FACE RECOGNITION BASED NEW GENERATION ATM SYSTEM

Dr S Sasipriya[1], Dr P. Mayil Vel Kumar[2], S. Shenbagadevi[3]
Professor[1], Department of Electronics and Communication Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, India 641008, sasipriyas@skcet.ac.in
Associate Professor and Head /CSE, Karpagam Institute of Technology, Coimbatore, India
Assistant Professor, Karpagam Institute of Technology, Coimbatore, India

Abstract - **In the technological advances in financial infrastructure, most bank customers prefer to use Automatic Teller Machines (ATM) for carrying out their banking transactions. To improve the security of these transactions, a new generation ATM machine which is based on face recognition system which replaces ATM card with RFID tag. In this, high quality image has important role in recognition process. Face image is used for authentication purpose. Firstly, the face image of particular person is compared with the database image. Then the compared output result is sent to the control unit through serial communication. If an unauthorized person is identified, an alert message is sent to the corresponding user. Thus, an ATM model which provides security by using Facial verification software by adding up facial recognition systems can reduce forced transactions to a great extent and provide hard-secure authentication. Here Raspberry Pi microcontroller is used in the controlling part.**

Keywords— **ATM,Raspberry Pi, RFID Tag, SEPIA.**

1. INTRODUCTION

Rapid development in science and technology, innovations are being built-up and this has made a positive impact overall, but various financial institutions are still subjected to thefts and frauds.ATM terminals are designed to facilitate easier withdrawal of money for the customers. ATM establishes the stability of the infrastructure in great deal because of their number of bank transactions. Due to their availability and general user friendliness ATMs have become very popular with general public. There are two types of ATMs: one is used for cash withdrawal and to get the receipt of account balance and another one is for deposits and money transfer. ATM provides PIN (Personal Identification Number) to all its users with the help of which they can access their account. To carry out consumers ATM financial transactions and/orbanking functions at any time ATMs are available on a continuous basis. Since the transaction is mostly dependent on PIN-based verification several usability factors have been studied to enhance the security for authentication of users at ATM. Socio-physical factors such as, queue length distractions length of time for the interaction, urgency physical hindrance, memorization of PINs, co-located user display, speed of interaction, and the environment are all determinants of the insecure for the procedure. The major concerns from all of these factors are correlated to detect fraudulent card transactions. Here we propose face recognition with 6-digit OTP generation to reduce the frauds during transactions in an ATM.

2. LITERATURE SURVEY

Financial institutions have registered major loses till today due to users being exposed of their credit and debit card information. For secure PIN authentication, in this paper, we propose Secure-PIN-Authentication-as-a-Service (SEPIA), a secure obfuscated PIN authentication protocol for ATM and other point-of-service terminals using cloud-connected personal mobile and wearable devices. It protects the user from intermediate transaction attacks. A SEPIA user utilizes a mobile device for scanning or QR code on the terminal screen to prove co-location to the cloud-based server and obtain a secure PIN template for point-of-service authentication [7].Features like face recognition and one time password are used for the enhancement of security of accounts and privacy of users. Face recognition technology helps the machine to identify each and every user uniquely thus making face as a key. This eliminates the chances of fraud due to theft and duplicity of the ATM cards. Moreover, the randomly generated OTP frees the user from remembering PINs as it itself acts as a PIN [4]. ATM are widely used nowadays by people. But It's hard if we forget the PIN number or it may get damaged and users can have a situation where they can't get access to their money. In this the use of biometrics for authentication instead of PIN and ATM card is encouraged. Here, The Face ID and Fingerprint are preferred to high priority. The fingerprint is preferred to high priority. The fingerprint of the user is identified and face image is verified, and the appropriate user is given authentication. For the prototype of the system, Raspberry pi microcontroller is used [8]. Faces are represented by labeled graphs, based on a Gabor wavelet transform.Image graphs of new faces are extracted by an elastic graph matching process and can be compared by a simple similarity function. Phase information is used for accurate node positioning. Object-adapted graphs are used to handle large rotations in depth [5].ATM with a currency dispenser includes a contactless card reader that can read data from an RFID tag of a customer's ATM card. The contactless card reader can also be used in conjunction with a magnetic stripe card reader. It is able to prevent the missing of the ATM card and dispensed money by the customer inside the ATM centre after the transaction [1]. An automatic teller machine security model that would combine a physical access card, a PIN, and electronic facial recognition having access only to actual owner of the card [2].Denis et. al., [9] explores the difficulties in Blockchain IoT applications, and outlines the huge work in order to analyze how Blockchain could be utilized in real money coordination. The author in [10] has examined the different error codes thrown by various ATM machines produced by different manufacturers and proposed a common code for very similar malfunctions made by the machine.

3. EXISTING METHOD

Existing ATMs are convenient and easy to use for most consumers. Existing ATMs typically provide instructions on an ATM display screen that are read by a user to provide for interactive operation of the ATM. Having read the display screen instructions, a user is able to use and operate the ATM via data and information entered on a keypad. However, the drawback in the existing system is that the user should carry their ATM card without fail. But in many cases, we forget it. So only we designed a system which helps us to use the ATM machine without the ATM card.

