** **

**INTELLIGENT SECURITY AND SAFETY SYSTEM FOR AUTOMOBILES**

**A PROJECT REPORT**

***Submitted by***

**AISHWARYA.S 211411205004**

**CHARANYA.S 211411205017**

**CHARUMATHI.V.S 211411205018**

***In partial fulfillment for the award of the degree***

***of***

**BACHELOR OF TECHNOLOGY**

**IN**

**INFORMATION TECHNOLOGY**

**PANIMALAR ENGINEERING COLLEGE, CHENNAI-600123**

**ANNA UNIVERSITY: CHENNAI-600 025**

**APRIL 2015**

**ANNA UNIVERSITY: CHENNAI 600 025**

**ANNA UNIVERSITY : CHENNAI 600 025**

**BONAFIDE CERTIFICATE**

Certified that this project report **“INTELLIGENT SECURITY AND SAFETY SYSTEM FOR AUTOMOBILES**” is the bonafide work of “**S.AISHWARYA (211411205004), S.CHARANYA (211411205017), V.S. CHARUMATHI (211411205018)”** who carried out the project work under my supervision.

**SIGNATURE SIGNATURE**

**Dr.HELDA MERCY, M.E., Ph.D., Mrs. M.SUMITHRA, M.E.,**

**HEAD OF THE DEPARTMENT SUPERVISOR**

Asst. Professor (Grade-I)

Department of IT Department of IT

Panimalar Engineering College Panimalar Engineering College

Chennai Chennai

Certified that the above mentioned students were examined in the university

project viva-voce held on \_\_\_\_\_\_\_\_\_\_\_\_\_

INTERNAL EXAMINER EXTERNAL EXAMINER

**DECLARATION**

I hereby declare that the project report entitled **“INTELLIGENCE SECURITY AND SAFETY SYSTEM FOR AUTOMOBILES**” which is being submitted in partial fulfillment of the requirement of the course leading to the award of the ‘Bachelor Of Technology in Information Technology’ in **PANIMALAR ENGINEERING COLLEGE, AFFILIATED TO ANNA UNIVERSITY- CHENNAI** is the result of the project carried out by us under the guidance and supervision of **Mrs. M.SUMITHRA,M.E,ASSOCIATE PROFESSOR GRADE-I IN THE DEPARTMENT OF INFORMATION TECHNOLOGY**. I further declare that I or any other person has not previously submitted this project report to any other institution/university for any other degree/ diploma or any other person.

Date: Signature of batch members

Place**: Chennai**

**(AISHWARYA.S)**

**(CHARANYA.S)**

**(CHARUMATHI V.S.)**

It is certified that this project has been prepared and submitted under my guidance.

Date:

Place: **Chennai**  **Mrs. M.SUMITHRA,M.E.**

**(ASSOCIATE PROFESSOR, GRADE-I, IT)**

**ACKNOWLEDGEMENT**

A project of this magnitude and nature requires kind co-operation and support from many, for successful completion . We pay our sincere thanks to all those who were involved in the completion of this project.

Our sincere thanks to our **Honorable Founder and Chairman, Dr.JEPPIAAR, M.A., B.L., Ph.D.,** for his sincere endeavor in educating us in his premier Institution.

We would like to express our deep gratitude to our **Most Respected** **Secretary and Correspondent, Dr. P. CHINNADURAI, M.A., M.Phil., Ph.D.,** for his kind words and enthusiastic motivation which inspired us a lot in completing this project and we also express our sincere thanks to **Our Dynamic Directors Mrs. C. VIJAYA RAJESHWARI, Mr. C. SAKTHI KUMAR, M.E.,** and **Mrs. SARANYA SREE SAKTHIKUMAR, B.E.,** for providing us with the necessary facilities for the completion of this project.

We also express gratitude to Our **Principal Dr. K.MANI, M.E., Ph.D.,** who has been a source of constant encouragement and support.

We would also wish to convey our sincere thanks and heart-filled gratitude to **Dr. M. HELDA MERCY, M.E., Ph.D., HEAD OF THE DEPARTMENT,** Information Technology, for her support without whose co-operation this venture would not have been a success.

We would also like to thank our internal guide **Mrs. M.Sumithra, M.E.,** for her valuable guidance.

Finally, we would like to thank our respected Professors, dear Parents and friends for their constant moral support, encouragement and the environment to work efficiently.

**ABSTRACT**

The vehicle accident and thefts are a major public problem in many countries. Despite awareness campaign, this problem is still increasing due to rider's poor behaviors such as speed driving, riding without helmet protection and sufficient sleep etc. The number of deaths and disability are very high because of late assistance to people who met with the accident. These causes huge social and economic burdens to people involved. Therefore, several research group and major motorcycle manufacturers have developed safety devices to protect riders from accidental injuries. However, good safety device for vehicle is difficult to implement and very expensive. To overcome these problem, we have proposed an embedded system for preventing vehicle theft and accidents. In this work we have developed door lock detection using metal sensor, seat belt detection using IR sensor, alcohol sensor to avoid drunk and drive along with heartbeat sensor for pulse rate detection. In fingerprint authentication, only the authorized person is passed and vehicle ignition will be initiated. If any other person rather than the authorized person is trying to access the vehicle, responsive GSM will be initiated and only the authorized person can give the permission rights.

**TABLE OF CONTENT**

**CHAPTER TITLE PAGE NO**

**ABSTRACT** iii

**LIST OF FIGURES** vi

**LIST OF TABLES** viii

**LIST OF ABBREVIATIONS** ix

**1 INTRODUCTION**

1.1 Overview1

1.2 Need for proposed system 2

1.3 Description of proposed system 2

1.4 Benefits of proposed system 3

**2 LITERATUTE SURVEY** 4

**3 SYSTEM ANALYSIS AND**

**DESIGN** 11

3.1 Proposed System Architecture 11

3.1.1 Specification 12

3.1.2 Pin Configuration 13

3.2 Module Description

3.2.1 Fingerprint Sensor 14

3.2.2 IR Sensor 23

3.2.3Heartbeat Sensor 26

3.2.4 Alcohol Sensor 28

**4 SOFTWARE AND HARDWARE DESCRIPTION**

4.1 Software Description 32

4.1.1 Embedded C

4.1.2 Hi-tech C Compiler

4.1.3 MPLAB

4.1.4 Proteus Software

4.2 Hardware Description 36

4.2.1 PIC Microcontroller

4.2.2 LCD 2X16 DISPLAY

4.2.3 GSM Interface

**5 IMPLEMENTATION**

5.1 Coding 54

5.2 Snapshot 77

**6 CONCLUSION**

6.1 Future Enhancement 83 **7 REFERENCES**  84

**LIST OF FIGURES**

**FIGURE CAPTION PAGE NO.**

3.1 Block diagram of proposed system 12

3.1.2 Schematic diagram of the hardware 13

3.2.1 Fingerprint sensor 14

3.2.1.3 Process of biometric system 16

3.2.1.4a Process of enrollment and verification 18

3.2.1.4b Generation of match score 19

3.2.1.4c Ridge ending for candidate 20

3.2.1.4d Detected Minutiae 21

3.2.2 IR transmitter and receiver 23

3.2.2.2 Circuit diagram of IR sensor 24

3.2.2.3 Working of IR sensor 25

3.2.3 Heartbeat Sensor 26

3.2.3.4 Working of heartbeat sensor 28

3.2.4a MQ135 Gas sensor 29

3.2.4b Pin diagram of MQ135 gas sensor 29

3.2.4.3 MQ135 gas sensor connection diagram 30

4.1.2 Hi-tech compiler 33

4.2.1 Typical PIC16F877A 36

4.2.1.2 Pin diagram of PIC16F877A 38

4.2.1.4a PIC16F877A Program memory 43

4.2.1.4b IC16F877A data memory 44

4.2.1.5 Internal architecture of PIC16F877A chip 46

4.2.2 LCD 2x16 display 47

4.2.3 GSM SIM900 49

4.2.3.1 GSM Structure 50

5.2 Overview of kit 72

5.2.1 Enroll Fingerprint 73

5.2.2 Unauthorized Fingerprint 74

5.2.3 Granting Access 75

5.2.4 IR sensor 76

5.2.5 Heartbeat Check 77

**LIST OF TABLES**

**TABLE CAPTION PAGE NO.**

2.6 Comparison table for all literature survey 7

3.2.2.2 Components of IR Sensor 24

4.2.1.2 Pin details 37

4.2.1.4 Register bank access 43

4.2.1.6c Status Registers 45

4.2.2 LCD pin details 48

**LIST OF ABBREVIATIONS**

**TP** True Positive

**TN** True Negative

**FP** False Positive

**FN** False Negative

**FAR** False acceptance rate

**FMR** False match rate

**FRR** False rejection rate

**FNMR** False non-match rate

**ROC** Receiver operating characteristic

**EER** Equal error rate

**CER** Crossover error rate

**FTE/ FER** Failure to enroll rate

**FTC** Failure to capture rate

**HLR** Home location register

**MSC** Mobile services switching center

**VLR** Visitor location register

**AUC** Authentication center

**EIR** Equipment Identity Register

**CHAPTER 1**

**INTRODUCTION**

**1.1 OVERVIEW:**

In current scenario vehicle security is provided by means of remote control access technology. In remote control access technology a keyless entry system(RKS) is used. A keyless entry system is an electronic lock that control access to a vehicle without using traditional mechanical key. It is widely used in automobiles.

An RKS(remote keyless system) performs the function of standard car key without physical contact. Within the few yards the car can lock or unlock the doors by pressing a button . The major disadvantage of this technology is that the vehicle can be accessed by any person when a remote is theft.

The main objective of this project is to prevent vehicle theft and accidents. The main cause for this problem is not following the safety precautions and traffic rules and regulations. Though many acts have been developed for preventing the vehicle accidents, many of us are not obeying it.

In the existing system various sensors are operating independently whereas in our proposed project sensors are operated in a sequence manner. These sensor operations are implemented using embedded system. An Embedded system is a special purpose computer controlled electro-mechanical system in which the computer is completely encapsulated by the device it controls. An embedded system has specific requirements and performs pre-defined task unlike a general-purpose personal computer. An embedded system is a computer- controlled system.

The core of any embedded system is a microprocessor which is programmed to perform a few tasks (often just one task). This is to be compared to other computer systems with general purpose hardware and externally loaded software . Embedded systems are often designed for mass production.

Apart from these sensor operations the heartbeat of the driver is continuously monitored through pulse detection. It also uses the responsive GSM technique. This technique provides strong anti-spoofing capabilities when compared to other technologies. As pulses are internal to the body, it is difficult to duplicate. In responsive GSM authorized person can give access rights to others.

**1.2 NEED FOR PROPOSED SYSTEM**

In the existing system, the authentication is done using fingerprint for the purpose of ignition in two wheelers. It provides security for the two wheeler from being theft. The fingerprint detection algorithm used is minutiae, ridge, image based matching. It can store up to 768 fingerprints. It eliminates the use of keys. It provides highly secure fingerprint identification and enrollment in database.

Existing security principle for the vehicles uses remote control access technology. No strong security systems designed so far. So car thefts have increased in large numbers. It does not notify the vehicle owner in case of an access by unauthorized person. As it is designed for a two wheeler no sensors are used for checking the health conditions of the driving person.

**1.3 DESCRIPTION OF PROPOSED SYSTEM**

The proposed system overcomes all the drawbacks of the existing system. The proposed system is designed for the four-wheelers especially cars. The finger print concept is used in the door lock itself for the purpose of car theft. The reversible GSM technique is used to grant access to the unauthorized person through messages. The location of the vehicle can be found using GPS and sent to nearby police station and owner in case of car theft. The sensors should be satisfied one after the other for the vehicle to start. The motion of the vehicle will be reduced in case of detection of low pressure during driving. The heartbeat of the person will be on a check throughout the journey. The alcohol sensor detects the alcohol content of the driving person.

**1.4 BENEFITS OF PROPOSED SYSTEM**

To prevent vehicle theft, accidents and also enhancing security (i.e.) Only the authorized person are allowed to access the respective vehicles. To provide safety and security concept to the drivers with the help of embedded systems. To find the current location of the vehicle and to allow the authorized person to control the motion of the vehicle. The unauthorized person can be granted access by the authorized person through the reversible GSM technique.This system can be used in call taxis which enhances the safety of the passengers.

**CHAPTER 2**

**2. LITERATURE SURVEY**

**2.1 A Fingerprint Recognition Algorithm Using Phase-Based Image Matching for Low-Quality Fingerprints**

**(Koichi Ito, Ayumi Morita, Takafumi Aoki, Tatuso Higuchi, Hiroshi Nakajima, Koji Kobayashi/ 2005)**

A major approach for fingerprint recognition today is to extract minutiae from fingerprint images and to perform fingerprint matching based on the number of corresponding minutiae pairings. One of the most difficult problems in fingerprint recognition has been that the recognition performance is significantly influenced by fingertip surface condition, which may vary depending on environmental or personal causes. Addressing this problem, this paper presents a fingerprint recognition algorithm using phase-based image matching. The use of phase components in 2D (two-dimensional) discrete Fourier transforms of fingerprint images makes possible to achieve highly robust fingerprint recognition for low-quality fingerprints. Experimental evaluation using a set of fingerprint images captured from fingertips with difficult conditions (e.g., dry fingertips, rough fingertips, allergic-skin fingertips) demonstrates an efficient recognition performance of the proposed algorithm compared with a typical minutiae-based algorithm.

