

Jaypee University of Information Technology
Waknaghat, Distt. Solan (H.P.)

Learning Resource Center

CLASS NUM:

BOOK NUM.:

ACCESSION NO.: *SP09114 / SP0913108*

This book was issued is overdue due on the date stamped below. If the book is kept over due, a fine will be charged as per the library rules.

Due Date	Due Date	Due Date

WIRELESS BIOMETRIC FINGERPRINT ATTENDANCE SYSTEM

Project Report submitted in partial fulfillment of the requirement for
the degree of

Bachelor of Technology

in

Electronics and Communication Engineering

under the Supervision of

Mr. Tapan Jain

By

Kapil Sachdev – 091093

Akshun Bharat – 091096

Anchal Pundir - 091099



Jaypee University of Information and Technology

Waknaghat, Solan – 173234, Himachal Pradesh





JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY

Waknaghat, P.O. Domehar Bani, Teh. Kandaghat,

Distt. Solan -173234 (H.P.)

Phone: 01792-245367 - 69

Fax: 01792-245362

Certificate

This is to certify that the thesis entitles, “**Wireless Biometric Fingerprint Attendance System**”, submitted by **Kapil Sachdev, Akshun Bharat and Anchal Pundir** in partial fulfillment for the award of Degree of Bachelor of Technology in Electronics and Communication engineering to Jaypee University of Information Technology, Waknaghat, Solan has been carried out under my supervision.

This work has not been submitted partially or fully to any other university or institute for the award of this or any other degree.

Date: 29.5.13


Mr. Tapan Kumar Jain

Department of Electronics and Communication Engineering

Jaypee University of Information Technology



JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY

Waknaghat, P.O. Domehar Bani, Teh. Kandaghat,

Distt. Solan –173234 (H.P.)

Phone: 01792-245367 - 69

Fax: 01792-245362

DECLARATION

I hereby declare that the work reported in Degree of Bachelor of Technology in Electronics and Communication engineering thesis entitled “**WIRELESS BIOMETRIC FINGERPRINT ATTENDANCE SYSTEM**” submitted by “Mr. Kapil Sachdev, Mr. Akshun Bharat and Ms. Anchal Pundir” at Jaypee University of Information Technology, Waknaghat, India is an authentic record of my work carried out under the supervision of “Mr. TAPAN KUMAR JAIN”. I have not submitted this work elsewhere for any other degree.

Kapil Sachdev – 091093

Akshun Bharat – 091096

Anchal Pundir – 091099

Department of Electronics and Communication Engineering

Jaypee University of Information Technology (JUIT)

Waknaghat, Solan-173234, India

ACKNOWLEDGMENT

Firstly, we would like to thank God for his grace and our parents for their motivation all through this work.

We express our gratitude and sincere thanks to **Mr. Tapan Kumar Jain** (Sr. Lecturer, ECE) for providing the opportunity to undertake the project under his able guidance. His directions and unparallel support for fetching solutions from the industry has helped us immensely in realization of the project.

The zeal to accomplish the task of formulating the project could not have been realized without the support and cooperation of the faculty members of the ECE Department. We sincerely thank **Prof. (Dr.) T.S Lamba** (Dean A&R), **Prof. (Dr.) Sunil V. Bhooshan** (HOD, ECE) and **Ms. Meenakshi Sood** (Sr. Lecturer, ECE) for their consistent support throughout the project work. We are also grateful to **Mr. Mohan** (Project Lab In charge, ECE) for his practical guidance and his continuous help regarding software details and resources.

Date:

Kapil Sachdev (091093)

Akshun Bharat (091096)

Anchal Pundir (091099)

Abstract

The goal of this project is to...

their time in lecturing...

Now how the system...

This system is a...

Giving 10 min (20%) of your time in a 55 min lecture???

Handout

A handy...

Proxy...

Proxies getting marked.....

Is that time worth giving???

Abstract

The goal of this project is to develop a complete system that will help teachers not only save their time in lectures but also prevent fake attendance.

Now how this system works???

This system is a combination of *hardware* as well as *software* aspects.

Hardware

A handy device that consists of zigbee module, fingerprint scanner with a internal memory, power supply. Scanner scans the fingerprint of the student stores it in the memory and then transmits the image.

Software

A Matlab code that will extract useful information from fingerprint called minutiae points and match them with the fingerprints in the original database.

The database will hold the fingerprints of the students segregated on the basis of various parameters

It also consists of a secondary database which will hold the images transmitted from the zigbee module.

Objective

The main objective of this project is to **DESIGN WIRELESS FINGERPRINT RECOGNITION SYSTEM** for our university that will enable us to overcome:

- ✓ Shortcomings of conventional method of marking attendance manually, giving away the time that can be put to better use.
- ✓ False attendance of friends suggested by their peers.
- ✓ Further wastage of time while uploading that attendance online.

Further our system which will analyze the attendance pattern of the student during the whole academic semester and take any necessary action for instance- sending the parents a notification, if the student falls short in the required attendance criteria.

Table of Contents

Title	Page No.
CERTIFICATE	I
DECLARATION	II
ACKNOWLEDGEMENT	III
ABSTRACT	V
OBJECTIVE	VI
CHAPTER 1: INTRODUCTION.....	1
1.1 Why biometrics?.....	1
1.2 Fingerprint.....	2
1.3 History of fingerprint.....	2
CHAPTER 2: TECHNICAL DETAILS.....	8
2.1 Components of Fingerprint.....	8
2.2 Different Patterns of Fingerprints.....	9
2.3 .DAT File.....	13
2.4 Different types of sensors.....	14
CHAPTER 3: SYSTEM ARCHITECTURE.....	17
3.1 Detailed version of the above block diagram.....	18
3.2 MATLAB.....	20
CHAPTER 4: IMAGE PROCESSING.....	21
4.1 System Level Design.....	21
4.2 Algorithm Level Design.....	21
4.3 Steps involved in fingerprint recognition algorithm.....	23
CHAPTER 5: CONNCLUSION.....	28

