A Seminar Report

On

"AN ATM WITH AN EYE"

Submitted By

Mr. JIGNESHSINGH ARVINDBHAI KUSHVAHA

Guided By

DR. HARDIKKUMAR VIKRAMKUMAR DESAI

Submitted To

NaranLala College of Professional and Applied Sciences,
Veer Narmad South Gujarat University, Surat.

Year: 2022-2023

NARANLALA
COLLEGE OF PROFESSIONAL & APPLIED SCIENCES
BHAGVATI SANKUL, NEAR ERU CHAR RASTA,
NAVSARI – 396 450

CERTIFICATE

This is to certify that **Mr. Jigneshsingh Arvindbhai Kushvaha,** Exam No. **453** student of **B.C.A. 6th semester** of our college have successfully prepared and submitted Seminar Report on "An ATM With An Eye" as a partial fulfillment for the course of **Bachelor of Computer Application** during the academic year **2022-2023**.

10-4-2023
DATE

DR. HARDIKKUMAR V. DESAI
Guided By

_____

Dr. S. M. NAIK
(PRINCIPAL, NLCPAS)

_____

Dr. A. B. PATEL
(DEPT. HEAD, BCA)

_____

(EXTERNAL EXAMINER)

AN ATM WITH AN EYE SCANNING

(THE FUTURE TECHNOLOGY)

Prepared by:

Kushvaha Jigneshsingh Arvindbhai

INDEX

FIGURE INDEX

CHAPTER 1: ACKNOWLEDGEMENT

As I write this acknowledgement, I must clarify that this is not just a formal acknowledgement but also a sincere note of thanks and regard from **JIGNESHSINGH ARVINDBHAI KUSHVAHA**. I feel a deep sense of gratitude and affection for our internal guide **DR. HARDIKKUMAR VIKRAMKUMAR DESAI** who were associated with this Project. Without their co-operation and guidance this project could not have been conducted properly.

We would like to say thanks to all people that helped me for successful completion of project development and for providing valuable guidance throughout our project work. So I take this opportunity to thanks the people to make this project and the report success.

Finally to naranlala college of professional & applied science and for giving me such an opportunity to put our first step of knowledge in the field in real world which increases my number of experiences by one for teaching me to see the silver lining in every dark cloud.

Our sincere thanks to all faculty member of BCA for mounding our thoughts and vision towards this subject we appreciate their concern and interest regarding the project. Their words of advice prior to living for the project help us a great deal during the project.

CHAPTER 2: ABSTRACT

There is an urgent need for improving security in banking region. With the advent of ATM though banking became a lot easier it even became a lot vulnerable. The chances of misuse of Automated Teller Machine (ATM) are manifold due to the exponential growth of 'intelligent' criminals day by day. ATM systems today use no more than an access card and PIN for identity verification. This situation is unfortunate since tremendous progress has been made in biometric identification techniques, including finger printing, facial recognition, and iris scanning.

This paper proposes the development of a system that integrates **Iris scanning** technology into the identity verification process used in ATMs. The development of such a system would serve to protect consumers and financial institutions alike from fraud and other breaches of security.

CHAPTER 3: INTRODUCTION

The rise of technology in India has brought into force many types of equipment that aim at more customer satisfaction. ATM is one such machine which made money transactions easy for customers to bank. The other side of this improvement is the enhancement of the culprit's probability to get his 'unauthentic' share. Traditionally, security is handled by requiring the combination of a physical access card and a PIN or other password in order to access a customer's account. This model invites fraudulent attempts through stolen cards, badly-chosen or automatically assigned PINs, cards with little or no encryption schemes, employees with access to non-encrypted customer account information and other points of failure.

This proposes an automatic teller machine security model that would combine a physical access card, a PIN, and electronic eye recognition. By forcing the ATM to match a live image of a customer's face with an image stored in a bank database that is associated with the account number, the damage to be caused by stolen cards and PINs is effectively neutralized. Only when the PIN matches the account and the live image and stored image match would a user be considered fully verified.