**DRAWBACKS:**

It is less secure against side channel attacks.

It is prone to transmission errors.

**2.2 A Prototype of a Fingerprint Based Ignition Systems in Vehicles**

**(Omidiora E. O. , Fakolujo O. A. , Arulogun O. T. , Aborisade D. O. / 2010 )**

Biometric systems have overtime served as robust security mechanisms in various domains. Fingerprints are the oldest and most widely used form of biometric identification. A critical step in exploring its advantages is to adopt it for use as a form of security in already existing systems, such as vehicles. This research work focuses on the use of fingerprints for vehicle ignition, as opposed to the conventional method of using keys. The prototype system could be divided into the following modules: fingerprint analysis software module that accepts fingerprints images; hardware interface module and the ignition system module. The fingerprint recognition software enables fingerprints of valid users of the vehicle to be enrolled in a database. Before any user can ignite the vehicle, his/her fingerprint image is matched against the fingerprints in the database while users with no match in the database are prevented from igniting the vehicle. Control for the ignition system of the vehicle is achieved by sending appropriate signals to the parallel port of the computer and subsequently to the interface control circuit. The developed prototype serves as an impetus to drive future research, geared towards developing a more robust and embedded real-time fingerprint based ignition systems in vehicles.

**DRAWBACKS:**

Chances of faking the fingerprint is possible.

Fingerprint concept is used only for ignition not on door locks.

**2.3 A Study of Biometric Approach for Vehicle Security System Using Fingerprint Recognition**

**(N. Kiruthiga1 and L. Latha2 M.E, Department of CSE, Kumaraguru College of Technology, Coimbatore, India 1 Associate Professor, Department of CSE, Kumaraguru College of Technology, Coimbatore, India / 2010)**

The use of vehicle is a must for everyone. In the same way, safeguarding the vehicle against theft is also very essential. Impediment of vehicle theft can be done remotely by an authorized person. Embedded computing technology is an emergent field used in all the areas. A competent automotive security system is implemented using embedded system along with Global System for Mobile (GSM) and Fingerprint Recognition. This paper gives a literature survey on the vehicle security system using person identification techniques. The survey mainly emphasizes on major approaches for automatic person identification, namely fingerprint recognition and various existing vehicle security system. The security system can be implemented using Microcontroller.

**DRAWBACKS:**

In this the GSM concept is used only for tracking and monitoring of vehicles.

**2.4 The Design Of Mobile Control Car Security System (Jiwa Abdullah/2011)**

The present car alarm systems are still of no match to the well-equipped thieves. It is just a matter of seconds to break through the system. This paper introduces

and describes the design of mobile controlled car security system offering higher level of car security features. The mobile controlled car security is capable of providing an effective two-way communications between the alarm system and the car owner. This system is able to notify the car owner immediately when intrusion is detected. Additionally, the car owner can remotely control any of the car features anytime at anywhere via a phone call. Based on the GSM positioning concept, this system has the potential to provide car location information to assist in stolen vehicle recovery therefore providing enhancement over the conventional car alarm system.

**DRAWBACKS:**In this in case of unauthorized person accessing the vehicle then it will automatically call the owner. There are chances of owner not noticing the call and it is not provided with any solution on how the owner can respond to it.

**2.5 Implementation of GSM Based Heart Rate and Temperature Monitoring System**

**(Subhani SK.M, Sateesh G.N.V, Chaitanya C.H, Prakash Babu C. / 2013)**

There is a vast growth of VLSI technology and GSM communication in these days. This project deals about the implementation of GSM technology in Medical applications. This wireless communications would not only provide them withsafe and accurate monitoring but also the freedom of movement. In this, heart beat and temperature of patient are measured by using sensors as analog data, later it is converted into digital data using ADC which is suitable for wireless transmissionusing paging messages through GSM modem. AT89S52 micro controller device is used for temporary storage of the data used for transmission.

**DRAWBACKS**

It is complex since it is done with wireless communications.

**2.6 COMPARISON TABLE FOR ALL LITERATURE SURVEY**

|  |  |  |
| --- | --- | --- |
| **TITLE** | **OBJECTIVES** | **DRAWBACKS** |
| **Secure Fingerprint Matching Technique** | To propose a secure fingerprint matching technique, which is secure against side channel attacks.  This is done by dividing the fingerprint recognition system into secure and non-secure parts. | Only part of the fingerprint is used which results in single function. |
| **A Fingerprint Recognition Algorithm Using Phase-Based Image Matching for Low-Quality** | To achieve highly robust fingerprint recognition  for low-quality fingerprints using fingerprint recognition  algorithm. | It is less secure against side channel attacks.  It is prone to transmission errors. |
| **The Design of an Intelligent Security Access Control**  **System Based on Fingerprint Sensor FPC1011C** | A fingerprint acquisition module and a wireless alarm module is used is used to provide intelligent sec. access control using GSM and GPRS. | Owner cannot control the access of the vehicle. |
| **A Prototype of a fingerprint based ignition systems in vehicles** | Implementing the concept of finger print in vehicles for the purpose of ignition. | Chances of faking the finger print is possible. |
| **A Study of Biometric Approach for Vehicle**  **Security System Using Fingerprint Recognition** | To implement a competent automotive security system using embedded system  along with Global System for Mobile (GSM) and Fingerprint Recognition for automatic person identification. | Only used for tracking and monitoring the vehicle. |
| **The Design of Mobile Control Car Security System** | Based on the GSM positioning concept, this system has the potential to provide car location information to assist in stolen vehicle recovery therefore providing enhancement over the conventional car alarm system. | In this system , the car owner can control the features of the car using GSM that involves phone call and no alert message is provided. |

|  |  |  |
| --- | --- | --- |
| **Intelligent Vehicle Control for Driver Behaviour using Wireless in Transportation System** | To provide multiple levels of security using GSM, GPS receiver, alcohol and heartbeat sensors, eyeblink sensors, RFID reader and accident sensors | This involves the use of more instruction sets  Practical implementation was not very successful as it is more complex |
| **Advanced Car Security System Using GSM** | This system proposes the design and construction of an advanced car security system using GSM using SMS protocol available in the mobile phone | The car owner cannot control the features of the car using reversible GSM as it is not supported. |
| **Implementation of GSM Based Heart Rate and Temperature Monitoring System** | To provide security of using temp. monitoring system and heart rate detection using sensors. | More technology is required for wireless transmission  High cost |
| **Fingerprint based locking system** | To overcome the inconveniences of the conventional fingerprint system that allows access to only those whose fingerprints are pre stored in the memory | No notification is given to the owner in case of unauthorized access |

**CHAPTER 3**

**3. SYSTEM ANALYSIS AND DESIGN**

**3.1 PROPOSED SYSTEM ARCHITECTURE**

The system operates in the following manner,

* Initially door lock detection is done using metal sensor. If the door is locked properly, the next stage i.e seat belt detection will be displayed in the LCD.
* Seat belt detection is done using IR sensor. When the seat belt is worn, the next stage will be displayed otherwise it will remain in the same process.
* The next operation will be alcohol sensor. This sensor detects the alcohol concentration in our breath. It acts like a normal breath analyzer.
* After the alcohol sensor, the next sequence of operation will be vibration sensor.
* After the completion of the sensors, biometric authentication takes place. In biometric authentication human body characteristics such as finger print is obtained and stored as a template in the database which is known as enrollment.
* Before vehicle ignition, the user’s finger print is compared with the template. If both the images are matched relay gets on and vehicle ignition takes place, otherwise responsive GSM will be initiated.
* Heartbeat sensor is used for detecting the pulse rate of the person driving the vehicle that will reduce the speed of the vehicle in case of low pulse rate i.e. low blood pressure or low sugar.

**Fig 3.1 Block diagram of proposed system**

**3.1.1 SPECIFICATIONS**

**3.1.1.1 HARDWARE COMPONENTS**

* + - PIC Microcontroller(16F877A)
    - Metal sensor
    - Alcohol sensor
    - IR sensor
    - Biometric sensor
    - LCD
    - Relay
    - GSM

**3.1.1.2 SOFTWARE COMPONENTS**

* + - Hi-Tech C compiler
    - MPLAB
    - Embedded C
    - Proteus

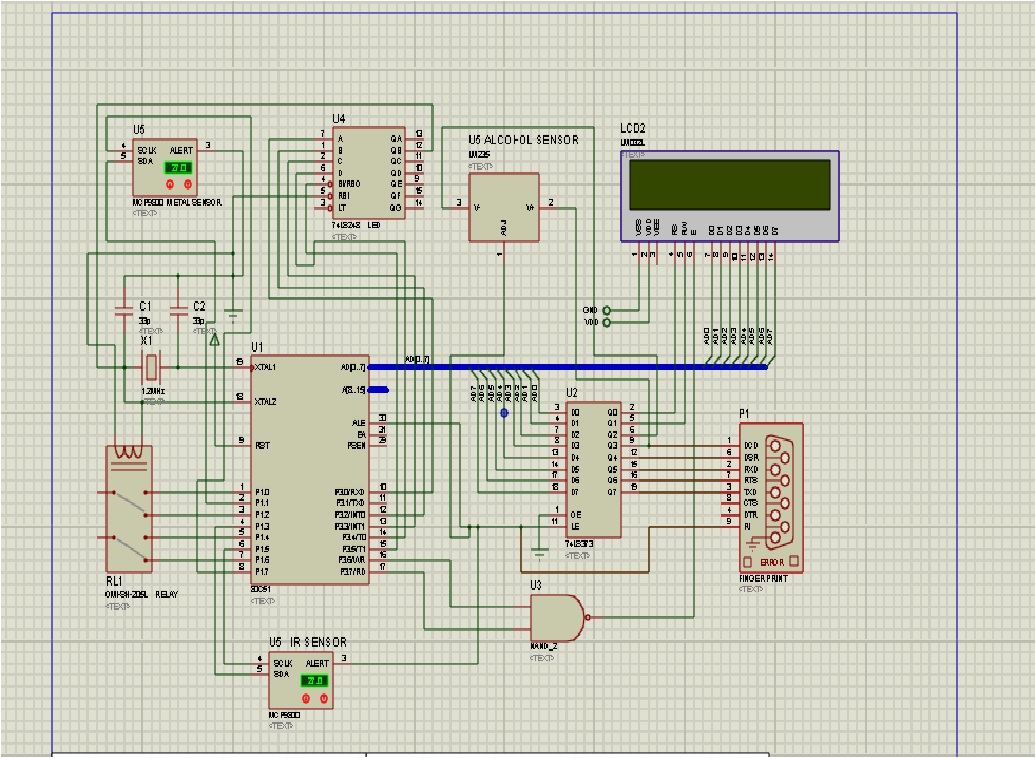
**3.1.2 CIRCUIT DIAGRAM:**

* Crystal oscillator’s operating frequency is 20MHZ
* Finger print reader- operates in three modes

-Enrollment

-Identification

-Deletion



**Fig3.1.2: Schematic diagram of the hardware**

* NAND gate- compare the obtained fingerprint with the stored template.
* ALERT PIN-when the vehicle is handled by unauthorized person, alert message will be sent to the controller.

**3.2 MODULE DESCRIPTION**

**3.2.1 FINGERPRINT SENSOR**

Biometrics is the science and technology of measuring and analyzing biological data such as DNA, fingerprints, eye retinas, irises, voice patterns, facial patterns and hand measurements for authentication purposes.   
Authentication by biometric verification is becoming increasingly common in corporate and public security systems, consumer electronics and point of sale (POS) applications. A biometric sensor is a device which is used to obtain the necessary verification data from a person. It is an essential component of a biometric system which uses physical traits to identify, verify and authenticate the identity of the user. In fingerprint biometrics application, an optical biometric sensor is employed to produce an image of the ridge structure at a fingertip.



**Fig 3.2.1: Fingerprint sensor module(R305)**

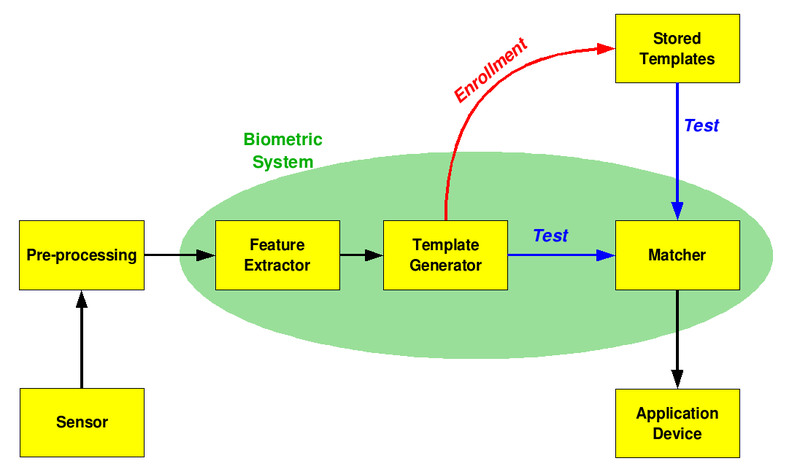
**3.2.1.1 FEATURES:**

* Low power consumption, low cost, small size, excellent performance.
* Professional optical technology, precise module manufacturing techniques.
* Good image processing capabilities.
* It can successfully capture image up to resolution 500 dpi.

**3.2.1.2 SPECIFICATIONS:**

* Fingerprint sensor type: Optical
* Supply voltage: 3.6 – 6.0VDC.
* Operating current: 120mA max.
* Peak current: 150mA max.
* Fingerprint imaging time: <1.0 seconds.
* Window area: 14mm x 18mm.
* Signature file: 256 bytes.
* Template file: 512 bytes.
* Storage capacity: 162 templates.
* Safety ratings (1-5 low to high safety).
* False Acceptance Rate: <0.001% (Security level 3).
* False Reject Rate: <1.0% (Security level 3).
* Interface: TTL Serial.
* Baud rate: 9600, 19200, 28800, 38400, 57600 (default is 57600).
* Working temperature rating: -20C to +50C.
* Working humidity: 40%-85% RH.
* Full Dimensions: 56 x 20 x 21.5mm.
* Exposed Dimensions (when placed in box): 21mm x 21mm x 21mm triangular.
* Weight: 20 grams.
* Resolution 500 DPI.
* Matching Method:  1: N.
* Image Capture Surface 15—18(mm).
* Verification Speed:  0.3 sec.
* Scanning Speed: 0.5 sec.
* Sensor Life: 100 million times.

**3.2.1.3 BIOMETRIC SYSTEM:**



**Fig 3.2.1.3: Process of biometric system**

**3.2.1.4 WORKING:**

Individuals must first register their form of identity with the system by means of capturing a raw biometric to be used in the system. This process is called Enrollment and is composed of three distinct phases: Capture, Process and Enroll.

* Capture: A raw biometric is captured by the Biometric sensing device.
* Process: Characteristics that are unique to individuals and distinguish individuals from one another are extracted from the raw Biometric and transformed into a biometric "template".
* **Enroll**: The processed template is stored in a suitable storage medium such as a database on a disk storage device or on a portable device such as a Smart Card, where by later comparisons can be made easily.

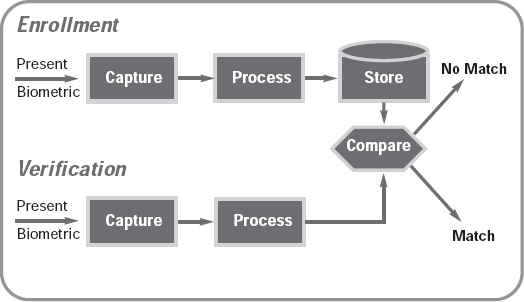
Once Enrollment is complete, the system can authenticate individuals by means of using the stored template. Authentication is the process whereby a new biometric sample is captured by the individual who is authenticating with the system and compared to the registered (enrolled) biometric template. There are two forms of Authentication: Verification and Identification.

* **Identification**: It performs the process of identifying an individual from their biometric features.
* **Verification** : It involves matching the captured biometric sample against the enrolled template that is stored and requires the user to assert a specific claim of identity such as a user name or unique ID.

The success of a system in performing verification is measured using the metrics below. Successful systems will have high True Positive and True Negative values, a poor system will have high False Positive and False Negative values. Each metric is defined as follows:

* **TP**: correctly allow access to an authorized user.
* **TN**: correctly deny access to an unauthorized user.
* **FP**: incorrectly allow access to an unauthorized user (FAR).
* **FN**: incorrectly deny access to an authorized user (FRR).

A diagram illustrating the process of Enrollment and Authentication is shown below:



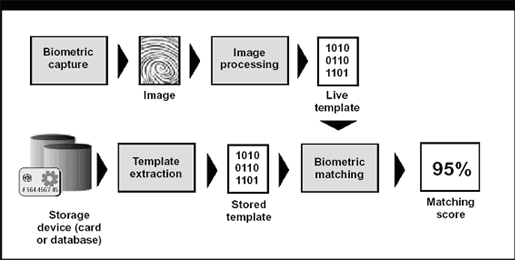
**Fig 3.2.1.4a: Process of enrollment and verification**

**Fig 3.2.1.4aa DFD for fingerprint**

* **Feature extraction**

The user places a finger on the scanner. The image is then encrypted and sent to the computer where the processing takes place. The image is formed of dark lines (ridges) and lighter lines (valleys). The methodology that most matching algorithms are based on minutia matching. Minutia are particular features of the lines on the fingerprint. The most commonly used one is bifurcation, where the ridge takes two different paths and ridge endings, where the ridge begins or ends.

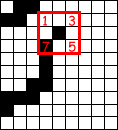
For the computer to be able to identify minutia , the image must undergo some pre-processing first. Most images from a fingerprint scanner are in grey scale, this makes it difficult to distinguish between ridges and valleys. Therefore the image is converted into a binary image. This is done by calculating the average pixel colour value over small areas of the image (typically an area is 8x8 pixels), any pixel with a value higher than the average colour value is converted to black, anything below is converted to white. Noise reduction then takes place to reduce interference. Finally the image is thinned so that the ridge lines are only one pixel thick.



**Fig 3.2.1.4b: Generation of match score**.

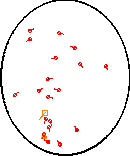
## The Matching Process

## Thinning enables the computer to identify ridge endings and bifurcation by pixel transition counting. This method involves counting how many transitions from black to white are made when traversing round the surrounding pixels of the candidate minutiae. If a candidate minutiae is truly a ridge ending then there will only be one transition, if it is a bifurcation there will be 3 transitions. The diagram below shows a candidate for a ridge ending; starting from square 1 and moving clockwise, the pixels are all white until square 7, where there is transition from black to white from square 7 to 8. As there is only one transition, the candidate is accepted as being a ridge ending.



**Fig 3.2.1.4c: Ridge ending for candidate**

The detected minutiae are stored on a template at their relative coordinates. The lines next to the minutiae represent the direction in which the line is travelling. This template is stored in a database if enrolling the user. If trying to authenticate the user, the template is then compared to templates already in the database. A predefined threshold is set; if the number of matching minutiae is greater than the threshold value it is deemed a match.



**Fig 3.2.1.4d: Detected minutia**

**3.2.1.5 PERFORMANCE:**

The following are used as performance metrics for biometric systems:

* **False acceptance rate or False match rate (FAR or FMR)**: The probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted.
* **False rejection rate or False non-match rate (FRR or FNMR)**: The probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.
* **Receiver operating characteristic or Relative operating characteristic (ROC)**: The ROC plot is a visual characterization of the trade-off between the FAR and the FRR.
* **Equal error rate or Crossover error rate (EER or CER)**: The rate at which both acceptance and rejection errors are equal. The value of the EER can be easily obtained from the ROC curve.
* **Failure to enroll rate (FTE or FER)**: The rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.
* **Failure to capture rate (FTC)**: Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.
* **Template capacity**: The maximum number of sets of data which can be stored in the system.

**3.2.1.6 ADVANTAGES**

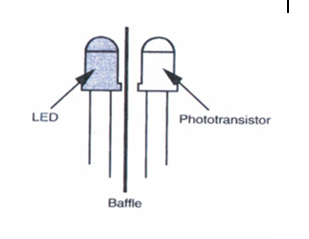
* They are lightweight and compact in design for use in a biometric system
* They do not require high investments or high maintenance.
* Fast and easy means of identification
* The level of accuracy is high.
* Non-invasive.
* High reliability.

**3.2.1.7 APPLICATIONS**

* Logical access control.
* ATM.
* Credit card transaction.
* Vault.
* Information technology .
* Internet banking.
* Government sector.
* Voter registration.
* Building door lock.

**3.2.2 IR SENSOR**

An infrared sensor is an electronic device that emits an infrared radiation in order to sense some aspect of its surroundings. Here we are using an active infrared sensor for seat belt detection. The principle behind an active infrared sensor is the transmission and receiving of infrared light. An element known as a light emitting diode (LED) transmits infrared light, which is reflected on the object and received by an optical receiver known as a photo diode (PD). As long as there is no movement or object in the path of the light beam, the light pattern is static and the sensor remains in stand-by. Active infrared sensors are generally immune to the effects of external factors such as rain, snow and falling leaves.

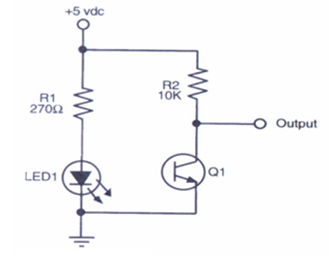


**Fig 3.2.2: IR Transmitter and receiver**

**3.2.2.1 FEATURES:**

* High accuracy and high sensitivity (110 V/W).
* Low resistance (50k/ohm).
* Very good signal-to-noise-ratio.
* Good response time (40 ms).
* Easy and accurate measurement of the sensor temperature.

**3.2.2.2 CIRCUIT DIAGRAM**

****

**Fig 3.2.2.2: Circuit diagram of IR sensor**

|  |  |
| --- | --- |
| **SYMBOL** | **DETAILS** |
| R1 | 270 ohm resistor |
| R2 | 10 kohm resistor |
| LED1 | Infrared LED |
| Q1 | IR sensitive Photo resistor |

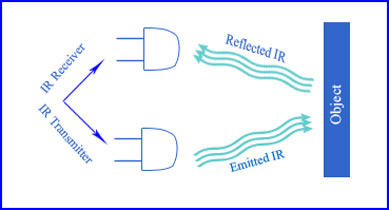
**Table3.2.2.2: Components of IR sensor**

**3.2.2.3 WORKING:**

IR LED emits an infrared radiation. This radiation illuminates the surface in front of LED and reflects the infrared light. Depending on reflectivity of the surface, amount of light reflected varies. This reflected light is made incident on reverse biased IR sensor.

When photons are incident on reverse biased junction of this diode, electron-hole pairs are generated, which results in reverse leakage current. Amount of electron-hole pairs generated depends on intensity of incident IR radiation.

More intense radiation results in more reverse leakage current. This current can be passed through a resistor so as to get proportional voltage. Thus as intensity of incident rays varies, voltage across resistor will vary accordingly. This voltage can then be given to OPAMP based comparator. Output of the comparator can be read by microcontroller.



**Fig 3.2.2.3: Working of IR sensor.**

**Fig 3.2.2.3aa: DFD for IR sensor**

**3.2.2.4 APPLICATIONS:**

* + - Augmentative communication devices.
    - Car locking systems.
    - Computers.
    - Emergency response systems.
    - Environmental control systems.
    - Headphones.
    - Home security systems.
    - Navigation systems.
    - Telephones, TVs, VCRs, CD players, stereos.

**3.2.3 HEART BEAT SENSOR**

Heart beat sensor is designed to give digital output of heat beat when a finger is

placed on it. When the heart beat detector is working, the beat LED flashes in unison with each heart beat. This digital output can be connected to microcontroller directly to measure the Beats Per Minute (BPM) rate. It works on the principle of light modulation by blood flow through finger at each pulse.

****

**Fig 3.2.3 Heart beat sensor**

**3.2.3.1 Features**

* + - Heat beat indication by LED
    - Instant output digital signal for directly connecting to microcontroller
    - Compact Size
    - Working Voltage +5V DC

**3.2.3.2 Specification**

* Operating Voltage +5V DC regulated
* Operating Current 100 mA
* Output Data Level 5V TTL level
* Heart Beat detection Indicated by LED and Output High Pulse
* Light source 660nm Super Red LED

**3.2.3.3 Pin Details**

Board has 3-pin connector for using the sensor. Details are marked on PCB as below :

1. +5V Power supply Positive input

2. OUT Active High output

3. GND Power supply Ground

**3.2.3.4 Working**

The sensor consists of a super bright red LED and light detector. The LED needs to be super bright as the maximum light must pass spread in finger and detected by detector. Now, when the heart pumps a pulse of blood through the blood vessels, the finger becomes slightly more opaque and so less light reached the detector. With each heart pulse the detector signal varies. This variation is converted to electrical pulse. This signal is amplified and triggered through an

amplifier which outputs +5V logic level signal. The output signal is also indicated by a LED which blinks on each heart beat. FIGURE 1 SENSOR PRINCIPLE LED OFF when no beat detected

when finger is not placed on sensor.



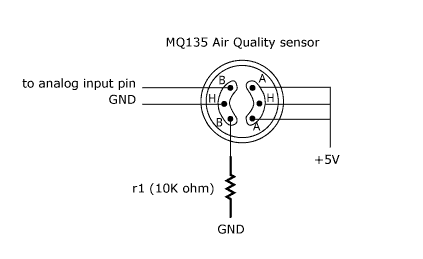
**Fig 3.2.3.4 Working of sensor**

**Fig 3.2.3.4aa DFD for Heart beat sensor**

**3.2.3.5 Applications:**

* + - Patient Monitoring System
    - Bio-Feedback control of robotics and applications

**3.2.4 ALCOHOL SENSOR**

This alcohol sensor is suitable for detecting alcohol concentration on our breath, just like common breath analyzer. It has a high sensitivity and fast response time. Sensor provides an analog resistive output based on alcohol concentration. The drive circuit is very simple, all it needs is one resistor. A simple interface could be a 0-3.3V ADC. MQ135 gas sensor is used here.