List of Figure

Title	Page No.
1.1 Image of Fingerprint	2
1.2 Thumb prints on clay seal	2
1.3 Handprint of Sir William James	3
1.4 Signatures of Thompson	4
1.5 Bertillon System	4
1.6 Right Thumb Impression and Signature of Juan Vucetich	5
1.7 U.S. Navy Logo	5
1.8 Aadhaar Logo	6
2.1 Ridges & Valleys	8
2.2 Core and Delta Points	8
2.3 Minutiae Points	9
2.4 Extracted Minutiae Points	9
2.5 Arch Pattern	10
2.6 Tented Arch Pattern	10
2.7 Loop Pattern	11
2.8 Whorl Pattern	11
2.9 Twinned Loop Pattern	12
2.10 Central Pocket Loop	12
2.11 Lateral Pocket Loop	12

2.12 Composite Pattern	13
2.13 Accidental Pattern	13
2.14 .DAT File	14
3.1 Basic Block Diagram	17
3.2 Detailed Block Diagram	18
3.3 Comparison between different protocols	19
4.1 System Level Design	21
4.2 Algorithm Level Design	22
4.3 Fingerprint Recognition Algorithm	23
4.4 Initial Image	24
4.5 After Histogram Equalization	24
4.6 After Fast Fourier Transform	24
4.7 After Binarization	25
4.8 Image showing Directions	25
4.9 ROI Area	25
4.10 Thinning	26
4.11 Remove H Breaks	26
4.12 Remove Spikes	26
4.13 Minutiae Extraction	27
4.14 Useful Minutiae	27
4.15 Save Image	27

CHAPTER 1: INTRODUCTION

Wireless Biometric Attendance System is a new concept of taking attendance in classrooms of schools and colleges so as to overcome the shortcomings of traditional method of taking attendance.

Following are the difficulties often faced by the teacher who is taking attendance:

- ✓ Teachers waste times in manually taking attendance, if a proxy is caught then teacher cross checks by taking attendance again. In this process more time is wasted.
- ✓ Further teachers upload attendance on net for the reference.

1.1 Why biometrics?

Biometrics, an emerging set of technologies, promises an effective solution. Biometrics accurately identifies or verifies individuals based upon each person's unique physical or behavioral characteristics. Biometrics work by unobtrusively matching patterns of live individuals in real time against enrolled records.^{[1][12]} Leading examples are biometric technologies that recognize and authenticate faces, hands, fingers, signatures, retina, and voice.

One of the world's largest fingerprint recognition systems is the integrated automated fingerprint identification system, maintained by the FBI in the US since 1999. The IAFIS currently contains fingerprints of more than 60 million persons, with corresponding demographic information, providing both latent-print search for crime scene investigation and 10-print ID for suspect identification and general population background checks.^[2]

The main reasons for the popularity of fingerprint recognition are:

1. The availability of compact and relatively inexpensive fingerprint readers.
2. Easy to use.

1.2 Fingerprint:

Fingerprint in its narrow sense is an impression left by the friction ridges of a human finger. In a wider use of the term, fingerprints are the traces of an impression from the friction ridges of any part of a human or other primate hand.^[3] A print from the foot can also leave an impression of friction ridges. A friction ridge is a raised portion of the epidermis on the digits (fingers and toes), the palm of the hand or the sole of the foot, consisting of one or more connected ridge units of friction ridge skin. These are sometimes known as "epidermal ridges" which are caused by the underlying interface between the dermal papillae of the dermis and the interpapillary (rete) pegs of the epidermis. These epidermal ridges serve to amplify vibrations triggered, for example, when fingertips brush across an uneven surface, better transmitting the signals to sensory nerves involved in fine texture perception. These ridges may also assist in gripping rough surfaces and may improve surface contact in wet conditions.^[4]

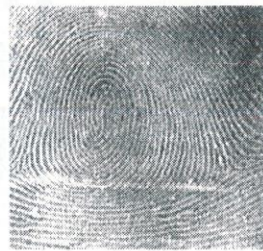


Fig: 1.1 Image of Fingerprint

1.3 History of fingerprint

In ancient Babylon, fingerprints were used on clay tablets for business transactions. In ancient China, thumb prints were found on clay seals.



Fig: 1.2 Thumb prints on clay seal

In 14th century Persia, various official government papers had fingerprints (impressions), and one government official, a doctor, observed that no two fingerprints were exactly alike. [5]

1686 - Malpighi

In 1686, Marcello Malpighi, an anatomy professor at the University of Bologna, noted fingerprint ridges, spirals and loops in his treatise.

1858 - Herschel

The English first began using fingerprints in July of 1858, when Sir William James Herschel, Chief Magistrate of the Hooghly district in Jungipoor, India, first used fingerprints on native contracts.



Fig: 1.3 Handprint of Sir William James

The idea was merely "... to frighten [him] out of all thought of repudiating his signature." The native was suitably impressed, and Herschel made a habit of requiring palm prints-- and later, simply the prints of the right Index and Middle fingers--on every contract made with the locals.

As his fingerprint collection grew, however, Herschel began to note that the inked impressions could, indeed, prove or disprove identity.^[6] While his experience with fingerprinting was admittedly limited, Sir William Herschel's private conviction that all

fingerprints were unique to the individual, as well as permanent throughout that individual's life, inspired him to expand their use.

1882 - Thompson

In 1882, Gilbert Thompson of the U.S. Geological Survey in New Mexico, used his own thumb print on a document to help prevent forgery.^[7] This is the first known use of fingerprints in the United States

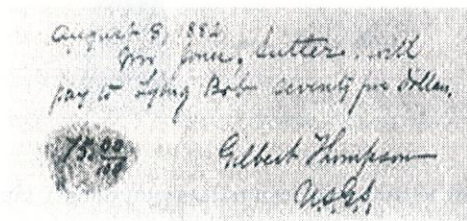


Fig: 1.4 Signature of Thompson

1882-Bertillon

Alphonse Bertillon, a Clerk in the Prefecture of Police of at Paris, France, devised a system of classification, known as Anthropometry or the Bertillon System, using measurements of parts of the body.^[8] Bertillon's system included measurements such as head length, head width, length of the middle finger, length of the left foot; and length of the forearm from the elbow to the tip of the middle finger.^[9]

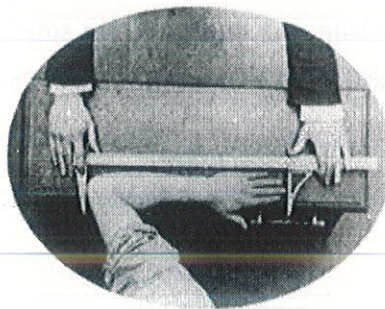


Fig: 1.5 Bertillon System

In 1888 Bertillon was made Chief of the newly created Department of Judicial Identity where he used anthropometry as the primary means of identification.

1891 - Vucetich

Juan Vucetich, an Argentine Police Official, began the first fingerprint files based on Galton pattern types. At first, Vucetich included the Bertillon System with the files.



Fig: 1.6 Right Thumb Impression and Signature of Juan Vucetich

1901 - Henry

The Fingerprint Branch at New Scotland Yard (London Metropolitan Police) was created in July 1901 using the Henry System of Fingerprint Classification.

1905:

U.S. Army begins using fingerprints.

1907:

U.S. Department of Justice forms the Bureau of Criminal Identification in Washington, DC to provide a centralized reference collection of fingerprint cards.^[10]



Fig: 1.7 U.S. Navy Logo

Two years later the U.S. Navy started, and was joined the next year by the Marine Corp. During the next 25 years more and more law enforcement agencies join in the use of fingerprints as a means of personal identification.

1924

In 1924, an act of congress established the Identification Division of the FBI. The IACP's National Bureau of Criminal Identification and the US Justice Department's Bureau of Criminal Identification consolidated to form the nucleus of the FBI fingerprint files

1977

At New Orleans, Louisiana on 1 August 1977, delegates to the 62nd Annual Conference of the International Association for Identification (IAI) voted to establish the world's first certification program for fingerprint experts.^[11] Since 1977, the IAI's Latent Print Certification Board has proficiency tested thousands of applicants, and periodically proficiency tests all IAI Certified Latent Print Examiners (CLPEs).

Contrary to claims (in the 1990s and later) that fingerprint experts profess their body of practitioners never make erroneous identifications, the Latent Print Certification program proposed, adopted, and in-force since 1977, specifically recognizes that such mistakes do sometimes occur, and must be addressed by the Latent Print Certification Board.

2013 - World's Largest Database



Fig: 1.8 Aadhaar Logo

As of March 2013, the Unique Identification Authority of India operates the world's largest fingerprint (multi-modal biometric) system, with over 200 million fingerprint, face and iris biometric records. UIAI plans to collect as many as 600 million multi-modal record by the end of 2014. India's Unique Identification project is also known as Aadhaar, a word meaning "the foundation" in several Indian languages. Aadhaar is a voluntary program, with the ambitious goal of eventually providing reliable national ID documents for most of India's 1.2 billion residents.^[13]

CHAPTER 2: TECHNICAL DETAILS

2.1 Components of Fingerprint:

- **Ridges & Valleys**
 - ✓ Light area of a fingerprint is called a **Valley**.
 - ✓ Dark area between two ridges is called a **Ridge**. ^{[14][15]}

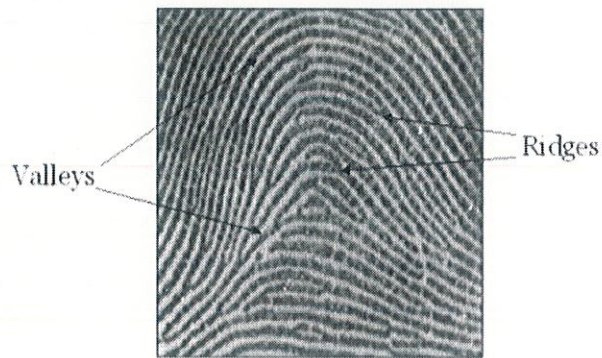


Fig: 2.1 Ridges & Valleys

- **Core and Delta Points**
 - ✓ Often known as similarity point of fingerprint.



Fig: 2.2 Core and Delta Points

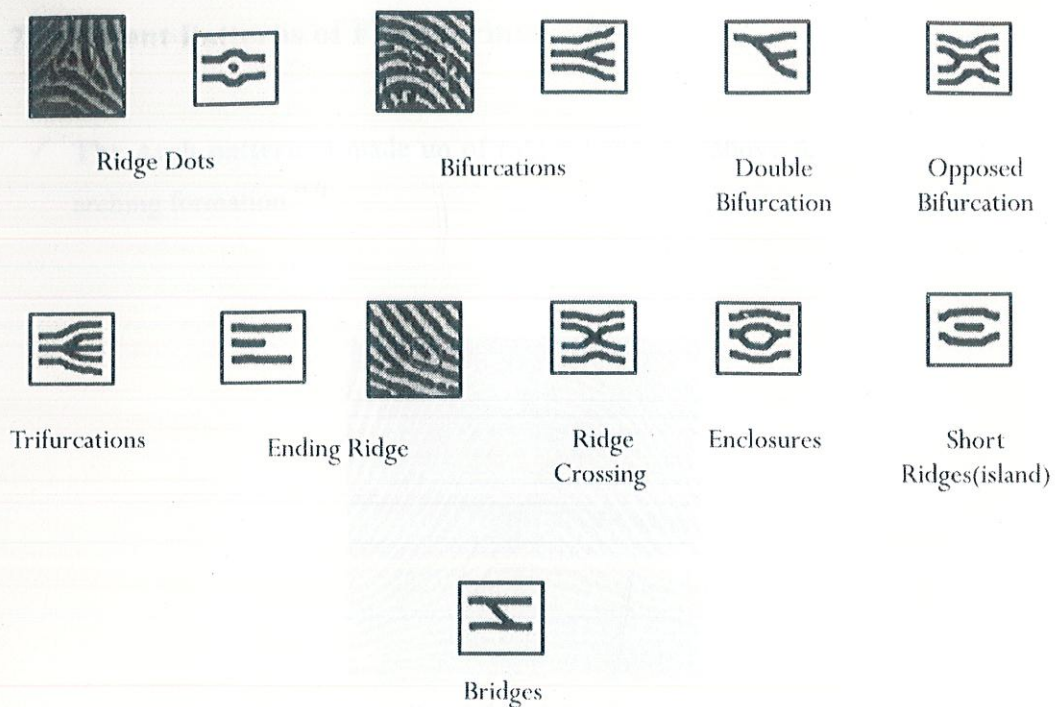


Fig: 2.3 Minutiae Points

- **Minutiae Points**
 - ✓ Minutiae points are around 50-150 and only 10 are required to maintain uniqueness.^[16]



Fig: 2.4 Extracted Minutiae Points

2.2 Different Patterns of Fingerprints:

- ✓ **The Arch pattern** is made up of ridges lying one above the other in a general arching formation.^[17]



Fig: 2.5 Arch Pattern

- ✓ **The tented arch pattern** consists of at least one upthrusting ridge, which tends to bisect superior ridges at right angles, more or less.



