BAT for Facial recognition using sensors in ATM

Jaganiga M[1] , Vaitheswari S[2] , Rasitra R[3] , Dr.S.Lakshmi[4]

[1,2,3] Department of Information Technology, Jeppiaar SRR Engineering College, Tamil Nadu, India
[4] Professor, Department of Information Technology, Jeppiaar SRR Engineering College, Tamil Nadu, India

---***---

Abstract – *We aim to avoid the ATM robberies and wrong person misuse the ATM so that we can make them to lead their life safely and securely. The proposed system is designed based on the intelligence system to ensure the ATM usage without any hesitation and make the world to be a part of digitalization. Once customer inserts the card into the ATM, a session is initiated, the system starts face detection using the camera located near the ATM and builds a temporary identity database for the customer and user face verification is performed on the ATM .Valid user would continue the normal process but the Invalid user cannot be access the ATM card so they give the secondary password to the system automatically the unauthorized person would continue the transaction.*

KeyWords: Local Binary Pattern Histogram (LBPH), Face recognition, ATM, noise reduction

1. Introduction

We are all living in technical era, usage of systems played a key role in our daily life. Automatic Teller Machines (ATMs) are widely used due to its time independent nature. 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. In this work, we propose a more secured scheme in which the retraction rate of an ATM is decreased using face detection and recognition methods via ATM's built-in camera. Face recognition technology analyzes the unique shape, pattern and positioning of the facial features. Face recognition is very complex technology and is largely software based. This Biometric Methodology establishes the analysis framework with PCA algorithms for each type of biometric device. Face recognition starts with a picture, attempting to find a person in the image. This can be accomplished using several methods including movement, skin tones, or blurred human shapes.

Fisherface method is used for better recognition. This method scans the image pixel by pixel to analyze the boundary values of the image like the fishing net which has tiny boxes. IoT is an ecosystem of connected physical objects that are accessible through the internet. In existing system, the private information is traditionally provided by using passwords or Personal Identification Numbers (PINs), which are easy to implement but is vulnerable to the risk of exposure and being forgotten. Generally, the biometric systems are effectively used in various applications and some of the drawbacks are identified. Fingerprints are usually frayed; voice, signatures, hand shapes and iris images are easily forged. It is very difficult to identify the invalid ATM users and banks are not able to provide more security.

Literature survey

Automatic identification of a person based on his/her physiological or behavioural characteristics[2]. Security is provided by a customer by entering a personal identification number[3]. Pointed out that the lack of cooperation among banks in the fight to stem the incidence of the ATM related frauds in the industry[4].

2. The proposed system

The general working procedure of the proposed work is depicted in Fig.1.
The proposed work consists of the following modules:

1. **Image acquisition**: The ATM user once enter into the ATM, the person's image is captured and is depicted in Fig.2

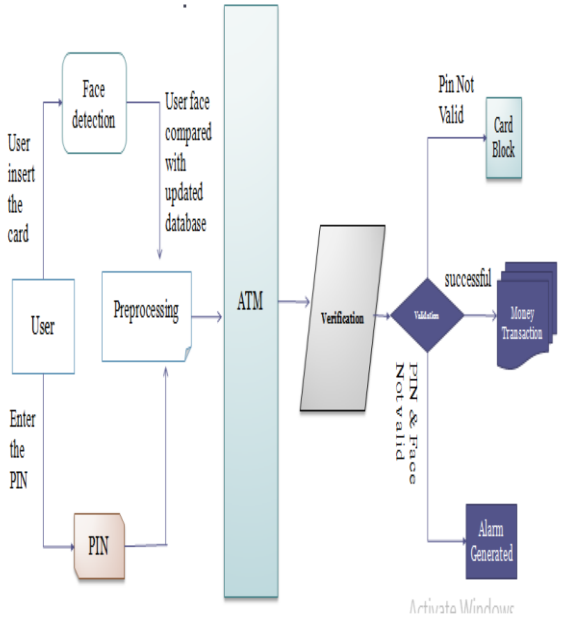


Fig.1. Work flow of Proposed system

Fig:2 A Image Acquisition

Fig.2 describes that the image is captured and the noise filters are reduced.

1.1 Noise reduction: There must be some unwanted information is added to any real world image pixels are eliminated before doing further processing.

1.2 By using histogram equalization technique, the contrast will be enhanced. This method usually increases the global contrast of many images, especially when the usable data of the image is represented by close contrast values.

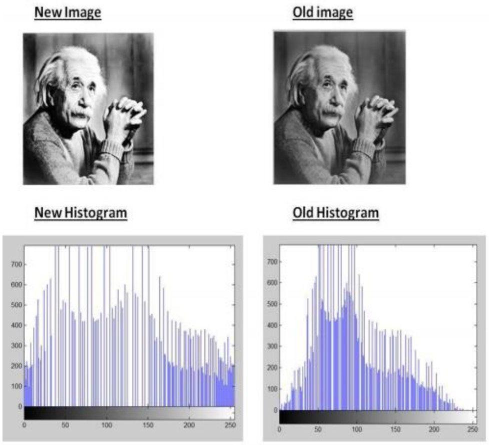


Fig.3 Sample Histogram equalization result

1.3 Through this adjustment, the intensities can be distributed on the histogram in a better way. This allows for areas of lower local contrast to gain a higher contrast. Histogram equalization accomplishes this by effectively spreading out the most frequent intensity values.

1.4 The user image is captured and then it is cropped using square shaped mask.

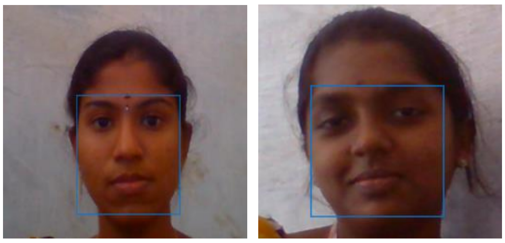


Fig:4 Crop the face

Fig.4 The image is cropped for further processing and to recognize the face.

2. This image is then compared with the image in the database. It also reduces the noise using filters like Gaussian smoothing filter in the 2D convolution operation which is used to remove noise and blur from image.

3. The proposed system consists of the secondary PIN for unauthorized person can access the card. ATM security model that would increase the performance that combines a physical access card, a PIN, and face recognition to increase the reliability of ATM transactions. Improve the ATM behavior in case of forgotten card or cash by re-identifying the user from an embedded ATM camera. Wrong person wearing visor /headdress will be unable to get the cash and the card will be blocked. Accuracy is high in this system.

4. Face Detection

Face detection is a computer technology being used in a variety of applications that identifies human faces in digital images. Face detection also refers to the psychological process by which humans locate and attend to faces in a visual scene. Face-detection algorithms focus on the detection of frontal human faces. The image of a person is matched bit by bit.

This module describes the whole face recognition and it matches to the updated images in the database. We proposed Local Binary Patterns Histograms (LBPH) on an FPGA-Based system on chip (SoC) using face recognition.

4.1 LBPH

Local Binary Pattern Histogram(LBPH) is constructed by comparing each pixel with its surrounding neighbor of pixels.

LBPH is the enhancement of Fisherface method.It is performed by taking a pixel as center and threshold as its neighbors against. If the intensity of the center pixel is greater-equal its neighbour, then denote it with 1 and 0 if not.
We will end up with a binary number for each pixel.

5 .Face Matching

Face matching is the method in which the user image is compared with the image in the database. The user's image features like iris,mouth,face have been scanned and matched with the image in the database. If the face is matched the user can be allowed to process the pin validation and is depicted in Fig.5.

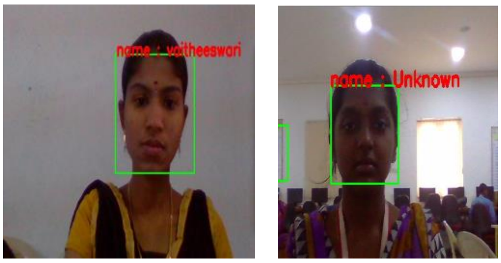


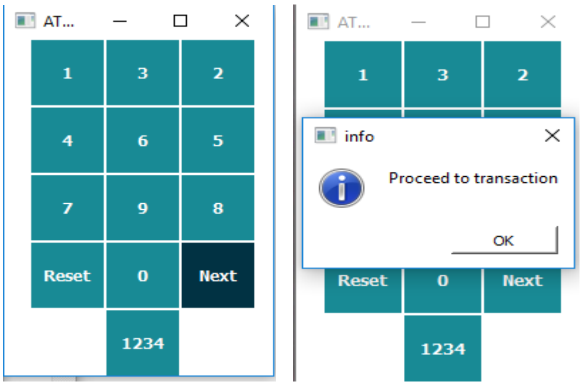
Fig.5 Face is matched

Fig.5 The face is matched with the image in the database and then proceeded for pin validation.

6. Pin validation

Virtual Keyboard

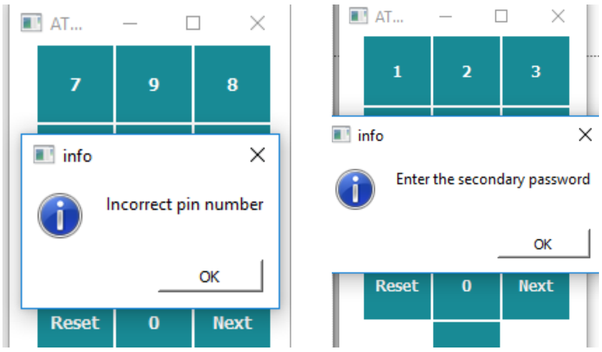
Physical keyboards with distinct keys comprising electronically changeable displays integrated in the keypads. Virtual keyboards with touch screen keyboard layouts or sensing areas. Optically protected keyboard layouts or similar arrangements of "keys" or sensing areas. Optically detected human hand and finger motions. Virtual keyboards to allow input from a variety of input devices, such as a computer mouse, switch or other assistive technology device.Online virtual keyboards for multiple languages that don't require OS settings change.



Proceed to transaction

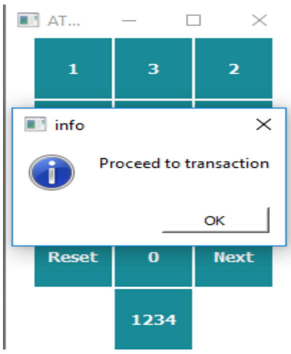
Fig.6 Valid user entering the PIN

Fig.6 describes that the valid user can enter the PIN and proceed the transaction.



Incorrect pin number

Enter the secondary password



Proceed to transaction

Fig.7 Invalid user entering wrong PIN

Fig.7 describes that the invalid user is entering the wrong PIN and then the secondary password is entered and then invalid user can proceed the transaction.

7. Security enhancement

However, ATM machines are becoming more complicated and they serve numerous functions, thus becoming a high priority target to robbers and hackers. If any user wears mask or helmet , that time the alarm will be raised to the near police station .The security measures has been enhanced using GSM and Arduino. Global system for mobile communication (GSM) is a globally accepted standard for digital cellular communication. GSM is used to generate the OTP message while the unauthorized user is accessing the card.

8. Conclusion

The security measures for ATM have been enhanced. A new secondary password has been introduced to provide more security for the ATM users. It is mainly generated to avoid fraudulent activities and theft detection. Already some measures are available for ATM security but we have introduced some features like identifying the valid or invalid user by face recognition, blocking the card for invalid user and the secondary password in case of emergency situations. More and more security is needed for the users. Thus we conclude that ATM security have been enhanced with new features and its implementation.

9. References

[1] Lusekelo Kibona,Face recognition as a biometric security for secondary password for ATM users , in Ruaha catholic university (RUCU),vol.1,2017.

[2] A.Jain L Hong and Pankanti,"Biometric Identification",Communication of the ACM,vol.43,pp,90-98,2000.

[3] A.S Adepoju and M.E Alhassan,"Challenges of Automatic Teller Machine(ATM) Usage of Fraud occurrences in Nigeria-A Case Study of selected Banks in Minna Metropolis".

[4] R.Ihejiahi ,"How to fight ATM fraud online,"Nigeria DailyNews,p-18,2009.

[5] E.Derman,Y.K.Gec,ici and A.A.Salah,Short Term Face Recognition for Automatic Teller Machine (ATM) Users, in ICECCO 2013, Istanbul, Turkey, pp.111-114.

[6] Ishan Bhardwaj, Narendra D.Londhe, Sunil K.Kopparapu, Study of the imposter attack on novel finger print dynamics based verification system, vol.5,2017.

[7] H. R. Babaei, O. Molalapata and A. A. Pandor, Face Recognition Application for Automatic Teller Machines (ATM), in ICIKAM, 3rd ed. vol.45, pp.211-216, 2016.

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