Proceedings of the Fifth International Conference on Intelligent Computing and Control Systems (ICICCS 2021)
IEEE Xplore Part Number: CFP21K74-ART; ISBN: 978-0-7381-1327-2

ENHANCED SECURITY FEATURE OF ATM'S THROUGH FACIAL RECOGNITION

Ms. SOUNDARI D V
Department of ECE
Sri Krishna College of Engineering and Technology
Coimbatore, India
soundaridv@skcet.ac.in

ARAVINDH R
Department of ECE
Sri Krishna College of Engineering and Technology
Coimbatore, India
aravindh10100@gmail.com

EDWIN RAJ K
Department of ECE
Sri Krishna College of Engineering and Technology
Coimbatore, India
mathaenggvdsr@gmail.com

ABISHEK S
Department of ECE
Sri Krishna College of Engineering and Technology
Coimbatore, India
abishek.srinivasan@gmail.com

2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS) | 978-1-6654-1272-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICICCS51141.2021.9432327

***Abstract*— Automated Teller Machines also known as ATM's are widely used nowadays by each and everyone. The ATM machine (Automated Teller Machine) is an electronic device that is used by the banks to perform banking tasks like withdrawal of money, transferring of money, and many to get many information about a user's bank account without the need to visit a bank. This System revolutionised the way of transactions. There were no long lines of queue in front of the bank for a simple withdrawal of money. The number of ATM's a bank has can be a factor in considering the strength of a bank. As there is increase in the number of ATM's, there is also increase in the fraudulent activities in the ATM. The main motivation of this project is to increase the security feature of the use of ATM. The current method uses static key (PIN) for security. The proposed method uses Face-id as a key incorporated with current method. The advantages can be found as that the face-id is unique for everybody; it cannot be used by anybody other than the user. For the implementation of the face-id scan, the machine learning and image processing algorithms (Eigenface algorithm) are used.**

Keywords—ATM, Face-id, Eigenface algorithm, Machine Learning.

I. INTRODUCTION

Nowadays, the uses of ATMs are inevitable in our day-to-day lives. Before the introduction of ATM, people used to travel with cash in their hands. This caused the risk of getting robbed or the cash might get lost due to the negligence of the user. To overcome this issues ATM played a big role. It is like cash in a card. As the ATM technology got improved the idea of mis-using it also got improved. The main disadvantage of this system is that if the PIN is known anybody can use it to take money.

To address this issue, Face-id is used as a key. The main use of the Biometric is that it is unique for a person. The proposed innovation is not an alternative for the conventional ATM security system. The proposed innovation is considered as an additional support for the existing method. In India, nearly 2000 ATM crimes are occurring every year. The proposed method will surely reduce this rate to a greater extent.

II. Related work

Mohsin Karovaliya in paper [2] proposes Eigenface based method for the face recognition. This system analyzes the algorithms used in the previous systems. PCA based algorithm is more reliable, very fast and the storage space takes is very less. The main drawback this method is that it can be manipulated by using photos of users. This method can be improved by using 3D face masks but the cost of making 3D masks is very high.

The paper [3] suggests a vibration sensor which senses vibrations produced from ATM machine whenever robbery occurs. This system processes real-time data collected by the vibration sensor using an ARM controller-based embedded system. The buzzer will emit a beep sound once the vibration is detected. The ATM door is closed with a DC motor. There are also some additional security measures in place. This will deter theft and make it possible to arrest the suspect. Two software programs are used to execute the software, the first of which is Keil Vision 3.0. The Flash magic simulator is the second. Keil Vision Debugger correctly simulates on-chip peripherals. This device aids in rapid reaction and minimization of failure by detecting the ATM machine at real-time when it has been stolen can be identified by GSM technology.

In paper [4], the finger print recognition is done with curvelet transform by finding the Euclidean distance between the two corresponding finger codes. The test finger code is compared with the entire finger codes in the database. An OTP will be sent to the matching registered mobile number if it matches. The built-in MATLAB feature ‘imread' is used for preprocessing. The histogram equalization approach improves an image's global contrast by shifting the intensity distribution on a histogram marginally. This helps low-contrast areas to achieve more contrast without affecting the overall contrast. This is achieved by histogram equalization, which essentially spreads out the most common strength values. Curvelet transform and FFT can also be used for function extraction.

