

FINGERPRINT BASED ATM SYSTEM

Submitted in partial fulfillment of the requirements for the award of
Bachelor of Engineering degree in
Electronics and Telecommunication Engineering.

by
BHAVANI A (Reg. No. 37250001)
JANCY J (Reg.No. 37250007)



**DEPARTMENT OF ELECTRONICS AND TELECOMMUNICATION
ENGINEERING**

SCHOOL OF ELECTRICAL AND ELECTRONICS

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

Accredited with Grade "A" by NAAC

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119

APRIL - 2021



SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

**Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in**

**DEPARTMENT OF ELECTRONICS AND TELECOMMUNICATION
ENGINEERING**

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of Bhavani A (37250001), Jancy J (37250007) who carried out the project entitled "FINGERPRINT BASED ATM SYSTEM" under my supervision from November 2020 to April 2021.

Internal Guide

Dr.Z.MARY LIVINSA M.E., Ph.D.

Head of the Department

Dr.V.VIJAYA BASKAR M.E., Ph.D.

Submitted for Viva voce Examination held on 19-04-2021

Internal Examiner

External Examiner

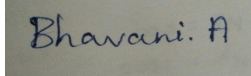
DECLARATION

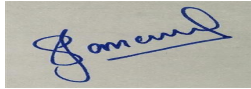
We, Bhavani A and Jancy J hereby declare that the Project Report entitled “Fingerprint based ATM System” done by us under the guidance of Dr.Z.Mary Livinsa M.E.,Ph.D, is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in Electronics and Telecommunication.

DATE: 19-04-2021

PLACE: CHENNAI

SIGNATURE OF THE CANDIDATE

1.  - BHAVANI A

2.  - JANCY J

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to the Board of Management of SATHYABAMA for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr.N.M.NANDHITHA M.E.,Ph.D**, Dean, School of Electrical and Electronics, **Dr.V.VIJAYA BASKAR M.E.,Ph.D**, Head of the Department, Dept. of Electronics and Telecommunication, for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr.Z.MARY LIVINSA M.E.,Ph.D**, for his valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the Department of Electronics and Telecommunication Engineering who were helpful in many ways for the completion of the project.

I wish to express my thanks to the Project Panel members for their valuable feedbacks during the Project Reviews which were useful in many ways for the completion of the project.

ABSTRACT

Humans recognize each other according to their various characteristics for ages. We recognize others by their face when we meet them and by their voice as we speak to them. Identity verification (authentication) in computer systems has been traditionally based on something that one has (key, magnetic or chip card) or one knows (PIN, password). Things like keys or cards, however, tend to get stolen or lost and passwords are often forgotten or disclosed.

To achieve more reliable verification or identification we should use something that really characterizes the given person. Biometrics offer automated methods of identity verification or identification on the principle of measurable physiological or behavioral characteristics. The characteristics are measurable and unique. Biometrics is the development of statistical and mathematical methods applicable to data analysis problems in the biological sciences. Physical characteristics such as fingerprints, retinas and irises, palm prints, facial structure, and voice recognition are just some of the many methods of biometric encryption. Depending on the context, a biometric system can be either a verification (authentication) system or an identification system. Biometrics is a rapidly evolving technology which has been widely used in forensics such as criminal identification and prison security. Recent advancements in biometric sensors and matching algorithms have led to the deployment of biometric authentication in a large number of civilian applications. With the increased use of computers as vehicles of information technology, it is necessary to restrict access to sensitive/personal data. Real- time biometric systems can be used to prevent unauthorized access to ATMs, cellular phones, smart cards, desktop PCs, workstations, computer networks and electronic banking.

TABLE OF CONTENTS

CHAPTER NO	CHAPTER NAME	PAGE NO
	ABSTRACT	v
	LIST OF FIGURES	vii
1	INTRODUCTION	1
	1.1 HISTORY AND DEVELOPMENT OF BIOMETRICS	3
	1.2 WHAT IS BIOMETRIC?	4
	1.2.1 SINGLE BIOMETRIC	4
	1.2.2 MULTIMODAL BIOMETRIC	6
	1.3 CLASSIFICATION OF BIOMETRICS	7
	1.4 BASIC STRUCTURE OF A BIOMETRIC SYSTEM	8
2	LITERATURE SURVEY	9
	2.1 ATM TRANSACTION SECURITY USING FINGERPRINT	9
	2.2 ATM SECURITY SYSTEM USING NONBIOMETRIC	16
3	SYSTEM DESIGN	18
4	BIOMETRIC SYSTEM COMPONENTS AND PROCESS	23
	4.1 COMPONENTS	23
	4.2 PROCESS	23
	4.2.1 ENROLLMENT	23
	4.2.2 VERIFICATION	24
	4.3 TYPES OF BIOMETRIC SYSTEM	25
	4.4 BIOMETRIC TECHNOLOGY	27
	4.4.1 FINGERPRINT SCANNING	27
	4.4.2 MATCHING APPROACH	28
	4.5 FACIAL RECOGNITION SYSTEM	29
5	SOFTWARE HARDWARE REQUIREMENTS	35
6	RESULTS AND CONCLUSION	45
	REFERENCES	48

LIST OF FIGURES

FIGURE NO	FIGURE NAME	PAGE NO
1.1	Single Biometric	4
1.2	Multimode Biometric	6
1.3	Classification of Biometrics	7
1.4	Basic Structure of Biometric	8
3.1	Block Diagram	21
3.2	Biometric System	22
4.1	Enrollment Process	24
4.2	Verification Process	24
4.3	Error Rate	26
4.4	Fingerprint Authentication Process	27
4.5	Facial Enroll & Recognition Stage	30
4.6	3D Face Masking	30
5.1	Fingerprint Scanner	36
5.2	R305 Fingerprint Sensor Module	37

CHAPTER 1

INTRODUCTION

Reliable user authentication is becoming an increasingly important task in the Web-enabled world. The consequences of an insecure authentication system in a corporate or enterprise environment can be catastrophic, and may include loss of confidential information, denial of service, and compromised data integrity. The value of reliable user authentication is not limited to just computer enhanced security.

The prevailing techniques of user authentication, which involve the use of either passwords and user IDs (identifiers), or identification cards and PINs (personal identification numbers), suffer from several limitations. Passwords and PINs can be illicitly acquired by direct covert observation. Once an intruder acquires the user ID or network access. Many other applications in everyday life also require user authentication, such as banking, e-commerce, and physical access control to computer resources, and could benefit from the password, the intruder has total access to the user's resources. In addition, there is no way to positively link the usage of the system or service to the actual user, that is, there is no protection against repudiation by the user ID owner. For example, when a user ID and password is shared with a colleague there is no way for the system to know who the actual user is. A similar situation arises when a transaction involving a credit card number is conducted on the Web. Even though the data are sent over the Web using secure encryption methods, current systems are not capable of assuring that the rightful owner of the credit card initiated the transaction. In the modern distributed systems environment, the traditional authentication policy based on a simple combination of user ID and password has become inadequate. Fortunately, automated biometrics in general, and fingerprint technology in particular, can provide a much more accurate and reliable user authentication method. Biometrics is a rapidly advancing field that is concerned with identifying a person based on his or her physiological or behavioural characteristics. Biometrics is derived from the conjunction of the Greek words *bios* and *metrics* that mean life and to measure respectively. Examples of automated biometrics include fingerprint, face, iris, and

speech recognition. 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 is 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. User authentication methods can be broadly classified into three categories. Because a biometric property is an intrinsic property of an individual, it is difficult to surreptitiously duplicate and nearly impossible to share. Additionally, a biometric property of an individual can be lost only in case of serious accident. Biometric readings, which range from several hundred bytes to over a megabyte.

The advantage that their information content is usually higher than that of a password or a passphrase. Simply extending the length of passwords to get equivalent bit strength presents significant usability problems. It is nearly impossible to remember a 2K phrase, and it would take an annoyingly long time to type such a phrase (especially without errors). Fortunately, automated biometrics can provide the security advantages of long passwords while retaining the speed and characteristic simplicity of short passwords.

Even though automated biometrics can help alleviate the problems associated with the existing methods of user authentication, hackers will still find there are weak points in the system, vulnerable to attack. Password systems are prone to brute force dictionary attacks. Biometric systems, on the other hand, require substantially more effort for mounting such an attack. Yet there are several new types of attacks possible in the biometrics domain. This may not apply if biometrics is used as a supervised authentication tool. But in remote, unattended applications, such as Web-based e-commerce applications, hackers may have the opportunity and enough time to make several attempts, or even physically violate the integrity of a remote.

A problem with biometric authentication systems arises when the data associated with a biometric feature has been compromised. For authentication systems based on physical tokens such as keys and badges, a compromised token can be easily cancelled and the user can be assigned a new token. Similarly, user IDs and passwords can be changed as often as required. Yet, the user only has a limited number of biometric features (one face, ten fingers, two eyes). If the biometric data are compromised, the user may quickly run out of biometric features to be used for authentication. Only the biometric authentication is based on an intrinsic part of a human being. So unlike a password or PIN or Smart Card, it can't be forgotten, misplaced, lost or stolen. We are having our identification with ourselves and therefore there is no need to carry any card or remember passwords for our identification. A biometric template is unique for an individual for whom it is created. Biometrics ensures that the person trying to access your network and applications is actually a sanctioned user, and not in a possession of a stolen smartcard or someone who found, hacked or cracked password. It is not only the initial cost that of the sensor or the matching hardware that is involved. Often the life cycle support cost can overtake the initial cost of the hardware. Most of the biometric systems like fingerprint recognition, iris recognition etc. are accurate. But some others like facial recognition etc. are not that accurate.

1.1 HISTORY AND DEVELOPMENT OF BIOMETRICS

The idea of using patterns for personal identification was originally proposed in 1936 by ophthalmologist 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.

Daugman algorithms are owned by Iridian technologies and the process is licensed to several other Companies who serve as System integrators and developers of special platforms exploiting iris recognition. In recent years several products have been developed for acquiring its images over a range of distances and in a variety of

applications. One active imaging system developed in 1996 by licensee Sensor deployed special cameras in bank ATMs to capture IRISImages at a distance of up to 1 meter. This active imaging system was installed in cash machines both by NCR Corps and by Diebold Corp in successful public trials in several countries during 1997to 1999. A new and smaller imaging device is the low cost “Panasonic Authenticam” digital camera for handheld, desktop, e-commerce and other information security applications. Ticketless air travel, check-in and security procedures based on iris recognition kiosks in airports have been developed by eye ticket. Companies in several countries are now using Daugman's Algorithms in a variety of products.

1.2 WHAT IS BIOMETRIC?

1.2.1 SINGLE BIOMETRIC:

Biometric technologies are defined as automated methods of identifying or authenticating the identity of a living person based on unique physiological or behavioural characteristics. Biometrics can provide very secure and convenient authentication for an individual since they cannot be stolen or forgotten and are very difficult to forge.

