FINGERPRINT BASED BANK LOCKER SYSTEM USING MICROCONTROLLER

[1]PAVITHRA.B.C, [2]MYNA.B.C, [3]KAVYASHREE.M

[1]16th Sem TCE Gsssietw Mysore, [2]26th Sem TCE Gsssietw Mysore, [3]36th Sem TCE Gsssietw Mysore

Abstract- The main aim of the paper is to design and implement the Fingerprint based bank locker system using microcontroller. Biometrics studies commonly include fingerprint, face, iris, voice, signature, and hand geometry recognition and verification. Many other modalities are in various stages of development and assessment. Among these available biometric traits finger Print proves to be one of the best traits providing good mismatch ratio and also reliable. The present scenario to operate a bank locker is with locks which are having keys. This does not provide good security to our lockers. To provide perfect security to the bank lockers and to make the work easier, this project is taking help of two different technologies viz. EMBEDDED SYSTEMS and BIOMETRICS.

Index Terms- finger printing, signature identification, voice recognition, face recognition, iris scan, bank locker security, identification number, digital code lock, biometrics.

I. INTRODUCTION

Security is of primary concern and in this busy, competitive world, human cannot find ways to provide security to his confidential belongings manually. Instead, he finds an alternative which can provide a full fledged security as well as atomized. In the ubiquitous network society, where individuals can easily access their information anytime and anywhere, people are also faced with the risk that others can easily access the same information anytime and anywhere. Because of this risk, personal identification technology, which can distinguish between registered legitimate users and imposters, is now generating interest.

Currently, passwords, Personal Identification Numbers (4-digit PIN numbers) or identification cards are used for personal identification. However, cards can be stolen, and passwords and numbers can be guessed or forgotten. To solve these problems, biometric authentication technology which identifies people by their unique biological information is attracting attention. Biometrics can be defined as recognizing and identifying a person based on physiological or behavioral characteristics. In biometric authentication, an account holder's body characteristics or behaviors (habits) are registered in a database and then compared with others who may try to access that account to see if the attempt is legitimate. Fujitsu has researched and developed biometric authentication technology focusing on the methods: fingerprints, faces, voiceprints.

Biometrics studies commonly include fingerprint, face, iris, voice, signature, and hand geometry recognition and verification. Many other modalities are in various stages of development and assessment. Among these available biometric traits fingerprint proves to be one of the best traits providing good mismatch ratio, high accurate in terms of security and also reliable. The present scenario to operate a bank locker is with locks which are having keys. By this we can't say that we are going to provide good security to our lockers. To provide perfect security and to make our work easier, we are taking the help of two different technologies viz. embedded systems and biometrics.

An Embedded system is a multi-agent system and computer system designed for specific control functions within a larger system, often with real-time computing constraints. Embedded systems contain processing cores that are either microcontrollers or digital signal processors (DSP).The key characteristic, however, is being dedicated to handle a particular task. Since the embedded system is dedicated to specific tasks, design engineers can optimize it to reduce the size and cost of the product and increase the reliability and performance. Some embedded systems are mass-produced, benefiting from economies of scale.

Firstly discussing about Biometrics we are concentrating on Fingerprint scanning. For this we are using R303A as a scanner. This module has in-built ROM, DSP and RAM. In this we can store up to 100 user's fingerprints. This module can operate in 2 modes they are Master mode and User mode. We will be using Master mode to register the fingerprints which will be stored in the ROM present on the scanner with a unique id.

1.1. IDENTIFICATION NUMBER

Identification number is the only thing which identifies the user as the registered nationalist as the password, government registered identification number can be anything driving license, passport, voter id, PAN card or any other proof. This is the same as the one used for the identification purpose while

opening an account or a locker. After verification it is set by the bank administration. This is the last step of authentication, after this the locker can be accessed. An alphanumeric key and the number of characters depend on the proof used. This gives three chances to validate the user and access the locker. After the trials are given, any further entry will give alarm to the bank officials.

