A

Seminar-I Report

on

SECURE ATM BY IMAGE PROCESSING

Submitted in Partial Fulfillment of
the Requirements for the Third Year
of

Bachelor of Engineering

in

Computer Engineering

to

North Maharashtra University, Jalgaon

Submitted by

Madhuri Rajendra Patil

Under the Guidance of

Mrs. Nilima Patil

DEPARTMENT OF COMPUTER ENGINEERING
SSBT's COLLEGE OF ENGINEERING AND TECHNOLOGY,
BAMBHORI, JALGAON - 425 001 (MS)

2015 - 2016

SSBT's COLLEGE OF ENGINEERING AND TECHNOLOGY, BAMBHORI, JALGAON - 425 001 (MS)

DEPARTMENT OF COMPUTER ENGINEERING

CERTIFICATE

This is to certify that the Seminar-I entitled *Secure ATM By Image Processing*, submitted by

Madhuri Rajendra Patil

in partial fulfillment of the Third Year of *Bachelor of Engineering* in *Computer Engineering* has been satisfactorily carried out under my guidance as per the requirement of North Maharashtra University, Jalgaon.

Date: April 8, 2016
Place: Jalgaon

Mrs. Nilima Patil
Guide

Prof. Dr. Girish K. Patnaik
Head

Prof. Dr. K. S. Wani
Principal

Acknowledgement

I would like to express our deep gratitude and sincere thanks to all who helps us to complete this Seminar work successfully. Our sincere thanks to principal **Prof. Dr. K. S. Wani**, SSBT COET for having provided us facilities to complete our Seminar work. Our deep gratitude goes to **Prof. Dr. G. K. Patnaik**, head of the department, for granting us opportunity to conduct this Seminar work.I would like to thanks to our college Director**Prof. Dr. Sanjay P. Shekhawat**. I am also sincerely thankful to**Mrs.Nilima Patil**, Seminar guide, for her valuable suggestions and guidance at the time of need. I am sincerely thankful to **Mr. Aakash Waghmare** of Seminar and Great thanks to our friends, our Seminar associates and all those who helped directly or indirectly for completion of this Seminar and thankful to my Parents.

Madhuri Rajendra Patil

Contents

List of Figures

Abstract

In this biometric systems the general idea is to use facial recognition to reinforce security on one of the oldest and most secure piece of technology that is still in use to date thus an Automatic Teller Machine. The main use for any biometric system is to authenticate an input by Identifying and verifying it in an existing database. Security in ATMs has changed little since their introduction in the late 70s. This puts them in a very vulnerable state as technology has brought in a new breed of thieves who use the advancement of technology to their advantage. With this in mind it is high time something should be done about the security of this technology beside there cannot be too much security when it comes to peoples money.Due to technological innovations in the banking domain, ATMs came into existence which facilitates customers to avail money round the clock. Moreover, the ATM network of one bank collaborates with other banks so as to enable customers to draw money from any bank's ATM. As ATMs are equipped with money there is possibility of robberies. In fact there were many such incidents reported.

Chapter 1

Introduction

Banking sector plays a pivotal role a countrys economy. One of its services is dispensing money through Automated Teller Machines (ATMs). As ATMs operate round the clock and interoperability with other banks, thanks to distributed computing, they get rid of time and geographical restrictions for monetary transactions. Moreover they are supporting a host of other services such as money transfer besides withdrawal of money. This led to ubiquitous usage of these wonderful machines across the globe. There have been plenty of ATM fraud cases reported in all counties where ATMs are operated. Security of Automated Teller Machine (ATM) is to be given paramount importance as financial institutions like banks heavily depend on them for facilitating monetary transactions. The term security refers to many aspects such as physical, transactional and integrity, customer identity integrity, device operation integrity, and customer security. Various attempts have been made in developed countries to have emergency PIN system but could not succeed due to lack of cooperation between banking lobby and police. With technological advances in ATM software, fraud cases are significantly reduced unless PIN is compromised. Though there is transactional security improved to the level of reliability, the misbehaving cases. [1]

In this chapter,section 1.1 describes the introduction related to ATM Image Processing.Section 1.2 describes the summary of chapter.