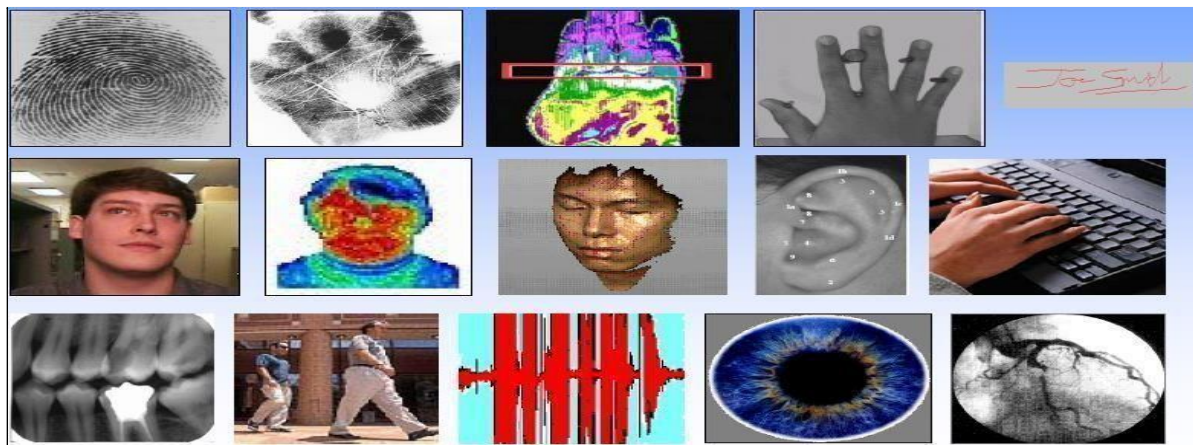


Figure 1.1 Single Biometric

The term “biometrics” is derived from two Greek words ‘bios’ for life and ‘metron’ for measure. A biometric can be described as a measurable physical and/or behavioral trait that can be captured and used to verify the identity of a person by comparing the metric to a previously stored template. The area of biometrics can therefore be defined as the task of automatically recognizing a person using his/her distinguishing traits. Examples of these “distinguishing traits” are fingerprints, voice patterns, facial characteristics etc. The idea of biometric identification is not new, it has been around for centuries. Example of a biometric is the photo on identification cards and passports, which still is the most important way of verifying the identity of a person. As early as the 14th century, the Chinese were reportedly using fingerprints as a form of signature. During the late 1890’s, a method of bodily measurement called “Bertillonage” (after its founder Alphonse Bertillon) was used by the Police Department in Paris & France and this identification was based on the number of bodily measurement and physical description. The difference today, is that we now have access to technologies enabling us to do these verifications automatically and almost in real- time.

Practically all biometrics systems work in the same manner, first a person is enrolled into a database using The specified method, information about a certain characteristics of the human being is captured, this information is usually placed through an algorithm that turns the information into a code that the database stores. When the person needs to be identified, the system will take the information about the person, again this new information is placed through the algorithm and then compares the new code with the ones in the database to discover a match and hence, identification.

1.2.2 MULTIMODAL BIOMETRIC:

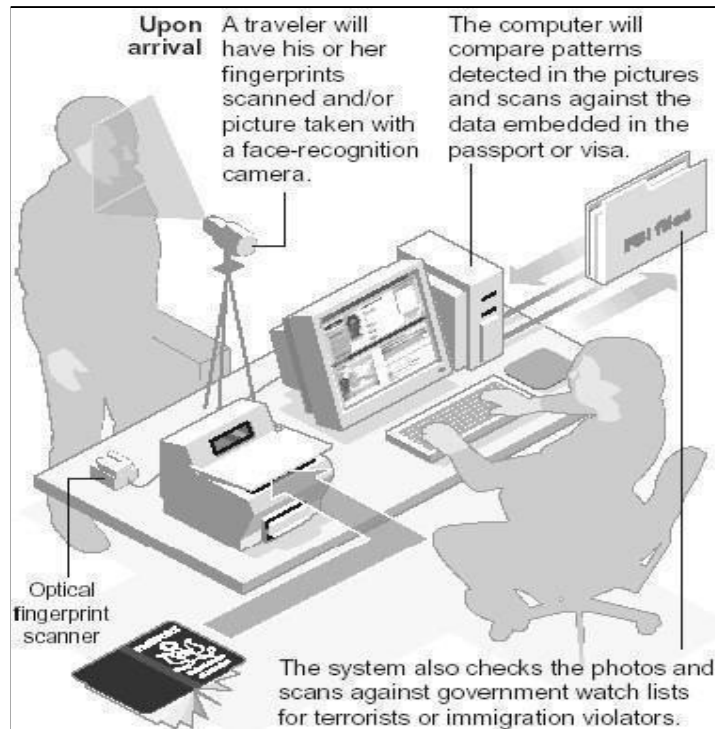


Figure 1.2 Multimode Biometric

A multimodal biometric system uses multiple applications to capture different types of biometric. This allows the integration of two or more types of biometric recognition and verification system in order to meet stringent performance requirements. A multimodal system could be a combination of finger print verification, face recognition, voice verification and smart card or any other combination of biometrics. For instance it is estimated that 5% of the population does not have legible fingerprints, a voice could be altered by a cold and face recognition systems are susceptible to changes in ambient light and the pose of the subject. This enhanced structure takes advantage of the proficiency of each individual biometric and can be used to overcome some of the limitations of a single biometric.

1.3 CLASSIFICATION OF BIOMETRICS

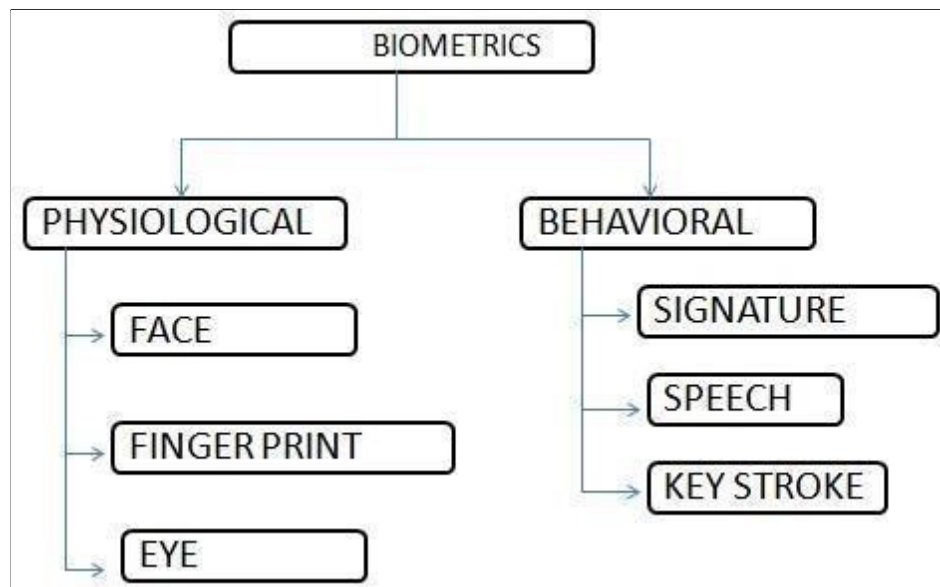


Figure 1.3 Classification of Biometrics

- A physiological characteristic is a relatively stable physical characteristic, such as an individual's fingerprint, hand geometry, iris pattern, or blood vessel pattern on the back of the eye. This type of biometric measurement is usually unchanging and unalterable without significant duress to the individual.

Physical biometrics :

- Fingerprint- Analyzing fingertip patterns.
- Facial Recognition- Measuring facial characteristics.
- Hand Geometry- Measuring the shape of the hand.
- Iris recognition- Analyzing features of colored rings of the eye.
- Vascular Patterns- Analyzing vein patterns.
- Retinal Scan- Analyzing blood vessels in the eye.
- Bertillonage- Measuring body lengths (no longer used).

A behavioral characteristic is more a reflection of an individual's psychological makeup. A signature is the most common behavioral biometric used for identification. Because most behavioral characteristics vary over time, an identification system using these must allow updates to enrolled biometric references.

Behavioral biometrics:

- Speaker Recognition- Analyzing vocal behavior.
- Signature- Analyzing signature dynamics.
- Keystroke- Measuring the time spacing of typed words.

1.4 BASIC STRUCTURE OF A BIOMETRIC SYSTEM

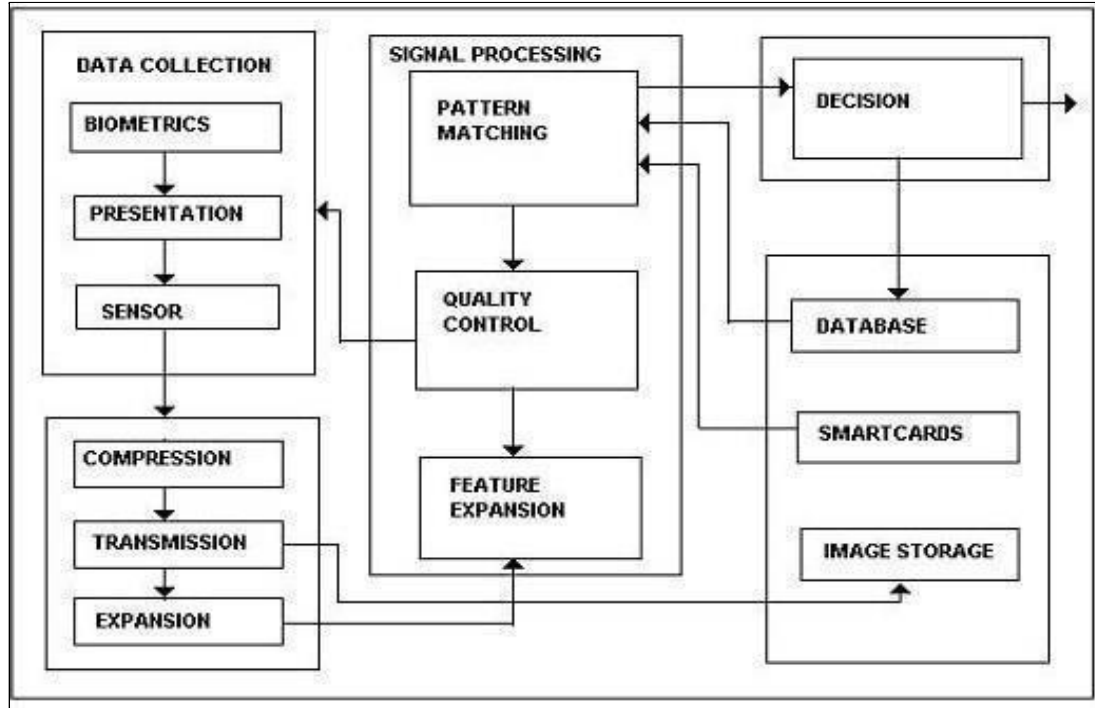


Figure 1.4 Basic Structure of Biometric

CHAPTER 2

LITERATURE SURVEY

2.1 ATM Transaction Security Using Fingerprint Recognition

This paper deals with the solutions related to the ATM (Automated Teller Machine) security. Today, ATMs and Credit cards are used for the purpose of money transactions which play a vital role in the nature of trade. The weaknesses of existing authentication schemes such as password and PIN number caused the leakage of information stored in ATM smartcards which lead to the loss of money in bank accounts and private information misuses. To overcome this shortcoming of piracy in money transactions, we propose the idea of using fingerprints of customers as passwords included with traditional PIN numbers. After authorized verification, the customer will be able to proceed for transaction else after three successive wrong attempts, the ATM card will be blocked for 24 hours and a message will be sent to the registered mobile number. Fingerprint biometric of every person is unique and unchangeable as well as one of the famous techniques for smart card security.

