A NEW MULTI-MODAL BIOMETRIC SYSTEM BASED ON FINGERPRINT AND FINGER VEIN RECOGNITION

Naveed AHMED

Master's Thesis
Department of Software Engineering
Advisor: Prof. Dr. Asaf VAROL

JULY-2014

REPUBLIC OF TURKEY
FIRAT UNIVERSITY
INSTITUTE OF NATURAL AND APPLIED SCIENCES

A NEW MULTI-MODAL BIOMETRIC SYSTEM BASED ON FINGERPRINT AND FINGER VEIN RECOGNITION

MASTER'S THESIS

Naveed AHMED

(121137109)

Thesis Submitted to the Institute Date : July 23, 2014
Thesis Defended Date : July 16, 2014

Thesis Advisor : **Prof. Dr. Asaf VAROL (F.U)**

Other Jury Members : **Assc. Prof. Dr. Abdulkadir SENGUR (F.U)**

Asst. Prof. Dr. Filiz VAROL (F.U)

JULY - 2014

DECLARATION

I am presenting this thesis with title “A New Multi-modal Biometric System Based on Fingerprint and Finger Vein Recognition” for the requirement of Master in Software Engineering. I declare that proposed system in thesis is my own work with all simulations and programming.

Naveed AHMED

Elazig, 2014

DEDICATION

I dedicate my thesis to my father, Abdul HAMID (Late).

ACKNOWLEDGEMENTS

I want to thank all the staff members of Department of Software Engineering at Firat University, without their help it was impossible for me to complete my Master. It was my first time in life to stay outside of my own country for as long but the love and care of all staff members including staff of my hostel never let me to feel any difference. Prof. Dr. Asaf VAROL he was not only chairman of my department, he was also advisor for my thesis. During the Master he helped me more than a chairman and teacher. Words cannot pay back anyone's kindness and help but still I want to say thanks to him. Res. Assist. Muhammet BAYKARA and Res. Assist. Zafer GULER, I also want to say thanks to them. They were staff members but during my entire Master they never let me to feel anytime that I am just a student in department. They always treated me like a colleague and a friend.

Naveed AHMED

TABLE OF CONTENTS

Page No

EXECUTIVE SUMMARY

In this thesis it has been proposed a system which is based on fusion of fingerprints and finger vein patterns. Both techniques are old and already in use, difference is this in proposed system the same processing steps have been used for fingerprint and finger vein pattern images so it is not required to have two different kinds of software for handling two different kinds of images and fortunately results are more accurate than expected. Fingerprints have lines in the language of biometric they are called ridges. Where these lines (ridges) end they are called termination points where these lines divide into two branches they are named bifurcation points. These points are actually main features their unique positions in the image of fingerprint help to differentiate between two fingerprint images. Same technique has been used for finger vein pattern. Finger veins appear same as ridges in the image and have same features It means veins also have termination points and bifurcation points. In proposed system both kinds of images have been prcocessed by using same steps with the help of MATLAB software then compared them with previously stored images and calculated some scores. These scores are actually number of matched points in both images. In last phase a final score has been calculated for decision that final score is actually an average of previously calculated fingerprint and finger vein pattern scores.

Results have proved the ability of the proposed system. Secondly it is multi-modal system so its accuracy and security level is much better than uni-modal systems. Input comes from two different sources and one of the source (finger vein pattern) is not very easy to alter or it can be said like that it is near to impossible. Equipment is also not very expensive or sensitive plus there is not any hesitation factor for users.

Keywords : Biometric, Fingerprints, Finger vein pattern, Score level fusion

LIST OF FIGURES

Page No

LIST OF TABLES

Page No

ACRONYMS

2D	: Two-dimensional
3D	: Three-dimensional
AFIS	: Automated Fingerprint Identification System
DNA	: Deoxyribo Nucleic Acid
FAR	: False Acceptance Rate

1. INTRODUCTION

Uni-modal systems are those systems which take single input from a single source. For example, fingerprint recognition system takes only fingerprint images either by using solid-state sensors or by using optical sensors. These kinds of systems are widely available in market. They are easy to use and much cheaper in price. But on other hand their accuracy and reliability level is also low. Anyone with very less effort can easily get access [1]. To overcome this problem multi-modal systems are introduced in market. There are different kinds of multi-modal systems but they can be easily divided into five different categories.

- Multiple inputs from same source (for example multiple fingerprint images by using different kind of sensors).
- Multiple inputs from same source (for example right and left fingerprint images by using same kind of sensors).
- Different image processing procedures for same inputs (for example using different kinds of software to process same image).
- Multiple samples but from same input [2] (for example multiple fingerprint images from same finger by using same sensor).
- Multiple inputs from multiple sources [3] (for example fingerprint and finger vein pattern images as it is used in this thesis).

1.1. Objective

The objective of this thesis is to develop a multi-modal (fingerprint and finger vein pattern) biometric system. System uses same processing procedure (MATLAB program) for both different kinds of images to save processing and memory storage capability of the system. Figure 1.1. shows the overall system.

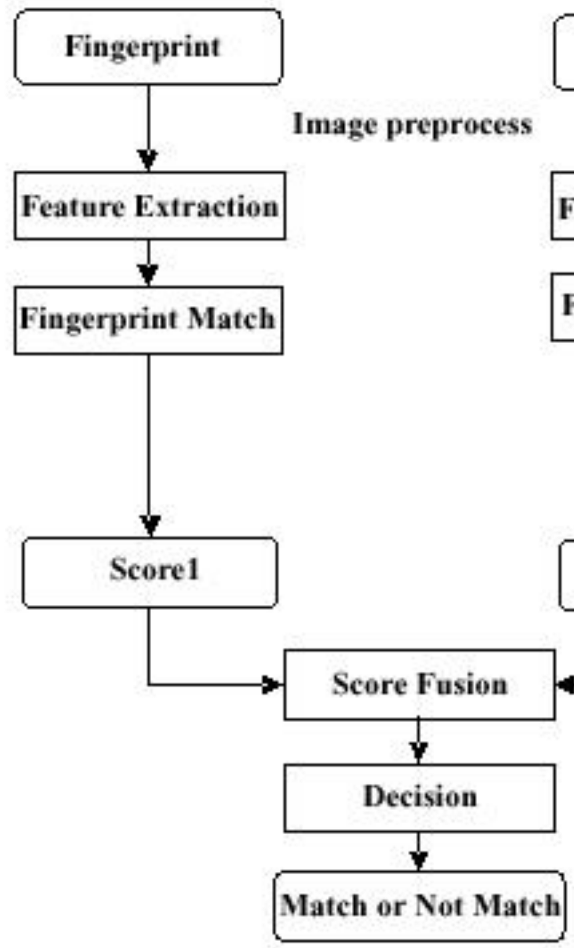


Figure 1.1. Overall system with fusion of fingerprint and finger vein matching scores.

System is initially divided into two sub systems, first sub system is responsible for processing of fingerprint images and second one is responsible for processing of finger vein pattern images. After processing of both kinds of images both sub systems generate scores. Then final system processes scores from both sub systems and compares it with a threshold value for final decision.

1.2. Literature Reviews

It has been reviewed a lot of literature published on biometric for this thesis which is referenced in respective sections. But for developing a multi-modal system with fusion of fingerprint and finger vein pattern images it was not enough. It is better to mention here these three master thesis which have provided a practical approach. First master thesis Analysis of Fingerprint and Voice Recognition Digital Evidence Processes [4] written by Gulsah Akkan has provided basic understanding about fingerprints and their handling and fingerprint recognition sub system in this thesis is the result of that guidance. Second thesis Determinatıon of Cancer Cells using an Expert System [5] written by Mustafa Kutukiz has helped in understanding of necessary image processing techniques for better results and handling of poor quality images. Last one Finger Vein Identification Technology [6] written by Songul San has given a motivation for introducing finger vein pattern recognition system as sub system in this thesis. All three above mentioned thesis were supervised by Varol [7].

1.3. Thesis Organization

Thesis is organized in this way; chapter 2 presents the historical background of biometric, how different biometric techniques are developed with working principles behind them and who were the developers. Chapter 3 focuses on different practical issues in biometric technology. Chapter 4 discusses the fingerprints details with the recognition sub system developed for this thesis. Chapter 5 is about finger vein pattern recognition sub system. Chapter 6 features score level fusion which makes final decision. Finally chapter 7 is conclusions and recommendations.

2. BIOMETRIC

Ancient Egyptians and Babylonia had been using different features of a human body for identification.

Fingerprints on clay in Figure 2.2. which had been using for identification in different kind of official works in Babylonian civilization [8].

Figure 2.2. Fingerprints on a piece of clay [9].

In 1890 Alphonse Bertillon, a French police man introduced a system of measuring different body parts for identification as shown in Figure 2.3. In beginning his system had adopted by many authorities but soon they realized that system is not so perfect because often people have same body measurements [10].

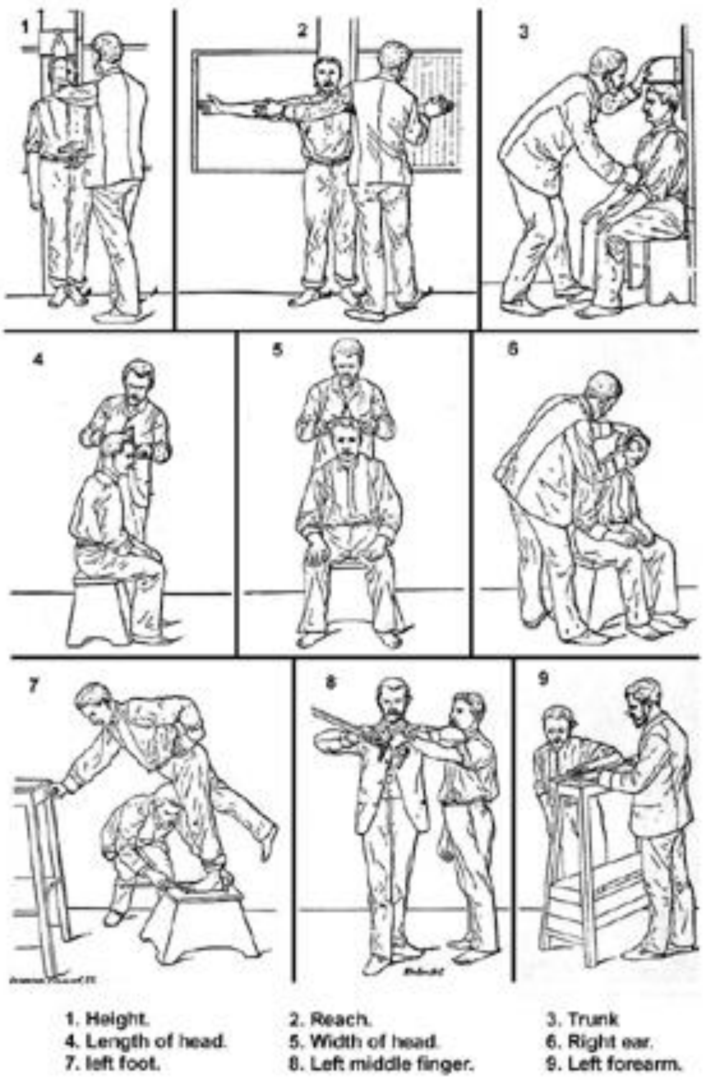


Figure 2.3. Bertillon system of measuring different body parts for identification [11].

A British anthropologist, Sir Francis Galton found that principle two people cannot have identical fingerprints not only this fingerprints stay same throughout the life [12]. In 1891 Juan Vucetich, an Argentine police officer used Galton's principle to solve a murder case [13].

In 1897 Sir Edward Henry with his colleagues from Bengal Police in India modified Galton’s principle of fingerprints and established a system for classification, storing and comparison shown in Figure 2.4. Scotland Yard of UK in 1901 adopted his system as a standard [14].

Figure 2.4. Sir Edward Henry system [15].

With the arrival of digital technology and computers biometric has entered into a new world. Only in UK different authorities record approximately 120,000 sets of fingerprints every year and it was not possible ever before. Canadian police in mid 60s started to use a video tape based automated filing system, similar system New Scotland Yard got in 1977 [16]. Federal Bureau of Investigation in USA around the same time was trying to build automated card reader for fingerprints [17].