1.2. DIGITAL CODE LOCK

Digital Code Lock is a lock which is individually installed at the door of every locker. This is a microcontroller based digital lock system which gets open if the right password is entered. The password is numeric without any characters. The password of 6 numbers is mandatory. This lock is interfaced with the microcontroller and has a memory with it for the storage of password. The whole system is not so expensive and hence can be installed at every locker. This will authenticate the person and will act as a medium to lead the locker holder to the next level of validation. This will be issued to the holder when they opt for the locker and can be changed only by the authorized bank officials after their validation is done. There are three trials given, if the validation is not done then the system gives in danger signal and the authentication fails. This lock consists of a LCD screen, keyboard and a microcontroller 8051.

The keyboard consist of 12 keys (4*3) from 1,2,3,4,5,6,7,8,9,*,0,# and is used to input the password. Where * is used to delete one single digit. When 6 digit passwords are being entered, # is pressed to submit that password. LCD screen is used for display. Here, LCD is used to show the typed digits and to acts as an interface between the microcontroller and the user. Unlike the use of above forms of authentication such as passwords, tokens or digital code lock, biometric recognition provides a strong link between an individual and a claimed identity. It is very difficult to perform the type of check without the use of biometrics.

1.3. BIOMETRICS

The term "Biometrics" is derived from the Greek words bio (life) and metric (to measure).

Biometrics can be defined as recognizing and identifying a person based on physiological or behavioral characteristics. Biometrics is becoming an interesting topic now in regards to computer and network security. However the ideas of biometrics have been around for many years.

1.4 .SIGNATURE IDENTIFICATION

Signature identification is the analyses of the way a user signs his or her name. The process used by a biometric system to verify a signature is called dynamic signature verification (DSV). The angle at which the pen is held, the number of times the pen is lifted, the time it takes to write the entire signature, the pressure exerted by the person while signing, the variations in the speed with which different parts of the signature are written. Advantages are, Unique for every individual and user himself can decide the identity, lesser false acceptance rate, relatively cheap technology, No expert training required. Disadvantages are signature of a person may change after a long time like if an user gone through an accident and he cannot use his hand and then he signs after a long time, his sign and pressure points may change, High false rejection rate Pressure points may change because of weather or some disease. System can be fooled by imitating Profile Database.

Figure 1.4. Signature Identification.

1.5. VOICE RECOGNITION

Voice recognition is the Identification using the acoustic features of speech that have been found to differ between individuals. Advantages are Easy to use and require no special training or equipment, relatively inexpensive compared to other biometrics and Consumers prefer to use voiceprints over other biometric technology for identification according to a Chase bank's research study. Disadvantages are When processing a person's voice over multiple channels such a microphone and then over a telephone reduces the recognition rate, Physical conditions of the voice such as those due to sickness, affect the voice verification process, Environment noise reduces the overall accuracy and effectiveness of the recognition, The storage requirement for voiceprint database can be very large, a person's voice changes over time.

1.6. FACE RECOGNITION

Face recognition uses the visible physical structure of the face and analyses the spatial geometry of distinguishing features in it identify an individual. Facial recognition systems have a higher relative unit cost, they do offer increased accuracy levels.

Inherently the technology has a number of advantages, most notably, that it is readily acceptable by the public and relatively easy to integrate with other security systems, particularly CCTV. But development work still needs to be done to improve its performance. It needs to make allowance for the changes that occur to the human face over time - aging, facial hair, skin tone, glasses, etc. All of which could impede the recognition software. And technically, the affect of prevailing light conditions and the angle of the image need to be

reduced, thereby allowing faster and more accurate processing.

Figure 1.6. Face recognition.

1.7. IRIS SCAN

The iris is the colored ring of textured tissue that surrounds the pupil of the eye.

Advantages are very high accuracy, verification time is generally less than 5 seconds, the eye from a dead person would deteriorate too fast to be useful, so no extra precautions have to been taken with retinal scans to be sure the user is a living human being. Disadvantages are Intrusive, a lot of memory for the data to be stored, Very expensive, difficult to use because of positioning eye requires more time for matching with database stored.

Figure 1.7.Iris scan.

Canadian airports started using iris scan in 2005 to screen pilots and airport workers. Pilots were worried about the possibility that repeated scans would negatively affect their vision, and Performance can be affected by certain eye problems, such as cataracts, and if the user is wearing colored contact lenses or sunglasses and these are the drawbacks.

1.8. FINGERPRINT TECHNOLOGY

In the 1890s, an anthropologist named Alphonse Bertillon sought to fix the problem of identifying convicted criminals and turned biometrics into a distinct field of study. He developed 'Bertillon age', a method of bodily measurement which got named after him. The problem with identifying repeated offenders was that the criminals often gave different aliases each time they were arrested. Bertillon realized that even if names changed, even if a person cut his hair or put on weight, certain elements of the body remained fixed, such as the size of the skull or the length of their fingers. His system was used by police authorities throughout the world, until it quickly faded when it was discovered that some people shared the same measurements and based on the measurements alone, two people could get treated as one. After this, the police used finger printing, which was developed by Richard Edward Henry of Scotland Yard, instead. Essentially reverting to the same methods used by the Chinese for years. There are many steps in the history of fingerprinting as a way to identify criminals. Bertillon included fingerprinting in his system, but not as an important element. An Argentine police official was the first person to keep fingerprint files. He classified fingerprints according to a system established by Sir Francis Galton, an anthropologist related to Charles Darwin. Galton later published a book, Fingerprints that contained a classification system.

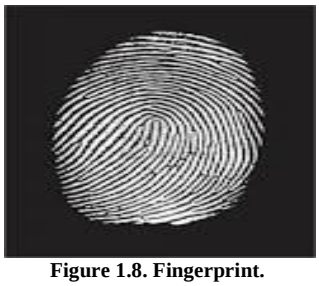

Figure 1.8. Fingerprint.

In this technology one's finger is the key i.e., one's finger prints are used as the "PASSWORD" for identification and verification. Finger print technology was developed by Fujitsu to help combat the increasing incidence of financial fraud and forgery. Among these available biometric traits, fingerprint proves to be one of the best traits providing good mismatch ratio, high accurate in terms of security and also reliable. To provide perfect security and to make the work easier we are taking the help of two different technologies viz. embedded systems and fingerprint biometrics in our project. [11]

II. PRAPOSED METHOD

2.1. BLOCK DIAGRAM OF FINGERPRINT BASED BANK LOCKER SYSTEM

The block diagram mainly consists of P8V51RD2 MCU, Finger Print Module, Keypad, 16x2 LCD, ULN Driver, Driver Circuit, Buzzer, Relays, Motor and Switch.

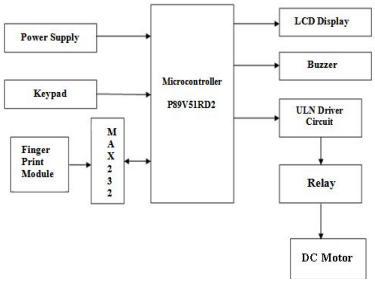

Figure 2.1. Block diagram of fingerprint based bank locker system using microcontroller.

Working

The block diagram consists of various blocks as shown in Figure 2.1. When fingerprint module is interfaced to the microcontroller, it will be in user mode. In this mode, stored images will be verified with the scanned images. When coming to our application the images of the person's fingerprint that are authorized to open the locker door will be stored in the module with a unique id. To prove that the persons are authorized to open the locker door they need to scan their fingerprint images.

The scanner is interfaced to 8051 microcontroller, this controller will be controlling the scanning process. After the scanning has been completed, user has to enter the password to open his locker with the help of a keypad. Immediately the locker will be opened. After the work has been completed if key is pressed again with help of keypad the locker door will be closed again. If an unauthorized person tries to scan his fingerprint image then an indication will be given by a buzzer which is interfaced to the controller and also if wrong password is entered by the user again indication will be given by the buzzer. The current user instead of him/her can make a new person as the user of the same locker by new registration process and the old user's fingerprint image will be deleted. Option for changing the password is also available.