Fig: 2.6 Tented Arch

- **The loop pattern** consists of one or more free recurving ridges and one delta.^[18]
 - ✓ In order to distinguish between ulnar and radial loops you must:

- ✓ know from which hand the loop pattern comes from and;
- ✓ place your hand palm side down over top of the impression and determine if the recurving ridges originate from the little finger side or the thumb side.
- ✓ If the ridges flow in from the little finger side this would be an 'ulnar' loop. If the ridges flow in from the thumb side this would be a 'radial' loop.



Fig: 2.7 Loop Pattern

- ✓ **The whorl pattern** consists of one or more free recurving ridges and two points of delta. When the line of the fingerprint disc is placed on the two points of delta, it will bisect at least one of the ridges belonging to the core group.



Fig: 2.8 Whorl Pattern

- ✓ In the **twinned loop pattern**, the recurving ridges present two loop formations, separate and apart. There are two points of delta. The flows for the deltas originate from the same side of the pattern.^{[19][20]}



Fig: 2.9 Twinned Loop Pattern

- ✓ The **central pocket loop** pattern consists of one or more free recurving ridges and two points of delta. When the line of the fingerprint disc is placed on the two points of delta, it will fail to bisect any of the ridges belonging to the core group.



Fig: 2.10 Central Pocket Loop

- ✓ In the **lateral pocket loop** pattern, the recurving ridges present two loop formations, separate and apart. There are two points of delta. The flows for the deltas originate from the same side of the pattern.^[21]



Lateral Pocket Loop

Fig: 2.11

- ✓ The **composite pattern** is composed of two or more different patterns, separate and apart exclusive of the arch.



Fig: 2.12 Composite Pattern

- ✓ The **accidental pattern** will contain two points of delta. One delta will be related to a recurve and the other will be related to an up thrust.^[22]



Fig: 2.13 Accidental Pattern

2.3 .DAT File:

.DAT, a common file format (typically, generic file extension for data files by various applications with no universal format). The DAT file type is primarily associated with 'Data'. Can be just about anything: text, graphic, or general binary data. There is no specific structure for a .DAT file. You can use an editor like Edit Pad Pro to look inside a .DAT file and possibly determine its contents and relationship with a program. The DAT file format is, in fact, one of the most common file formats in existence.^{[23][24]}

In our application minutia points are extracted and that file is stored in .dat format. It contains information about the relative position of minutia points. These patterns are matched with patterns of other fingerprints.



Fig: 2.14 .DAT File

2.4 Different types of sensors

Capacitive sensors

Capacitive sensors use an array capacitor plates to image the fingerprint. Skin is conductive enough to provide a capacitive coupling with an individual capacitive element on the array. Ridges, being closer to the detector, have a higher capacitance and valleys have a lower capacitance. Some capacitive sensors apply a small voltage to the finger to enhance the signal and create better image contrast.^[25]

Optical sensors

Optical sensors use arrays of photodiode or phototransistor detectors to convert the energy in light incident on the detector into electrical charge. The sensor package usually includes a light-emitting-diode (LED) to illuminate the finger.

There are two detector types used by optical sensors, charge-coupled-devices (CCD) and CMOS based optical imagers. CCD detectors are sensitive to low light levels and are capable of making excellent greyscale pictures.^[26] However, CCD fabrication is relatively expensive and neither low-light sensitivity or greyscale imaging are required for fingerprint recognition. CMOS optical imagers are manufactured in quantity and can be made with some of the image processing steps built into the chip resulting in a lower cost.

Optical sensors for fingerprints may be affected by a number of real world factors such as stray light and surface contamination, possibly even a fingerprint impression left by a prior user. Common contaminants that deteriorate image quality include oil and dirt, scratches on the sensor surface, and condensation or ice. Some suppliers have tried to sidestep the contamination problem by directly taking a 3D image from the surface of a finger. 3D imaging technology is more hygienic but introduces a whole new set of problems and was not included in this study.

Impostor prints are more of a problem for optical sensors than it is for other detectors because it is relatively easy to present the scanner with a convincing picture of a fingerprint. Suppliers have come up with several techniques to validate a live finger. For example optical sensors can be enhanced and made more resistant to deception with Electro-Optical imaging.^[27] This works by placing a voltage across a light-emitting polymer film. When a finger is presented, the ridges provide a ground to the polymer surface creating a small current that generating light. The fingerprint valleys remain dark so a high contrast image is produced. The polymer is directly coupled to an optical detector.^[7]

Thermal sensors

Thermal sensors use the same pyro-electric material that is used in infrared cameras. When a finger is presented to the sensor, the fingerprint ridges make contact with the sensor surface and the contact temperature is measured, the valleys do not make contact and are not measured. A fingerprint image is created by the skin-temperature ridges and the ambient temperature measure for valleys.^[28]

The biggest drawback of this technique is that the temperature change is dynamic and it only takes about a tenth of a second for the sensor surface touching ridges and valleys to come to the same temperature, erasing the fingerprint image. Additionally, this technology has many of the same contamination and wear issues as other sensors. While it can operation over a wide range of temperatures, if the ambient temperature is close to

the finger surface temperature the sensor requires heating to create a temperature difference of at least 1 degree Centigrade.

RF sensors

A low radio frequency (RF) signal is applied to the user's finger and then read by the detector array, with each pixel operating like a tiny antenna. The advantage of this detector is that it reads the fingerprint from the dermal layer underneath the surface making it less susceptible to damaged or dry fingertips.^[29]

CHAPTER 3: SYSTEM ARCHITECTURE

Following is the block diagram for Wireless Biometric Fingerprint Recognition System.