The main issues faced in developing such a model are keeping the time elapsed in the verification process to a negligible amount, allowing for an appropriate level of variation in a customer's face when compared to the database image, and that credit cards which can be used at ATMs to withdraw funds are generally issued by institutions that do not have in-person contact with the customer, and hence no opportunity to acquire a photo.

Because the system would only attempt to match two (and later, a few) discrete images, searching through a large database of possible matching candidates would be unnecessary. The process would effectively become an exercise in pattern matching, which would not require a great deal of time. With appropriate lighting and robust learning software, slight variations could be accounted for in most cases. Further, a AN ATM WITH AN EYE Seminar is positive visual match would cause the live image to be stored in the database so that future transactions would have a broader base from which to compare if the original account image fails to provide a match – thereby decreasing false negatives.

CHAPTER 4: WHAT IS ATM?

An ATM (*Automated Teller Machine*) is an electronic machine used for financial transactions. As the term implies, it is an 'automated' banking platform that does not require any banking representative/teller or a human cashier.

FIG 4.1 ATM MACHINE

ATMs are machines that dispense cash and allow you to make other banking transactions. An ATM typically consists of a screen, a card reader, a keypad, a cash dispenser and a printer.

ATMs can be found in many locations throughout the U.S. and the world. On-premise ATMs are located at financial institutions such as banks, while off-premise ones are commonly offered at places like airports, grocery stores and gas stations.

4.1 DEFINITION:

ATM full form is Automated Teller Machine which is a self-service banking outlet. You can withdraw money, check your balance, or even transfer funds. Different banks provide their ATM services by installing cash machines in different parts of the country. You can withdraw money from any of these machines irrespective of whether or not you are an account holder in the same bank.

Transactions are either free or bear a nominal charge depending upon the banks. Banks usually do not charge for the first 3-5 transactions in a month. Once you cross the limit

of free transactions, you may have to pay a nominal charge. Also, some banks levy charges if you withdraw money from another bank's ATM of which you are not an account holder.

4.2 TYPES OF AUTOMATED TELLER MACHINE (ATM):

Automated Teller Machines (ATMs) are mainly of two types. One is a simple basic unit that allows you to withdraw cash, check your balance, change the PIN, get mini statements and receive account updates. The more complex units provide facilities for cash or cheque deposits and line of credit & Bill Payments.

4.3 ATM SYSTEMS

Our ATM system would only attempt to match two (and later, a few) discrete images, searching through a large database of possible matching candidates would be unnecessary. The process would effectively become an exercise in pattern matching, which would not require a great deal of time. With appropriate lighting and robust learning software, slight variations could be accounted for in most cases. Further, a positive visual match would cause the live image to be stored in the database so that future transactions would have a broader base from which to compare if the original account image fails to provide a match – thereby decreasing false negatives.

When a match is made with the PIN but not the images, the bank could limit transactions in a manner agreed upon by the customer when the account was opened, and could store the image of the user for later examination by bank officials. In regards to bank employees gaining access to customer PINs for use in fraudulent transactions, this system would likewise reduce that threat to exposure to the low limit imposed by the bank and agreed to by the customer on visually unverifiable transactions.

In the case of credit card use at ATMs, such a verification system would not currently be feasible without creating an overhaul for the entire credit card issuing industry, but it is possible that positive results (read: significant fraud reduction) achieved by this system might motivate such an overhaul.

The last consideration is that consumers may be wary of the privacy concerns raised by maintaining images of customers in a bank database, encrypted or otherwise, due to possible hacking attempts or employee misuse. However, one could argue that having the image compromised by a third party would have far less dire consequences than the account information itself. Furthermore, since nearly all ATMs videotape customers engaging in transactions, it is no broad leap to realize that banks already build an archive of their customer images, even if they are not necessarily grouped with account information.

4.4 HISTORY

The first ATMs were off-line machines, meaning money was not automatically withdrawn from an account. The bank accounts were not (at that time) connected by a computer network to the ATM. Therefore, banks were at first very exclusive about who they gave ATM privileges to. Giving them only to credit card holders (credit cards were used before ATM cards) with good banking records. In modern ATMs, customers authenticate themselves by using a plastic card with a magnetic stripe, which encodes the customer's account number, and by entering a numeric passcode called a PIN (personal identification number), which in some cases may be changed using the machine. Typically, if the number is entered incorrectly several times in a row, most ATMs will retain the card as a security precaution to prevent an unauthorised user from working out the PIN by pure guesswork..

4.5 RELIABLITY:

ATMs are generally reliable, but if they do go wrong customers will be left without cash until the following morning or whenever they can get to the bank during opening hours. Of course, not all errors are to the detriment of customers; there have been cases of machines giving out money without debiting the account, or giving out higher value notes as a result of incorrect denomination of banknote being loaded in the money cassettes. Errors that can occur may be mechanical (such as card transport mechanisms; keypads; hard disk failures); software (such as operating system; device driver; application); communications; or purely down to operator error.

4.6 SECURITY:

Early ATM security focused on making the ATMs invulnerable to physical attack; they were effectively safes with dispenser mechanisms. ATMs are placed not only near banks, but also in locations such as malls, grocery stores, and restaurants. The other side of this improvement is the enhancement of the culprit's probability to get his 'unauthentic' share.

ATMs are a quick and convenient way to get cash. They are also public and visible, so it pays to be careful when you're making transactions. Follow these general tips for your personal safety.

4.6.1 STAY ALERT:

If an ATM is housed in an enclosed area, shut the entry door completely behind you. If you drive up to an ATM, keep your car doors locked and an eye on your surroundings. If you feel uneasy or sense something may be wrong while you're at an ATM, particularly at night or when you're alone, leave the area.

FIG 4.6.1 WORKING SCREEN

4.6.2 KEEP YOUR PIN CONFIDENTIAL:

- Memorize your Personal Identification Number (PIN); don't write it on your card or leave it in your wallet or purse.
- Keep your number to yourself.
- Never provide your PIN over th telephone, even if a caller identifies himself as a bank employee or police officer. Neither person would call you to obtain your number.

FIG 4.6.2 WORKING DASHBOARD

CHAPTER: 5 Different Techniques That Can Be Used With Atm

1. Finger Print Scanning
2. Facial Recoginition
3. Iris Recoginition

5.1 FINGER PRINT SCANNING:

Fingerprint Based ATM is a desktop application where fingerprint of the user is used as a authentication. The finger print minutiae features are different for each human being so the user can be identified uniquely. Instead of using ATM card Fingerprint based ATM is safer and secure. There is no worry of losing ATM card and no need to carry ATM card in your wallet. You just have to use your fingerprint in order to do any banking transaction. The user has to login using his fingerprint and he has to enter the pin code in order to do further transaction. The user can withdraw money from his account. User can transfer money to various accounts by mentioning account number. In order to withdraw money user has to enter the amount he want to withdraw .The user must have appropriate balance in his ATM account to do transaction. User can view the balance available in his respective account.

5.1.1 FEATURES:

- **Login: -** User will login to the system using his fingerprint.
- **Add Pin Code: -** User has to add pin code in order to do transactions.
- **Withdrawal of cash: -** User can withdraw cash by entering the amount he want to withdraw.
- **View Balance:** - User can view balance which is available in his respective account.

5.1.2 ADVANTAGES:

- Fingerprint based ATM System is more secure than ATM card.
- User can make transaction using his fingerprint anywhere and at anytime he need not have to carry ATM card.

5.1.3 DISADVANTAGES:

- If the User finger pattern has some cut or got damaged the system might not recognize the user.

5.1.4 APPLICATION:

- The system can be used in various Banks.

5.2 FACIAL RECOGNITION:

ATMs allow you to carry out a variety of money transactions with your card account. Each person has a unique facial structure. Facial recognition technology allows automatic identification of the ATM user.

- The algorithm for facial recognition technology consists of two steps:
  1. Identification (who is this person?)
  2. Verification (is this the person pretends to be?)

Facial biometrics involves scanning with special points to create a map. This map is converted into a unique representation associated with the identity of a particular user. This process includes an identification stage, followed by an ATM cash, check, placement of money trays and selection of bills for the customer.

