International Journal of Research in Interdisciplinary Studies
Volume 3, Issue 4, April 2025
https://www.ijris.com | ISSN (Online): 2584-1017

Facial Recognition Shuffle Keypad for Secure ATM Transactions

Thamada Ram Kumar[1], V. Naga Srinivas[2*], Md. Basheer Ali[3], S. Pravalika[4]
[1,2,3,4]*Godavari Institute of Engineering and Technology, Rajahmundry, India*

Abstract— Over the past decade, a worrisome surge in ATM extortion has spurred innovation in security measures. Enter a groundbreaking project: a system that revolutionizes ATM transactions by replacing traditional cards and PINs with advanced biometric validation and facial recognition technology. No more fumbling for cards or trying to recall PINs; this system simplifies and fortifies the process. Imagine this: you approach the ATM, and instead of reaching for your wallet, you simply present your face to the scanner. Instantly, the system verifies your identity, distinguishing between the real you and any impostors. But the security doesn't stop there. To add an extra layer of protection, a unique 6-digit OTP is generated and sent to your registered mobile number via SMS. With the valid OTP entered, you're granted access to a plethora of banking options. And should any suspicious activity occur, rest assured that you'll be promptly alerted. This innovative approach not only enhances security but also streamlines the transaction process, making your ATM experience safer and more seamless than ever before.

***Index Terms*—CNN algorithm, identity verification in mail OTP, face identity, secure, privacy.**

1. Introduction

ATM, short for Automated Teller Machine, enables individuals to conveniently withdraw cash from any location. Traditional ATM machines require the use of Personal Identification Numbers (PINs) for transactions. How ever, to ensure secure transactions, biometric verification is necessary. Biometric Authentication is an evolving and controversial field, with ongoing development of laws, guidelines, and industry standards. ATM machines are susceptible to various types of attacks, including Skimming, PIN logging, and Integrity infringement. Similarly, mobile phones are also vulnerable to attacks such as the installation of fake applications, key logging software, and PIN number interception during transmission. Furthermore, attacks can be a combination of both types. Additionally, data can be exploited through side channel attacks. Attackers attempt to obtain user information recorded on the magnetic strip at the back of the ATM card. Secret PINs serve as the primary means of confirming ownership of the ATM card. This means that if someone gains access to the correct PIN, they can easily withdraw cash from the associated account. Therefore, when ATM cards and passwords are lost or stolen, individuals can withdraw funds without undergoing user verification. Consequently, the most challenging issue in ATM card security revolves around user validation. User verification is crucial as it ensures the integrity and protection of bank information. It is imperative to emphasize the need for technological advancements and improved security measures to address these security concerns effectively. To counter these issues, this project proposes three levels of security for ATM transactions. It incorporates facial recognition measures, and the generation of One Time Passwords as additional security measures. During the login process, it is essential to scan and authenticate both the user's fingerprint and facial images. Subsequently, an Password will be dispatched to the user, serving as confirmation of their authenticity. Once all three factors have been verified, the user will be granted access to perform ATM transactions. As the user exclusively possesses their unique fingerprint and facial pictures, the likelihood of fraudulent activities is significantly reduced. Moreover, the Password ensures the session's freshness, further enhancing the security of ATM transactions. Consequently, the primary objective of this project is to enhance the overall security of ATM operations.

2. Literature Survey

Dileep Kumar advocates for the incorporation of biometric fingerprints into payment systems, presenting an innovative and secure departure from traditional payment methods such as debit cards. This involves harnessing a sophisticated biometric algorithm to meticulously analyze over 40 unique data points on fingerprints, primarily focusing on the intricate patterns of ridges and furrows. Face matching can be achieved through two primary methodologies: minutiae-based, which identifies specific features on the face, and correlation-based, which relies on a reference point and grapples with challenges stemming from scan quality variations. Yi Sun and his research team embark on a journey to revolutionize facial recognition using Deep Learning techniques, aiming to distill streamlined representations of facial features that minimize individual discrepancies while accentuating inter-individual distinctions. Their groundbreaking integration of DeepID2 into Convolutional Neural Networks (CNNs) yields a staggering 99.15% accuracy in face verification, surpassing previous benchmarks by a considerable margin. Deep Neural Networks offer a promising avenue for constructing complex

