Available online @ https://jjem.jnnce.ac.in
https:www.doi.org/10.37314/JJEM.2020.040203
Indexed in International Scientific Indiexing (ISI)
Impact factor: 1.025 for 2018-19
Published on: 30 March 2020

Face Authentication System Embedded with PIC18F458 for Automated Teller Machines

Rashmi M Hullamani [1*], Sushma S [2], Choodarathnakara A L[3], Karibasappa R[4]

[1*] Dept. of Electronics and Telecommunication Engineering,
JNN College of Engineering, Shimoga, India

[2,3,4] Dept. of Electronics and Communication Engineering,
Govt. Engineering College Kodagu, India

rashmimh@jnnce.ac.in, sushmas2790@gmail.com, choodarathnakara@gmail.com,
karibasappa2010@gmail.com

Abstract

Face recognition system is one of the biometric information process. Its applicability is easier and working range is wider than other biometric systems like signature, fingerprint, iris, etc. This paper proposes, a face recognition based authentication scheme for automated teller machine banking systems. The designed detection method extract face features from input image. The output image of the face detection algorithm has to be similar with the input image recognized for successful authentication. The proposed PIC18F458 Microcontroller based face recognition biometric scheme is successfully fused with the automated teller machine banking system for personal authorization with increased social security.

Keywords: *Face Recognition, GSM Technology, ATM, LCD, UART*

1. Introduction

Due to rapid development in science and technology, upcoming innovations are being built up with strong security. But on the other hand, threats are also being posed to destroy this security level. Though enhancement in automation has made a positive impact overall, but various financial institutions like banks and applications like ATM are still subjected to thefts and frauds. The existing ATM model uses a card and a PIN which gives rise to increase in attacks in the form of stolen cards, or due to statically assigned PINs, duplicity of cards and various other threats [1], [2].

Automatic Teller Machines are widely used in our daily lives due to their convenience, wide-spread availability and time-independent operation. Automatic retraction of forgotten card or cash by ATMs is a problem with serious consequences (lost time and money), typically caused by user inattention or negligence. This proposes a scheme in which the retraction rate of an ATM is decreased using face detection and recognition methods via ATMs built-in camera [3].

The human face is a dynamic structure with characteristics that can quickly and radically change with time. Face recognition is useful in many areas such as medical records, online banking, Passports, driver licenses, video surveillances, investigation, biometrics, access control, law enforcement, surveillance system, security systems, identification of criminals, verification of credit cards and so on [4].

2) The following four-stage process illustrates the way of biometric system operates. 1) Capture: A physical or behavioral sample is captured by the enrolment 2) Extraction: Unique data is extracted from the sample and a template is created 3) Comparison: The template is then compared with a new sample 4) Matching;

The system then decides if the features extracted from the new sample are matching or not. Fig. 1 depicts the four stage process of face authentication system.

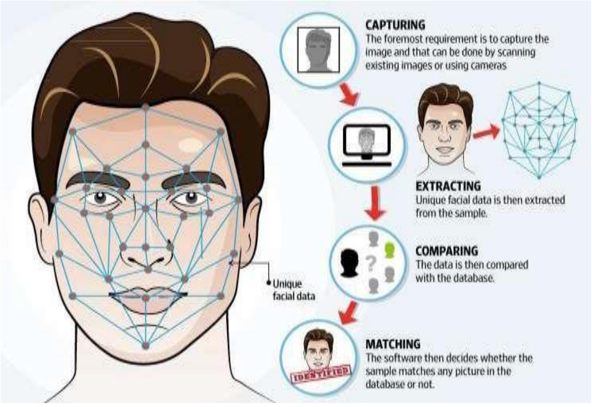

CAPTURING
The foremost requirement is to capture the image and that can be done by scanning existing images or using cameras
EXTRACTING
Unique facial data is then extracted from the sample.
COMPARING
The data is then compared with the database.
MATCHING
The software then decides whether the sample matches any picture in the database or not.
Unique facial data
IDENTIFIED

Figure1: Face authentication system

This paper is categorized into five sections. Section I consists of brief Introduction about Face Recognition Based Smart Banking Machine Embedded with GSM Technology. Section II describes the hardware design and Section III details software implementation. Section IV shows the experimental results and Section V concludes the final outcomes.

2. Hardware Implementation

With the technological advances in financial infrastructure, most bank customers prefer to use Automatic Teller Machines (ATMs) and Internet websites for carrying out their banking transactions. Financial users especially utilize ATMs for physical transactions like cash withdrawal or cash deposit. However, just like any other system, ATMs are also suffering from numerous issues caused by users. Among these problems, card and/or cash forgetting (CCF) is a common issue. The main goal of our work is to propose a computer vision framework which uses web ATM camera to performs face detection and recognition in case of forgotten pin, card lost, card cancellation.

Face recognition technology is the least intrusive and fastest biometric technology. It works with the most obvious Individual Identifier of human face. Instead of requiring people to place their hand on a reader (a process not acceptable in some cultures as well as being a source of illness transfer) or precisely position their eye in front of a scanner, face recognition systems unobtrusively take pictures of people's faces as they enter a defined area. There is no intrusion or delay, and in most cases the subjects are entirely unaware of the process. They do not feel "under surveillance" or that their privacy has been invaded. Every face has numerous, distinguishable landmarks, the different peaks and valleys that make up facial features. Each human face has approximately 80 nodal points. Some of these measured by the Facial Recognition Technology: Distance between the eyes, Width of the nose, Depth of the eye sockets, shape of the cheekbones and length of the jaw line.

Figure 2: GSM module

A. GSM Module

Figure 2 shows GSM module.

Global system for mobile communication is a globally accepted standard for digital cellular communication. GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard that would formulate specifications for a pan-European mobile cellular radio system operating at 900 MHz it is estimated that many countries outside of Europe will join the GSM partnership.

GSM is an open, digital cellular technology used for transmitting mobile voice and data services. GSM uses a variation of Time Division Multiple Access (TDMA) and is the most widely used of the three digital wireless telephone technologies (TDMA, GSM, and CDMA). It operates at either the 900 MHz or 1,800 MHz frequency band. It supports voice calls and data transfer speeds of up to 9.6 kbps, together with the transmission of SMS.

B. LCD Display

This component is specialized to be used with the microcontrollers, which means that it cannot be activated by standard IC circuits. It is used for displaying different messages on a miniature liquid crystal display. Because of its low price and great capabilities this model frequently used in practice. It can display messages in two lines with 16 characters each as shown in figure 3. It displays all letters of alphabet, Greek letters, punctuation marks, mathematical symbols. In addition, it is possible to display symbols made up by the user. Other useful features include automatic message shift (left and right), cursor appearance and LED backlight.

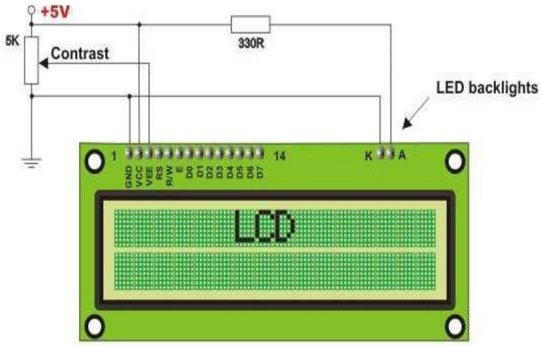


Figure 3: LCD connection with resistor

Figure 4 shows LCD screen which consists of two lines with 16 characters each.

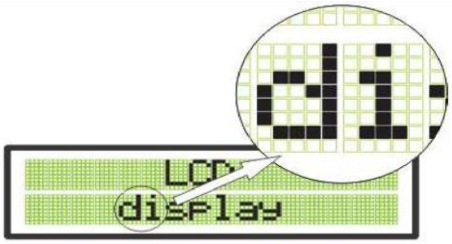


Figure 4: LCD Screen

Every character consists of 5x8 or 5x11 dot matrix and it covers 5x8 character display, which is indeed the most commonly used one display contrast depends on power supply voltage and whether messages are displayed in one or two lines. For that reason, varying voltage 0-Vdd is applied on the pin marked as Vee. Trimmer potentiometer is usually used for that purpose. Some LCD displays have built in backlight (blue or green diodes). When it is used during operation, a current limiting resistor should be serially connected to one of the pins for backlight (similar to LED diodes). If there are no characters displayed or if all of them are dimmed upon the display is switched on, it should be done to check the potentiometer for contrast adjustment. It is properly adjusted then it applies the mode of operation has been changed.

C. UART

The UART is a 16 bytes Receive and Transmit with FIFOs. The receiver FIFO triggers points at 1, 4, 8, and 14 bytes. The built-in fractional baud rate generator covers wide range of baud rates without a need of external crystals of particular values. The transmission FIFO control enables implementation of software (XON/XOFF) flow control in UART.

D. PIC Microcontroller

PIC18F458 Microchip believes that its family of PIC microcontroller is one of the most secure products of its kind on the market today. When used in the intended manner and under normal conditions. There are dishonest and possibly illegal methods used to breach the code protection feature..The person doing so may be engaged in theft of intellectual property. Microchip is willing to work with the customer who is concerned about the integrity of their code. Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as “unbreakable”. Code protection is constantly evolving and Microchip is committed to continuously improving the code protection features of product.

E. Face Authentication System

Figure 5 shows the proposed Face Authentication System.

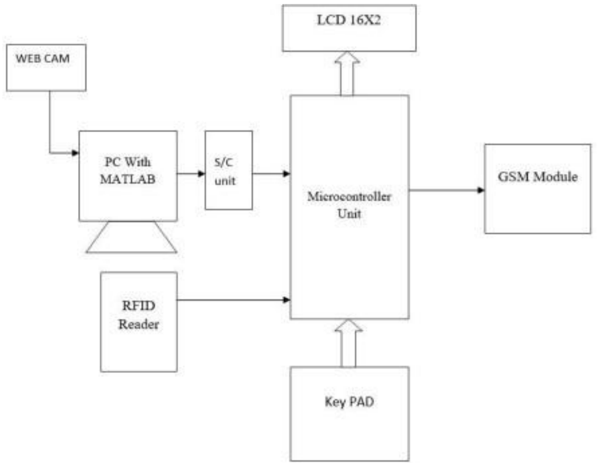


Figure 5: Proposed Face Authentication System.

The proposed system consists of cooperative components of a webcam in PC, PIC18F458 microcontroller unit, signal conditioning unit 16X2 LCD Display, ULN2003, stepper motor, RFID reader and Tag, DTMF keypad, GSM module. Hard ware description of proposed system. This system is placed in the ATM centers and MATLAB technology is used for facial recognition and identifies the face of the person. Once the person enters into the ATM centre, the person lost the ATM card; he wants to withdraw the amount by using face recognition. For face recognition technology a snap of yours ID already in the database of your bank account, once the face is matched with the already stored image, the person can withdraw the money.

Signal conditioning unit is used in this system is to give the voltage compatibility between the microcontroller and pc of the system. RFID reader and tag module are used to read the RFID tag. If the person lost the ATM card, then if the unauthorized person uses that card for withdraw purpose, customer must swipe the card that time. A SMS is sent to the account holder ATM card is used by an unauthorized person. For that purpose, RFID reader is used. For sending the SMS information a GSM is used and is connected to microcontroller, it works by sending an AT commands to GSM by microcontroller. Driver unit is used to drive the stepper motor by providing the suitable current. i.e., by current amplification. LCD display 16 x 2 is used for display the transaction mode, cancellation mode, enter amount, enter password, swipe the card, and whether face recognition or not. Dual tone multi frequency signal is used to enter the inputs by using keypad by touch the keypad.

When, the user faces the camera, standing about two feet from it. The system will locate the user's face and perform matches against the claimed identity or the facial database. It is possible that the user may need to move and reattempt the verification based on his facial position. The system usually comes to a decision in less than 5 seconds.

3. Software Implementation

A. Flow Chart

Flow chart is shown in figure 6.

B. Algorithm

Step 1: Initialize the PIC18F458 Microcontroller

Step 2: Initialization of PIC18F458 Microcontroller ports, LCD, UART, and input and output variables.

Step 3: Check while (n) condition.

Step 4: Read the data from the Dual-Tone Multi- Frequency [DTMF] keypad.

Step 5: Check if condition is 1; then the condition is yes, it display the normal withdraw mode for withdrawal of amount.

Step 6: If the condition is No, then it go back to read again the data from DTMF keypad.

Step 7: Check if condition is 2, then the condition is yes, then it displays the face recognition-based transaction and card cancellation mode. If the face is recognized then the amount is withdrawn and then customer's card is automatically deactivated after transaction.

Step 8: If the condition is No, than again it go back to read the data from DTMF keypad again.

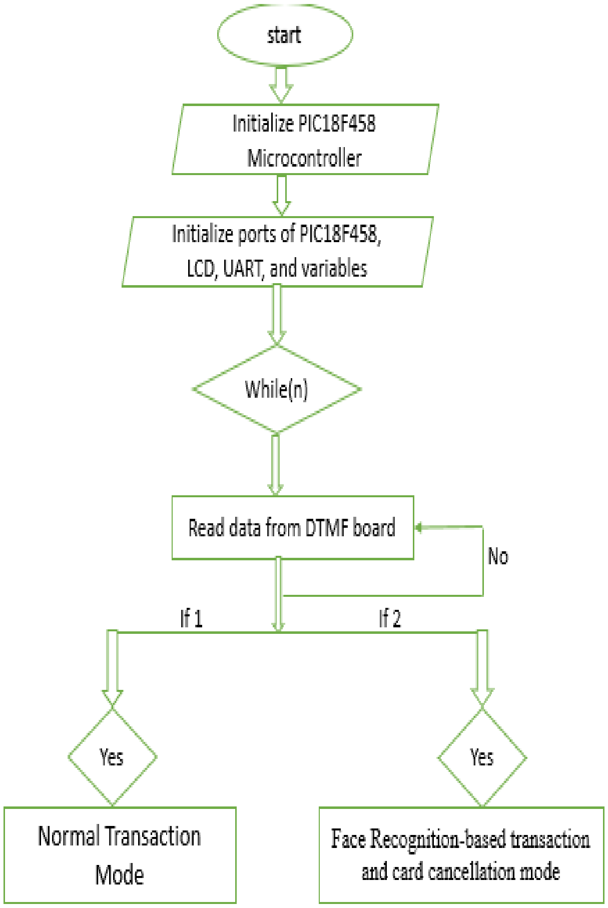

start
Initialize PIC18F458 Microcontroller
Initialize ports of PIC18F458, LCD, UART, and variables
While(n)
Read data from DTMF board
No
If 1
If 2
Yes
Yes
Normal Transaction Mode
Face Recognition-based transaction and card cancellation mode

Figure 6: Flow Chart

4. Experimental Results

The proposed hardware connection circuit of the system is shown in figure 7, which presents a biometric method using face recognition technology. This technology includes one-time face recognition transaction and card deactivation and transaction mode works by recognizing the face of the customer.

The proposed system follows two operation modes namely: Normal transaction mode and face recognition mode**.**

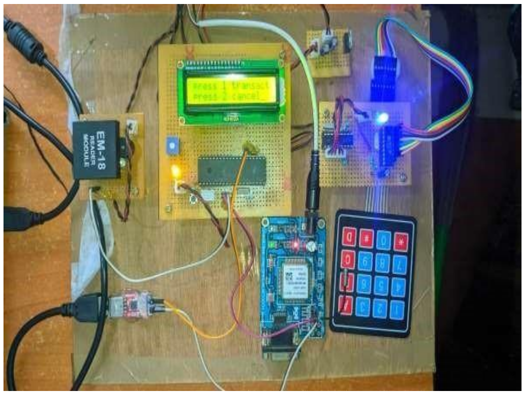
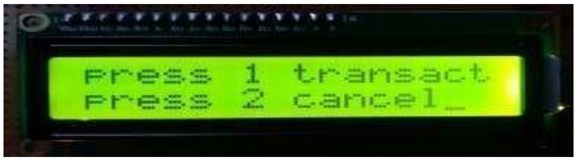


Figure 7: Hardware connection circuit of proposed face authentication system

A. Normal Transaction Mode

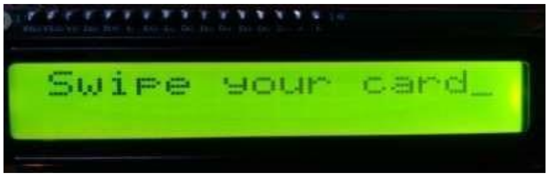
Process of Normal transaction in ATM includes: Press 1 for transaction mode for withdrawal of amount (figure 8).



press 1 transact
press 2 cancel_

Figure 8: Mode selection

If the user as his/her having ATM card, he/she can swipe the card (figure 9) and can withdraw the amount.



Swipe your card_

Figure 9: Swipe the card

To withdraw the amount he/she can swipe the card then enter the ATM password, next enter the amount, after selecting the transaction then enter amount have to be withdrawn. After, the display shows that the transaction is being process and go to collect the money which you have entered to be withdrawn. After collecting money, transaction is completed. A message is received by the corresponding mobile number which is linked with the bank account. These steps are illustrated in figures 10 - 17.

