IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125261

Real Time Secure Clickbait and Biometric ATM User Authentication and Multiple Bank Transaction System

Mrs.P.Brinda B.Tech.,M.Tech.[1], Pranish.S[2], Pragadeesh.S[3], Thirumalai Raju.R[4]

Vel Tech High Tech Dr. Ranagarajan Dr. Sakunthala, Engineering College, Avadi, India[1-4]

Abstract: Nowadays, people use ATMs widely. Withdrawals from ATMs are increasing day by day. The current traditional ATM is vulnerable to crime due to the rapid development of technology. With a total of 270,000 reports of bank card fraud, it was the most reported form of identity theft in 2021. This project proposes an automated teller security model that uses electronic facial recognition using a deep convolutional neural network. Face verification Click bait link is generated and sent to the bank account holder to verify the identity of the unauthorized user through some special AI agent for remote authentication. However, it is clear that human biometric characteristics cannot be imitated.. Experimental results on real-time datasets show superior performance of the proposed approach compared to state-of-the-art deep learning techniques in terms of both learning efficiency and equal accuracy. .Using this real-time dataset, the proposed system achieves the highest accuracy of 97.93%.

Keywords: ATM, Face Recognition, Safety , Modules.

I. INTRODUCTION

Automated Teller Machines, often called cashiers, are one of the most useful advances in banking. ATMs allow bank customers to use fast self-service transactions such as cash withdrawals, deposits and money transfers. ATMs allow people to do banking without the help of an actual bank teller. Customers can also use banking services without visiting a bank branch. Most ATMs can be used to pay by debit or credit card. Some transactions do not require a debit or credit card. Facial recognition can be used to secure ATM transactions and is used as a means of authenticating users to verify the cardholder. Financial fraud is a very serious problem for banks, and the current secure data on the magnetic strip of the ATM card is very vulnerable to theft or loss. By using facial recognition to authenticate users at an ATM, the cardholder can be verified. When "Shoulder Surfers" try to peek over the cardholder's shoulder to get the PIN as the cardholder enters it, an ATM automatically reminds the cardholder to be careful. If the user is wearing a mask or sunglasses, the ATM will refuse to serve them until the protections are removed. Contactless- no need to remember passwords. Just looking at the ATM's camera registers the cardholder instantly. No physical contact is required. Protected - Because your face is your password, you don't have to worry about your password being forgotten or stolen. In addition, the facial recognition engine locks the cardholder's access to the account and transaction pages if the cardholder moves away from the ATM camera and another face appears.

II. LITERATURE REVIEW

Taking security monitoring for granted can lead to additional threats and risks. Surveillance camera placement guidelines and standards can mitigate this vulnerability to some extent[1] In the current system, a user must visit the nearest ATM, swipe that ATM's card, to withdraw money. This physical contact between the card and the machine makes it easy for fraudsters to collect and misuse data. The proposed solution eliminates this physical contact. The mobile application consists of a special code that flashes on the screen for 1 minute. This code provides strong authentication by dynamically generating a one-time security code. This code can be generated even when there is no network or internet connection. Here, the user first logs into the mobile application using details such as username and password. The user then creates a reference number of their choice and also sets the amount withdrawn. This reference number is valid for a certain time and can only be used once. Once the reference number is generated, the user visits the nearest ATM and enters the username and password and code into the application to log in. If the authorized user is present, he/she will log in and have to enter the reference number to withdraw the specified amount. If the reference number is correct, the amount will be withdrawn, otherwise the transaction will fail. This idea is a combination of the current ATM system and OTP online transactions. By removing the use of OTP, the problems related to sharing of OTP will be successfully solved. This system offers three levels of protection, first when the user's identity is verified when logging into the system, secondly through the username, password and code in the mobile application. – Entered through the ATM and finally the reference

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.125261

number[2] Today, the banking dependence of the virtual world has risen to the highest position. Advanced techniques must be used to make it consistent. Since OTP is currently used worldwide for security reasons, it can be bypassed using a QR code. A QR code reader is required to detect and decode the codes stored in the QR code. A scanner must be installed in the ATM so that the user can receive the input data. We offer additional functionality to the existing system, so there is also a traditional withdrawal option. On the other hand, the ATM scans the QR code generated by the Android application GetNote and decrypts it with the key

I. stored in the database. After decryption, the ATM will receive the necessary identification information such as card number, amount, PIN code, cvv number on the card etc. It checks all the information from the bank's database. After successful authentication, the ATM will dispense money. The ATM is responsible for validating the QR code, such as the time when the discrepancy occurs and the scan time is a maximum of five minutes. The ATM can recognize the QR code individually from the image, the duplicate QR code will be rejected. The system only recognizes the QR code generated by GetNote (android application)[3] The cardholder swipes the card and enters the PIN according to the previous ATM process, but after entering the PIN, it is not enough to just enter the PIN, he must select the option of OTP or To create fingerprint recognition. of a successful business. This increases ATM card security and safer transactions[4] This system is more secure and faster and helps provide better options[5] Security analysis and threat modeling highlight the security strength of the proposed system against vulnerable attacks during authentication[6] . The proposed method increases security by detecting and reducing fraud[7].