1.1 Introduction

To use an ATM with facial recognition system, all need is walk to the atm. its digital camera is on 24hours a day, and its computer will automatically initiate a face recognition procedure, whenever the computer detects a human face in camera obtains a picture of your face, the computer compares the image of face to the images of registered customers in its database .If face (as seen by the ATMs camera) matches the picture of the in the data base are automatically recognized by the machine. The machine will then play a recording will be heard through a loudspeaker, the recording will say face is recognized. 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 customers 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. An automatic teller machine security model that would combine a physical access card, a PIN, and electronic facial recognition. By forcing the ATM to match a live image of a customers 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. [1]

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 . [1]

1.2 Summary

In this chapter, an overview of the problem statement along with its solution for the work contained in this introduction is provided. In the next chapter, Face Recognition For ATM Transaction of architecture is presented.

Chapter 2

Literature Survey

The aim of the thesis is to design and implement a fool proof system that secures ATMs using digital image processing. It automatically identifies misbehaving humans who entered into ATM cabin and take necessary steps in such a way that the criminal who tries to misbehave is caught and brought to justice besides safeguarding interests of bankers and customers. This section provides an overview of the technology that supports the Face Recognition platform, discusses the potential benefits of Face Recognition, and makes predictions about ATM Image Processing future.

In this chapter,Section 2.1 describes background of ATM Image Processing .Section 2.2 is describes the related work to ATM Image Processing and section 2.3 is describes the summary of chapter.

2.1 What is ATM ?

An Automated Teller Machine(ATM) is a computerized telecommunication device that provides a customer of a financial institution with access to financial transaction in a public space without the need for a human clerk or bank teller.On most modern ATM's ,the customer is identified by inserting a plastic ATM card with magnetic stripe or a plastic smartcard with a chip, that contains a unique card number and some security information ,such as an expiration date or CVVC (CVV)security is provided by customer entering a personal identification number(PIN). [2]

The idea of out-of-hours cash distribution developed from banker's needs in Asia (Japan), Europe (Sweden and the United Kingdom) and North America (the United States). Little is known of the Japanese device. In the US patent record, Luther George Simjian has been credited with developing a "prior art device". Specifically his 132nd patent (US3079603), which was first filed on 30 June 1960 (and granted 26 February 1963). The roll-out of this

Figure 2.1: Automated Teller Machine

machine, called Bankograph, was delayed by a couple of years, due in part to Simjian's Reflectone Electronics Inc. being acquired by Universal Match Corporation. An experimental Bankograph was installed in New York City in 1961 by the City Bank of New York, but removed after six months due to the lack of customer acceptance. The Bankograph was an automated envelope deposit machine (accepting coins, cash and cheques) and did not have cash dispensing features. [2]

Figure 2.1 It is widely accepted that the first cash machine was put into use by Barclays Bank in its Enfield Town branch in north London, United Kingdom, on 27 June 1967. This machine was inaugurated by English comedy actor Reg Varney. This instance of the invention is credited to John Shepherd-Barron of printing firm De La Rue, who was awarded an OBE in the 2005 New Year Honours.This design used paper cheques issued by a teller or cashier, marked with carbon-14 for machine readability and security, which in a latter model were matched with a personal identification number (PIN). Shepherd-Barron stated; "It struck there must be a way could get own money, anywhere in the world or the UK. They hit upon the idea of a chocolate bar dispenser, but replacing chocolate with cash." In 1969, the first cash machine installed in Australia was in Sydney. [2]

2.2 Biometrics

Biometrics refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication)is used in computer science as a form of identification and access control.It is also used to identify individuals in groups that are under surveillance.Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice.Some researchers have coined the term behaviometrics to describe the latter class of biometrics.More traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information. [1]

2.3 Types Of Biometrics

2.3.1 Iris Scan

Figure 2.2 is Iris recognition of automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of one or both of the irises of an individual's eyes, whose complex random patterns are unique, stable, and can be seen from some distance.Retinal scanning is a different, ocular-based biometric technology that uses the unique patterns on a person's retina blood vessels and is often confused with iris recognition. Iris recognition uses video camera technology with subtle near infrared illumination to acquire images of the detail-rich, intricate structures of the iris which are visible externally. Digital templates encoded from these patterns by mathematical and statistical algorithms allow the identification of an individual or someone pretending to be that individual. Databases of enrolled templates are searched by matcher engines at speeds measured in the millions of templates per second per (single-core) CPU, and with remarkably low false match rates. [1]

Figure 2.2: Iris Scan

2.3.2 Retina Scan

Figure 2.3 shows a retinal scan is a biometric technique that uses the unique patterns on a person's retina blood vessels. It is not to be confused with another ocular-based technology, iris recognition, commonly called an "iris scanner."The human retina is a thin tissue composed of neural cells that is located in the posterior portion of the eye. Because of the complex structure of the capillaries that supply the retina with blood, each person's retina is unique. The network of blood vessels in the retina is not entirely genetically determined and thus even identical twins do not share a similar pattern. [1]

Although retinal patterns may be altered in cases of diabetes, glaucoma or retinal degenerative disorders, the retina typically remains unchanged from birth until death. Due to its unique and unchanging nature, the retina appears to be the most precise and reliable biometric, aside from DNA. The National Center for State Courts estimate that retinal scanning has an error rate of one in ten million. [1]

A retinal scan is performed by casting an unperceived beam of low-energy infrared light into a persons eye as they look through the scanner's eyepiece. This beam of light traces a standardized path on the retina. Because retinal blood vessels absorb light more readily than the surrounding tissue, the amount of reflection varies during the scan. The pattern of variations is digitized and stored in a database. [1]

Figure 2.3: Retina Scan

2.3.3 Hand Geometry

Figure 2.4 shows Hand geometry is a biometric that identifies users by the shape of their hands. Hand geometry readers measure a user's hand along many dimensions and compare those measurements to measurements stored in a file. Viable hand geometry devices have been manufactured since the early 1980s, making hand geometry the first biometric to find widespread computerized use. It remains popular; common applications include access control and time-and-attendance operations.

Since hand geometry is not thought to be as unique as fingerprints, palm veins or irises, fingerprinting, palm veins and iris recognition remain the preferred technology for high-security applications. Hand geometry is very reliable when combined with other forms of identification, such as identification cards or personal identification numbers. In large populations, hand geometry is not suitable for so-called one-to-many applications, in which a user is identified from his biometric without any other identification. [1]

2.4 Summary

In this chapter, background of ATM Image Processing is provided. In the next chapter, methodology used to implement technologies is presented.

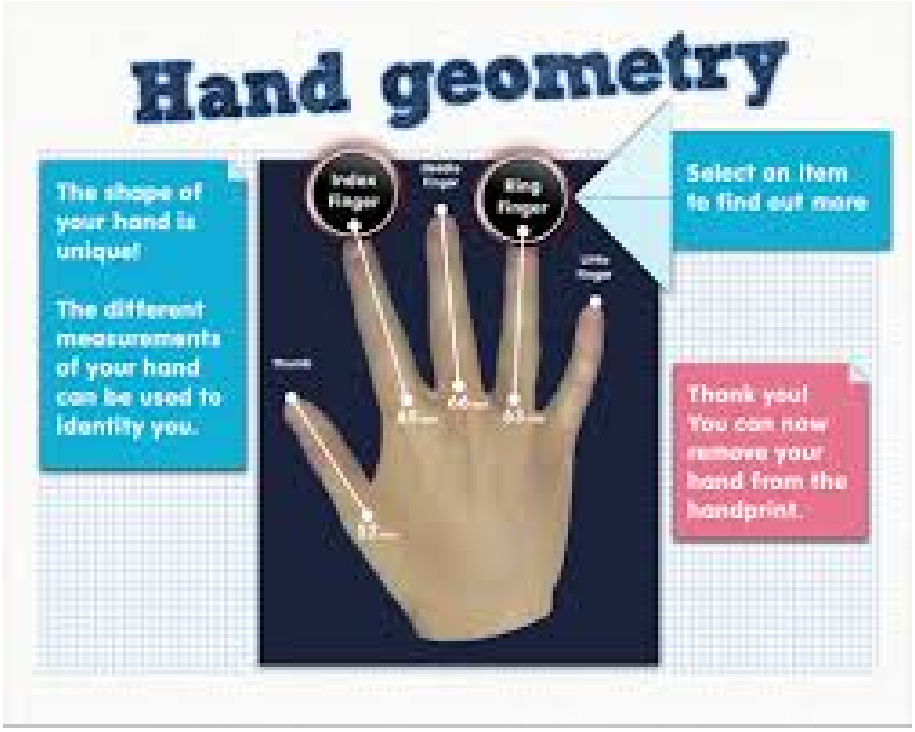

Figure 2.4: Hand Geometry

Chapter 3

Methodology

ATMs have brought so much relief to the financial world. Various problems were solved with the advent of these machines ranging from keeping the banking hall free of traffic with its attendant issues. Gone are the days of maintaining long queues in the banking hall which made the work of bankers more difficult thus leading to all forms of errors. Even to customers, having to leave the comfort of their homes for financial transactions before bankers close for the day's business is a major problem solved by Automated Teller Machines. However, as man begins to realize the gains of technology brought about by this machine to supplement human tellers, little did one know that the joy shall be short lived by the various sharp practices leading to financial losses. As banks are losing, so are the customers. News Media are filled with various forms of complaints on how users are losing money to fraudsters. Some have vowed never to come near usage of various cards like debit, credit or prepaid, local or international. The problem may even go as deep as engaging in legal battle between banks and their customers. [5]

In this chapter,Section 3.1 describes Face Recognition of Image Processing Architecture and Section 3.2 describes Types of Verification Process.Section 3.3 discuss summary of chapter.

3.1 Architecture

3.1.1 Algorithm

Figure 3.1 shows algorithm for secure ATM by Image Processing.

- Take Customer's pictures when account is opened and allow user to set non verified transaction limit.
- At ATM ,use access card and PIN to preverify user.
- Take Customer's picture ,attempt to match it to database images.

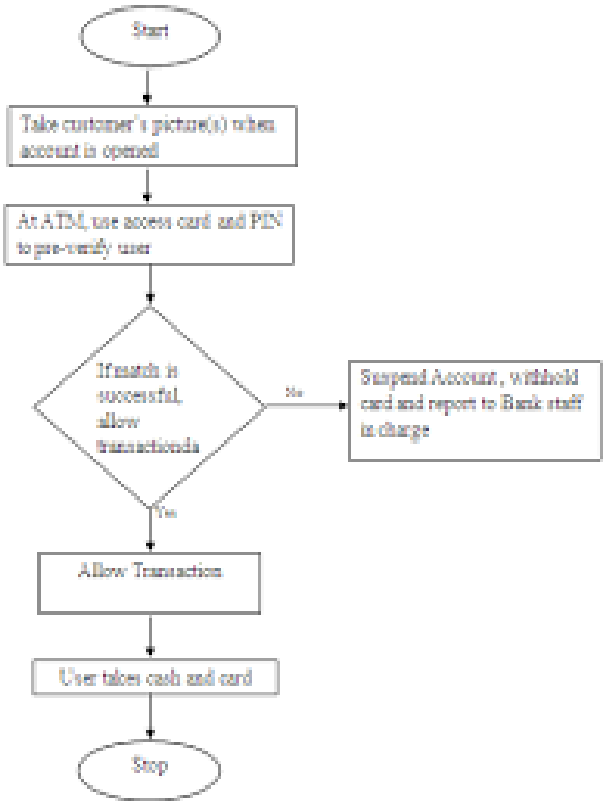

Figure 3.1: Flowchart For ATM Image Processing

- if match is successful,allow transaction.
- if match is unsuccessful,limit available transaction.

3.1.2 Reliable Facial Recognition

A facial recognition system is a computer application capable of identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a facial database.

It is typically used in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems.Some facial recognition algorithms identify facial features by extracting landmarks, or features, from an image of the subject's face. For example, an algorithm may analyze the relative position, size, or shape of the eyes, nose, cheekbones, and jaw. These features are then used to search for other images with matching features. Other algorithms normalize a gallery of face images and then compress the face data, only saving the data in the image that is useful for face recognition. A probe image is then compared with the face data. One of the earliest successful systems is based on template matching techniques applied to a set of salient facial features, providing a sort of compressed face representation. [1]

Recognition algorithms can be divided into two main approaches, geometric, which looks at distinguishing features, or photometric, which is a statistical approach that distills an image into values and compares the values with templates to eliminate variances.

Popular recognition algorithms include Principal Component Analysis using eigenfaces, Linear Discriminate Analysis, Elastic Bunch Graph Matching using the Fisherface algorithm, the Hidden Markov model, the Multilinear Subspace Learning using tensor representation, and the neuronal motivated dynamic link matching. [2]

3.2 Verification

Please follow these guidelines to help us verify your identity: 1.Face the camera,holding still until hear the beep 2.Maintain the normal facial expression 3.If wearing the glasses,please remove them

- Lighting
- Angle Of View
- Extreme Facial Expression
- Facial Hair
- Glasses

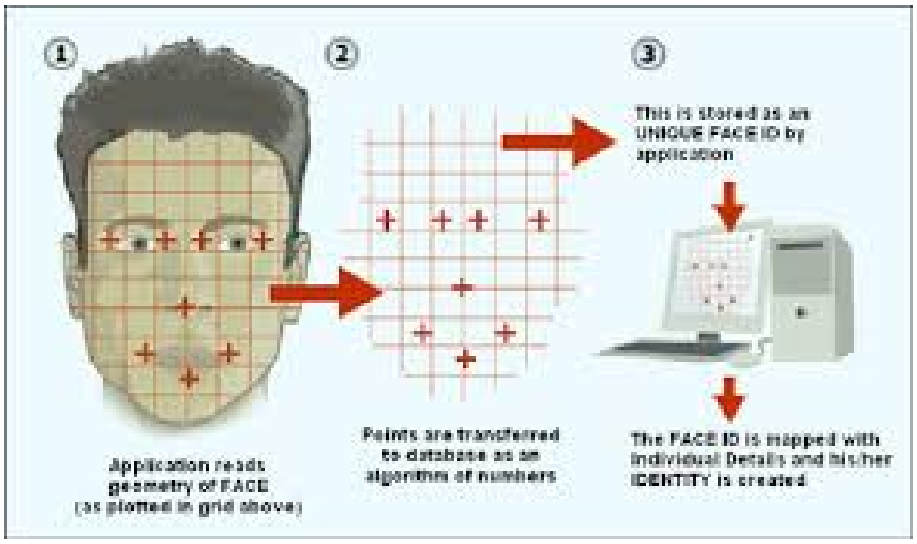

Figure 3.2: Face Recognition Process

3.2.1 Implementation of Face Recognition Technology

Figure 3.2 shows the Face Recognition Process And the following are Processes which required for Face Recognition Process.

1.Data Acquisition

- The input can be recorded video of the speaker or a still image.A sample of 1 sec duration consists of a 25 frame video sequence.
- More than 1 camera can be used to produce a 3D presentation of the face and to protect against the usage of photographs to gain unauthorized access. [3]

2.Input Processing

- A preprocessing module locates eye position and takes care of surrounding lighting condition and color variance.
- First the presence of faces of face in a scene must be detected.Once the face is detected, it must be localized and Normalization process may be required to the bring the dimension of the live facial sample in alignment with the one on the [3]

3.Face Image Classification

- The appearance of the face can change considerably during speech and due to facial expression .In the particular the mouth is subjected to fundamental changes but is also very important source of discriminating faces.

- So an approach to person's recognition is developed based on patio-temporal modeling of feature extracted from talking face.models are trained specific to a person's speech articulate and the way that the person speak. [3]

4.Desicion Making

- Face Recognition starts with a picture, attempting to find a picture in the image.The face recognition system locates the head and finally the eyes of the individual.
- A metrics is than developed based on the characteristics of the individual's face .The method of defining the metrics varies according to the algorithm.
- This metrics is then compared to matrices that are in database and similarly code is generated for each comparison. [3]

3.3 Summary

In this chapter, an overview of the methodology used to implement technologies is presented. In the next chapter,discussion related with ATM Image Processing Technology is presented.

