IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

Enhancing ATM Transaction Security Through Face Recognition

[1]Dr. Sudha Arvind, [2]Ankush Kumar Singh, [3]Baddam Sai Teja Reddy, [4]Gopiti Nithish Reddy, [5]Vadlakonda Vivek

[1]Associate Professor, [2]Student, [3]Student, [4]Student, [5]Student

[1]Department of Electronics and Communication Engineering

[1]CMR Technical Campus, Hyderabad, Telangana, India

***Abstract*—** Because of technological developments in financial facilities the majority of bank clients choose to conduct their banking transactions using Automatic Teller Machines (ATMs). To strengthen the security of these transactions, we proposed a new generation ATM in this paper. This works by using facial recognition technologies. The recognition technique considerably benefits from using high-quality photos in this case. A facial picture is used for authentication purposes. First, the face picture of a person is contrasted with the database image. If an unauthorised user is found, it will not allow to login. As a consequence, an ATM model that provides security using facial recognition devices may significantly reduce forced transactions and provide strong secure authentication. The Histogram algorithm method and Local Binary Pattern for face recognition is used in Python for providing security.

Index Terms **- ATM, face recognition technology, security, authentication, facial image, database image, unauthorized person, forced transactions, Histogram algorithm, Local Binary Pattern.**

I. INTRODUCTION

A financial institution's customers can conduct financial transactions, such as cash withdrawals, deposits, funds transfers, or account information inquiries, at any time and without having to speak with a bank employee directly using an automated teller machine (ATM). At the end of December 2019, there were 10,924 cash machine (ATM) booths in Bangladesh, with Tk 147.05 billion worth of cash being transacted through these machines overall in 2019[2]. To ensure that customers may perform their transections with the necessary safety, this constantly evolving technology necessitates a high level of security. create these components, incorporating the applicable criteria that follow. To guarantee secure ATM service for customers, physical security measures like CCTV coverage of the ATM booth and security guards (human) are already in place. Additional technology-based security measures like firewalls, data encryptions, network security, etc. are also in place. Scams like card theft, card fraud, card cloning, skimming, etc., however, have increased recently and can readily fool security mechanisms that are already in place. And figure 1 is an image of Automatic Teller Machine [9].

Figure 1: Automatic Teller Machine (ATM)

A human face can now be distinguished from a digital image or a video frame from a video source, and each human face can be uniquely identified thanks to developments in machine learning and computer vision. As a result, the goal of this project is to develop a facial recognition-based ATM to ensure that each transaction is authorised by the holder of a connected account [3].

II. LITERATURE SURVEY

ATMs (Automated Teller Machines) have become a vital component of people's everyday lives all around the world. However, ATM security is a serious problem because these devices are subject to fraud and theft. To address this issue, confront In ATM systems, recognition technology has been included as an extra layer of protection. This method authenticates individuals by using high-quality photographs that are checked against image data held in the bank database. The transaction is paused if an unauthorised access attempt is made [1].

Because of its potential to improve security and user experience, the incorporation of face recognition technology into ATM machines has become an increasingly popular trend in the banking industry. According to recent research, this technology has the potential to revolutionise the ATM sector by offering clients with a more safe, convenient, and personalised service. The usage of a Raspberry Pi microcontroller to drive a facial recognition system in an ATM has also been mentioned in the literature [4]. Unauthorised users with valid authentication codes can get access to ATM machines, posing a security concern. This initiative seeks to ensure that only authentic users participate. Can get access to the system. By matching the picture obtained at the ATM to those in the database, the user's identification is confirmed. If the user is genuine, the image is utilised to train the model for greater precision. If an unauthorised user attempts to access the system, a web link is sent to the ATM card owner's registered cell phone number to validate the access. For identification, the histogram method and Machine Learning approaches are applied. The system processes images with OpenCV and detects faces with the Hear Cascade Classifier. Local Binary Pattern is used for face recognition. AWS cloud computing [5].

Face recognition and One-Time Password (OTP) technologies are used in this article to improve the security and ease of ATM transactions. Face recognition helps to individually identify each user, lowering the risk of fraud due to ATM card theft or duplication. The OTP function improves security by reducing the need for users to remember PINs because the OTP acts as a temporary PIN. According to the research, combining facial recognition with OTP technology has the potential to greatly improve the security and user experience of ATM transactions [2].