The introduction of facial recognition technology in ATMs helps speed up transactions and eliminate card misuse.The biometric face identification system is easily integrated into the normal ATM software. Every bank can adjust this procedure to its own needs.

FIG 5.2 FACE RECOGNITION

5.2.1 STAGES OF FACIAL RECOGNITION:

1. Face Detection
2. Facial Features Detection
3. Face Normalization
4. Feature Extraction And Descriptor Computation
5. Face Verification

5.2.2 HOW DOES FACIAL RECOGNITION WORKS AT ATMs:

ATMs with the facial recognition help avoid fraud and increase security in banking. All modern face recognition technologies use systems that are trained using test images. Bases with images containing faces and non-face images are used for training. Each image fragment is characterized as a feature vector. The feature vector allows to determine whether a given part of the image is a face or not.

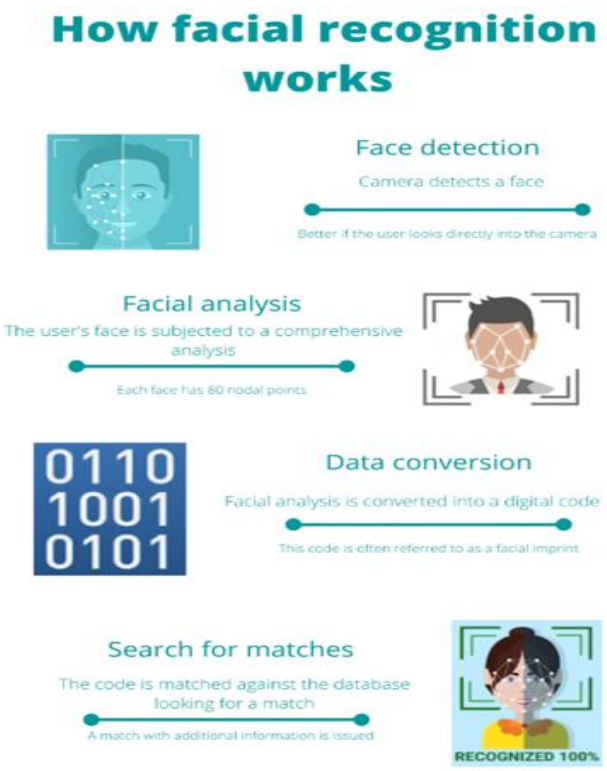

FIG 5.2.2 FACIAL RECOGNITION WORK

5.2.3 ADVANTAGES:

The main advantages of facial recognition are: ease of use, security, contactless, speed, convenience, identification reliability and scalability. In addition, the advantage of face recognition compared to other biometric identification systems is that cameras can capture images from a distance.

5.2.4 DISADVANTAGES :

The main disadvantage of the facial recognition technology is the deterioration of the recognition quality when the light is dim or the position of the user's head is changed. The result of facial recognition does not exclude errors caused by changes in the camera angle or the user's appearance (hairstyle, makeup, etc.).

Face recognition systems can cause identification errors. For example, if there are flaws in the image used to create the face image, the system will not be able to match it to another in the face recognition database. Low resolution and strong shadows can distort the final facial print and cause false positives.

In addition, face recognition may be ineffective if a relative of the cardholder, with his/her permission, wants to use the ATM.

5.2.5 FACIAL VS FINGERPRINT RECOGNITION

Like Face ID, fingerprint authentication is the fast and convenient method of identifications. In this case, the authorized user has access to a list of certain functions of the device. ATMs that support fingerprint recognition allow to identify with the system, withdraw cash, and use other functions.

Face and fingerprint recognition are methods that have obvious advantages: physical operative connection to the user, simplicity and speed of use.

The main disadvantage of fingerprint recognition is that fingerprints can be faked. In addition, if the fingerprint pattern is cut or damaged, the system may not recognize it. Some fingerprints may be difficult to distinguish if the user has been engaged in manual labor for several years.

