet-based fingerprint anti-spoofing," *Signal, Image and Video Processing,* vol. 4, pp. 75-87, 2010.

[98] C. Jin, S. Li, H. Kim and E. Park, "Fingerprint liveness detection based on multiple image quality features," *Information Security Applications,* pp. 281-291, 2011.

[99] Q. Zhao, D. Zhang, L. Zhang and N. Luo, "Adaptive fingerprint pore modeling and extraction," *Pattern Recognit,* vol. 43, pp. 2833-2844, 2010.

[100] P. Coli, G. Marcialis and F. Roli, "Vitality Detection from Fingerprint Images: A Critical Survey," *Advances in Biometrics,* pp. 722-731, 2009.

[101] J. P. Bindra B.1 Singla A.K., "Poroscopy: A method of personal identification revisited," *Anil Aggrawal's Internet Journal of Forensic Medicine and Toxicology,* vol. 1, 2000.

[102] Sharma B. K., Khajuria H., Misra V. C., Lukose S., "Poroscopy – A study of similar characteristics of pores in individuals," *Amity Journal of Behavioural and Forensic Sciences,* vol. 3, 2007.

[103] H. Choi, R. Kang, K. Choi and J. Kim, "Aliveness detection of fingerprints using multiple static features," in *Proc. of World Academy of Science, Engineering and Technology,* 2007, .

[104] C. L. Wilson and National Institute of Standards and Technology (US), *Studies of Fingerprint Matching using the NIST Verification Test Bed (VTB).* US Dept. of Commerce, Technology Administration, National Institute of Standards and Technology, 2003.

[105] D. Petrovska-Delacrétaz, G. Chollet and B. Dorizzi, *Guide to Biometric Reference Systems and Performance Evaluation.* Springer-Verlag New York Inc, 2009.

[106] C. I. Watson. NIST special database 9, fingerprint database. National Institute of Standards and Technology. USA. 2011[Online]. Available: http://www.nist.gov/srd/upload/Spec-db-9.pdf.

[107] C. I. Watson. NIST special database 14: Mated fingerprint card pairs 2. National Institute of Standards and Technology. USA. [Online]. Available: http://www.nist.gov/srd/upload/Spec-db-14.pdf.

[108] C. I. Watson. NIST special database 29, plain and rolled images from paired fingerprint cards. National Institute of Standards and Technology. USA. [Online]. Available: ftp://sequoyah.nist.gov/pub/nist_internal_reports/ir_6801.pdf.

[109] C. I. Watson, "NIST Special Database 30 Dual Resolution Images from Paired Fingerprint Cards," *National Institute of Standards and Technology, Gaithersburg, MD,* .

[110] D. Maio, D. Maltoni, R. Cappelli, J. Wayman and A. Jain, "ªFVC2000: Fingerprint verification competition," in º *Proc. 15th IAPR Int'l Conf. Pattern Recognition, Sept,* 2000, .

[111] D. Maltoni, R. Cappelli, J. Wayman and A. Jain, "FVC2002: Second fingerprint verification competition," in *International Conference on Pattern Recognition,* 2002, pp. 811-814.

[112] R. Cappelli, M. Ferrara, A. Franco and D. Maltoni, "Fingerprint verification competition 2006," *Biometric Technology Today,* vol. 15, pp. 7-9, 2007.

[113] R. Cappelli, D. Maio and D. Maltoni, "Synthetic fingerprint-database generation," *Pattern Recognit,* vol. 3, pp. 30744, 2002.

[114] R. Cappelli, D. Maio and D. Maltoni, "Synthetic fingerprint-database generation," *Pattern Recognit,* vol. 3, pp. 30744, 2002.

[115] D. Maio and D. Maltoni. SFinGE. *Biometric System Laboratory,University of Bologna* [Online]. *2011(10/15),* pp. 1. 2011. Available: http://biolab.csr.unibo.it/research.asp?organize=Activities&select=&selObj=12&pathSubj=111 ; ; 12&.

[116] A. M. Bazen, G. T. B. Verwaaijen, S. H. Gerez, L. P. J. Veelenturf and B. J. van der Zwaag, "A correlation-based fingerprint verification system," in *Proceedings of the ProRISC2000 Workshop on Circuits, Systems and Signal Processing, Veldhoven, Netherlands,* 2000, .

[117] R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman and A. K. Jain, "Performance evaluation of fingerprint verification systems," *IEEE Trans. Pattern Anal. Mach. Intell.,* pp. 3-18, 2006.

[118] J. Fierrez-Aguilar, Y. Chen, J. Ortega-Garcia and A. K. Jain, "Incorporating image quality in multi-algorithm fingerprint verification," *Advances in Biometrics,* pp. 213-220, 2005.

[119] J. Fierrez-Aguilar, L. Nanni, J. Ortega-Garcia, R. Cappelli and D. Maltoni, "Combining multiple matchers for fingerprint verification: A case study in FVC2004," *Image Analysis and Processing–ICIAP 2005,* pp. 1035-1042, 2005.

[120] J. Galbally-Herrero, J. Fierrez-Aguilar, J. Rodriguez-Gonzalez, F. Alonso-Fernandez, J. Ortega-Garcia and M. Tapiador, "On the vulnerability of fingerprint verification systems to fake fingerprints attacks," in *Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International,* 2006, pp. 130-136.

[121] Y. He, J. Tian, X. Luo and T. Zhang, "Image enhancement and minutiae matching in fingerprint verification," *Pattern Recog. Lett.,* vol. 24, pp. 1349-1360, 2003.

[122] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman and A. K. Jain, "FVC2002: Second fingerprint verification competition," *Pattern Recognit,* vol. 3, pp. 30811, 2002.

[123] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman and A. K. Jain, "FVC2004: third fingerprint verification competition," *Biometric Authentication,* pp. 1-5, 2004.

[124] J. Galbally, "ATVS-fake fingerprint database," Biometric Recognition Group-ATVS,Universidad Autonoma de Madrid, Spain, Tech. Rep. 1, 2011.

[125] G. L. Marcialis and F. Roli, "Liveness detection competition 2009," *Biometric Technology Today,* vol. 17, pp. 7-9, 2009.

[126] G. L. Marcialis and F. Roli, "Liveness detection competition 2009," *Biometric Technology Today,* vol. 17, pp. 7-9, 3, 2009.

[127] G. Marcialis, A. Lewicke, B. Tan, P. Coli, D. Grimberg, A. Congiu, A. Tidu, F. Roli and S. Schuckers, "First international fingerprint liveness detection competition—livdet 2009," *Image Analysis and Processing–ICIAP 2009,* pp. 12-23, 2009.

[128] L. Zhang. Poly U-high-resolution-fingerprint (HRF) database. *The Hong Kong Polytechnic University* [Online]. *2011(09/12),* pp. 1. 2011. Available: http://www4.comp.polyu.edu.hk/~biometrics/.

[129] N. Manivanan, S. Memon and W. Balachandran, "Automatic detection of active sweat pores of fingerprint using highpass and correlation filtering," *Electron. Lett.,* vol. 46, pp. 1268-1269, 2010.

[130] D. G. Bailey, "Detecting regular patterns using frequency domain self-filtering," in *Icip,* 1997, pp. 440.

[131] N. Mannivannan, M. Neil and E. Paige, "Optical multiple pattern recognition with a correlator using a single binary phase-only filter," *Opt. Commun.,* vol. 178, pp. 37-51, 2000.

[132] B. V. K. V. Kumar, C. Xie and M. Savvides, "Correlation filters for large population face recognition," in Orlando, FL, USA, 2007, pp. 65390F.

[133] Y. Han, A. Dang, J. Tang and H. Guo, "Weak beacon detection for air-to-ground optical wireless link establishment," *Optics Express,* vol. 18, pp. 1841-1853, 2010.

[134] F. Transforms and A. L. Schoenstadt, "An Introduction to Fourier Analysis," 2006.

[135] S. Memon, N. Manivannan and W. Balachandran, "Active pore detection for liveness in fingerprint identification system," in *Telecommunications Forum (TELFOR), 2011 19th,* 2011, pp. 619-622.

[136] Richard D. Granstein, Thomas A. Luger, *Neuroimmunology of the Skin: Basic Science to Clinical Practice.* Springer, 2008.

[137] Henry C. Lee, Robert E. Gaensslen, *Advances in Fingerprint Technology.* CRC Press, 2001.

[138] Keithley, *Low Level Measurement Handbook.* eithley Instrument, Inc., 2008.

[139] D. R. Cantrell, S. Inayat, A. Taflove, R. S. Ruoff and J. B. Troy, "Incorporation of the electrode–electrolyte interface into finite-element models of metal microelectrodes," *Journal of Neural Engineering,* vol. 5, pp. 54, 2008.

[140] A. Lavacchi, U. Bardi, C. Borri, S. Caporali, A. Fossati and I. Perissi, "Cyclic voltammetry simulation at microelectrode arrays with COMSOL Multiphysics®," *J. Appl. Electrochem.,* vol. 39, pp. 2159-2163, 2009.

[141] Anonymous *COMSOL Multiphysics Modeling Guide-Version 3.5a.* COMSOL Lab, 2008.