The ATM security is enhanced by adding GSM module to generate OTP in paper [5]. Where there is a network issue with GSM technologies, this system uses Bluetooth to link to an ATM, which produces an OTP relation from the user's cell phone. Since no special subscription to an SMS service provider is needed, GSM modems can be a fast and easy way to get started with SMS. A GSM modem can also be a regular GSM phone with the required cable and software. A GSM modem may also be a regular GSM phone with the required cable and software driver to connect to a serial port or USB port.

III. Proposed Method

Most people use an ATM for a lot of purposes and in a lot of scenarios. The most common three scenarios are considered here and the solutions are found.

- The user as himself using the ATM machine.
- If the user is threatened by somebody to get money without the user’s willing.
- If the user’s friend uses the card of the user.

First of all, when a user enters the ATM, two choices are given. Whether the user comes with his card (Number 1) or if the user’s friend comes with the card (Number 2).

A. User uses the ATM by himself

When a user by himself uses the ATM machine, first the card must be inserted. Now a camera captures the image of the user. Now, the captured image is compared with the image stored in the database. If both the image is matched (Eigenface algorithm does the comparison part) then a successfully authenticated message is displayed. Now the user needs to enter the PIN. If the PIN entered is correct then further transactions can be done.

B. User is threatened by somebody

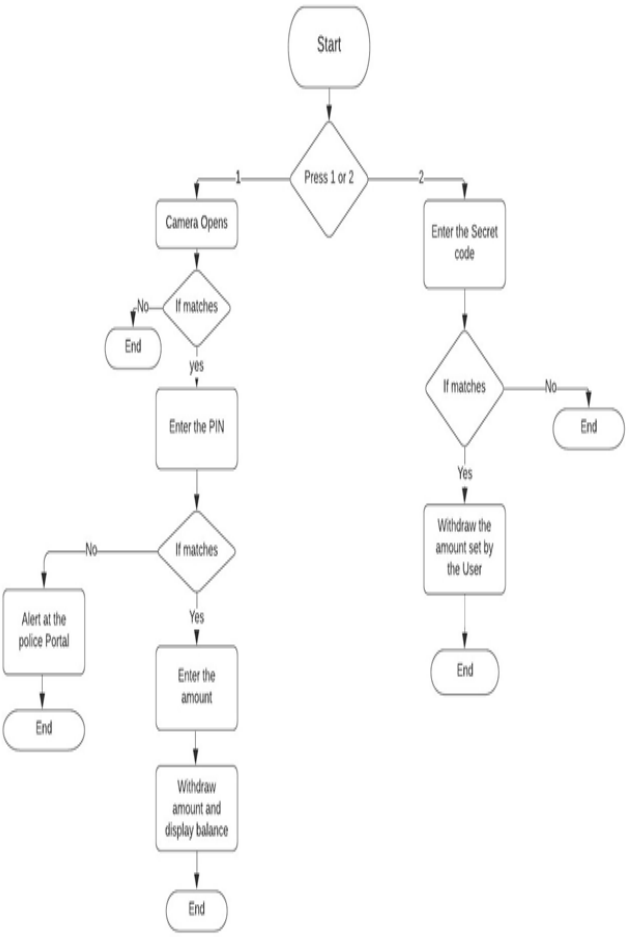
Now the user is threatened by somebody to get money. For this scenario we have a robust solution. First the face of the user will match. Now for entering the right PIN, the user must enter a wrong PIN. This causes a alert at the police portal which is at the backend. The police portal will be at idle stage if the transactions were smooth. If the wrong PIN is entered then the alert is received.

C. User’s friend user the card

When the user’s friend uses the card, obviously the face will not be matched. For this case, we proposed a clear method. The user should set a PIN and withdrawal limit in the mobile app. This must be set for each and every transaction. Now the user’s friend must

enter this secret PIN. If the PIN matches, then the amount set by the user will be automatically withdrawn.

Flowchart




```
user@user-HP-Laptop-15-da1xxx:~/Desktop/ATM$ python3 Main.py
ENTER 1 FOR FACE TRANSACTION
 ENTER 2 FOR OTHER TRANSACTION1
0
SUCESSFULLY AUTHENTICATED
ENTER THE pin:1234
edwin
ENTER THE AMOUNT TO TAKE:100
AMOUNT PROCESSED SUCESSFULLY
Your Balance amount is
4900
ENTER 1 FOR FACE TRANSACTION
 ENTER 2 FOR OTHER TRANSACTION
```

Result of csae1. The face is authenticated, The PIN is matched. Now the amount is entered. The process is done successfully.

Result of case 2:if the face is matched and the PIN is entered wrong then an alert is sent at the police terminal at the back end.

```
user@user-HP-Laptop-15-da1xxx:~/Desktop/ATM$ python3 Main.py
ENTER 1 FOR FACE TRANSACTION
 ENTER 2 FOR OTHER TRANSACTION2
ENTER SECRET PIN:4567
-500
processed Sucessfully
ENTER 1 FOR FACE TRANSACTION
 ENTER 2 FOR OTHER TRANSACTION
```

Result of case 3: If the users friend uses the card, Then the PIN (set by the user) must be entered correctly After correct entry of the PIN amount is withdrawn.

DRAWBACKS OF THE EXISTING SYSTEM

- Anybody who knows the PIN can use the card for the transactions.
- Since the PIN is static it is easy for criminals to extract it from the users, through hacking or even through brute force applied to the person.
- Scanning the magnetic strip in the ATM cards will give the complete details of the card. This causes the duplication of the cards.
- Threatening people in front of ATM is done in some places and the security feature of PIN cannot be useful in these situations.

ADVANTAGES OF PROPOSED SYSTEM

- The proposed method uses a biometric, this increases the security feature of the existing system drastically.
- Since we use biometric it is unique for each and every individual.
- The condition of threatening the user is well addressed here, and this can result in the safety of the user and the user's money.
- The withdrawal limit is set if the user's friend uses the card. This helps the user to be in control of his account.
- Implementation of this method is easy, cheap, and efficient.

Biometrics	Performance	Accuracy	Cost
Iris	Medium	Medium	High
Fingerprint	High	Medium	Low
Retina	High	High	High

ALGORITHMS USED

Since we use face data as the key here. We use image processing algorithms here. The implementation is done using OpenCV in python which has built in image recognising algorithms. There algorithms are trained using machine learning. We use Eigenface Algorithm.

FACE RECOGNITION

Face recognition is an easy task for humans. Seeing the geometric features of the face is considered as the most easy and efficient way in facial recognition. On early days the first automatic face recognition uses the marker points like position of ears, position of nose etc. These points were used in framing the feature vector like distance between them or angle between them. The facial recognition process was done by finding the distance between the feature vector of the captured image with a reference image. Some of the latest work on geometric face recognition was, a 22-dimensional feature vector and experiments on large datasets have shown that geometrical features alone may not carry enough information for face recognition.

Mainly Computer coding facial recognition can be broken down into three simple stages that are identical to the steps used by the human brain to recognize faces. These are the steps:

(1) Data Collection: Gather face data (in this case, face images) of the individuals you want to recognize.

(2) Train the Recognizer: Feed the recognizer the face data as well as the names of each face so that it can remember.

(3) Recognition: Feed the face recognizer with new faces of certain individuals to see how it knows them.

OpenCV has two built-in face recognizers. The names of those face recognizers are: Eigenfaces and Fisher faces.

3.3.4 Eigenfaces Face Recognizer Algorithm

In this algorithm, a facial image is a point from a high-dimensional image space and a lower-dimensional representation is found, where classification becomes easy. The lower-dimensional subspace is found with Principal Component Analysis (PCA), which identifies the axes with maximum variance. While this kind of transformation is optimal from a reconstruction standpoint, it doesn't take any class labels into account. Imagine a situation where the variance is generated from external sources, let it be light. The axes with maximum variance do not necessarily contain any discriminative information at all, hence a classification becomes impossible.

The functioning of the algorithm is that it considers that not all parts of a face are important equally to recognize a face. Instead, the main feature like the shape of nose, ears, fore-head are used and considered how they vary from one another The main idea is to find the region with maximum difference. Let us consider that there will a drastic amount of variation will be there when we compare the region of eyes and nose. When multiple faces are to be compared, the comparison between the faces is done looking at the maximum variation among the faces, and they help to distinguish the faces. This is the process behind Eigenfaces recognizer. This recognizer works by looking at all the pictures that are used to train and extracts the key components that are considered to be relevant and ignores the other components. Those key components are called as Principal components and these functions as main source for the recognizer.

