Enhanced Cardless Transaction Using Biometric Atms

Geetha.A[1], Monesha B[2], Sandhya R[2], Sivashankari P[2]

[1]Assistant professor, [2]Undergraduate student

Department of Computer Science Engineering,

Easwari Engineering College, Chennai, India

geetha.vinodh1@gmail.com moneshasri@gmail.com sandhyagramesh@gmail.com psshankari1999@gmail.com

Abstract

Automated Teller Machines (ATM) are widely used now-a-days by people. These are electronic machines which are operated by customers to deposit or withdraw cash from banks. ATM provides services round the clock and is installed at convenient places including both onsite and offsite. In traditional ATM system card and pin numbers are used for authentication, where security plays a big concern such as losing cards, stolen pin numbers. In order to minimize these issues this paper discusses a system where ATM cards and pins are replaced by biometrics thus the combination of biometrics will be difficult to break the security. This process provides authentication for withdrawal of cash from ATM when the user's fingerprint and face recognition matches the collected datasets. In this system Raspberry pi microcontroller is used in the controlling part. It performs the search operation in the Database and sends necessary information to a display device. Open CV libraries are used for the method of recognition verification and identification of face images. Moreover to improve the efficiency of the system Haar Cascade is used.

Keywords: *Haarcascade, Raspberry pi, embedded system, sensor.*

1. INTRODUCTION

With the introduction of technology in the banking sector by introducing the ATMs and online banking, usage of credit and debit cards have increased throughout the world. Banks reduce their infrastructure costs by introducing Automatic Teller Machine(ATM) and Internet websites by which the customers' transactions will be carried out effortlessly. The customers will definitely prefer ATMs for all physical transaction purposes, like cash withdrawal and cash deposit without going to the bank. By the introduction of ATMs and online banking, the user experience has become a very important thing to be provided by the banks. But this may also lead to an increase in theft and attacks in ATM and online banking by various fraudulent methods. However the technological development in the Banking sector provides enhanced security to avoid fraudulent activities. In the present ATM system, debit cards and pin numbers are being used which has a higher possibility of being threatened. Thus the sole purpose of our paper is to lower these crimes by applying a user-friendly and safe method for accessing ATMs for all transaction purposes.

Haar Cascade is an object detection algorithm that is an efficient way for distinguishing objects in an image or in video .Raspberry pi 3 is a mini version of a computer which is user friendly and very compact in size. The Raspberry pi 3 holds the operating system, programs for compilation and running of a project also holds a document. This project discusses the secure transaction in ATMs with above kit - Raspberry pi which is used to operate the system.

2. RELATED WORKS

The works of various researchers and scholars are studied for survey and analyzing the advantages and drawbacks in order to improvise the system to function better.

Maninder et.al.,[1] proposes a system that uses either two fingers(thumb, middle) or three fingers(thumb, middle, ring) as input data, producing a unique identity by combining all the inputs. Matching result is produced from the minutiae formed from the combination. Fast Fourier Transform (FFT) is the technique used for the enhancement of image quality. Though this combination produces a unique identity which will not be easy to hack, the system may be difficult to implement since it leads to storage of all large amounts of data and leads to confusion between different finger details.

Abhijeet S. Kale et.al.,[2] proposes a system which uses an ARM Controller for both fingerprint and Aadhaar card verification. Initially both fingerprint and Aadhaar details of the customer are stored in a database. During a money transaction, both details are verified and when successful the customer gets authenticated.When fingerprint and Aadhaar card recognition doesn't match, a message is sent to higher authorities through GSM modem. This system is proposed as a measure to reduce fraudulent activities. But, since every personal detail of an individual are linked to an account, problems related to privacy issues needs to be figured out.

G.ReneeJebaline et.al.,[3] proposes a system which combines fingerprint recognition along with pin number. The first process includes the technique of Blowfish algorithm used for the encryption of the captured client's fingerprint. Minutiae is extracted from the fingerprint image, which involves techniques of Binarized fingerprint images and gray scale fingerprint images. The encrypted image is then decrypted through a secure network to the server. During the process, both images are compared and when successful, pin number authentication is carried out to fetch account details. The time of transaction is only 10 seconds and since encryption is performed it reduces power consumption but the issues in this system is that ATM pins can be easily guessed, stolen or misused and fingerprints can also be forged.

Yogesh.H.Dandawate et.al.,[4] proposes a system which captures two biometric traits-Fingerprint and Palm Vein. The first process involves feature extraction which includes fingerprint extraction using smoothing algorithm and palm vein extraction using curvelet transform. These features are then fused using normalization and augmentation technique. This proposed work is used for the authentication followed by a cash transaction. The palm biometrics is opted as a good identifying factor and the multimodal system is opted for greater security. However, this system leads to more processing and execution time.

Rasib Khan, et.al.,[5] proposes the system in which Secure PIN Authentication as a service(SEPIA) is used for authentication of PIN for ATMs which uses cloud connected personal mobile and wearable devices. The process gets initiated when the user touches the screen. This in turn is transmitted to the ATM server as a request message. A QR code gets generated and is transmitted to the ATM machine as a response. This QR code is scanned by user's wearable device like Google glass where the user location and details can be retrieved and the template of the PIN is generated in the ATM screen for the PIN to be extracted which is already sent to the users mobile phone for user to be authenticated for money transaction. SEPIA is more resistant to security attacks. However the wearable cannot be afforded by all and this also leads to problems for users wearing glasses or users with vision problems.

Sweta Singh et.al.,[6] proposes a system which uses pin number followed by fingerprint verification limited only for cash withdrawal which exceeds the daily cash limit by using the technique electronic data capture and constraint based biometric system. For balance enquiry and withdrawal of amounts which is less than the cash limit, only pin number verification is taken into account. While, when the user wants to withdraw an amount that exceeds the daily cash limit, fingerprint verification is carried out to reduce the working capability and accuracy of the system. It includes the advantage of reduction in the matching time during fingerprint verification. However, this system does not provide security for low cash withdrawal.

Joyce Soares et.al.,[7] proposes a system of using physiological biometrics such as fingerprint and iris recognition for ATM banking systems which replaces the use of cards and pins. This recognition system uses an algorithm of minutiae matching and a GUI based circular Hough transform. Thus this process is carried out in the form of verifying the fingerprint and the iris authentication of the genuine user and is verified with the collected datasets. When it gets matched, the user receives an One Time Password (OTP) in his phone. Withdrawal of cash is processed followed by above authentication. This system uses an embedded system which is user friendly and non invasive. But absence of the registered mobile phone at the point of transaction would become a disadvantage. Also, use of iris scanning technique is quite expensive.

G¨uneyKayım et.al.,[8] proposes a system in which when the card is inserted into the ATM, a session is initiated and the system starts appearance detection of the face and body with camera in the ATM and a short lived identity database is built for the user. When the card or cash is forgotten by the user and is left in the bank, instead of retracting the forgotten item ,the ATM waits for the user to retrieve it. If a different customer approaches the ATM, the item gets retracted instantly. For the behavioural recognition, Local Binary Pattern (LBP) operator and Support Vector Machines are used as classifiers. Though the system reduces the theft of cards, it doesn't provide a solution for forgetting pin numbers or cards.

Prakash Chandra Mondal et.al.,[9] proposes a system which uses behavioral biometrics for authentication with more security. In this system, authentication is performed using three factors which includes online handwriting signature verification, chip based card and PIN verification. This method does not involve the need for further enhancement like using physical biometrics (finger print, face images, etc.). However forging of signatures would become a threat to the user.

Sweedle Machado et.al.,[10] proposes a system that uses a fuzzy vault system for the security of ATM pins and passwords using a user's fingerprint data. It involves encryption and decryption. In the encryption process, the minutiae points gets extracted from the fingerprint which is encoded using pin password. While accessing the user's account the data encoded is decrypted using the same fingerprint impression to retrieve the pins and the passwords. The main advantage of this system is securing ATM pins and passwords with fingerprint data. However generating chaff points takes more time and forging of fingerprints may lead to revealing of all user pin details and data.