III. METHODODLOGY

A.Face registration

This module starts with the front page registration of some bank payment templates. These patterns then become a reference for evaluating and recording other posture patterns: leaning up/down, getting closer/farther and turning left/right.

B. Face image acquisition

Cameras must be used to record the corresponding video at the ATM. The computer and the camera are connected together, and the webcam is used here.

C. Dismantling the frame

Frames are extracted from the video input. The video must be divided into a series of images that will be further processed. The speed with which video is divided into images depends on the activity of individuals. It can be said that usually 20-30 images are taken per second, which are sent to the next steps.

D. Pretreatment

Face image preprocessing is the steps to shape images before using them for model training and inference. The steps to be followed are:

• Read the picture
• RGB grayscale conversion
• Resize the image
Original size (360, 480, 3) — (width, height, no RGB channels)
Resized (220, 220, 3)
• Remove noise (Denoise)
smooth our image to remove unwanted noise. We do this using a Gaussian blur.
• Binarization
Binarizing an image is taking a grayscale image and converting it to black and white, which effectively reduces the information contained in the image from 256 shades of gray to two: a black and white, binary image.

IV.OUTPUT

Account holder receives a message and mail when the face unmatched in the ATM machine. Then the account holder can be block the card or accept the transaction with whatever the amount they want to withdrawal. This brings high security for the account holders.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125261

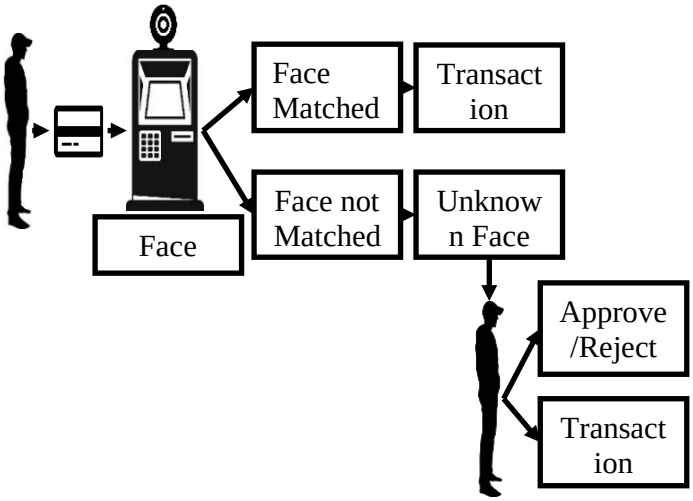
V.PROPOSED SYSTEM

Facial Biometric Authentication System using Deep Learning TechniquesDeep learning is a subset of machine learning, which, in turn, is a subset of artificial intelligence (AI). When it comes to Face recognition, deep learning enables us to achieve greater accuracy. Deep FR system with face detector and alignment. First, a face detector is used to localize faces. Second, the faces are aligned to normalized canonical coordinates. Third, the FR module is implemented. In FR module, face anti-spoofing recognizesWhether the face is live or spoofed; face processing is used to handle variations before training and testing, e.g., poses, ages;`. Unknown Face Verification Link Generator– When the stored image and the captured image don't match, it means that he is an unauthorized user. Face Verification Link will be generated and sent to user to verify the identity of unauthorized user through some dedicated artificial intelligent agents, for remote certification, which either authorizes the transaction appropriately or signals a security-violation alert to the banking security system.

A. Advantages of proposed system

- The advantages can be found as that the face-id is unique for everybody; it cannot be used by anybody other than the user.
- It can be used to reduce fraudulent attempts.
- To prevent theft and other criminal activities.
- Secure facial authentication platform that users can trust
- Provide safe and secure lifestyle infrastructure
- Prevent unauthorized access using Face verification Link.
- Fast and Accurate Prediction

B. Block diagram



VI.RESULTS

The ROC curve detection results show that the traditionalface detection method VJ recall rate is only 66.6%, the detection method based on deep learning has been greatlyimproved. It is very encouragingto see that our model consistently achieves the competitiveperformance across the three subsets. It has higher robustnessfor faces with large occlusion and Angle change, which isbasically consistent with the evaluation results in the FDDBdataset.