2.2.CIRCUIT DIAGRAM

The circuit explanation includes the detailed pin connections of every device with the microcontroller . Power is available in the form of AC 230V, 50Hz but microcontroller operates at 5V so, 7805 constant 5V, 1A positive voltage regulator which provides output of 5V is used. Crystal is connected to 18th and 19th pins of microcontroller. The microcontroller 10th and 11th pins are connected to 11th and 12th pins of MAX232 to initialize fingerprint module and to enable serial communication. The fingerprint module's pins 2 and 3 are connected to DB9 connector which is inturn connected to 13th and 14th pins of MAX232 through the pins 2 and 3. LCD module consists of 8 data lines D0 – D7, out of which four pins are connected to port1 (P1).Additionally this module is having 3 control lines namely RS, R/W and EN, where RS and EN are connected to P1.0 and P1.1 respectively and R/W is grounded. Keypad connections are given to Port0 entirely because it is a 4x4 matrix keypad. DC motor is connected to microcontroller's P2.0 and P2.1 through ULN2003 driver circuit.

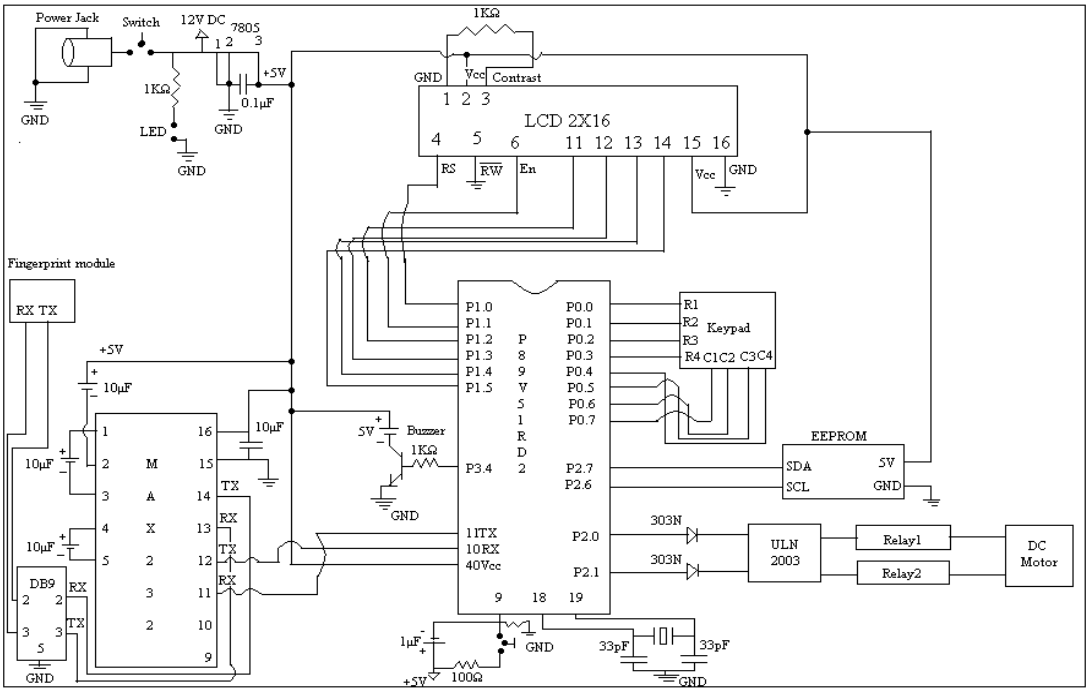

Figure2.2. Circuit diagram of the proposed method

2.3. FLOWCHART

The Flowchart is shown in the Figure 2.3. It shows how the working of the project goes according to the program. First when system is switched on, welcome note will be displayed on LCD. User scans his finger, if his/her finger does not match with stored database it is indicated by the buzzer. If finger matches then two options will be displayed on LCD like, first one is open door option, and next is modify user option, if user selects option 1 it asks for the 4 digit password if it matches with previously stored password then locker door opens otherwise buzzer will be ON. After using the locker user should press key 3 through keypad to close the door. Else if option 2 is selected again it asks password and if password is wrong buzzer will be ON if password is correct again four options will be displayed on LCD.

Like, first is new registration option for registration of new user, second is delete option to delete the old

user's fingerprint image, third is change password option to change the current password, and fourth one is the cancel option to get back to main note. If option one is selected it scans new finger and stores it and goes back to main note, else if option two is selected it asks the id to be deleted after deletion is successful it goes back to the main note, else if option three is selected it asks for old password then for new password after entering passwords it goes back to main note, else last option is cancel if it is selected it directly goes to main note.

