International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 05 | May - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

THE REAL TIME HIGH PRECISION CRIMINAL FACE RECOGNITION FOR ATM SECURITY IN DEEP LEARNING

V.GOKULAKRISHNAN [1], PARAMESHWARAN.V[2], SANJAY PRASATH.S[2], SANJAY S [2], SANTHOSH R [2]

1. **Department of CSE Assistant Professor, Dhanalakshmi Srinivasan Engineering College, Perambalur.**

2. **Final year CSE, Dhanalakshmi Srinivasan Engineering College, Perambalur.**

ABSTRACT: The proposed ATM security system, utilizing composable deep face recognition, emphasizes user protection during transactions with a specific focus on eye retina accuracy. In the event of a potential threat identified through real-time face detection and tracking, an automatic alert is initiated. Prioritizing precision, the system employs advanced face detection algorithms for accurate location and tracking, even in dynamic scenarios. A down sampling technique ensures efficient processing of facial data, crucial for meticulous identification in crowded ATM locations. The integration of a face tracking ID unit enhances accuracy, providing continuous monitoring and persistence in identification, particularly focusing on the distinctive patterns in the eye retina. The scoring method, rooted in face tracking and embedding distance, significantly elevates user identification reliability, minimizing the risk of false positives, especially in criminal identification based on unique eye retina features. In response to potential threats, the system promptly generates automatic alerts and dispatches secure emails to relevant entities, including the affected card user, the respective bank, and cybersecurity authorities. These emails include comprehensive information, such as a high-precision image of the detected criminal's face, detailed facial recognition data, and a thorough summary of their known criminal history. This accuracy-driven and retina focused approach enhances safety, emphasizing continuous refinement and adherence to privacy and ethical considerations during implementation.

KEYWORDS: Crime prevention, down-sampling, face recognition.

1.INTRODUCTION:

Automated Teller Machines (ATMs) have become an indispensable part of our modern financial infrastructure, enabling convenient access to cash and account management. However, the security of these ubiquitous machines remains a critical concern. Traditional authentication methods relying solely on physical cards and Personal Identification Numbers (PINs) have proven susceptible to various forms of fraud and theft. Stolen cards, skimmed information, and compromised PINs through social engineering or shoulder surfing leave user accounts vulnerable. These limitations necessitate the exploration of more robust and secure authentication methods for ATMs. This paper delves into the potential of deep learning, a subfield of artificial intelligence, to revolutionize ATM security through real-time, high-precision criminal face recognition. Deep learning algorithms excel at identifying complex patterns within vast amounts of data. Convolutional Neural Networks (CNNs), a prominent deep learning architecture, have demonstrated remarkable success in facial recognition tasks. CNNs can extract intricate features from facial images, including geometric contours, distances between key landmarks (eyes, nose, mouth), and even subtle variations in texture and skin tone. This ability to analyze intricate facial characteristics allows for robust identification even under challenging conditions, such as variations in lighting, pose, and facial expressions.

Fig-1 ATM

2.RELATED WORK

X. Pan et.al,.[1] proposes a novel approach to access control systems by combining Radio Frequency Identification (RFID) technology with Fuzzy Neural Networks (FNN) for face recognition. Traditionally, access control systems rely on methods like key cards or PINs, which can be lost, stolen, or compromised. