MAPLE TREE PUBLISHING HOUSE

INTERNATIONAL RESEARCH JOURNAL OF MULTIDISCIPLINARY TECHNOVATION (IRJMT)

http://www.mapletreejournals.com/index.php/IRJMT
Received 20 March 2019 ISSN 2582-1040
Accepted 23 March 2019 2019; 1(2); 106-110
Published online 25 March 2019

Enhanced Security for ATM Machine with OTP and Facial Recognition Features

Manikandan B[1*], Kishore R[2], Saran Kumar K[2], Suriya S[2], Vivek K V[2]

[1]*Assistant professor, Department of Information Technology, Hindusthan Institute of Tech, Coimbatore, TN, India*
[2]*UG Scholar, Department of Information Technology , Hindusthan Institute, Coimbatore, TN, India*

**Corresponding author E-Mail ID: mani_sari2003@yahoo.co.in, Mobile: +91 8072023275*

DOI: https://doi.org/10.34256/irjmt19215

ABSTRACT

The purpose of this paper is to reinforce security of the conventional ATM model. We have developed a new concept that enhances the overall experience, usability and convenience of the transaction at the ATM. Features like face recognition and One-Time Password (OTP) 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 completely eliminates the chances of fraud due to theft and duplicity of the ATM cards.

Keyword: Online Collaboration, Assessment, Course Discussion, Small Group Work, Collaborative Exams.

1. INTRODUCTION

With the technological advances in financial infrastructure, most bank customers prefer to use Automatic Teller Machines and Internet websites for carrying out their banking transactions. The main goal of our work is to propose a computer vision framework which uses the embedded ATM camera to perform face detection. First, the user will swipe the ATM card. A live image is captured automatically through a webcam installed on the ATM, which is compared with the images stored in the database. If it matches, an OTP will be sent to the corresponding registered mobile number. This randomly generated code has to be entered by the user in the text box. If the user correctly enters the OTP, the transaction can proceed. Therefore, the combination of face recognition algorithm and an OTP drastically reduces the chances of fraud plus frees a user from an extra burden of remembering complex passwords.

2. EXISTING SYSTEM

In the existing system, the user will swipe the ATM card. A live image is captured automatically through a webcam installed on the ATM, which is compared with the images stored in the database. If it matches, an OTP will be sent to the corresponding registered mobile number. The user will receive OTP immediately after passing the face recognition test. Once OTP is received, user has to enter the code which is of 6-digit.

User gets three chances to enter the code. If the code is entered incorrectly in three consecutive attempts account gets temporarily blocked and notification is sent to registered mobile number. This feature is added in order to restrict the fraudulent means of attacking the account of a user by wearing masks or in rare cases, if unauthorized user's face mistakenly matches authorized user's face.

3. PROPOSED SYSTEM

The proposed system is all about the emergency purposes. When the authenticated person wants USER(B) to take the cash instead of him from the ATM, The following process takes place. In this we have created a web page containing "Enter the email ID", the person will enter the ATM. The user will swipe the ATM card. The face will not recognize from the database, the image will be captured and OTP will be sent along to the email id in which we have given in the web page.

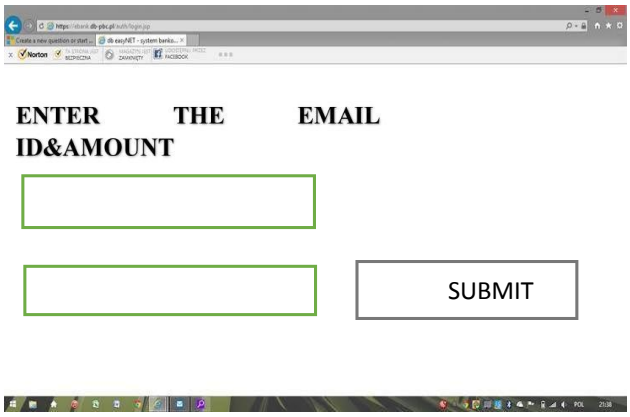

Fig 1. Entering the Email ID Amount

4. METHODOLOGY

4.1 Face detection and recognition

At this stage a user simply needs to look into the camera installed on ATM. If the user is recognized, then OTP is sent to user's mobile phone. We have seen thefts in ATM like the criminal entering into the room and forcing the user to access his or her account. To overcome this problem we have found a simple solution; if more than one faces are detected by the machine then the account gets temporarily locked. This additional feature is simple yet effective. Therefore, this system ensures that transaction proceeded only when user alone is accessing the machine.

In general, face recognition techniques can be divided into two groups based on the face representation they use.

4.1.1 Appearance-based

It uses holistic texture features and is applied to either entire face or only to the specific regions in face image. Principal Component Analysis (PCA), Independent Component Analysis (ICA) and Linear Discriminate Analysis (LDA) fall under this category.

4.1.2 Feature-based

It uses geometric facial features (mouth, eyes, nose, etc.) and geometric relationships between them. Our model uses Principal Component Analysis. To build Eigen faces, good data is required for component matching. The Eigen faces are ordered from largest to lowest, where the Eigen faces having larger eigenvalue finds greater variance as compared to those having less eigenvalue.

