GOVERNMENT POLYTECHNIC COLLEGE

MATTANNUR-670702

(Department of Technical Education, Kerala)

SEMINAR REPORT ON

BIOMETRIC ATM SECURITY SYSTEM

SUBMITTED BY

AKSHAY VINOD K

(Reg.No:19041639)

DEPARTMENT OF ELECTRONICS ENGINEERING

2021-22

GOVERNMENT POLYTECHNIC COLLEGE

MATTANNUR-670702

(Department of Technical Education, Kerala)

CERTIFICATE

Certified that seminar work entitled “***BIOMETRIC ATM SECURITY SYSTEM***”*is a bonafide work carried out by* **“*AKSHAY VINOD K* ”** *in partial fulfilment for the award of Diploma in Electronics Engineering from Government Polytechnic College Mattannur during the academic year* 2021-2022.

Seminar Co-ordinator **Head of Section**

Internal Examiner **External Examiner**

DECLARATION

I hereby declare that the report of *the* ***BIOMETRIC ATM SECURITY SYSTEM*** work entitled which is being submitted to the Govt. Polytechnic College Mattannur, in partial fulfilment of the requirement for the award **of *Diploma in Electronics Engineering*** *i*s a confide report of the work carried out by me. The material in this report has not been submitted to any institute for the award of any degree.

Place:Mattannur **AKSHAY VINOD K**

ACKNOWLEDGEMENT

I would like to take this opportunity to extend my sincere thanks to people who helped me to make this seminar possible. This seminar will be incomplete without mentioning all the people who helped me to make itreal.

Firstly, I would like to thank GOD, almighty, our supreme guide, for bestowing his blessings upon me in my entire endeavor.

I would like to express my deepest gratitude **Mr. M C PRAKASHAN** (Principal GPTC, Mattannur), **Mr. GEORGE KUTTY P P (**Head of Department of Electronics Engg.), for the help rendered by him to prepare and present this Seminar in proper way. Moreover I am very much indebted to **Mr. SREEJITH A** (Lecturer, Electronics Engg, seminar co-ordinator), for their advice.

I am also indebted to all my friends and classmates who have given valuable suggestion and encouragement.

AKSHAY VINOD K

ABSTRACT

Now a days ATM systems are not secure because, there are some hackers which are capable of accessing ATM accounts of the people seeking ATM facility. Inorder to put ATM accounts of people to a more secure side we are introducing our new idea of finger print module to verify the actual user more precisely.So in this way the hackers will not be able to hack the personal accounts of different people.In our project we are using a finger print module along with ARM processor. In which the different finger patterns of different people are coded and stored by module itself. The codes generated by module will be monitored by processor consisting all the codes of users in the form of (their name, account number, balance, etc.) data. And whatever the service needed to the users will beoffered in a very efficient way. The basic aim of this project is to study the system, which is used for ATM access to cash withdrawal with more security. In this system, Bankers will collect the customer finger prints and mobile number while opening the account then only customer can access ATM machine. The working of system will start when our customer goes at ATM center. First there is switch for entry. After getting entry customer has to places his finger on the finger print module. Then system will check for user identity and checks validity of finger.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Biometrics are automated methods of identifying a person or verifying the identity of a person based on a physiological or behavioral characteristic. Biometric-based authentication is the automatic identity verification, based on individual physiological or behavioral characteristics, such as fingerprints, voice, face and iris. Since biometrics is extremely difficult to forge and cannot be forgotten or stolen, Biometric authentication offers a convenient, accurate, irreplaceable and high secure alternative for an individual, which makes it has advantages over traditional cryptography-based authentication schemes. It has become a hot interdisciplinary topic involving biometric and Cryptography. Biometric data is personal privacy information, which uniquely and permanently associated with a person and cannot be replaced like passwords or keys. Once an adversary compromises the biometric data of a user, the data is lost forever, which may lead to a huge financial loss. Hence, one major concern is how a person’s biometric data, once collected, can be protected The idea of using patterns for personal identification was originally proposed in 1936 byophthalmologist Frank Burch. By the 1980’s the idea had appeared in James Bond films, but it still remained science fiction and conjecture. In 1987, two other ophthalmologists Aram Safir and Leonard Flom patented this idea and in 1987 they asked John Daugman to try to create actual algorithms for this iris recognition. These algorithms which Daugman patented in 1994 are the basis for all current iris recognition systems and products.