3. PROPOSED SYSTEM:

System architecture depicts the clear model of structure and behaviour of the system. The System architecture and Functional architecture of the proposed system are depicted in the following Figure 3.1 and Figure 3.2 respectively.

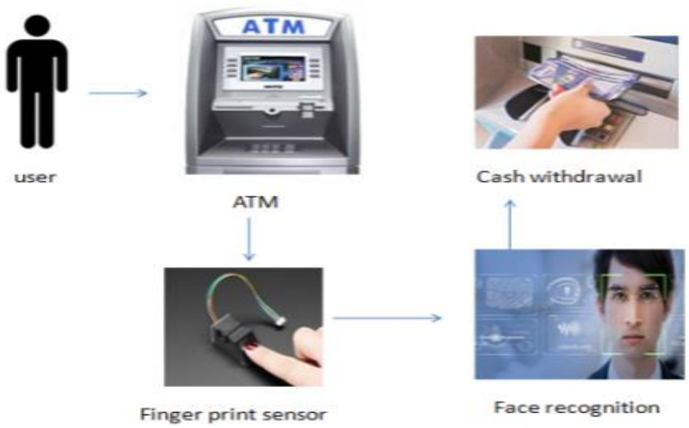


Figure 3.1 System Architecture

3.1 SYSTEM MODEL

A technology which uses the principle of matching patterns is used in the design of biometric based system. The various patterns may include an individual's particular physiological or behavioral traits. These traits are then matched, stored and then compared for the owner identity verification. The system includes both hardware and software components. Hardware section includes electronic kit, sensors, cameras, etc. to record the input data while the software section uses algorithms for security enhancement and generation of unique template ID for each individual as their own identity.

Figure 3.2 depicts the functional architecture which includes collection of fingerprint and face ID of each individual, then processed into training and test data which is later used while mapping for verification. The final process includes the notification of the amount withdrawn to the individual mobile number using the GSM technology. The system is composed of three modules: Fingerprint authentication, Face recognition and Notification

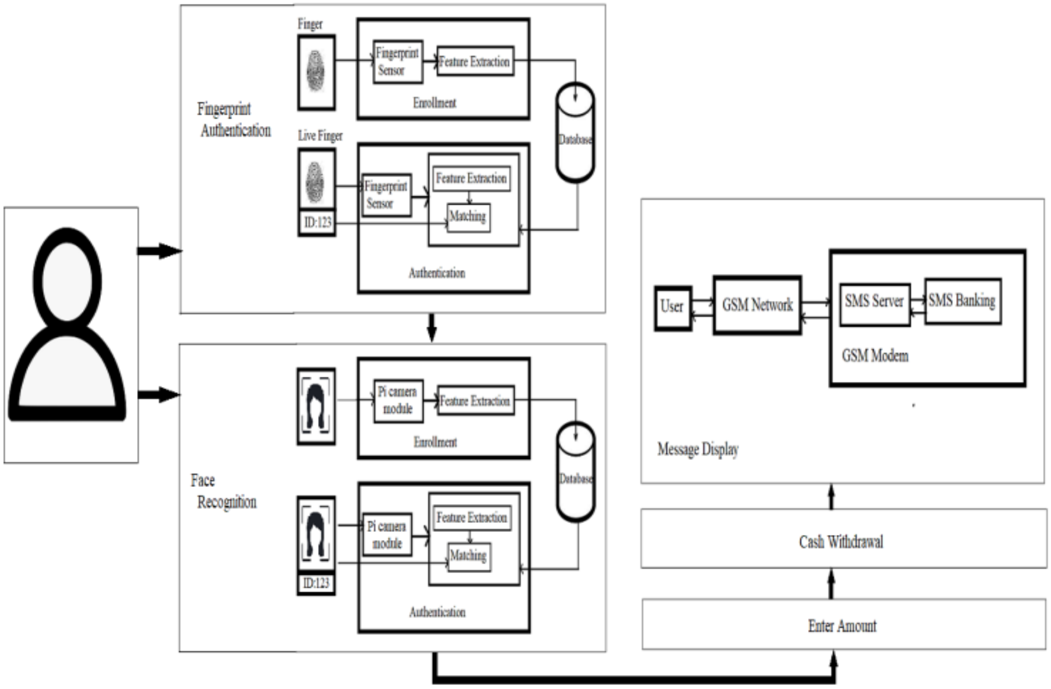


Figure 3.2 Functional architecture of proposed system

3.2 MODULAR DESIGN

The proposed system consists of the following modules

3.2.1 Fingerprint Authentication

This module makes use of an optical fingerprint sensor for the scanning process. An optical fingerprint scanner works based on the principle of Total Internal Reflection (TIR). In an optical fingerprint scanner, a glass prism is used to facilitate TIR. Light from an LED (usually blue color) is allowed to enter through one face of the prism at a certain angle for the TIR to occur. The reflected light exits the prism through the other face where a lens and an image sensor (essentially camera) are placed. When there's no finger on the prism, the light will be completely reflected off from the surface, producing a plain image in the image sensor. When we touch a glass surface, only the ridges make good contact with it. The valleys remain separated from the surface by air packets. Our skin and air have different Refractive Indexes (RI). This effect alters the intensities of the internally reflected light and is detected by the image sensor. The image sensor data is processed to produce a high contrast image which will be the digital version of the fingerprint.

Various advantages of fingerprint scanner includes they are highly unique and are secure. It is easier to setup and the time taken is also less. Fingerprint Scanner has high accuracy and hence used as an economical biometric user authentication technique. Space required for storage is also small and hence reduces the memory size of the database.

This module referred to in Figure 3.3 explains the Fingerprint Enrollment and Fingerprint Authentication process.

3.2.1.1 Fingerprint Enrollment

This process includes collection of each individual's unique fingerprint detail using a fingerprint scanner. This fingerprint is then saved in the form of character files for which a unique template ID is produced as an identity for the particular individual. The template is stored for the future verification of the individual for access into his/her account.

3.2.1.2 Fingerprint Authentication

After the successful enrollment, the individual should use the registered fingerprint for the login procedure. It is done by similarly scanning the same finger into the scanner. Now the character file gets generated for the current fingerprint and is stored using a template. This template is then matched with the template produced during the enrollment process. If the matching gets successful, then the individual gets authenticated and enters into the next process of face recognition.

