

Fingerprint Based Biometric ATM Authentication System

Dhiraj Sunehra

Department of Electronics & Communication Engineering, Jawaharlal Nehru Technological University Hyderabad, India

Abstract: Biometrics technology is rapidly progressing and offers attractive opportunities. In recent years, biometric authentication has grown in popularity as a means of personal identification in ATM authentication systems. The prominent biometric methods that may be used for authentication include fingerprint, palmprint, handprint, face recognition, speech recognition, dental and eye biometrics. In this paper, a microcontroller based prototype of ATM cashbox access system using fingerprint sensor module is implemented. An 8-bit PIC16F877A microcontroller developed by Microchip Technology is used in the system. The necessary software is written in Embedded 'C' and the system is tested.

Keywords: Automatic Teller Machine, PIC16 microcontroller, Finger print recognition, Liquid Crystal Display

I. INTRODUCTION

Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. Biometric-based solutions are able to provide for confidential financial transactions and personal data privacy. The various features used are face, fingerprints, hand geometry, handwriting, iris, retina, vein and voice [1]. Fingerprinting or finger-scanning technologies are the oldest of the biometric sciences and utilize distinctive features of the fingerprint to identify or verify the identity of individuals. Finger-scan technology is the most commonly deployed biometric technology, used in a broad range of physical access and logical access applications. All fingerprints have unique characteristics and patterns. A normal fingerprint pattern is made up of lines and spaces. These lines are called ridges while the spaces between the ridges are called valleys. It is through the pattern of these ridges and valleys that a unique fingerprint is matched for verification and authorization. These unique fingerprint traits are termed "minutiae" and comparisons are made based on these traits [2]. On average, a typical live scan produces 40 "minutiae". The Federal Bureau of Investigation (FBI) has reported that no more than 8 common minutiae can be shared by two individuals.

1.1 Finger Scan Technology

There are five stages involved in finger-scan verification and identification. Fingerprint (FP) image acquisition, image processing, and location of distinctive characteristics, template creation and template matching [3]. A scanner takes a mathematical snapshot of a user's unique biological traits. This snapshot is saved in a fingerprint database as a minutiae file. The first challenge facing a finger-scanning system is to acquire high-quality image of a fingerprint. The standard for forensic-quality fingerprinting is images of 500 dots per inch (DPI). Image acquisition can be a major challenge for finger-scan developers, since the quality of print differs from person to person and from finger to finger. Some populations are more likely than others to have faint or difficult-to-acquire fingerprints, whether due to wear or tear or physiological traits. Taking an image in the cold weather also can have an affect. Oils in the finger help produce a better print. In cold weather, these oils naturally dry up. Pressing harder on the platen (the surface on which the finger is placed, also known as a scanner) can help in this case.

Image processing is the process of converting the finger image into a usable format. This results in a series of thick black ridges (the raised part of the fingerprint) contrasted to white valleys. At this stage, image features are detected and enhanced for verification against the stored minutia file. Image enhancement is used to reduce any distortion of the fingerprint caused by dirt, cuts, scars, sweat and dry skin [3]. The next stage in the fingerprint process is to locate distinctive characteristics. There is a good deal of information on the average fingerprint and this information tends to remain stable throughout one's life. Fingerprint ridges and valleys form distinctive patterns, such as swirls, loops, and arches. Most fingerprints have a core, a central point around which swirls, loops, or arches are curved. These ridges and valleys are characterized by irregularities known as minutiae, the distinctive feature upon which finger-scanning technologies are based. Many types of minutiae exist, a common one being ridge endings and bifurcation, which is the point at which one ridge divides into two. A typical finger-scan may produce between 15 and 20 minutiae. A template is then created. This is accomplished by mapping minutiae and filtering out distortions and false minutiae. For example, anomalies caused by scars, sweat, or dirt can appear as minutiae. False minutiae must be filtered out before a template is

created and is supported differently with vendor specific proprietary algorithms. The tricky part is comparing an enrollment template to a verification template. Positions of a minutia point may change by a few pixels, some minutiae will differ from the enrollment template, and false minutiae may be seen as real. Many finger-scan systems use a smaller portion of the scanned image for matching purposes. One benefit of reducing the comparison area is that there is less chance of false minutiae information, which would confuse the matching process and create errors.