CHAPTER 2

LITERATURE REVIEW

Most finger-scan technologies are basedon 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 matchingis thatit is more sensitive to the placement of the finger during verification and the created template is several times larger in byte size.Finger-scan technologyis 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 may 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 frompersonal information. Biometric templates cannot be reverse-engineered to recreate personal information and they cannot be stolen and used to access personal information

CHAPTER 3

WORKING

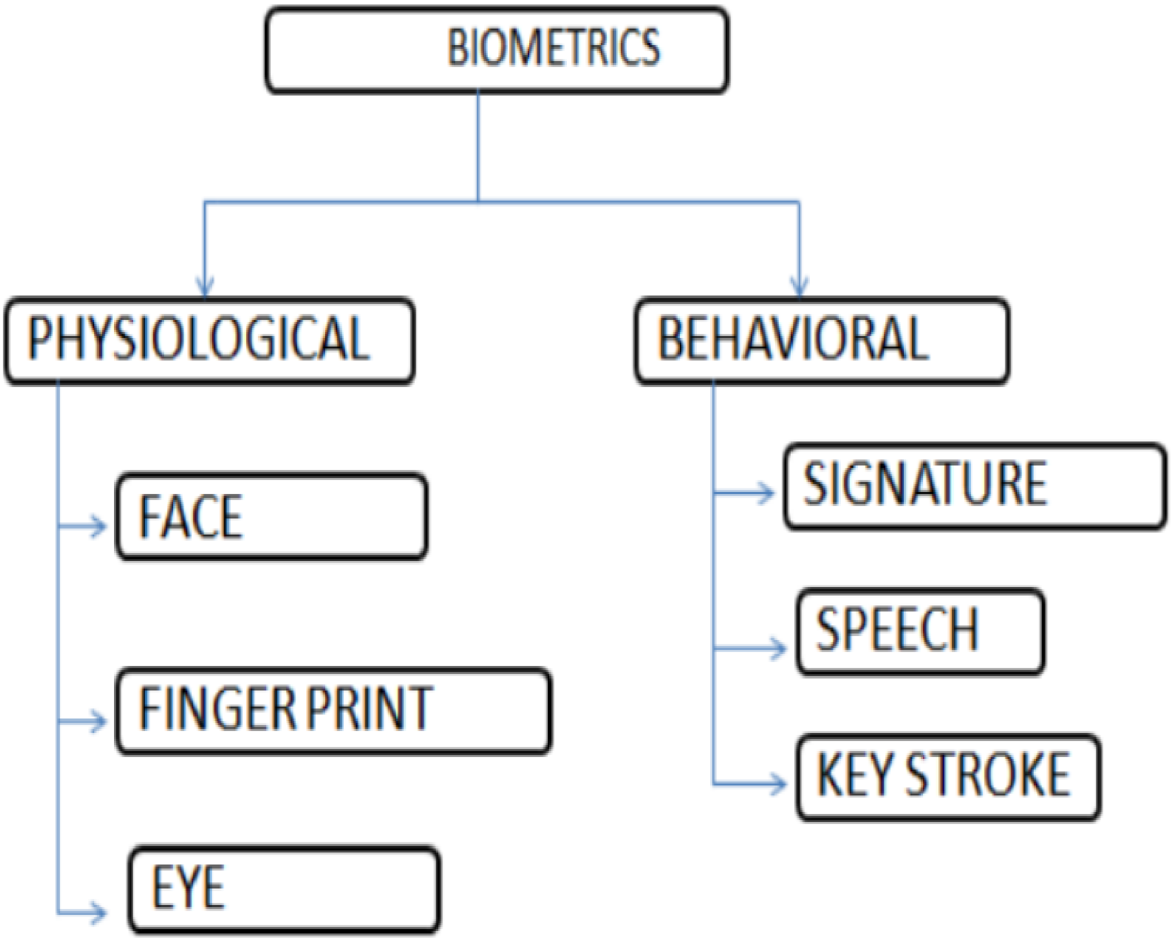

Fig 3.1 Classification of biometrics

Biometrics encompasses both physiological and behavioral characteristics. A physiological characteristic is a relatively stable physical feature such as finger print, iris pattern, retina pattern or a Facial feature. A behavioral trait in identification is a person’s signature, keyboard typing pattern or a speech pattern. The degree of interpersonal variation is smaller in a physical characteristic than in a behavioral one

3.1 Types of biometrics

Fingerprints: The patterns of friction ridges and valleys on an individual's fingertips are unique to that individual. For decades, law enforcement has been classifying and determining identity by matching key points of ridge endings and bifurcations. Fingerprints are unique for each finger of a person including identical twins. One of the most commercially available biometric technologies, fingerprint recognition devices for desktop and laptop access are now widely available from many different vendors at a low cost. With these devices, users no longer need to type passwords – instead, only a touch provides instant access.

Face Recognition: The identification of a person by their facial image can be done in a number of different ways such as by capturing an image of the face in the visible spectrum using an inexpensive camera or by using the infrared patterns of facial heat emission. Facial recognition in visible light typically model key features from the central portion of a facial image. Using a wide assortment of cameras, the visible light systems extract features from the captured image(s) that do not change over time while avoiding superficial features such as facial expressions or hair.

Speaker Recognition: Speaker recognition uses the acoustic features of speech that have been found to differ between individuals. These acoustic patterns reflect both anatomy and learned behavioral patterns . This incorporation of learned patterns into the voice templates has earned speaker recognition its classification as a "behavioral biometric." Speaker recognition systems employ three styles of spoken input: text-dependent, text-prompted and text independent. Most speaker verification applications use text-dependent input, which involves selection and enrollment of one or more voice passwords. Text-prompted input is used whenever there is concern of imposters. The various technologies used to process and store voiceprints include hidden Markov models, pattern matching algorithms, neural networks, matrix representation and decision trees.

Iris Recognition: This recognition method uses the iris of the eye which is the colored area that surrounds the pupil. Iris patterns are thought unique. The iris patterns are obtained through a video-based image acquisition system. Iris scanning devices have been used in personal authentication applications for several years. Systems based on iris recognition have substantially decreased in price and this trend is expected to continue. The technology works well in both verification and identification modes.

Hand and Finger Geometry: To achieve personal authentication, a system may measure either physical characteristics of the fingers or the hands. These include length, width, thickness and surface area of the hand. One interesting characteristic is that some systems require a small biometric sample. It can frequently be found in physical access control in commercial and residential applications, in time and attendance systems and in general personal authentication applications.

Signature Verification: This technology uses the dynamic analysis of a signature to authenticate a person. The technology is based on measuring speed, pressure and angle used by the person when a signature is produced. One focus for this technology has been e-business applications and other applications where signature is an accepted method of personal authentication

CHAPTER 4

FINGERPRINT

Humans have used fingerprints for personal identification for many centuries and the matching accuracy using fingerprints has been shown to be very high. Fingerprinting is probably the bestknown biometric- method of identification used for 100 years. There are a few variants of image capture technology available for such commercially oriented fingerprint sensor, including optical, silicon, ultrasound, thermal and hybrid. Among all the biometric techniques, fingerprint-based Identification is the oldest method that has been successfully used in numerous applications. Everyone is known to have unique, immutable fingerprints. A fingerprint is made of a series of ridges and furrows on the surface of the finger as shown in the fig 3.1.1. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as minutiae points. Minutiae points are the local ridge characteristics that occur either at a ridge ending or a ridge bifurcation. A ridge ending is defined as the point where the ridge ends abruptly and the ridge bifurcation is the point where the ridge splits into two or more branches. When a user places their finger on the terminals scanner the image is electronically read, analyzed, and compared with a previously recorded image of the same finger which has been stored in the database. The imaging process is based on digital holography, using an electro-optical scanner about the size of a thumbprint. The scanner reads three-dimensional data from the finger such as skin undulations, and ridges and valleys, to create a unique pattern that is composed into a template file.

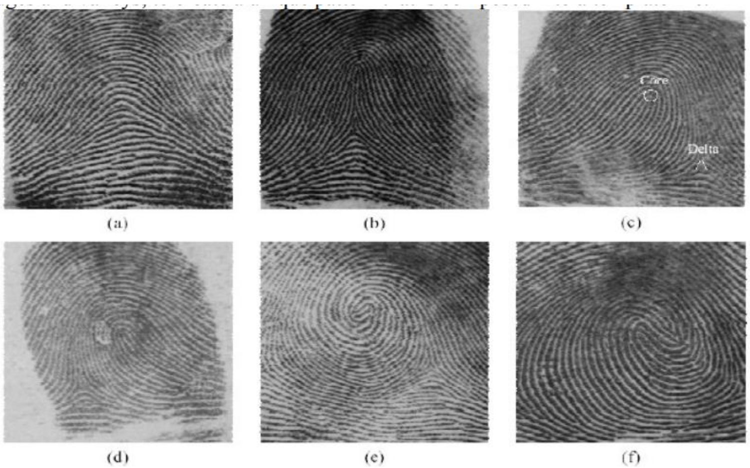

Fig 4.1: Fingerprint classification of 6 categories (a) arch, (b) tented arch, (c) right loop, (d) left loop, (e) whorl, and (f) twin loop

An algorithm is developed to classify fingerprints into five classes, namely, whorl, right loop, arch and tented arch as shown in figure 3. Critical points in a finger print, called core and delta are marked on one of the fingers .The core is the inner point, normally in the middle of the print, around which swirls, loops, or arches center. It is frequently characterized by a ridge ending and several acutely curved ridges. Deltas are the points, normally at the lower left and right hand of the fingerprint around which a triangular series of ridges center. The algorithm separates the number of ridges present in four directions (o degree, 45 degree, 90 degree and 135 degree) by filtering the central part of a fingerprint with a bank of Gabor filters.This information is quantized to generate a finger code which is used for classification. To avoid fake-finger attacks, some systems employ so-called liveness detection technology, which takes advantage of the sweat activity of human bodies. High-magnification lenses and special illumination technologies capture the finger's perspiration and pronounce the finger dead or alive.

