Enhanced Security For ATM Machine With OTP And Facial Recognition Features

Benak Patel M P[1], Aparna[2]
[1, 2] Dept of Electronics and Telecommunication Engineering

Abstract- *The purpose of this research presented is to reinforce the security of the conventional ATM model. We have posited 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 the security of accounts and the privacy of users. Face recognition technology helps the machine to identify every user uniquely and thus, making face a key. This eliminates the chances of fraud due to the theft and duplicity of the ATM cards. Moreover, the randomly generated OTP frees the user from remembering PINs as OTP itself acts as a PIN. A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. The proposed research presented uses face recognition techniques for verification in ATM systems. For face recognition, there are two types of comparisons. The first is verification, this is where the system compares the given individual with who that individual says they are and gives a yes or no decision. The next one is identification; this is where the system compares the given individual to all the other individuals in the database and gives a ranked list of matches.*

Keywords- ATM, security, fraud, face recognition, OTP, LBPH

I. INTRODUCTION

Due to rapid development in science and technology, upcoming innovations are being built-up with strong security. But on the other hand, threats are also being posed to destroy this security level. Though enhancement in automation has made a positive impact overall, various financial institutions like banks and applications like ATMs are still subjected to thefts and fraud. The existing ATM model uses a card and a PIN which gives rise to an increase in attacks in the form of stolen cards, or due to statically assigned PINs, duplicity of cards, and various other threats. To overcome these issues, a hybrid model which consists of conventional features along with additional features like face recognition and one-time password (OTP) is used. The database holds information about a user's account details, images of his/her face, and a mobile number which will improve security to a large extent. First, 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. OTP 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 a face recognition algorithm and an OTP drastically reduces the chances of fraud plus frees a user from the extra burden of remembering complex passwords.

II. OVERVIEW

A. History

The debut of Automated Teller Machine (ATM) dates back to 1967. The first machine was installed in Barclays' Enfield Town in London. In Europe at that time, banks were already searching for ways to make cash withdrawal services to be made available to the general public after working hours. This is when John Shepherd-Barron thought about vending machines which sold chocolate bars and the idea struck as to why a similar mechanism wasn't being used to withdraw cash. This is the revolutionary idea that changed the face of retail banking. The Personal Identification Number (PIN) was introduced much later in 1970. James Goodfellow was the person behind the concept of a PIN which could be stored on cards. This was one of the most important moments in the history of ATMs since it meant that humans could be identified and verified by machines without the need for human intervention.

B. Existing Problems

In the recent past, banking frauds have been on a constant rise. The fraudsters aim at looting money through online banking methods and also target transactions via debit, credit, and ATM cards. ATM card frauds have been present since the time ATMs were invented but the number and types of fraud cases have increased drastically. Two things are required to access the account of an individual- a card issued by the bank and the PIN. Fake cards can then easily be created and funds can be withdrawn from the account of the unsuspecting individual. In such times it is essential to be well informed about such frauds and dedicate the research towards

overcoming these problems. There are various types of frauds such as –

i. Card Skimming

This is one of the most popular and common techniques. Skimming essentially refers to stealing or duplicity of the data present in the electronic card which ultimately enables the criminal to forge the ATM card. During this process, the customer can use their card normally and won't be notified of any suspicious activity till the time the amount has been withdrawn and the account has been defrauded. Here the card details are stolen by placing a foreign device in the ATM. The PIN is also then captured and eventually, the card is closed.

ii. Eavesdropping

Similar to its contextual meaning, eavesdropping is a technique via which the card data is stolen by a foreign device placed by the criminal on the card. This can be achieved via methods like wire trap, reading the card reader functionality, or having a magnetic reader installed within the reader. The principle of this method is the use of proper card reading functionality.

iii. Cash shimming

In the Card Shimming method, the data is targeted which is present on the chip of the ATM card. Here, foreign material is placed between the ATM card and the card reader present in the ATM. By using this method, the fraudster can capture the data of multiple cards. Also, the attacks can be carried out in multiple ways like capturing the data equivalent magnetic strip or relay, etc.

C. Motivation

Keeping the above-mentioned problems in mind, we wanted to devise a solution that would enable customers to use their cards without any fear in a secure environment. This was the motivation behind this research presented. Some measures which have been included to boost the safety of ATM cards involve chip-enabled cards which are used to verify whether the card is fake or genuine. Other methods like NFC (Near field communication), have been implemented for debit and credit card purchasing methods but for ATM services such a method is still not available which is what motivated us to develop something which could omit the contact of the ATM card with the machine altogether. Many ideas have been proposed to solve the issues related to banking fraud. Biometric techniques have been a topic of research for a long time. This includes authentication using fingerprint sensors [1], voice and face [2] recognition, iris scanner [3], etc. In [4], the author has proposed the use of fingerprints to verify the identity of the user. The system requires that fingerprints be installed in all ATMs. In [5], the author proposes to provide a three-tier security system involving the use of NFC cards and OTP verification. Encryption techniques to provide a secure exchange of data over the cloud have been discussed in [7].