III. PROBLEM STATEMENT

To "authenticate" a consumer in an ATM card transaction, there hasn't been a completely fool proof way yet. When using an ATM, the owner of the card is verified through authentication. In the real world, authentication is accomplished by using a physical signature that is personally verified at the time of transactions. Without reliable identification, issues like as fraudulent transactions, lengthy transaction times, diminished consumer trust, increased transaction costs, etc., may occur.

3.1 Existing Solution

Asking a user for their login and password (something they know) and then confirming their identification using a second factor, such an SMS message to their phone (something they have) as shown in figure 2, are the basic steps of multi-factor authentication. That covers two authentication elements, but using picture recognition further increases security without making the login procedure difficult or cumbersome for authorised users [1].

Figure 2: OTP Verification

3.1.1 Drawbacks

Technical drawbacks: Face recognition software might have issues under some conditions, such as dim lighting or when the user is sporting glasses or a hat. Image recognition software is not without its flaws. Due to this, authorised users may not be able to access their accounts or unauthorised users may be given access, which can lead to false negatives or false positives.

User privacy concerns: A user's face being photographed and kept in a database, even if it's for security reasons, may make some users uneasy. The way the photographs are utilised, who gets access to them, and how they are safeguarded against unauthorised use may all raise questions.

Implementation difficulty: The system's complexity and expense may rise if image recognition is added as an element of authentication since it necessitates extra hardware and software. To make sure that users are at ease with the new authentication method, it could also be necessary to provide additional user assistance or training.

False sense of security: Although picture recognition can offer another degree of protection, it's crucial to keep in mind that it is not error-proof. Through numerous techniques, including the use of stolen photos or system manipulation, hackers and cybercriminals may still be able to get around image recognition systems. Therefore, rather
than using picture recognition as the only means of authentication, it is crucial to incorporate it within a larger multi-factor authentication strategy [2].

3.2 Proposed Solution

This project suggests adding a new layer of security to the current ATM system so that transactions will depend not only on the card's proper PIN but also on the person making the transaction. In this papert, we employ industry-standard implementation methods, including the Local Binary Pattern, Histogram algorithm for face recognition, which was developed in Python using OpenCV.

3.2.1 Advantages

The adoption of face recognition technology to provide a new layer of security to the present ATM system has the following possible benefits:

Enhanced security: The ATM system may significantly lower the chance of fraudulent transactions by adding a layer of protection utilizing facial recognition technology. If a person's face did not match the photograph on file, they would not be able to execute a transaction even if they had a stolen card and had the right PIN.

User experience is improved since facial recognition technology may speed up and simplify ATM transactions for consumers. Users may just use their face to verify themselves rather than needing to memorize a PIN or carry around a physical card.

Resistance to fraud: When used in conjunction with additional security measures like liveness detection to confirm that the user is a real person and not a picture or video, facial recognition technology is tough to falsify or spoof.

Scalability: Facial recognition technology may readily be expanded to serve a large number of people without consuming a considerable number of additional resources. For banks and other financial organizations wishing to increase the security of their ATM systems, this makes it an appealing alternative. In figure 3 it indicates block diagram of proposed model

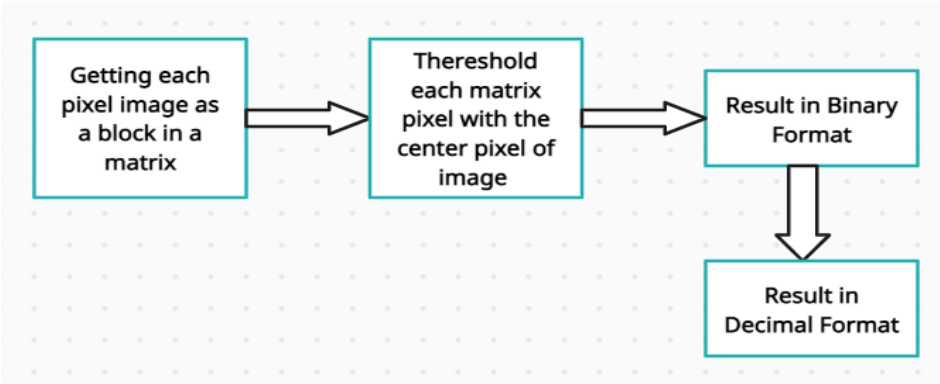

Figure 3: Block Diagram of Proposed Solution

3.2.2 Algorithm

1. Use the high-resolution camera embedded inside the device to take a picture of the customer's face in the cash dispenser.