Automatic fingerprint identification system was biggest achievement of 1980 in the field of crime detection. That achievement had reduced the fingerprint processing time from months and weeks to minutes [18]. Figure 2.5. shows an Automatic fingerprint identification system (AFIS).

Figure 2.5. Automatic fingerprint identification system [19].

2.1. Current Biometric Systems

Normally a biometric system has five basic components as shown in Figure 2.6: Sensors which are to collect the data and convert the data into digital format, Signal processing algorithms to develop the template ready for matching and storing, Data Storage to record templates for future use, Matching algorithms to match the input with previously stored templates and Decision process to make final decision about authentication [20].

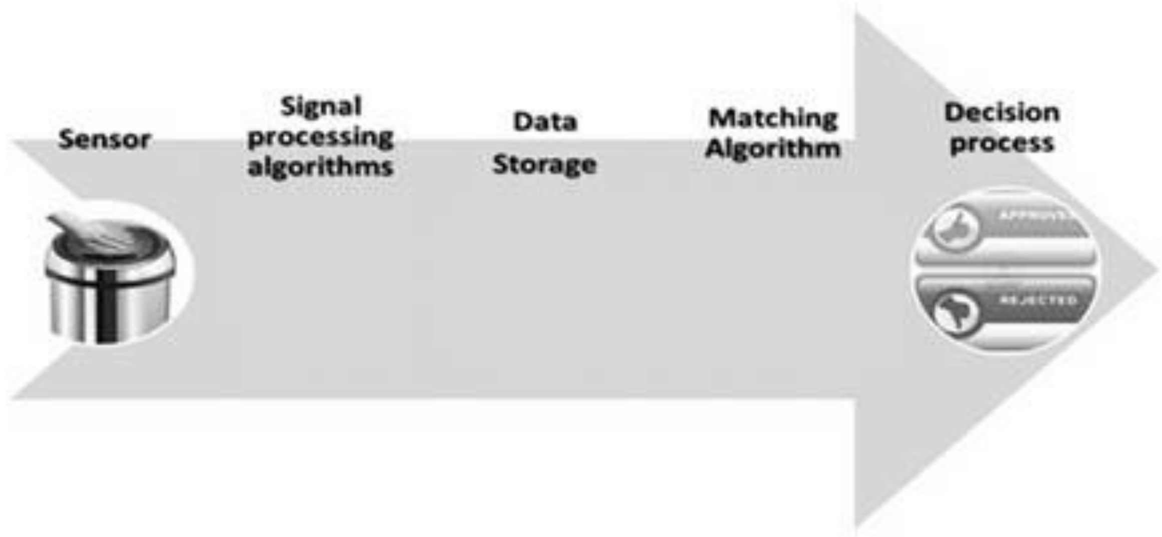


Figure 2.6. Biometric system components.

A lot of biometric systems are available in market now days. Still researcher and scientist are working to develop new ideas like odor analysis. No one system or technology can be considered better than other. Selection of any system or technology purely depends where we are going to use it.

2.1.1. Fingerprint Recognition

Fingerprint recognition is the oldest technique used for identification. Optical and silicon readers have taken place of paper and ink but the principle behind is still same.

Optical readers work on the principle of change in reflection. Some new readers have processing and memory capability. Figure 2.7. shows an example of commonly available finger print reader [21].

Figure 2.7. Optical fingerprint reader [22].

Usually optical readers are reliable but if they not get properly cleaned they have problems. They cannot be easily fooled by a picture of fingerprint but 3D model of a finger can be accepted by reader. Some modern readers have liveness detectors to overcome this problem. [23]. Silicon is older technology as compared to optical ones and it is based on capacitance of the finger [24].

Human finger acts as a plate of capacitor while other plate is made up of metal. When someone places his finger on the reader finger ridges shows high capacitance and valleys shows comparatively less and get more visible. Figure 2.8. shows working of an Active capacitance fingerprint reader. [25].

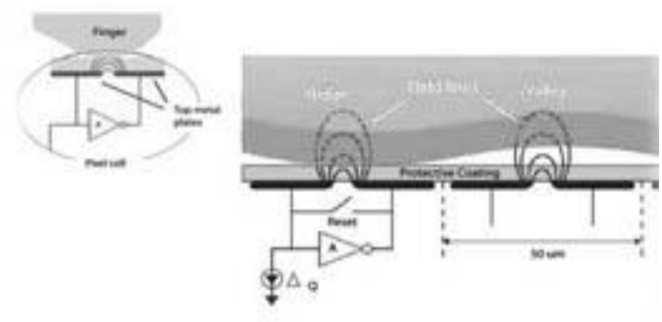


Figure 2.8. Active capacitance fingerprint reader [26].

Performance of silicon reader gets significantly affected by moisture. Wet fingers by sweat or by water make problems. Normally silicon and optical readers are fast enough that we can use them in real time applications.

Ultrasonic readers are comparatively new and least common in market. They are better in performance, more fast and accurate and results not affected usually by dirt or moisture [27].

Ultrasonic waves have ability to penetrate and scanner works on the principle of difference in acoustic impedance. Sound waves are transmitted and reflected. Low velocity propagation produces pulse-echo which is timed to vary depth and capturing image [27]. Figure 2.9. shows Schematic of ultrasound scan.

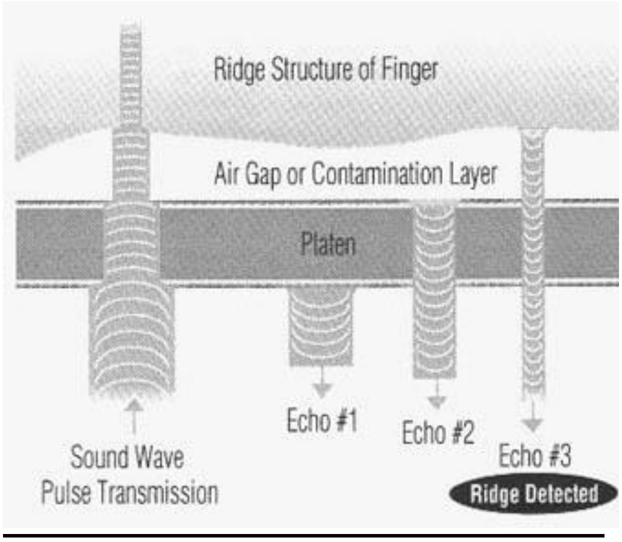


Figure 2.9. Schematic of ultrasound scan [28].

2.1.1.1. Fingerprint Processing

Matching techniques can be divided into two categories: Minutiae-based and Correlation based.

Minutiae-based: This technique works on the mapping of minutiae points and their relative placement. Most of automated fingerprint comparisons use this technique but low quality images affects a lot on accuracy [18].

Correlation-based: The biggest advantage of this technique is its ability to counter some difficulties of minutiae-based technique even it has some of its own short comes like precise location for registration and accuracy easily get affected by rotation of the image [29].

In any fingerprint image area loop is 65% of total pattern. Arch is also a kind of curve but have bigger opening than loop. Normally ach patterns can be divided into two plain and tented arches. Whorls are approximately 30% of any finger print pattern and have at least one ridge that makes a complete circle [30]. Three basic fingerprint patterns are in shown in Figure 2.10.

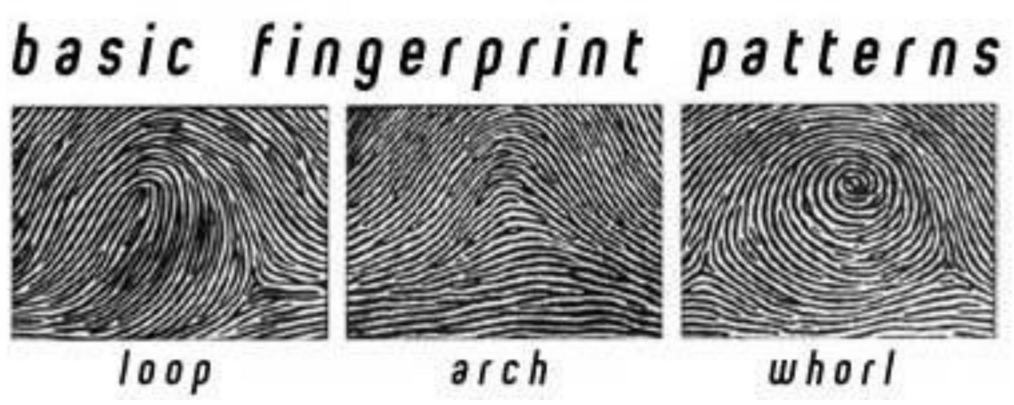


Figure 2.10. Three basic fingerprint patterns [31].

Fingerprint readability depends on many factors like age of someone, his or her gender and occupation also sometime race. A normal fingerprint have approximately 30 minutiae and 7 to 8 often resembles with someone but not more than this limit. In the USA court allows testimony based on 12 minutiae [32]. Image quality usually depends on how someone place finger on scanner plus condition of finger. Moisture and pressure plays a very important role.

Ridges are not straight lines as shown in Figure 2.11. sometime they are forked, sometime they are broken and sometime they change directions. The points where ridges forked, broke or change direction are called minutia and are used for identification. Even there are many different types of minutia exist in a fingerprint pattern but mostly endings and bifurcations are used [30].

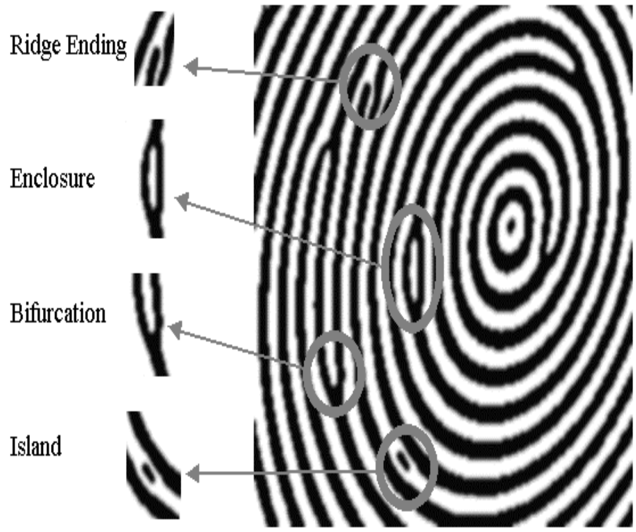


Figure 2.11. Ridge characteristics [33].

Negative results usually take more time than positive ones and it affect the overall speed of the system secondly there is no direct relation between accuracy and speed of the system. Image minutiae first get encoded and compressed then stored for future comparisons. Template sizes are between 24 bytes to 1 kilo byte. It is now possible to use fingerprints data within large databases. The reason behind this is the requirement of a search system for identification. Present available AFIS systems give 98% of identification rate with less than 1% of FAR [34]. Access control systems even they are automated but their accuracy level is relatively lower. Quality of the image as much depends on the reader as much it also depend on the user such as correct position and pressure of the finger on reader. Some systems have capability to find even pores (spatial distribution) but these kinds of systems depend too much on the input image quality. Hardware devices only provide bitmap images to system while software does all the processing for result. In market now some hardware are also available to perform all tasks but their accuracy level is relatively very low. Same like this there are some software available in market which is independent from input device but they have some accuracy problem [21].

2.1.2. Iris Pattern Recognition

Iris is the colored ring of textured tissue surrounds the eye pupil. Twins even have different patterns and everyone's right and left irises are different. Research shows that accuracy of iris identification is greater than testing DNA. The pattern is taken by a gray-scale special scanner in the distance of 10–40 cm. The scanner does not need any special kind of lighting conditions even if the background is too dark any traditional lighting can be used. Some scanners also have a light source that is automatically turned on when necessary. The pattern remains stable over a life, being only affected by some diseases [35].

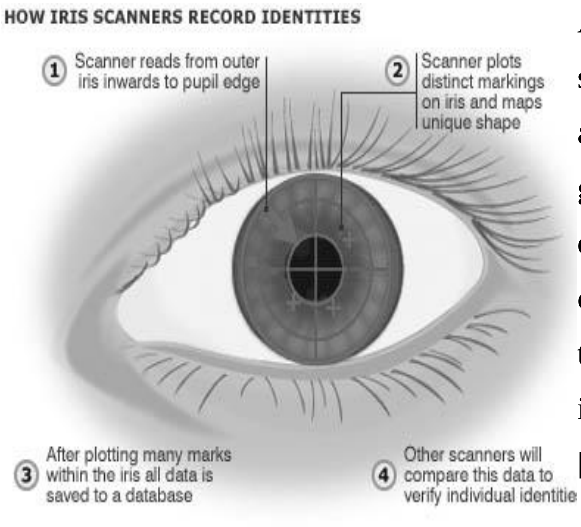


Figure 2.12. Illustration of iris recognition method [37].

After getting image from scanner software tries to locate the iris and creates a net of curves. In second step software generates the codes based on points of darkness along the lines. Lighting condition and pupil size directly effect on the iris-code. Figure 2.12. shows the illustration of iris recognition method [36].

In decision phase with the help of iris-codes software calculates hamming distance in the range of 0 and 1, where 0 shows similarity. Modern systems are as faster that they can calculate hamming distance for more than 4,000,000 iris-codes in 1 second [35]. Indeed in all available biometrics systems iris pattern recognition is most fasted and reliable one with lowest false rejection rate [38]. Iris pattern is nearly impossible to duplicate because it is connected directly to human brain and it is one of the first part of human body who get decay after death. Also new systems have liveness tests.

2.1.3. Retinal Scan

There are blood vessels pattern in retina and retinal scan technology depends on it. As compared to iris scan it is older and also uses human eye. In 1985 it was first time introduced and intrusiveness is the main drawback of it.

For retinal scan a coherent light source is required. Blood in the vessels absorb the infrared light and image of pattern get visible. While retina is more susceptible compared than iris to some diseases but these diseases are relatively rare [39]. Figure 2.13. shows new iPhone 6 with retina scan technology.

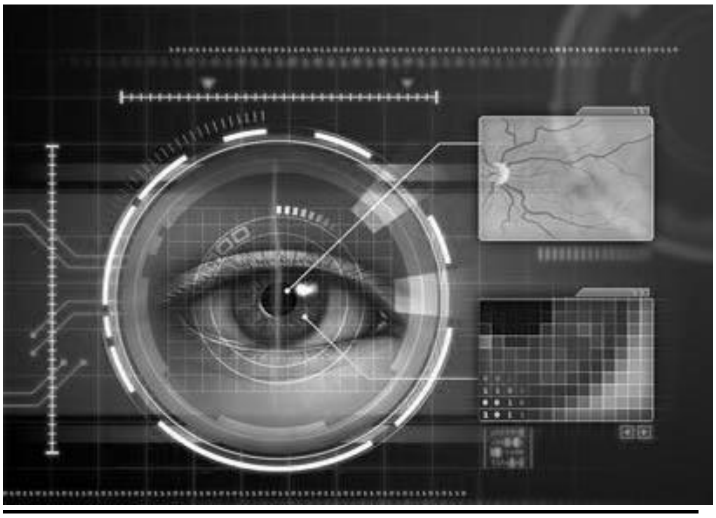


Figure 2.13. iPhone 6 with retina scan [40].

A professional operator is required for retinal scan system because light must be directed through the center of cornea. On one side retinal scan results are very accurate but on other side false rejection ration is also very high because taking a perfect image is not so easy work [41]. It is not only very expensive technology but also not very user friendly that’s why it is still rarely used. This technology can be found mostly on very high security areas where user’s acceptance is not an issue and not cost.

2.1.4. Hand Geometry Recognition

The principle behind this technique is everyone’s hand is different in shape and size than others and after a certain age they not get change. Mostly fingers length and width get measured in this technique.

Optical scanners take image of hand and then use different algorithms to calculate characteristics of hand. There are two types of scanners right now available in market 2D and 3D. 3D scanners are more sophisticated in measurements and give more accurate and reliable results [42]. Figure 2.14. presents a commonly available hand geometry scanner in market.

Figure 2.14. A hand geometry scanner [43].

Hand geometry scanners are usually very easy to use and need no special care or maintenance. Even fingers with dirt, moisture or any other thing do not affects as much on results. 90% scanners can take images only and send to computer for further processing but now in market some scanners are available with processing and storing capability. Scanners are mostly big in sizes and are used in areas where very high security is not required [44].

2.1.5. Signature Dynamics Recognition

Usually when someone talk about signature dynamics recognition it comes to the mind that it is something like comparison of two signatures, but in reality it is not like this it is measurement of how someone does his signature or how someone does write. How he makes some alphabets how many times his pen strikes with paper and with how much pressure and in which direction. It was first time introduced in 1970s [45].

Figure 2.15. Digital signature pad [47].

There are a lot of devices available in market for signature recognition. Some devices work on 2D co-ordinates and some more expensive ones work with 3D. But all devices have one big drawback and it is when someone does signature he or she cannot see what he or she is writing and mostly people when they write on these devices their signatures get different than original ones. Figure 2.15. shows a digital signature pad available in market [46].

It is also observed that many people don't make signatures every time same so it also affects the result of the system. Majority of available systems only do consideration on how someone do signature not on signature, but some systems consider both for verification. Speed is also a very important factor for verification and it is easy to forge the system even the resultant signature looks so different than real one.

2.1.6. Facial Recognition

This is most oldest and natural way of identification. All people can identify each other by looking at face. In biometric it is not eyes just camera and processor instead of the brain.

Systems normally use only gray scale images some systems use some colors but just to locate the face in the image. Lightning conditions and quality of camera plays a very important role. Some systems now even use infrared cameras. For an image a person must stand at a particular distance from camera and also face in the front of the camera. System first locates the face in the image then difference characteristics of the face are gathered [48]. Figure 2.16. is about one of the method used for facial recognition.

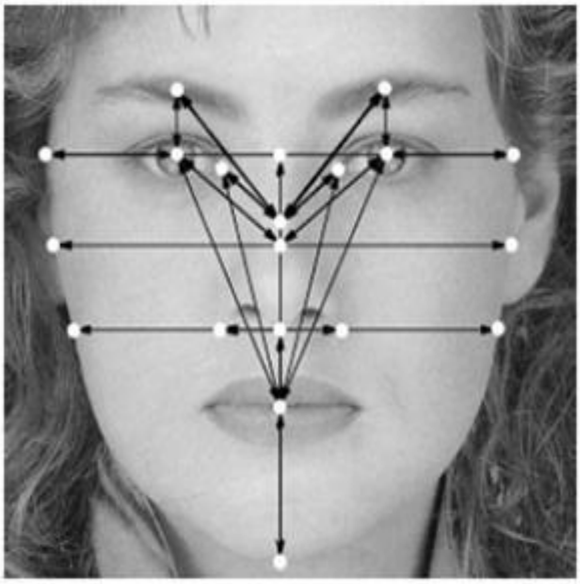


Figure 2.16. Fiducial method [49].

There are two methods which are normally used in facial recognition technique.

Facial Metrics: In this method position of eyes, nose and mouth are used also measure the distance between all these features of face to recognize someone [50].

Eigenfaces: This method is the same as method which police uses to make sketches of criminals, only difference is in this technique everything is automated and nothing is done by hand [50].

This biometric technique is not so accurate and easy. Systems need a lot of processing for images and very slightly change can cause big difference in results for example change in beard style or use of glasses need re-enrollment for authentication. Also someone can fool the system very easily with a picture if there is no other security arrangement for system. Some modern systems use two cameras to overcome this problem [48].

2.1.7. Speaker Verification and Speech Recognition

In this technique voice of someone is get stored for identification and recognition. Actually identification and recognition is two different things. In identification system tries to find who the speaker was, while in the recognition systems tries to find what someone has said [51]. Figure 2.17. gives a demonstration of process of converting spoken words in a machine readable form.

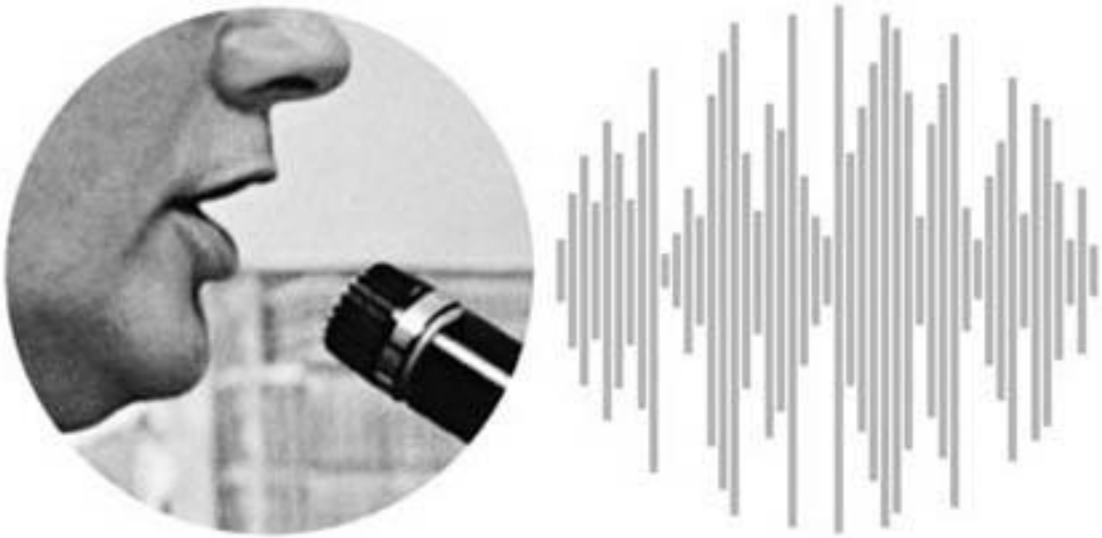


Figure 2.17. Process of converting spoken words in a machine readable form.

The biggest plus point of this technique is this it does not require a very expensive hardware. A simple microphone is enough for this even a home phone can be used for remotely storing the voice prints just need to be careful about background noise. It is also very easy to use and not a lot professional skills are required and secondly it is very user friendly. In older systems user had to pronounce some phrases in enrollment time and repeat same during the verification time but these systems were very vulnerable to attacks because if someone records someone's voice he could use later [52]. In new systems users have to pronounce several phrases for enrollment and at the time of verification system can randomly ask to pronounce a certain phrase. Emotional or any physical condition which can affect voice of someone can affect directly the performance of the system. Most of the systems are dependent of vocabulary limit but now some systems are available in markets which are independent [53].

2.1.8. Other Biometric Methods

Palmprint Verification

Palmprints are nearly the same as fingerprints just difference is they contain some additional features like texture, indents and marks which system use during comparison process [54]. Figure 2.18. is a male left hand palm print.

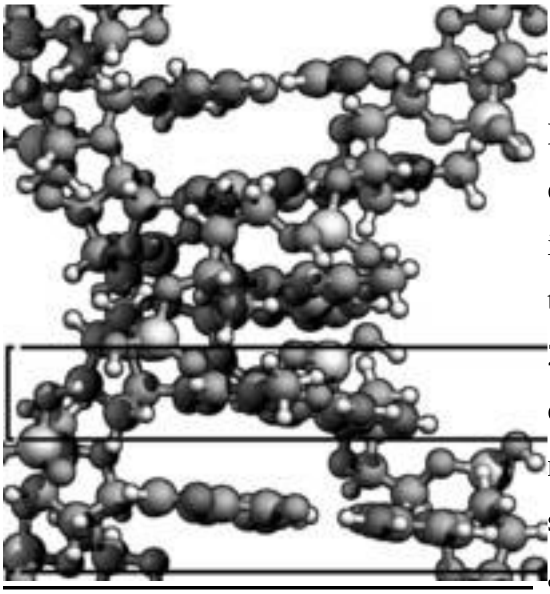
Figure 2.18. Male left palm print [55].

Hand Vein Geometry

Human all body parts have veins and can be used for identification like finger veins and retina veins but hands are always preferred because it is easy to scan them. Principle is almost same blood in vessels absorbs infrared light and creates a pattern for comparison [56]. Figure 2.19. shows a hand vein pattern.

Figure 2.19. Hand vein pattern [57].

DNA Sampling



Humans have 23 pairs of chromosomes containing DNA blueprint and chance of 2 individuals sharing the same profile is less than one in a hundred billion [58]. Figure 2.20. is a DNA structure. It can be collected from many sources: blood, hair, nails, saliva and any number of other sources that has been attached to the body at some time.

Figure 2.20. DNA structure [59].

Thermal Imaging

Thermal technology is the same as other technologies just difference is in other systems they use cameras which work in visible light and in thermal systems they use cameras which work with infrared light. Figure 2.21. shows an image of a hand captured by infrared camera.

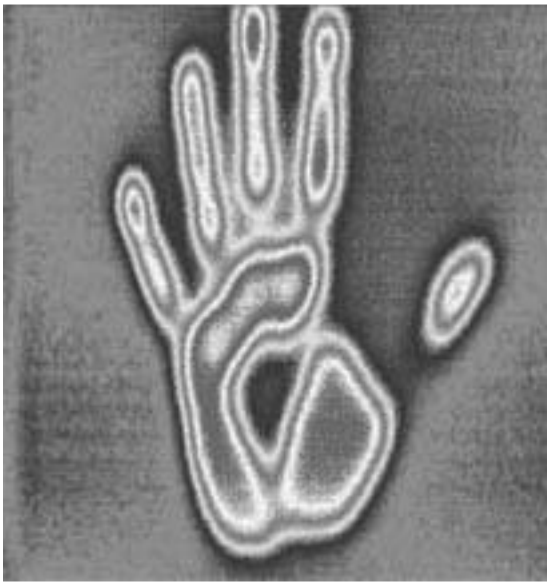


Figure 2.21. Thermal imaging technology [60].

Figure 2.22. TypeSense a software for authentication [62].

Keystroke Dynamics

In this technique system just observes how someone types what is someone habit of typing and his typing speed and use of fingers [61]. Figure 2.22. is about a typing software for authentication.

Fingernail Bed

An American company AIMS has developed a scanning system for fingernail dermal structure. . Tongue and grooves have parallel rows and system measures distance between them [63]. Figure 2.23. shows inside fingernail structure.

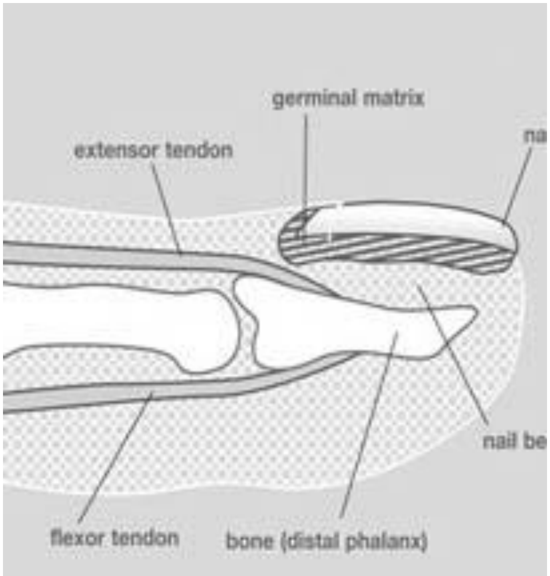


Figure 2.23. Fingernail structure [64].

Ear Shape

A French company ART Techniques has produced an ear shape verifier (Optophone) It is a telephone type set with a special camera to take images of an ear for authentication. Figure 2.24. is an ERGO smartphone with ear shape authentication option.

Figure 2.24. ERGO smartphone [65].

Body Odor

This technique is based on the principle that every human have his own unique smell. System takes samples from non-intrusive body parts like back of the hand and then analysis the chemical composition to make a template for future comparisons [66]. Figure 2.25. shows sweat on the back skin of a hand.

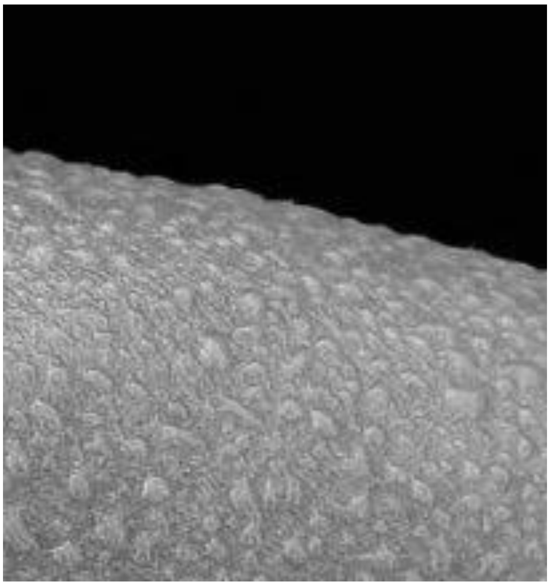


Figure 2.25. Body odor patterns [67].

3. PRACTICAL ISSUES IN BIOMETRIC TECHNOLOGY

What are the important factors which need to be considered before giving any physical or behavioral measurement to the status of biometric technique?

Universality: It is the basic factor for any biometric technique. That physical or behavioral characteristic which is going to be measured should be present in all living human beings [68].

Uniqueness: Not only that characteristic should be present in all living human beings but it also should be unique [69].

Permanence: Not only it should be unique but also it should be permanent for all life [68].

Collectability: Some body characteristics measurements are possible but very expensive, difficult and time consuming. An ideal system is that who give better result in less time and with less efforts and cost [69].

Performance: It is very important factor. Accuracy level for that characteristic should be achievable to at least should be possible to achieve in reality not just theoretical approach.

Acceptability: Technique should be like this that user not feels any kind of fear or hesitation to use it. [69].

Circumvention: Last and one of the most important factor is this technique should be not so easy to forge or by-pass [69].

3.1 The Biometric Model

Every technique has some of its own procedures and steps but basic steps of all techniques are almost same and here are some details about them:

Acquisition: It is the first step of any biometric system. In this step system takes sample from user for further processing. Sample can be anything like image for facial recognition or blood sample for DNA test. The quality of the sample is directly proportional to the accuracy of the result. Sometime there are professionals or skilled people present at systems to help the user in acquisition step.

Master Characteristics: Image or any other kind of sample which system gets in acquisition step is mostly in raw form, it needs further processing for noise and un-useful data removal to make it able for comparison process. In this step system process the initial image by different algorithms and then store it for future use.

Storage: After processing next major step is to store the resultant sample for future comparison and in storing system must be very careful that sample data will not be stored with any additional information or with any other data which was not present in the initial sample. Mostly systems do encryption before storing so data will be safe and secure.

Mostly all procedure is fully automated one from enrollment to comparisons. But still some steps are necessary for maintaining the accuracy. Device for capturing sample for enrollment should be the same for capturing sample comparisons. Secondly making system more secure it should have some liveness tests or have an attendant who make sure that user is someone human not a 3D model of a finger or any other body part or just an image. Attendant can also help new users how to use the system because mostly new users have some hesitation about using biometric devices.

Comparison: In this step system compares the user data with the already stored data. It depends also which kind of technology are being used and what parameters are declared for comparison. Sometime system compares user data with the already stored data in the storage and sometime system compares the data with the threshold point or range which have been set for the system.

Decision: Final step of the system is decision it depends on comparison results and procedure what have been declared for decision making. Mostly it is range of threshold values if comparison results lie in that range system permits someone for authentication otherwise he gets rejected.

3.2. Cryptography and Biometrics

Question is this: Is cryptography necessary for biometric systems?
Answer is: Yes it is.

Basically there are two kinds of systems:

- Automated identification systems are mostly used by authorities to find any offender of a crime. These kind of systems are mostly more accurate and complex in working. Also they need cryptography and other security measures for protection of sensitive data.

- Access control systems are not so complicated in nature and mostly they do not have any cryptography procedure.

Indeed biometric is not a secret or not anything which can be hidden or should be hidden. Just it is necessary to be careful about storage of data that no one can get access to system data or can do any changes according to his own will.

Liveness Problem: Liveness is the biggest challenge for all biometric technologies available in the market. Difference is this some systems are easy to forge and some systems are not so easy but still there is possibility in almost all systems. 3D artificial fingers, faces and many more ways are possible. One easiest thing to cope with this problem is to have an attendant for system.

Authentication: As much user is important as much system is too for authentication. System should be trustworthy. Some image capturing devices and some systems are like that they can authenticate anyone and this is dangerous. So before installing any system it is necessary to be very careful about selection.

4. FINGERPRINT RECOGNITION

This chapter presents a brief detail about fingerprint recognition technique.

4.1. Fingerprint Details

Fingerprints have two very important features ridges and valleys. Ridges appear as black or dark lines in the image while the areas between these lines are valleys. If finger gets burn or skin gets any cut or injury when new skin recovers again pattern naturally stays the same as before [70]. The details about ridges and valleys are called minutiae. According to biometric ridges have two very important characteristics either ridges go to an end which are called termination or they split into two branches and continue which are called bifurcation. There are some other types of minutiae too which are actually combination of these two minutiae but here in this thesis it is going to be work only on these two characteristics [70]. Figure 4.26. illustrates basic types of minutiae in fingerprint images.

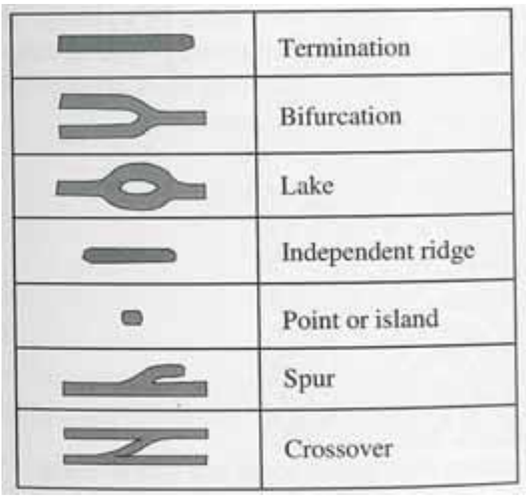


Figure 4.26. Basic types of minutiae [70].

4.2. Fingerprint Recognition Techniques

4.2.1. Minutiae-Based

There are many methods for fingerprint recognition. One method is to extract minutiae from pattern image and compare it to the previously stored data. Some systems store minutiae data as the minutiae location in the X-Y coordinates with the orientation angle and minutiae type. In this thesis same method is used. Even this method needs a lot of processing on raw image to make it able to extract minutiae. The main advantage of this method is it can even use not so high quality images as input and then process it and make it able to extract better results [71].

4.2.2. Image-Based

It is another method for fingerprint recognition. The main advantage in this method is it does not require a lot of processing on input image. Also this method gives better results on low quality input images. The input image is divided into non-overlapping square blocks of equal size and then calculates the wavelet features. The global feature vector is formed for each sub-image block and then apply matching sequence with previously stored image [72]. This is a very good option for small scale fingerprint recognition systems.

4.2.3. Ridge Feature-Based

This is best alternative method when it is too difficult to extract data from minutiae. System adds additional information for better results like location of sweat pores along the ridges. This additional information undoubtedly increases the accuracy and robustness of a system [70].

4.3. Fingerprint Recognition System

All the results depend on the minutiae detection and its accuracy. And for that it is required to apply many pre-processing steps on the image for better results.

4.3.1. Image Pre-processing

In the minutiae extraction procedure there are many pre-processing steps like binarization, removal of noise and thinning. In this thesis, SFINGE software is used for input images. Figure 4.27. shows a fingerprint image which is tooken from SFINGE database for pre-processing steps.

Figure 4.27. Input image for pre-processing steps.

Binarization: Binarization is a process of converting a gray scale image into a pure black and white image. In other words it can be said that it is a process of converting different intensity values of an image to 0 and 1 range. This method will be applied on the image which is token from SFINGE online database of fingerprint images. Figure 4.28. is about the results of image binarization.

Figure 4.28. Results of image binarization.

Thinning: Thinning is second major pre-processing step and its purpose is to reduce the thickness of all ridge lines to the single pixel without disturbing the location and orientation of minutiae from the original image.

a. Block Filtering: There are seven steps in block filtering method and it is mostly commonly used method because it tries to keep the image in most original form. Table 4.1. outlines these steps with a brief description.

Table 4.1. Steps in block filtering process [73].

