Face Biometric Authentication System For ATM

M.Karthikeyan[1], Dr. D. Swamydoss[2],
[1]Dept of Computer Applications
[2]HOD, Dept of Computer Applications
[1, 2] Adhiyamaan College Of Engineering (Autonomous), Hosur, Tamil Nadu, India

Abstract- *The objective of this project is to proposes the alliance of Face Recognition System for authentication process, unknown face forwarder mechanism and enhancing the security in the banking region.With the rise of security concerns in banking transactions, traditional PIN-based authentication systems are proving to be increasingly vulnerable to fraud and security breaches. In response, advanced biometric authentication methods have emerged as promising alternatives, leveraging unique physiological characteristics for enhanced security. Among these, facial recognition technology stands out for its non-invasive and user-friendly nature.Utilizing deep learning techniques, FacePIN aims to provide a robust and secure authentication mechanism by analyzing facial features unique to each individual. Through convolutional neural networks (CNNs) trained on large datasets of facial images, the system can accurately identify and authenticate users within seconds.*

Keywords- ATM Simulator, Face Recognition, Unknown Face Forwarder Mechanism,Transaction Model.

I. INTRODUCTION

The objectives of the Face Biometric Authentication System for ATM project ,which proposes a FacePIN project align with the broader goals of enhancing security, improving user experience, and fostering innovation within the banking industry. By achieving these objectives, FacePIN has the potential to revolutionize ATM security and authentication processes, ultimately benefiting banks, customers, and the broader financial ecosystem. To encompass several key goals aimed at enhancing security, improving user experience, and advancing technological innovation within the banking sector.

The project aims to significantly enhance security measures at ATMs by implementing advanced biometric authentication technology. FacePIN leverages facial recognition algorithms to provide a robust and secure authentication mechanism, reducing the risk of unauthorized access, card skimming, and other fraudulent activities. FacePIN seeks to improve the user authentication process at ATMs by replacing or supplementing traditional PIN-based methods with facial biometrics. By offering a more secure and convenient authentication option, the project aims to enhance user confidence and trust in the banking system. One of the primary objectives of FacePIN is to minimize fraudulent transactions and mitigate financial losses for banks and customers.

The system incorporates real-time fraud detection mechanisms to identify suspicious activities and trigger additional security measures, thereby preventing unauthorized access and fraudulent transactions. The project strives to enhance the overall user experience at ATMs by providing a seamless and intuitive authentication process. FacePIN eliminates the need for users to remember and input complex PIN codes, offering a more user-friendly and accessible authentication option for individuals of all ages and abilities.FacePIN aims to ensure compliance with regulatory standards and data privacy laws governing the handling of biometric data and financial transactions.

II. LITERATURE SURVEY

The literature survey presented here provides a comprehensive overview of existing research, advancements, and technologies relevant to the development and implementation of the FacePIN project. By synthesizing insights from a diverse range of scholarly sources, this survey aims to contextualize the FacePIN project within the broader landscape of biometric authentication systems, facial recognition technology, and ATM security.

1. Biometric Authentication Systems:

- Overview of Biometric Technologies: The survey begins with an overview of biometric authentication systems, highlighting key concepts, principles, and modalities such as fingerprint recognition, iris scanning, and facial recognition.
- Evolution of Biometric Authentication: This section traces the historical development and evolution of biometric authentication systems, from early fingerprint-based systems to modern, multimodal approaches integrating multiple biometric modalities for enhanced security.

2. Facial Recognition Technology:

- Fundamentals of Facial Recognition: The survey explores the principles and methodologies underlying facial recognition technology, including feature extraction, pattern recognition, and machine learning algorithms.
- Recent Advancements in Facial Recognition: This section reviews recent advancements in facial recognition technology, such as deep learning techniques, convolutional neural networks (CNNs), and generative adversarial networks (GANs), which have significantly improved the accuracy and performance of facial recognition systems.

3. ATM Security and Authentication:

- Challenges in ATM Security: The survey examines the key challenges and vulnerabilities associated with traditional ATM security mechanisms, such as PIN-based authentication and card-based access control.
- Emerging Trends in ATM Security: This section discusses emerging trends and innovations in ATM security, including the adoption of biometric authentication systems, real-time fraud detection algorithms, and blockchain-based transaction verification mechanisms.

III. EXISTING SYSTEM

The existing system of Face PIN is a sophisticated biometric authentication system designed to enhance security and streamline the user authentication process at Automated Teller Machines (ATMs). The system analysis of Face PIN involves a detailed examination of its various components, functionalities, and operational processes, ensuring a comprehensive understanding of its requirements and capabilities. By conducting a systematic analysis of Face PIN, stakeholders can gain valuable insights into its functionality, usability, security, and performance characteristics.

Presently, ATM systems use no more than an access card which usually has a magnetic stripe (magstripe) and a fixed Personal Identification Number (PIN) for identity verification. Some other cases utilize a chip and a PIN which sometimes has a magstripe in case the chip fails as a backup for identification purposes.

PIN verification is combined with fingerprint recognition, to identify a customer during ATM transaction. Fingerprint is verified using efficient minutiae feature extraction algorithm. To assure the security while doing transaction through swipe machine, the client will confirm the transaction by an approval message through GSM technology. In both cases, location will be identified through GPS. If any illegitimate person tries to use the card it will automatically be blocked by the system and detail information will be sent to the customer through the message.