4. PROPOSED SYSTEM

A. *HardwareDesign*

Multilevel RFID, Face Recognition and OTP (or) PIN numberbased user authentication and Alert mails send with the face and OTP. Haar-cascade and Local binary pattern (LBP) was utilized to extract the texture features of the face for recognition. Face Recognition based user authentication system with SMS alert 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. The aim of our work is to use embedded ATM camera to perform face detection with the help new computer vision framework. Authentication of customers at computerized teller machines (ATMs) is normally dependent on PIN-based totally verification. Several elements had been studied so far in enhancing the security for authentication of customers at ATMs. In first scenario, tag number and face recognition are matched means transaction proceeds. In the second scenario, tag number and face recognition are not matched means captured image and OTP is sent to the card holder. The particular user is known means OTP can be shared and the transaction proceeds. The particular user is not known means the OTP is not shared and the transaction failed.

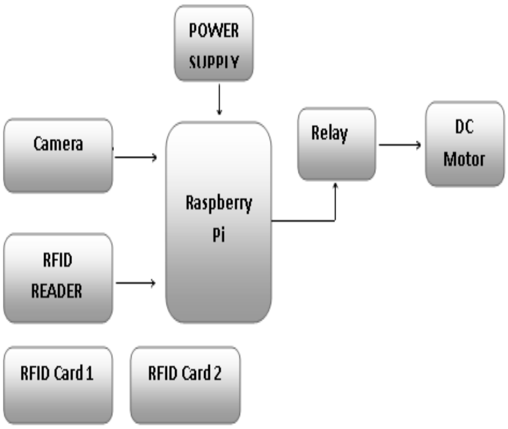


Fig 1: Block diagram Of ATM architecture

1) Raspberry Pi

The Raspberry Pi is a low cost, credit-card sized computer that plugs into a computer monitor or TV, and uses a standard keyboard and mouse. It is a device that enables people of all ages to explore computing, and to learn how to program in languages like Scratch and Python.

2) RFID

- ✓ Radio frequency Identification (RFID) is to identify the presence of RFID tags with the help of wireless identification technology that uses radio waves for identification.
- ✓ Just like Bar code reader, RFID technology is used for identification of people, object etc. presence.
- ✓ In barcode technology, optical scanning of the barcode by keeping in front of the reader is used, but in RFID technology it is enough to bring RFID tags in range with the readers. Barcodes can get damaged or unreadable easily, so RFID is preferred.
- ✓ RFID is used in many applications like attendance system in which every person will have their separate RFID tag which will help identify person and their attendance.
- ✓ RFID is used in many companies to provide access to their authorized employees. It is also helpful to keep track of goods and in automated toll collection system on highway by embedding Tag (having unique ID) on them.

2.1 RFID READER AND MODULE

RFID TAG is used to read unique ID from RFID tags. Whenever RFID tags comes in range, RFID reader reads its unique ID and transmits it serially to the microcontroller or PC. RFID reader has transceiver and an antenna mounted on it. It is mostly fixed in stationary position. Basically, RFID systems categorised as active and passive based on how they are powered and their range.

1. *Active RFID system*

Active RFID tags have their own transmitter and power source (Mostly battery operated). They operate at 455 MHz, 2.45 GHz, or 5.8 GHz, and they typically have a read range of 60 feet to 300 feet (20 meters to 100 meters).

2. *Passive RFID system*

Passive RFID tags do not have a transmitter, they simply reflect energy (radio waves) back coming from the RFID reader antenna. They operate in Low frequency (~125 KHz) as well as High frequency (~13 MHz) band and have limited read range of up to ~1m.

2.2 EM18 MODULE

EM18 is a RFID reader which is used to read RFID tags of frequency 125 kHz. After reading tags, it transmits unique ID serially to the PC or microcontroller using UART communication on respective pins. EM18 RFID reader reads the data from RFID tags which contains stored ID which is of 12 bytes. EM18 RFID reader doesn't require line-of-sight. Also, it has identification range which is short i.e. in few centimetres.

3) Relay

A relay is an electrically operated transfer. Current flowing via the coil of the relay creates a pressure that attracts a lever and modifications the switch contacts. The coil current will be on or off consequently. Relays have two transfer positions and they may be double throw (changeover) switches. Relays allow one circuit to alter a second circuit which can unfastened the primary. For instance an occasional voltage battery circuit will use a relay to regulate a 230V AC mains circuit. There is no electric affiliation in the relay between the two circuits. The hyperlink is magnetic and mechanical.

4) Camera Module

A camera is a record and stores photographic image in digital form. Many current models are also able to capture sound or video, in addition to still images. Capture is usually accomplished by use of a photo sensor, using a charged coupled device.