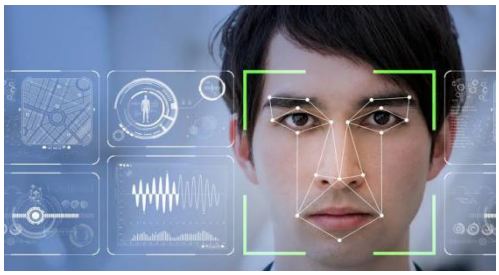

Fig 2. Face Recognition

4.1.3 The purpose of using PCA

Time taken for computation is very less as it considers only the essential components from images. Based on multiple face images as input, i.e. it considers multiple input images of each person with different expressions and under different lightening conditions. Demands less storage space for storing dataset. Smaller database representation since only the trainee images are stored in the form of their projections on a reduced basis. Reduced dimensions increase the efficiency of the process.

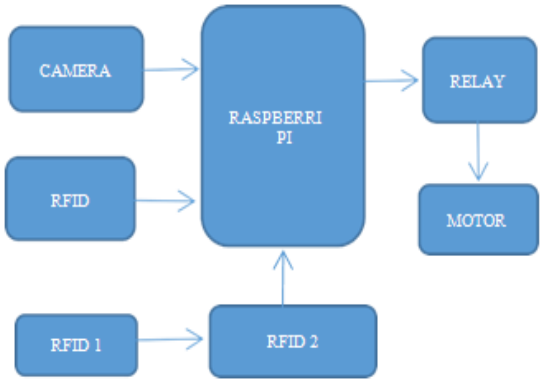

Fig 3. Architecture for ATM

5. IMPLEMENTATIONS

First, the user will swipe the ATM card. A live image is captured automatically through a web cam installed on the ATM, which is compared with the images stored in the database. If it matches with the database, a dialogue box displays As “Enter the Password”, the authenticated person can enter the password and make the transaction successful. When the person is in the emergency situation , if the person wants someone else to make the transaction, the following process is proceeded.

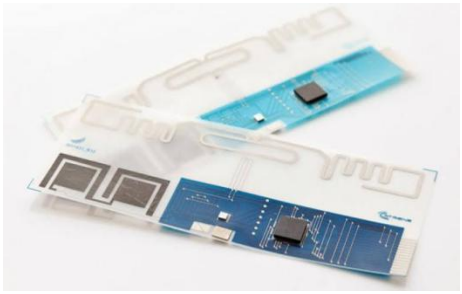

Fig 4. RFID TAG

Now USER(B) gets OTP number in his email id, so that if the USER(B) Enters the OTP number in the screen, he or she can make the transaction successful. Here instead of ATM card we are using RFID TAG.

Our proposed system's linear dependency of three phases, i.e. card requirement, face recognition and OTP plays a crucial role in preventing theft as explained below. If a thief creates a duplicate card to access a user account, the thief's face will not match with user's face. In+ rare cases, if the thief manages to match the user's face by using masks, then OTP will be sent to the user's registered number, which in turn will alert the user that someone is trying to access the account. Suppose if a user's mobile phone is stolen, the user can deactivate the phone number by contacting the service provider which will prevent OTP to reach the stolen phone which will help to prevent unauthorized access to the account.To break through these three phases, a thief needs to steal/duplicate cards, then match a user's face and then steal user's phone. Thus passing through this system is only possible if the user is careless to report a stolen/misplaced phone or stolen/misplaced ATM card to deactivate account.

Fig 5. Three phases

6. PROS AND CONS OF ENHANCED SECURITY FOR ATM MACHINE

The main advantage is Network is not dependent when the user is accessing the ATM The disadvantage in our project is ,In the proposed system the OTP generation depends on the network, if there is a proper network connection the OTP will be generated as soon as possible

7. FUTURE SCOPE

As we mentioned in the table , facial recognition technique seems more challenging as compared to other biometrics, thus more efficient algorithm can be developed. The flaws in face recognition technique like the inability to detect face when beard, aging, glasses and caps can be rectified and eliminated or reduced. If the cost of retina or iris recognition reduces, it can be used instead of face recognition

8. CONCLUSION

This project is still under development. The model shows the qualitative analysis of algorithms used based on the metrics of existing algorithms. According to the statistics PCA based face recognition is very accurate, requires less computation time and less storage space. After the completion of the project we will collect the quantitative aspects of the model and compare it with the qualitative results for further proof.

REFERENCES

[1] RupinderSaini,Narinder Rana,Rayat 'Comparison of various biometric methods', Institute of Engineering and IT, International Journal of Advances in Science and Technology (IJAST) Vol 2 Issue I

[2] Devinaga R, ATM risk management and controls. European journal of economic, finance and administrative sciences. ISSN 1450- 2275 issue 21

[3]Forouzan, Cryptography and Network Security, Tata McGraw Hill.

[4]Anil K. Jain and Arun Ross. Introduction to Biometrics. In Anil K. Jain, Patrick Flynn, and Arun. A. Ross, editors, Handbook of Biometrics, Springer US.

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

[6] Aru, O. Eze and I. Gozie, Facial Verification Technology for Use in ATM Transactions, in American Journal of Engineering Research (AJER), [Online].

Conflict of Interest

None of the authors have any conflicts of interest to declare.

About the License