Today the ATM users are increasing. An Automated Teller Machine (ATM) is a computerized telecommunications device that enables the clients of any financial institution to perform financial transactions like deposits, transfers, balance enquiries, mini statements, withdrawal and fast cash. The ATM machine has a card Reader and keys as input devices and display screen, cash dispenser, receipt printer, speaker as output devices. ATMs are connecting to a host processor, which is a common gateway through which various ATM networks become available to users. Various banks, independent service providers owned this host processor. ATM card holders pins are different from each other. The number is verified by the bank and allows the customers to access their account. The password is only identity so anyone can access the account when they have the card and correct password. Once the card and the password is stolen by the culprit they can take more money from the account in the shortest period, it may bring huge financial losses to the users [2]. Biometric technology is the most widely accepted and mature biometric method and is the easiest to deploy and for a higher level of security. Using biometric identifiers offers several advantages over traditional and current methods. It is simple to install and also it takes little time and effort to acquire one's fingerprint with a fingerprint

identification device. Thus, fingerprint recognition is considered among the least intrusive of all biometric verification techniques. Though fingerprint images are initially captured, the images are not stored anywhere in the system. Instead, the fingerprints are converted to templates from which the original fingerprints cannot be recreated; hence no misuse of the system is possible. ATM can be described as Any Time Money. We can get money at any time anywhere only through ATM machines. To do the secure transactions we need biometric authentication. Biometric authentication is a growing and controversial field. Today biometric laws and regulations are in process and biometric industry standards are being tested. According to [11], there are three popular attacks against ATM: Skimming, PIN logging and Integrity violation. There are also attacks against mobile phones: Fake mobile apps installation, key logging software and grab PIN number during transmission. Besides that, an attack may also be a combination of both types of said attacks. Information also can be exploited by a side channel attack [4]. It is found that attackers try to get the user's account information that is stored on the magnetic strip present at the back side of the ATM card. Password is the only identity that can be used to authenticate the owner of an ATM card. It means anyone can access the account bank through the ATM machine as the password entered is correct. So, once the ATM card and password is lost or stolen by anyone, they can withdraw the money from that account easily without the problem of user authentication [4]. Thus, it can be seen that the most serious issue raised in ATM card security is about user authentication. User authentication is important because it leads to the integrity violation of bank account information. It seems that this issue is worse as anyone can access all information stored when they entered the correct password towards accessing an ATM card at an ATM machine. Other than that, it is strongly emphasized that the security issues need technology improvements and better security policy as a countermeasure. Murthy and Reddy developed an embedded fingerprint system, which is used for ATM security applications. In their system, bankers collect customers' finger prints and mobile numbers while opening accounts, then customer only access ATM machine. The working of the ATM machine is such that when a customer place a finger on the finger print module it automatically generates every time different 4-digit code as a message to the mobile of the authorized customer through GSM modem connected to the microcontroller. The code received by the customer is entered into the ATM machine by pressing the keys on the touch screen. After entering it checks whether it is a valid one or not and

allows the customer further access. Biometrics can be defined as measurable physiological and behavioral characteristic that can be captured and subsequently compared with another instance at the time of verification. It is automated methods of recognizing a person based on a physiological or behavioral characteristic FINGER VEIN EXTRACTION AND AUTHENTICATION BASED ON GRADIENT FEATURE SELECTION ALGORITHM SYSTEM FOR ATM In this project, we propose a real-time embedded finger-vein recognition system for authentication on mobile devices. The system is implemented on an embedded platform and equipped with a novel finger-vein recognition algorithm. The proposed system consists of three hardware modules: image acquisition module, embedded main board, and human machine communication module. The structure diagram of the system is, the image acquisition module is used to collect finger-vein images. The Embedded main board including the Microcontroller chip, memory (flash), and communication port is used to execute the finger-vein recognition algorithm and communicate with the peripheral device. The human machine communication module (LED or keyboard) is used to display recognition results and receive inputs from users. Our proposed system is an intelligent security system. Here we developed the teller machine concept. If finger vein matched, means transaction successful via GSM technology.

- Private information is traditionally provided by using passwords or Personal Identification Numbers (PINs), which are easy to implement but is vulnerable to the risk of exposure and being forgotten.
- Biometrics, which uses human physiological or behavioral features for personal identification, has attracted more and more attention and is becoming one of the most popular and promising alternatives to the traditional password or PIN based authentication techniques
- There is a long list of available biometric patterns, and many such systems have been developed and implemented, including those for the face, iris, fingerprint, palmprint, hand shape, voice, signature, and gait. Notwithstanding this great and increasing variety of biometrics patterns, no biometric has yet been developed that is perfectly reliable or secure. For example, fingerprints and palm prints are usually frayed; voice, signatures, hand shapes, etc.

- There has been a newspaper report of a man selling stolen watches sending images of them on a mobile phone, and those images included parts of his hands in enough detail for police to be able to identify fingerprint patterns.
- Classifying fingerprints Before computerisation replaced manual filing systems in large fingerprint operations, manual fingerprint classification systems were used to categorize fingerprints based on general ridge formations (such as the presence or absence of circular patterns on various fingers), thus permitting filing and retrieval of paper records in large collections based on friction ridge patterns alone.
- The most popular ten-print classification systems include the Roscher system, the Juan Vucetich system, and the Henry Classification System. Of these systems, the Roscher system was developed in Germany and implemented in both Germany and Japan, the Vucetich system (developed by a Croatian-born Buenos Aires Police Officer) was developed in Argentina and implemented throughout South America, and the Henry system was developed in India and implemented in most English- speaking countries.
- In the Henry system of classification, there are three basic fingerprint patterns: Loop, Whorl and Arch, which constitute 60–65%, 30–35% and 5% of all fingerprints respectively.
- There are also more complex classification systems that break down patterns even further, into plain arches or tented arches, and into loops that may be radial or ulnar, depending on the side of the hand the tail points towards. Whorls may not have subgroup classifications it including only plain whorls.
- 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 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 from personal information. Biometric templates cannot be reverse-engineered to recreate personal information and they cannot be stolen and used to access personal information

1) Fingerprint is a dependable biometric trait as it is idiosyncratic and dedicated. It is a technology that is increasingly used in various fields like forensics and security purposes. The vital objective of our system is to make ATM transactions more secure and user friendly. This system replaces traditional ATM cards with fingerprints. Therefore, there is no need to carry ATM cards to perform transactions. The money transaction can be made more secure without worrying about the card to be lost. In our system we are using an embedded system with biometrics i.e r305 sensor and UART microcontroller. The Fingerprint and the user_id of all users are stored in the database. Fingerprints are used to identify whether the Person is genuine. A Fingerprint scanner is used to acquire the fingerprint of the individual, after which the system requests for the PIN (Personal Identification Number). The user gets three chances to get him authenticated. If the fingerprints do not match further authentication will be needed. After the verification with the data stored in the system database, the user is allowed to make transactions. (Fingerprint based ATM System By Nisha Bhanushali, Meghna Chapaneria ,Krishani Mehta, Mansing Rathod).

2) The main objective of this system is to develop an system which is used for ATM security applications. In these systems, Bankers will collect the customer fingerprints and mobile number while opening the accounts then the customer only accesses the ATM machine. The working of these ATM machines is when a customer places a finger on the finger print module when access automatically generates every time different 4-digit code as a message to the mobile of the authorized customer through GSM modem connected to the microcontroller. The code received by the customer should be entered by pressing the keys on the screen. After entering it checks whether it is a valid one or not and allows the customer further access. (ATM Transaction Using Biometric Fingerprint Technology By Mr. Mahesh A. Patil Mr.Sachin P.Wanere Mr.Rupesh P.Maighane Mr.Aashay R.Tiwari).

3) The main objective of this system is to develop a system that will increase the ATM security. However, despite the numerous advantages of the ATM system, ATM fraud has recently become more widespread. In this paper, we provide an overview of the possible fraudulent activities that may be perpetrated against ATMs and investigates recommended approaches to prevent these types of frauds..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. An 8-bit ATmega16 microcontroller developed by Microchip Technology is used in the system. The necessary software is written by an AVR studio programmer and the system is tested. (RBI 3X-Fingerprint Based ATM Machine By Bharti Patil¹, Bhagwan S. Chandrika R², Mahesh P. Chavan³, Bhavesh S. Chaudhri⁴ E&TC Dept, PVPIT, Bavdhan, Pune^{1,2,3,4}).

4) The existing ATM machine uses PIN-Card as a security which is very weak and easy to contravene. This paper tries to find a solution to the above problems by introducing fingerprint authentication into the existing ATM machine. A program prototype was designed to imitate a typical ATM system that uses fingerprint identification to enhance the security of the ATMs. The proposed system demonstrated a three-tier architectural structure. The verification system which centered on the enrolment, enhancement, feature extraction and matching of fingerprints. The backend database system that serves as warehouse of the templates of all ATM account holders' pre-registered fingerprints. The system's platform creates related transactions such as withdrawals, bill payment, buying of credit cards and balance enquiries etc. The results obtained confirm that the current approach could significantly reduce ATM fraud if not totally eradicate

During the early 1960's, people accessed their bank accounts by going to bank tellers for all transactions: deposits, cash withdrawals, money transfers and balance inquiries. The introduction of Automated Teller Machines (ATMs) during the late 1960's reduced the overhead of traveling time to banks to make transactions. An electronic telecommunications device to perform financial transactions without a human cashier's need is an Automated Teller Machine [1]. They are made accessible at banks, hotels, gas stations, airports, grocery stores, shopping malls, school campuses or any other public places that promote consumerism. Debit/credit cards are mainly printed with a unique sixteen-digit number, a three-digit CVV (Card Verification Value) number and an expiration date. To help prevent fraud, card number combinations remain unique and CVV numbers are displayed on the back for additional security. The current ATM systems require users to swipe a debit/credit card to authenticate. To verify the user's identity, existing ATM systems authenticate

in two steps: First, swipe the magnetic stripe of the credit/debit card to access account details. Second, enter a four-digit PIN (Personal Identification Number) to unlock the account associated with the credit/debit card's chip. 2 To access an ATM, users stand in front of the machine while those waiting stand in a line a few feet away from the user. The keypads do not have a protective cover, so the clear scope over user's shoulder allows on-lookers to decipher the PIN number. A user's account is easily accessed if the credit/debit card is stolen and used with the deciphered PIN number. The objective of this project is to provide a safer ATM authentication system addressing the drawbacks of the current system. Authentication is a mechanism that makes sure a user is who he claims to be when using a system or data that is sensitive. It confirms the claim of attestation to identity of a person or a thing. For example, a digital certificate assigned to it by Certificate Authority verifies a website's authenticity. Similarly, an ATM authenticates the identity of a user with a PIN number. Therefore, it is important to protect the PIN number, as it is sensitive data. Authentication systems must be made strong and transparent. The proposed solution consists of three steps of authentication, which are as follows: 1. a scrambling keypad to input PIN; 2. color-coded combination password; 3. biometric fingerprint authentication,

2.2 ATM Security system using Non biometric technology

[1]. Sankhwar et al. talk about how fraudsters trick the ATM users into handing over their card and PIN numbers to the fraudsters after a shoulder suffering attack (on-lookers deciphering PINs) with the use of hidden cameras to decipher the user's PIN or skimmer devices to create fraud copies of ATM cards

[2]. Furthermore, fraudsters use keypad overlays that do not function properly for the user but the actual device underneath captures user information to withdraw money from the user's account. They proposed the idea of a One Time Password (OTP) to mitigate the security risks.

The user receives an OTP after swiping his card to access the ATM and to further make transactions through the ATM machine, he needs to manually feed the ATM machine with the OTP sent to him. Another idea proposed to protect ATMs from fraudsters is to use a digital swapping 4 keypad. Oruh proposed an authentication mechanism, which consists of reading data from the smart card reader chip,

transmitting the PIN number to the server in an encrypted form and using a biometric fingerprint system

[3]. Enhanced biometric systems were produced which take fingerprint input from the user, convert it to an image, encrypt the image using the blowfish algorithm and store it in the database to retrieve it when accessed by the user going forward

[4]. The time limit to make transactions on the proposed system is as low as 10 seconds in order to achieve high security to make transactions in an ATM.

One of the low-tech ATM frauds discussed was a shoulder-surfing attack where onlookers observe the PIN number and mug users for the cards. Although the attempts for banks to make ATM keypads tamper-proof were mentioned, no such mechanisms were implemented so far

[5]. Due to the predominant increase in the percentage of ATM frauds during the past few years in Nigeria a literature, review was conducted to address these concerns

[6]. One of the tricks fraudsters used were to steal the PIN number, get hold of user's funds and withdraw all the cash before he realizes it.

The federal commission's issue states that a user is not responsible for any unauthorized withdrawals if reported at an early stage otherwise can be held responsible for those fraudulent withdrawals

[7]. 5 Common security measures of hiding the keypad when entering a PIN with the second hand or a wallet to prevent on-lookers to decipher PIN were discussed

[8]. But this is not always possible due to physical hindrances. For example, he might be holding shopping bags. So, it is recommendable to provide a strong and user-friendly authentication system.

CHAPTER 3

SYSTEM DESIGN

Design Approach This project was developed using functional design approach. It is a modular approach. Each module is a function of its own and as the modules are independent, the change in functional implementation of module will affect the functional implementation of the other modules minimally. Each authentication step in the proposed solution is identified into three independent modules for implementation purposes and integrated. The first module implements a scrambling keypad, second a color-coded password combination and finally a biometric fingerprint authentication. Each functional module consists of its own implementation and sub modules.

2.2 Detailed Design This project consists of three steps of authentication: The 6-digits ATM PIN number on a scrambling keypad, color-coded combination password identification and fingerprint recognition. A user must first register with all three before accessing his records. The user records are stored in a SQLite database in the form of rows. When a user authenticates using his account details, they are matched against the records in the database and the result (“valid” or “invalid” user) is returned. The registration and authentication processes are further explained with respective activity, sequence and architecture diagrams.

7 2.2.1 Registration The activity diagram below shows the workflow of activities for user registration process. In real world, a user swipes his debit/credit card to authenticate and use a teller machine. The bank issues these cards to users with bank accounts, so the user details are already registered with the bank. For demonstration purposes, this project stores user details entered by the user and the user needs to enter his account number to authenticate with the three steps.

Objective

1. In our proposed system we introduce an ATM which is purely based on biometrics. The use of multiple biometrics adds more security to the system.
2. The illegal access to the account can be prevented by the use of biometrics. Our prime objective is to reduce the effort of carrying smart cards and memorizing the PINs and to enhance the security of ATMs.

EXISTING SYSTEM:

- D. Wang et al. describes the fingerPrint pattern identification for electronics devices. In this, old biometric techniques are vulnerable for spoofing attacks. X. Sun et al. developed a DSP-based Authentication system using Print images. It made use of an LED illuminator for NIR light source. But the drawback is that the shadow will also appear in the scanned images.
- Private information is traditionally provided by using passwords or Personal Identification Numbers (PINs), which is vulnerable to the risk of exposure and being forgotten.
- There is a long list of available biometric patterns, and many such systems have been developed and implemented, including those for the face, iris, fingerprint, palm print, hand shape, voice, signature, and gait.
- Notwithstanding this great and increasing variety of biometrics patterns, no biometric has yet been developed that is perfectly reliable or secure.

PROBLEM STATEMENT

- ATM Card frauds
- Use of ATM card duplicators
- Card sharing by family and friends
- Inability to trace the wrongful users
- ATM PINs can be shared on phone or recorded using secret cameras

PROPOSED SYSTEM:

- The growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication.
- The finger-Print is a promising biometric pattern for personal identification in terms of its security and convenience.

- It is difficult to steal since the Print is hidden inside the body and is mostly invisible to human eyes. The non-invasive and contactless capture of finger-Prints ensures both convenience and hygiene for the user, and is thus more acceptable
- The finger-Print pattern can only be taken from a live body.
- Hence it is a natural and convincing proof that the subject whose finger-Print is successfully captured is alive.
- An embedded fingerprint biometric authentication scheme for automated teller machine (ATM) banking systems is proposed in this paper. In this scheme, a fingerprint biometric technique is fused with the ATM for person authentication to ameliorate the security level.

ADVANTAGES:

- Single/Multi factor Biometric Authentication: Fingerprint, Face.
- Multi Factor Authentication: Card + PIN + Biometrics
- Online or offline Authentication using smart cards
- Card less Authentication
- Biometrics is combination of card or PIN
- Biometric based ATM system
- Give acknowledgement to customer
- Avoid malfunctions
- Time maintenance system
- High Security systems

BLOCK DIAGRAM:

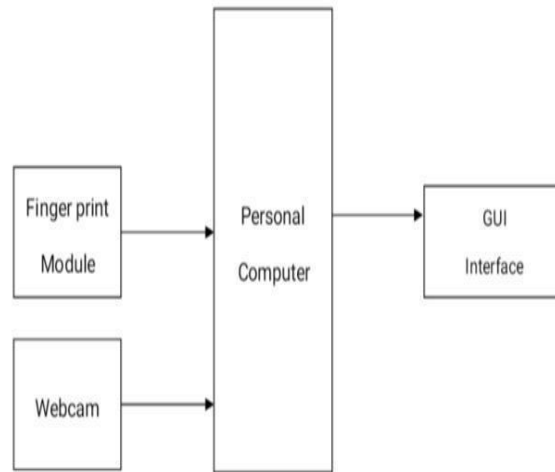


Figure 3.1 Block Diagram

This is the basic block diagram of our project, It includes

- A personal computer (laptop)
- A fingerprint module hardware which is externally connected to the laptop
- Here the web cam is inbuilt in the laptop which is used for face recognition
- And we get the output as a gui interface

Biometric System

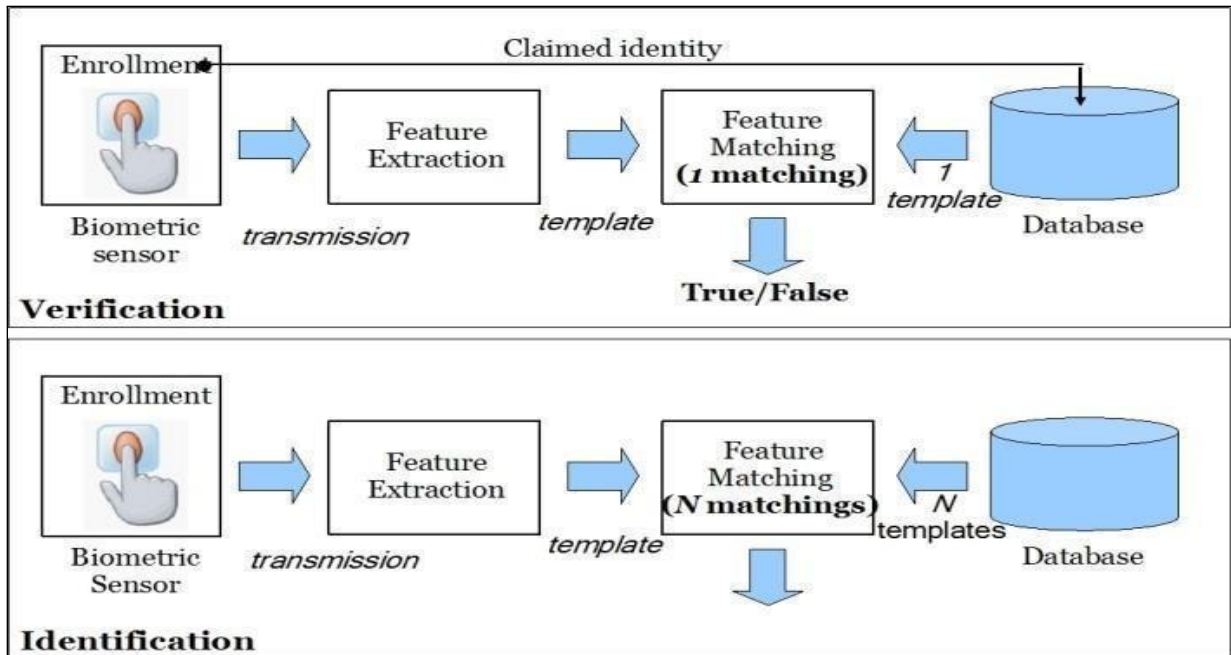


Figure 3.2 Biometric System

- As shown in the figure biometric image of the individual is captured during the enrollment process using the fingerprint module.
- This image is then transmitted and features are extracted (for eg. Features like length of the finger, breadth of the finger, lines on the finger, etc)
- These unique characteristics are then stored in user's biometric template.
- In verification The unique characteristics are extracted from the biometric image to create the users "live" biometric template.
- This new template is then compared with the template previously stored and a numeric matching score is generated, based on the percentage of duplication between the live and stored template.

CHAPTER 4

BIOMETRIC SYSTEM COMPONENTS AND PROCESS

4.1 COMPONENTS:

Three major components are usually present in a biometric system:

- A mechanism to scan and capture a digital or analog image of a living person's biometric characteristic.
- Software for storing, processing and comparing the image.
- An interface with the applications system that will use the result to confirm an individual's identity.

4.2 PROCESS:

Two different stages are involved in the biometric system process –

1) Enrollment,

2) Verification.

4.2.1 ENROLLMENT:

As shown in Figure 4.2.1, the biometric image of the individual is captured during the enrollment process (e.g., using a sensor for fingerprint, microphone for voice verification, camera for face recognition, scanner for eye scan). The unique characteristics are then extracted from the biometric image to create the user's biometric template. This biometric template is stored in a database or on a machine-readable ID card for later use during an identity verification process.