II. LITERATURE REVIEW

Most finger-scan technologies are based on minutiae. Samir Nanavati [3] states that 80 percent of finger-scan technologies are based on minutiae matching but that pattern matching is a leading alternative. This technology bases its feature extraction and template generation on a series of ridges, as opposed to discrete points. The use of multiple ridges reduces dependence on minutiae points, which tend to be affected by wear and tear [4]. The downside of pattern matching is that it is more sensitive to the placement of the finger during verification and the created template is several times larger in byte size.

Finger-scan technology is proven and capable of high levels of accuracy. There is a long history of fingerprint identification, classification and analysis. This along with the distinctive features of fingerprints has set the finger-scan apart from other biometric technologies. There are physiological characteristics more distinctive than the fingerprint (the iris and retina, for example) but automated identification technology capable of leveraging these characteristics have been developed only over the past few years. The technology has grown smaller, more capable and with many solutions available. Devices slightly thicker than a coin and an inch square in size are able to capture and process images. Additionally, some see the large number of finger-scan solutions available today as a disadvantage; many see it as an advantage by ensuring marketplace competition which has resulted in a number of robust solutions for desktop, laptop, physical access, and point-of-sale environments. Biometric data are separate and distinct from personal information. Biometric templates cannot be reverse-engineered to recreate personal information and they cannot be stolen and used to access personal information [5].

III. METHODOLOGY

3.1 Methodology Used

An embedded system is a combination of software and hardware to perform a dedicated task. Some of the main devices used in embedded products are microprocessors and microcontrollers. In this paper a fingerprint based ATM cashbox accessing system using PIC microcontroller is implemented. Microcontroller forms the controlling module and it is the heart of the device. Initially we store the fingerprint of bank manager and that will be verified with the fingerprint that we are giving when the time of authentication. If both the fingerprints are matched then ATM cashbox will open, otherwise buzzer will give alarm. The task related instructions are loaded into the PIC microcontroller which is programmed using Embedded C language. The system consists of Microcontroller Unit, Fingerprint module, LED indicators and a buzzer alarm system and microcontroller that collect data from the fingerprint module. As it is based on the fingerprint authentication there is no chance of disclosing of password or pin to the third parties.

3.2 Advantages and Limitations

One advantage of finger-scan technology is accuracy. Identical matches are nearly impossible since fingerprints contain a large amount of information making it unlikely that two fingerprints would be identical. Fingerprint technology has another advantage offered by technology; the size of the memory required to store the biometric template is fairly small. There are some weaknesses to finger-scanning, most of which can be mitigated. There is a fraction of the population that is unable to be enrolled. There are certain ethnic groups that have lower quality fingerprints than the general populations. Testing has shown that elderly populations, manual laborers, and some Asian populations are more difficult to be enrolled in some finger-scanning systems [3]. Another problem is that over time, sometimes in as short a period as few months, the fingerprint characteristics of an individual can change, making identification and verification difficult. This problem is seen with manual workers who work extensively with their hands. There are also privacy issues attached to finger-scanning technologies. Some fear that finger-scans may be used to track a person's activities. Others fear that data collected may be improperly used for forensic purposes. Paying with a government meal card at checkout instead of with cash would identify the student as a program recipient. The solution was for the school to provide students the option of using a finger-scan peripheral to purchase meals [3]. At the end of each month, a bill is sent to their parents for payment or to the free food program for reconciliation.

IV. SYSTEM DESCRIPTION

The block diagram of the proposed system and design aspects of independent modules are considered. Hardware is essential to any embedded system. Figure 1 shows the block diagram of the fingerprint based ATM authentication system. The main blocks of this system are: (i) Regulated Power Supply, (ii) PIC 16F877A Microcontroller, (iii) Fingerprint Module, (iv) Liquid Crystal Display, (v) DC Motor and Driver Circuit, (vi) Buzzer.