III. PROPOSED SYSTEM ALGORITHM

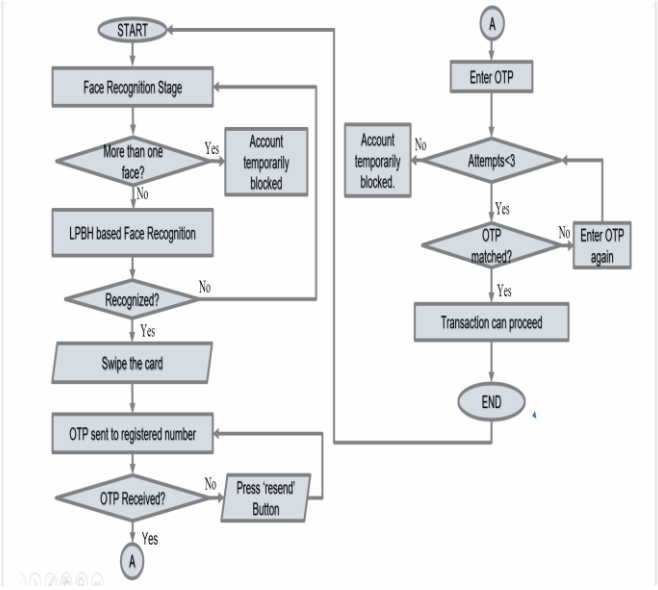

Fig. 1. Flowchart of Proposed System

IV. PROPOSED SYSTEM DESIGN

A. Block Diagram

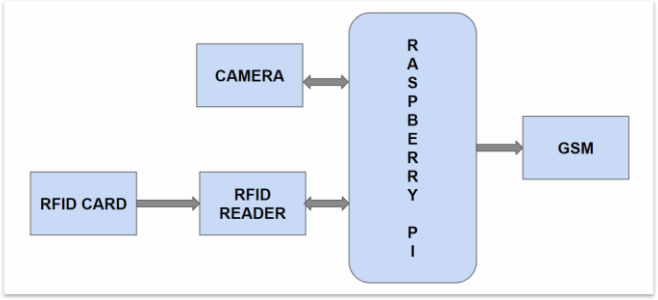

Fig. 2. Block Diagram of Proposed System

B. Working of Block Diagram

RFID stands for Radio Frequency Identification. RFID Reader is connected to the Raspberry Pi module. RFID Tag acts as an ATM card. Whenever some person shows an RFID tag to the RFID reader, the camera gets triggered and captures the image of that person. Once the camera captures

the image, it will send the captured image to the Raspberry Pi module.

Raspberry Pi is a small board having the ability to act as a controller. After receiving the captured image from the camera module, the Raspberry Pi module will compare the received image with the stored face image. First, we will capture the images to create the database for the Raspberry Pi module storage system.

After the database is created, we use this database to compare with the live captured face images. After comparing the images, the output of the Raspberry Pi module is considered Positive or Negative since it is a controller and the output is digital. Based on the output response, the Raspberry Pi module will send commands to the GSM module.

GSM stands for Global System for Mobile Communication. GSM is used to send the randomly generated OTP for registered mobile numbers after comparing the images and it is also based on whether the output of the Raspberry Pi module is Positive or Negative. If the output is Positive, then GSM will send OTP to the registered mobile number. Otherwise, the RFID reader needs to scan the RFID card once again. After receiving the OTP, the user needs to enter the OTP, and only when the OTP matches, the transaction will proceed otherwise denied.