CHAPTER: 6 IRIS RECOGNITION

Iris scan biometrics employs the unique characteristics and features of the human iris in order to verify the identity of an individual. The iris is the area of the eye where the pigmented or colored circle, usually brown or blue, rings the dark pupil of the eye.The iris-scan process begins with a photograph. A specialized camera, typically very close to the subject, no more than three feet, uses an infrared imager to illuminate the eye and capture a very high-resolution photograph. This process takes only one to two seconds and provides the details of the iris that are mapped, recorded and stored for future matching/ verification. Eyeglasses and contact lenses present no problems to the quality of the image and the iris-scan systems test for a live eye by checking for the normal continuous fluctuation in pupil size.

The inner edge of the iris is located by an iris-scan algorithm which maps the iris' distinct patterns and characteristics. An algorithm is a series of directives that tell a biometric system how to interpret a specific problem. Algorithms have a number of steps and are used by the biometric system to determine if a biometric sample and record is a match. Iris' are composed before birth and, except in the event of an injury to the eyeball, remain unchanged throughout an individual's lifetime. Iris patterns are extremely complex, carry an astonishing amount of information and have over 200 unique spots. The fact that an individual's right and left eyes are different and that patterns are easy to capture, establishes iris-scan technology as one of the biometrics that is very resistant to false matching and fraud.

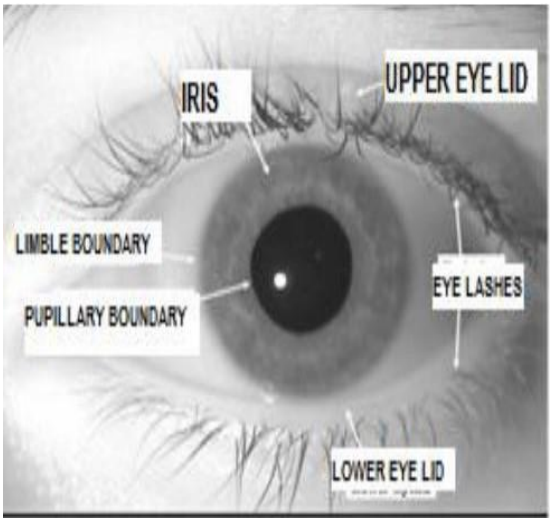

FIG 6 A FRONT VIEW OF THE HUMAN EYE

The false acceptance rate for iris recognition systems is 1 in 1.2 million, statistically better than the average fingerprint recognition system. The real benefit is in the false-rejection rate, a measure of authenticated users who are rejected. Fingerprint scanners have a 3 percent false-rejection rate, whereas iris scanning systems boast rates at the 0 percent level. A highly accurate technology such as iris-scan has vast appeal because the inherent argument for any biometric is, of course, increased security.

6.1 IRIS RECOGNITION:

A complete iris recognition system can be split into four stages: Image acquisition, segmentation, encoding and matching.

The data acquisition step captures the iris images. Infra-red illumination is used in most iris image acquisition.

The iris segmentation step localizes the iris region in the image. For most algorithms, and assuming near-frontal presentation of the pupil, the iris boundaries are modelled as two circles, which are not necessarily concentric. The inner circle is the papillary boundary (between the pupil and the iris). The outer circle is the limbic boundary (between the iris and the sclera). The noise processing is often included in the segmentation stage.

The encoding stage encodes the iris image texture into a bit vector code. In most algorithms, filters are utilized to obtain information about the iris texture. Then the outputs of the filters are encoded into a bit vector code.

The corresponding matching stage calculates the distance between iris codes, and decides whether it is an authorized match or unauthorized match.