Step 1: ridge width reduction-reduces width of thick ridges to enable more effective block filtering.
Step 2: passage of block filter-right to left and left to right filtering attempts to preserve outer boundaries of ridges.
Step 3: removal of isolated noise-removes unsegments produced by filtering.
Step 4: scan combination-images from right to left and left to right filtering are combined into one image.
Step 5: elimation of one from two-by-two squares of black-further thins image following scan combination.
Step 6: removal of unwanted spurs-removes short line segments protruding from ridges after scan combination.
Step 7: removal of duplicate horizontal and duplicate vertical lines-removes these imperfections produced when scans are combined.

b. Central Line: This method is used in the thesis for thinning procedure. The biggest significant advantage of this method is it produces same thinned images as output regardless of rotation. It deletes all the points which lie on the outer boundaries with the width greater than 1 pixel. Figure 4.29. illustrates the results of central line thinning process.

Figure 4.29. Results of central line thinning process.

Final Noise Removal: The final step of pre-processing of the input image is noise removal. Binarization and thinning processes produce some noise in the image as a by-product which is very necessary to eliminate before the minutiae extraction phase. Figure 4.30. is about the impact of noise removal.

Figure 4.30. Impact of noise removal.

4.3.2. Minutiae Extraction

In minutiae extraction procedure system tries to locate the terminations and bifurcations in the thinned image.

Terminations

Thinned image is filtered first time only for locating the termination points. Figure 4.31. presents the resultant image with termination points inside the red colored circles.

Figure 4.31. Termination points.

Bifurcations

Same as done for termination points once again has to filter the thinned image for bifurcation points. Figure 4.32. shows the resultant image with bifurcation points inside the green colored circles.

.

Figure 4.32. Bifurcation points.

Figure 4.33. shows the termination and bifurcation points combinely in the thinned image.

Figure 4.33. Termination and bifurcation points.

As it can be seen in the Figure 4.34. that there are many minutiae points which are so close to each other and appearing as overlapping. This condition affects the results.

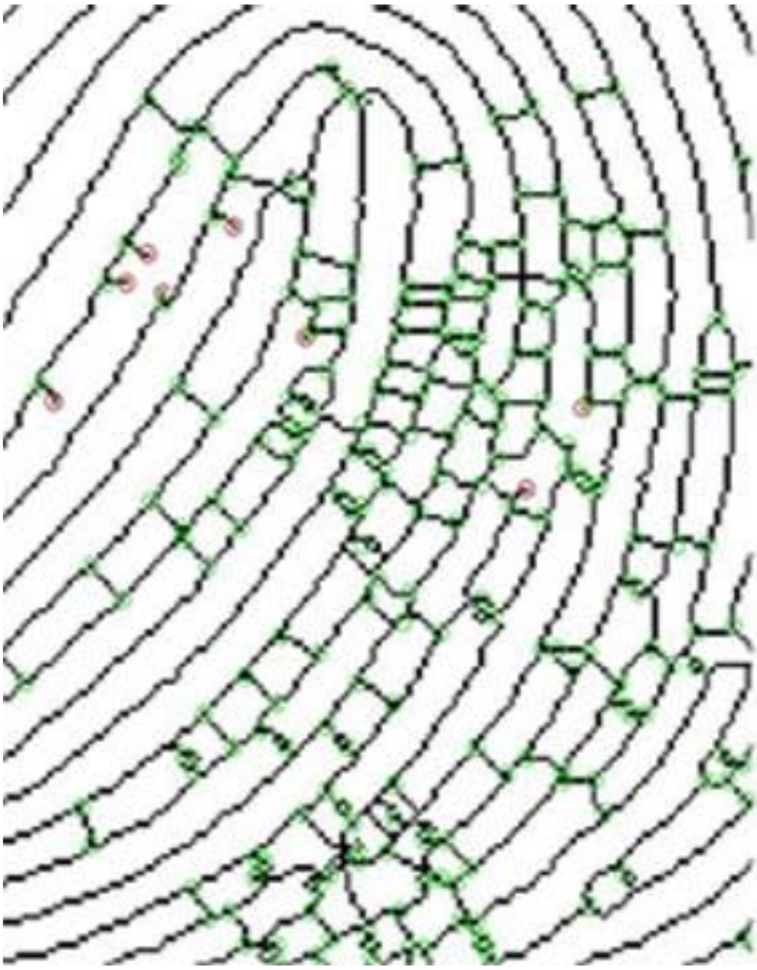


Figure 4.34. Minutiae overlapping.

It has to process the image in 3 steps to remove the overlapping minutiae.

Step 1: In first step process the image for removing the overlapping termination points and those termination points which are very close to each other. Figure 4.35. shows the resultant image after the first step of process.

Figure 4.35. Resultant image after the first step.

Step 2: In second step it has to process the image for removing the overlapping bifurcation points and those bifurcation points which are very close to each other same as step 1. Figure 4.36. presents the resultant image after the second step.

Figure 4.36. Resultant image after the second step.

Step 3: After removal of overlapping termination and bifurcation points still there are some termination and bifurcation points near to each other or overlapping to each other which need to be removed before going to start other process. Figure 4.37. shows the resultant image after first and second steps and Figure 4.38. illustrates the final image after third step.

Figure 4.37. Resultant image after the first and second steps.

Figure 4.38. Final image after third step.

After above three steps image is still not ready for final minutiae matching process. First it has to select region of interest from the image. There is not any fixed rule for selecting region of interest just it is needed to be careful about the parameters which are consider for selection of region of interest for enrollment of user and will be the same at the time of recognition.

Region of Interest: Now it has to select the region of interest from the image. Region of interest is actually any part of image which is selected0 for ease to save time and efforts rather than to process all image for results. Figure 4.39. shows the selected region of interest from the image.

Figure 4.39. Region of interest.

After selecting the region of interest now has to call the extracted minutiae in the region of interest. Figure 4.40. shows the extracted minutiae in the region of interest and Figure 4.41. is about the extracted minuate according to the first input image.

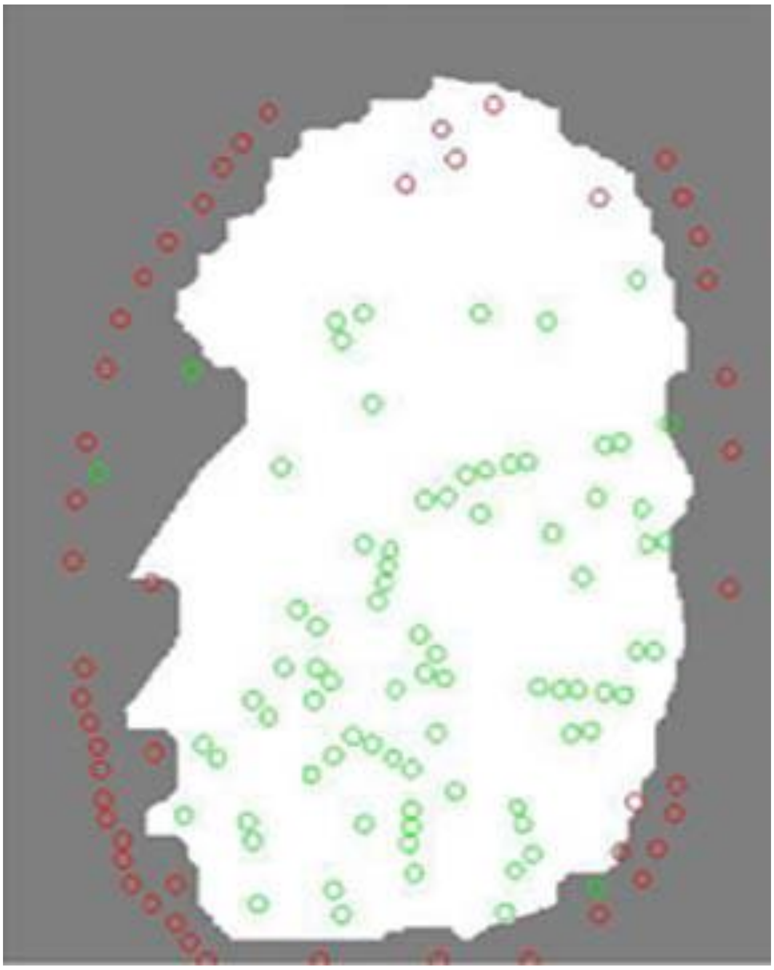


Figure 4.40. Minutiae in the region of interest.

Figure 4.41. Minutiae superimposed on original input image.

Now it has to calculate the termination angle and bifurcation angle also orientation. Termination angle is the angle between the ridge and the horizontal line while the bifurcation angle is the angle between the area and the horizontal line. Figure 4.42. illustrates termination and bifurcation angles while Figure 4.43. gives details about rules for calculating termination angles.

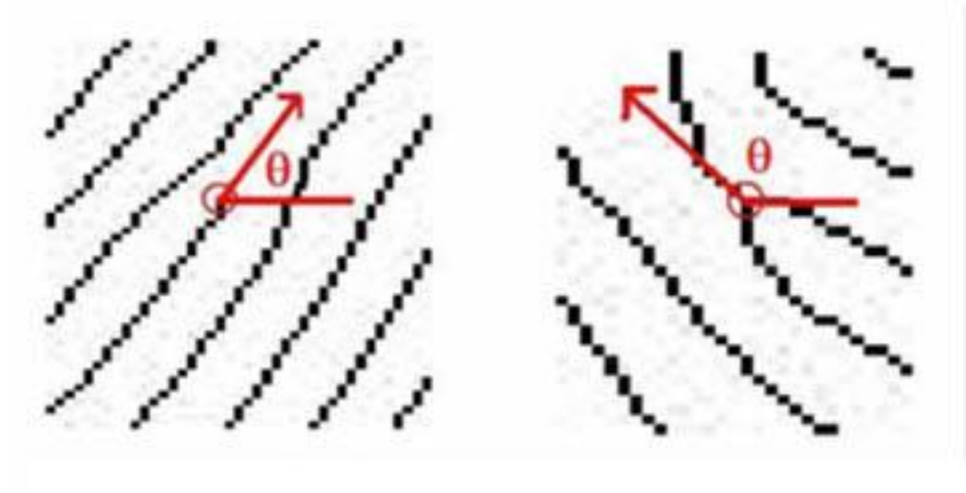


Figure 4.42. Termination and bifurcation angles [73].