fingerprint sensing, in which the fingerprint of an individual is acquired by a fingerprint scanner to produce a raw digital representation; pre processing, in which the input fingerprint is enhanced and adapted to simplify the task of feature extraction; feature extraction, in which the fingerprint is further processed to generate discriminative properties, also called feature vectors; and matching, in which the feature vector of the input fingerprint is compared against one or more existing templates. The templates of approved users of the biometric system, also called clients, are usually stored in a database. Clients can claim an identity and their fingerprints can be checked against stored fingerprints.

Fingerprint Sensing The acquisition of fingerprint images has been historically carried out by spreading the finger with ink and pressing it against paper card. The paper card is then scanned, resulting in a digital representation. This process is known as off-line acquisition and is still used in law enforcement applications. Currently, it is possible to acquire fingerprint images by pressing the finger against the flat surface of an electronic fingerprint sensor. This process is known as online acquisition.

There are three families of electronic fingerprint sensors based on the sensing technology

- Solid-state or silicon sensors These consist of an array of pixels, each pixel being a sensor itself. Users place the finger on the surface of the silicon, and four techniques are typically used to convert the ridge/valley information into an electrical signal: capacitive, thermal, electric field and piezoelectric. Since solid-state sensors do not use optical components, their size is considerably smaller and can be easily embedded. On the other hand, silicon sensors are expensive, so the sensing area of solid-state sensors is typically small.

• Optical: The finger touches a glass prism and the prism is illuminated with diffused light. The light is reflected at the valleys and absorbed at the ridges. The reflected light is focused onto a CCD or CMOS sensor. Optical fingerprint sensors provide good image quality and large sensing area but they cannot be miniaturized because as the distance between the prism and the image sensor is reduced, more optical distortion is introduced in the acquired image.

• Ultrasound: Acoustic signals are sent, capturing the echo signals that are reflected at the fingerprint surface. Acoustic signals are able to cross dirt and oil that may be present in the finger, thus giving good quality images. On the other hand, ultrasound scanners are large and expensive, and take some seconds to acquire an image. A new generation of touch less live scan devices that generate a 3D representation of fingerprints is appearing . Several images of the finger are acquired from different views using a multi camera system, and a contact-free 3D representation of the fingerprint is constructed. This new sensing technology overcomes some of the problems that intrinsically appear in contact-based sensors such as improper finger placement, skin deformation, sensor noise or dirt.

Preprocessing and Feature Extraction fingerprint is composed of a pattern of interleaved ridges and valleys. They smoothly flow in parallel and sometimes terminate or bifurcate. At a global level, this pattern sometimes exhibits a number of particular shapes called singularities, which can be classified into three types: loop, delta and whorl , we can see an example of loop and delta singularities (the whorl singularity can be defined as two opposing loops). At the local level, the ridges and valleys pattern can exhibit a particular shape called minutia. There are several types of minutiae, but for practical reasons, only two types of minutiae are considered: ridge ending and ridge bifurcation . Singularities at the global level are commonly used for fingerprint classification, which simplifies search and retrieval across a large database of fingerprint images. Based on the number and structure of loops and deltas, several classes are defined

CHAPTER 5

HARDWARE DESIGN

To implement the proposed security for ATM terminals with the use of fingerprint recognition, we use the different hardware and software platforms. Fig 1 shows the major system modules and their interconnections.

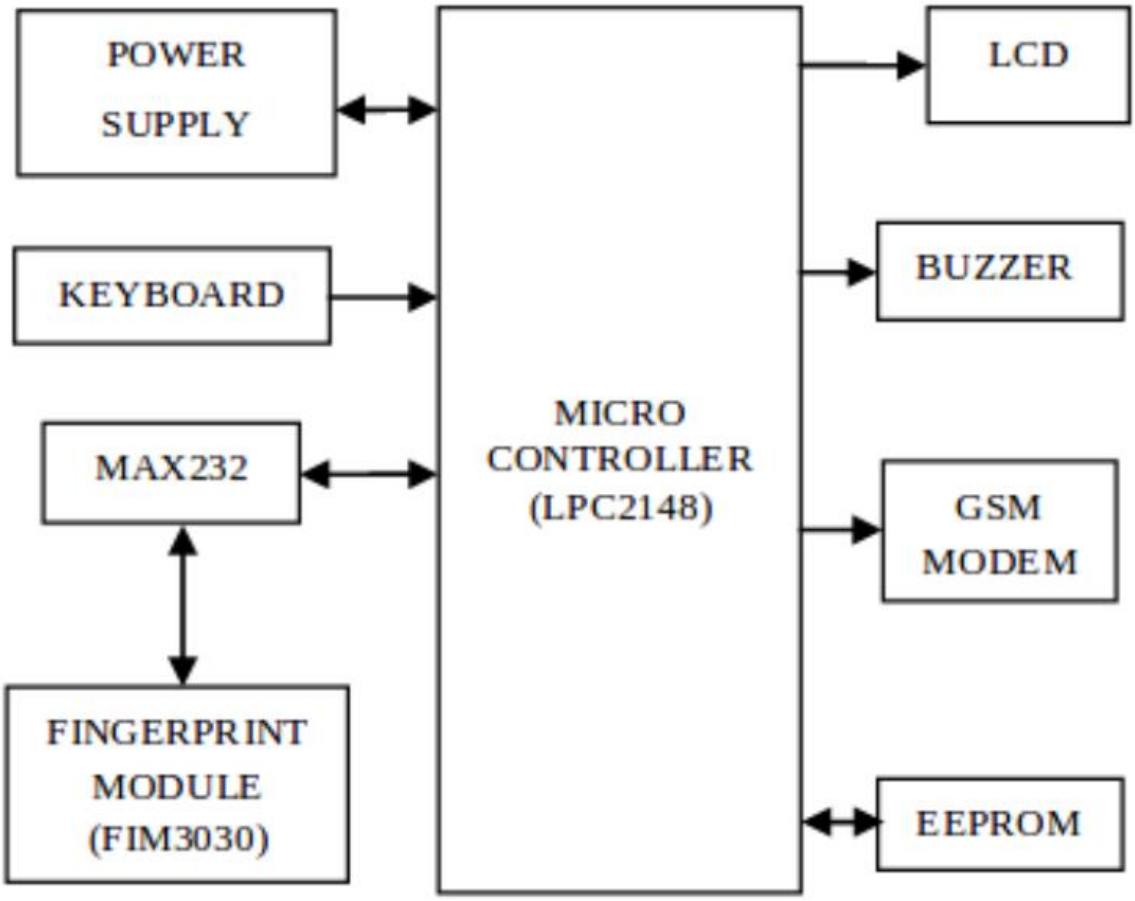

Fig 5.1 Overview of the sytem

5.1 Microcontroller(LPC2148)

The system uses LPC2148 from ARM7 family.It is the core controller in the system. It hasARM7TDMI core which is a member of the Advanced RISCMachines (ARM) a family of general purpose 32-bitmicroprocessors. It offershigh performance for verylow power consumption and price. The ARM architectureis based on RISC (Reduced Instruction Set Computer)principles, and the instruction set and related decodemechanism are much simpler than those of micro-programmedComplex Instruction Set Computers (CISC)[26]. This simplicity results in a high instruction throughputand impressive real-time interrupt response from a smalland cost-effective chip. Allparts of the processing and memory systems can operatecontinuously since, pipelining is employed. Typically, while one instruction is beingexecuted, its successor is being decoded, and a thirdinstruction is being fetched from memory [27]. The ARMmemory interface has been designed to allow theperformance potential to be realized without incurring highcosts in the memory system. Speed-critical control signalsare pipelined to allow system control functions to beimplemented in standard low-power logic, and thesecontrol signals facilitate the exploitation of the fast localaccess modes offered by industry standard dynamic RAMs[28].The LPC2148is interfaced to different modules via GPIO (General Purpose I/O) pins. It receives the fingerprint template produced by the fingerprint module. It will match the same with the reference template stored at installation of the system. If the received template gets matched with the reference one, the person is allowed to access the further system. In case of successive mismatch of templates, the system will initialize the GSM module to send message to the enrolled user and simultaneously will raise the alarm through buzzer.

We have used LPC2148 from NXP semiconductors(founded by Philips). It shows features as follows

a)16/32-bit ARM7TDMI-S microcontroller in a tinyLQFP64 package.

b)240 kB of on-chip static RAM and 512 kB of on-chipflash program memory.

c)In-System/In-Application Programming (ISP/IAP) viaon-chip boot-loader software.

d)Two 10-bit A/D converters provide a total of 14analog inputs, with conversion times as lowas 2.44μs per channel.

e)Single 10-bit D/A converter provide variable analogoutput.

f)Multiple serial interfaces including two UARTs(16C550), two Fast I2C-bus (400 kbit/s), SPI and SSPwith buffering and variable data length capabilities.

g)Vectored interrupt controller with configurablepriorities and vector addresses.

h)Up to 45 of 5 V tolerant fast general purpose I/O pinsin a tiny LQFP64 package.