C. Circuit Connection

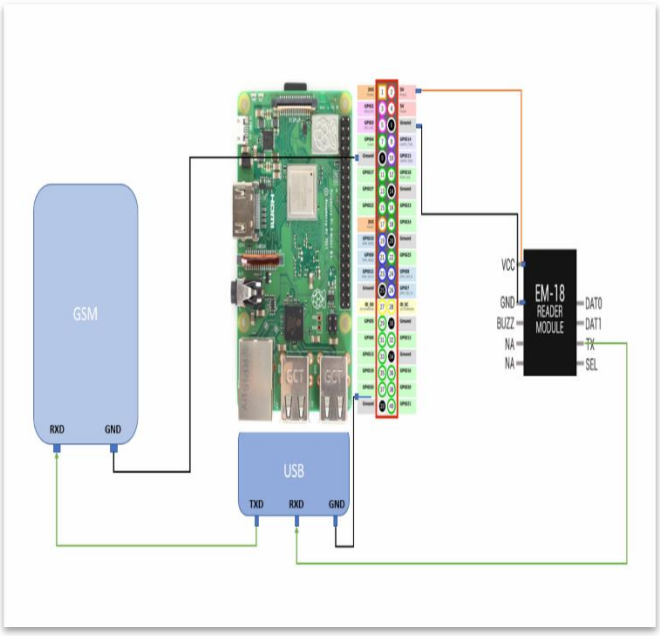

Fig. 3. Circuit Connection of Proposed System

V. IMPLEMENTATION

A. Face Recognition using LBPH

Local Binary Pattern (LBP) is a simple yet very efficient texture operator which labels the pixels of an image by thresholding the neighborhood of each pixel and considers the result as a binary number. It was first described in 1994 (LBP) and has since been found to be a powerful feature for texture classification. It has further been determined that when LBP is combined with histograms of oriented gradients (HOG) descriptors, it improves the detection performance considerably on some datasets. Using the LBP combined with histograms we can represent the face images with a simple data vector. As LBP is a visual descriptor it can also be used for face recognition tasks, as can be seen in the following step-by-step explanation.

STEP-BY-STEP PROCESS

1.Parameters: the LBPH uses 4 parameters:

- Radius: the radius is used to build the circular local binarypattern and represents the radius around the central pixel. It is usually set to 1.
- Neighbors: the number of sample points to build the circular local binary pattern. Keep in mind: the more sample points you include, the higher the computational cost. It is usually set to 8.
- Grid X: the number of cells in the horizontal direction. The more cells, the finer the grid, the higher the dimensionality of the resulting feature vector. It is usually set to 8.
- Grid Y: the number of cells in the vertical direction. The more cells, the finer the grid, the higher the dimensionality of the resulting feature vector. It is usually set to 8.

2.Training the Algorithm: First, we need to train the algorithm. To do so, we need to use a dataset with the facial images of the people we want to recognize. We need to also set an ID (it may be a number or the name of the person) for each image, so the algorithm will use this information to recognize an input image and give you an output. Images of the same person must have the same ID. With the training set already constructed, let's see the LBPH computational steps.

3.Applying the LBP operation: The first computational step of the LBPH is to create an intermediate image that describes the original image in a better way, by highlighting the facial characteristics. To do so, the algorithm uses a concept of a sliding window based on the parameters such as radius and neighbors.

The image below shows this procedure:

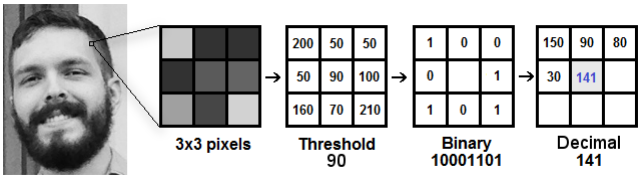

Fig.4. Application of LBPH Algorithm

4.Extracting the Histograms: Now, using the image generated in the last step, we can use the Grid X and Grid Y parameters to divide the image into multiple grids, as can be seen in the following image:

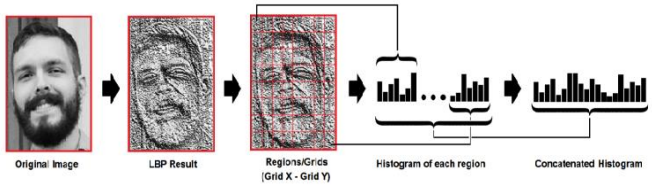

Fig.5. Extraction of Histograms

Based on the image above, we can extract the histogram of each region as follows:

As we have an image in grayscale, each histogram (from each grid) will containonly 256 positions (0~255) representing the occurrences of each pixel intensity.

Then, we need to concatenate each histogram to create a new and bigger histogram. Supposing we have 8x8 grids, we will have 8x8x256=16.384 positions in the final histogram. The final histogram represents the characteristics of the image original image.

3.Performing face recognition: In this step, the algorithm is already trained. Each histogram created is used to represent each image from the training dataset. So, given an input image, we perform the steps again for this new image and create a histogram that represents the image.

So, to find the image that matches the input image we just need to compare two histograms and return the image with the closest histogram.