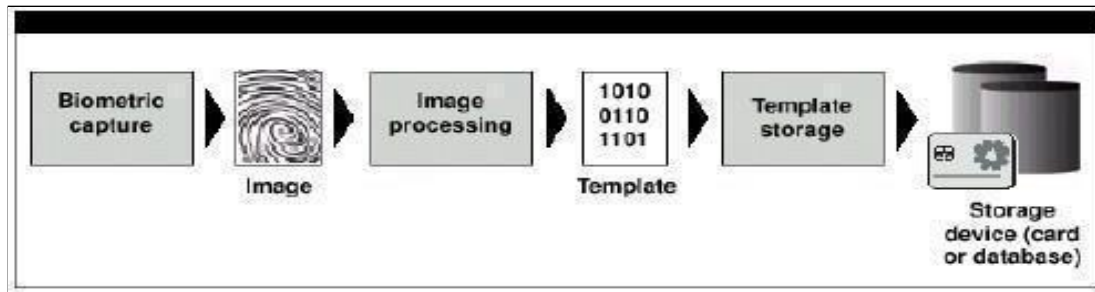


Figure 4.1 Enrollment Process

4.2.2 VERIFICATION:

Figure 4.2.2 illustrates the identity verification process. The biometric image is again captured.

The unique characteristics are extracted from the biometric image to create the users “live” biometric template. This new template is then compared with the template previously stored and a numeric matching score is generated, based on the percentage of duplication between the live and stored template. System designers determine the threshold value for this identity verification score based upon the security requirements of the system.

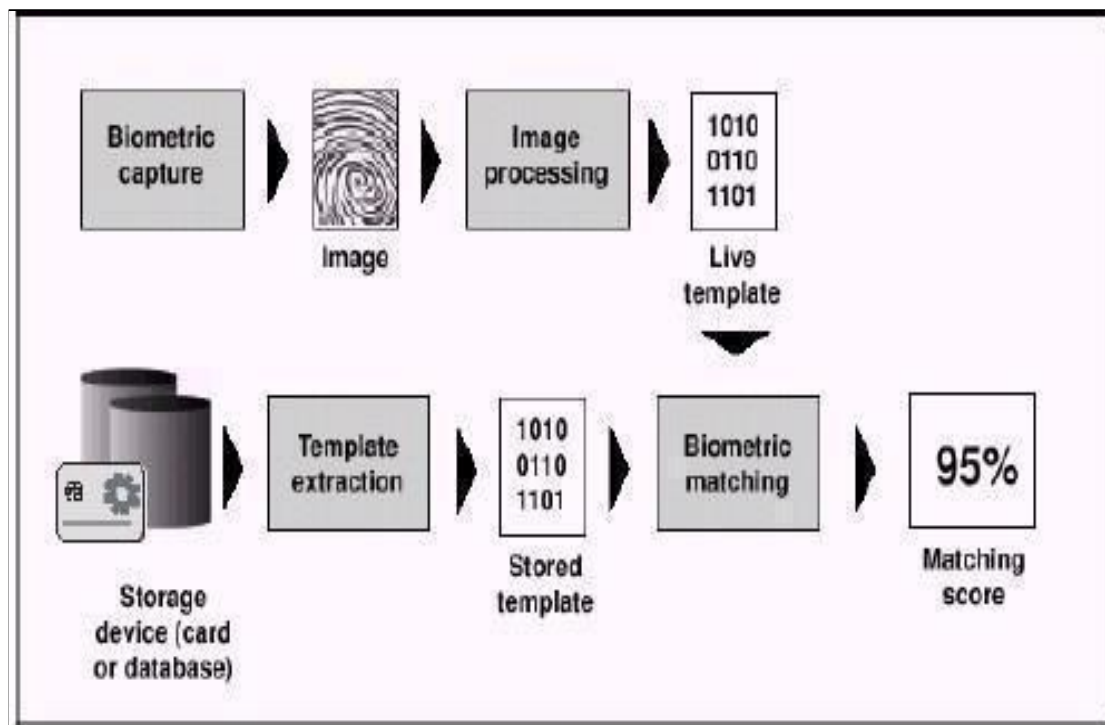


Figure 4.2 Verification Process

4.3 TYPES OF BIOMETRIC SYSTEM

There are two kinds of Biometric System

★ Recognition Systems

- ❖ Identifying a person among the whole group of users enrolled in the system.
- ❖ It must be an online system.

Typical applications : Forensics **Identification** (1-to-many comparison) verifies if the individual exists within a known population. Identification confirms that the individual is not enrolled with another identity and is not on a predetermined list of prohibited persons. Identification will typically need a secured database containing a list of all applying individuals and their biometrics. The biometric for the individual being considered for enrollment would be compared against all stored biometrics. For many applications, an identification process is used only at the time of enrollment to verify that the individual is not already enrolled.

★ Authentication Systems

- ❖ Verifying the identity that user claims to have.
- ❖ It can be offline.
- ❖ Typical applications: Access Control, all kinds of applications where cards are used.

Authentication(1-to-1 comparison) confirms that the credential belongs to the individual presenting it. In this case, the device that performs the authentication must have access only to the individual's enrolled biometric template, which may be stored locally or centrally.

BIOMETRIC ACCURACY

A key factor in the selection of the appropriate biometric technology is its accuracy.

Biometric accuracy is the system's ability of separating legitimate matches from imposters. When the live biometric template is compared to the stored biometric template, a matching score is used to confirm or deny the identity of the user. System designers set this numeric score to accommodate the desired level of accuracy for the system, as measured by the (FAR) and False Rejection Rate (FRR).

- **False Rejection Rate (FRR)** refers to the statistical probability that the biometric system is not able to verify the legitimate claimed identity of an enrolled person, or fails to identify an enrolled person.
- **False Acceptance Rate (FAR)** refers to the statistical probability of False Acceptance or incorrect verification. In the most common context, both False Rejection and False Acceptance represent a security hazard.
- **Equal-Error Rate** When the decision threshold is adjusted so that the false-acceptance rate equal the false-rejection rate.

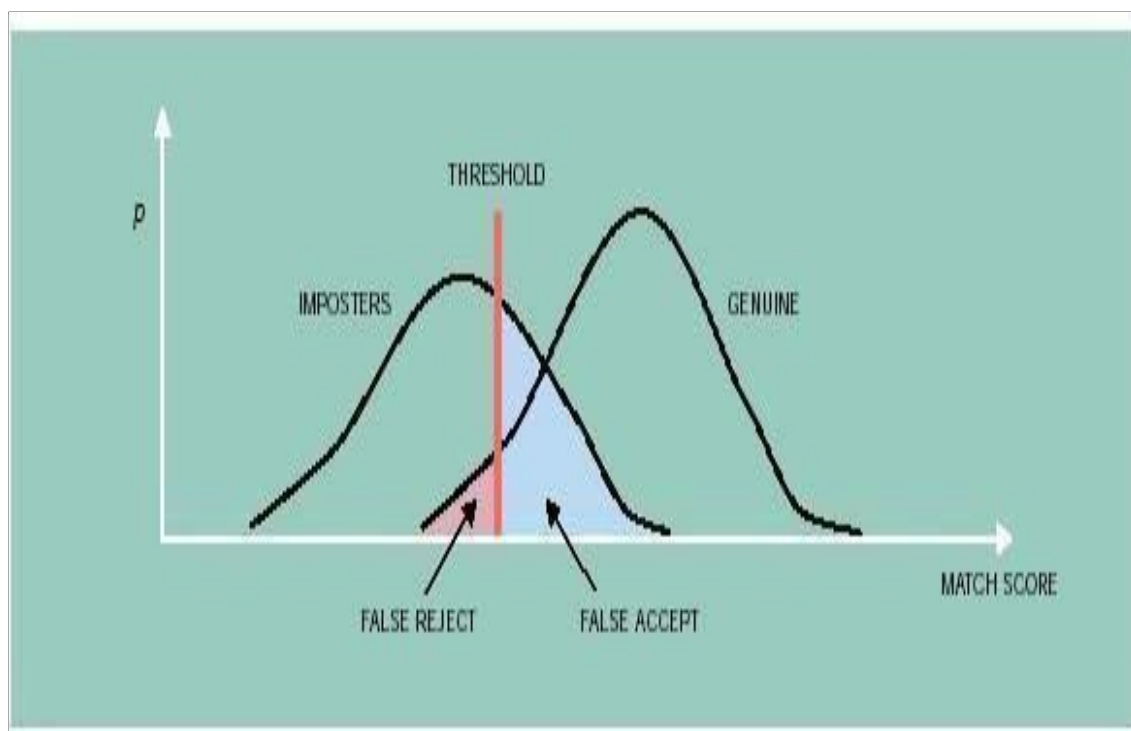


Figure 4.3 Error Rate

If a mismatching pair of fingerprints is accepted as a match, it is called a false accept. On the other hand, if a matching pair of fingerprints is rejected by the system, it is called a false reject. The error rates are a function of the threshold as shown in Figure 2.3. Often the interplay between the two errors is presented by plotting FAR against FRR with the decision threshold as the free variable. This plot is called the ROC (Receiver Operating Characteristic) curve. The two errors are complementary in the sense that if one makes an effort to lower one of the errors by varying the threshold, the other error rate automatically increases. In a biometric authentication system, the relative false accept and false reject rates can be set by

choosing a particular operating point (i.e., a detection threshold). Very low (close to zero) error rates for both errors (FAR and FRR) at the same time are not possible. By setting a high threshold, the FAR error can be close to zero, and similarly.

4.4 BIOMETRIC TECHNOLOGY

4.4.1 FINGERPRINT SCANNING:

- "Fingerprint authentication" describes the process of obtaining a digital representation of a fingerprint and comparing it to a stored digital version of a fingerprint.
- Fingerprints have long been recognized as a primary and accurate identification method.