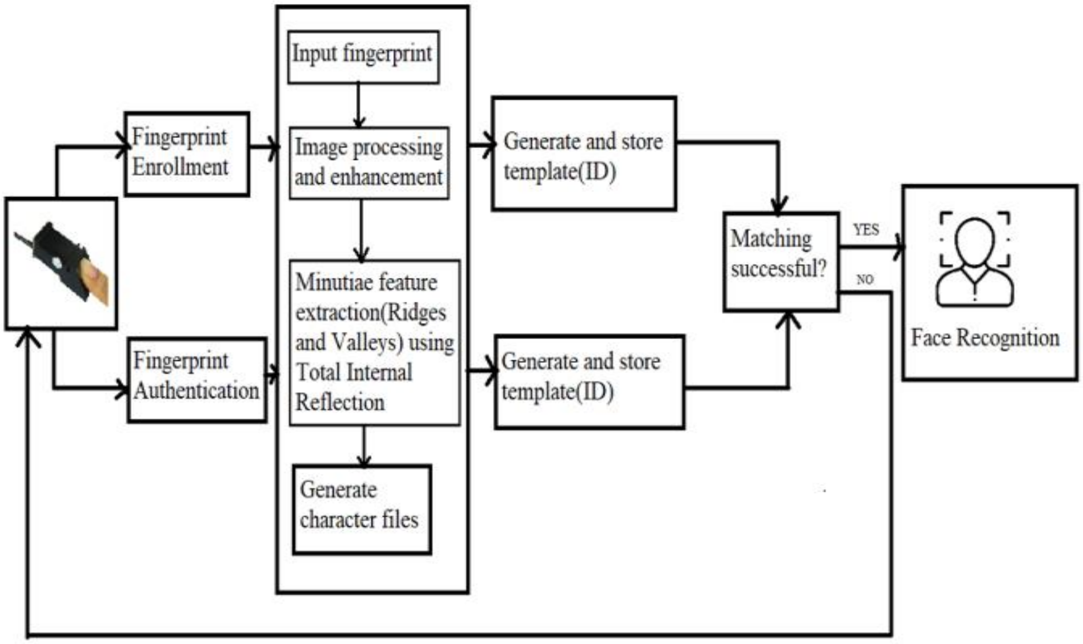

Fingerprint Enrollment
Fingerprint Authentication
Input fingerprint
Image processing and enhancement
Minutiae feature extraction(Ridges and Valleys) using Total Internal Reflection
Generate character files
Generate and store template(ID)
Generate and store template(ID)
Matching successful?
YES
NO
Face Recognition

Figure 3.3 Functional architecture of Fingerprint Authentication

3.2.2 FACE RECOGNITION

In face recognition, a camera is inserted in the raspberry pi which can capture the person's face and recognize it through certain processing stages. After the fingerprint authentication gets over, the second stage of face authentication of appropriate person gets verified. The process included here, records a number of images instructed in the program and are saved in the database. In the database there are file in the name of the person and their face record as an enrollment stage. And when the person needs to get authenticated they need to verify their face image to get authenticate. in this case ,during the authentication the image of the person get verified with no of images which are saved in their name in the database which is recorded during the enrollment .

The main advancement in using the raspberry kit is that it can be used anywhere in an ease manner. Here Opencv and Haar cascade are used in order to make the face recognition process in an efficient way. Opencv used to detect face of the user using the camera which is installed in the raspberry kit. In order to detect and recognize the user's face appropriately along with Opencv and Haar cascade technique is used to detect the required feature user's face. When using Haar cascade it makes the way for authentication in an clear way. Since these techniques are embedded in their own ways (in built characters) ,it makes sure that it only recognize the required features.

This module referred in Figure 3.3 explains the Face recognition system with OpenCV and Face Detection using Haar Cascade. Examples of face detection and face recognition are included below in figure 3.4 and 3.5.