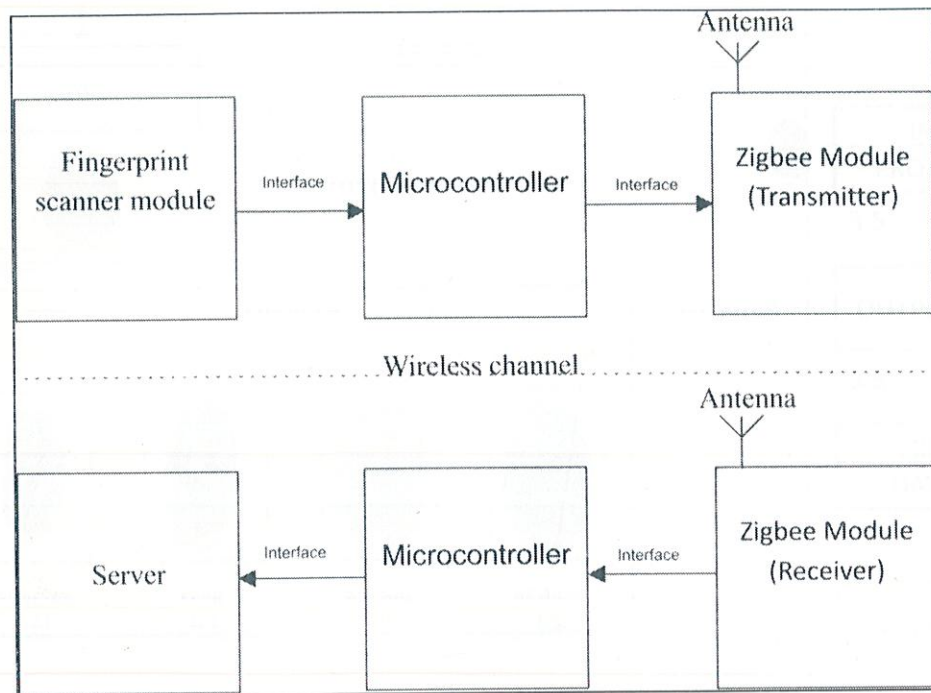


Fig: 3.1 Basic Block Diagram

Fingerprint is scanned through fingerprint scanner module. Then the image is sent through the microcontroller in the form of serial bits to the transmitter i.e. a ZigBee module, which sends the bits to the receiver ZigBee, then through the microcontroller it goes to the server where the attendance is updated.^[30]

3.1 Detailed version of the above block diagram

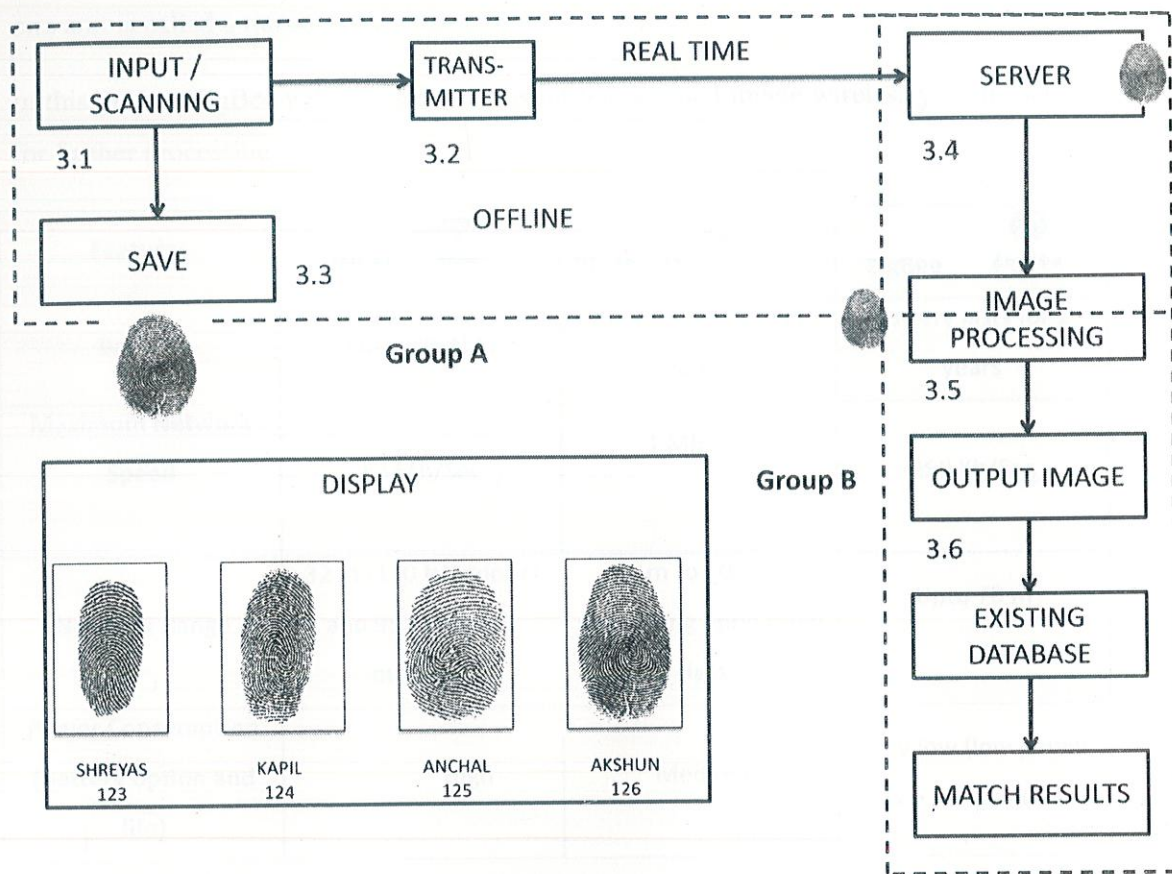


Fig: 3.2 Detailed Block Diagram

Now, explanation of the above block diagram is as follows:

3.1-Scanning- This is a method by which we can electronically obtain and store human fingerprints. The digital image obtained by such scanning is called a finger image. Fingerprint scanning is a biometric process involves the automated capture, analysis and comparison of specific characteristic of human fingerprint.

3.2-Transmitter- It is an electronic device which, with the aid of an antenna, produces radio waves. The transmitter itself generates a radio frequency alternating current, which is applied to the antenna. When excited by this alternating current, the antenna radiates radio waves. A transmitter can be a separate piece of electronic equipment, or an

electrical circuit within another electronic device. A transmitter and receiver combined in one unit is called a transceiver.