**Fig 3.2.4: a). MQ135 gas sensor. b).Pin diagram of MQ135 gas sensor**

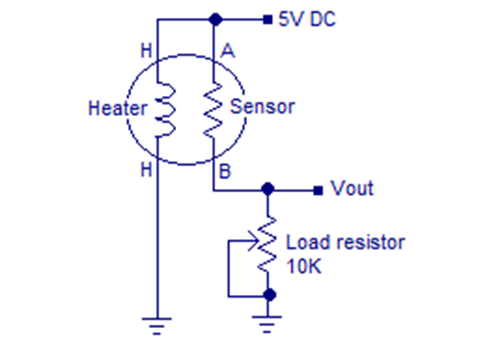
**3.2.4.1 FEATURES:**

* + - Requires heater voltage.
    - High sensitivity to alcohol and small sensitivity to Benzine.
    - Stable and long life.
    - Simple drive circuit.

**3.2.4.2 SPECIFICATIONS:**

* + - Working voltage: DC 5V.
    - Working Current: 150mA.
    - Heater Voltage: 5.0V.
    - Operation Temperature: -10 to 70 degrees C.
    - Heater consumption: less than 750mW.
    - Detection Range: 10 - 1,000 ppm Alcohol.
    - Fast Response Time: <10s.
    - Preheat time: Over 20s.
    - Dimension: 32mm x 22m x 27mm (HIGH 27mm).

**3.2.4.3 CIRCUIT DIAGRAM**



**Fig 3.2.4.3: MQ135 gas sensor connection diagram**

**3.2.4.4 WORKING:**

MQ135 is a stable and sensitive gas sensor which can detect  ammonia, carbon dioxide, alcohol, smoke, nitrogen dioxide etc. The sensor consists of a tin dioxide sensitive layer inside aluminium oxide micro tubes, measuring electrode and a heating element inside a tubular aluminium casing. The front end of the sensor is covered using a stainless steel net and  the rear side holds the connection terminals.

The ethyl alcohol present in the breath is oxidized into acetic acid while passing over the heating element. This ethyl alcohol falls on the  tin dioxide sensing layer and as a result, its resistance decreases. This resistance variation  is converted into a suitable voltage variation using an external load resistor.

MQ135 has different resistance values at different temperature and different concentration of gases. The manufacturer recommends to calibrate the sensor at 50ppm of alcohol. The recommended value of the load resistor is between 10K to 47K.

**Fig 3.2.4.3aa DFD for alcohol sensor**

**3.2.4.5 APPLICATIONS:**

* They are suitable for alcohol checker, Breath analyser.
* They are used in air quality control equipments for buildings or offices.
* It is suitable for detecting of NH3,NOx, alcohol, Benzene, smoke, CO2 etc.

**CHAPTER 4**

**4. SOFTWARE AND HARDWARE DESCRIPTION**

**4.1 SOFTWARE DESCRIPTION**

**4.1.1 EMBEDDED C**

Embedded C is a set of language extensions for the C programming language by the C standards committee to address commonality issues that exist between C extensions for different embedded systems. Historically, embedded C programming requires nonstandard extensions to the C language in order to support exotic features such as fixed point arithmetic, multiple distinct memory banks, and basic I/O operations.

In 2008, the C Standards Committee extended the C language to address these issues by providing a common standard for all implementations to adhere to. It includes a number of features not available in normal C, such as, fixed-point arithmetic, named address spaces, and basic I/O hardware addressing.

Embedded C uses most of the syntax and semantics of standard C, e.g., main() function, variable definition, data type declaration, conditional statements (if, switch, case), loops (while, for), functions, arrays and strings, structures and union, bit operations, macros, etc.

**4.1.1.1Main characteristics of an Embedded programming environment:**

• Limited ROM.

• Limited RAM.

• Limited stack space.

• Hardware oriented programming.

• Critical timing (Interrupt Service Routines, tasks, …).

• Many different pointer kinds (far / near / rom / uni / paged / …).

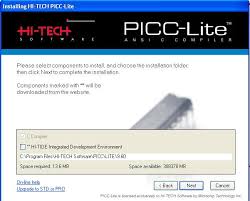
• Special keywords and tokens (@, interrupt, tiny, …).

**4.1.2 HI-TECH COMPILER**

This compiler supports Microchip PIC devices with Baseline, Mid-Range and

Enhanced Mid-Range cores. All are 8-bit devices. The Baseline core uses a 12-bit wide instruction set and is available in PIC10, PIC12 and PIC16 part numbers. The Mid-Range core utilizes a 14-bit wide instruction set that

includes additional instructions to those provided by Baseline parts. Its data memory banks and program memory pages are larger than those on Baseline devices. It is available in PIC12, PIC14 and PIC16 part numbers. The Enhanced Mid-Range core also uses a 14-bit wide instruction set, but incorporates additional instructions and features over the Mid-Range devices. There are both PIC12 and PIC16 part numbers that are based on the Enhanced Mid-Range core.



**Fig 4.1.2: Hi-tech Compiler**

**4.1.3 MPLAB**

MPLAB Integrated Development Environment (IDE) is a comprehensive editor, project manager and design desktop for application development of embedded designs using Microchip PIC micro and PIC microcontrollers.

The initial use of MPLAB IDE is covered here. How to make projects, edit code and test an application will be the subject of a short tutorial. By going through the tutorial, the basic concepts of the Project Manager, Editor and Debugger can be quickly learned. The complete feature set of MPLAB IDE is covered in later chapters. This section details the installation and uninstall of MPLAB IDE. It is followed by a simple step-by-step tutorial that creates a project and explains the elementary debug capabilities of MPLAB IDE. Someone unfamiliar with MPLAB IDE will get a basic understanding of using the system to develop an application. No previous knowledge is assumed, and comprehensive technical details of MPLAB IDE and its components are omitted in order to present the basic framework for using MPLAB IDE.

MPLAB IDE is a Windows® OS based Integrated Development Environment for the PIC micro MCU families and the PIC Digital Signal Controllers. The MPLAB IDE provides the ability to:

• Create and edit source code using the built-in editor.

• Assemble, compile and link source code.

• Debug the executable logic by watching program flow with the built-in simulator or in real time with in-circuit emulators or in-circuit debuggers.

• Make timing measurements with the simulator or emulator.

• View variables in Watch windows.

• Program firmware into devices with device programmers.

**4.1.4 PROTEUS**

Proteus was initially created as a multiplatform (DOS, Windows, Unix) system utility, to manipulate text and binary files and to create CGI scripts. The language was later focused on Windows, by adding hundreds of specialized functions for: network and serial communication, database interrogation, system service creation, console applications, keyboard emulation, ISAPI scripting (for IIS). Most of these additional functions are only available in the Windows flavour of the interpreter, even though a Linux version is still available.

Proteus was designed to be practical (easy to use, efficient, complete), readable and consistent.

Its strongest points are:

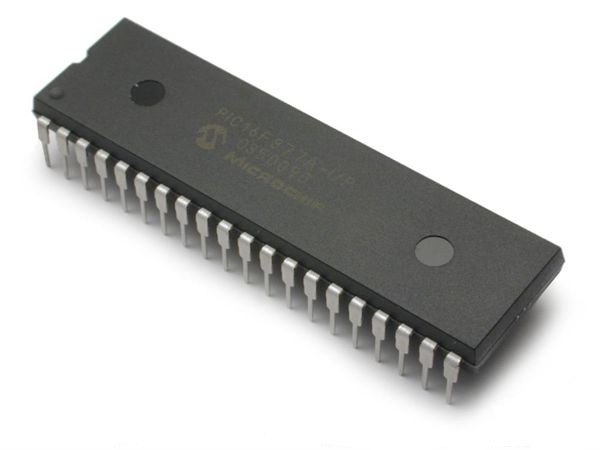
* + powerful string manipulation;
  + comprehensibility of Proteus scripts;
  + availability of advanced data structures: arrays, queues (single or double), stacks, bitmaps, sets, AVL trees.

The language can be extended by adding user functions written in Proteus or DLLs created in C/C++.

**4.2 HARDWARE DESCRIPTION**

**4.2.1 PIC CONTROLLER**

PIC16F877A is one of the PIC Family microcontroller which is popular at this moment, start from beginner until all professionals, because it is very easy to use. PIC16F877A uses FLASH memory technology so that data can be write or erased many times. The superiority of this Risc Microcontroller when compared with other microcontroller is speed of operation and code compression. PIC16F877A have 40 pins.



**Fig 4.2.1:Typical PIC16F877A**

PIC16F877A perfectly fits many uses, from automotive industries and controlling home appliances to industrial instruments, remote sensors, electrical door locks and safety devices. It is also ideal for smart cards as well as for battery supplied devices because of its low power consumption. EEPROM memory makes it easier to apply microcontrollers to devices where permanent storage of various parameters is needed (codes for transmitters, motor speed, receiver frequencies, etc.). Low cost, low power consumption, easy handling and flexibility makes PIC16F877A applicable even in areas where microcontrollers had not previously been considered (example: timer functions, interface replacement in larger systems, coprocessor applications, etc.).

System Programmability of this chip makes possible the flexibility of this product, after assembling and testing have been completed. This capability can be used to create assembly-line production, to store calibration data available only after final testing.

**4.2.1.1 FEATURES:**

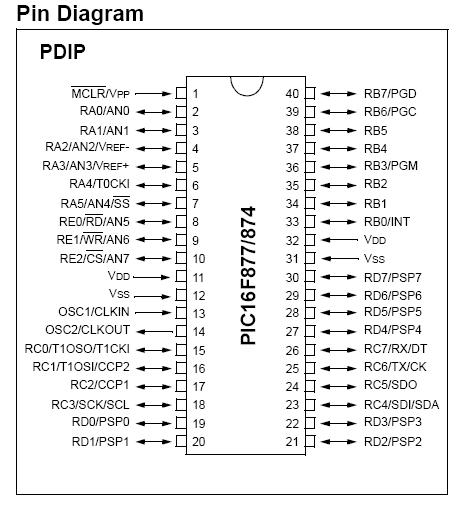
**4.2.1.1a Peripheral Features:**

* + Timer0: 8-bit timer/counter with 8-bit pre scaler
  + Timer1: 16-bit timer/counter with pre scaler, can be incremented during Sleep via external crystal/clock
  + Timer2: 8-bit timer/counter with 8-bit period register, pre scaler and post scaler.
  + Two Capture, Compare, PWM modules
  + Capture is 16-bit, max. resolution is 12.5 ns
  + Compare is 16-bit, max. resolution is 200 ns
  + PWM max. resolution is 10-bit
  + Synchronous Serial Port (SSP) with SPI™(Master mode) and I2C™ (Master/Slave)
  + Universal Synchronous Asynchronous Receiver Transmitter (USART/SCI) with 9-bit address detection
  + Parallel Slave Port (PSP) – 8 bits wide with external RD, WR and CS controls (40/44-pin only)
  + Brown-out detection circuitry for Brown-out Reset (BOR)

**4.2.1.1b Analog Features:**

* + 10-bit, up to 8-channel Analog-to-Digital Converter (A/D)
  + Brown-out Reset (BOR)
  + Analog Comparator module with:
    - Two analog comparators
    - Programmable on-chip voltage reference (VREF) module
    - Programmable input multiplexing from device inputs and internal voltage reference
    - Comparator outputs are externally accessible

**4.2.1.2 PIN DIAGRAM**



**Fig 4.2.1.2:Pin diagram of PIC16F877A**

**PIN DETAILS**

|  |  |  |
| --- | --- | --- |
| **PORT** | **PINS** | **APPLICATION** |
| A | 2, 3, 4, 5, 7 | ADC |
| B | 33 to 40 | Digital |
| C | 15 to 18, 23 to 26 | Digital |
| D | 19 to 22, 27 to 30 | Digital |
| E | 8, 9, 10 | ADC |
| **-** | 1 | MCLR |
| **-** | 11, 12, 31, 32 | Power supply |
| **-** | 13, 14 | Quartz crystal oscillator |
| **-** | 6 | No use |

**Table 4.2.1.2: pin details**

**4.2.1.3 INPUT/OUTPUT PORTS:**

PIC16F877 has 5 basic input/output ports. They are usually denoted by PORT A (R A), PORT B (RB), PORT C (RC), PORT D (RD), and PORT E (RE). These ports are used for input/ output interfacing. The five input/output ports and its functions are given below:

**PORT A and the TRIS A Registers**

PORT A is a 6-bit wide bi-directional port, the direction of this port is controlled by TRIS  A data direction register. Setting a TRIS A (=1) makes corresponding PORT A pin as an input, clearing the TRIS A (=0) making the corresponding PORT A pin as an output.

Pin RA4 is multiplexed with the “Timer0” module clock input to become the RA4/T0CKI pin and functioning either input/output operation or Timer 0 clock functioning module. The RA4/T0CKI pin is a Schmitt Trigger input and an open-drain output. All other PORT A pins have TTL input levels and full CMOS output drivers.

Other PORT A pins in this microcontroller multiplexed with analog inputs and the analog VREF input for both the A/D converters and the comparators. The operation of each pin is selected by clearing/setting the appropriate control bits in the ADCON1 and/or CMCON registers. The TRIS A register controls the direction of the PORT pins even when they are being used as analog inputs. The user must ensure the bits in the TRISA register are maintained set when using them as analog inputs.