B. SOFTWAREDESIGN

1) LBP ALGORITHM

Local Binary Pattern (LBP) is a simple algorithm which is very efficient in texture classification. In this, labelling the pixels of an image by thresholding the neighbourhood of each pixel and the result is considered as a binary number**.** The binary results combined with the histograms, representation of the face images with a simple data vector is made. There are four steps in LBP algorithm which includes,

- ✓ **Parameters of LBP Algorithm**: LBP uses four parameters which includes Radius, Neighbours, Grid X and Grid Y.
- ✓ **Training the Algorithm:** The first step in LBP is to train the algorithm. For that we need to use a dataset with the facial images of the person whose face has to be recognized. The dataset should be set with an ID (it may be a number or name of the person for each image) for each image, so that it will be easy to use use this information for recognition of an input image and gives you an output. If the image of the person is same it should have the same ID (i.e overridden of new image in the existing dataset). If the training is done then the next step is the LBP operation.
- ✓ **Applying the LBP operation:** In this an intermediate image which gives a description of the original image is created. A sliding window concept is used for recognizing facial characteristics, based on the parameters such as radius and grids. Original image is converted into binary scale image in this step.
- ✓ **Extracting the Histograms:** The image that we took is converted into gray scale, so in the gray scale images there are only 256 positions (0~255) for each histogram (from each grid). These positions represent each pixel intensity. Since we divide the image and extract the histograms, we have to concat each histogram to form a single histogram. The characteristics of the original image is seen in the final histogram image.

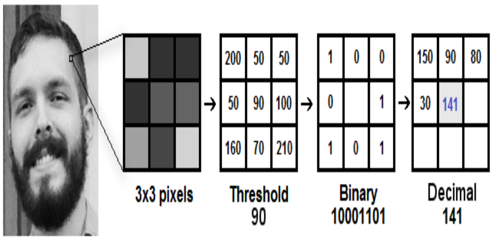


Fig 2: Applying LBP Algorithm

Let us consider the above image and apply LBP algorithm,

- Consider the facial image in a gray scale and take a part of the image as 3x3 pixels window.
- This image can be represented as 3x3 matrix having intensity of 0~255 for each pixel.
- Now take the central value of 3x3 pixel which is used as the threshold value and it is new values are defined to 8 neighbouring pixels using this threshold.
- Set a new binary value for each neighbouring pixel. If the value is equal or greater than the threshold then set 1 otherwise set 0 for lower values.
- Now ignoring the central pixel value, the 3x3 matrix will contain only binary values and concate all the binary values from each position from the matrix in line order and we get the new binary value (1001101).
- On converting this binary value into decimal value and when setting the central value, it gives the pixel value of the original image. In this final step we now get an original image with better features.
- Now this image is compared the the dataset image (histogram image compared) on calculating the distance between the two histogram gives a value. If that value is nearer to the value we fixed for the image, the image is recognized.

2) HAAR CASCADE ALGORITHM

Haar Cascade algorithm is a deep learningbased approach for face detection. Face detection is made possible by training a cascade function from a lot of positive and negative images.

Three are four stages in Haar Cascade algorithm which includes:

- Haar Feature Selection
- Creating Integral Images
- Adaboost Training
- Cascading Classifiers

When an image is captured by the camera, the first step is to extract the features in the image. Suppose, let us take an image with 8x8 pixels we can able to extract 160000+ features in single image. Since face detection is not possible with features with the single image, the second step is to train the system with lot of positive and negative images. From each image features are selected with some threshold value and all the features are added which is further used for detection. At this the 160000+ features get lowered to 6000 features. The next step is the face detection, Since, comparing the captured image with 6000 features is also tedious, divide the features into cascading classifiers where a small portion of feature is compared with the captured image. If any of the feature selected is not matched with the captured image, the image is not detected.