We can use various approaches to compare the histograms (calculate the distance between two histograms), for example, Euclidean distance, chi-square, absolute value, etc. In this example, we can use the Euclidean distance (which is quite known) based on the following formula:

$$D = \sqrt{\sum_{i=1}^{n}(hist1_i - hist2_i)^2}$$

So, the algorithm output is the ID from the image with the closest histogram. The algorithm should also return the calculated distance, which can be used as a 'confidence' measurement. Note: don't be fooled about the 'confidence' name, as lower confidences are better because it means the distance between the two histograms is closer.

We can then use a threshold and the 'confidence' to automatically estimate if the algorithm has correctly recognized the image. We can assume that the algorithm has successfully recognized if the confidence is lower than the threshold defined.

B. OTP Working

For implementing OTP, we will make use of a GSM modem to send SMS (an OTP) to the user's mobile number. The idea to use mobile phones is preferred over e-mail because the people in rural areas have simple phones which can receive text messages but have no internet connections and e-mail facilities. Since mobile phones are ubiquitous, we intend to use mobile phones so that everyone can take benefitfrom the new proposed system. The user will receive OTP immediately after passing the face recognition test. Once OTP is received user has to enter the code. The user gets three chances to enter the code. If the code is entered incorrectly in three consecutive attempts account gets temporarily blocked and a notification is sent to the registered mobile number. This feature is added to restrict the fraudulent means of attacking the account of a user by wearing masks or in rare cases if an unauthorized user's face mistakenly matches the authorized user's face.

VI. HOW THIS MODEL HELP TO PREVENT THEFT

Our proposed system's linear dependency is of three phases, i.e., card requirement, face recognition, and OTP play a crucial role in preventing theft as explained below:

1. If a thief creates a duplicate card to access a user account, the thief's face will not match with user's face.
2. 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.

3. 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 the 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 the account.