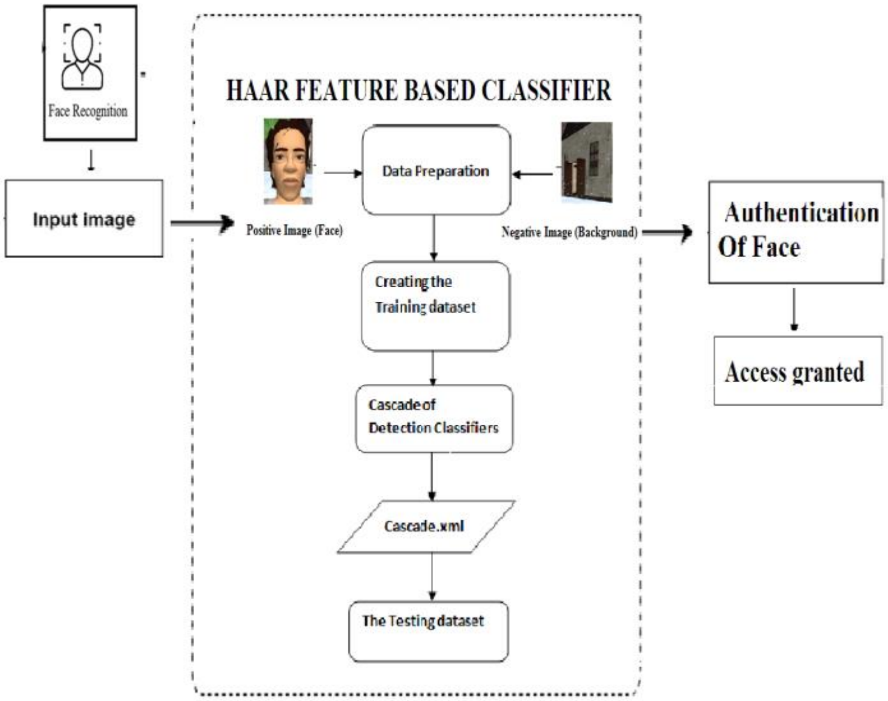
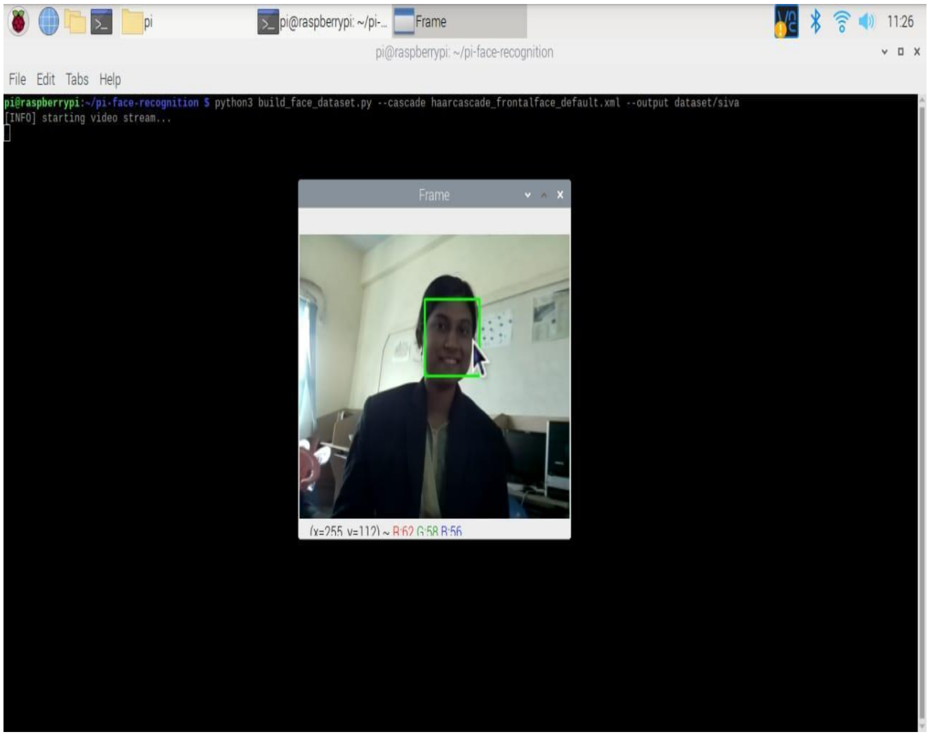


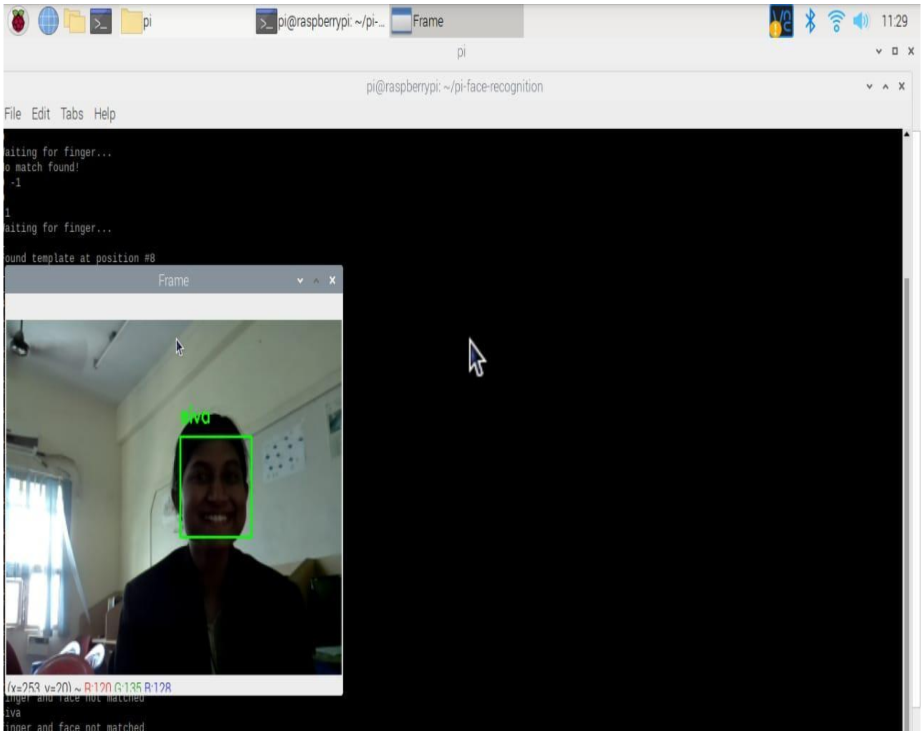
Figure 3.3 Functional architecture of Face Recognition