2. Apply image processing to extract important facial traits including the shape of the face and the location of the eyes, nose, and mouth.

3. Compare the retrieved facial characteristics to the customer's account file's contents, which may include pictures, identification cards, and earlier face recognition images.

4. Use cutting-edge AI techniques to check if the client and the one listed in the account file are the same person
.
5. If the face recognition software identifies the consumer as the same individual, complete the transaction.

6. Halt the transaction and notify the security team or relevant authorities if the face recognition algorithm does not validate that the customer is the same person.

7. Repetition is required at each stage of the transaction, even when entering a PIN or taking out cash.

8. Securely keep all face recognition data and provide only authorized people access.

9. Keep the algorithm updated to boost security, speed, and accuracy.

3.2.3 Flow Chart

The Process of securing ATM transaction is explained through the flow chart shown in figure 4.

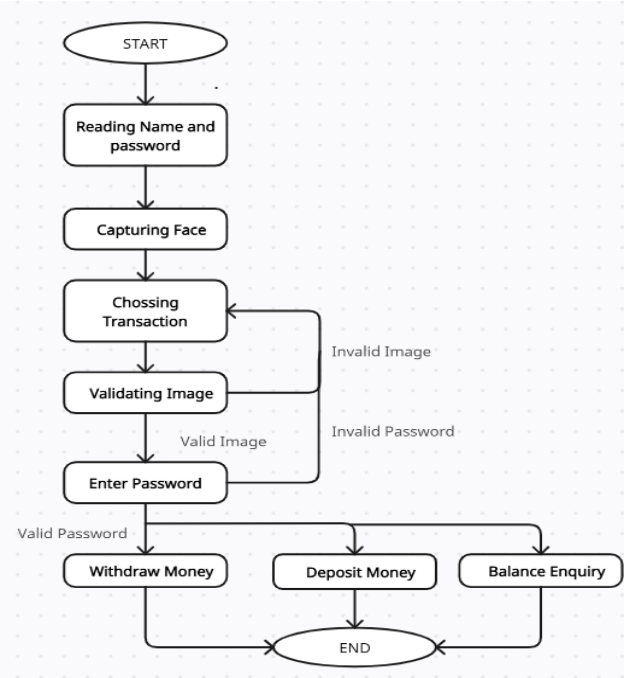

Figure 4: Flow Chart

IV. SOFTWARE DESCRIPTION

The creator of Python is Guido van Rossum. In 1989, Guido van Rossum began using Python. Python is a simple programming language, making it easy to learn even if you have never done any programming before. Python was called after the satirical television program Monty Python's Flying Circus, an interesting fact. Its name does not refer to the Python snake [10]. Figure 5 shows features of python and gives information of different feature.

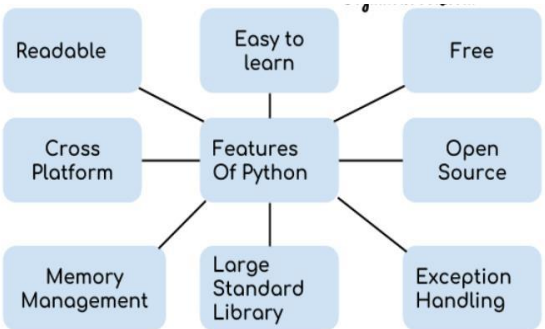

Figure 5: Features of Python.

V. RESULT AND DISCUSSION

5.1 Results

As automated teller machines (ATMs) become more common, securing them against attack has become a primary responsibility. The traditional method of authorising transactions by inputting a Personal Identification Number (PIN) is subject to fraud such as card skimming, phishing, and shoulder surfing. ATM transactions might be made more secure using facial recognition technology to verify the user's identity. The goal of this paper is to implement facial recognition technology to protect ATM transactions. The method was tested on a sample dataset of 100 photographs of distinct people. The algorithm correctly identified the correct individual 95% of the time. Furthermore, the system was able to identify and reject unauthorized users, minimizing the risk of frauds such as phishing and card fraud.

