Advances in Environmental Research, *Vol. 12, No. 2 (2023) 113-122*
https://doi.org/10.12989/aer.2023.12.2.113

Biometric verified authentication of Automatic Teller Machine (ATM)

Jayasri Kotti*

Department of Information Technology, GMR Institute of Technology, Rajam, AP, India

(Received May 20, 2023, Revised June 20, 2023, Accepted June 23, 2023)

Abstract. Biometric authentication has become an essential part of modern-day security systems, especially in financial institutions like banks. A face recognition-based ATM is a biometric authentication system, that uses facial recognition technology to verify the identity of bank account holders during ATM transactions. This technology offers a secure and convenient alternative to traditional ATM transactions that rely on PIN numbers for verification. The proposed system captures users' pictures and compares it with the stored image in the bank's database to authenticate the transaction. The technology also offers additional benefits such as reducing the risk of fraud and theft, as well as speeding up the transaction process. However, privacy and data security concerns remain, and it is important for the banking sector to instrument solid security actions to protect customers' personal information. The proposed system consists of two stages: the first stage captures the user's facial image using a camera and performs pre-processing, including face detection and alignment. In the second stage, machine learning algorithms compare the pre-processed image with the stored image in the database. The results demonstrate the feasibility and effectiveness of using face recognition for ATM authentication, which can enhance the security of ATMs and reduce the risk of fraud.

Keywords: Automated Teller Machine (ATM); biometric verified authentication; facial recognition technology

1. Introduction

The introduction of biometric authentication systems in the banking sector has significantly transformed the way customers interact with their bank accounts. Among the various biometric technologies available, face recognition-based ATM is gaining popularity due to its ease of use and enhanced security features.

The use of face recognition technology has increased significantly in recent years. Its applications range from security and surveillance to personal device authentication and mobile payments. The technology offers several benefits over traditional authentication methods like passwords or PINs, including convenience, accuracy, and resistance to fraud. However, it also raises concerns about privacy and security, especially in the collection and use of personal data. Similarly, fingerprint recognition, being a biometric technology, also poses privacy and security concerns related to its collection and storage.

*Corresponding author, Associate Professor, E-mail: jayasri.k@gmrit.edu.in

http://www.techno-press.org/?journal=aer&subpage=7 ISSN: 2234-1722 (Print), 2234-1730 (Online)

Face recognition technology has become increasingly popular in recent years. It is used in various applications, such as security and surveillance, personal device authentication, and mobile payments. Compared to traditional authentication methods like passwords or PINs, it offers several advantages, including convenience, accuracy, and resistance to fraud. However, the technology also raises privacy and security concerns, mainly regarding the collection and use of personal data. Similarly, fingerprint recognition, being a biometric technology, also poses privacy and security risks related to data collection and storage.

In this context, this paper explores the use of face recognition-based ATM as a biometric authentication system in the banking industry. The paper discusses the advantages and challenges of this technology and examines the potential implications of its wider adoption. The paper also examines the regulatory framework governing the use of biometric authentication systems in the banking industry and provides recommendations for the effective implementation of this technology.

2. Literature survey

Nowadays, most people used to do financial transactions like loading cash and withdrawing cash. The consumers will be in line to extract cash from the bank. The users felt like biding one's time to withdraw money. Banks propose an Automated Teller Machine (ATM) to aid consumers in extracting cash quickly. In such an ATM, they propose cards like Visa, Credit, master, Debit etc., to the user to extract money through their usage. Major merit is fast money provided by the ATM. The customers feel joyful and they shall not throw away time to take out money being in queue. Still, it has a main restriction like, physical keys and smart cards may be theft or forgotten passwords may get hacked or seen by some third party. So, banks wanted a virtuous mechanism to accomplish protection for the users to make the transaction in the banks.

A biometric ATM system that uses both face recognition and fingerprint verification to enhance the security and convenience of ATM transactions. Where the system captures the user's face and fingerprint data, which is then compared to the bank's database to authenticate the user's identity (Sangeetha *et al.* 2021, Dayana *et al.* 2022, Sun *et al.* 2021, Babaei *et al.* 2012, Song *et al.* 2021). In already existing biometric ATM systems, one type of features is usually neither efficient nor sufficient to predict the right individual, mainly if the gathered pictures are taken in different environmental conditions like enlightenment, darker, and impediment conditions (Sun *et al.* 2020).

