

Face Detection and Recognition for Bank Transaction

Sudarshan Dumbre¹, Shamita Kulkarni², Devashree Deshpande³, Prof P.V.Mulmule⁴

Department of Electronics and Telecommunication
P.V.P.I.T Pune.

Abstract— There is a crucial need for improving security in banking region. With the birth of the Automatic Teller Machines, banking became a lot easier though with its own troubles of insecurity. Due to tremendous increase in the number of criminals and their activities, the ATM has become insecure. ATM systems today use no more than an access card and PIN for identity verification. An attempt is made for developing a system that integrates facial recognition technology into the identity verification process and use of RFID card for handling multiple accounts in same card with Raspberry pi controller. The development of such a system would serve to protect consumers and financial institutions alike from intruders and identity thieves. This paper proposes an automatic teller machine security model that would combine a RFID card, a PIN, and electronic facial recognition that will go as far as with holding the fraudsters' card. If this technology becomes widely used, faces would be protected as well as PINs. However, it obvious that manes biometric features cannot be replicated, this proposal will go a long way to solve the problem of Account safety making it possible for the actual account owner alone have access to his accounts. The combined biometric features approach is to serve the purpose both the identification and authentication.

Index Terms—ATM, Face Recognition, RFID, Raspberry pi, Security.

I. INTRODUCTION

Automated Teller Machines (ATMs) are increasingly used in banking operations to dispense cash with additional banking operations from deposits, checking current balance. It is the electronic machine generally found outside the bank to dispense the cash whenever personal coded card is inserted. There are many ways by which security of this ATM card is provided, out of which most important is biometrics.

Fake biometrics means by using the real images iris images captured from a printed paper and Fingerprint captured (from dummy finger) of human identification characteristics create the fake identities like fingerprint, iris on printed paper. Fake user first capture the original identities of the genuine user and then they make the fake sample for authentication but biometric system have more method to detect the fake users and that's why the biometric system is more secure, Because each person have their unique characteristics identification. Biometrics system is more secure than other security methods like password, PIN, or card and key. A Biometrics system measures the human characteristics so users do not need to remember passwords or PINs which can be forgotten or to carry cards or keys which can be stolen.

This paper proposes an automatic teller machine security model that would combine a RFID card, a PIN, and electronic facial recognition using Raspberry pi. 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 RFID tag number. Only when the face matches the user's face, there is PIN facility for double security and then only it is fully verified. Unique feature about the proposed system is that it manages multiple accounts in single card.

II. PREVIOUS WORK DONE

In paper [2], Olutola Fagbolu et. al. have proposed a more secured ATM with more secured feature of biometrics- facial recognition as PIN. Security is an indispensable issue in banking operations; with the advent of technology such as e-banking, mobile banking etc security has become an issue that needs utmost priority. Principal Component Analysis (PCA) are employed in face recognition system, it seeks to capture the variations in a collection of face images and use them to encode and compare images of individual faces by using statistical dimensionality reduction method to produce the optimal linear squares decomposition of a training set and eigen faces. Thus the research paper proposed a reliable ATM model which would prove beneficial to entire society and the declined confidence of the customers would be obliterated.

In paper [3] another approach of Face Recognition used to access Automated teller machines (ATMs) is proposed. ATMs are used for banking function like checking balance; withdraw money, changing pin numbers, etc. The ATM cards and pin numbers are used for security purpose. In this research work SIM card is used in place of ATM cards. In order to improve security the system first authenticate the person if he/she is recognized then it will ask the password of the account. The proposed system uses Spartan 3 FPGA board to control the system. One speaker is connected on the FPGA board which gives instructions to the user to access the account. If the person is not authenticated then the process is terminated and the output is show on FPGA board with the help of LEDs.