In this project ZigBee will be used to transmit the scanned image wirelessly to the server for further processing.




Features	Wi-Fi 	Bluetooth 	ZigBee 
Battery	Rechargeable	Intended for frequent charging	Battery lasts for 2 years
Maximum Network Speed	54 Mb/Sec	1 Mb/Sec	250 Kb/Sec
Network Range	32 m (120 ft) indoors and 95 m (300 ft) outdoors	1 m to 100 m depending upon radio class	Upto 70 m
Power Consumption (Battery option and life)	High	Medium	Very low (low power is a design goal)

Fig: 3.3 Comparison Between different protocols

3.3- Save- In case we do not want to send our data wirelessly, our device even has a provision to save the scanned images on any portable device to carry it manually to the server.

3.4- Server- It is a physical computer (a computer hardware system) dedicated to run one or more services (as a host) to serve the needs of the users of other computers on a network. Depending on the computing service that it offers it could be a database server, file server, mail server, print server, web server, gaming server, or some other kind of server. ^[31]

In our project we are mainly using DATABASE SERVER in order to store the scanned fingerprints of the students which is a onetime process and would be taken at the time of admission. In addition to this, all the processing related to these fingerprints and updation of attendance automatically will take place at server.

3.5- Image Processing- Image processing is a form of signal processing for which the input is an image. The output of image processing may be either an image or a set of characteristics or parameters related to the image. Detailed explanation of image processing is done in the next chapter.

3.2 - MATLAB:

Image processing is done using MATLAB which is a programming language for algorithm development, data analysis, visualization and numerical computation. Using MATLAB, we can solve technical computing problems faster than with traditional programming languages, such as C, C++ and FORTRAN.

We can use MATLAB in a wide range of applications, including signal and image processing, communications, control design, test and measurement, financial modeling and analysis, and computational biology. For a million engineers and scientists in industry and academia, MATLAB is the language of technical computing. MATLAB is widely used in academic and research institutions as well as industrial enterprises.^[32]

CHAPTER 4: IMAGE PROCESSING

This is an algorithm to recognize the fingerprint of any individual.

4.1 System Level Design

A fingerprint recognition system constitutes of fingerprint acquiring device, minutia extractor and minutia matcher.

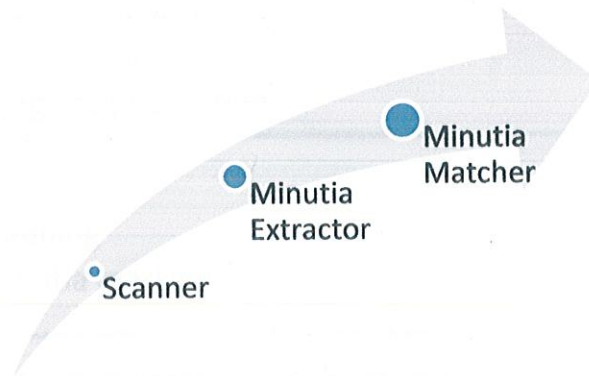


Fig: 4.1 System Level Design

For fingerprint acquisition, optical or semi-conduct sensors are widely used. They have high efficiency and acceptable accuracy except for some cases that the user's finger is too dirty or dry. So no acquisition stage has been implemented. ^[8]

4.2 Algorithm Level Design

To implement a minutia extractor, a three-stage approach is widely used by researchers. They are preprocessing, minutia extraction and post processing stage. For the fingerprint image preprocessing stage, Histogram Equalization and Fourier Transform have been used to do image enhancement. And then the fingerprint image is binarized using the locally adaptive threshold method. The image segmentation task is fulfilled by a three-step approach: block direction estimation, segmentation by direction intensity and Region of Interest extraction by Morphological operations. For minutia extraction stage, iterative parallel thinning algorithm is used. The minutia marking is a relatively simple task. For

the postprocessing stage, a more rigorous algorithm is developed to remove false minutia. Also a novel representation for bifurcations is proposed to unify terminations and bifurcations. [33][34]