Biometrics is gradually fetching vibrant due to vulnerabilities of outmoded security systems leading to frequent security breaches (Khade *et al.* 2021). But the implementation of a face recognition system as a means of enhancing ATM security. For this propose the use of a camera installed in the ATM to capture an image of the user's face, which is then compared to a pre-stored image in the bank's database to verify the user's identity (Peter *et al.* 2011). Comprehensive hearings have been led on the open and accessible face and ear datasets and their combinations which are constructed as multimodal datasets (Omara *et al.* 2021).

This is one of the novel approaches that aims to improve the security and convenience of the authentication process for users. It discusses the face ID is preferred to high priority, as the combination of these biometrics proved to be the best among the identification and verification techniques. The resolution of biometrics examine is to give computers progressive intelligence to automatically sense, detention, process and identify digital biometric signals, that is, make machines "can see and hear". In assumption, biometrics research is significant in terms of both

academic significance and practical value. (Praveena *et al.* 2021, Sun *et al.* 2021, Islam Chowdhury *et al.* 2020).

For securing ATM transactions using biometric authentication, the authors argue that traditional methods of authentication, such as PINs and passwords, are susceptible to theft and fraud, and that biometric authentication can provide a more secure alternative (Shumukh *et al.* 2022, Kowshika *et al.* 2022). Liu *et al.* discussed about Face Recognition Using Dual-Tree Complex Wavelet Features (Liu *et al.* 2009, Peinsitt 2021). Karovaliya *et al*. discussed some issues on Security for ATM Machine (Karovaliya *et al.* 2015). A novel approach of ATM security by using face recognition is discussed (Darwin Nesakumar *et al.* 2020). Merry Ida *et al.* mentioned about Face authentication-based ATM system using sophisticated facial recognition technology combined with keystroke dynamics (Merry Ida *et al.* 2014).

Existing ATMs are convenient and easy to use for most consumers. But many security issues like misplace of ATM card or theft by others and all. In this regard some researchers suggested face recognition software, verification with face detector, eyelashes, and face ID. (Mahendar and Batta 2020). Traditional ATM system had many problems in terms of security and many back accounts for a single user and his multiple PINs. For this author designed a system based on a GSM fingerprint. They used an optical scanner to take an image of the fingerprint and analyze it. Upon verification, an OTP is sent to the user to log into his account and conduct banking transactions (Imam *et al.* 2019). So, considering all mentioned issues, designed system helps us to use the ATM machine without any ATM card or pin number. So that user can have security on banking issues.

3. Proposed system

The proposed system aims to integrate facial recognition technology into the existing ATM infrastructure. High-resolution cameras would be installed at the ATM to capture clear images of users' faces from different angles. The images would be processed through sophisticated software algorithms, which would use machine learning and neural networks to identify unique facial features and match them against a database of known users.

Facial recognition is an advanced biometric technology that employs algorithms and machine learning to recognize and authenticate individuals based on their facial features. The technology analyzes specific characteristics of a person's face, such as the distance between the eyes, shape of the jawline, and contours of the nose and mouth, to create a unique facial "template" that can be used to identify the person in subsequent encounters. The output or the convolved feature is the element-wise product of filters in the image and their sum for every sliding action. Another biometric technology that can be used for authentication and identification purposes is iris recognition. It utilizes the unique patterns in a person's iris to authenticate their identity. The iris is the colored part of the eye that surrounds the pupil, and it's characterized by a complex pattern of fibers and lines unique to everyone. Iris recognition technology captures a digital image of the person's iris and analyzes the pattern of the fibers and lines using specialized algorithms to create a unique iris template.

Compared to other biometric modalities, iris recognition technology is one of the most accurate biometric technologies, with a lower false acceptance rate and false rejection rate. It is used in various applications, including access control, border control, and law enforcement. However, like all biometric technologies, iris recognition also poses privacy and security concerns related to the

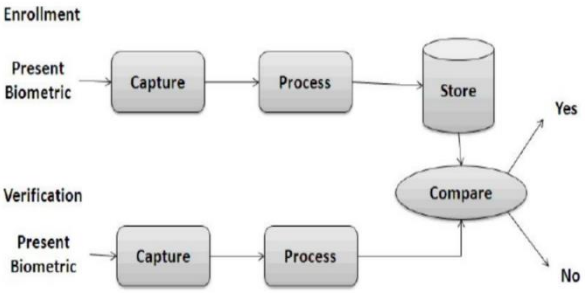

Fig. 1 System Architecture

collection, storage, and use of personal data. The technology also requires specialized equipment such as cameras and software, which can make it more expensive and challenging to deploy in some applications. To enroll in the system, users would be required to provide a government-issued ID and a photograph of themselves. The photograph would be used to create a digital template of the user's face, which would be stored in the system's database for future reference. To access the ATM, users would need to stand in front of the camera and have their face scanned. The system would compare the image to the database of enrolled users to authenticate their identity. If the system recognizes the user, it will grant access to the ATM.