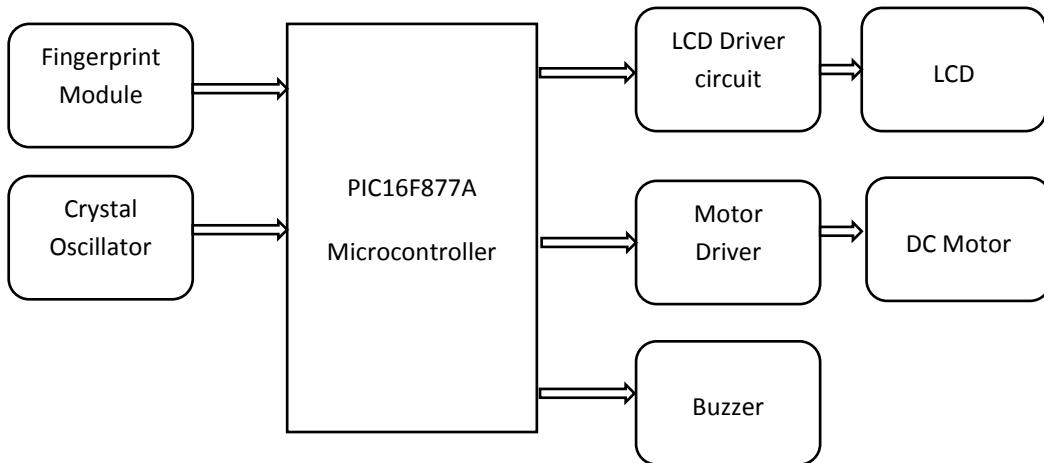


Fig. 1 Block diagram of Fingerprint based ATM cashbox authentication system

4.1 Power supply unit

The power supply section is required to convert AC signal to DC signal and also to reduce the amplitude of the signal. The available voltage signal from the mains is 230V/50Hz which is an AC voltage, but the required is DC voltage (no frequency) with the amplitude of +5V and +12V for various applications.

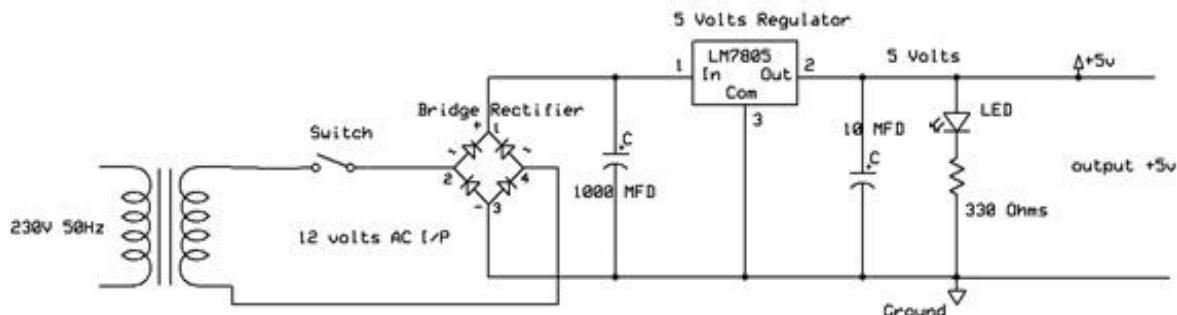


Fig. 2 Power supply section

The components used in the power supply unit are: step down transformer, bridge rectifier, capacitor filter, voltage regulator (IC 7805), $330\ \Omega$ resistor and LED. Bridge rectifier is available in IC form (IC DB107). In the present project IC bridge rectifier is used. This device is ideal for use with printed circuit boards. Electronic filters are electronic circuits, which perform signal-processing functions, specifically to remove unwanted frequency components from the signal, to enhance wanted ones. Here a $1000\ \mu\text{F}$ capacitor filter is used. The process of converting a varying voltage to a constant regulated voltage is called as regulation. For the process of regulation we use voltage regulators. A voltage regulator with only three terminals appears to be a simple device, but it is in fact a very complex integrated circuit. It converts a varying input voltage into a constant ‘regulated’ output voltage. Voltage Regulators are available in a variety of outputs like 5V, 6V, 9V, 12V and 15V. IC LM 7805 regulator is used.