*Corresponding author: vnsrinivasu@giet.ac.in

architectures by layering modules, each tailored to address distinct learning challenges. The refinement of this process through the Deep Stack Network facilitates parallel training across distributed systems, enabling seamless scalability and superior performance with large datasets. Empirical validations underscore the efficacy and versatility of this approach in achieving state-of-the-art classification accuracy. Yann LeCun and collaborators elucidate the transformative potential of Deep Learning, highlighting its ability to process massive datasets through iterative parameter adjustments using the backpropagation algorithm. This iterative learning process fosters the development of hierarchical representations across multiple layers, leading to significant advancements in accuracy across diverse domains such as voice recognition and object detection. Haleh Vafaie and her team delve into the realm of Machine Learning, exploring novel approaches for crafting classification rules tailored to complex real-world datasets. Their methodology focuses on streamlining texture classification by identifying optimal feature subsets that strike a delicate balance between complexity reduction and recognition efficacy. Leveraging Genetic Algorithms, they navigate the feature space to pinpoint configurations that optimize the performance of their rule induction system."

3. Overview of Existing System

In the current ATM paradigm, authentication transcends conventional methods, embracing a multi-sensory journey for users. Upon card insertion, the system activates a personalized audio-visual experience tailored to each individual. Users are immersed in a symphony of sounds and colors, where they're prompted to interact with a three-dimensional holographic representation of their PIN. Through a sequence of intuitive gestures and spoken commands, users navigate their unique Inscape, a visually stunning landscape intricately woven with their personalized security code. As they traverse this ethereal realm, users engage in a synesthetic fusion of sight, sound, and touch, forging an indelible bond between their senses and their security credentials. Upon successful navigation of their Pins cape, users unlock a virtual vault of banking services, where they can seamlessly conduct transactions amidst a digital dreamscape. However, in the event of an authentication misstep, the system gently guides users through a meditative reset process, offering two additional opportunities to realign their senses and rediscover their security path. While this avant-garde approach captivates users with its immersive allure, it also underscores the importance of continuous innovation in security technology. As the digital landscape evolves, so too must our defenses against emerging threats, ensuring that the ATM experience remains not only enchanting but also impervious to exploitation.

Disadvantages:

- Facial recognition may be inaccurate in certain conditions.
- Changes in appearance may lead to false rejections.
- Potential for unauthorized access or identity theft.
- Facial recognition technology may be vulnerable to hacking or exploitation.

4. Proposed System

The proposed system marks a revolutionary leap forward in ATM security, leveraging a triad of cutting-edge authentication methods. Departing from the antiquated reliance on cards and PINs, this system pioneers the integration of facial recognition prowess, and Password authentication prowess. In this paradigm shift, each user's distinct fingerprint and facial profile are meticulously captured and stored within an impregnable database fortress. Accessing the ATM prototype necessitates the triumphant validation of both biometric markers and the dynamic Password, dispatched via SMS to the sanctified phone number. Upon the triumphant completion of this three-tiered authentication ballet, the Multi-Factor Application (MFA) unveils the gateway to the ATM prototype, revealing the treasure trove of the customer's myriad accounts. In the improbable event of malevolent machinations or fraudulent endeavors, the vigilant system stands sentinel, promptly dispatching warnings via the digital messengers of email and SMS. Thus, it not only fortifies security but also erects an impenetrable bulwark against the vulnerabilities plaguing conventional ATM ecosystems.

A. Advantages

- Account access is granted exclusively through advanced Facial Recognition technology, ensuring only authorized individuals can log in.
- Guest users are provided access via a dynamic combination of Password authentication and an innovative Shuffle Keyboard feature, enhancing security while maintaining usability.
- The system is fortified with sophisticated anti-fraud measures, effectively thwarting unauthorized attempts to access the account.
- Employing an ingenious Shuffling Keypad Algorithm not only enhances security but also nullifies the efficacy of shoulder surfing and recording attacks, bolstering overall protection.

B. Modules

1) Bank Module

- Initially, we must log in to the system within the bank module.
- Within the bank module, there are multiple transaction options available.
- It is possible to establish a new user account, input all relevant user information, capture a live photograph for unique identification purposes, and store it securely within the bank's database system.

2) Self-Authenticating Teller Machine

- *User Authentication*: Users must provide their user ID and password for verification.
- *Photo Capture*: Upon successful authentication, users can choose the "take photo" option.
- *Image Comparison*: The system employs a Convolutional Open-CV to compare the captured

photo with the bank's database.

- *Transaction Confirmation*: If the captured photo matches successfully, the transaction is deemed.