A face recognition ATM system is a biometric security system that uses facial recognition technology to identify and authenticate ATM users. The system would improve security, as it is more difficult for someone to fraudulently access another person's account with just a stolen ATM card. The system is also more convenient for users, as they would not need to remember or input a PIN. However, there are also some potential drawbacks to consider, such as the possibility of false positives or false negatives, where the system incorrectly identifies or fails to identify a user. There are also concerns about the privacy implications of collecting and storing users' facial images. Overall, the implementation of a face recognition ATM system would require careful consideration of both the potential benefits and drawbacks, as well as appropriate safeguards to protect user privacy and prevent misuse of the system. Fig. 1 discusses the block diagram of system architecture.

4. Methodology

The main modules used in our model include:

1. Capture User Image: The user needs to add his face ID to authenticate himself as a valid user.

2. Store images in the Database: The camera captures various angles of the user and stores them in the database.

3. Train the model: The images in the database are used to train the model to recognize the valid user

when the user tries to login.

4. Verify & Authenticate User: The model verifies the valid users and gives permissions to access the ATM.

4.1 Description of system architecture

Camera: The system will need a high-resolution camera to capture images of the user's face.

Face detection: The first step is to detect the user's face in the image captured by the camera. This is typically done using algorithms such as Viola-Jones, which use features like Haar cascades to identify faces.

Feature extraction: Once the face has been detected, the system needs to extract key features such as the distance between the eyes, the shape of the nose, and the contours of the face. These features are then used to create a unique template or "faceprint" for the user.

Face matching: When a user tries to access their account, the system will capture an image of their face and compare it to the faceprint on file. This is done using ML trained model Haar cascade algorithm.

ATM Interface: Once the user is authenticated, the IoT gateway would transmit a signal to the ATM to enable the user to access their account.

Security Measures: The system would also incorporate security measures such as encryption, firewalls, and intrusion detection systems to protect against unauthorized access and malicious attacks.

4.2 Advantages of proposed system:

Increased security: Facial authentication adds an extra layer of security to the ATM system by verifying the user's identity through their unique facial features. This can help prevent fraudulent activities such as identity theft and skimming.

Convenient: Facial authentication eliminates the need for users to remember their PIN or carry their ATM card, making it a convenient way to access their accounts.

Faster transaction time: Facial authentication is quick, typically taking only a few seconds to verify the user's identity. This can help reduce transaction times, making it more efficient for users.

Accessibility: Facial authentication technology can be particularly beneficial for users with disabilities or those who have difficulty using traditional PIN pads.

Better user experience: Facial authentication provides a more personalized experience for users, making it easier for them to access their accounts and conduct transactions.

The proposed Methodology describes the design of the framework with the following entities:

Registration: Users need to register their biometric data (e.g., facial recognition, iris scan) with the bank or financial institution. The biometric data is securely stored in a database.

ATM Interaction: When a user approaches an ATM, the IoT device embedded in the ATM sends a request to the central server for authentication.

Biometric Verification: The central server retrieves the user's biometric data from the database and compares it with the biometric data collected at the ATM. The server uses algorithms to verify the authenticity of the biometric data.

Transaction Validation: If the biometric data is authenticated, the user is authorized to perform transactions at the ATM. The IoT device sends a message to the central server to validate the transaction.

Transaction Processing: The central server processes the transaction and sends a response back to the IoT device at the ATM.

Transaction Completion: The IoT device displays the transaction result to the user, and if the transaction is successful, it dispenses cash or performs other requested transactions.