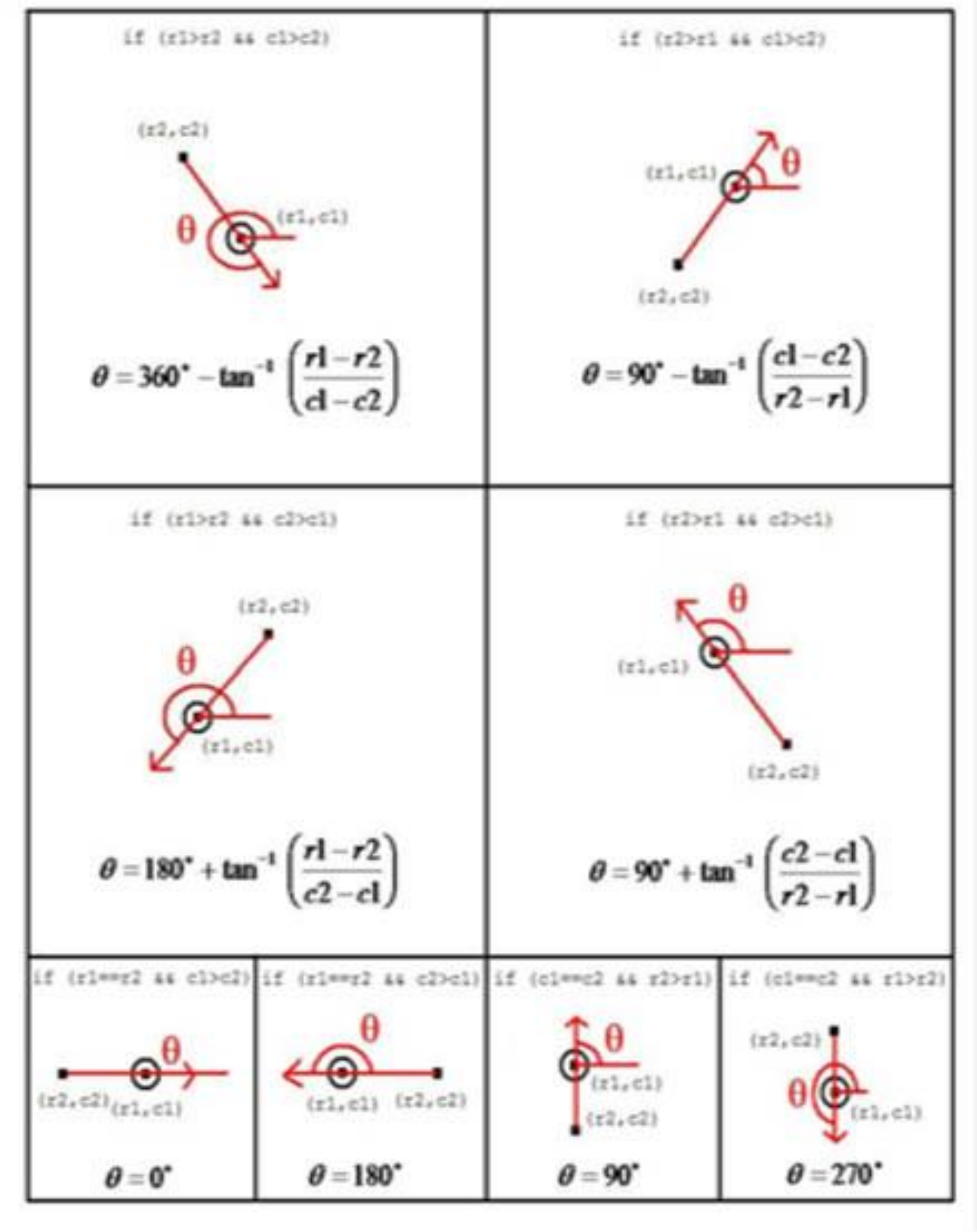


Figure 4.43. Rules for calculating termination angles [73].

Figure 4.44. presents termination points for calculating termination angles and the orientation same as Figure 4.45. shows bifurcation points for bifurcation angles and orientation.

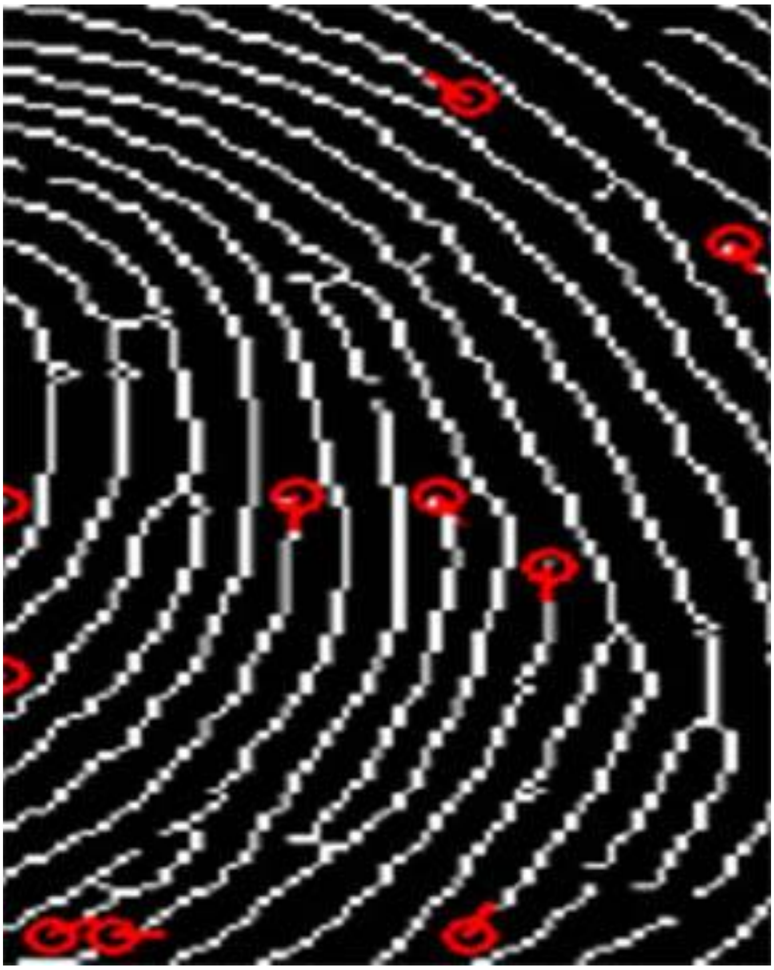


Figure 4.44. Termination points for calculating termination angles.

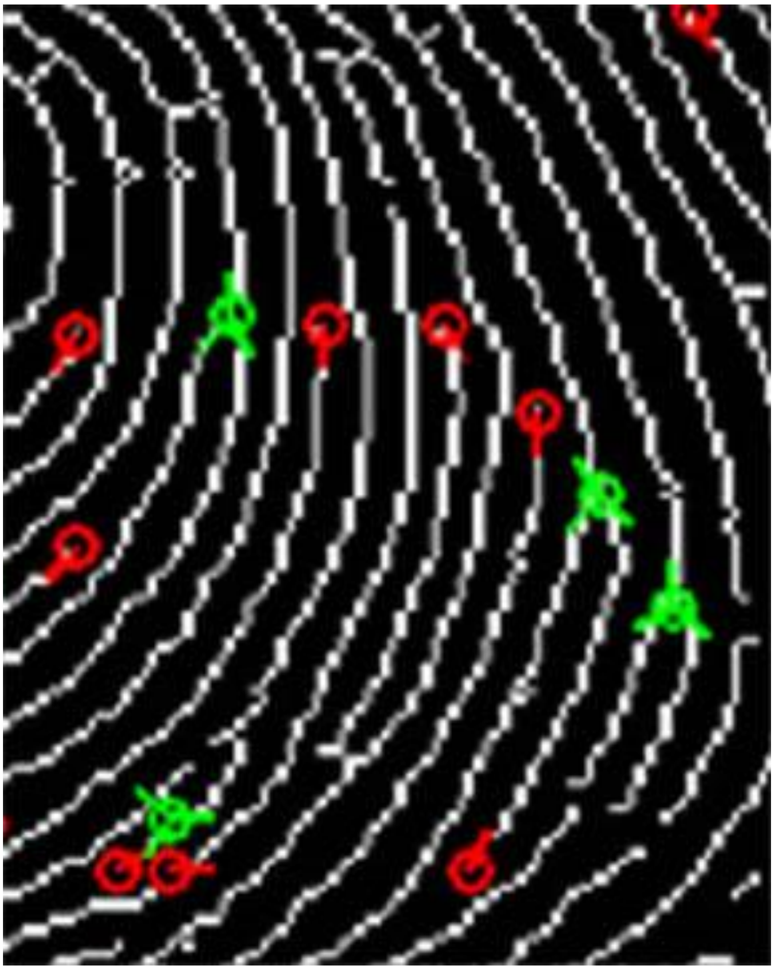


Figure 4.45. Termination and bifurcation points for their respective angles.

Minutiae data system stores in matrix form for matching process. Table 4.2. presents a matrix of minutiae data. First column of the table is row index, second is column index, third is minutiae angles while fourth is type of minutiae. 1 represents termination and 2 represents bifurcation.

Table 4.2. Matrix of minutiae data.

Row	Column	Angle	Minutiae Type
307	165	319.94	1

254	159	132.08	1
310	184	330.80	1
258	224	311.43	1
212	80	69.46	2
135	81	212.98	2
305	109	219.69	2
232	129	78.90	2

4.3.3. Minutiae Matching

In matching process it is compared input set of data with the previously stored data. Comparison starts with creating a matrix of the orientation angle Tk ($1 \leq k \leq NT$), and Im ($1 \leq m \leq NI$). Input and template data are selected as reference points for each possible combination. NT and NI are the total number of minutiae in the template and input set. k and m are the difference between the orientation angles of Tk and Im while Tk and Im are the extracted data. Process starts with selection of first minutiae point from template T1 and input I1. After processing it the system takes I2 as reference point till all combinations of Tk and Im finishes.

A matching score is calculated using total number of minutiae matched in each case. Equation 4.1. shows the formula for matching score.

$$\text{matching score} = \frac{\text{matching minutiae}}{\max(NT,NI)} \qquad \textbf{(4.1)}$$

NT and NI are the total number of minutiae in the template and input. The denominator is always the maximum value among both. By this formula, the matching score takes on a value between 0 and 1. 1 means the data matches perfectly and 0 shows when there are no matching minutiae.

4.3.4. Experimental Results

As it is written before all fingerprint images have token from SFINGE software database which is available freely online.

Experiment 01

In first experiment right and left side thumb prints of a same person is used. It is considered left side of the thumb as template while right side as input. Following data is received after performing all steps which are mentioned above.

Total number of minutiae in template = 35
Total number of minutiae in input = 32
Total number of matched minutiae = 7

All necessary data for calculating the matching score are available. Now it have to put all values in the formula.

$$\text{matching score} = \frac{\text{matching minutiae}}{\max(NT,NI)}$$

$$\text{matching score} = 7/35$$

$$= 0.2$$

Note: It is always the maximum value between template and input minutiae for denominator. In this experiment it is 35.

Experiment 02

In second experiment both left side thumb prints of a same person is used. First image of the thumb is considered as template while second as input. Following data is delivered to the system after performing all steps which are mentioned above.

Total number of minutiae in template = 35

Total number of minutiae in input = 33

Total number of matched minutiae = 30

All necessary data for calculating the matching score have received now it have to put in the formula.

$$\text{matching score} = \frac{\text{matching minutiae}}{\max(NT, NI)}$$

$$\text{matching score} = 30/35$$

$$= 0.85$$

Note: It is always the maximum value between template and input minutiae for denominator. In this experiment maximum value is 35.

Experiment 03

In third experiment both left side thumb prints of different persons are used. First person thumb image as template while second person as input are considered. Following data are the result after performing all steps.

Total number of minutiae in template = 35

Total number of minutiae in input = 34

Total number of matched minutiae = 11

After having all necessary data it is just have to put all values in the formula.

$$\text{matching score} = \frac{\text{matching minutiae}}{\max(NT, NI)}$$

$$\text{matching score} = 11/35$$

$$= 0.31$$

Note: It is always the maximum value between template and input minutiae for denominator. In this experiment maximum value is 35.

Results

These are the results of all three experiments.

Matching score of experiment 01 = 0.2 (20%)

Marching score of experiment 02 = 0.85 (85%)

Matching score of experiment 03 = 0.31 (31%)

According to US Judicial system [32] score 0.4 (40%) or more can be considered for case processing.

5. FINGER VEIN PATTERN RECOGNITION

Finger vein pattern recognition has become one of the main trends of biometrical systems in recent years. Fingerprint and finger vein pattern can be represented with the same feature as minutiae (termination and bifurcation points). The basic procedure is same the as fingerprint to extract features in a gray image. The extracted features are filtered and thinned as shown in Figure 5.46.

Figure 5.46. Finger vein pattern.

It is going to apply the same procedures for finger vein pattern too as it was applied before for fingerprint images. Binarization, thinning and noise removal as pre-processing steps. After that minutiae extraction steps these are also same. Finger vein pattern have arteries which will be considered as ridges and their end as terminations and their division into branches as bifurcations. Only difference is that a finger vein pattern has less minutiae points as compared to fingerprints as shown in Figure 5.47.

Figure 5.47. Finger vein minutiae.

As it can be seen in the Figure 5.48. that there are many minutiae points which are so close to each other and appearing as overlapping. This condition affects the results.