5.2 Fingerprint Module(FIM3030)

The important module of the system is fingerprint scanner. We used FIM3030 by NITGEN. It has ADSP-BF531 as central processing unitwith 8 MBof SDRAM and 1 MB of flash ROM.It uses overall supply voltage of 3.3 V. The communication with the fingerprint moduleis made through RS-232 via UART0 of LPC2148.A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching. FIM3030is an evolutionary standalone fingerprint recognition module consisted of optic sensor OPP03 and processing board. As CPU and highly upgraded algorithm are embedded into a module, it provides high recognition ratio even to small size, wet, dry, calloused fingerprint. High speed 1: N identification and 1: N verification. FIM3030 has functions of fingerprint enrollment, identification, partial and entire deletion and reset in a single board, thereby offering convenient development environment. Off-line functionality stores logs on the equipment memory (up to 100 fingerprints) and it’s identified using search engine from the internal algorithm. Evolutionary standalone fingerprint recognition module FIM3030is ideal for on-line applications, because allows ASCII commands to manage the device from the host. On-line functionality, fingerprints to verify (1:1) or identify (1: N) can be stored on non volatile memory, or be sent by RS-232 port.

5.3 GSM Modem

While accessing the system, we don’t replace the password verification. If password is correct, the system will capture and match fingerprint of the customer.As shown in Fig 4, if fingerprint does not match with the account registry for three times, buzzer will be made ON and a message will be delivered to customer’s cellphoneand bank authority.Thus, GSM MODEM to communicate with the mobile phone to which we are going to send the message isalso interfaced with LPC2148.

5.4 User Interface

The user interface makes the communication between user and the system model easier. It includes a display unit and a function keyboard.For displaying the status of the process running in system and instructional steps for the user, we interfaced 16 x 2 LCD matrix with LPC2148 through GPIO pins of port 1

5.5 Power Supply

This section is meant for supplying power to all the sections mentioned above. It basically is consisted of a transformer to step down the 230V ac to 18V ac followed by diodes. Thediodes are used to rectify the ac to dc. After rectificationprocess,the obtained rippled dc is filtered using a capacitor Filter. A positive voltageof 12V and 5V are made available through LM7812 and LM7805. Further, LM317 is used to provide variable power e.g. 3.3V to LPC2148

CHAPTER 6

SOFTWARE DESIGN

The embedded platform discussed above is programmed in C languagewith KeilµVision4 to follow the program logic.

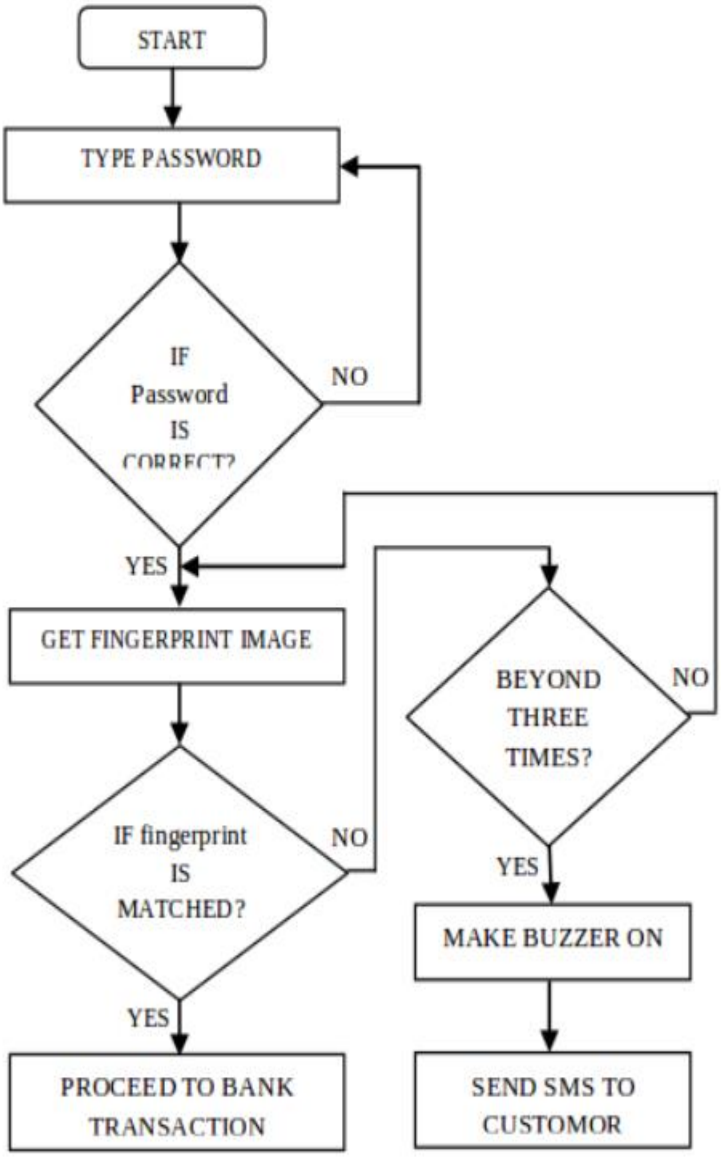

Fig 6.1 Flow chart of the system

CHAPTER 7

ADVANTAGES AND DISADVANTAGES

7.1 Advantages:

- All the bank accounts are managed in a single finger touch thus no need to carry multiple cards and remember their passwords.