4.4.1 PROCESS:

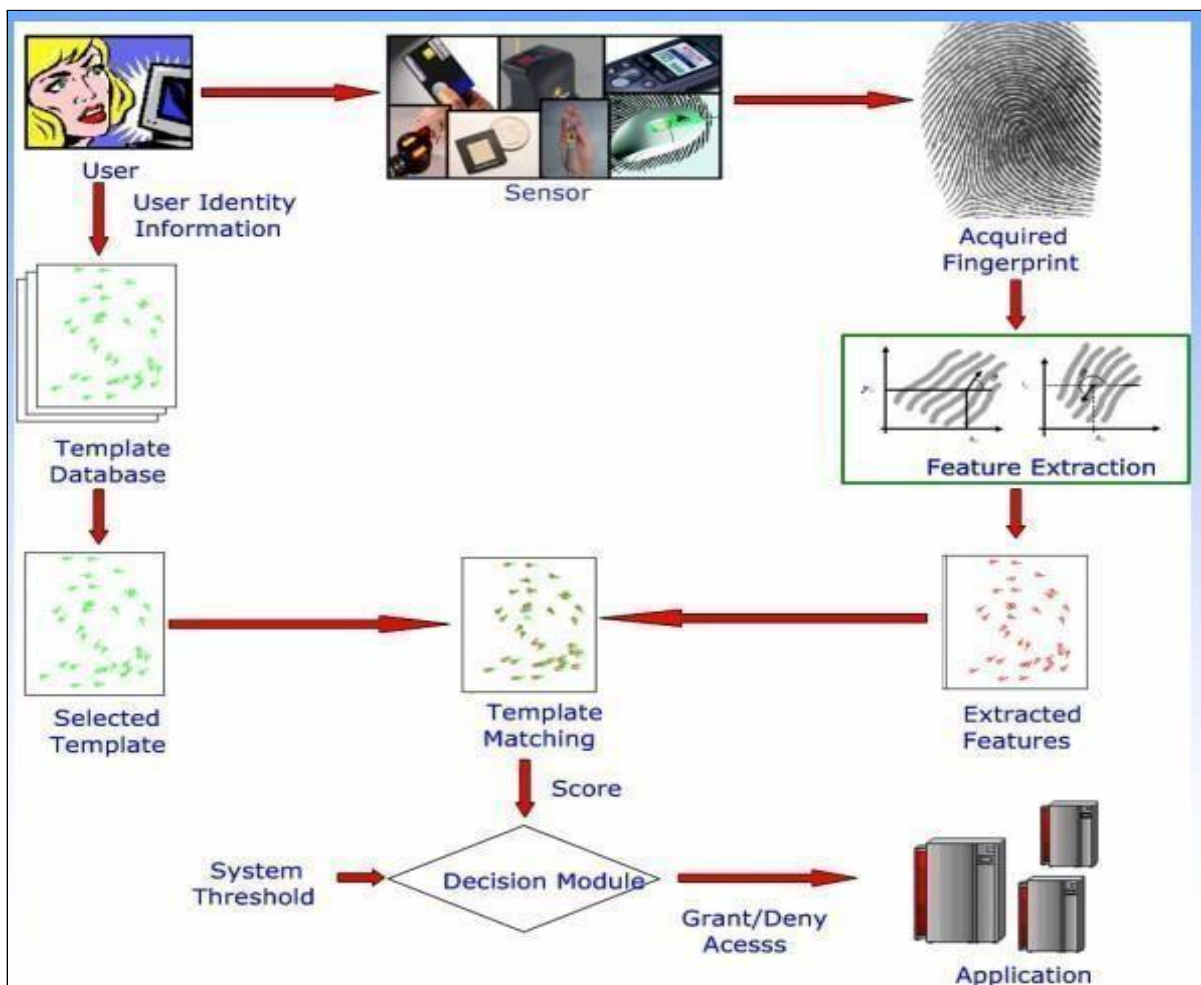


Figure 4.4.1 Fingerprint Authentication Process

- Electronic fingerprint scanners capture digital "pictures" of fingerprints, either based on light reflections of the finger's ridges and valleys, or the electrical properties of the finger's ridges and valleys.
- These pictures are then processed into digital templates that contain the unique extracted features of a finger. Uses the ridge endings and bifurcations on a person's finger to plot points known as Minutiae. The number and locations of the minutiae vary from finger to finger in any particular person, and from person to person for any particular finger
- These digital fingerprint templates can be stored in databases and used in place of traditional passwords for secure access.
- Instead of typing a password, users place a finger on an electronic scanner. The scanner, or reader, compares the live fingerprint to the fingerprint template stored in a database to determine the identity and validity of the person requesting access.
- Finally it gives a decision that access to application or access denied.

4.4.2. MATCHING APPROACH:

Two basic classes of matching techniques:

- Image Techniques :
Use both optical and numerical image correlation techniques.
- Feature Technique:
Extracts features and develops representations from these features.
- Combining the above two techniques:
Hybrid techniques ,with improved accuracy

4.4.2 ADVANTAGES AND DISADVANTAGES:

Advantages:

- ❖ Very high accuracy.
- ❖ Is the most economical biometric PC user authentication technique.
- ❖ It is one of the most developed biometrics.
- ❖ Easy to use.
- ❖ Small storage space required for the biometric template, reducing the size of the database memory required

Disadvantages:

- For some people it is very intrusive, because it is still related to criminal identification.
- It can make mistakes with the dryness or dirtiness of the finger's skin, as well as with the age (is not appropriate with children, because the size of their fingerprint changes quickly).
- Image captured at 500 dots per inch (dpi). Resolution: 8 bits per pixel. A 500 dpi fingerprint image at 8 bits per pixel demands a large memory space, 240 Kbytes approximately → Compression required.

4.5 FACIAL RECOGNITION SYSTEM:

- A **facial recognition system** is a computer-driven application for automatically identifying a person from a digital image. It does that by comparing selected facial features in the live image and a facial database.
- It is typically used for security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems. Popular recognition algorithms include eigenface, fisherface, the Hidden Markov model, and the neuronal motivated Dynamic Link Matching. A newly emerging trend, claimed to achieve previously unseen accuracies.

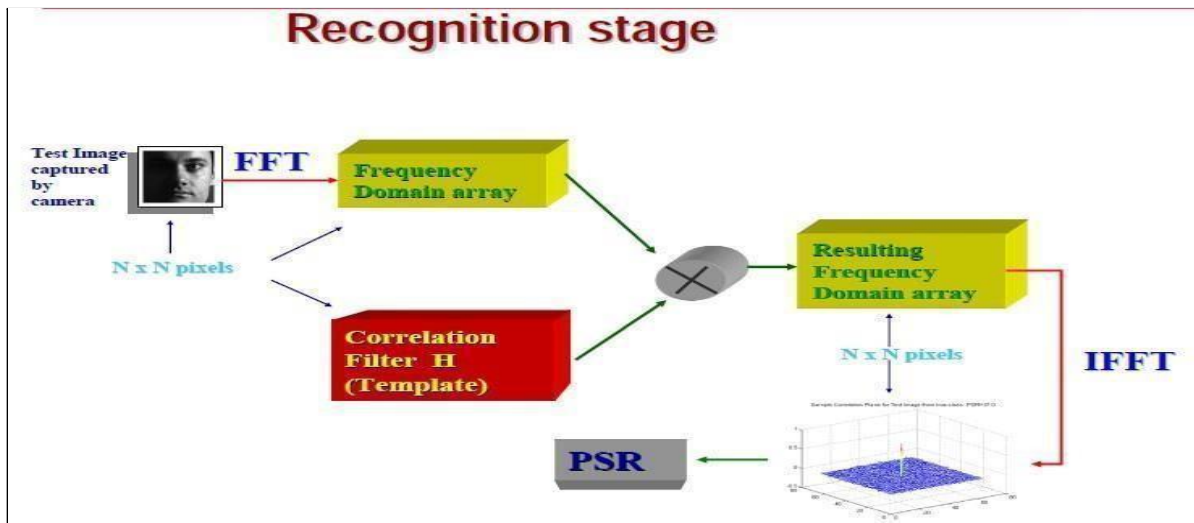


Figure 4.5 Facial Enroll and Recognition Stage

THREE DIMENSIONAL FACE RECOGNITION

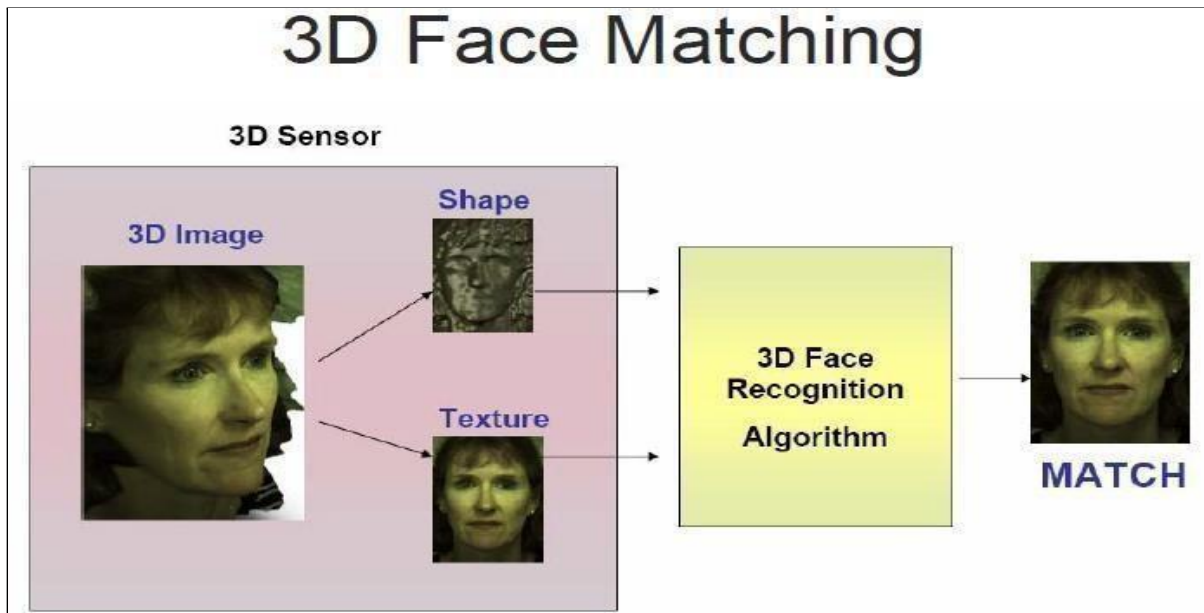


Figure 4.6 3D Face Masking

Three-dimensional face recognition (3D face recognition) is a modality of facial recognition methods in which the three-dimensional geometry of the human face is used. It has been shown that 3D face recognition methods can achieve significantly higher accuracy than their 2D counterparts, rivaling fingerprint recognition.

3D face recognition achieves better accuracy than its 2D counterpart by measuring geometry of rigid features on the face.[citation needed] This avoids such pitfalls of 2D face recognition algorithms as change in lighting, different facial expressions, make-up and head orientation. Another approach is to use the 3D model to improve accuracy of traditional image based recognition by transforming the head into a known view.

The main technological limitation of 3D face recognition methods is the acquisition of 3D images, which usually requires a range camera. This is also a reason why 3D face recognition methods have emerged significantly later (in the late 1980s) than 2D methods. Recently commercial solutions have implemented depth perception by projecting a grid onto the face and integrating video capture of it into a high resolution 3D model. This allows for good recognition accuracy with low cost off-the-shelf components.

A biometric system which relies only on a single biometric identifier in making a personal identification is often not able to meet the desired performance requirements. Identification based on multiple biometrics represents an emerging trend. We introduce a multimodal biometric system, which integrates face recognition, fingerprint verification, and speaker verification in making a personal identification. This system takes advantage of the capabilities of each individual biometric. It can be used to overcome some of the limitations of a single biometrics. Preliminary experimental results demonstrate that the identity established by such an integrated system is more reliable than the identity established by a face recognition system, a fingerprint verification system, and a speaker verification system.