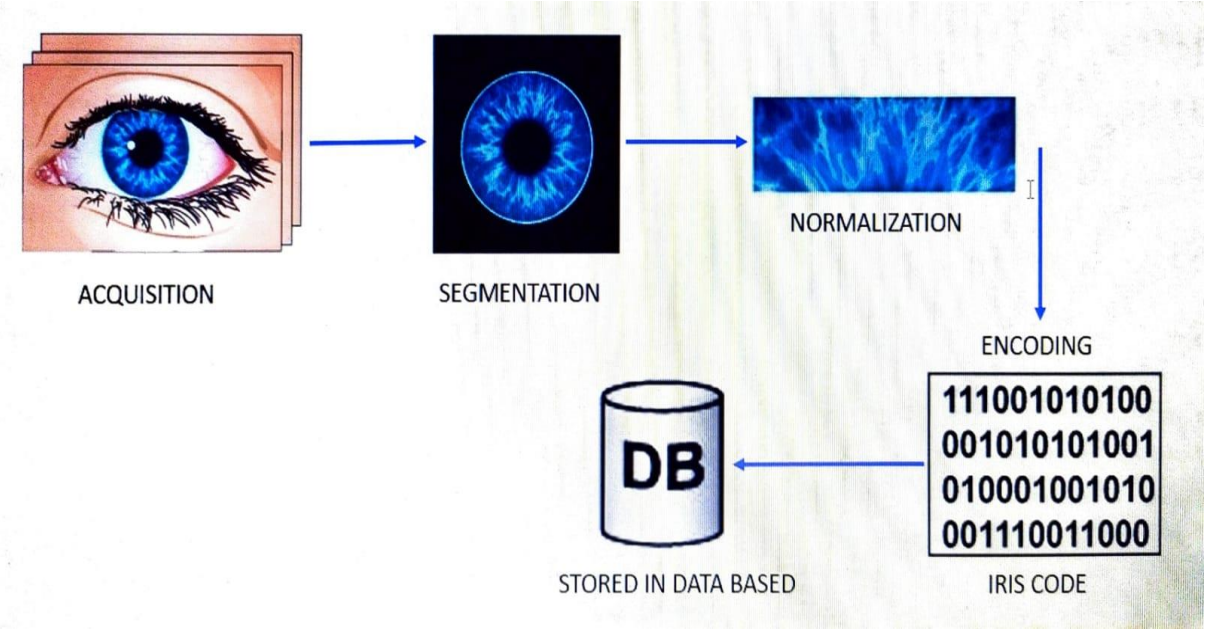

FIG 6.1 ARCHITECTURE OF IRIS RECOGNITION SYSTEM

6.1.1 ENROLLMENT:

The enrollment phase creates a user profile for subsequent authentication activities. Typically, a new user provides multiple biometric reading samples that are combined to form one stored record.

6.1.2 AUTHENTICATION:

Where a template is created for an individual and then a match is searched for in the database of pre-enrolled templates.

6.1.3 IMAGE ACQUISITION:

An important and complex step of iris recognition system is image acquisition. One of the major challenges of automated iris recognition is to capture a high-quality image of the iris while remaining non-invasive to the human operator. Especially for Indians, the iris is small in size and dark in color.

6.1.4 IMAGE SEGEMENTATION:

At this stage, the iris is extracted from the eye image. The extracted iris region was then normalized into a rectangular block with constant dimensions to account for imaging inconsistencies. The integro-differential operator for locating the circular iris and pupil regions, and also the arcs of the upper and lower eye lids.

6.1.5 IMAGE NORMALIZATION:

Encoding- Encoding is the process of generation of the iris code. In this process, the most discriminating feature in the iris pattern is extracted .The phase information in the pattern only is used because the phase angles are assigned regardless of the image contrast [6]. In this process, amplitude information is not used since it depends on the extraneous factors. Also, extraction of the phase information is done using the 2D Gabor wavelets. 2D Gabor wavelets are used to determine the quadrant in which the resulting phasor lies.

6.1.6 MATCHING:

This phase consists of two steps, namely matching and identification. In the matching process, the extracted features of the iris are compared with the iris images in the database. If enough similarity is found, the subject is then identified. The Hamming distance gives a measure of how many bits are the same between two bit patterns. Using the Hamming distance of two bit patterns, a decision can be made as to whether the two patterns were generated from different irises or from the same one.