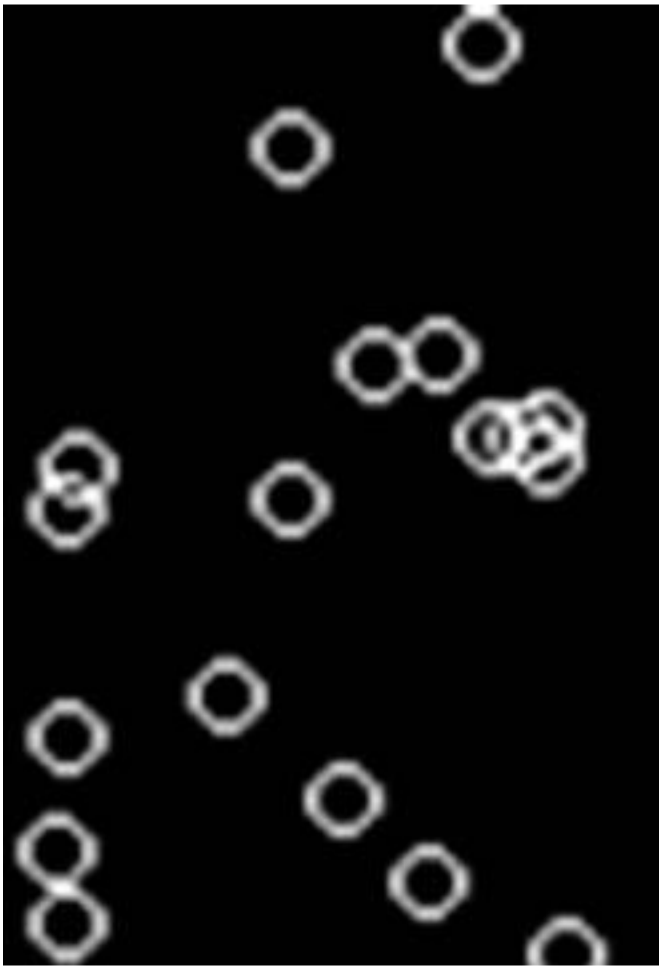


Figure 5.48. Overlapping minutiae.

5.1. Redundant Point Elimination

The accuracy of the system directly depends on the minutiae extraction. Redundant feature elimination aims at enhance the reliability while minimize the computational processing complexity. For each minutia of finger vein, neighborhood elimination removes those points that lie within a certain radius r around it. For a given minutia (x, y), points satisfy Sd as shown in Equation 5.2. will be eliminated.

$$S_d = \sqrt{(x - x_i)^2 + (y - y_i)^2} \le r \quad \textbf{(5.2)}$$

Where (xi,yi) is a minutia from a finger vein image. r is computed . After neighborhood redundant point elimination the reduced finger vein minutiae point-sets are obtained.

Minutiae data system stores in matrix form for matching process. Table 5.3. shows a matrix of minutiae data. First column of the table is row index, second is column index, third is minutiae angles while fourth is the type of minutiae. 1 represents termination and 2 represents bifurcation.

Table 5.3. Matrix of minutiae data.

Row	Column	Angle	Minutiae Type
184	301	276.54	1
81	253	319.08	1
155	307	156.67	1
119	224	213.23	1
112	180	89.78	2
135	254	245.41	2
105	238	266.15	2
132	239	179.82	2

In matching process it is compared input set of data with the previously stored data same as fingerprint. Comparison starts with creating a matrix of the orientation angle Tk (1 ≤ k ≤ NT), and Im (1 ≤ m ≤ NI). Input and template data are selected as reference points for each possible combination. NT and NI are the total number of minutiae in the template and input set. k and m are the difference between the orientation angles of Tk and Im while Tk and Im are the extracted data. Process starts with selection of first minutiae point from template T1 and input I1. After processing it system takes I2 as reference point till all combinations of Tk and Im finishes.

A matching score formula for finger vein is the same as it is used for fingerprint matching.

5.2. Experimental Results

There is no image database available for finger vein pattern as SFINGE was used previously to develop fingerprints free of sensor noise. So this time images from internet free available are used.

Experiment 01

In first experiment right and left hand side finger veins patterns of a same person is used. Left side finger as template while right side as input are considered. Following data is delivered to the system after performing all steps which are mentioned above.

Total number of minutiae in template = 15

Total number of minutiae in input = 17

Total number of matched minutiae = 5

All necessary data for calculating the matching score have received now it have to put in the formula.

$$\text{matching score} = \frac{\text{matching minutiae}}{\max(NT,NI)}$$

$$\text{matching score} = 5/17$$

$$= 0.29$$

Note: It is always the maximum value between template and input minutiae for denominator. In this experiment maximum value is 17.

Experiment 02

In second experiment both left side finger vein patterns of a same finger and same person are used. First image as template while second as input are considered. Following data are the result after performing all steps.

Total number of minutiae in template = 17

Total number of minutiae in input = 17

Total number of matched minutiae = 17

After having all necessary data it is just have to put all values in the formula.

$$\text{matching score} = \frac{\text{matching minutiae}}{\max(NT,NI)}$$

$$\text{matching score} = 17/17$$

$$= 1.0$$

Note: It is always the maximum value between template and input minutiae for denominator. In this experiment maximum value is 17.

Experiment 03

In third experiment both left side finger vein patterns of different persons are used. First person image as template while second person as input are considered. Following data is received after performing all steps which are mentioned above.

Total number of minutiae in template = 17

Total number of minutiae in input = 14

Total number of matched minutiae = 4

All necessary data for calculating the matching score are available. Now it have to put all values in the formula.

$$\text{matching score} = \frac{\text{matching minutiae}}{\max(NT,NI)}$$

$$\text{matching score} = 4/17$$

$$= 0.23$$

Note: It is always the maximum value between template and input minutiae for denominator. In this experiment it is 17.

Results

These are results of all three experiments.

Matching score of experiment 01 = 0.29 (29%)

Marching score of experiment 02 = 1.0 (100%)

Matching score of experiment 03 = 0.23 (23%)

There is not standard for finger vein pattern matching scores as it was 0.4 for fingerprints for US Judicial system [32].

6. MATCHING BASED ON THE FUSION

Matching is the process of comparing concatenated set of points from the query samples with the reference template. Fusion of fingerprint and finger vein is at matching score level. Fingerprint recognition is responsible for matching the input fingerprint against the templates stored in the database to obtain scores for matching. Vein recognition is responsible for the same. Score level fusion integrates matching scores which are from fingerprint and finger vein recognition to new scores which make final decision as shown in Equation 6.3.

$$\text{Final matching score} = \frac{\text{matching fingerprint minutiae} + \text{matching finger vein pattern minutiae}}{\max(NT,NI)(\text{fingerprint}) + \max(NT,NI)(\text{finger vein pattern})} \tag{6.3}$$

Matching Score

For calculating the final matching score, it is going to use values from experiment 02 of fingerprint and experiment 02 of finger vein pattern.

Note: All those matching scores whose values will be lesser than 0.4 will be rejected before final matching procedure.

Fingerprints

Total number of fingerprint minutiae in template = 35

Total number of fingerprint minutiae in input = 33

Total number of matched fingerprint minutiae = 30

Finger vein patterns

Total number of finger vein pattern minutiae in template = 17

Total number of finger vein pattern minutiae in input = 17

Total number of matched finger vein pattern minutiae = 17

Final matching score =

30 + 17

35 + 17

= .90

90%

7. CONCLUSIONS AND RECOMMENDATIONS

The performance of any biometric system purely depends on the precision of extracted minutiae. The multi-model biometric system which is proposed in this thesis is actually combination of fingerprint and finger vein pattern recognition systems. Both individual systems depend on quality of input images. At some extent it can be processed the image to find better accuracy levels but still very poor quality images and especially high noise ratio effects badly the results.

In this thesis the most important point is that the same processing steps are used for both different kind of biometric traits in this way it can save processing capability secondly system does not need a lot of storage for processing procedures. Proposed system performed well during the experimental tests but still there are a lot of points which need further improvements like in minutiae extraction phase termination and bifurcation points were only under considerations. For achieving higher accuracy level it can also be considered sweat pores which lie along the ridges and these pores orientation is also unique from person to person. Secondly in pre-processing steps noise removal also need more better performance because noise in input image can create false minutiae in the extraction phase and these false minutiae directly effect on the matching scores. In the end of thesis it is an answer of this question which comes in mind why it was selected fingerprint and finger vein pattern fusion? There are many different biometric techniques available now days some gives very accurate results like iris and retina scan techniques but their scanners are not only very expensive also users feel hesitation to use it. In speaker recognition systems they always need a very sound proof environment where no noise can get add in user voice second emotional condition or any health issue can affect directly on user voice quality. Hand geometry and signature dynamics results are often not so accurate and cannot be trusted always. In alone fingerprint technique is not so secure any 3D model of a finger can get access so its combination with finger vein pattern adds better security level because for finger vein pattern finger must has blood in veins to produce image and any 3D model cannot work. And other reason was this both fingerprints and finger vein patterns have the same kind of features which let us use the same processing steps for both and save processing and storage capacity of the system with time.

8. REFERENCES

[1] A.K. Jain, A. Ross. Multibiometric systems. In Commun. ACM 47 (1) (special issue on multimodal interfaces), pages 34–40, 2004.

[2] L. Hong, A.K. Jain, S. Pankanti. Can multibiometrics improve performance? In Proceedings of IEEE Workshop on Automatic Identification Advanced Technologies, NJ, USA, pages 59–64, 1999.

[3] A. Ross, A.K. Jain, J. A. Reisman. A Hybrid Fingerprint Matcher. In Pattern Recognition 36(7), pages 1661-1673, 2003.

[4] Akkan Gülşah, Sayısal Kanıt İşlemlerinin Analizi, Yüksek Lisans Tezi, Fırat Üniversitesi Fen Bilimleri Enstitüsü, supervised by Prof. Dr. Asaf Varol, 2013, http://www.asafvarol.com/en/index.php. Accessed February 21, 2014.

[5] Kutukız Mustafa, Bir Uzman Sistem Yardımıyla Kanser Hücrelerinin Belirlenmesi , Yüksek Lisans Tezi, Fırat Üniversitesi Fen Bilimleri Enstitüsü, supervised by Prof. Dr. Asaf Varol, 2014, http://www.asafvarol.com/en/index.php. Accessed February 25, 2014.

[6] Şan Songül, Parmak Damar Tanıma Teknolojisi, Yüksek Lisans Tezi, Fırat Üniversitesi Fen Bilimleri Enstitüsü, supervised by Prof. Dr. Asaf Varol, 2013, http://www.asafvarol.com/en/index.php. Accessed February 26, 2014.

[7] Webpage of Prof. Dr. Asaf VAROL. http://www.asafvarol.com/en/index.php

[8] Margot, Pierre and Quinche, Nicolas, "Coulier, Paul-Jean (1824-1890): A Precursor in the History of Fingermark Detection and Their Potential Use for Identifying Their Source (1863)", Journal of forensic identification, 60 (2), March-April 2010, pp. 129-134, (published by the International Association for Identification).

[9] Fingerprints on a piece of clay (From: WORLD UNIQUE IDENTIFICATION NUMBER, http://worlduin.homestead.com/HISTORY-OF FINGERPRINT.html/). Accessed February 21, 2014.

[10] Pierre Piazza. Alphonse Bertillon and the Identification of Persons (1880-1914), Criminocorpus [En ligne] publiée le 4 avril 2014, consultée le 1 juin 2014. URL : https://criminocorpus.org/expositions/16875/. Accessed February 21, 2014.

[11] Bertillon system of measuring different body parts for identification (From: Alphonse Bertillon, http://en.wikipedia.org/wiki/Alphonse_Bertillon/). Accessed February 21, 2014.

[12] Digital edition of “Fingerprints” by Francis Galton, 1892, (McMillan & Co., London and New York). This version has been enhanced and indexed for rapid search by Biometric Bits, and can be found at http://www.BiometricBits.htm/. Accessed February 21, 2014.

[13] Rodriguez, J. South Atlantic Crossing: Fingerprints, Science, and the State in Turn-of-the-Century Argentina. The American Historical Review, April 2004 [Online], 109.2, http://www.historycooperative.org/journals/ahr/109.2/rodriguez.html/. Accessed February 21, 2014.

[14] Tewari, RK; Ravikumar, KV (2000). "History and development of forensic science in India". J. Postgrad Med (46): 303–308.

[15] Sir Edward Henry system (From: http://www.thamespilot.org.uk/asset_arena/image/2000/sl/sl/sl-sl-1526_herschelfprint-i-01-000.jpg/). Accessed February 21, 2014.