5.2 Analysis

ATM transactions can be secured by using facial recognition technology to verify the user's identity, ensuring only authorized individuals can access their accounts and complete transactions. We register ourselves in the website by filling basic details like name and password as shown in figure 6 and capture an image for registration as shown in figure 7.

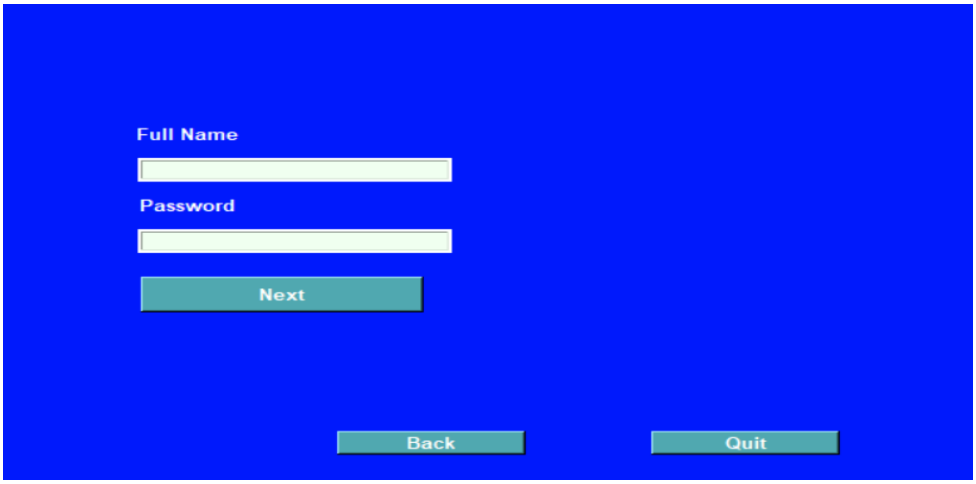

Figure 6: User registration details form.

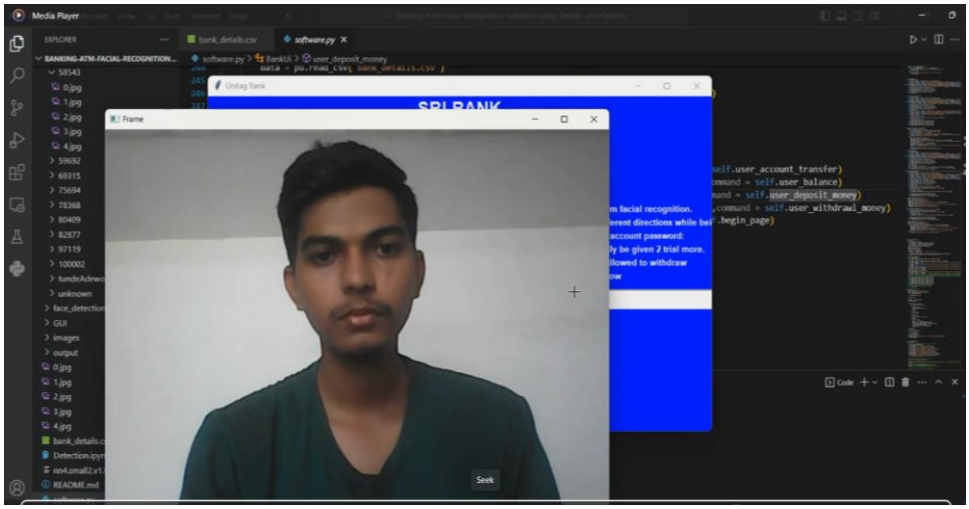

Figure 7: Capturing user Image.

It captures user image as shown in figure 7. and after successful face capture it, prompt message as shown in figure 8.