6.2 WHAT IS AN IRIS SCAN?

The camera can be installed at a distance of 10 cm to 1 meter, depending on the scanning equipment. The term «scanning» can be misleading, as the process of obtaining an image is not scanning but simple photographing. The iris' texture resembles a network with many surrounding circles and patterns that can be measured by a computer. Iris scanning software uses about 260 anchor points to create a sample.

6.2.1 HOW DO IRIS SCANNER WORKS?

The unique iris pattern must be recognized to pass such a biometric scan, allowing an identification response.

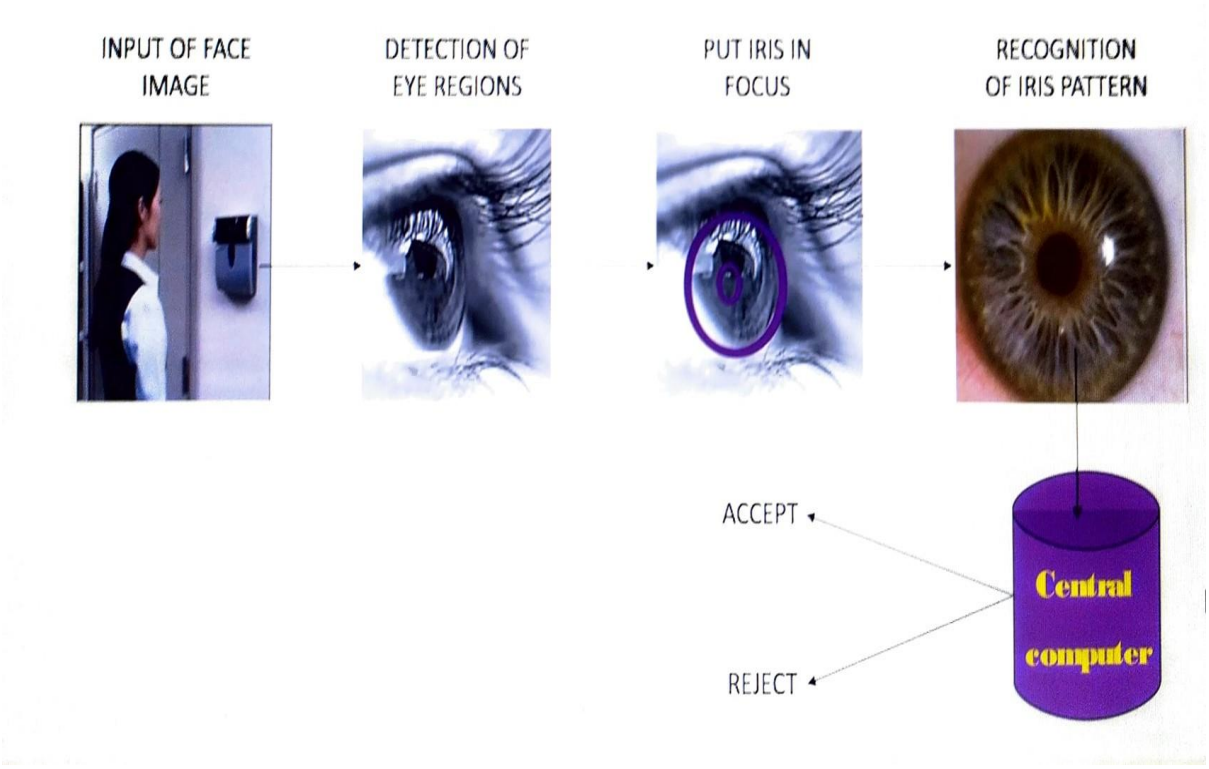

FIG 6.2.1 IRIS IDENTIFICATION STEPS

6.3 WHY IS IRIS SCANNER UNIQUE TECHNOLOGY?

The iris is a circular piece of colored muscle tissue that frames the human pupil and helps it to clench/unclench like a camera shutter. Our iris' color pattern is formed at the genetic level even when we are in the womb, but it finally completes its formation during the first two years of our life. The color of the eye's iris depends on the amount of melanin pigment: the more melanin, the more the eyes have a brown tint, the less — the more pronounced the blue color.