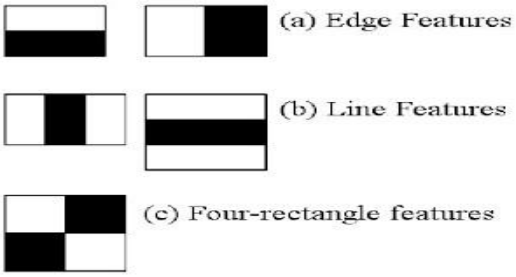


Fig 3: Features of Haar cascade

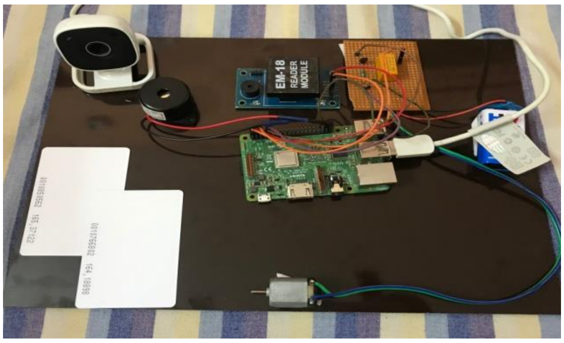


Fig 4: Working Model

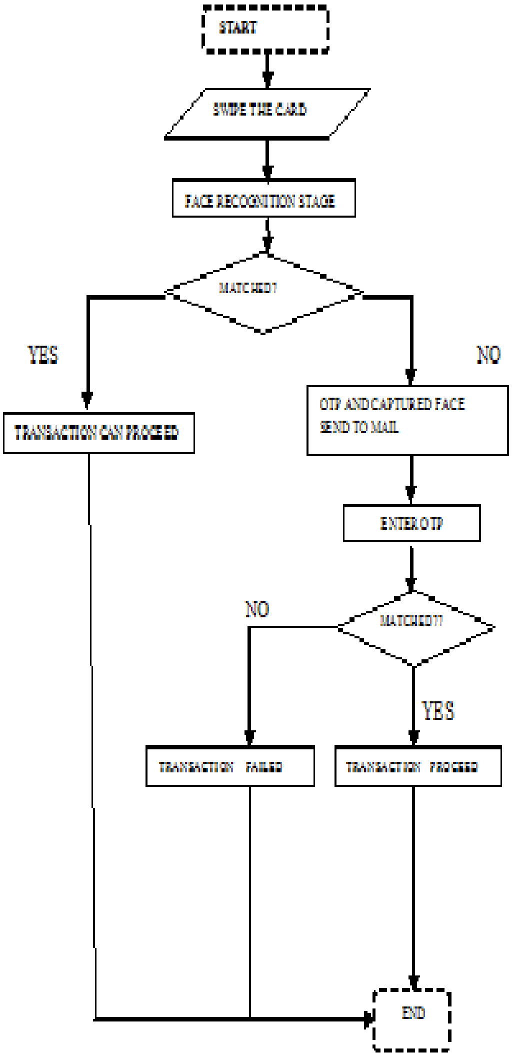
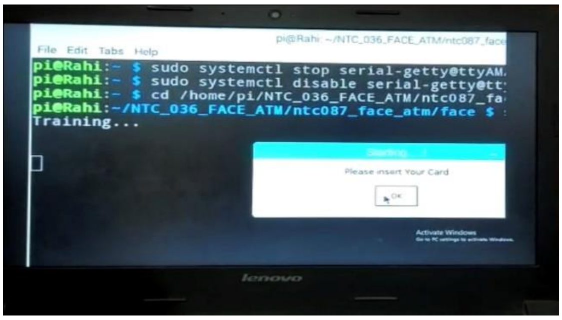


Fig 5: Flowchart of ATM model

5. RESULT DISCUSSIONS

Case 1: When face matched

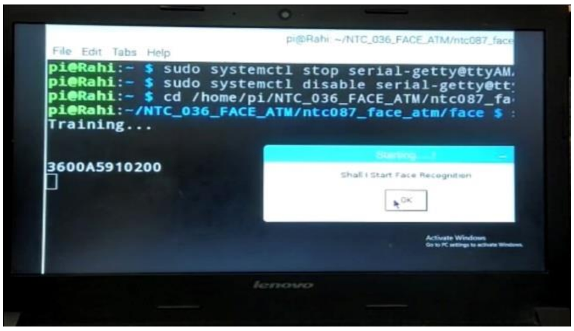


```
pi@Rahi: ~/NTC_036_FACE_ATM/ntc087_face
File  Edit  Tabs  Help
pi@Rahi:~ $ sudo systemctl stop serial-getty@ttyAM
pi@Rahi:~ $ sudo systemctl disable serial-getty@tt
pi@Rahi:~ $ cd /home/pi/NTC_036_FACE_ATM/ntc087_fa
pi@Rahi:~/NTC_036_FACE_ATM/ntc087_face_atm/face $
Training...
```

Please insert Your Card

Fig 6.1(a) Inserting the card

On inserting the card (Figure 6.1(a)), face recognition is started (Figure 6.1(b)), if the face is matched with the face in the card, then the transaction is successful (Figure 6.1(c)).

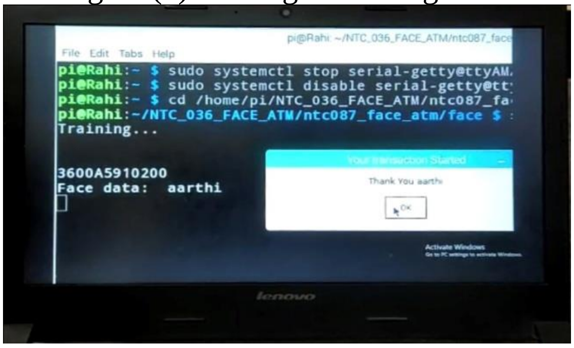


```
pi@Rahi:~ $ sudo systemctl stop serial-getty@ttyAM
pi@Rahi:~ $ sudo systemctl disable serial-getty@tt
pi@Rahi:~ $ cd /home/pi/NTC_036_FACE_ATM/ntc087_fa
pi@Rahi:~/NTC_036_FACE_ATM/ntc087_face_atm/face $ :
Training...

3600A5910200
```

Shall I Start Face Recognition

Activate Windows
Go to PC settings to activate Windows.