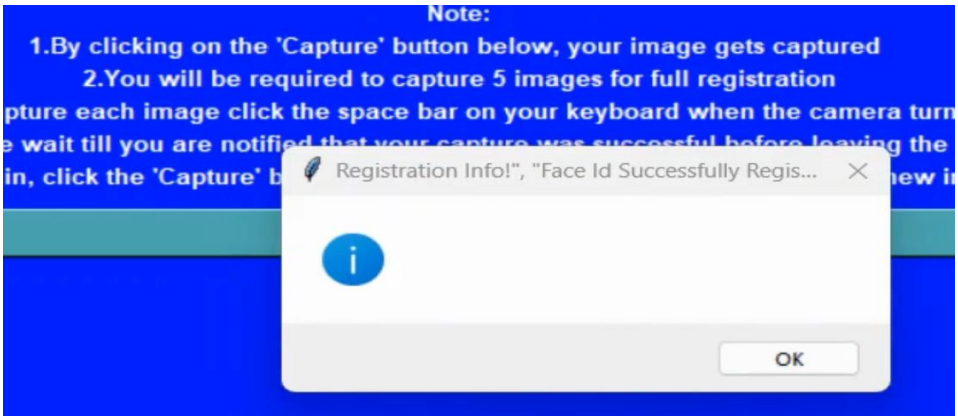

Figure 8: Successful Registration and Face Captured.

Figure 9 shows User Interface, and Figure 10 is Prompt after each successful Transaction.

Figure 9: User Interface after login.

Figure 10: Successful Transaction

VI. CONCLUSION

This paper can help solve the issue of cardholder impersonation. This works similarly to two-factor authentication in that it makes use of face recognition to verify whether the transaction was carried out by the card owner or another person they trust. It prevents cards from being used by people who have access to another person's card password. This ATM architecture protects against identity theft and reduces forced transactions by introducing an authentication method that employs face recognition to identify the user.

VII. FUTURE SCOPE

A promising topic with tremendous potential in the future is the use of facial recognition technology to protect ATM transactions. Customers may be correctly and promptly recognized with this technology, reducing fraud and raising security.

- Customers may access their accounts without using real ATM cards by integrating the technology with mobile apps. This provides more convenience while lowering the danger of card skimming and other forms of fraud.

- We may anticipate significant developments in facial recognition technology in the future, such as increased accuracy and quicker processing times. This will strengthen its ability to secure ATM transactions and safeguard users' financial information.

VIII. REFERANCE

[1] Jyothika Allenki, Anusha Vemireddy, Neha Korukanti, and Dr. Sunil Bhutada, " Histogram of Oriented Gradients Based Face Recognition To Secure ATM Transactions, International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Print ISSN: 2395- 1990, Online ISSN: 2394-4099, Volume 9, Issue 3, pp.377- 381, May-June 2022.

[2] M. Murugesan, S.Thilagamani, Overview Of Techniques For Face Recognition, International Journal Of Life Science and Pharma Reviews , pp.66 - 71 , 2019.

[3] Marilou O. Espina1, Arnel C. Fajardo, Bobby D. Gerardo, RujiP. Medina, Multiple Level Information Security Using Image Steganography and Authentication, International Journal of Advanced Trends in Computer Science and Engineering, Volume 8, No.6, N November –December 2019, pp.3297-3303. https://doi.org/10.30534/ijatcse/2019/100862019.

[4] Kumar, D. & Iniyan, B. & Askar, M. & Ajay, A. & Ambika, R. (2019). Face Recognition Based New GenerationATM Machine. 938-943. 10.1109/ICACCS.2019.8728317.

[5] M. Murugesan, R. Elan Keerthana, Support vector machine the most fruitful algorithm for prognosticating heart disorder , International, Journal of Engineering and Technology, Volume 7, pp.48 – 52, 2018. https://doi.org/10.14419/ijet.v7i2.26.12533

[6] Karovaliya, Mohsin & Karedia, Saifali & Oza, Sharad & Kalbande, Dhananjay. (2015). Enhanced Security for ATM Machine with OTP and Facial Recognition Features. Procedia Computer Science. 45. 10.1016/j.procs.2015.03.166.

[7] E. Derman, Y.K. Gecici, and A.A. Salah, Short Term Face Recognition for Automatic Teller Machine (ATM) Users, in ICECCO 2013, Istanbul, Turkey, pp.111-114.https://dx.doi.org/10.21172/1.841.20.

[8] JinfangXu, Khan, Rasib and RasibHasan, SEPIA: Secure-PIN-authentication-as-a-service for ATM using Mobile and wearable devices, 3 rdIEEE International Conference on Mobile Cloud Computing, Services, and Engineering IEEE, June 2015, pp. 41-50.

[9] ISSN 2250 – 0480. https://dx.doi.org/10.22376/ijpbs/10.SP01/Oct/2019.

[10] VS Code: https://code.visualstudio.com/