VII. RESULTS

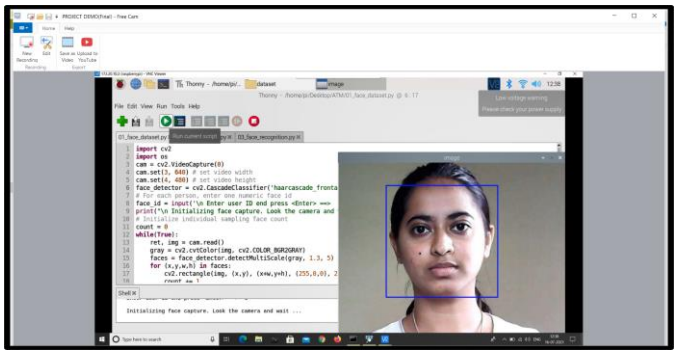

Fig. 6. Dataset Creation for User 1

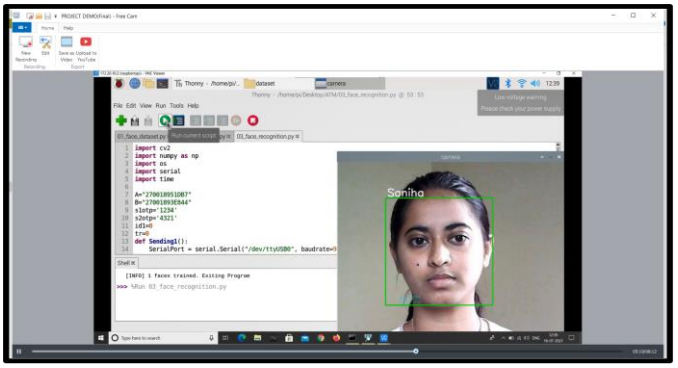

Fig. 7. Face Recognition of User 1

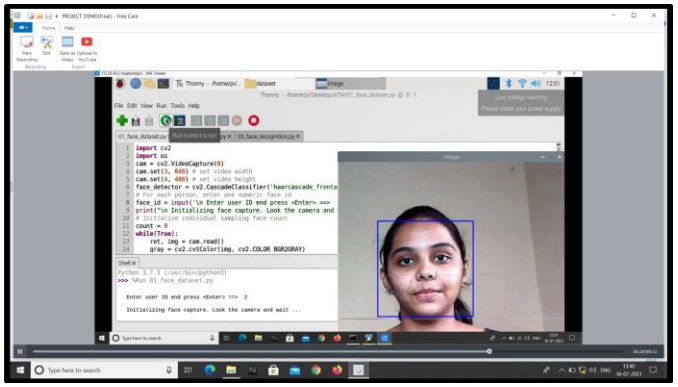

Fig. 8. Dataset Creation for User 2

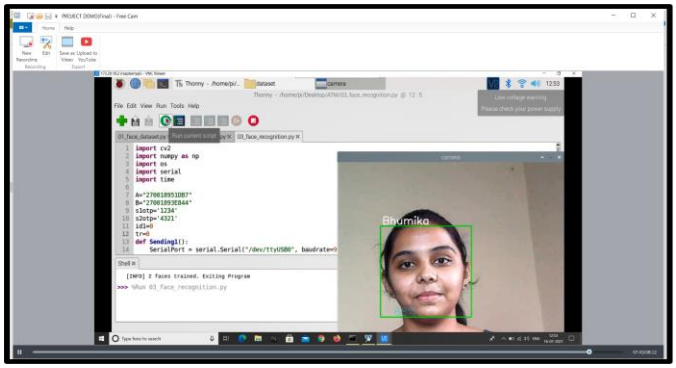

Fig. 9. Face Recognition for User 2

VIII. CONCLUSION

Reports of successful application of Face recognition algorithms, such as Local Binary Patterns Histograms (LBPH) algorithm, Fisherfaces and Speed Up Robust Features (SURF) have inspired the research presented in this paper.ATM security, a problem that has been formulated as an face recognition problem, has been approached through the LBPH algorithm here. A brief introduction to the Local Binary Patterns Histograms LBPH has been provided andstep by step process has been outlined. The model shows the qualitative analysis of algorithms used based on the metrics of existing algorithms.Results of LBPH face recognition have been presented and discussed briefly. The research presented here can be extended in many possible directions.According to the statistics, LBPH based face recognition is very accurate, requires less computation time and less storage space as trainee images are stored in the form of their projections on a reduced basis.

IX. FUTURE SCOPE

Facial recognition technology seems more challenging as compared to other biometrics, thus more efficient algorithms can be developed. The flaws in face recognition techniques like the inability to detect a 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.

X. ACKNOWLEDGMENT

Authors gratefully acknowledge the support received from J N N college of Engineering, Shimoga, India, and Project intern students of Electronics and Telecommunication Branch, J N N C E, Shimoga, India. They also express sincere thanks to the anonymous reviewers of this paper for their constructive criticism.

REFERENCES

[1] Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition," IEEE Transactions Circuits Systems. Video Technology, Vol. 14, No. 1, pp. 4–20, 2004.

[2] Y. Feng and P. Yuen, "Protecting face biometric data on smartcard with Reed–Solomon code," in Proc. CVPR Workshop Privacy Res.Vis., 2006.

[3] Y. Lee, K. Park, S. Lee, K. Bae and J. Kim, "A New method for Generating an Invariant Iris Private Key Based on the Fuzzy Vault System", IEEE Transactions On Systems, Man, And Cybernetics— Part B: Cybernetics, Vol. 38, No. 5, 2008, pp. 1304-1313.

[4] Abhinav Muley, Vivek Kute, "Prospective solution to bank card system Using fingerprint", Proceedings of the Second International Conference on Inventive Systems and Control (ICISC 2018)

[5] Anshuman Mohanty, Pranav Giria, Saptaswa Pal, Vishruthi K Acharya, "NFC Featured Triple Tier ATM Protection", 978-1-5386-5657- 0/18/$31.00 c 2019 IEEE

[6] Sweedle Machado , Prajyoti D'silva , Snehal D'mello , Supriya Solaskar , Priya Chaudhari, "Securing ATM pins and passwords using Fingerprint based Fuzzy Vault System" 978-1-5386-5257-2/18/$31.00 ©2019 IEEE

[7] Prachi More, Shubham Chandugade, Shaikh Mohammad Shafi Rafiq , Prof. Priya Pise, "Hybrid Encryption Techniques for Secure Sharing of a Sensitive Data for Banking Systems Over Cloud", 2019 International Conference On Advances in Communication and Computing Technology (ICACCT) Amrutvahini College of Engineering, Sangamner, Ahmednagar, India. Feb 8-9, 2019 Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[8] Khushboo Yadav, Suhani Mattas and Lipika Saini, "Secure Card-less ATM Transactions", University of Gothenburg -2020.

[9] Sameer Sheikh, Kunal Pawar, Pooja Bhondave, Sanyogita Borade, "Implementation of secured ATM by Wireless Password Transfer and keypad Shuffling.", International Research Journal of Engineering and Technology (IRJET-2019).

[10] R Mahendran and C Karthik, "The New Embedded ATM Security based on Machine Vision using MATLAB", International Journal of Innovative Research in Electrical, Instrumentation and Control Engineering Vol. 4, April 2016.

[11] Mohsin Karovaliya, Saifali Karedia, Sharad Oza and D.R Kalbande, "Enhanced security for ATM machine with OTP and Facial Recognition features.", International Conference on Advanced Computing Technologies and Applications Published (ICACTA-2015) by Elsevier B.V.