4.2 PIC 16F877A microcontroller

PIC stands for Peripheral Interface Controller given by Microchip Technology to identify its single-chip microcontrollers. These devices have been very successful in 8-bit microcontrollers. The main reason is that Microchip Technology has continuously upgraded the device architecture and added needed peripherals to

the microcontroller to suit customers' requirements. The popularity of the PIC microcontrollers is due to the following factors [6,7]:

1. Speed: Harvard Architecture, RISC architecture, 1 instruction cycle = 4 clock cycles.
2. Instruction set simplicity: The instruction set consists of just 35 instructions (as opposed to 111 instructions for 8051).
3. Power-on-reset and brown-out reset. Brown-out-reset means when the power supply goes below a specified voltage (say 4V), it causes PIC to reset; hence malfunction is avoided. A watch dog timer (user programmable) resets the processor if the software/program ever malfunctions and deviates from its normal operation.
4. PIC microcontroller has four optional clock sources.
 - Low power crystal
 - Mid-range crystal
 - High range crystal
 - RC oscillator (low cost).
5. Programmable timers and on-chip ADC.
6. Up to 12 independent interrupt sources.
7. Powerful output pin control (25 mA (max.) current sourcing capability per pin.)
8. EPROM/OTP/ROM/Flash memory option.
9. I/O port expansion capability.

PIC16F877 is a 40 pin microcontroller. It has 5 ports port A, port B, port C, port D, port E. All the pins of the ports are for interfacing input output devices. The crystal oscillator speed that can be connected to the PIC microcontroller range from DC to 20MHz [7]. Using the CCS 'C' compiler normally 20MHz oscillator will be used and the price is relatively cheaper. The 20 MHz crystal oscillator should be connected with about 22pF capacitor.

4.3 Fingerprint module

Fingerprint processing includes two parts: fingerprint enrollment and fingerprint matching (the matching can be 1:1 or 1:N). When enrolling, user needs to enter the finger two times. The system will process the two time finger images, generate a template of the finger based on processing results and store the template. When matching, user enters the finger through optical sensor and system will generate a template of the finger and compare it with templates of the finger library. For 1:1 matching, system will compare the live finger with specific template designated in the module; for 1:N matching, or searching, system will search the whole finger library for the matching finger. In both circumstances, system will return the matching result, success or failure.

4.4 Serial Communication

When the Fingerprint (FP) module communicates with user device, definition of J1 is given in Table 1.

4.4.1 Hardware Connection

The fingerprint module may communicate via serial interface, with MCU of 3.3V or 5V power: TD (pin 2 of P1) connects with RXD (receiving pin of MCU), RD (pin3 of P1) connects with TXD (transferring pin of MCU). Should the upper computer (PC) be in RS-232 mode, please add level converting circuit, like MAX232, between the module and PC.

Table 1 Pin configuration of Serial interface

| Pin number | Name | Type | Function Description |
|-------------------|-------------|-------------|---|
| 1 | Vin | IN | Power input |
| 2 | TD | IN | Data Output, TTL Logic Level |
| 3 | RD | OUT | Data Input, TTL Logic Level |
| 4 | NC | --- | Not Connected |
| 5 | NC | --- | Not Connected |
| 6 | GND | --- | Signal Ground Connected To Power Ground |

4.4.2 Serial Communication Protocol

The mode is semi-duplex asynchronous serial communication. The default baud rate is 57600 bps. The user may set the baud rate between 9600~115200bps. Transferring frame format is 10 bit: the low-level starting bit, 8-bit data with the LSB first, and an ending bit. There is no check bit. The data format is shown in Fig. 3. To address demands of different customer, module system provides abundant resources at users use.