- The problems like fraud, unlawful entry, cards getting stolen forgetting the PINs are prevented.

- The system is using biometric instead of PIN for validation. Thus the transactions get more secure.

- It suspends the fraud calls related to the ATM card verification and all

7.2 Disadvantages:

- Costly

- Facial imaging can also hinder accurate identifications.

- Missing body part problem.

- False acceptances and rejections.

- The scanning of eye is fearful.

- The nervousness that people feel about the scanners identification.

CHAPTER 8

APPLICATIONS

Biometric ATM has gained acceptance in a number of different areas. Application of iris recognition technology can he limited only by imagination. The important applications are those following:--

- Used in ATM’s for more secure transaction.
- Used in airports for security purposes.
- Computer login: The finger print as a living password
- Credit-card authentication
- Secure financial transaction (e-commerce, banking).
- “Biometric—key Cryptography “for encrypting/decrypting messages.
- Driving licenses and other personal certificates.
- Entitlements and benefits authentication.
- Forensics, birth certificates, tracking missing or wanted person

CHAPTER 9

FUTURE SCOPES

9.1 Authentication

It is reasonable to expect, thatin a relatively short time,all personal documents will contain some form of biometric data. Moreover, in time, we could expect that all such documents will no longer be needed, because, in every instance where this type of authentication would be necessary, biometric readers will be connected to the location via network. This would allow a comparison with stored data to be used in lieu of documentation.

9.2 Access and attendance control

In the relatively near future, biometrics will certainly gain increased acceptance in all kinds of access and attendancecontrol applications. We can expect to see biometrics used for these applications in homes, offices, computers, machines, devices, etc. In fact, this will be probably the largest market for biometric technology in terms of the amount of devices installed. However, for the most part, the use of these devices will only replace existing access control methods and technologies, providing increased convenience and security. There will be no need to carry keys, identity cards, personal documents, etc. Furthermore, this implementation of biometrics will add to the overall security solution: precluding the possibility of theft or unauthorized use of equipment/technologies. Biometric devices will offer new quality to security solutions, but not necessarily new market opportunities or potential.

9.3 Travel control

For a variety of reasons, there is an increasing requirement to have people traveling via planes, ferries, and even trains to be individually registered, with interim checks at multiple locations. Today these requirements are being driven mostly by security concerns, visa regulations and other such reasons. And, because the amount of people traveling is already large and predicted to increase at significant rates, all organizations involved in the management and control of mass transportation industries are very interested in the rationalization and automation of necessary procedures. This is especially the case in International Civil Aviation Organization. The pressure caused by the growing number of passengers is surely one of the largest reasons for the introduction of biometric passports, visas and other controls/documents. This organization recommends very clearly, that "ContractingStates should incorporate biometric data in their machine readable passports, visas and other official travel documents, using one or more optional data storage technologies to supplement the machine readable zone, as specified in Doc 9303”1,

9.4 Financial and other transactions requiring authorization

In applications having to do with money it is already apparent, that money in physical form (bank notes and coins) is being replaced more and more by virtual forms of financial transactions 17 – digital transactions via data base entry. Today this happens in form of credit or bank cards, pocket electronic money, etc. However, it is clear that, in most cases, the physical card is not important, because money has an owner and can be directly connected to a person. Spreading of biometric authentication in the economic sector (i.e. banking and trade) will decrease the need for physical objects, such as cards – since virtual money can be directly connected to a person (or to the legal person). This will result in a significant change both in the behavior of people, but also in the abilities that governmental organizations will have in their surveillance of money movements (financial transactions). I would expect two possible developments in response to this situation. First, the attitudes of people can be against the sole use of virtual money or they can also try to change the tax and economic systems to allow them to live exclusively with virtual money. The second development, or solution, will evolve over a longer period of time, but is significantly better. That is, the possibility to authorize all legal transactions through biometric mechanisms will make many of these operations much easier and more convenient.