pi
pi@raspberrypi: ~/pi-...
Frame
11:26
pi@raspberrypi: ~/pi-face-recognition
File Edit Tabs Help
Frame
(x=255 y=112) ~ R:62 G:58 B:56

```
pi@raspberrypi:~/pi-face-recognition $ python3 build_face_dataset.py --cascade haarcascade_frontalface_default.xml --output dataset/siva
[INFO] starting video stream...
```

Figure 3.4 process of Face detection



pi
pi@raspberrypi: ~/pi-...
Frame
11:29
pi
pi@raspberrypi: ~/pi-face-recognition
File Edit Tabs Help
Frame
siva
(x=253 y=20) ~ R:120 G:135 B:128

```
aiting for finger...
o match found!
 -1

1
aiting for finger...

ound template at position #8
```

```
inger and face not matched
iva
inger and face not matched
```

Figure 3.5 process of Face recognition

3.2.3 NOTIFICATION

After the user has been validated and verified using their biometrics, the user enters the amount to be withdrawn in the ATM machine. Then the user successfully withdraws the cash from the ATM. As soon as the user withdraws cash, a message has been sent to the registered mobile number of the user as a way of notifying the user about their transaction through the GSM module .The system communicates to the registered mobile number of user through SMS which is sent through GSM module . This GSM module consists of a SIM card holder, GSM antenna and serial port. The SIM card is placed in the SIM card holder and it operates through a network. GSM module is a simple device which can be able to connect to the computer and to the system or microcontroller through a serial port. The notification message is sent to the registered mobile number of a user using the network through a SIM card which is attached to the GSM module.

The advantage of using this GSM technology is that it consumes less power. Thus messages to notify the user are automatically induced by the Bank server and sent to the registered mobile number of the user. This notification message consists of the details of the user, amount withdrawn and the balance in their account.