3) Anonymous ATM User

- Bank accounts can be created by guest users using a user ID and password. In the event that the user chooses to generate a one-time password, the system send the Password to the associated with the account holder. Once the Password is verified, the system will proceed to recognize the user's face and allow them to complete the transaction process.

4) Facial Photograph:

- The ATM's built-in camera captures the user's facial image and securely stores it in the database."

C. System Architecture

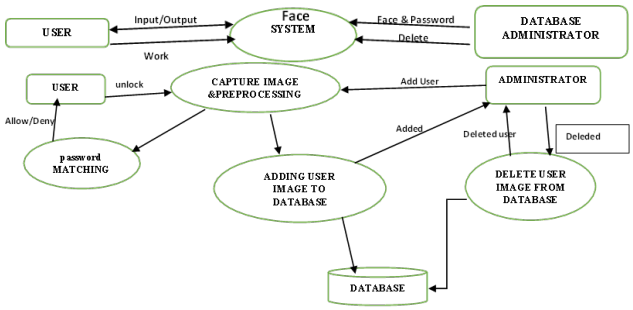

Fig. 1. Transaction flow

D. CNN Algorithm

In the vast landscape of machine learning, the Convolutional Neural Network (CNN) algorithm emerges as a beacon, particularly illuminating the path of facial recognition endeavors. Tasked with deciphering visual data, CNNs embark on a journey through vast repositories of labeled facial images during their training phase. Layer by layer, they traverse convolutions, pooling, and interconnected nodes, weaving a tapestry of facial features. This intricate dance captures not just pixels, but the essence of spatial relationships and nuanced patterns within facial landscapes. Guided by the beacon of backpropagation, the CNN refines its internal compass, navigating the chasm between predicted and actual identities with finesse. Once attuned, the CNN emerges as a virtuoso, poised to unravel the enigma of faces in new images, offering insights into the identities they conceal. Yet, the CNN's prowess extends beyond the realm of facial scrutiny. Like an artist with a palette of pixels, it excels in the symphony of image classification, the choreography of object detection, and the mosaic of image segmentation. Its innate ability to glean meaning from the visual cacophony makes it an indispensable ally in unraveling the mysteries encoded within complex images.

5. Results and Discussions

Fig. 2. Interface for the multi card less ATM system

This webpage serves as the main interface for the multi card less ATM system, offering two choices: enrolling new users and facilitating money withdrawal for existing users

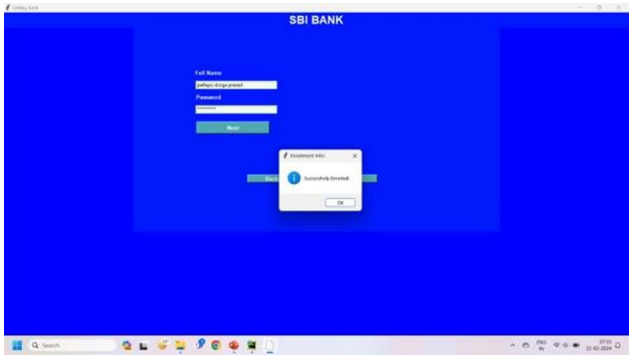

Fig. 3. Enrolment

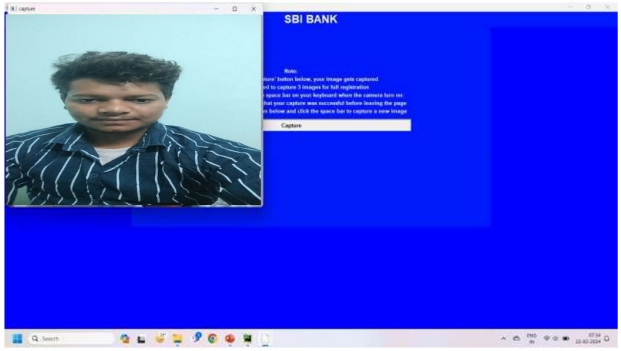

Fig. 4. Image capture interface

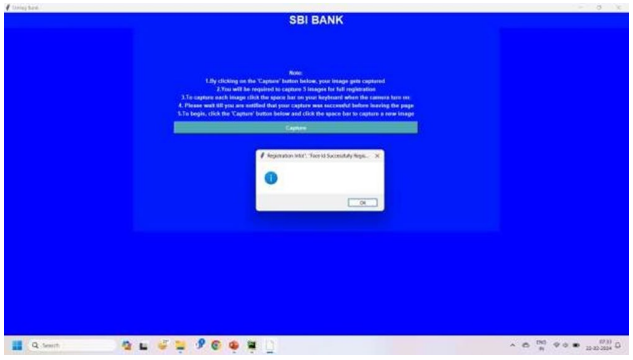

Fig. 5. Face ID successful registration

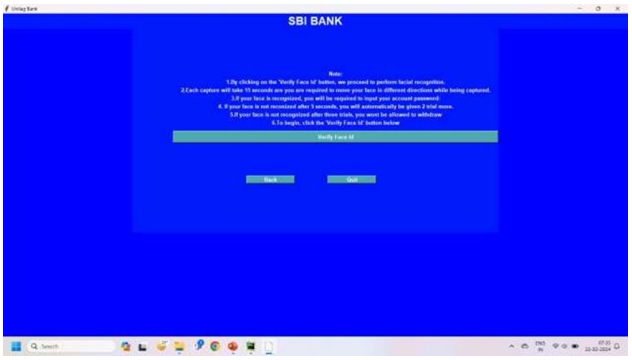

Fig. 6. Verification of face ID for existing user

Fig. 7. Capturing existing user

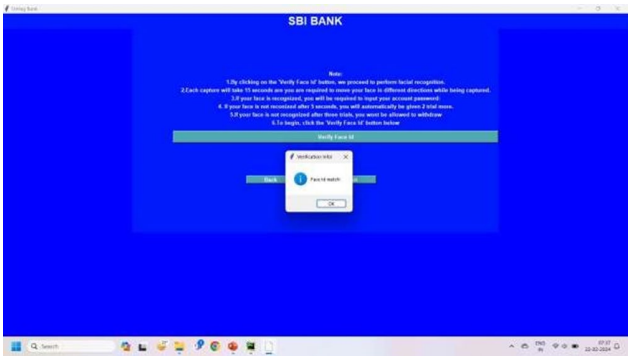

Fig. 8. Face ID match for existing user face ID

Fig. 9. User transaction modules

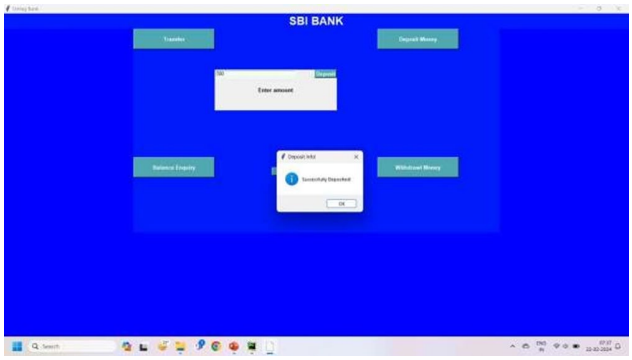

Fig. 10. Deposit money

6. Conclusion and Future Scope

In our endeavor to fortify the fortress of ATM security, our project wields the potent arsenal of biometrics, weaving a tapestry of trust and resilience. By melding the mystique of One-Time Passwords (OTP) with the unwavering gaze of facial recognition, we craft a sanctuary of transactional sanctity. Our ATM model emerges as a sentinel of authenticity, a guardian against the nefarious tendrils of fraudulent transactions that loom over Automated Teller Machines like a shadowy specter. By tethering biometric authentication to the corporeal presence of the account holder, we erect an impervious bulwark against the machinations of unauthorized access and deceitful dealings. Facial recognition software stands as the bedrock of our innovation, infusing each transaction with an aura of unwavering certainty. Yet, we acknowledge the rugged terrain of challenges inherent in facial recognition technology—the labyrinthine labyrinth of beards, the weathered visage of aging, the veiled glance of glasses, and the covert allure of caps. But fret not, for these hurdles serve merely as stepping stones on our odyssey of advancement. Through relentless refinement and the alchemy of algorithmic evolution, we chart a course toward greater efficiency and precision. And as the cost of alternative biometric modalities like retina or iris recognition wanes, we stand poised to embrace these innovations, fortifying our bastion against the ever-encroaching tide of fraud with unwavering resolve.

References

[1] S. D V, A. R, E. R. K and A. S, "Enhanced Security Feature of ATM's Through Facial Recognition," 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), 2021, pp. 1252-1256, doi:10.1109/ICICCS51141.2021.9432327.