[16] Ashbaugh, David R. "Ridgeology". Royal Canadian Mounted Police, can be found at http://onin.com/fp/ridgeology.pdf. Accessed February 21, 2014.

[17] Criminal Justice Information Services, Federal Bureau of Investigation. CJIS Informational Letter; U.S. Department of Justice, U.S. Government Printing Office: Washington, DC, August 20, 1999.

[18] K. Asai, Y. Hoshino and K. Kiji, “Automatic fingerprint identification by minutia-network feature - Feature extraction process,” Transactions of IEICE D-II, J72-D-II, 5, pp.724-732, May 1989.

[19] Automatic fingerprint identification system (From: http://oreilly.com/catalog/dbnationtp/chapter/dn_0301.gif/). Accessed February 21, 2014.

[20] L. O’Gorman, “Fingerprint Verification,” in Biometrics: Personal Identification in Networked Society, pp.43-64, Kluwer Academic Publishers, 1999.

[21] L. O’Gorman, An overview of commercial biometric systems, Workshop on Automatic Identi cation Advanced Technologies, Long Island, NY, 1997, pp. 23–26.

[22] Optical fingerprint reader (From: SAFRAN Morpho, http://www.morpho.com/identification/secure-biometric-access/fingerprint-sensors/?lang=en/). Accessed February 23, 2014.

[23] STMicroelectronics image division products, 2000, http://www.vvl.co.uk/products/image_sensors/. Accessed February 23, 2014.

[24] S. Shigematsu, H. Morimura, Y. Tanabe, K. Machida, A Single-chip fingerprint sensor andidentier, IEEE J. Solid-State Circuits 34 (12) (1999) 1852–1859.

[25] S. Jung, A Low-power andhigh-performance CMOS fingerprint sensing andencoding architecture, IEEE J. Solid-State Circuits 34 (7) (1999) 978–984.

[26] Active capacitance fingerprint reader (From: P6500 Fingerprint Device, http://www.zvetcobiometrics.com/Products/P6500/features.php/). Accessed February 23, 2014.

[27] W. Bicz, D. Banasiak, P. Bruciak, Z. Gumienny, S. Gumuli_ski, D. Kosz, A. Krysiak, W. Kuczy_ski, M. Pluta and G. Rabiej "Fingerprint Structure Imaging Based on an Ultrasound Camera." 1997. [Online]. Available: http://www.optel.com.pl/article/eng. Accessed February 23, 2014.

[28] Schematic of ultrasound scan (From: http://www.jaypeetex.com/products/Biometrics/Fingerprints/WhyUltraSound.htm/). Accessed February 23, 2014.

[29] 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 Workshop on Circuits Systems and Signal Processing, pages 205–213, 2000.

[30] A. K. Jain, S. Pankanti, and A. Ross, "Fingerprint Matching: Data Acquisition and Performance Evaluation," March 1999. [Online]. Available: http://www.ese.msu.edu/publications/ techITPIMSU-CPS-99-14-ps-4. Accessed February 23, 2014.

[31] Three basic fingerprint patterns (From: Forensic Biology, http://www.bxscience.edu/publications/forensics/articles/fingerprinting/r-fing01.htm/). Accessed February 23, 2014.

[32] S. Pankanti, S. Prabhakar, and A. K. Jain. On the Individuality of Fingerprints. IEEE Transactions on Pattern Analysis and Machine Intelligence, 24(8):1010–1025, 2002.

[33] Ridge characteristics (From: Forensic Biology, http://www.bxscience.edu/publications/forensics/articles/fingerprinting/r-fing01.htm/). Accessed February 23, 2014.

[34] N. K. Ratha, K. Karu, S. Chen, and A. K. Jain. A Real-Time Matching System for Large Fingerprint Databases. IEEE Transactions on Pattern Analysis and Machine Intelligence, 18(8):799–813, 1996.

[35] Probing the uniqueness and randomness of IrisCodes: Results from 200 billion iris pair comparisons." Proceedings of the IEEE, vol. 94 (11), 2006, pp. 1927-1935.

[36] J. Daugman. How Iris Recognition Works. Proceedings of 2002 International Conference on Image Processing, Vol. 1, 2002. Available at http://www.ncits.org/tc_home/m1htm/docs/m1020044.pdf. Accessed February 23, 2014.

[37] Illustration of iris recognition method (From: BBC NEWS In Depth, http://news.bbc.co.uk/2/shared/spl/hi/guides/456900/456993/html/nn3page1.stm/). Accessed February 23, 2014.

[38] Y. Zhu, T. Tan, Y. Wang: Biometric Personal Identification Based on Iris Patterns. Proceedings of ICPR, International Conference on Pattern Recognition Vol. II (2000) 805-808.

[39] H. Borgen, P. Bours, and S.D. Wolthusen. Visible-spectrum biometric retina recognition. Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP ’08 International Conference on, pages 1056–1062, Aug. 2008.

[40] iPhone 6 with retina scan (From: IPHONE 6 JAILBREAK, http://www.iphone6jailbreak.net/iphone-6-with-retina-scan-a-k-a-eye-id-concept.html/). Accessed February 23, 2014.

[41] A. Can, C.V. Stewart, B. Roysam, and H.L. Tanenbaum. A feature-based, robust, hierarchical algorithm for registering pairs of images of the curved human retina. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 24(3):347–364, Mar 2002.

[42] Sanchez-Reillo, R. Biometric identification through hand geometry measurements. IEEE Transactions on Pattern Analysis and Machine Intelligence. ISSN: 0162-8828. Washington, 2000.

[43] A hand geometry scanner (From: Indian Point Energy Center, http://www.safesecurevital.com/about-us/photo-gallery.html/). Accessed February 27, 2014.

[44] Jain, A., Ross, A. A prototype hand geometry-based verification system. In Proceedings of 2nd Int. Conference on Audio- and Video based Biometric Person Authentication. Washington (USA), 1999.

[45] Gupta, G., A. McCabe, “A Review of Dynamic Handwritten Signature Verification”, http://www.cs.jcu.edu.au/~alan/Work/HSV-Lit_rev.html/ James Cook University, September 1997. Accessed February 27, 2014.

[46] Griess, F. D., “Online Signature Verification”, Project Report, http://www.cse.msu.edu/publications/tech/TR/MSU-CSE-00-15.ps/ Michigan State University, May 2000. Accessed February 27, 2014.

[47] Digital signature pad (From: Blog for Computer & Gadget Tech Fans, http://www.cpureview.com/choosing-the-right-signature-pad-for-electronic-signatures-44899.html/). Accessed February 27, 2014.

[48] P. Melin and O. Castillo, "Human Recognition using Face, Fingerprint and Voice," in Hybrid Intelligent Systems for Pattern Recognition Using Soft Computing, Vol.172, Studies in Fuzziness and Soft Computing: Springer Berlin / Heidelberg, 2005, pp.241-256.

[49] Fiducial method (From: Culture And Facial Recognition, http://www.mbpgsa.ca/mbpblog/2010/02/culture-and-facial-recognition-more-than-meets-the-eye/). Accessed February 27, 2014.

[50] V.I. Belhumeur, J.P. Hespanha, and D.J. Kriegman. Eigenfaces vs. sherfaces: Recognition using class specific linear projection. IEEE Transactions on Pattern Analysis and Machine Intel ligence, PAMI-19(7):711-720, July 1997.

[51] J. Baker, L. Deng, J. Glass, S. Khudanpur, C.-H. Lee, N. Morgan, and D. O’Shgughnessy, “Research developments and directions in speech recognition and understanding, part i,” IEEE Signal Process. Mag., vol. 26, no. 3, pp. 75–80, 2009.

[52] L. R. Bahl, P. V. de Souza, P. S. Gopalakrishnan, D. Nahamoo, and M. A. Picheny, “Robust methods for using context-dependent features and models in a continuous speech recognizer,” in Proceedings of ICASSP, pp. 533–536, Adelaide, 1994.

[53] X. Aubert and H. Ney, “Large vocabulary continuous speech recognition using word graphs,” in Proceedings of ICASSP, vol. 1, pp. 49–52, Detroit, 1995.

[54] X. Wu, D. Zhang, and K. Wang, Palm line extraction and matching for personal authentication. IEEE Transactions on Systems, Man, and Cybernetics, 2006. 36: p. 978-987.

[55] Male left palm print (From: Palmprint-Based Biometric Personal Identification, http://www.advancedsourcecode.com/palmid.asp/). Accessed March 3, 2014.

[56] X. Wu, D. Zhang, and K. Wang, Palm line extraction and matching for personal authentication. IEEE Transactions on Systems, Man, and Cybernetics, 2006. 36: p. 978-987.

[57] Hand vein pattern (From: Creating Identities for all, http://www.identium.in/Palm%20vein.html/). Accessed March 3, 2014.

[58] Hashiyada Masaki. Development of biometric DNA ink for Authentication Security. Tohoky Journal of Exp. Med., 2004, 204(2): 109-117.

[59] DNA structure (From: Wikipedia, http://en.wikipedia.org/wiki/File:DNA_Structure+Key+Labelled.pn_NoBB.png/). Accessed March 3, 2014.

[60] Thermal imaging technology (From: Thermal Imaging Technology for Video Surveillance, http://www.2mcctv.com/blog/2012_10_16-thermal-imaging-technology-video-surveillance/). Accessed March 3, 2014.

[61] Bleha, C. Slivinsky, B. Hussein, Computer-access security systems using keystroke dynamics, IEEE Trans. Pattern Anal. Mach. Intell. PAMI-12 (12) (1990) 1217–1222.

[62] TypeSense a software for authentication (From: deepnet security, http://www.deepnetsecurity.com/authenticators/biometrics/typesense/). Accessed March 3, 2014.

[63] J. L. Wayman, A. K. Jain, D. Maltoni, and D. Maio, Eds., “Biometric Systems: Technology, Design and Performance Evaluation”, New York: Springer Verlag, 2005.

[64] Fingernail structure (From: Anatomy 5203, http://classconnection.s3.amazonaws.com/67/flashcards/780067/png/fs1328746283928.png/). Accessed March 3, 2014.

[65] ERGO smartphone (From: Biometric Security: The Future of Keeping Your Smartphone Safe?, http://community.giffgaff.com/t5/Blog/Biometric-Security-The-Future-of-Keeping-Your-Smartphone-Safe/ba-p/12098684/). Accessed March 3, 2014.

[66] Akutsu, T.; Sekiguchi, K.; Ohmori, T.; Sakurada, K. Individual Comparisons of the Levels of (E)-3-Methyl-2-Hexenoic Acid, an Axillary Odor–Related Compound, in Japanese. Chem. Senses 2006, 31, 557–563.

[67] Body odor patterns (From: Body Scent Biometric ID Sensors, http://www.security-technologynews.com/news/body-scent-biometric-id-sensors-announced.html/). Accessed March 3, 2014.

[68] R. Brunelli and D. Falavigna, "Person Identification Using Multiple Cues", IEEE Trans. PAMI, vol. 17, no. 10, pp. 955-966, 1995.

[69] J. Kittler, M. Hatef, R.P.W. Duin, and J. Matas, "On Combining Classifiers", IEEE Trans. PAMI, vol. 20, no. 3, pp. 226-239, 1998.

[70] Maltoni, D., Maio, D., Jain, A.K., & Prabhakar, S. (2003). Handbook of fingerprint recognition. New York: Springer.

[71] Jain, A.K., Prabhakar, S., Hong, L., & Pankanti, S. (2000). Filterbank-based fingerprint matching. IEEE Transactions on Image Processing, 9, 846-859.

[72] Tico, M., Immonen, E., Rämö, P., Kuosmanen, P., & Saarinen, J. (2001). Fingerprint recognition using wavelet features. IEEE International Symposium on Circuits and Systems, 2, 21-24.

[73] From: Graig T. Diefenderfer (June 2006). Postgraduate thesis titled Fingerprint Recognition. Naval Postgraduate School Monterey, CA 93943-5000, USA.

CURRICULUM VITAE

He was born on September 3rd, 1983 in Karachi Pakistan. He completed his bachelor's degree program in Electronics Engineering from Sir Syed University of Engineering and Technology in August 2008. He worked for Sir Syed University of Engineering and Technology as Research Assistant for four years before going to begin his master's degree in September 2012.