Biometrics measure the unique physical or behavioral characteristics of an individual as a means to recognize or authenticate their identity. Common physical biometrics include fingerprints, hand or palm geometry, and retina, iris, or facial characteristics .Biometrics may be used for identity establishment. A new measurement that purports to belong to a particular entity is compared against the data stored in relation to that entity. If the measurements match, the assertion that the person is whom they say they are is regarded as being authenticated.

IV. PROPOSED SYSTEM

This project proposes an automatic teller machine multi modal security model that would combine a physical access card and electronic facial recognition using Deep Convolutional Neural Network.

- **Facial Biometric Authentication System.**

Deep 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 than traditional machine learning methods.

Deep Face Recognition (DFR) 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 recognizes Whether the face is live or spoofed ,face processing is used to handle variations before training and testing, e.g., poses, ages, Different architectures and loss functions are used to extract discriminative deep feature wheN training, face matching methods are used to do feature classification after the deep features of testing data are extracted.

- **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.

V. METHODOLOGY

In the development and evaluation of the FacePIN project, focusing on the integration of facial recognition technology with deep learning algorithms to create a robust and secure biometric authentication system for ATM environments.

Based on the identified requirements, a detailed system design and architecture are developed, outlining the components, interfaces, and workflows of the FacePIN system. This includes defining the data flow, user interactions, and integration points with existing ATM infrastructure, as well as selecting appropriate technologies and algorithms for facial recognition and deep learning.

The methodology involves collecting a diverse dataset of facial images for training and testing the deep learning models used in the FacePIN system. This includes sourcing images from public datasets, as well as collecting real-world data through controlled experiments or collaborations with ATM operators. The collected data is then preprocessed to remove noise, standardize formats, and enhance the quality of facial images for training.

Deep learning models, such as convolutional neural networks (CNNs), are trained on the preprocessed dataset to learn facial features and patterns relevant to user authentication. This involves partitioning the dataset into training, validation, and testing sets, fine-tuning model parameters, and evaluating model performance using metrics such as accuracy, precision, recall, and F1-score.

The trained deep learning models are integrated into the FacePIN system, alongside other components such as user interfaces, database management systems, and communication protocols. This involves developing software modules, configuring hardware components, and ensuring seamless interoperability between different system elements.

The performance of the FacePIN system is evaluated using benchmarking tests and performance metrics, such as response times, throughput, and accuracy rates. Any identified bottlenecks or inefficiencies are addressed through optimization techniques, such as algorithmic optimizations, hardware upgrades, or system tuning.

The FacePIN project aims to develop and validate a state-of-the-art biometric authentication system that meets the highest standards of security, reliability, and usability for ATM users. Through a systematic approach to problem-solving, design, implementation, and evaluation, the FacePIN project seeks to contribute to the advancement of biometric authentication technologies and their application in real-world security environments.

VI. WORKING

The working of the FacePIN biometric authentication system involves a seamless integration of facial recognition technology with deep learning algorithms to authenticate users accessing ATM services. Initially, users initiate the authentication process by selecting a transaction type on the ATM interface. Subsequently, the system captures the user's facial biometric data using a standard camera integrated into the ATM.

The captured image is then processed using convolutional neural networks (CNNs) trained on a large dataset of facial images to extract unique facial features and patterns. The deep learning algorithms analyze these features to verify the user's identity against pre-registered biometric data stored in the system's database. Upon successful authentication, the user gains access to ATM functionalities, such as cash withdrawals or balance inquiries.

The entire authentication process is executed in real-time, ensuring prompt and secure access to ATM services while maintaining high accuracy and reliability. Through this innovative approach, the FacePIN system revolutionizes ATM security by providing a user-friendly, non-invasive, and highly secure authentication solution powered by advanced facial recognition technology and deep learning algorithms.

VII. CONCLUSION

Biometrics as means of identifying and authenticating account owners at the Automated Teller Machines gives the needed and much anticipated solution to the problem of illegal transactions. In this project, we have developed to proffer a solution to the much-dreaded issue of fraudulent transactions through Automated Teller Machine by biometrics and Unknown Face Forwarder that can be made possible only when the account holder is physically or far present. Thus, it eliminates cases of illegal transactions at the ATM points without the knowledge of the authentic owner.

Using a biometric feature for identification is strong and it is further fortified when another is used at authentication level.The ATM security design incorporates the possible proxy usage of the existing security tools (such as ATM Card) and information (such as PIN) into the existing ATM security mechanisms. It involves, on real-time basis, the

bank account owner in all the available and accessible transactions.

The FacePIN project exemplifies the potential of biometric authentication systems to revolutionize ATM security and user authentication processes. By combining cutting-edge technology with rigorous testing, implementation, and maintenance practices, FacePIN sets a new standard for ATM security, offering a secure, user-friendly, and reliable authentication solution for banking transactions in the digital age.

Looking ahead, continuous monitoring, maintenance, and improvement efforts will be crucial to ensuring the ongoing reliability, security, and performance of the FacePIN system. By staying abreast of emerging technologies, security threats, and user feedback, the FacePIN project team can continue to innovate and enhance the system to meet the evolving needs and expectations of users and stakeholders.

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 based on 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, "Raspberry Pi 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 system using RFID andIOTusingcloud"inProc.OnlineInt.Conf.GreenEng.Technol.(ICGET),Nov.2016, pp.1-4.