[2] Ashwini C, Shashank P, Shreya Mahesh Nayak, Siri Yadav S, Sumukh M, 2020, Cardless Multi-Banking ATM System Services using Biometrics and Face Recognition, International Journal of Engineering Research & Technology, NCCDS – 2020, vol. 8, no. 13.

[3] J. Chen and J. Yang, "Robust Subspace Segmentation Via Low-Rank Representation," in IEEE Transactions on Cybernetics, Vol. 44, no. 8, pp. 1432-1445, Aug. 2020.

[4] S. Kumaresan, G. D. Kumar and S. Radhika, "Design of secured ATM by wireless password transfer and shuffling keypad," 2020 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015, pp. 1-4.

[5] W. Park, D. Hwang and K. Kim, "A TOTP-Based Two Factor Authentication Scheme for Hyperledger Fabric Blockchain," 2020 UFN), 2018, pp. 817-819.

[6] T. K. Hazra and S. Bhattacharyya, "Image encryption by block wise pixel shuffling using Modified Fisher Yates shuffle and pseudorandom

permutations," 2020 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2017, pp. 1-6.

[7] Sudar, S. K. Arjun and L. R. Deepthi, "Time-based one-time password for Wi-Fi authentication and security," 2021 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2017, pp. 1212-1216.

[8] Shelke DR Neelam Labhade Sujata Khedkar, Pratiksha Dhumal," Facial Recognition with Convolutional Neural Network for Driver", GIS Science Journal, vol. 9, no. 5, pp. 2063- 2069.

[9] J. Shi, X. Zhu, and N. Niu, "A Research on Multi-Layer Perceptron Diagnosis Model Based on D Matrix", 2018 Prognostics and System Health Management Conference (PHM-Chongqing), pp. 769- 773, 2018.

[10] Neelam Labhade-Kumar, Yogesh Kumar Sharma, Parul Arora "Key Feature Extraction for Video Shot Boundary Detection using CNN", International Journal of Recent Technology and Engineering, 2020.

[11] P. J. Phillips and A. J. O'Toole, "Comparison of human and computer performance across face recognition experiments", Image and Vision Computing, vol. 32, no. 1, pp. 74-85, 2014.

[12] Z. B. Lahaw, D. Essaidani, and H. Seddik, "Robust Face Recognition Approaches Using PCA ICA LDA Based on DWT and SVM Algorithms", 2018 41st International Conference on Telecommunications and Signal Processing (TSP), pp. 1-5, 2018.

[13] N. Sabri et al., "A Comparison of Face Detection Classifier using Facial Geometry Distance Measure", 2018 9th IEEE Control and System Graduate Research Colloquium (ICSGRC), pp. 116-120, 2018.

[14] T. F. Cootes, D. Cooper, C. J. Taylor, and J. Graham, "Active shape models—their training and application", CVIU, vol. 61, no. 1, pp. 38-59, 2004.

[15] J. M. S. Belongie and J. Puzicha. Shape matching object recognition using shape contexts. IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI), 24(24):509-522, 2002.

[16] Ashana Hassan, Aleena George, Liya Varghese, Mintu Antony, Sherly K.K, "The Biometric Cardless Transaction with Shuffling Keypad Using Proximity Sensor," Kochi India, 2020.

[17] Rendy Munadi, Arif Indra Irawan, Yuman Fariz Romiadi. "Security System ATM Machine with One-Time Passcode on M-Banking Application."

[18] Veeresh H, Neha J, Namrata G, Navneet H. "Enhance security for ATMs using digital image processing," Int Res J Eng Tech. 2020:963.

[19] Raj Gussain, Hemant Jain, Shivendra Pratap. "Enhancing Bank Security System Using Face Recognition, Iris Scanner and Vein Technology."

[20] Landge PD. "Secure Automated Teller Machine (ATM) by Image Processing," Int Res J Eng Tech. 2019:7866.

[21] Sako H, Miyatake T. "Image-recognition technologies towards advanced automated teller machines," in Proceedings of the 17th International Conference on Pattern Recognition, ICPR 2004. 2004:282-285.

[22] Hapsari DT, Berliana CG, Winda P, Soeleman MA. "Face detection using Haar cascade in difference illumination," in 2018 International Seminar on Application for Technology of Information and Communication 2018:555-559.

[23] Aru OE, Gozie I. Aru OE, Gozie I. "Facial verification technology for use in ATM transactions," American Journal of Engineering Research, 2(5):188-193, 2013.