K.Naveen Reddy et. al., in paper [5] have proposed a novel software-based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. The objective of the proposed system is to enhance the security of biometric recognition frameworks, by adding liveness assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment. The proposed approach presents a very low degree of complexity, which makes it suitable for real-time applications, using 25 general image quality features extracted from one image (i.e., the same acquired for authentication purposes) to distinguish between legitimate and impostor samples.

III. PROPOSED SYSTEM

The proposed system consist Raspberry Pi, camera, RFID card (Tag and reader), monitor. In this system, when a user is trying to make any transaction firstly it will detect face and recognize whether the user is fake or not by matching the face stored in database. Once the face is recognized, further process is carried out which includes Pin authentication and further transactions.

The card used in proposed system is not a regular magnetic strip card but a RFID card and reader (EM18). Thus for pin authentication it will have to match the tag's number first and then enter the code. This measure is taken to avoid frauds. One thing by which the proposed system stands out or is unique as compared to other systems is that it can manage the functions of Multiple Banks.

For Multiple bank transaction, RFID number and database will remain same for the security purpose. After the PIN is entered there will be separate transactions for each bank.

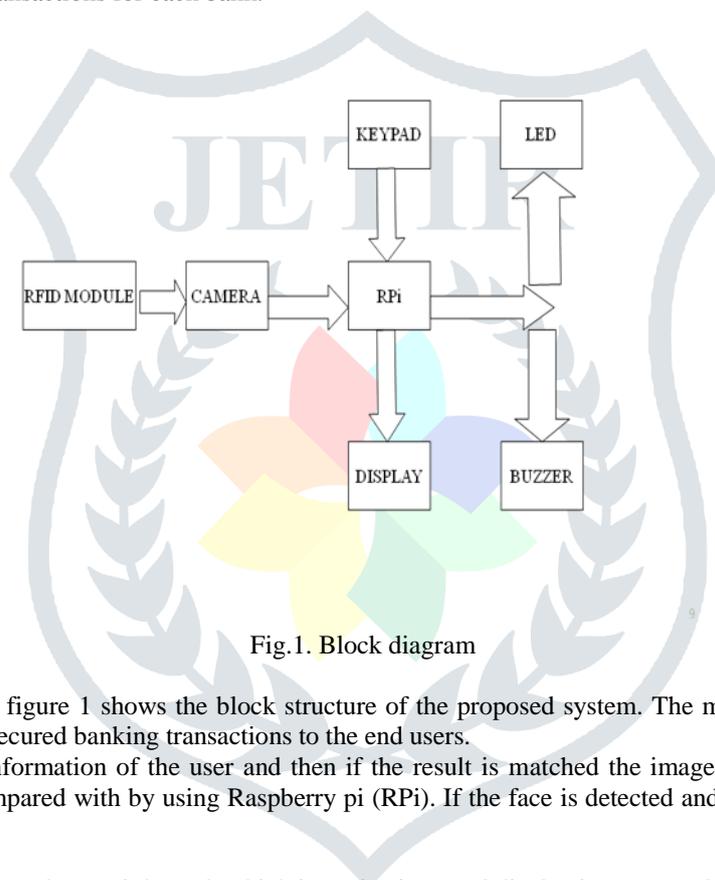


Fig.1. Block diagram

The above diagram in figure 1 shows the block structure of the proposed system. The main motive and objective of the proposed system is to provide secured banking transactions to the end users.

The RFID module scans the information of the user and then if the result is matched the image is captured through the camera which is pre-processed and compared with by using Raspberry pi (RPi). If the face is detected and recognized the LEDs will glow else buzzer will be on.

The keypad is connected to the raspberry pi through which input is given and display is connected to Raspberry pi on which output (i.e) name of banks will be displayed.

IV. WORKING OF SYSTEM

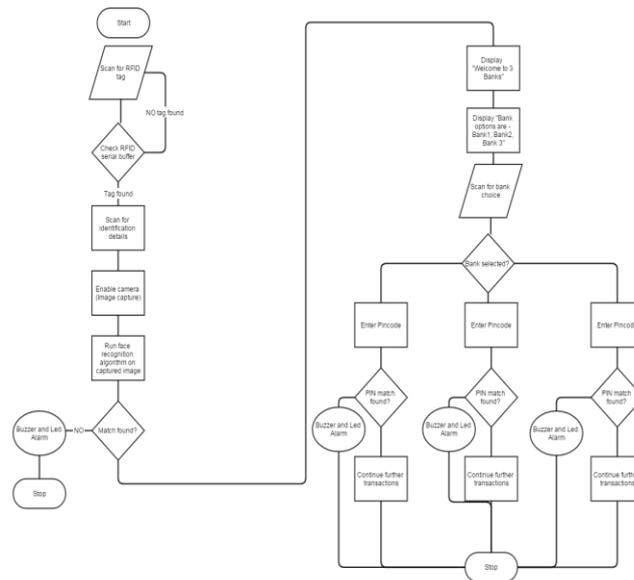


Fig.2. Flow chart

1. Face Recognition

Face recognition technology: Ideal for access control, financial transactions and ATM machines. The face key recognition technology performs the following tasks:

- a. Locates a moving object within the camera view
- b. Determines if the moving object is face
- c. Compares live faces with samples from database
- d. Face recognition technology can work with both low resolution USB
- e. 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.

2. RFID

Many types of RFID exist, but at the highest level, we can divide RFID devices into two classes: active and passive. Active tags require a power source they're either connected to a powered infrastructure or use energy stored in an integrated battery. In the latter case, a tag's lifetime is limited by the stored energy, balanced against the number of read operations the device must undergo.

3. RaspberryPi

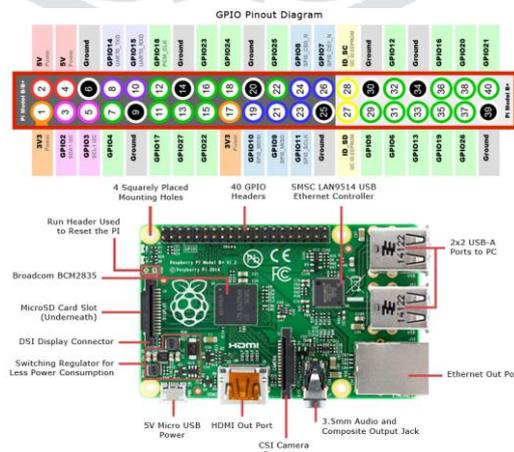


Fig. 3. Raspberry pi gpio configuration

It has Broadcom BCM2836 Arm7 Quad Core Processor powered Single Board Computer running at 900MHz,1GB RAM,40pin extended GPIO.It has CSI camera port for connecting the Raspberry Pi camera,DSI display port for connecting the Raspberry Pi touch screen display.

V. RESULTS



Fig. 4. Image above shows face recognition using raspberry pi.

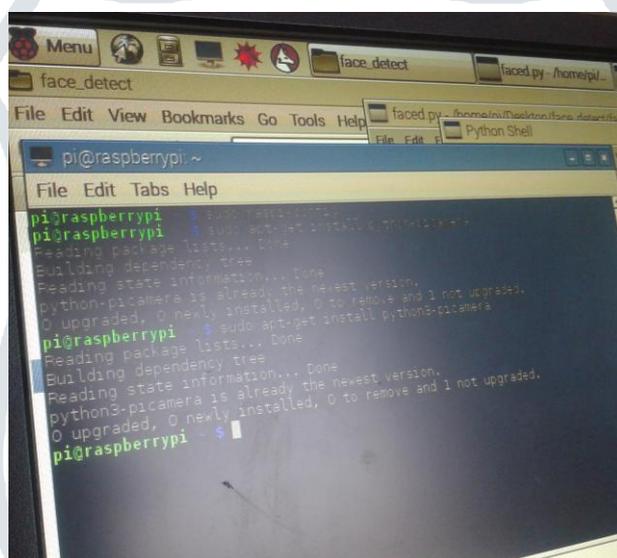


Fig. 5. Image above shows commands for face detection in python.