**PORT B and the TRIS B Registers**

PORT B is also an 8 bit bi-directional PORT. Its direction controlled and maintained by TRIS B data direction register. Setting the TRIS B into logic ‘1’ makes the corresponding   “PORT B” pin as an input. Clearing the TRIS B bit make PORT B as an output. Three pins of PORT B are multiplexed with the In-Circuit Debugger and Low-Voltage Programming function: RB3/PGM, RB6/PGC and RB7/PGD for performing its alternate functions.

**PORT C and the TRIS C Registers**

PORT C is an 8-bit wide, bidirectional PORT which controlled and maintained by TRIS C data direction register. Setting a TRIS C bit (= 1) will make the corresponding PORT C pin an input (i.e., put the corresponding output driver in a High-Impedance mode). Clearing a TRIS C bit (= 0) will make the corresponding PORT C pin an output PORT C is also multiplexed with several peripheral functions. PORT C pins have Schmitt Trigger input buffers.

When enabling peripheral functions, more care should be taken in defining TRIS bits for each PORT C pin as compared to other. Some peripherals override the TRIS bit to make a pin an output, while other peripherals override the TRIS bit to make a pin an input. Since the TRIS bit override is in effect while the peripheral is enabled, read-modify write instructions (BSF, BCF, and XORWF) with TRISC as the destination, should be avoided.

**PORT D and TRIS D Registers**

PORT D is an 8-bit PORT with bi-directional nature. This port is also with Schmitt Trigger input buffers, each pin in this PORT D can be individually configurable as either input or output. PORT D can be configured as an 8-bit wide microprocessor PORT (functioning as Parallel Slave PORT) by setting control bit, PSPMODE ((TRISE<4>). In this mode, the input buffers are TTL.

**PORT E and TRIS E Registers**

PORT E has only three pins (RE0/RD/AN5, RE1/WR/AN6 and RE2/CS/AN7) which are individually configurable as inputs or outputs. These pins are controllable by using its corresponding data direction register “TRIS E”. These pins also have Schmitt Trigger input buffers. The PORT E pins become the I/O control inputs for the microprocessor PORT when bit PSPMODE is set. In this mode, the user must make certain that the TRIS E bits are set and the pins are configured as digital inputs. Also, ensure that ADCON1 is configured for digital I/O. In this mode, the input buffers are TTL.

TRISE register which also controls the Parallel Slave PORT operation. PORT E pins are multiplexed with analog inputs. When selected for analog input, these pins will read as ‘0’s. TRIS E controls the direction of the RE pins, even when they are being used as analog inputs. The user must make sure to keep the pins configured as inputs when using them as analog inputs.

**4.2.1.4 MEMORY ORGANISATION:**

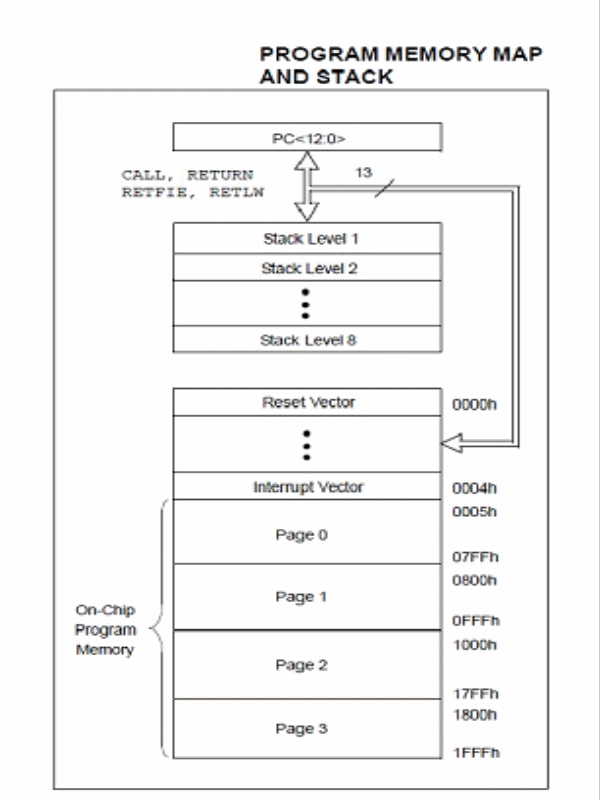
The memory of a PIC 16F877 chip is divided into 3 sections. They are

* + Program memory
  + Data memory
  + Data EEPROM

**Program memory**

Program memory contains the programs that are written by the user. The program counter (PC) executes these stored commands one by one. Usually PIC16F877 devices have a 13 bit wide program counter that is capable of addressing 8K×14 bit program memory space. This memory is primarily used for storing the programs that are written (burned) to be used by the PIC. These devices also have 8K\*14 bits of flash memory that can be electrically erasable /reprogrammed. Each time while writing a new program to the controller, we must delete the old one at that time.

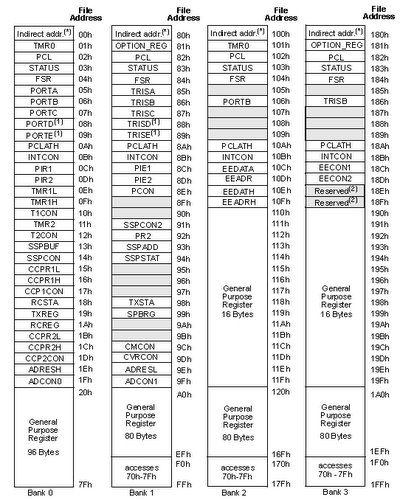
The figure below shows the program memory map and stack.

[](http://www.circuitstoday.com/wp-content/uploads/2011/01/PIC16f877-Program-Memory.gif)

**Fig 4.2.1.4a: PIC16f877A Program Memory**

**Data memory:**

The data memory of PIC16F877 is separated into multiple banks which contain the general purpose registers (GPR) and special function registers (SPR). According to the type of the microcontroller, these banks may vary. The PIC16F877 chip only has four banks (BANK 0, BANK 1, BANK 2, and BANK4). Each bank holds 128 bytes of addressable memory.

[](http://www.circuitstoday.com/wp-content/uploads/2011/01/Data-Memory-Organization.jpg)

**Fig 4.2.1.4b: PIC 16F877A data memory**

The banked arrangement is necessary because there are only 7 bits are available in the instruction word for the addressing of a register, which gives only 128 addresses. The selection of the banks are determined by control bits RP1, RP0 in the STATUS registers Together the RP1, RP0 and the specified 7 bits effectively form a 9 bit address.

The first 32 locations of Banks 1 and 2 and the first 16 locations of Banks2 and 3 are reserved for the mapping of the Special Function Registers (SFR’s).

|  |  |  |
| --- | --- | --- |
| BANK | RP0 | RP1 |
| 0 | 0 | 0 |
| 1 | 1 | 0 |
| 2 | 0 | 1 |
| 3 | 1 | 1 |

**Table 4.2.1.4: Register Bank Access**

A bit of RP1 & RP0 of the STATUS register selects the bank access.

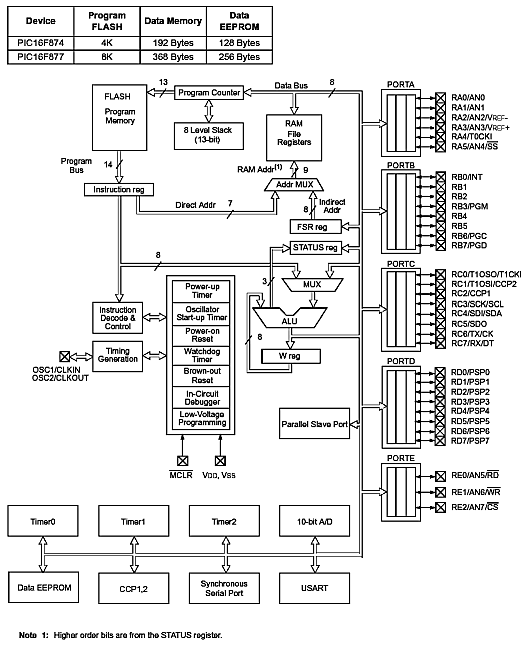
**Data EEPROM and FLASH**

The data EEPROM and Flash program memory is readable and writable during normal operation (over the full VDD range). This memory is not directly mapped in the register file space. Instead, it is indirectly addressed through the Special Function Registers. There are six SFRs used to read and write this memory:

* + - * + EECON1
        + EECON2
        + EEDATA
        + EEDATH
        + EEADR
        + EEADRH

The EEPROM data memory allows single-byte read and writes. The Flash program memory allows single-word reads and four-word block writes. Program memory write operations automatically perform an erase-before write on blocks of four words. A byte write in data EEPROM memory automatically erases the location and writes the new data (erase-before-write). The write time is controlled by an on-chip timer. The write/erase voltages are generated by an on-chip charge pump, rated to operate over the voltage range of the device for byte or word operations.

**4.2.1.5 ARCHITECTURE OF PIC 16F877A**

[](http://www.circuitstoday.com/wp-content/uploads/2011/01/Internal-Architecture-of-PIC16F877A-Chip.gif)

**Fig 4.2.1.5 : Internal Architecture of PIC16F877A Chip**

**4.2.1.6 REGISTERS:**

**4.2.1.6a. GENERAL PURPOSE REGISTERS (GPR)**

GPR is a small amount of storage that can be accessible more quickly than any other memory. These register files can be accessed either directly, or indirectly, through the File Select Register (FSR).

**4.2.1.6b. SPECIAL FUNCTION REGISTERS (SFR)**

The special function registers are also memory registers which is used for special dedicated functions. These registers perform various dedicated functions inside the PIC chip. Each special function inside this PIC chip is controlled by using these registers. These registers are used by the CPU and peripheral modules for controlling the desired operation of the device. These registers are normally implemented as in the form of static RAM memory.

**4.2.1.6c. STATUS REGISTERS**

Status register is an eight bit register that contains the arithmetic status of the arithmetic logic unit (ALU), the reset status and the bank select bits for the data memory. The detailed explanation of status register is given below.

Status registers (address 03h, 83h, 103h, and 183h)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| R/W\*-0 | R/W-0 | R/W-0 | R-1 | R-1 | R/W-x\*\* | R/W-x | R/W-x |
| IRP | RP1 | RP0 | TO | PD | Z | DC | C |

**Table 4.2.1.6c: Status Registers**

(\*R/W-readable/writable, \*\*x-unknown bit)

Bit 7 – (IRP): this is a Register Bank Select Bit usually used for indirect addressing

Bit 6-5 (RP1:RP0): these bits are Register Bank Select bits commonly used for direct addressing mode (each banks in this mode carry 128 byes)

(11 = Bank 3 (180h-1FFh)

10 = Bank 2 (100h-17Fh)

01 = Bank 1 (80h-FFh)

00 = Bank 0 (00h-7Fh))

Bit 4 (TO): this is a time-out bit used for timing and counting, sleep and reset functions.

Bit 3 (PD): Power-down bit

(1 = after power-up or by the CLRWDT instruction

0 = by execution of the SLEEP instruction)

Bit 2 (Z): Zero bit

(1 = the result of an arithmetic or logic operation is zero

0 = the result of an arithmetic or logic operation is not zero.)

Bit 1 (DC): Digit carry/borrow bit (ADDWF, ADDLW, SUBLW, SUBWF instructions)

**4.2.2 LCD DISPLAY**

LCD (Liquid Crystal Display) screen is an electronic display module and find a wide range of applications. A 16x2 LCD display is very basic module and is very commonly used in various devices and circuits. These modules are preferred over seven segments and other multi segment LEDs. The reasons being: LCDs are economical; easily programmable; have no limitation of displaying special & even custom characters(unlike in seven segments), animations and so on.

A **16x2 LCD** means it can display 16 characters per line and there are 2 such lines. In this LCD each character is displayed in 5x7 pixel matrix. This LCD has two registers, namely, Command and Data. The command register stores the command instructions given to the LCD. A command is an instruction given to LCD to do a predefined task like initializing it, clearing its screen, setting the cursor position, controlling display etc. The data register stores the data to be displayed on the LCD. The data is the ASCII value of the character to be displayed on the LCD. Click to learn more about internal structure of a LCD.

****

**Fig 4.2.2 LCD 2x16 DISPLAY**

**Pin Description:**

|  |  |  |
| --- | --- | --- |
| **Pin No** | **Function** | **Name** |
| 1 | Ground (0V) | Ground |
| 2 | Supply voltage; 5V (4.7V – 5.3V) | Vcc |
| 3 | Contrast adjustment; through a variable resistor | VEE |
| 4 | Selects command register when low; and data register when high | Register Select |
| 5 | Low to write to the register; High to read from the register | Read/write |
| 6 | Sends data to data pins when a high to low pulse is given | Enable |
| 7 | 8-bit data pins | DB0 |
| 8 | DB1 |
| 9 | DB2 |
| 10 | DB3 |
| 11 | DB4 |
| 12 | DB5 |
| 13 | DB6 |
| 14 | DB7 |
| 15 | Backlight VCC (5V) | Led+ |
| 16 | Backlight Ground (0V) | Led- |

**Table 4.2.2: LCD pin details**

**4.2.3 GSM INTERFACE**

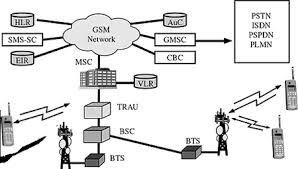
GSM (Global System for Mobile communication) is a digital mobile telephony system that is widely used in Europe and other parts of the world. GSM uses a variation of time division multiple access (TDMA) and is the most widely used of the three digital wireless telephony technologies (TDMA, GSM, and CDMA). GSM digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot. It operates at either the 900 MHz or 1800 MHz frequency band.