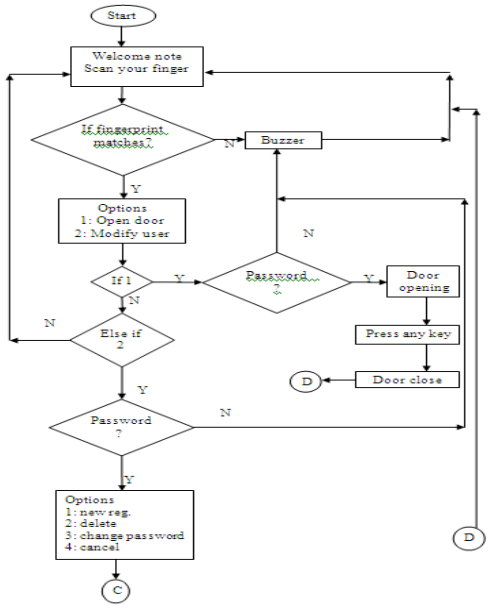

Figure 2.3.flowchart

III. RESULT

3.1 EXPERIMENTAL OBSERVATIONS

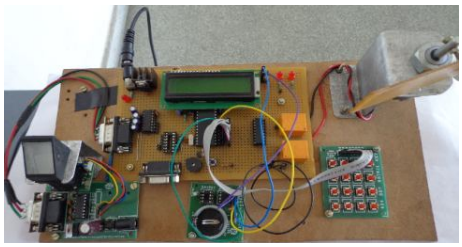

Figure 3.1 Hardware part

Step 1: When power is supplied to the board, the initial displays on the LCD are as shown below.

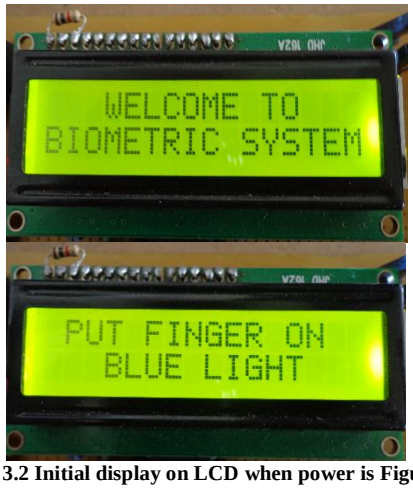

Figure 3.2 Initial display on LCD when power is turned on

Figure 3.3 Indication to scan the finger.

Figure 3.4 Scanning the finger.

Step 2: When the fingerprint is mismatched.
Step 3: When the persons fingerprint matches, display on LCD .
Step 4: We need to enter the valid password.
Step 5: When invalid password is entered display on LCD .
Step 6: When the password is matched, it displays two options.
Step 7: When option 1 is selected, displays on LCD .
Step 8: After work has been completed, we have to press key 3 for closing the locker door and it goes back to step 1.
Step 9: After step 5 when option 2 is selected, it displays four options. Select required option, for example if option 4 i.e. cancel option is selected it goes back to step 1.

IV. ADVANTAGES

1. Easy to use and requires no special training or equipment.
2. Fingerprint is unique for every person it cannot be imitated or fabricated .It is not same in the case of twins also.
3. High accuracy in terms of security.
4. No manual errors.
5. No false intrusion

CONCLUSION

A step by step approach in designing the microcontroller based system for securing the transactions of the user and providing the security for the locker system and even more for the PASSPORT verification using a finger print scanner has been followed.

The result obtained in providing the security is quite reliable in all the three modes. The system has successfully overcome some of the aspects existing with the present technologies, by the use of finger print Biometric as the authentication Technology.

REFERENCES

[1] Signals, Systems and Computers, 2004 Conference Record of the Thirty-Eighth Asilomar Conference on Publication 7-Nov-2004 Volume: 1, on page(s): 577-581 Vol.1.

[2] International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, October 2012.

[3] International Journals of Biometric and Bioinformatics, Volume (3): Issue (1).

[4] R. A. Fisher Biometrics, Vol. 20, No. 2, In Memoriam: Ronald Aylmer Fisher, 1890-1962 (Jun., 1964), pp. 261-264.

[5] John Wharton: An Introduction to the Intel MCS-51™ Single-Chip Microcomputer Family, Application Note AP-69, May 1980.

★★★