Fig. 6. Image above shows face detection and recognition process.

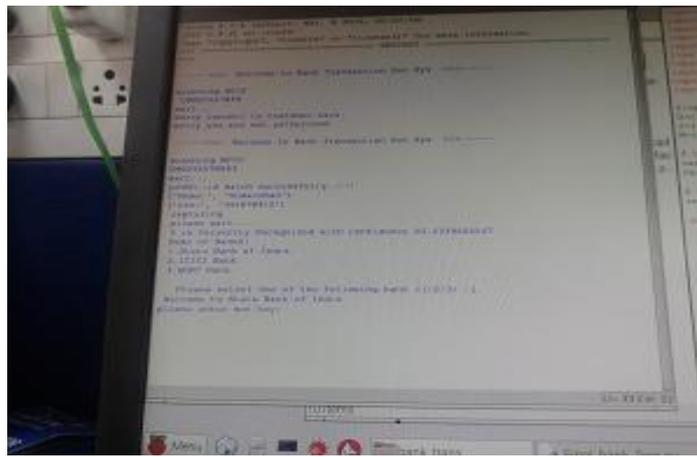


Fig. 7. Image above shows the verified user for bank transaction

VI. CONCLUSION

A single RFID card is very handy rather than different ATM card for multiple banks. An ATM model that is more reliable in providing security by using facial recognition approach is presented with conceptual framework for use of face based access control in ATMs. Also face detection technique avoids the threat of losing money even if the card is in wrong hand or lost. In this system the access to the ATM is provided in more secure manner. Any fraudulent access by the fake user is eliminated with the help of biometric techniques like face detection and recognition and radio frequency identification card. A significant advantage of RFID device is that it does not need to be positioned precisely relative to the scanner. The users face difficulty during use of credit cards and ATM cards as they must be swiped through a special reader. The proposed system based on RFID and facial recognition will be most secured approach for any kind of bank transaction. Crime at ATMs has become a nationwide issue that faces not only customers but bank also and hence need for security measures at banks must play critical contributory role in preventing attacks on customers which brought about the proposition of design of face based ATM. An ATM model that is more reliable in providing security by using facial recognition approach is presented with conceptual framework for use of face based access control in ATM's. In this system the access to the ATM is provided in more secure manner. Any fraudulent access by the fake user is eliminated with the help of biometric techniques like face detection and recognition and radio frequency identification card.

REFERENCES

- [1] H. T. Ngo, R. Gottumukkal, and V. K. Asari, "A flexible and efficient hardware architecture for real-time face recognition based on eigenface," in IEEE Computer Society Annual Symposium on VLSI, 2005.
- [2] Olutola Fagbolu , Olumide Adewale Boniface Alese and Osulale Festus, "Secured Banking operations with face-based Automated Teller Machine", IJSET, December 2014.
- [3] Prof Neelam S Khatkale, "Face Recognition Application in ATM Security", IJARCSSE 2015.
- [4] K Krishan Kumar Subudhi And Ramshankar Mishra, "Human Face Detection And Recognition", Department of Electronics and Communication Engineering National Institute of Technology, Rourkela.
- [5] Veerla Lakshmi Venkateswara Rao , Md.Jabirullah, K.Naveen Reddy, "High End Security Approach for Banking Transaction and Image Quality Assessment through Iris and Face Recognition", IJERA January 2015
- [6] Qiu Chen, Koji Kotani, Feifei Lee and Tadahiro Ohmi,"Face Recognition Using Self-Organizing Maps" - www.intechopen.com
- [7]Element14, www.raspberrypi.org,IEEE.com,adafruit.com.
- [8] RFID Reader Module-datasheet