**Fig 4.2.3 GSM SIM900**

The **Switching System** (SS) is responsible for performing call processing and subscriber-related functions. The following functional units:

* **Home location register (HLR)**—The HLR is a database used for storage and management of subscriptions. The HLR is considered the most important database, as it stores permanent data about subscribers, including a subscriber's service profile, location information, and activity status. When an individual buys a subscription from one of the PCS operators, he or she is registered in the HLR of that operator.
* **Mobile services switching center (MSC)**—The MSC performs the telephony switching functions of the system. It controls calls to and from other telephone and data systems. It also performs such functions as toll ticketing, network interfacing, common channel signaling, and others.
* **Visitor location register (VLR)**—The VLR is a database that contains temporary information about subscribers that is needed by the MSC in order to service visiting subscribers. The VLR is always integrated with the MSC. When a mobile station roams into a new MSC area, the VLR connected to that MSC will request data about the mobile station from the HLR. Later, if the mobile station makes a call, the VLR will have the information needed for call setup without having to interrogate the HLR each time.
* **Authentication center (AUC)**—A unit called the AUC provides authentication and encryption parameters that verify the user's identity and ensure the confidentiality of each call. The AUC protects network operators from different types of fraud found in today's cellular world.
* **Equipment Identity Register (EIR)**—The EIR is a database that contains information about the identity of mobile equipment that prevents calls from stolen, unauthorized, or defective mobile stations. The AUC and EIR are implemented as stand-alone nodes or as a combined AUC/EIR node.



**Fig 4.2.3.1 GSM Structure**

**CHAPTER 5**

**5. IMPLEMENTATION**

**5.1 CODING**

#include <htc.h>

#include "smcl\_lcd8.h"

#include "AT\_serial.h"

sbit ent=P1^0;

sbit inc=P1^1;

sbit dec=P1^2;

sbit set=P1^2;

unsigned char rc=0,data\_rcv[86],i,fp\_id,fpid1,count=0,chk\_sum,va,k=0;

bit chk0,chk1,chk2;

void fpid(unsigned char val);

void ent\_fpid();

void result();

void fd()

{

Lcd8\_Command(0x01);

// Lcd8\_Display(0x80,"Finger Print ",16);

Lcd8\_Display(0xc0,"Welcome ",16);

}

void display(unsigned char val)

{

switch(val)

{

case 1:

Lcd8\_Display(0xc0,"--Enrl Usr FP.--",16);

break;

case 2:

Lcd8\_Display(0xc0,"--identify FP.--",16);

break;

case 3:

Lcd8\_Display(0xc0,"--Del All FP.---",16);

break;

default:

fd();

break;

}

}

void Serial() interrupt 4

{

if(RI)

{

RI=0;

data\_rcv[rc]=SBUF;

rc++;

}

}

void txs(unsigned char val)

{

Serial\_Out(val);

}

void delay1()

{

long i;

for(i=0;i<50000;i++);

}

void delay2()

{

int i;

for(i=0;i<15000;i++);

}

void delay3(unsigned int del)

{

while(del--);

}

void sendd1()

{

txs('A');txs('T');txs('+');txs('C');txs('M');txs('G');

txs('S');txs('=');

txs('"');

txs('9');txs('7');txs('8');txs('9');

txs('7');txs('2');txs('8');txs('7');txs('9');txs('0');

txs('"');

txs(13); txs(10);

delay3(60000); delay3(60000);delay3(60000); delay3(60000);delay3(60000); delay3(60000);

}

void sms1()

{

sendd1(); delay3(10000);

txs('A');txs('l');txs('e');txs('r');txs('t');

txs(26);

delay3(60000);

delay3(60000);

delay3(60000);

delay3(60000);

delay3(60000);

delay3(60000);

}

unsigned char rxs()

{

int c=0;

while(RI==0)

{

c++;

if(c>25000)

break;

}

RI=0;

return SBUF;

}

void rxmo()

{

char i;

txs('A');txs('T');txs('+');txs('C');txs('M');txs('G');

txs('R');txs('=');txs('1');txs(13); txs(10);

for(i=0;i<86;i++)

{

data\_rcv[i]=rxs();

}

}

void del1()

{

char i;

txs('A');txs('T');txs('+');txs('C');txs('M');txs('G');

txs('D');txs('=');txs('1');txs(13); txs(10);

for(i=0;i<13;i++)

{

data\_rcv[i]=rxs();

}

}

void main()

{

Lcd8\_Init();

EA=1;

SCON=0x50;

PCON=PCON | 0x80;

TMOD=0X20;

TH1=0XFf;

TR1=1;

txs('A');txs('T');txs(13);txs(10);

delay1();

txs('A');txs('T');txs('+');txs('C');txs('M');txs('G');

txs('F');txs('=');txs('1');txs(13);txs(10);

Delay(60000);

del1();

Lcd8\_Display(0x80,"Show Finger ",16);

fd();

Receive(1);

Delay(65000);

for(k=0;k<=80;k++)

{

data\_rcv[k]=0;

}

while(1)

{

if(!inc && !chk0)chk0=1;

if(inc && chk0){count++;if(count>5)count=0;chk0=0;}

if(!ent && !chk1)chk1=1;

if(ent && chk1){chk1=0;fpid(count);}

if(!dec && !chk2)chk2=1;

if(dec && chk2){count--;if(count>5)count=5;chk2=0;}

display(count);

if(rc>10)

{

for(k=0;k<=49;k++) //11

{

Lcd8\_Decimal3(0xc0,data\_rcv[k]);

Delay(6500);

}

Lcd8\_Decimal3(0x80,data\_rcv[49]);//

Lcd8\_Decimal3(0x85,data\_rcv[47]);

Lcd8\_Decimal3(0x8c,rc);

Delay(6500);

result();

rc=count=0;

for(k=0;k<=80;k++)

{

data\_rcv[k]=0;

}

}

}

}

void fpid(unsigned char val)

{

Lcd8\_Display(0xc0,"--Processing.---",16);

for(rc=0;rc<50;rc++)data\_rcv[rc]=0;

rc=0;

switch(val)

{

case 1:

ent\_fpid(); Serial\_Conout("\xEF\x01\xFF\xFF\xFF\xFF\x01\x00\x03\x01\x00\x05",12);

Delay(65000);Delay(65000); Serial\_Conout("\xEF\x01\xFF\xFF\xFF\xFF\x01\x00\x04\x02\x01\x00\x08",13);

Delay(65000);Delay(65000); Serial\_Conout("\xEF\x01\xFF\xFF\xFF\xFF\x01\x00\x03\x01\x00\x05",12);

Delay(65000);Delay(65000); Serial\_Conout("\xEF\x01\xFF\xFF\xFF\xFF\x01\x00\x04\x02\x02\x00\x09",13);

Delay(65000);Delay(65000); Serial\_Conout("\xEF\x01\xFF\xFF\xFF\xFF\x01\x00\x03\x05\x00\x09",12);

Delay(5000); Serial\_Conout("\xEF\x01\xFF\xFF\xFF\xFF\x01\x00\x06\x06\x02",11);

Serial\_Out(0);

Serial\_Out(fp\_id);

chk\_sum=fp\_id+15;

Serial\_Out(0);

Serial\_Out(chk\_sum);

Delay(65000);Delay(65000);Delay(65000) ;

i=1;

break;

case 2: Serial\_Conout("\xEF\x01\xFF\xFF\xFF\xFF\x01\x00\x03\x01\x00\x05",12); //read or search

Delay(65000);Delay(65000);Delay(40000);//Delay(30000);

Serial\_Conout("\xEF\x01\xFF\xFF\xFF\xFF\x01\x00\x04\x02\x01\x00\x08",13);//read

Delay(40000);Delay(20000);//Delay(10000);

Serial\_Conout("\xEF\x01\xFF\xFF\xFF\xFF\x01\x00\x08\x1b\x01\x00\x00\x01\x01\x00\x27",17);//read

Delay(65000);Delay(65000);i=2;

break;

case 3://EF 01 FF FF FF FF 01 00 03 0D 00 11

Serial\_Conout("\xEF\x01\xFF\xFF\xFF\xFF\x01\x00\x03\x0D\x00\x11",12);

i=4;

break;

default:

break;

}

fd();

}

void ent\_fpid()

{

Lcd8\_Display(0x80,"Enter ID No: 000",16);

fp\_id=0;

while(ent)

{ if(!inc){while(!inc);fp\_id++;if(fp\_id>=255)fp\_id=0;Lcd8\_Decimal3(0x8D,fp\_id);}

if(!dec){while(!dec);fp\_id--;if(fp\_id>=255)fp\_id=255;Lcd8\_Decimal3(0x8D,fp\_id);}

}

}

void result()

{

char flg=0,hbt=0,hbtt=0,hb=0,f1=0;

Lcd8\_Command(0x01);

Delay(65000);

if(i==1)

{ if((data\_rcv[69]==0x00)&&(rc>70))

{

Lcd8\_Display(0xC0," Success ",16);

}

else if(data\_rcv[69]==0x02)

{

Lcd8\_Display(0x80," No Finger ",16);

}

else

{

Lcd8\_Display(0xC0," Not Success ",16);

}

i=0;

}

else if(i==2)

{

if((data\_rcv[33]==0x00)&&(data\_rcv[35]!=0))

{

Lcd8\_Display(0x80," Success ",16);

Lcd8\_Display(0xc0," Finger ID: ",16);

Lcd8\_Decimal3(0xcb,data\_rcv[35]);

Lcd8\_Display(0x80,"IR SENSOR ",16);

while(P0\_6==1)

{

}

while(1)

{

// Lcd8\_Display(0x80,"Vibration ",16);

//while(P3\_5==1)

//{

//}

Lcd8\_Display(0xc0,"ALCOHOL CHECK ",16);

if(P0\_7==1)

{

Lcd8\_Display(0xc0,"ALCOHOL DETECTED ",16);

sms();

while(1);

}

if(P0\_5==1)

{

if(flg==0)

if(hbt<100)

{

hbt++;

flg=1;

}

}

if(P0\_5==0)

{

flg=0;

}

hb++;

if(hb==120)

{

hbtt=hbt\*3;

hbt=0;

hb=0;

}

Lcd8\_Command(0x80);

Lcd8\_Write(0x80,'H');

Lcd8\_Write(0x81,'e');

Lcd8\_Write(0x82,'a');

Lcd8\_Write(0x83,'r');

Lcd8\_Write(0x84,'t');

Lcd8\_Write(0x85,' ');

Lcd8\_Write(0x86,'B');

Lcd8\_Write(0x87,'t');

Lcd8\_Write(0x88,'=');

Lcd8\_Write(0x89,((hbtt/100)+0x30));

Lcd8\_Write(0x8a,(((hbtt%100)/10)+0x30));

Lcd8\_Write(0x8B,((hbtt%10)+0x30));

Lcd8\_Write(0x8c,' ');

Lcd8\_Write(0x8d,((hbt/100)+0x30));

Lcd8\_Write(0x8E,(((hbt%100)/10)+0x30));

Lcd8\_Write(0x8F,((hbt%10)+0x30));

if(hbtt>10)

{

if(hbtt<50)

{

if(f1==0)

{

sms();

P0\_1=0;

f1=1;

}

}

else

{

f1=0;

P0\_1=1;

}

}

}

}

else //if(data\_rcv[33]==0x09)

{

sms1();

P0\_0=0;

Lcd8\_Display(0x80,"Not Find Finger ",16);

ES=0;

while(1)

{

rxmo();

delay1();

delay1();

Lcd8\_Write(0xc0,data\_rcv[72]);

Lcd8\_Write(0xc1,data\_rcv[73]);

Lcd8\_Write(0xc2,data\_rcv[74]);

Lcd8\_Write(0xc3,data\_rcv[75]);

Lcd8\_Write(0xc4,data\_rcv[76]);

Lcd8\_Write(0xc5,data\_rcv[77]);

Lcd8\_Write(0xc6,data\_rcv[78]);

Lcd8\_Write(0xc7,data\_rcv[79]);

Lcd8\_Write(0xc8,data\_rcv[80]);

Lcd8\_Write(0xc9,data\_rcv[81]);

Lcd8\_Write(0xcA,data\_rcv[82]);

Lcd8\_Write(0xcB,data\_rcv[83]);

Lcd8\_Write(0xcC,data\_rcv[84]);

Lcd8\_Write(0xcD,data\_rcv[85]);

if(data\_rcv[75]=='H')

{

del1();

delay1();

Lcd8\_Display(0x80,"IR SENSOR ",16);

while(P0\_6==1)

{

}

while(1)