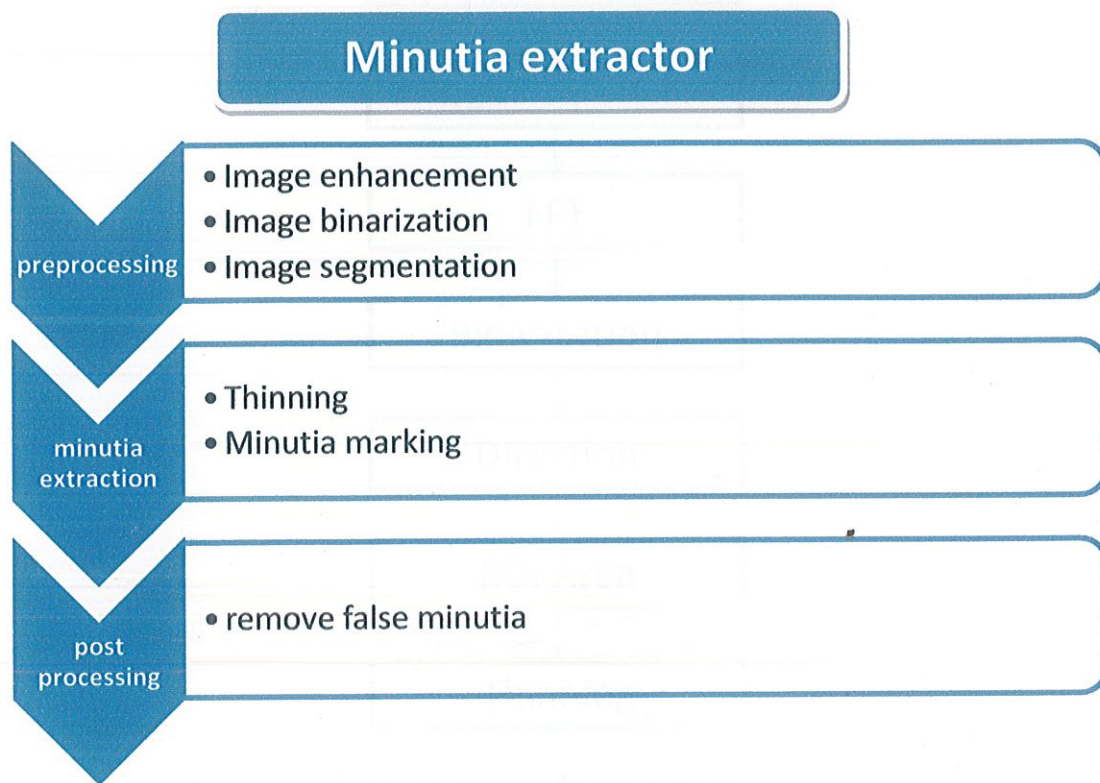


Fig: 4.2 Algorithm Level Design

4.3 Steps involved in fingerprint recognition Algorithm

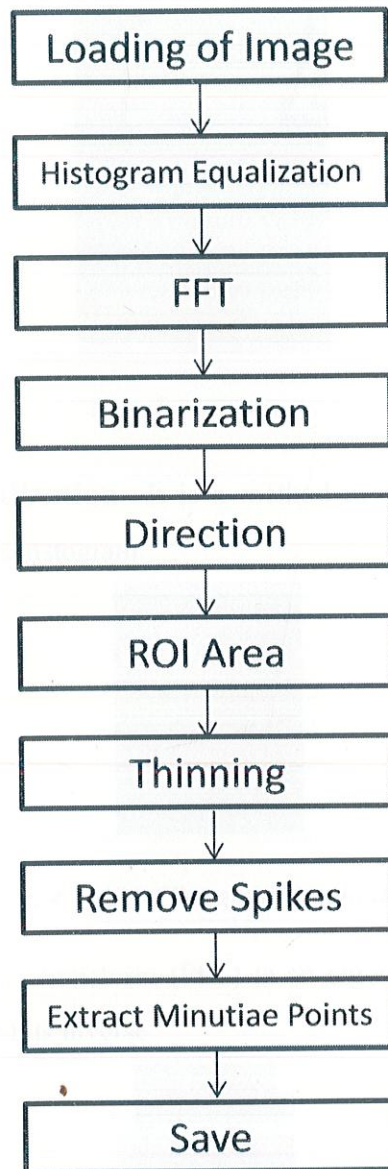


Fig: 4.3 Fingerprint Recognition Algorithm

Detailed explanation of the above block diagram:

1. **Loading of Image-** In this step, image is loaded in the system.

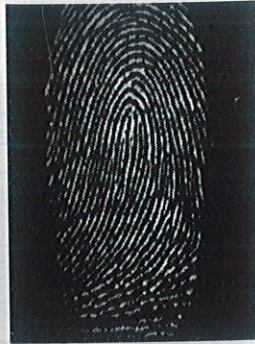


Fig: 4.4 Initial Image

2. **Histogram Equalization-** It is a method in image processing of contrast adjustment using the image's histogram.



Fig: 4.5 After Histogram Equalization

3. **FFT-** A fast Fourier transform (FFT) is an algorithm to compute the discrete Fourier transform (DFT) and its inverse.



Fig: 4.6 After Fast Fourier Transform

4. **Binarization-** Image binarization converts an image of up to 256 gray levels to a black and white image. The simplest way to use image binarization is to choose a threshold value, and classify all pixels with values above this threshold as white, and all other pixels as black.^[35]

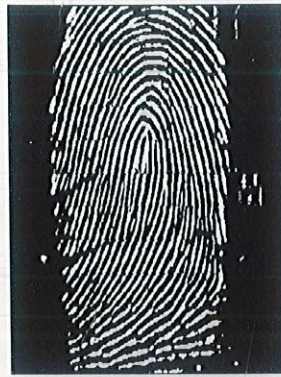


Fig: 4.7 After Binarization

5. **Directions-** Finds the direction of the ridge flow.



Fig: 4.8 Image showing Directions

6. **ROI Area-** Determines the region of interest.

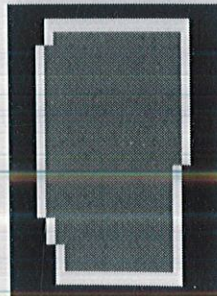


Fig: 4.9 ROI Area

7. **Thinning-** Thinning is a morphological operation that is used to remove selected foreground pixels from binary images, somewhat like erosion or opening. It can be used for several applications, but is particularly useful for skeletonization. In this mode it is commonly used to tidy up the output of edge detectors by reducing all lines to single pixel thickness. Thinning is normally only applied to binary images, and produces another binary image as output.^[36]



Fig: 4.10 Thinning

8. **Remove H Breaks-**



Fig: 4.11 Remove H Breaks

9. **Remove Spike-** Spikes are removed from the image.

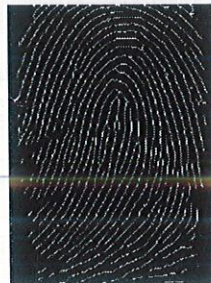


Fig: 4.12 Remove Spikes

10. **Extract-** All the minutiae points are extracted.

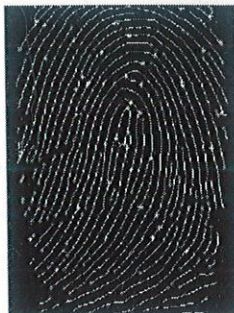


Fig: 4.13 Minutiae Extraction

11. **Real Minutiae Points-** Some of the minutiae points extracted in the previous step are now used to match the image and these are known as Real minutiae points.



Fig: 4.14 Useful Minutiae

12. **Save-** Image is saved in '.dat' format.

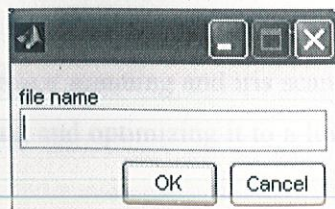


Fig: 4.15 Save Image

13. **Match-** Image is matched with the database and result will be displayed.

CHAPTER 5: CONCLUSION

It is a well known fact that accuracy of any biometric system depends upon the quality of the input data. The quality of input data depends on various factors as follows:

1. Quality of the biometric device.
2. Current condition of the biometric trait.
3. Environment.
4. How the user interacts with the device.

In this project the data can also be uploaded on the kiosk and hence save teacher's time and once the data is saved it is secure and no discrepancies can occur.