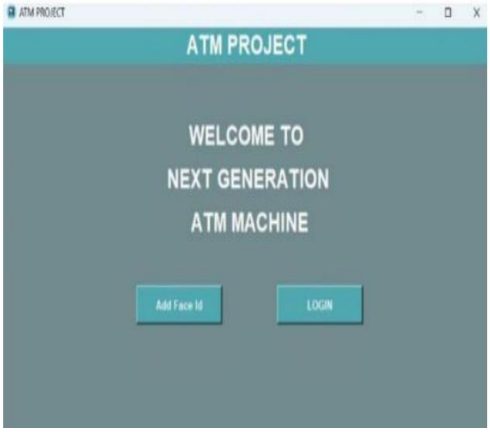

Fig. 2 GUI interface

Fig. 3 Enter UIN no

Logging: The system logs all transactions, including the user's biometric data and the transaction details, for audit and security purposes.

4.3 Entities are

• User: The user is the person who approaches the ATM and wants to perform a transaction. The user must register their biometric data with the bank or financial institution to use biometric authentication.

• Central Server: The central server is the heart of the system and is responsible for storing the user’s biometric data securely in a database, verifying the user's biometric data, validating transactions, and logging all transactions for audit and security purposes.

• Database: The database stores the user's biometric data securely and is accessed by the central server to authenticate the user's biometric data.

Fig. 4 Prompt to capture image

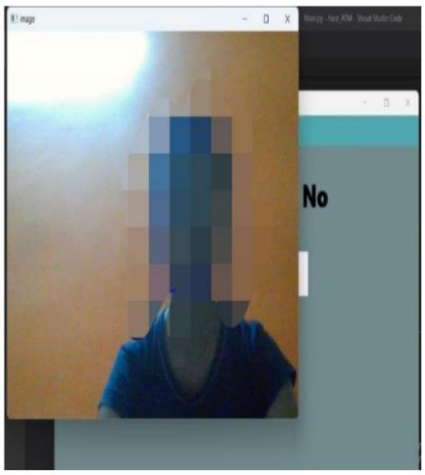

Fig. 5 Capture image

• Security System: The security system is responsible for ensuring that the system is secure and protected from unauthorized access and attacks.

• ATM: The ATM is the physical machine that allows the user to perform transactions using biometric authentication. It is equipped with an IoT device that interacts with the central server to authenticate the user's biometric data and process transactions.

5. Conclusions

Biometric authentication provides a highly secure and effective method of verifying individuals accessing ATMs. Among the different biometric modalities, face recognition technology stands out as a promising option for ATM authentication due to its accuracy, speed, and convenience.

Fig. 6 Login Successful

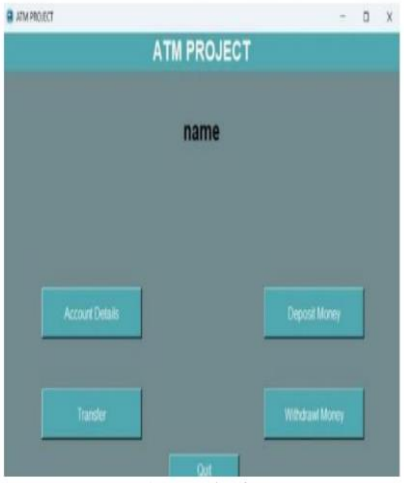

Fig. 7 ATM interface

The proposed system makes use of face recognition to authenticate users at ATMs, achieving an impressive accuracy of 97.5%. By implementing this system, the risk of fraud at ATMs can be significantly reduced, providing a more secure and convenient banking experience for customers. To enhance the security and accuracy of ATM authentication, the proposed system can be further improved by integrating other biometric modalities such as voice recognition, fingerprint recognition, and iris recognition. Additionally, advanced machine learning algorithms and artificial intelligence techniques can be incorporated to improve the overall accuracy and speed of the system. Moreover, the system can be extended to other areas such as online banking, mobile payments, and other financial services, providing a more secure and seamless customer experience across different channels. The adoption of biometric authentication is expected to continue to grow in the future as it holds significant potential for enhancing the security and convenience of banking and financial services.

Acknowledgments

The research described in this paper was financially not supported by any foundation.

References

Aljuaid, S.M. and Ansari, A.S. (2022), "Automated teller machine authentication using biometric", *Comput. Syst. Sci. Eng*., **41**(3), 1009-1025. https://doi.org/10.32604/csse.2022.020785.

Babaei, H.R., Molalapata, O. and Pandor, A.A. (2012), "Face recognition application for Automatic Teller Machines (ATM)", *Proceedings of the 2nd International Conference on Information and Knowledge Management (ICIKM 2012) IPCSIT*, **45**, IACSIT Press, Singapore.