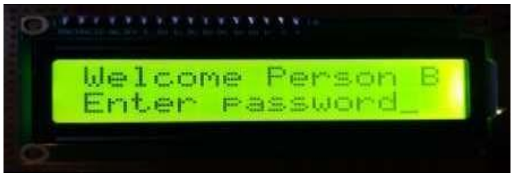

Welcome Person B
Enter password_

Figure 10: Enter password

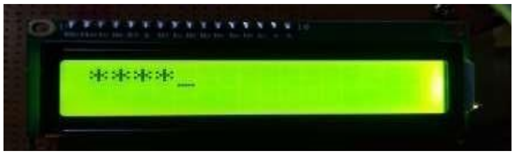

****_

Figure 11: Password Entered

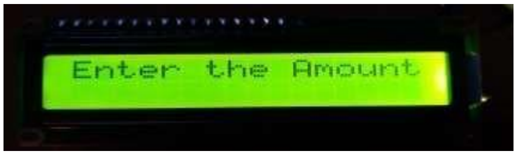

Enter the Amount

Figure 12: Entering Amount

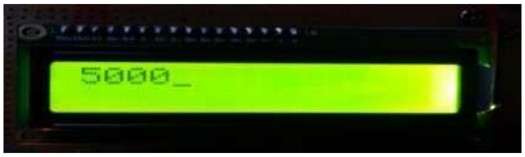

5000_

Figure 13: Entering Amount

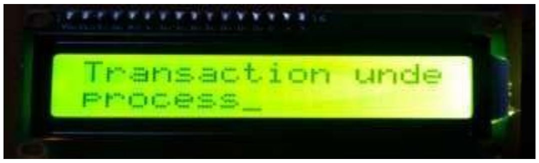

Transaction unde
process_

Figure 14: Process of Transaction

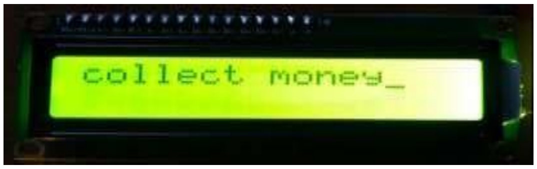

collect money_

Figure 15: Collecting Money

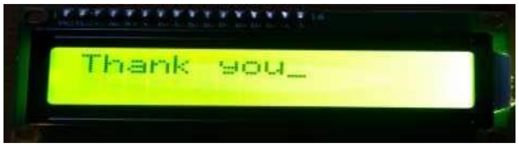
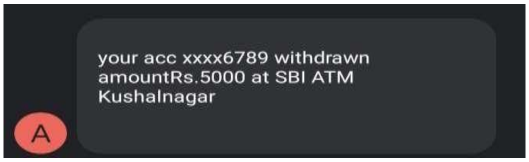

Thank you_

Figure 16: Transaction Completed



your acc xxxx6789 withdrawn amountRs.5000 at SBI ATM Kushalnagar

Figure 17: Message Received

B. Biometric Transaction Mode

This transaction mode works by recognizing the face of the customer, if the customer face matches with the card holder face which is saved in the database of the card holder bank account. After the face matches the above process is repeated, the steps as follows: enter amount to be withdraw, collect the money, transaction is completed. The face recognition technology is implemented by MATLAB software.

The image of card holder is captured. If face is recognized, the amount can be withdrawn successfully as like as normal transaction mode. Steps are same as normal transaction mode except the card swipe; here the face will be recognized. Message is received from the bank after receiving cash from the ATM than that card is deactivated. If face is not recognized, it will show that the card holder is unknown person and card is deactivated automatically. Also when unauthorized person uses the card at that time, the system sends SMS to the corresponding bank that the card is assessed by unauthorized person and the process is shown below:

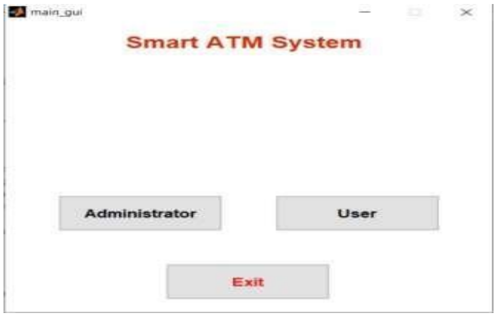
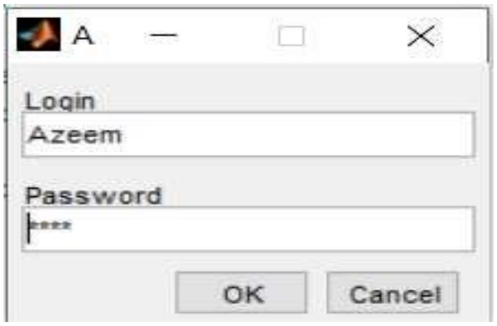


Figure 18: Biometric ATM Screen

Figure 18 shows the biometric ATM screen displayed during experimentation. The process is continued by login into account by entering the password provided by the bank (figure 19).



Login
Azeem
Password
****

Figure 19: Admin Page of Biometric ATM Screen

After login to the account, the image of card holder is captured. If face is recognized the amount can be withdrawn successfully as like as normal transaction mode. Steps are same as normal transaction mode except the card swipe; the face will be recognized (figure 20).