Although we are used to distinguishing the color of each person's eyes clearly — brown eyes, green eyes, blue eyes — the color and pattern for each particular iris is unique. For example, even two people's eyes have two different shades and patterns of their irises. The same goes for the eyes of genetic twins.

6.4 IS IT POSSIBLE TO FOOL A SYSTEM?

Automatically detecting new types of cosmetic contact lenses in iris images is a highly complex pattern recognition task. But recently, experimental datasets have emerged to help researchers investigate the problem. Given the pace of progress in other aspects of iris recognition, the research community is likely to make rapid progress in addressing the tampering problem. You can also use retina recognition to improve recognition accuracy.

6.5 HOW SAFE ARE EYE SCANNERS?

There are concerns regarding iris identification, fearing that an iris scan’s infrared rays could negatively affect vision. Our eyes do not have protective reactions to infrared radiation. When rays of bright light blind us, we reflexively squint or turn away, and the pupil of the eye narrows spontaneously. Since we do not see infrared light, we cannot determine when we fall under its influence, and the eyes do not respond to this radiation by constricting the pupil.

AN ATM WITH AN EYE

To reduce the harmful effects of infrared light on the eyes, designers use visible white light before infrared scanning. The use of such illumination causes the pupil to contract spontaneously, which reduces the penetration of infrared rays into the cornea of the eye. Another positive aspect of the pupil's constriction when identifying by the iris of the eye is the expansion of the identifiable area. The increase in the iris' visible area allows you to get unique information for its encoding and recording in the biometric template.

Conventional photo and video cameras of telephones and cameras have a built-in IR-cut filter designed to exclude infrared radiation's influence on the quality of the resulting image. Biometric facial identification from the front-facing 2D camera is easy enough to deceive. To detect deception, the developers began to use point IR illumination, with the help of forming a depth map of the object being shot.

Controlling a three-dimensional FIGure in front of the camera prevents simple methods of deceiving biometric identification systems using a photograph or video recording of an identified person.

This happens due to the lack of an IR filter in the front cameras of most modern smartphones. Manufacturers are implementing solutions that minimize the harmful effects of infrared radiation on the eyes:

- The power of the radiation source and the wavelength is limited.
- The radiation time is reduced. IR illumination is turned on only for the time necessary for identification, which is continually decreasing due to algorithms' improvement.
- The distance from the source of infrared radiation to the eyes is controlled. The infrared light will not turn on if the camera is very close to your face to avoid harm to your eyes.
- White pre-illumination is used to reduce the pupil diameter.

6.6 IRIS ADVANTAGES:

Following are the advantages of Iris recognition:

- **Stability** — A unique iris pattern is formed at the age of 10 months and remains unchanged throughout life.
- **Uniqueness** — the probability that two different irises will have the same pattern is practically zero.
- **Flexibility** — the technology can be used both independently and in conjunction with other security systems.
- **Reliability** — the iris pattern cannot be lost, stolen, or counterfeited.
- **Non-Contact** — Unlike retinal recognition, iris recognition is contactless and fast, providing unrivaled accuracy from a distance of about 30 cm.

6.6 IRIS DISADVANTAGES:

Following are the disadvantages of Iris recognition:

- **Higher initial costs** — This technology's cost is more compared to other biometric recognition systems like fingerprint sensors.
- **Mass tracking and bulk collection** — Governments can use this technology for mass surveillance and tracking.
- **Can be hacked** — Some commercial iris scanners can be bypassed by using high-resolution images of a user’s iris.

CHAPTER: 7 CONCULSION

Iris recognition is a very useful and versatile technique. Iris recognition is highly accurate technique. This technique has successful applications. This technique increases both privacy and identity. Highly secure biometric method. Iris recognition is a very easy process involving very less steps. Iris recognition consumes less time in comparison to other biometric recognition techniques. Iris recognition is a quick and accurate way of identifying an individual. This technique is now into use in fields involving high security concerns.

We thus develop an ATM model that is more reliable in providing security by using Iris recognition software. By keeping the time elapsed in the verification process to a negligible amount we even try to maintain the efficiency of this ATM system to a greater degree.