{

// Lcd8\_Display(0x80,"Vibration ",16);

//while(P3\_5==1)

//{

//}

Lcd8\_Display(0xc0,"ALCOHOL CHECK ",16);

if(P0\_7==1)

{

Lcd8\_Display(0xc0,"ALCOHOL DETECTED ",16);

sms();

while(1);

}

if(P0\_5==1)

{

if(flg==0)

if(hbt<100)

{

hbt++;

flg=1;

}

}

if(P0\_5==0)

{

flg=0;

}

hb++;

if(hb==120)

{

hbtt=hbt\*3;

hbt=0;

hb=0;

}

Lcd8\_Command(0x80);

Lcd8\_Write(0x80,'H');

Lcd8\_Write(0x81,'e');

Lcd8\_Write(0x82,'a');

Lcd8\_Write(0x83,'r');

Lcd8\_Write(0x84,'t');

Lcd8\_Write(0x85,' ');

Lcd8\_Write(0x86,'B');

Lcd8\_Write(0x87,'t');

Lcd8\_Write(0x88,'=');

Lcd8\_Write(0x89,((hbtt/100)+0x30));

Lcd8\_Write(0x8a,(((hbtt%100)/10)+0x30));

Lcd8\_Write(0x8B,((hbtt%10)+0x30));

Lcd8\_Write(0x8c,' ');

Lcd8\_Write(0x8d,((hbt/100)+0x30));

Lcd8\_Write(0x8E,(((hbt%100)/10)+0x30));

Lcd8\_Write(0x8F,((hbt%10)+0x30));

if(hbtt>10)

{

if(hbtt<50)

{

if(f1==0)

{

sms();

P0\_1=0;

f1=1;

}

}

else

{

f1=0;

P0\_1=1;

}

}

}

}

if(data\_rcv[85]=='H')

{

del1();

delay1();

Lcd8\_Display(0x80,"IR SENSOR ",16);

while(P0\_6==1) { }

while(1)

{

// Lcd8\_Display(0x80,"Vibration ",16);

//while(P3\_5==1)

//{

//}

Lcd8\_Display(0xc0,"ALCOHOL CHECK ",16);

if(P0\_7==1)

{

Lcd8\_Display(0xc0,"ALCOHOL DETECTED ",16);

sms();

while(1);

}

if(P0\_5==1)

{

if(flg==0)

if(hbt<100)

{

hbt++;

flg=1;

}

}

if(P0\_5==0)

{

flg=0;

}

hb++;

if(hb==120)

{

hbtt=hbt\*3;

hbt=0;

hb=0;

}

Lcd8\_Command(0x80);

Lcd8\_Write(0x80,'H');

Lcd8\_Write(0x81,'e');

Lcd8\_Write(0x82,'a');

Lcd8\_Write(0x83,'r');

Lcd8\_Write(0x84,'t');

Lcd8\_Write(0x85,' ');

Lcd8\_Write(0x86,'B');

Lcd8\_Write(0x87,'t');

Lcd8\_Write(0x88,'=');

Lcd8\_Write(0x89,((hbtt/100)+0x30));

Lcd8\_Write(0x8a,(((hbtt%100)/10)+0x30));

Lcd8\_Write(0x8B,((hbtt%10)+0x30));

Lcd8\_Write(0x8c,' ');

Lcd8\_Write(0x8d,((hbt/100)+0x30));

Lcd8\_Write(0x8E,(((hbt%100)/10)+0x30));

Lcd8\_Write(0x8F,((hbt%10)+0x30));

if(hbtt>10)

{

if(hbtt<50)

{

if(f1==0)

{

sms();

P0\_1=0;

f1=1;

}

}

else

{

f1=0;

P0\_1=1;

}

}

}

}

}

}

// Serial\_Init(9600);

i=0;

}

else if(i==3)

{

if(data\_rcv[9]==0x00)

{

// Lcd8\_Display(0x80," Finger Id ",16);

Lcd8\_Display(0xc0," Deleted ",16);

}

else if(data\_rcv[9]==0x10)

{

// Lcd8\_Display(0xC0,"Fail To delete ",16);

// Lcd8\_Display(0xc0," Finger Id ",16);

}

else if(data\_rcv[9]==0x01)

{

// Lcd8\_Display(0x80,"Receiving ",16);

Lcd8\_Display(0xc0," Error ",16);

}

i=0;

}

else if(i==4)

{

if(data\_rcv[9]==0x00)

{

Lcd8\_Display(0xc0," Deleted ",16);

}

else if(data\_rcv[9]==0x11)

{

// Lcd8\_Display(0x80,"Fail To delete ",16);

// Lcd8\_Display(0xc0,"Finger Id's ",16);

}

else if(data\_rcv[9]==0x01)

{

// Lcd8\_Display(0x80,"Receiving ",16);

// Lcd8\_Display(0xc0," Error ",16);

}

i=0;

}

else if(i==5)

{

va=data\_rcv[49]-data\_rcv[47];

Lcd8\_Decimal3(0xcA,va);

Delay(65000);Delay(65000);

//if(va==0x0c||va==12)

if(data\_rcv[45]==0x00&&va==12)

{

// Lcd8\_Display(0x80,"Matching ",16);

Lcd8\_Display(0xc0," Success ",16);

}

else if(va==13)

{

//Lcd8\_Display(0x80,"Receiving ",16);

Lcd8\_Display(0xc0," Error ",16);

}

else

{

//Lcd8\_Display(0x80,"Matching ",16);

Lcd8\_Display(0xc0," Not Success ",16);

P3\_7=1;

P3\_5=0;

P0=0;

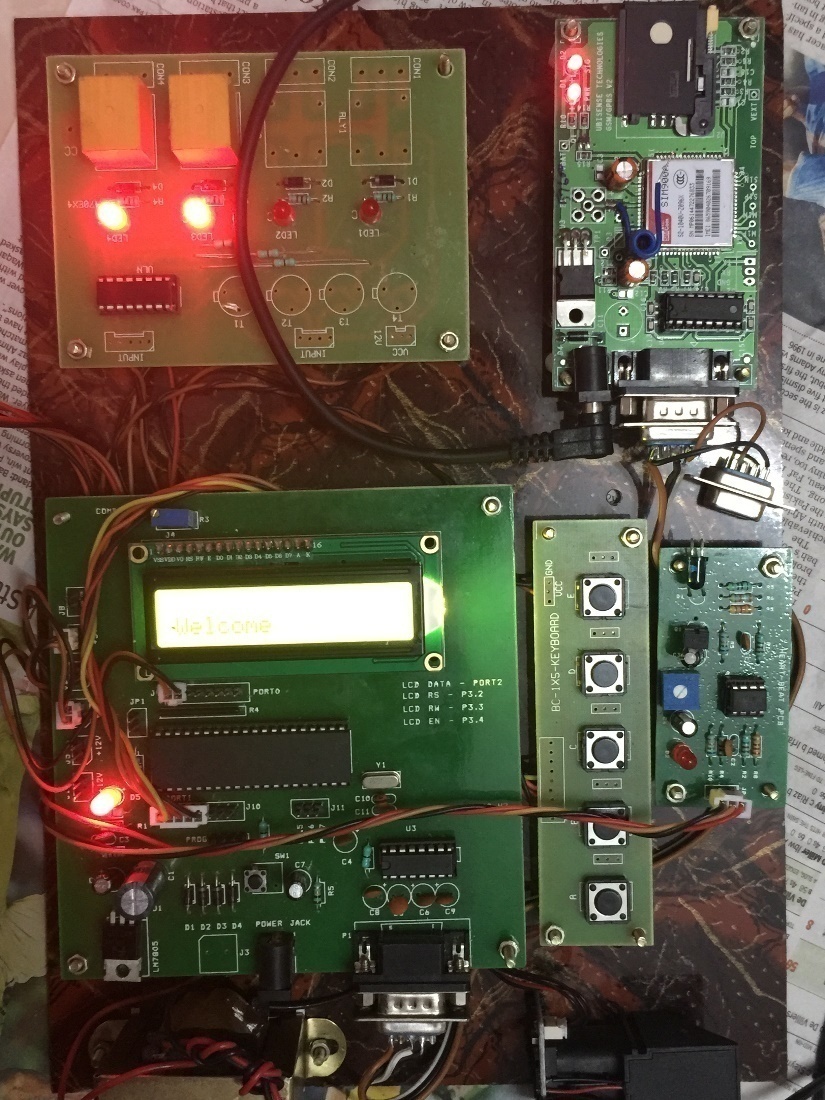
} i=0;

}

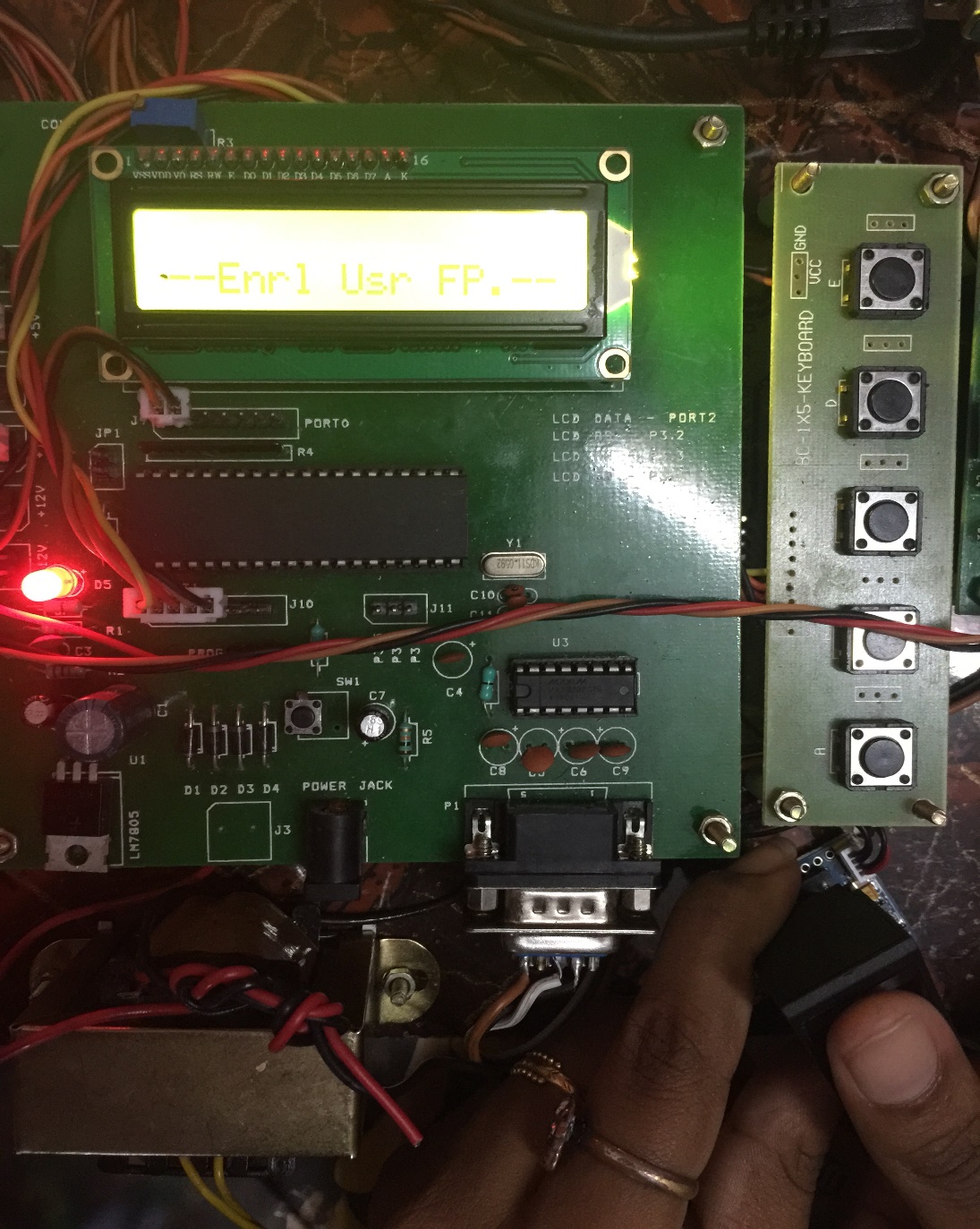
Delay(6500);