Chapter 4

Discussion

To use an ATM with facial recognition system, all need is walk to the ATM. its digital camera is on 24hours a day, and its computer will automatically initiate a face recognition procedure, whenever the computer detects a human face in camera obtains a picture of human face, the computer compares the image of face to the images of registered customers in its database .If face (as seen by the ATMs camera) matches the picture of the in the data base are automatically recognized by the machine. An Image may be defined as a two dimensional function f (x,y) where x and y are spatial(plane) coordinates x, y is called intensity or gray level of the image at that point. When x, y and the amplitude values of f are all finite, discrete quantities, it call the image a digital image. Interest in digital image areas: improvement of pictorial information for human interpretation: and representation for autonomous machine perception. [2]

In this chapter,Section 4.1 describes Payment methods of ATM Image Processing .Section 4.2 describes Face Recognition Software and Section 4.3 discuss Advantage of ATM Image Processing with other technologies.Section 4.4 describes the summary.

4.1 Techniques And Methods

They are of three types 2-D 3-D Surface Texture Analysis.

4.1.1 2D Technique

The 2-D recognition method was individual of the original techniques employed. It maintained details of faces as seen two dimensionally. Details like width of the nose, width of the eyes, distance between the eyes, jaw line, cheek bone figure were used for contrast. This type of face recognition was not too precise. Change in facial expression or difference in ambient lighting on a appearance that is not directly looking into the camera did not produce expected results. [4]

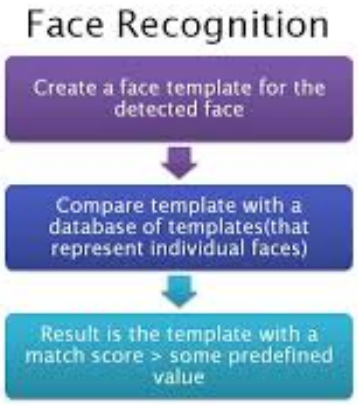

Figure 4.1: Face Recognition

4.1.2 3D Technique

Progression in face recognition gave origin to the 3-D recognition system. This stepped up technique, used facial appearance like contours of the eye sockets, chin, nose,peaks and valley on the visage for identification. The database will store details of faces also. The advantage of3-D technique over 2-D method is that 3-D face identification works fine even if the face is turned at 90 degree to the camera. It is self-governing of lighting environment and facial expressions. [5]

4.1.3 Surface Texture Analysis

The most superior method is Surface Texture Analysis(STA). STA does not examine the entire face but a patch of membrane on it. This patch is divided into separate blocks. The skin surface, the pore on the skin and other face characteristics are converted to a code. This code is used for comparison [6]

Figure 4.2: Enter ATM Card Into ATM Machine

4.2 Face Recognition Software

Figure 4.1 Face recognition technology: Ideal for access control, financial transactions and ATM machines.

4.2.1 The face key recognition technology performs the following tasks:

- Locates a moving object within the camera view.
- Determines if the moving object is face.
- Compares live faces with samples from database.
- Face recognition technology can work with both low resolution USB.
- Cameras and low or high resolution CCTV cameras.

Face finding technology captures all the faces in a cameras view .Then is stores each image in a separate folder for quick reviews-or for use with another face key technology. Each face is saved with a time and date stamp. In addition to faces, facial profiles and images of human bodies can be captured and stored. Search and match advisory technology is available to assist in the identification of facial images extracted from the video stream or from a watch list database. This function operates by comparing a subject.s photo to a database of faces and selecting the faces from the database which look the most like the subjects face. [6]

Figure 4.3: Face Recognition

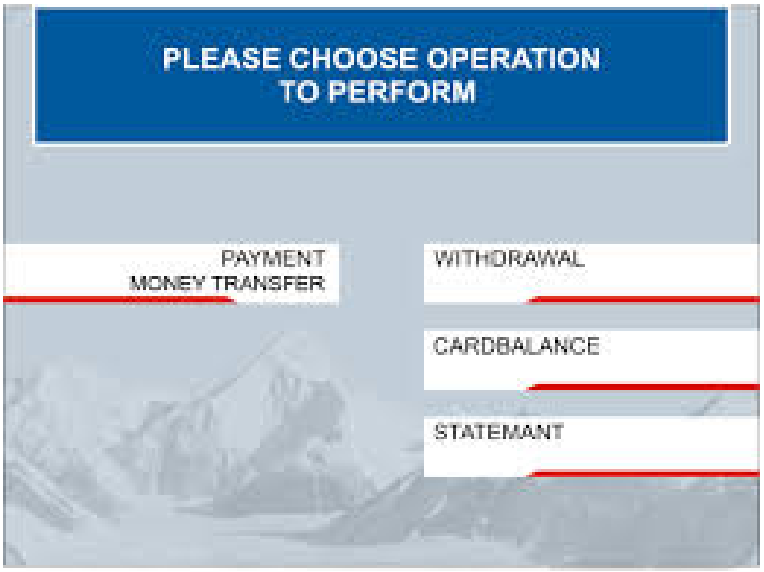

Figure 4.4: Generate A Message

Figure 4.5: Withdraw Money From ATM

4.3 Advantages And Disadvantages

4.3.1 Advantages:

- Verification rates as high as 90 percent have been attained when face recognition system had used in ATMs.
- It has been used to strengthen security.
- It can be used to reduce fraudulent attempts.
- The procedure used in Face Recognition Systems handle the changes in the light effectively. This is important since ATM use occur day and night, with or without fake light.
- With appropriate lighting and strong learning software, slight variations in the images could be accounted for.
- Positive visual match would cause the existing picture to be stored in the record so that future transactions would have a broader foot from which to compare if the original account photograph fails to provide a match.
- When a match is complete with the PIN but not the imagery, the bank could limit the transactions in a way granted upon by the user when the account was opened, and could store the photograph of the client for later examination by bank official.
- In regards to bank staff gaining access to customer PINs for use in fraudulent transactions, this system will reduce the threat to contact to the low limit forced by the bank and agreed to by the user on visually unverifiable transactions [4]

4.3.2 Disadvantages:

- Not identifying people correctly even if their photo is in the database. Changes in lighting and expressions like scream expressions, squinted eyes, changes in disguise like wearing hats; glasses drop recognition rates significantly even though the user is a genuine account holder.
- Matching profile changes worked reasonably well when the first guidance image(s) were frontal, which allowed 70-80 percent success rates for up to 45 degrees of profile change however, 70-80 percent achievement isn.t amenable to keeping ATM users content with the system.

- Consumers may be cautious of privacy concerns raised by maintaining images of clients in a bank database, encrypted or else, due to feasible hacking attempts or employee abuse. [3]

4.4 Summary

In this chapter,discussion on related with Security Of ATM is describe . In the next chapter,conclusion of ATM Image Processing Technology.

Chapter 5

Conclusion

Thus develop an ATM model that is more reliable in providing security by using facial recognition software. By keeping the time elapsed in the verification process to a negligible amount even try to maintain the efficiency of this ATM system to a greater degree. Biometrics as means of identifying and authenticating account owners at the Automated Teller Machines gives the needed and much anticipated solution to the problem of illegal transactions. It tried to proffer a solution to the much dreaded issue of fraudulent transactions through Automated Teller Machine by biometrics that can be made possible only when the account holder is physically present. Thus, it eliminates cases of illegal transactions at the ATM points without the knowledge of the authentic owner. Using a biometric feature for identification is strong and it is further fortified when another is used at authentication level.

Bibliography

[1] American Journal of Engineering Research (AJER) e-ISSN : 2320-0847p-ISSN : 2320-0936 Volume-02, Issue-05, pp-188-193 www.ajer.us

[2] Hossein Reza Babaei+, Ofentse Molalapata and Abdul-Hay Akbar Pandor Faculty of Information and Communication Technology, Limkokwing University of Creative Technology,Cyberjaya, Malaysia

[3] International Journal of Advanced Research in Computer Science and Software Engineering

[4] https:www.imagestechnology.org

[5] https:www.autherstream.com

[6] https:www.facereg.info

[7] https:www.wikipedia.com