9.5 Remote voting (authorization)

Perhaps the most important change in the society will result from the creation of an entirely new market for biometric devices that I call remote authorization. The merging of existing and future networking developments with biometric solutions will allow people to have the opportunity to authorize a wide range of transactions (e.g. voting, purchasing, accessing, decision-making authorizations, etc.) via the network, from remote locations. No longer will they be required to personally present at a given location in order to authenticate a specific action. Indeed, this is a capability that is partially possible today. However, the viability of remote authorization on a large scale, such as public elections, will not be realistic until appropriate biometric solutions are operating without the major shortcomings that plague existing biometric solutions. From my perspective, it will be necessary to develop new, more robust and capable devices. However, the same devices can also be used for many others purposes, such as computers accessories, access control devices, etc. Even so, it is certain that the existing devices that are in use today cannot provide the degree of accuracy necessary to recognize a person whose biometric identity is only available through a distributed network.

The risk of betraying them through identity theft is much too large. However, after more accurate, reliable and cost-effective devices are developed that are not constrained by shortcomings associated with existing technologies, the potential for authenticating remote transactions, such as voting (decision making) can drive major changes in all democratic societies – that is, the idea that direct democratic participation by the public can be realized on a large scale and work at low cost. Necessary democratic decisions can be made practically every day at minimal cost, even in large societies. The possibility of low cost remote voting by the public will not only open up the potential for increased participation, but also for increased frequency in voting activities. It is only speculation today, but I would think that this perspective can lead to some of the largest changes in democratic societies – all facilitated by the introduction of accurate, reliable, high speed biometric technologies that enable remote authentication (voting, et al.) at minimal cost. The corresponding changes in political systems and 18 power structures will provide the potential to have a more representative democracy. In association with changes in banking and money transfer techniques remote voting and authorization can also significantly influence economy and tax system: the control of money transfers will be easier, it will be also easier to compete within the “black economy”, but this can also result in people with a much stronger interested in controlling politicians regarding the questions of spending taxes and lowering the cost incurred by the operation of their governments. The possibility to authorize any transaction remotely will surely cause additional changes in other transactions that require such authorization, which currently implies a personal contact. This is also something that will have impact on life in the near future – it will minimize, or eliminate the need for many personal contacts. Such operations will be easier and can be done automatically (by machines – without clerks operating them, as it is done today).

9.6 Use of automatic working devices

With the help of biometrics it will be easier to track the actions of user of any devices and machines, adapt their functions to his needs and to demand his liability for actions caused. I assume that this can slowly change many areas of life and create a large market for devices that are able to recognize their users and react according to their needs. The development of such machines began already, some devices are working, other are proposed as ideas: The main goal of this development is the creation of machines able to recognize their user or people doing something in their vicinity. This feature can be very important for work in factories, offices, hospitals, for use of cars, home appliances, etc. In all such cases it may be important or convenient, that the machine “knows” who is using it (or try to do it, but shouldn’t). This allows automatic adaptation to the needs of people, but also tracking of their actions and reacting in the case of misuse. Such a feature means naturally, that actions of people will be associated by machines, that can be more useful, more convenient to use, but also allows to control, eventually improve the actions of people. These kind of biometric functions do not require (in most cases) a very high degree of secure recognition, but will require techniques, that are called today multimodal biometrics: face, voice, gait and habits recognition and probably much more. It is already visible today that such functions will be implemented in many devices, because of the convenience, that they are offering. In industrial environment the importance of their use will grow with the percentage of automatic devices. Their use will also offer significant advantages: quicker reaction to the user for example in the form of establishing the environment that suits to the person, actual using the device. It can be a seat that is adjusting its position to the needs of the user, but also the computer desktop, loudness of the speaker, etc. This offers not only a convenience, but also a time gain: adjusting such functions requires some time that must be not lost, if automatically done by the machine. It allows also implementing such functions for correction of specific errors, often made by the user, use of shortcuts that can be adjusted individually. Broad use of such technologies will also support the development of automatic shops and other facilities that can be now operated without employees. I think, that this kind of devices will be developed slowly, with growing amount of functionality and in the future will cause, that many machines will be able to recognize the needs of their users automatically, becoming more and more able to serve people in the similar way as live servants.

CHAPTER 10

CONCLUSION

It is vital step to understand the basics, i.e. the advantages, disadvantages, requirements and most importantly the feasibility of a biometric based security system. The implementation of ATM security system by using biometric method is a crucial procedure, as well as very challenging and difficult. But for security purposes and to have a control on the criminal records it is very important to bring this system in motion. Fingerprints have intrinsic features that do not change for whole life and are different individually. They are easy to use, cheap and provide the most suitable miniaturization. Biometrics is one of the most popular and effective means for identification/verification of an individual and is used as forensic evidence. It becomes important to take help of two technologies, namely embedded system and biometrics in order to provide enough security. Hybridization, along with the above two technologies is useful for fingerprint verification since it refers to the automated method of verifying/ identifying a match or similarities between two human fingerprints.

CHAPTER 11

REFERNCES

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.

8. .www.scribd.com/doc/50033821