}

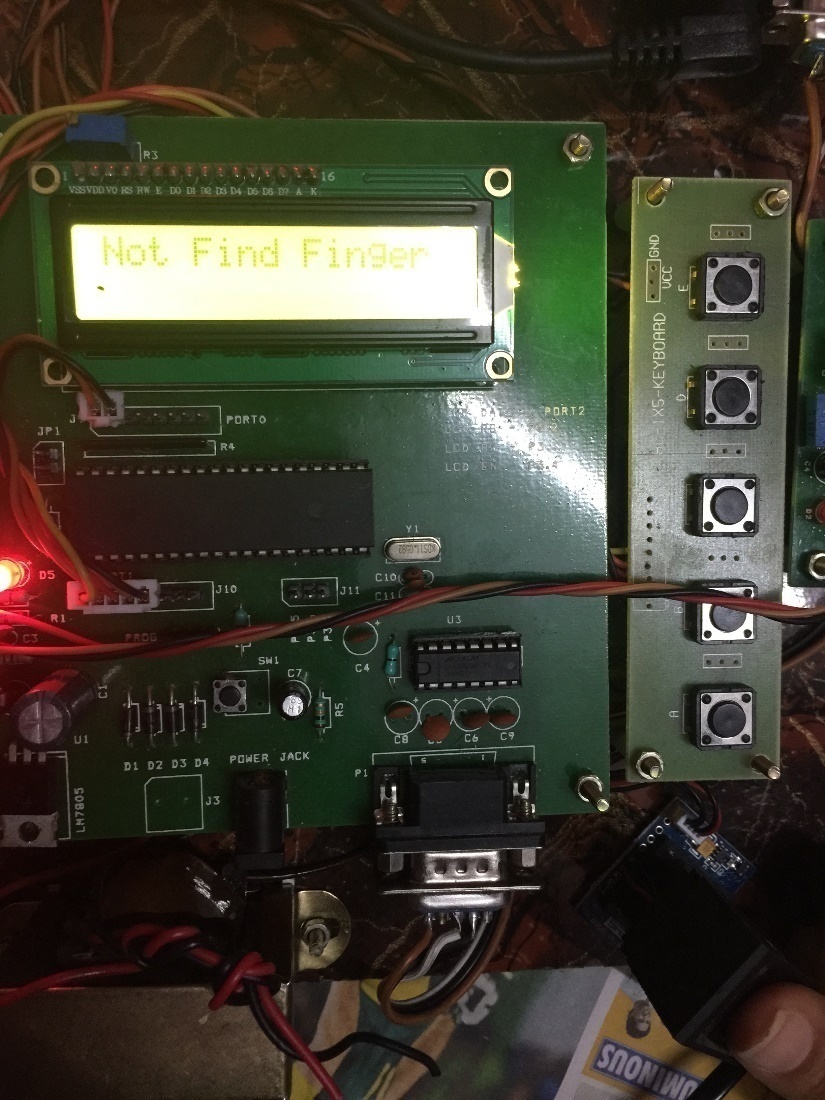
**5.2 SNAPSHOTS**

****

**Fig 5.2 Overview of kit**

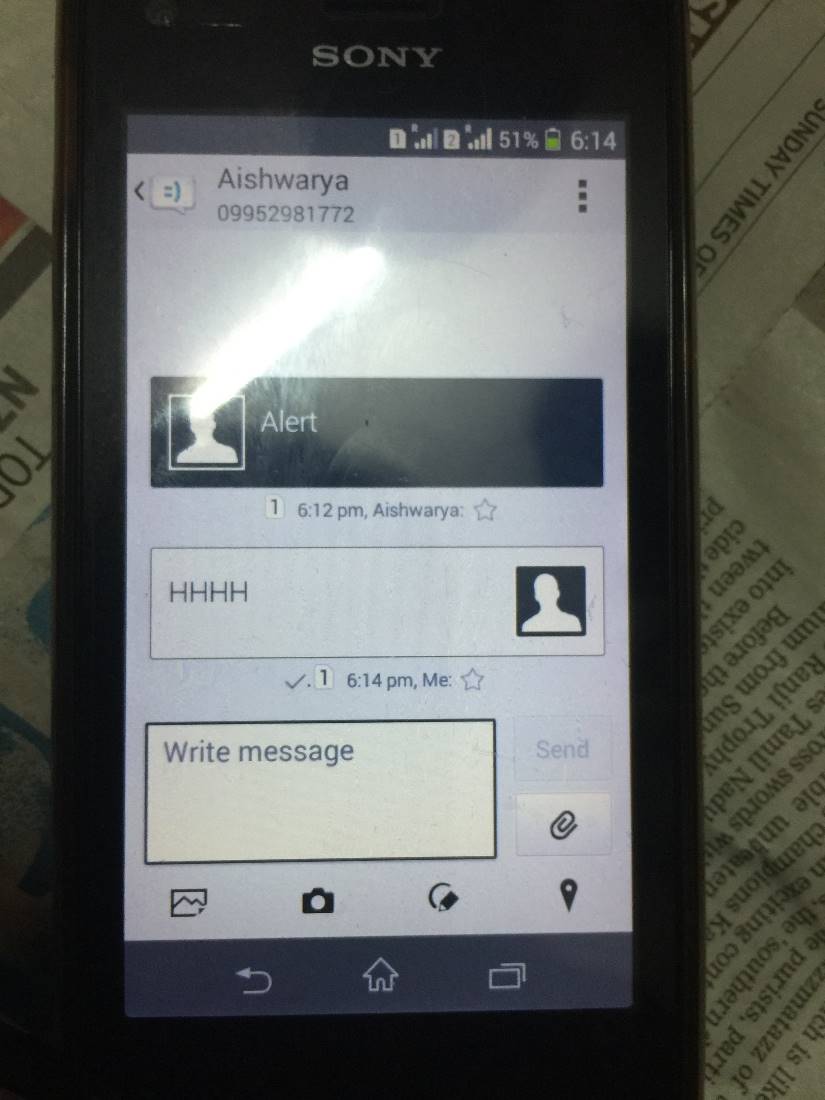
****

**Fig 5.2.1 Enroll Fingerprint**

****

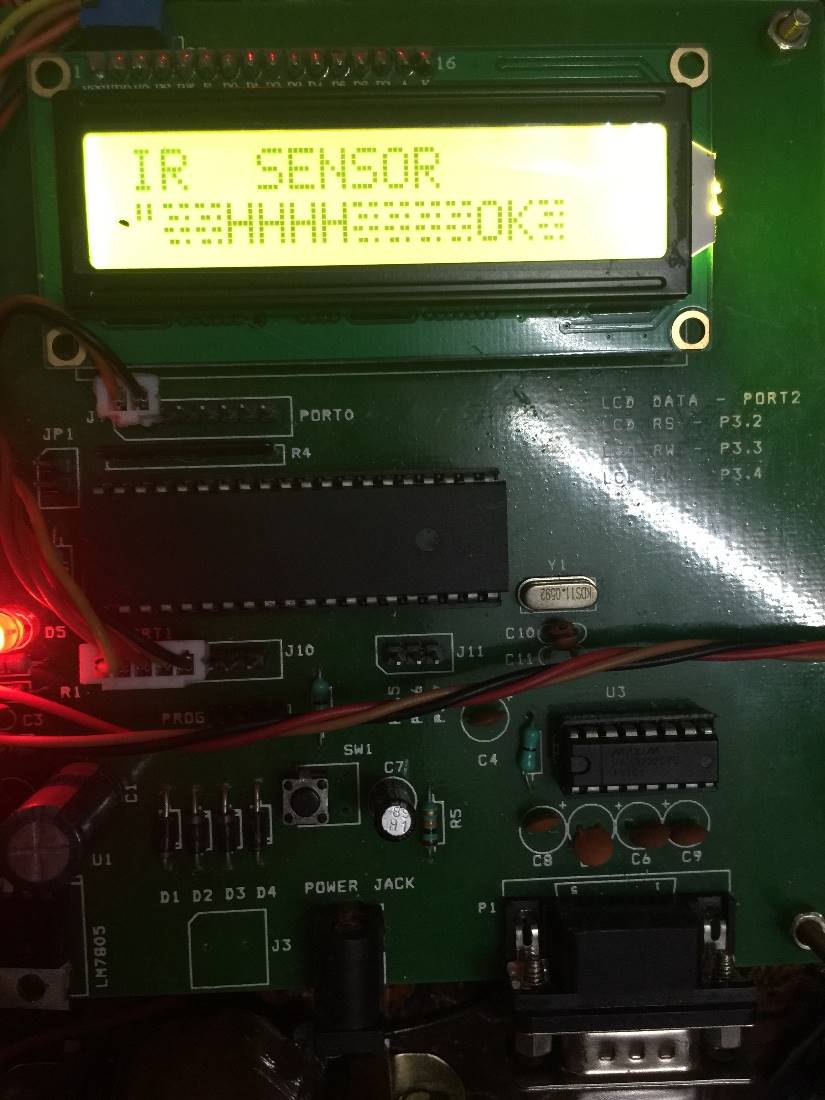
****

**Fig 5.2.2 Unauthorized fingerprint**

****

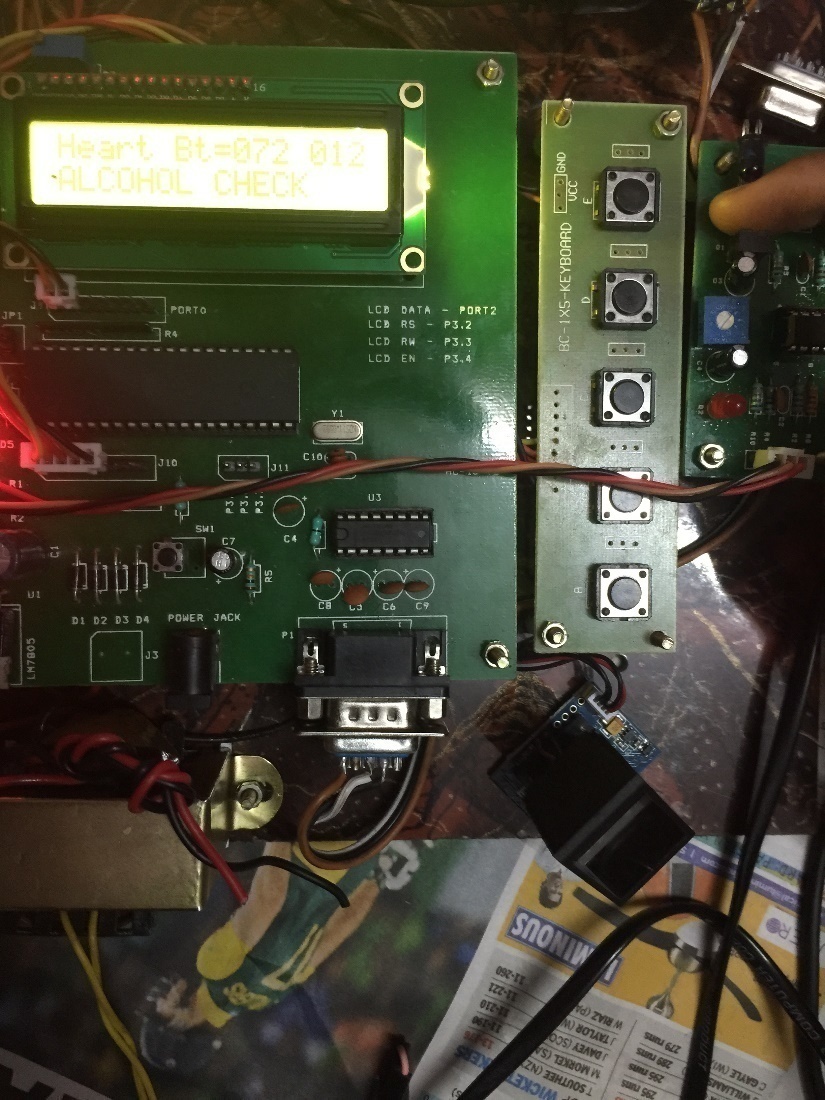
****

**Fig 5.2.3 Granting access**

****

****

**Fig 5.2.4 IR Sensor**

****

**Fig 5.2.5 Heart Beat Check**

**CHAPTER 6**

**6. CONCLUSION**

By the realization of the above proposed system one can learn many aspects of a digital electronics circuit. It gives the complete knowledge of designing microcontroller based system and developing embedded software. Thus fingerprint identification and reversible GSM technique enhances the security of a vehicle makes it possible only for some selected people to start the car. Thus by implementing this relatively cheap and easily available system on a car one can ensure much greater security and exclusively than that offered by a conventional lock and key. The reliability of any automatic fingerprint system strongly relies on the precision obtained in the minutia extraction process. As this system also provides a sensor for the heartbeat check throughout driving, it becomes a very useful system for all prepaid cabs which are one of the biggest needs in today's generation. It also encapsulates the passenger's safety.

**6.1 FUTURE ENHANCEMENT**

There is a scope for future enhancement in terms of efficiency and accuracy which can be achieved by improving the hardware to capture the image or by improving the image enhancement techniques. Also that an enhancement can be made by notifying the nearby police station in case of theft and the nearby hospitals in case of accidents.

**CHAPTER 7**

**7. REFERENCES**

1. Shenglin Yang , Ingrid M. Verbauwhede, UCLA Dept. of EE /2003

2. Koichi Ito, Ayumi Morita, Takafumi Aoki, Tatuso Higuchi, Hiroshi Nakajima, Koji Kobayashi/ 2005

3. Yen wang, Hong liu, Jun feng/ 2009

4. Omidiora E. O. , Fakolujo O. A. , Arulogun O. T. , Aborisade D. O. / 2010

5. N. Kiruthiga1 and L. Latha2 M.E /2010

6. Jiwa Abdullah /2011

7. Jayapriya.P, 2Prof. Prabhakaran.S, 3Ashok T.1ME-EST, Assistant Professor Nandha Engineering College, Erode. /2012

8. Hnin Pwint Han, Hla Myo Tun /2012

9. Subhani SK.M, Sateesh G.N.V, Chaitanya C.H, Prakash Babu C. / 2013

10. Ajinkya Kawale / 2013