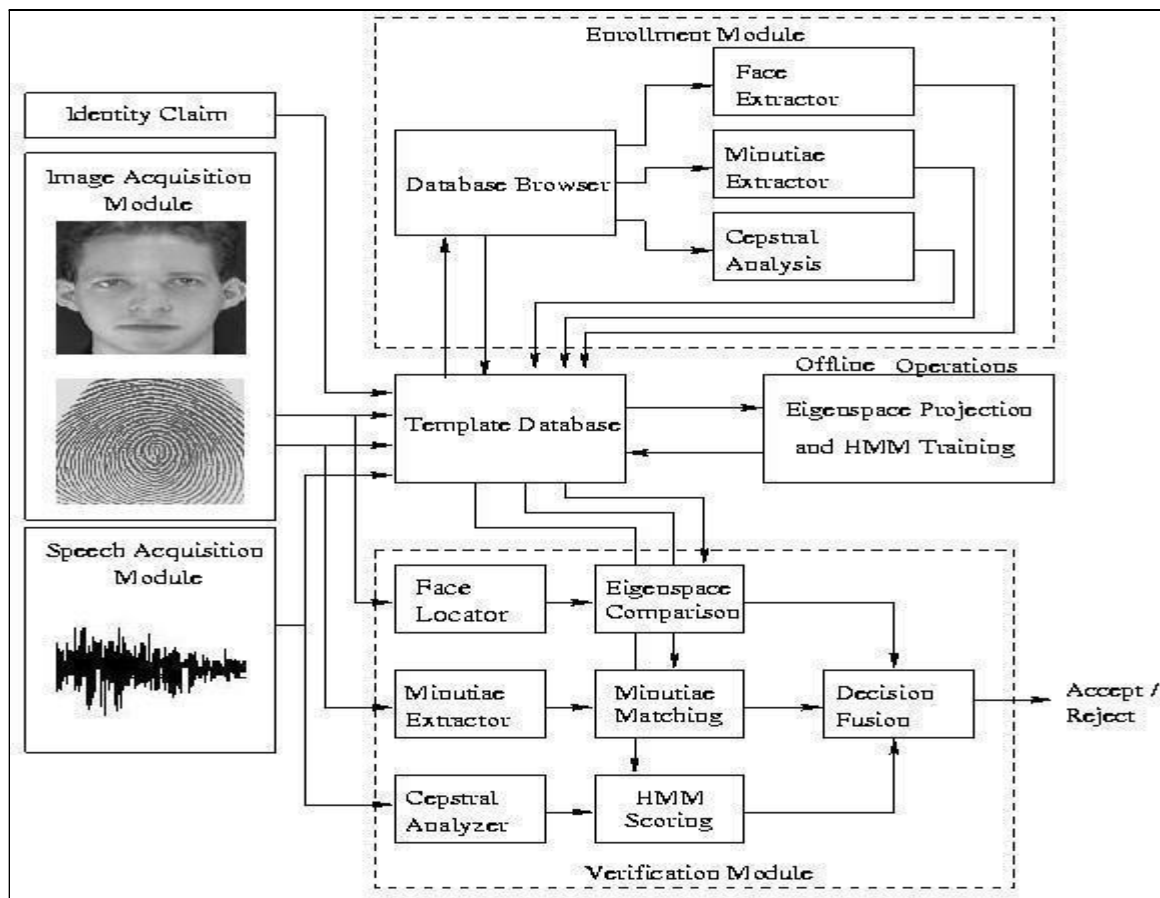


Figure 4.7 Multimode Biometric Using Fingerprint, Face and Voice

PROPOSED PLAN

Fingerprint verification is to verify the authenticity of one person by his fingerprint and PIN code and Fingerprint identification is by matching the information of user such as pin code and fingerprint matching. Basically we can explain complete Fingerprint base ATM system in two phases:

1) Enrolment Phase 2) Authentication phase

1. **Enrolment phase:** In the robust fingerprint application, 3-4 fingers should be enrolled. This enables the system to set high security threshold and still be able to cope with everyday real life issue like skewed finger placement dirty, wet dry, cut or worn fingers. Biometric reference data is collected enrolment and stored in database or in portable data carrier such Fig-3: Enrolment Phase The Enrolment is crucial because the once recorded reference data will normally be used over the active lifetime of user or his/her biometric

hardware device. Multiple Finger enrolment: It is strongly recommended enrolling more than one finger. During daily life injuries can happen that turn a registered fingerprint currently unusable while minor cuts not affect a robust sized sensor system.

2. **Authentication Phase:** In these phase user can make transaction by using their fingers. User can place finger on the Biometric scanner and user's finger scan can be matched through database, where all authenticated user's fingerprints are stored .If User wants to do transaction they simply place their finger on biometric scanner and get their money in few seconds. If user's fingerprint cannot matched by database due to some accidental cuts on their fingers than they can used their other fingers and we will also provide a 4 pin code option ,user can also use this option with their convinces. Feature extraction: Feature extraction from a fingerprint image is generally categorized into three levels. Feature can used to categorize into major pattern type such as loop or whorl.

SOFTWARE OF FINGERPRINT SENSOR BASED ATM SYSTEM

The core section includes the software part utilizes two different programs-enroll and fingerprint.getFingerprintEnroll(int,id), Adafruit Fingerprint (& mySerial) and getFingerprintEnroll(id) are some of the different functions syntax used in those programs. These are in-built functions found in library and they pass arguments when these functions are called at different locations of programs. Once the enroll part of the program has been uploaded in the Arduino Uno, go through the Arduino IDE and then open the serial monitor by opening tabs like tools and then select serial monitor options. It is necessary to set the baud rate to a value lower than the serial monitor window to 38400. At the same time choose Newline option. And now, one by one execute the instructions given on the serial monitor. Once you place a finger on the fingerprint module, type an ID number. It can be any whole number. Then when send key is entered, the corresponding ID number is transmitted to the main portion i.e. Arduino Uno form the serial monitor section. Thus sent information (fingerprint) is digitized and converted into storable form which is piled up in R305 module database. This system can withstand a total of 200+ fingerprints which is remarkable. However, each fingerprint must have unique ID number assigned since this is the prime factor to be utilized in identification of the valid individuals name. The serial monitor assists the client in an effective way. Every real-time information of when to place the finger on the sensing module and when it is okay to remove, is all provided by the

serial monitor which makes this project more userfriendly. If you prefer to debug the system without implementing LCD display, initially upload the fingerprint program and then set the same settings as mentioned above for the serial monitor configuration. Here again the serial monitor performs the guide function. This technique of implementing circuit is employed to make necessary comparisons between the current sensed fingerprint sample with the samples already stored in the database. The programming flexibility feature permits customer to amend necessary changes in names and ID number by changing the code to a slight extent as per the requirement.

What is Face Detection:

In computer vision, one essential problem we are trying to figure out is to automatically detect objects in an image without human intervention. Face detection can be thought of as such a problem where we detect human faces in an image. There may be slight differences in the faces of humans but overall, it is safe to say that there are certain features that are associated with all the human faces. There are various face detection algorithms but Viola-Jones Algorithm is one of the oldest methods that is also used today and we will use the same later in the article. You can go through the Viola-Jones Algorithm after completing this article as I'll link it at the end of this article.

Face detection is usually the first step towards many face-related technologies, such as face recognition or verification. However, face detection can have very useful applications. The most successful application of face detection would probably be photo taking. When you take a photo of your friends, the face detection algorithm built into your digital camera detects where the faces are and adjusts the focus accordingly.

CHAPTER 5

SOFTWARE HARDWARE REQUIREMENTS

- Python 2.7.14 compile
- Personal computer
- Finger print module and web camera
- Python programming language.

HARDWARE REQUIREMENTS:

Finger print module

- Security with biometrics can be done with the help of R305 Fingerprint Module. This fingerprint sensor module will make adding fingerprint detection and verification super simple.
- These modules are typically used in safes – there's a high powered DSP chip that does the image rendering, calculation, feature-finding, and searching. Connect to any microcontroller or system with TTL serial, and send packets of data to take photos, detect prints, hash, and search.
- You can also enroll new fingers directly- up to 162 fingerprints can be stored in the onboard FLASH memory. There's a red LED in the lens that lights up during a photo so you know it's working.

Integrated image collecting and algorithm chip together .ALL in one ,fingerprint reader can conduct secondary development,can be embedded into a variety of end products ,low power consumption ,low cost ,small size,excellent performance ,professional optical technology,precise module manufacturing techniques ,good image processing capabilities,can successfully capture image up to resolution 500dpi.

FINGERPRINT SCANNER



Figure 5.1 Fingerprint Scanner

A fingerprint scanner is an electronic device used to capture a digital image of the fingerprint pattern. This scan is digitally processed to create a biometric template which is stored and used for matching.

What is the Fingerprint Sensor?

The fingerprint sensor is one kind of sensor which is used in a fingerprint detection device. These devices are mainly inbuilt in the fingerprint detection module and it is used for computer safety. The main features of this device mainly include accuracy, better performance, robustness based on exclusive fingerprint biometric technology. Both fingerprint scanner otherwise reader are an extremely safe & suitable device for safety instead of a secret word. Because the password is easy to scan and also it is hard to keep in mind

So, better to use USB based fingerprint reader or scanner using biometric software for verification, identification, and authentication, that allow your fingerprints to perform similar to digital passwords. These passwords cannot be forgotten, lost otherwise stolen.

R305 Fingerprint Sensor Module

There are different types of fingerprint modules available in the market like R305, R307. For a better understanding of this sensor, here we are going to discuss an overview of R305 fingerprint sensor module.



Figure 5.2 R305 Fingerprint Sensor Module

R305-fingerprint-sensor-module

The R305 is one kind of fingerprint sensor module used in biometrics for security in fingerprint detection as well as verification. These devices are mainly used in safes where there is a high- powered DSP chip used in the rendering of image, feature-finding, searching and calculation by connecting it to any microcontroller with the help of TTL serial, & senddata packets to get photos, notice prints, search and hash. The enrollment of new fingers can be stored directly within the flash memory of on board.

Features of Fingerprint Sensor

The features of this sensor include the following.

- It includes image collection as well as chip algorithm
- The fingerprint reader can perform lesser growth and can be fixed into a range of end products
- Power use is low, excellent performance, small in size, and less cost
- Optical technology which is used is professional, and exact module developed techniques
- The capabilities of image processing are good, and can effectively capture pictures up to 500 dpi resolution

Fingerprint Sensor Working Principle

The working principle of the fingerprint sensor mainly depends on the processing. The fingerprint processing mainly includes two elements namely enrollment and matching. In fingerprint enrolling, every user requires to place the finger twice.

So that the system will check the finger images to process as well as to generate a pattern of the finger and it will be stored. When matching, a user places the finger using an optical sensor then the system will produce a pattern of the finger & compares it with the finger library templates.

For 1:1 fingerprint matching, the system will evaluate the exits finger with a precise pattern which is selected within the module. Similarly, for 1: N matching, the scanning system will look for the complete finger records for the finger matching. In both situations, the scanning system will go back to the corresponding result, success otherwise crash.

Specifications

The specifications of this sensor include the following.

- The fingerprint sensor is an optical type
- The interface is USB1.1/ TTL logical level (UART)
- The speed of scanning is 0.5 sec
- The speed of verification is 0.3 sec
- The capacity storage is 1000
- The security level is 5
- The baud rate of RS232 is 4800BPS ~115200BPS variable
- Current is typical 50 mA, and peak 80mA
- The corresponding technique is 1: N
- Fixed indicators-15KV bright green backlight
- The life of the sensor is 100 million times
- The dimension is 44.1 X 20 X 23.5mm
- The size of the character file is 256 bytes
- The template size is 512 bytes
- The FRR (False Rejection Rate) is <1.0%
- The FAR (False Acceptance Rate) is 0.001%
- Voltage is 4.2 to 6.0 VDC
- Operating surroundings temperature is -20° C to 40° C

Hardware interface

The module itself does all complex tasks behind reading and identifying the fingerprints with an on- board optical sensor and fingerprint algorithm. All you need to do is send it simple commands, and the fingerprint scanner can store different fingerprints.