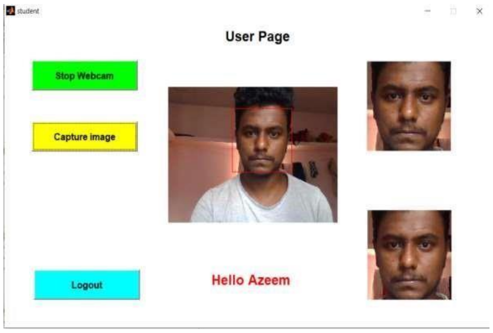
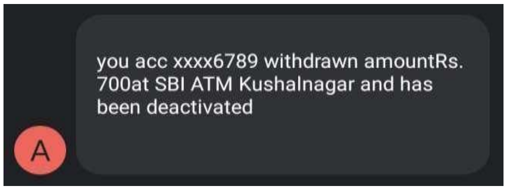


Figure 20: Face Matched as Authorized Person

Message received from the bank after receiving cash from the ATM, after that the card is deactivated (figure 21).



you acc xxxx6789 withdrawn amountRs. 700at SBI ATM Kushalnagar and has been deactivated

Figure 21: Message of Transaction by authorized person

If the face is not recognized, it will show that the card holder is unknown person (figure 22) and card is deactivated automatically. When unauthorized person uses the card at that time an SMS is sent from the bank that the card is assessed by unauthorized person is used.

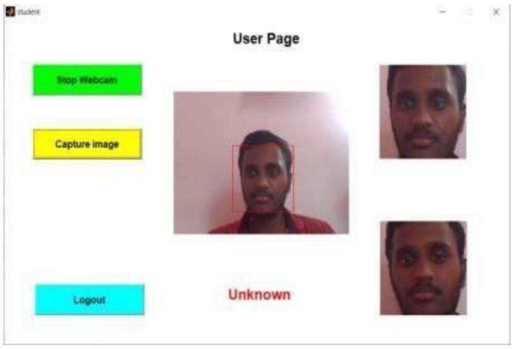


Figure 22: Face Not-matched as unauthorized person

Automatic Teller Machines is the most used technology in the increasing financial transaction of the current world. There are many possible ways to misuse ATM card when it lost. Fingerprint recognition helps to achieve an authentic state of security access through verification and validation to block the ATM card. This system identifies a high-level model for the modification of existing ATM systems using both security protocols as PIN & Biometric fingerprint strategy and GSM technology. It is able to develop a fingerprint mechanism as a biometric measure to enhance the security features of the ATM for effective banking.

5. Conclusion

In this proposed system, face recognition technology for transaction of money and cancellation of card without using ATM card only by using our face texture. But in future this proposed system can be implemented by adapting a new technology that is by developing a new application in mobile to deactivation of ATM Card instead of going to ATM centers and deactivate there. This future scope will helpful and very advantageous because it reduces time and increases security to our Bank account.

The advantages of Smart banking machine with GSM technology are the proposed system will improve the level of security of ATM transaction system, initially captured fingerprint images are converted to templates instead of storing anywhere which makes misuse of the system totally impossible, voids the Misuse cards, when card is lost.

Disadvantages are not always accurate, hindered by glasses, masks, long hair. Musk asks users to have a neutral face when pictures are being taken, by considered an invasion of privacy to be watched. Applications are Voting Machines, Biometric Door security system, Ration Cards, RC book and Driving License, Personal health recorder.

References

1. Anil K. Jain, Jianj Feng, Karthik Nandakuma, Fingerprint Matching, IEEE Computer Society, 0018- 9162/10, 2010, 36-44,

2. Mohsin Karovaliyaa, Saifali Karediab, Sharad Ozac, Dr. D. R. Kalbanded, Enhanced security for ATM machine with OTP and Facial recognition features". Procedia Computer Science, Vol. 45, 2015, 390 – 396, doi: 10.1016/j.procs.2015.03.166

3. Ekberjan Derman, Y. Korat Gecici, Short Term Face Recognition For Automatic Teller Machine (ATM) Users, Proceedings of the International Conference on Electronics, Computer and Computation (ICECCO), Ankara, Turkey, Nov. 2013.

4. K. Sai Prasad Reddy, Dr. K Nagabhushan Raju, "Design and Implementation of Algorithm for Face Recognition by using Principal Component Analysis (PCA) in MATLAB". International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 10, October 2016, 115-119.