Fig 6.2(b) Starting face recognition



```
pi@Rahi:~ $ sudo systemctl stop serial-getty@ttyAM
pi@Rahi:~ $ sudo systemctl disable serial-getty@tt
pi@Rahi:~ $ cd /home/pi/NTC_036_FACE_ATM/ntc087_fa
pi@Rahi:~/NTC_036_FACE_ATM/ntc087_face_atm/face $ :
Training...

3600A5910200
Face data:  aarthi
```

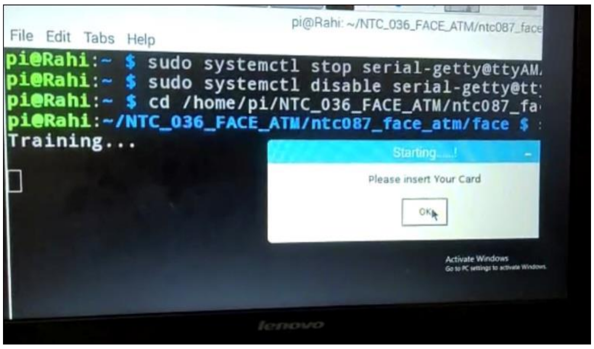
Thank You aarthi

Activate Windows
Go to PC settings to activate Windows.

Fig 6.3(c) Transaction successful

Case 2: When face matched and OTP is correct

On inserting the card (Figure 6.2(a)), face recognition started (Figure 6.2(b)), if the face recognised matches with the face in the card then transaction successful. If not matched, it asks to enter an OTP (Figure 6.2(c)). An OTP along with the face is sent to the card holder's mail(Figure 6.2(d)). If the card holder knows the person, he can convey the OTP to the person. If the person enters the correct OTP (Figure 6.2(e)) then the transaction is successful (Figure 6.2(f)).

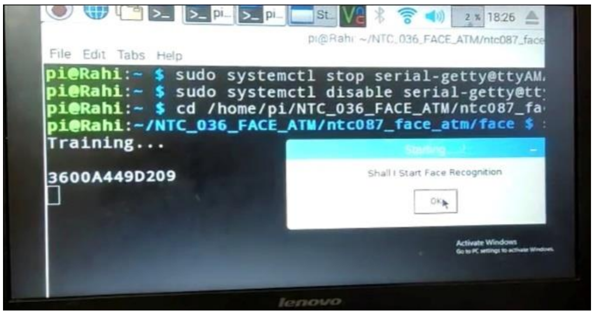


```
pi@Rahi:~ $ sudo systemctl stop serial-getty@ttyAM
pi@Rahi:~ $ sudo systemctl disable serial-getty@tt
pi@Rahi:~ $ cd /home/pi/NTC_036_FACE_ATM/ntc087_fa
pi@Rahi:~/NTC_036_FACE_ATM/ntc087_face_atm/face $ :
Training...
```

Please insert Your Card

Activate Windows
Go to PC settings to activate Windows.

Fig 6.2(a) Inserting the card

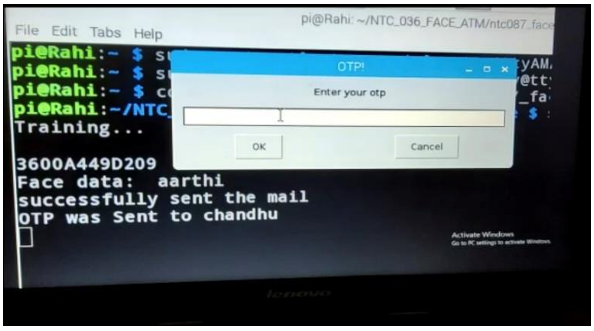


```
pi@Rahi:~ $ sudo systemctl stop serial-getty@ttyAM
pi@Rahi:~ $ sudo systemctl disable serial-getty@tt
pi@Rahi:~ $ cd /home/pi/NTC_036_FACE_ATM/ntc087_fa
pi@Rahi:~/NTC_036_FACE_ATM/ntc087_face_atm/face $ :
Training...

3600A449D209
```

Shall I Start Face Recognition

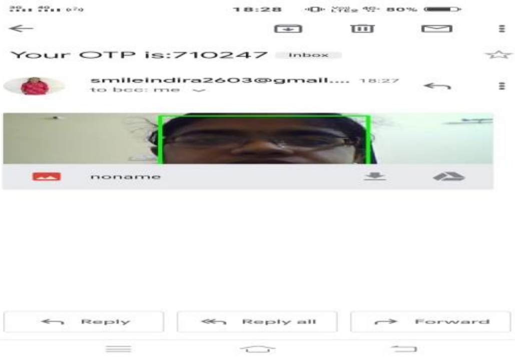
Activate Windows
Go to PC settings to activate Windows.