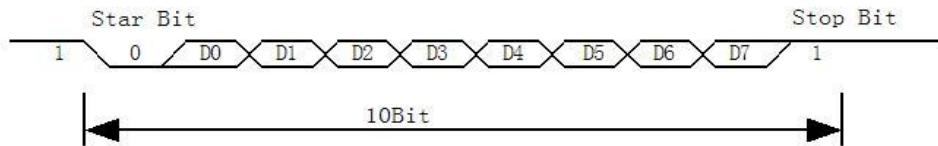


Fig. 3 Serial communication data format

4.5 Buffer

There is an image buffer and two 512-byte character-file buffer within the RAM space of the module. Users can read and write any of the buffers by instructions. Image buffer serves for image storage and the image format is 256*288 pixels. When transferring through UART, to quicken speed, only the upper 4 bits of the pixel is transferred (that is 16 grey degrees). And the two adjacent pixels of the same row will form a byte before the transferring. When uploaded to PC, the 16-grey-degree image will be extended to 256-grey-degree format. i.e. 8-bit BMP format. When transferring through USB, the image is 8-bit pixel, that's 256 grey degrees. Character file buffer, CharBuffer1, CharBuffer2 can be used to store both character file and template file.

4.6 Fingerprint Library

System sets aside certain space within flash for fingerprint template storage, that's the fingerprint library. The contents of the library remain at power off. The capacity of the library changes with the capacity of flash, system will recognize the latter automatically. Fingerprint template's storage in flash is in sequential order. Assume the fingerprint capacity N, then the serial number of template in library is 0,1,2,3...N. The user can only access library by template number.

4.7 Liquid Crystal Display

Figure 4 shows a schematic diagram of a basic 16 × 2 character display. The LCD requires 3 control lines as well as either 4 or 8 I/O lines for the data bus. The user may select whether the LCD is to operate with a 4-bit data bus or an 8-bit data bus. If a 4-bit data bus is used the LCD will require a total of 7 data lines (3 control lines plus the 4 lines for the data bus). If an 8-bit data bus is used the LCD will require a total of 11 data lines (3 control lines plus the 8 lines for the data bus). The three control lines are referred to as Enable (EN), Register Select (RS), and Read/Write (RW).

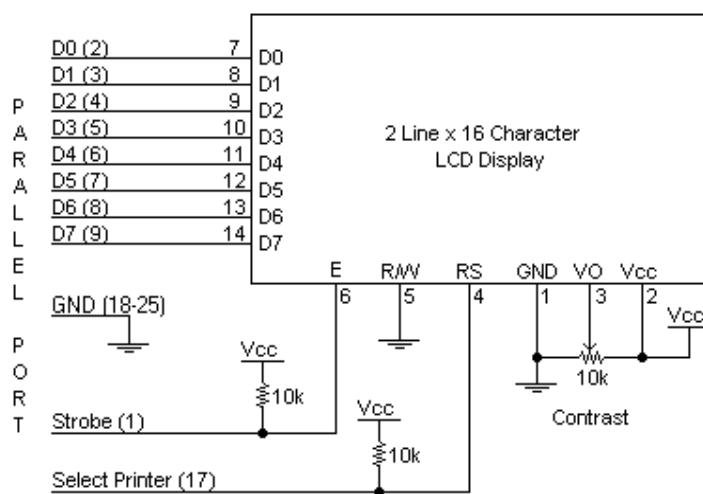


Fig. 4 Schematic diagram of LCD

4.8 DC Motor Driver

The L293D is a quadruple high-current half-H driver. It is designed to provide bidirectional drive currents of up to 600-mA at voltages from 4.5 V to 36 V. It is designed to drive inductive loads such as relays, solenoids, dc and bipolar stepping motors, as well as other high-current/high-voltage loads in positive-supply applications. All inputs are TTL compatible. Each output is a complete totem-pole drive circuit, with a Darlington transistor sink and a pseudo-Darlington source. When the enable input is low, those drivers are disabled and their outputs are off and in the high-impedance state. With the proper data inputs, each pair of drivers forms a full-H (or bridge) reversible drive suitable for solenoid or motor applications.

V. SYSTEM IMPLEMENTATION

The fingerprint based ATM authentication system is designed such that the door access can be controlled using fingerprint authentication. The status of the door access is displayed on the LCD. The complete schematic is shown in Fig. 5.