VII. CONCLUSIONS

Biometrics for identification and authentication of account holders in ATMs offers a necessary and expected solution to the problem of illegal payment transactions. In this project, we have developed a solution to the much feared problem of fraudulent transactions through ATMs using biometrics and Unknown Face Forwarder. This is only possible if the owner of the account is physically or remotely present. Thus, it eliminates cases where illegal transactions are made at ATM points without the knowledge of the genuine owner. The use of a biometric feature for identification is strong and is further strengthened when another level of authentication is used.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.125261

The security design of the ATM takes into account the possible proxy use of existing security tools (eg ATM card) and data (eg PIN code).existing ATM security mechanisms. It engages the bank account in real time with all available and receivable transactions

VIII.FUTURE ENHANCEMENTS

We Some possible future enhancements for real-time secure swipe and facial biometric ATM user authentication and multi-bank systems may include:

1. Better accuracy: The system could be further optimized to improve the accuracy of face recognition and verification, reducing the chance of false positives or false negatives.
2. Integration with additional security features: The system can be integrated with additional security features such as biometric authentication or OTP verification to improve the security of ATM transactions.
3. Multi-factor authentication: The system could be extended to support multi-factor authentication, where users must provide other authentication methods such as a password or fingerprint in addition to facial recognition.
4. Real-time alerts: The system can be configured to send real-time alerts to bank administrators or security personnel in the event of a security breach or suspicious activity.
5. Integration with mobile banking: The system could be integrated with mobile banking applications so that users can complete payment transactions and account management tasks on their mobile devices.
6. Multilingual Support: The system can be extended to support multiple languages, making it more accessible to users who do not speak the system's default language.
7. Support for additional transaction types: The system could be extended to support other transactions, such as bank transfers or bill payments, to provide users with a more comprehensive banking experience. Overall, these improvements can help further improve the security, accessibility and functionality of Real Time Secure Clickbait and Face Biometric ATM user authentication and multiple bank transfer systems, providing users with a more secure and convenient banking experience.

REFERENCES

[1] J. Liang, H. Zhao, X. Li, and H. Zhao, ``Face recognition system basedon deep residualnetwork," in Proc. 3rd Workshop Adv. Res. Technol. Ind.(WARTIA), Nov. 2017, p. 5.
[2] I. Taleb, M. E. Amine Ouis, and M. O. Mammar, ``Access control usingautomated face recognition: Based on the PCA & LDA algorithms," inProc. 4th Int. Symp. ISKO-Maghreb, Concepts Tools Knowl. Manage.(ISKO-Maghreb), Nov. 2014, pp. 1-5.
[3] X. Pan, ``Research and implementation of access control system basedon RFID and FNN-face recognition," in Proc. 2nd Int. Conf. Intell. Syst.Design Eng. Appl., Jan. 2012, pp. 716-719, doi: 10.1109/ISdea.2012.400.
[4] A. A. Wazwaz, A. O. Herbawi, M. J. Teeti, and S. Y. Hmeed, ``RaspberryPi and computers-based face detection and recognition system," in Proc.4th Int. Conf. Comput. Technol. Appl. (ICCTA), May 2018, pp. 171-174.
[5] A. Had, S. Benouar, M. Kedir-Talha, F. Abtahi, M. Attari, and F. Seoane,``Full impedance cardiography measurement device using raspberryPI3 and system-on-chip biomedical instrumentation solutions," IEEE J.Biomed. Health Informat., vol. 22, no. 6, pp. 1883-1894, Nov. 2018.
[6] A. Li, S. Shan, andW. Gao, ``Coupled bias-variance tradeoff for cross-poseface recognition," IEEE Trans. Image Process., vol. 21, no. 1, pp. 305-315,Jan. 2012.
[7] C. Ding, C. Xu, and D. Tao, ``Multi-task pose-invariant face recognition,"IEEE Trans. Image Process., vol. 24, no. 3, pp. 980-993, Mar. 2015.
[8] J. Yang, Z. Lei, D. Yi, and S. Li, ``Person-specific face antispoofong withsubject domain adaptation," IEEE Trans. Inf. Forensics Security, vol. 10,no. 4, pp. 797-809, Apr. 2015.
[9] H. S. Bhatt, S. Bharadwaj, R. Singh, and M.Vatsa, ``Recognizing surgicallyaltered face images using multiobjective evolutionary algorithm," IEEETrans. Inf. Forensics Security, vol. 8, no. 1, pp. 89-100, Jan. 2013.
[10] T. Sharma and S. L. Aarthy, ``An automatic attendance monitoring systemusing RFID and IOT using cloud," in Proc. Online Int. Conf. Green Eng.Technol. (IC-GET), Nov. 2016, pp. 1-4