Fig 6.2(b) Starting face recognition


pi@Rahi: ~/NTC_036_FACE_ATM/ntc087_face
File Edit Tabs Help
OTP!
Enter your otp
OK
Cancel
Activate Windows
Go to PC settings to activate Windows.

```
pi@Rahi:~ $ s
pi@Rahi:~ $ s
pi@Rahi:~ $ c
pi@Rahi:~/NTC_
Training...

3600A449D209
Face data:  aarthi
successfully sent the mail
OTP was Sent to chandhu
```

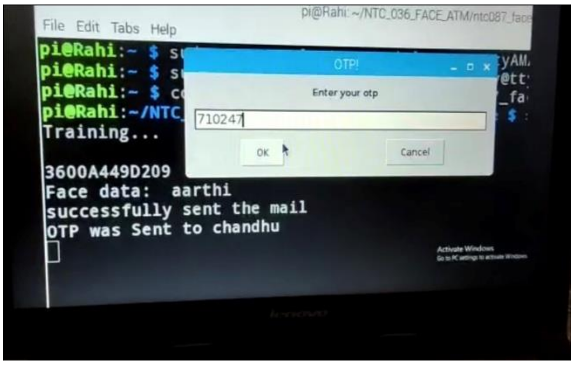
Fig 6.2(c) Enter the OTP



Your OTP is:710247

smileindira2603@gmail.... 18:27
to bcc: me

Fig 6.2(d) OTP and Image sent to mail


pi@Rahi: ~/NTC_036_FACE_ATM/ntc087_face
File Edit Tabs Help
OTP!
Enter your otp
OK
Cancel
Activate Windows
Go to PC settings to activate Windows.

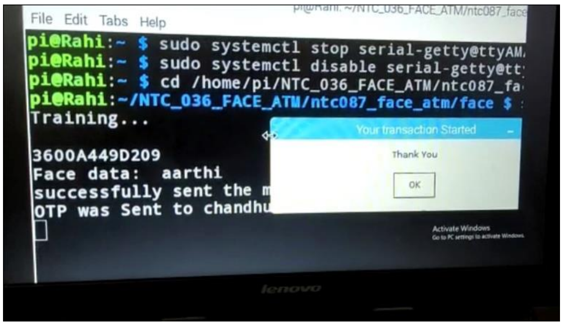
710247

```
pi@Rahi:~ $ s
pi@Rahi:~ $ s
pi@Rahi:~ $ c
pi@Rahi:~/NTC
Training...

3600A449D209
Face data:  aarthi
successfully sent the mail
OTP was Sent to chandhu
```

Fig 6.2(e) Entering received OTP

Case 3:When face not matched and OTP is incorrect

On inserting the card (Figure 6.3(a)), face recognition started (Figure 6.3(b)), if the face recognised matches with the face in the card then transaction successful. If not matched it ask to enter the OTP (Figure 6.3(c)). An OTP along with the face is sent to the card holder's mail (Figure 6.3(d)). If the card holder knows the person, he can convey the OTP to the person. If the person enters the correct OTP (Figure 6.3(e)) then the transaction is successful otherwise the transaction is not successful (Figure 6.3(f)).


pi@Rahi: ~/NTC_036_FACE_ATM/ntc087_face
File Edit Tabs Help

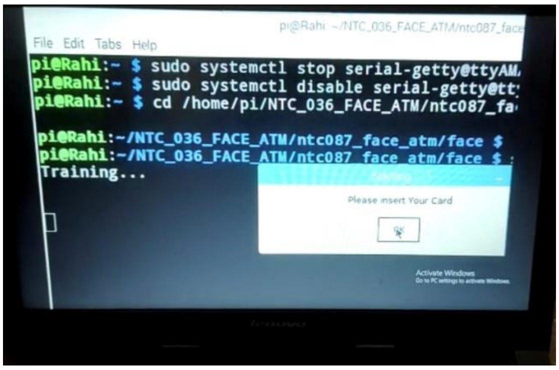
```
pi@Rahi:~ $ sudo systemctl stop serial-getty@ttyAM
pi@Rahi:~ $ sudo systemctl disable serial-getty@tt
pi@Rahi:~ $ cd /home/pi/NTC_036_FACE_ATM/ntc087_fa
pi@Rahi:~/NTC_036_FACE_ATM/ntc087_face_atm/face $
Training...

3600A449D209
Face data:  aarthi
successfully sent the m
OTP was Sent to chandhu
```

Your transaction Started

Thank You

OK
Activate Windows
Go to PC settings to activate Windows.
lenovo

Fig 6.2(f) Transaction successful

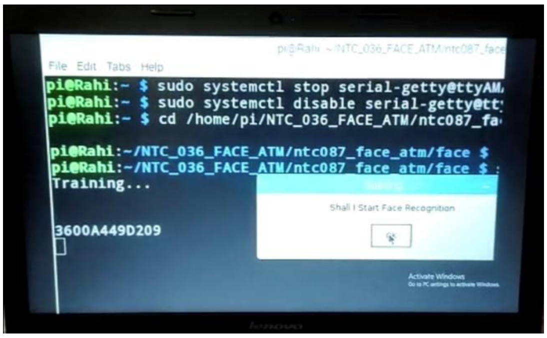

pi@Rahi: ~/NTC_036_FACE_ATM/ntc087_face
File Edit Tabs Help

```
pi@Rahi:~ $ sudo systemctl stop serial-getty@ttyAM
pi@Rahi:~ $ sudo systemctl disable serial-getty@tt
pi@Rahi:~ $ cd /home/pi/NTC_036_FACE_ATM/ntc087_fa

pi@Rahi:~/NTC_036_FACE_ATM/ntc087_face_atm/face $
pi@Rahi:~/NTC_036_FACE_ATM/ntc087_face_atm/face $
Training...
```

Please insert Your Card

OK
Activate Windows
Go to PC settings to activate Windows.
lenovo

Fig 6.3(a) Inserting the card

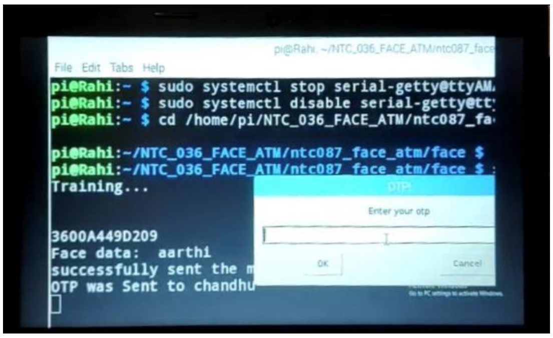

pi@Rahi: ~/NTC_036_FACE_ATM/ntc087_face
File Edit Tabs Help

```
pi@Rahi:~ $ sudo systemctl stop serial-getty@ttyAM
pi@Rahi:~ $ sudo systemctl disable serial-getty@tt
pi@Rahi:~ $ cd /home/pi/NTC_036_FACE_ATM/ntc087_fa

pi@Rahi:~/NTC_036_FACE_ATM/ntc087_face_atm/face $
pi@Rahi:~/NTC_036_FACE_ATM/ntc087_face_atm/face $
Training...


3600A449D209
```

Shall I Start Face Recognition

Activate Windows
Go to PC settings to activate Windows.
lenovo

Fig 6.3(b) Starting face recognition


pi@Rahi: ~/NTC_036_FACE_ATM/ntc087_face
File Edit Tabs Help

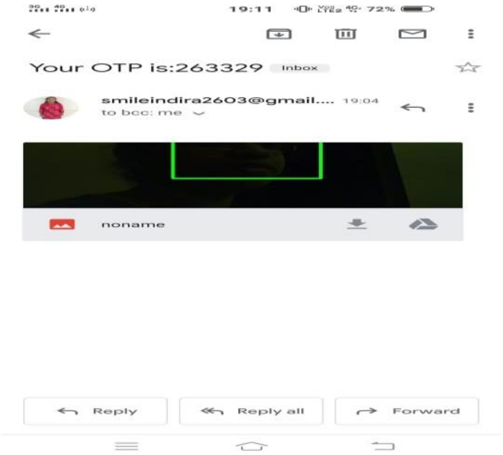
```
pi@Rahi:~ $ sudo systemctl stop serial-getty@ttyAM
pi@Rahi:~ $ sudo systemctl disable serial-getty@tt
pi@Rahi:~ $ cd /home/pi/NTC_036_FACE_ATM/ntc087_fa

pi@Rahi:~/NTC_036_FACE_ATM/ntc087_face_atm/face $
pi@Rahi:~/NTC_036_FACE_ATM/ntc087_face_atm/face $
Training...


3600A449D209
Face data:  aarthi
successfully sent the m
OTP was Sent to chandhu
```

OTP!

Enter your otp

OK
Cancel
Go to PC settings to activate Windows.

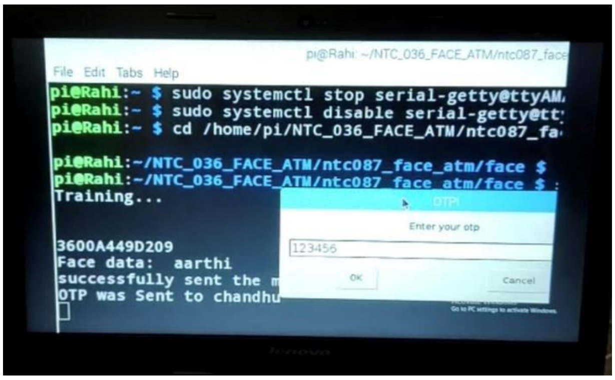
Fig 6.3(c) Enter the OTP



Your OTP is:263329

smileindira2603@gmail.... 19:04
to bcc: me

Fig 6.3(d) OTP and Image sent to mail



```
pi@Rahi:~ $ sudo systemctl stop serial-getty@ttyAM
pi@Rahi:~ $ sudo systemctl disable serial-getty@tt
pi@Rahi:~ $ cd /home/pi/NTC_036_FACE_ATM/ntc087_fa

pi@Rahi:~/NTC_036_FACE_ATM/ntc087_face_atm/face $
pi@Rahi:~/NTC_036_FACE_ATM/ntc087_face_atm/face $ :
Training...


3600A449D209
Face data:  aarthi
successfully sent the m
OTP was Sent to chandhu
```