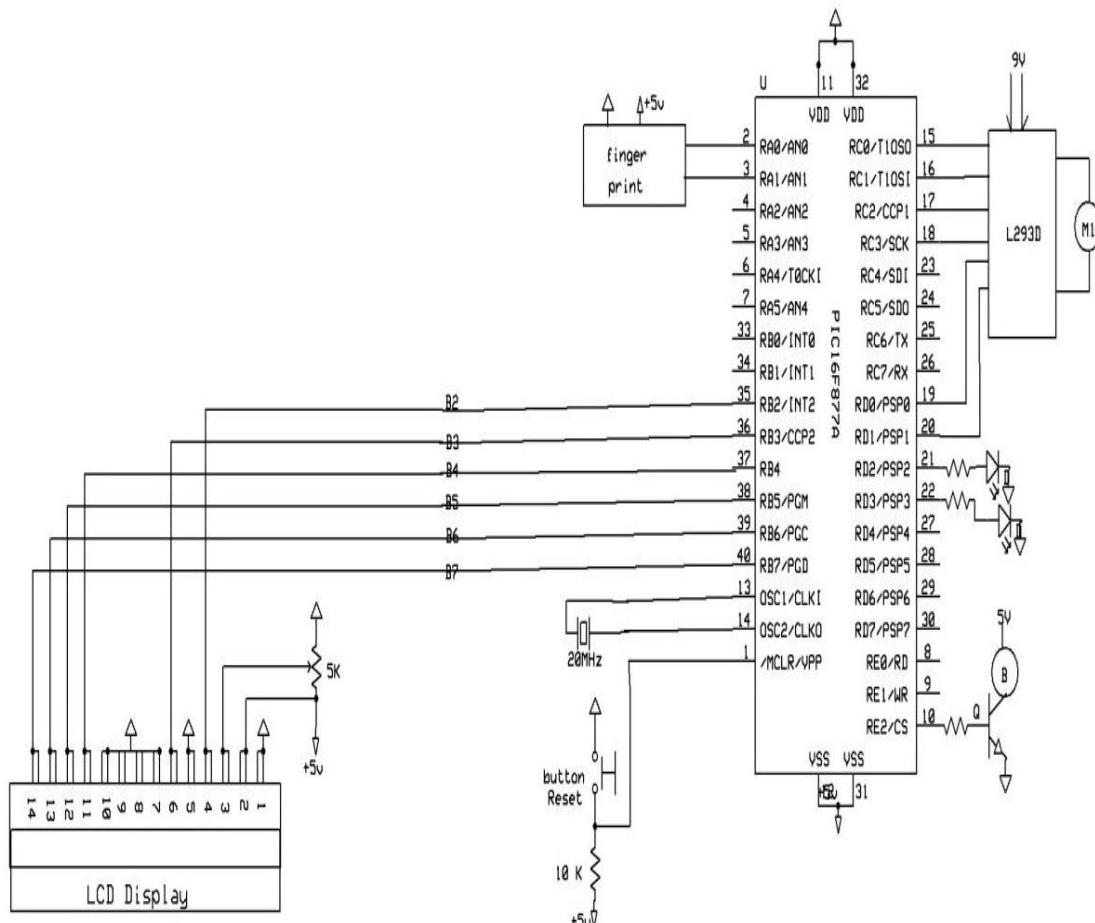


Fig. 5 Schematic diagram of Fingerprint based ATM Authentication System

The schematic depicts the interfacing of each component with microcontroller and input output modules. The experimental setup of the fingerprint based ATM authentication system is shown in Fig. 6.