This face recognizer also maps the records of the face to the person whose record is that. So, when a new record needs to be added it follows the following process. The principal component is extracted first. The comparison process is done next with the images used to train. Find the image which matches the best. Now map the record with the person name. In eigenface recognizer the light acts as one of the important needs. Only with the help of light the, shadowed and illuminated parts of the face is found. These details are used to find an eigenface which are used to represent a face. The shadows and shapes of two eyes, a nose, a mouth is the most used parameter in facial recognition.

Image showing how the Eigenface algorithm works.

IV. Conclusion

On summing up, the method what we proposed is far better in increasing the security feature. The main goal of our paper is to incorporate the facial recognition feature along with the existing conventional method for the betterment of the user. The Eigenface algorithm used here is used for the comparing the face of the user with the face in the database. Machine learning is used to train (used in OpenCV inbuilt face recogniser) the face recogniser. The Adaboost face recognition algorithm has the success rate of 75% but the eigenface Algorithm produces the success rate of 80%.

The main limitation of this system is that it requires periodic maintenance of the cameras. Twins can be an exception in this system. In rare cases, photos can be used to bypass the security. The future scopes of this method are that the use of high-quality durable cameras. 3-d cameras can be used for the condition of twins and photo bypassing.

References

[1] J.J.Patoliya, M.M. Desai, "Face Detection based ATM Security System using Embedded Linux Platform ", *2nd International Conference for Convergence in Technology (I2CT)*, 2017.

[2] M.Karovaliyaa, S.Karediab, S.Ozac, Dr.D.R.Kalbande, "Enhanced security for ATM machine with OTP and Facial recognition features",*International Conference on Advanced Computing Technologies and Applications (ICACTA)*, 2015.

[3] [3]Sivakumar T. 1 , G. Askok 2 , k. S. Venuprathap, "Design and Implementation of Security Based ATM theft Monitoring system", *International Journal of Engineering Inventions*, Volume 3, Issue 1, 2013.

[4] [4]C. Bhosale, P. Dere, C. Jadhav, "ATM security using face and fingerprint recognition", *Interna- tional Journal of Research in Engineering, Technology and Science*, Volume VII, Special Issue, Feb 2017.

[5] [5]Manoj V , M. Sankar R , Sasipriya S , U. Devi E, Devika T , "Multi Authentication ATM Theft Prevention Using iBeacon", *International Research Journal of Engineering and Technology (IRJET)*.

[6] L. Wang,H. Ji, Y. Shi, " Face recognition using maximum local fisher discriminant analysis",18th IEEE International Conference on Image Processing, 2011

[7] K.Shailaja and Dr.B.Anuradha, "Effective Face Recognition using Deep Learning based Linear Discriminant Classification ", *IEEE International conference on Computational Interlligence and Computing Research,2016.*

[8] H. R. Babaei, O. Molalapata and A.H.Y Akbar Pandor, "Face Recognition Application for Au- tomatic Teller Machines (ATM)",International Conference on Information and Knowledge Management(ICIKM),2012.

[9] Chen, Joy Iong Zong. "Smart Security System for Suspicious Activity Detection in VolatileAreas." Journal of Information Technology 2, no. 01 (2020): 64-72.

[10] Suma, V. "Computer vision for human-machine interaction-review." Journal of trends inComputer Science and Smart technology (TCSST) 1, no. 02 (2019): 131-139.

[11] Face Recognition using Eigenface algorithm on Laptop camera by Rika Rosnelly, Mutiara S. Simanjuntak, Ade Clinton sitepu, Mulkan Azhari, Sandy Kosasi in 2020 8th International Conference on Cyber and IT service Management.

[12] Comparison of the performance of Eigen face and Fisher Face Algorithm in the face recognition process by Delpiah Wahyuningsih, Chanda Kirana, Rahmat Sulaiman, Hamidah, Triwanto in 2019 7th International Conference on Cyber and IT service Management(CITSM).

[13] Face Detection based ATM security system using embedded Linux platform Jignesh J. Patoliya, Miral M Desai in 2017 2nd International Conference for Convergence in Technology(I2CT).

[14] Real Time Facial Expression and emotion recognition using Eigenfaces, LBPH and Fisher Algorithms Shrayan Mukhopadhyay, Shilpu Sharma 2020 10th International Conference on cloud computing, Data Science and Engineering.

[15] Face recognition alert mechanism and idealness for monitoring user motion by Web Services C. Jayaprakash, V Maheshwari 2016 10th International Conference on Intelligent Systems and Control(ISCO).