In future, we would be working on the hardware part of the project and would endeavor to make it error free. We would be also working on the following:

1. Improving the battery life of the device.
2. Optimizing the transmission rate.
3. Securing the transmission channel (data encryption).
4. Maximizing the range between the transmitter and receiver.

The project has a few limitations and a major ones being the high cost of the project and maintaining the huge database would cumbersome job. In the case of fingerprints frauds can be done easily by students and the transmission channel is not secure enough and can be hacked and manipulated with some expertise. For the jaw scanning, we require x ray machines and as of now very compact models are available at a very high cost.

Seeing the limitations with the jaw scanning and iris scanning the better option would be working on fingerprint scanning and optimizing it to a level would make it cost effective and beneficial for university.

REFERENCES

- [1] http://www.biometricfoundation.org/why_biometrics.html (accessed on 10 Jan, 2013)
- [2] <http://www.computer.org/csdl/mags/co/2010/02/mco2010020036-abs.html>
- [3] <http://onin.com/fp/fphistory.html>
- [4] Fingerprints: Analysis and Understanding MARK HAWTHORNE
- [5] Davide Maltoni (2009). Handbook of Fingerprint Recognition. London: Springer
- [6] Automatic Fingerprint Recognition Systems AUTHOR Nalini Ratha, Ruud Bolle
- [7] Handbook of fingerprint recognition Dario Maio, Anil K. Jain
- [8] Digital Image Processing / S. Sridhar (2010)
- [9] Textbook of Digital Image Processing / M. Anji Reddy (2006)
- [10] Alonso-Fernandez, F., Fierrez, J., Ortega-Garcia, J., Fronthaler, H., Kollreider, K., Bigun, J.: Combining Multiple Matchers for fingerprint verification, Vol. 62, (2007)
- [11] Antonelli, A., Capelli, R., Maio, D., Maltoni, D.: IEEE Trans. on Information Forensics and Security 1, 306–373 (2006)
- [12] Bazen, A., Gerez, S.: Segmentation of fingerprint images. Proc. Workshop on Circuits Systems and Signal Processing, ProRISC pp. 276–280 (2001)
- [13] Bazen, A., Gerez, S.: IEEE Trans. on Pattern Analysis and Machine Intelligence 24, 905–919 (2002)
- [14] Bigun, E., Bigun, J., Duc, B., Fischer, S.: International Conference on Audio- and Video-Based Biometric Person Authentication, AVBPA LNCS-1206, 291–300 (1997)
- [15] Bigun, J.: Vision with Direction. Springer (2006)

- [16] Bigun, J., Granlund, G.: Optimal orientation detection of linear symmetry. First International Conference on Computer Vision pp. 433–438 (1987)
- [17] BioSec: Biometrics and security, FP6 IP, IST - 2002-001766 - <http://www.biosec.org> (2004)
- [18] BioSecure: Biometrics for secure authentication, FP6 NoE, IST - 2002-507634 -
- [19] <http://www.biosecure.info> (2004)
- [20] Bolle, R., Serior, A., Ratha, N., Pankanti, S.: Fingerprint minutiae: A constructive definition. Proc. Workshop on Biometric Authentication, BIOAW LNCS-2359, 58–66 (2002)
- [21] Cappelli, R., Maio, D., Maltoni, D., Wayman, J.L., Jain, A.K.: IEEE Trans. on Pattern Analysis and Machine Intelligence 28(1), 3–18 (2006)
- [22] CBEFF: Common Biometric Exchange File Format - <http://www.itl.nist.gov/div893/biometrics/documents/NISTIR6529A.pdf> (2001)
- [23] Chang, J., Fan, K.: Fingerprint ridge allocation in direct gray scale domain. Pattern Recognition 34, 1907–1925 (2001)
- [24] Chen, Y., Jain, A.: Dots and incipients: Extended features for partial fingerprint matching. Proceedings of Biometric Symposium, Biometric Consortium Conference (2007)
- [25] Chen, Y., Parziale, G., Diaz-Santana, E., Jain, A.: 3d touchless fingerprints: Compatibility with legacy rolled images. Proceedings of Biometric Symposium, Biometric Consortium Conference (2006)
- [26] Chikkerur, S., Ratha, N.K.: Impact of singular point detection on fingerprint matching performance. Proc. IEEE AutoID pp. 207–212 (2005)
- [27] Chikkerur, S., Wu, C., Govindaraju, V.: A systematic approach for feature extraction in fingerprint images. Intl. Conf. on Bioinformatics and its Applications pp. 344–350 (2004)

- [28] Daugman, J.: How iris recognition works. IEEE Transactions on Circuits and Systems for Video Technology 14, 21–30 (2004)
- [29] Derakhshani, R., Schuckers, S., Hornak, L., O’Gorman, L.: Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners. Pattern Recognition 36, 383–396 (2003)
- [30] Fierrez, J., Torre-Toledano, J.D., Gonzalez-Rodriguez, J.: BioSec baseline corpus: A multimodal biometric database. Pattern Recognition 40(4), 1389–1392 (2007)
- [31] Fierrez-Aguilar, J., Chen, Y., Ortega-Garcia, J., Jain, A.: Incorporating image quality in multialgorithm fingerprint verification. Proc. International Conference on Biometrics, ICB LNCS- 3832, 213–220 (2006)
- [32] Fierrez-Aguilar, J., Munoz-Serrano, L., Alonso-Fernandez, F., Ortega-Garcia, J.: On the effects of image quality degradation on minutiae- and ridge-based automatic fingerprint recognition.
- [33] Proc. IEEE Intl. Carnahan Conf. on Security Technology, ICCST pp. 79–82 (2005)
- [34] Fronthaler, H., Kollreider, K., Bigun, J.: Local feature extraction in fingerprints by complex filtering. Proc. Intl. Workshop on Biometric Recognition Systems, IWBR LNCS-3781, 77–84 (2005)
- [35] Fronthaler, H., Kollreider, K., Bigun, J., Fierrez, J., Alonso-Fernandez, F., Ortega-Garcia, J., Gonzalez-Rodriguez, J.: Fingerprint image quality estimation and its application to multialgorithm verification. IEEE Trans. on Information Forensics and Security (to appear) (2008)
- [36] FVC2006: Fingerprint Verification Competition
<http://bias.csr.unibo.it/fvc2006/default.asp> (2006)