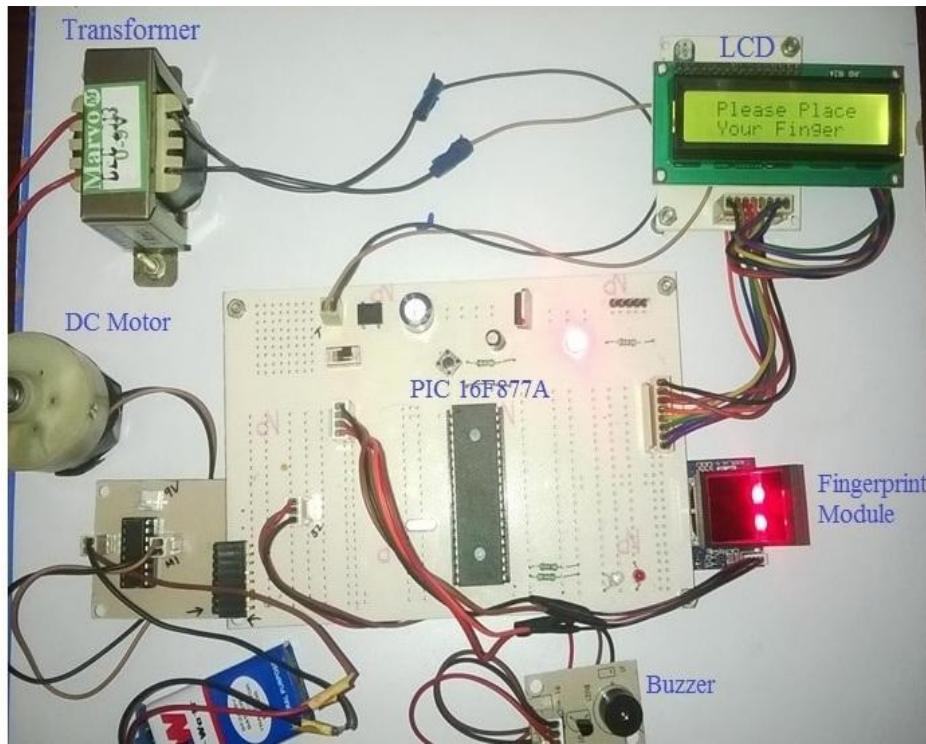


Fig. 6 Experimental Setup of fingerprint based ATM authentication system

The manager can access the vault based on the fingerprint authentication. His fingerprint is previously stored in fingerprint module. When the manager tries to access it for the next time to store the money in ATM his fingerprint will be checked for verification. If the fingerprint matches with the initially stored data, then cashbox is opened. Otherwise the system denies the operation by producing a buzzer on the alarm.

VI. CONCLUSIONS

The paper presented a prototype design of an ATM access system using finger print technology. The system consists of finger print module, DC motor, LCD display. These are interfaced to the PIC microcontroller. When a user registers his fingerprint to the finger print module, this is fed as input to the microcontroller. The micro controller is programmed in such a way that the input from the user is checked compared with user database and displays the relevant information on the LCD display. When a authorized person is recognized using finger print module the door is accessed using DC motor. Finger-scan technology is being used throughout the world and provides an able solution. In the present days it is being used for computer network access and entry devices for building door locks. Fingerprint readers are being used by banks for ATM authorization and are becoming more common at grocery stores where they are utilized to automatically recognize a registered customer and bill their credit card or debit account. Finger-scanning technology is being used in a novel way at some places where cafeteria purchases are supported by a federal subsidized meal program. The system can be extended using a GSM module. The GSM module sends alert messages to the respective authorities when unauthorized person's finger print is detected.

REFERENCES

- [1] The Biometric Consortium, "Introduction to Biometrics", (<http://www.biometrics.org>), 2006.
- [2] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, "Handbook of Fingerprint Recognition", Springer, London, 2009.
- [3] Samir Nanavati, Michael Thieme, and Raj Nanavati, "Biometrics: Identity Verification in a Networked World", John Wiley & Sons, 2002.
- [4] Julian Ashbourn, "Biometrics: Advanced Identity Verification", Springer-Verlag, London, 2002.
- [5] Edmund Spinella, "Biometric Scanning Technologies: Finger, Facial and Retinal Scanning", SANS Institute, San Francisco, CA, 2003.
- [6] Peatman, John B., "Design with PIC Microcontrollers", Pearson Education, India, 1998.
- [7] Microchip Technology Inc., "PIC16F87XA data sheet, DS39582C, 2013.