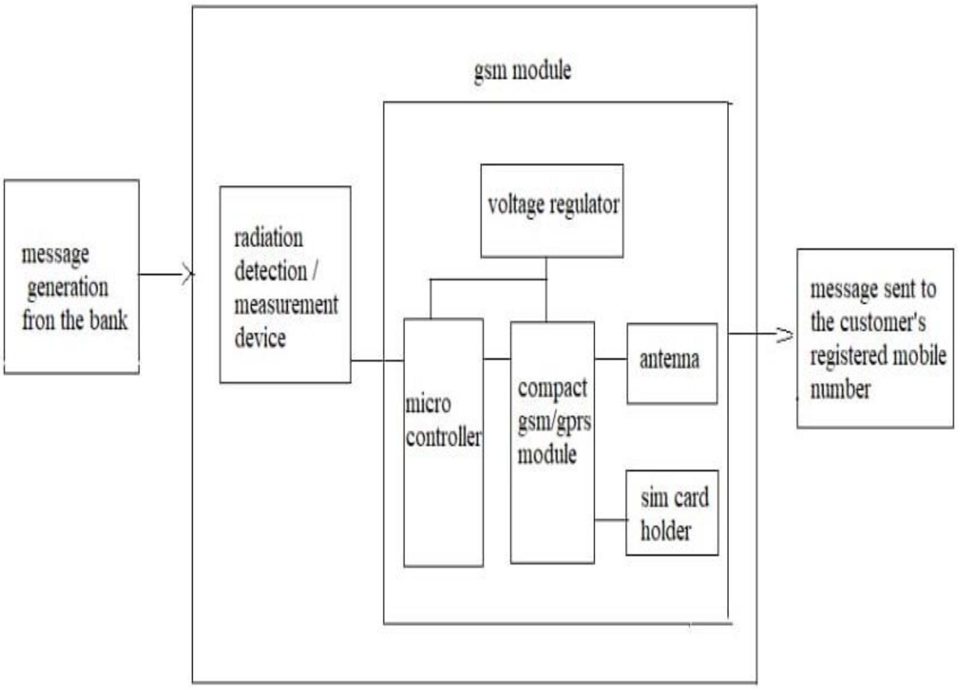

gsm module
message generation fron the bank
radiation detection / measurement device
voltage regulator
micro controller
compact gsm/gprs module
antenna
sim card holder
message sent to the customer's registered mobile number

Figure 3.6 Functional architecture of Notification

4. CONCLUSION AND FUTURE WORK

This method of biometrics ATM systems in the future will guarantee us by providing the advancement in technology and secure money transaction machine as well. In recent times the existing ATM systems racked up so many hackers and fraud towards the fraudulent activities such as pin pad overlays card skimming etc. these loopholes came into existence because of the insecure ATM systems. In this method two level authentication phases are used. One of the authentication include fingerprint scan followed by the face recognition system which grant access to the new ATM model when the data of the user stored in the database obtained during the enrollment stage get verified with the user who want to access the ATM. these procedure generates the secure and trustworthy money transaction machine for the user. Since nowadays every government systems gathers individual biometrics to verify the person. Thus from above procedure we conclude that biometric ATM can provide high level securities and efficient processing. This would be more efficient if we can include more upcoming technology and algorithms along with the above used algorithms

References

[1] ManinderSingh, ShahanazAyub, and Raghunat Verma,"Enhancing Security by averaging Multiple fingerprints",International Conference on Communication Systems and Network Technologies,2013.

[2] MrAbhijeet S Kale,Prof.Sunpreet Kaur Nanda.,"Design of Highly Secured Automated Teller MachineSystem by usingAadhaar card and Fingerprint",International Journal of Engineering Science Invention ,2014, Vol.3,no.5 pp:22-26.

[3] G.ReneeJebaline and S Gomathi, ''A Novel Method to Enhance Security of ATM using Biometrics", International Conference on Circuit, Power and ComputingTechnologies, 2015.

[4] Yogesh.Dandawate and Sajeeda. R Inamdar,"Fusion based Multimodal Biometric System", Conference on Industrial Instrumentation and Control College Of Engineering Pune, India.,2015.

[5] Rasib Khan, Ragib Hasan, and Jinfeng Xu,"SEPIA- Secure PIN Authentication as a service for ATM using Mobile and wearable devices' ', 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering , 2015.

[6] Sweta Singh, Akhilesh Singh, Rakesh Kumar," A Constraint based Biometric Scheme on ATM and Swiping Machine"International Conference on Computational Techniques in Information and Communication Technologies,2016.

[7] Joyce Soares, A.N.Gaikwad," Fingerprint and Iris Biometric Controlled Smart Banking Machine Embedded with GSM Technology for OTP", International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), 2016.

[8] G¨uneyKayım, Ekberjan Derman, Albert Ali Salah, "Short term Re identification of Automated Teller Machine User via Face and Body Appearance Features ",IEEE,2016.

[9] Prakash Chandra Mondal , Rupam Deb, Md. Nasim Adnan,"On Reinforcing Automated Teller Machine Transaction Authentication Security Process by imposing Behavioral Biometrics", International Conference on Advances in Electrical Engineering (ICAEE),2017.

[10] Sweedle Machado, PrajyotiD'silva, SnehalD'mello,SupriyaSolaskar and Priya Chaudhary,"Securing ATM pins and passwords using Fingerprint based Fuzzy Vault System", IEEE ,2018.