The database of prints can even be downloaded from the unit and distributed to other modules. As well as the fingerprint template, the analyzed version of the print, you can also retrieve the image of a fingerprint and even pull raw images from the optical sensor.

Although a number of fingerprint reader/sensor modules with slight variations are available now, most have a 4-pin external connection interface. By way of the serial interface, fingerprint reader/sensor module can communicate with a microcontroller (uC) runs on of 3.3V or 5V power supply. TX/TD pin of the module connects with RXD (RX-IN pin of the uC), and RX/RD pin connects with TXD (TX-OUT pin of the uC).

If you are building a personal computer (PC) – based project, remember to add a level converting circuit (for instance, the MAX232) between the module and the personal computer. Serial communication protocol mode is semi-duplex asynchronous serial communication, and user can set the baud rate in 9600 – 115200bps. Recommended working voltage of the module is 3.6 to 6.0 Volt DC, and the typical working current is 90 to 100 mA (150mA peak).

WEBCAM:

A **webcam** is a video camera which feeds its images in real time to a computer or computer network, often via USB, Ethernet or Wi-Fi. Their most popular use is the establishment of video links, permitting computers to act as videophones or videoconference stations. This common use as a video camera for the World Wide Web gave the webcam its name. Other popular uses include security surveillance and computer vision. Webcams are known for their low manufacturing cost and flexibility, making them the lowest cost form of video telephony. They have also become a source of security and privacy issues, as some built- in webcams can be remotely activated via spyware.

LENS:

Webcams typically include a lens, an image sensor, support electronics, and may also include a microphone for sound. Various lenses are available, the most common in consumer- grade webcams being a plastic lens that can be screwed in and out to focus the camera. Fixed focus lenses, which have no provision for adjustment, are also available. As a camera system's depth of field is greater for small image formats and is greater for lenses with a large f-number (small aperture), the systems used in webcams have a sufficiently large depth of field that the use of a fixed focus lens does not impact image sharpness to a great extent.

Image sensors can be CMOS or CCD, the former being dominant for low-cost cameras, but CCD cameras do not necessarily outperform CMOS-based cameras in the low cost price range. Most consumer webcams are capable of providing VGA resolution video at a frame rate of 30 frames per second. Many newer devices can produce video in multi-megapixel resolutions, and a few can run at high frame rates such as the PlayStation Eye, which can produce 320×240 video at 120 frames per second.

PORTABILITY:

Most webcams feature built-in microphones to make video calling and videoconferencing more convenient. The USB video device class (UVC) specification allows for interconnectivity of webcams to computers without the need for proprietary device drivers. Microsoft Windows XP SP2, Linux and Mac OS X (since October 2005) have UVC support built in and do not require extra device drivers, although they are often installed to add additional features.

FEATURES (LOGITECH WEBCAM C100):-

Plug-and-play setup (UVC)

Video capture: Up to 640 x 480 pixels

Photos: Up to 1.3 megapixels (software enhanced)

Frame rate: Up to 30 frames per second (with recommended system) Hi-Speed USB 2.0 certified

Fixed focus

Universal clip fits notebooks, LCD or CRT monitor



Python:

What is Python? Executive Summary

Python is an interpreted, object-oriented, high-level programming language with dynamic semantics. Its high-level built in data structures, combined with dynamic typing and dynamic binding, make it very attractive for Rapid Application Development, as well as for use as a scripting or glue language to connect existing components together. Python's simple, easy to learn syntax emphasizes readability and therefore reduces the cost of program maintenance. Python supports modules and packages, which encourages program modularity and code reuse. The Python interpreter and the extensive standard library are available in source or binary form without charge for all major platforms, and can be freely distributed.

Often, programmers fall in love with Python because of the increased productivity it provides. Since there is no compilation step, the edit-test-debug cycle is incredibly fast. Debugging Python programs is easy: a bug or bad input will never cause a segmentation fault. Instead, when the interpreter discovers an error, it raises an exception. When the program doesn't catch the exception, the interpreter prints a stack trace. A source level debugger allows inspection of local and global variables, evaluation of arbitrary expressions, setting breakpoints, stepping through the code a line at a time, and so on. The debugger is written in Python itself, testifying to Python's introspective power. On the other hand, often the quickest way to debug a program is to add a few print statements to the source: the fast edit-test-debug cycle makes this simple approach very effective.

Installing Python is generally easy, and nowadays many Linux and UNIX distributions include a recent Python. Even some Windows computers (notably those from HP) now come with Python already installed. If you *do* need to install Python and aren't confident about the task you can find a few notes on the [BeginnersGuide/Download](#) wiki page, but installation is unremarkable on most platforms.

Learning

Before getting started, you may want to find out which IDEs and text editors are tailored to make Python editing easy, browse the list of introductory books, or look at code samples that you might find helpful.

There is a list of tutorials suitable for experienced programmers on the [BeginnersGuide/Tutorials](#) page. There is also a list of resources in other languages which might be useful if English is not your first language. The online documentation is your first port of call for definitive information. There is a fairly brief tutorial that gives you basic information about the language and gets you started. You can follow this by looking at the library reference for a full description of Python's many libraries and the language reference for a complete (though somewhat dry) explanation of Python's syntax. If you are looking for common Python recipes and patterns, you can browse the [ActiveState Python Cookbook](#)

Looking for Something Specific?

If you want to know whether a particular application, or a library with particular functionality, is available in Python there are a number of possible sources of information. The Python web site provides a Python Package Index (also known as the *Cheese Shop*, a reference to the Monty Python script of that name). There is also a search page for a number of sources of Python- related information. Failing that, just Google for a phrase including the word "python" and you may well get the result you need. If all else fails, ask on the python newsgroup and there's a good chance someone will put you on the right track.

CHAPTER 6

RESULTS AND CONCLUSION

CONCLUSIONS: The project 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.

Result :

- Biometric tokens are the safest means of preventing ATM frauds.
- The main reason for introducing biometric systems is to increase overall security.
- Biometrics offers greater security and convenience than traditional methods of personal recognition.
- In some applications, biometrics can replace or supplement the existing technology. In others, it is the only viable approach.
- The biometric system is only one part of an overall identification or authentication process, and the other parts of that process will play an equal role in determining its effectiveness.

FUTURE WORK:

- Today's biometric scanners go far beyond basic fingerprint recognition.
- In Poland and Japan, consumers are already using Hitachi's infrared scanners that capture the unique pattern of capillaries in the finger and hand.
- The most secure biometric technology uses a device designed to perform an iris scan based on more than 2,000 unique measurement points.
- According to developers, people and pets all over the world will be connected to a system that uses iris scan identification within the next decade.

CONCLUSION

Biometrics can only be limited by limiting one's imagination. Biometric technology is now being used in almost every area. Not only that, but various types of biometric systems are being used to achieve various functionalities.

There are many mature biometric systems available now. Proper design and implementation of the biometric system can indeed increase the overall security. There are numerous conditions that must be taken in account when designing a secure biometric system. First, it is necessary to realize that biometrics is not secrets. This implies that care should be taken and it is not secure to generate any cryptographic keys from them. Second, it is necessary to trust the input device and make the communication link secure. Third, the input device needs to be verified .

The ultimate form of electronic verification of a person's identity is biometrics; using a physical attribute of the person to make a positive identification. People have always used the brain's innate ability to recognize a familiar face and it has long been known that a person's fingerprints can be used for identification. The challenge has been to turn these into electronic processes that are inexpensive and easy to use.

Banks and others who have tested biometric-based security on their clientele, however, say consumers overwhelmingly have a pragmatic response to the technology. Anything that saves the information-overloaded citizen from having to remember another password or personal identification number comes as a welcome respite. Biometrics can address most of the security needs, but at what cost? Surprisingly, the benefits quickly outweigh the costs. Like so many technological developments, innovative people have found new ways to implement biometric systems, so prices have come down dramatically in the last year or two. As prices have come down, the interest level and the knowledge about how to effectively utilize these systems have increased. So the investment is decreasing and the recognizable benefits are increasing. Biometrics, when properly implemented, not only increase security but also often are easier to use and less costly to administer than the less secure alternatives. Biometrics can't be forgotten or left at home and they don't have to be changed periodically like passwords.

REFERENCES

1. Sergey Tulyakov, Faisal Farooq, Praveer Mansukhani, Venu Govindaraju, "Symmetric Hash functions for Secure Finger print biometric systems".
2. Y.Donis, L. Reyzin and A.Smith, "Fuzzy Extractors" In security with Noisy Data: Private Biometrics, Secure key Storage and Anti-Counterfeiting, P.Tuyls, B.Skoric and T.Kevenaar, Eds., chpt5,pp.79-77, Springer-Verlag, 20012.
3. Direct Indirect Human Computer Interaction Based Biometrics International Journal of Emerging Engineering Research and Technology Volume 3, Issue 3, March 2015.
4. A.A.E. Ahmed, I. Traore, "A new biometric technology based on mouse dynamics, IEEE Transactions on dependable and Secure Computing" 4 (3) (2007) 165–179.
5. Deshpande, S. Chikkerur, V. Govindaraju, Accent classification in speech, Fourth IEEE Workshop on Automatic Identification Advanced Technologies, 17–18 October, 2014, pp. 139– 143.
6. F. Bannister and R. Connolly, "New Problems for Old? Defining e-Governance", proceedings of the 44th Hawaii International Conference on System Sciences, **(2012)**.
7. W.-S. Chen, K.-H. Chih, S.-W. Shih and C.-M. Hsieh, "Personal Identification Technique based on Human Iris Recognition with Wavelet Transform", 2005 IEEE, ICASSP, **(2012)**, pp. II - 949.

8. R. Germain, A. Califano, and S. Colville, "*Fingerprint Matching Using Transformation Parameter Clustering*," IEEE Computational Science and Engineering 4, No. 4, 42–49 (2014).
9. L. O’Gorman, "*Practical Systems for Personal Fingerprint Authentication*," IEEE Computer 33, No. 2, 58–60 (2013).
- 10 N. K. Ratha and R. M. Bolle, "*Smart Card Based Authentication*," in Biometrics: Personal Identification in Networked Society, A. K. Jain, R. M. Bolle, and S. Pankanti, Editors, Kluwer Academic Press, Boston, MA (2013), pp. 369–384.
11. T. Rowley, "*Silicon Fingerprint Readers: A Solid State Approach to Biometrics*," Proceedings of the CardTech/SecureTech Conference, CardTech/SecureTech, Bethesda, MD (2013), pp. 152–159.
12. B. Miller, "*Vital Signs of Identity*," IEEE Spectrum 31, No.2, 22–30 (2013).
13. B. Schneier, "*The Uses and Abuses of Biometrics*," Communications of the ACM 42, No. 8, 136 (2012).
14. W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "*Techniques for Data Hiding*," IBM Systems Journal 35, Nos. 3&4, 313–336 (2013).
15. Biometric Digest-<http://biometrics.cse.msu.edu>.