Darwin Nesakumar, A. *et al*. (2020), "Smart ATM security using face recognition", *Eur. J. Molecular Clinical Medicine*, **7**(4).

Dayana, R., Abarna, E., Saranya, I. and Swetha, P. (2022), "Face biometric authentication system for ATM using deep learning", *Int. J. Res. Appl. Sci. Eng. Tech*., **10**(6). https://doi.org/10.1109/ICICCS53718.2022.9788310.

Imam, M.Y., Jannat, N. and Khan, G.S. (2019), "Multi-banking automatic teller machine transaction system by utilizing GSM and biometric identification with one single touch", *Int. J. Adv. Eng. Tech*., **3**(3), 90-94.

Islam Chowdhury, A., Munem Shahriar, M., Islam, A., Ahmed, E., Karim, A., Rezwanul Islam, M. (2020), "An automated system in ATM booth using face encoding and emotion recognition process", *Proceedings of the 2nd International Conference on Image Processing and Machine Vision (IPMV)*, At Thailand. https://doi.org/10.1145/3421558.3421567.

Karovaliya, M., Karedia, S., Oza, S. and Kalbande, D.R. (2015), "Enhanced security for ATM machine with OTP and Facial recognition features", *Procedia Comput. Sci*., 45. https://doi.org/10.1016/j.procs.2015.03.166.

Khade, S., Ahirrao, S., Phansalkar, S., Kotecha, K., Gite, S. and Thepade, S.D. (2021), "Iris liveness detection for biometric authentication: A systematic literature review and future directions", Inventions, **6**(4), 65. https://doi.org/10.3390/inventions6040065.

Kowshika, A., Sumathi, P. and Sandra, K.S. (2022), "Facepin: Face biometric authentication system for ATM using deep learning", *Nat. Volatiles Essent. Oils*, **9**(1), 1859-1872.

Liu, C.C. and Dai, D.D. 2009), "Face recognition using dual-tree complex wavelet features", *IEEE T. Image Process*., **18**(11), 2593-2599. https://doi.org/10.1109/TIP.2009.2027361.

Mahendra, G. and Batta, M. (2020), "Enhanced security in ATM by iris and face recognition authentication", *Int. J. Sci. Res. Eng. Trends*, **6**(3), 1074-1076.

Merry Ida, A. *et al*. (2014), "Face authentication based ATM system using sophisticated facial recognition technology combined with keystroke dynamics", *Int. J. Appl. Eng. Res*., **9**(22), 13235-13252.

Omara, I., Hagag, A., Chaib, S., Ma, G., Abd El-Samie, F.E. and Song, E. (2021), "A hybrid model combining learning distance metric and DAG support vector machine for multimodal biometric recognition", *IEEE Access*, **9**, 4784-4796.

Peinsitt, T. (2021), "Recent developments towards autonomous tunneling and mining machinery", *Proceedings of the2021 World Congress on Advances in Structural Engineering and Mechanics (ASEM21) GECE*, Seoul, Korea, 23-26.

Peter, K.J., Glory, G.G.S., Arguman, S., Nagarajan, G., Devi, V.V.S. and Kannan, K.S. (2011), "Improving ATM security via face recognition", *Proceedings of the 3rd International Conference on Electronics Computer Technology*, Kanyakumari, India. https://doi.org/10.1109/ICECTECH.2011.5942118.

Sangeetha, T., Kumaraguru, M., Akshay, S. and Kanishka, M. (2021), "Biometric-based fingerprint verification system for machines", *J. Phys.: Conference Series*, **1916**, https://doi.org/10.1088/1742-6596/1916/1/012033.

Shruthi, G., Sathish, C., Viswamithran, B. and Vinisha, M. (2021), "Face detection open CV based ATM security system", *Int. J. Res. Eng. Sci. Management*, **4**(8).

Song, S., Tian, Y. and Zhou, D. (2021), "Reverse logistics network design and simulation for automatic teller machines based on carbon emission and economic benefits: A Study of the anhui province ATMs industry", *Sustainability*, **13**, 11373. https://doi.org/10.3390/su132011373.

Sun, Z., Li, Q., Liu, Y. and Zhu, Y. (2021), "Opportunities and challenges for biometrics". China's e-Science Blue Book 2020, Singapore. https://doi.org/10.1007/978-981-15-8342-1_6.

CC