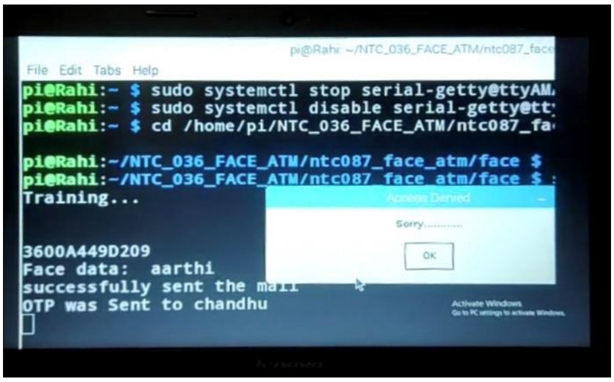
OTP!

Enter your otp

123456

pi@Rahi: ~/NTC_036_FACE_ATM/ntc087_face
File Edit Tabs Help
OK
Cancel
Go to PC settings to activate Windows.

Fig 6.3(e) Entering the received OTP



```
pi@Rahi:~ $ sudo systemctl stop serial-getty@ttyAM
pi@Rahi:~ $ sudo systemctl disable serial-getty@tt
pi@Rahi:~ $ cd /home/pi/NTC_036_FACE_ATM/ntc087_fa

pi@Rahi:~/NTC_036_FACE_ATM/ntc087_face_atm/face $
pi@Rahi:~/NTC_036_FACE_ATM/ntc087_face_atm/face $ :
Training...


3600A449D209
Face data:  aarthi
successfully sent the mail
OTP was Sent to chandhu
```

Access Denied

Sorry............

pi@Rahi: ~/NTC_036_FACE_ATM/ntc087_face
File Edit Tabs Help
OK
Activate Windows
Go to PC settings to activate Windows.

Fig 6.3(f) Transaction failed

6. CONCLUSION AND FUTURE SCOPE

ATM model which provides security by using Facial verification software adding up facial recognition systems to the identity confirmation process used in ATMs can reduce forced transactions to a great extent and provide hard-secure authentication.

As facial recognition technique seems more challenging as compared to other biometrics, thus more efficient algorithm can be developed. The inability to detect face when beard and aging can be rectified and eliminated or reduced. Instead of face recognition retinal or iris recognition can be used if the cost is reduced.

7. REFERENCES

[1] R. Babaei, O. Molalapata and A. A. Pandor, Face Recognition Application for Automatic Teller Machines (ATM), in ICIKM, 3rd ed. vol.45, pp.211-216, 2012.

[2] Aru, O. Eze and I. Gozie, Facial Verification Technology for Use in ATM Transactions, in American Journal of Engineering Research (AJER), [Online] 2013, pp. 188-193.

[3] K. J. Peter, G. Nagarajan, G. G. S. Glory, V. V. S. Devi, S. Arguman and K. S. Kannan, Improving ATM Security via Face Recognition, in ICECT, Kanyakumari, 2011, vol.6, pp.373-376.

[4] Moshin Karovaliya, Saifali Karedia, Sharad Oza Enhanced Security for ATM Machine with Otp And Facial Recognition Features, 2015.

[5] Laurenz Wilskott, Jean-Marc Fellous, NorbertKruger, Christoph von der Malsburg, Face Recognition by Elastic Bunch Graph Matching., Chapter 11, pp,355-396, (1999) ISBN 0-8493-2055-0.

[6] T. Ahonen, B. Hadid and M. Pietikainen, Face Description with Local Binary Patterns: Application to Face Recognition, in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 28, pp. 2037-2041, Dec.2006.

[7] Rasib Khan, Ragib Hasan, and Jinfang Xu SEPIA: Secure-Pin-Authentication-As-A-Service For Atm Using Mobile And Wearable Devices, 2015.

[8] Dr.G. Ranjitham, Face Recognition and Fingerprint Based New Generation ATM, Volume 3, Issue 3, March – 2018 International Journal of Innovative Science and Research Technology.

[9] Denis, L., Krishnakumar, T., Karthikeyan, M., Sasipriya, S, “IOT based architecture for banking cash logistics and ATM operations with sensors based networks”, International Journal of Scientific and Technology Research, 9(2), pp. 2071-2076, Jan. 2020.

[10] Denis, L., Krishnakumar, T., Karthikeyan, M., Sasipriya, S, “Global ATM reconciliation error codes mapping for all OEM manufacturers with common codes for rectification and reconciliation", International Journal of Advanced Research in Engineering and Technology, 11(1), pp. 52-60, Jan. 2020.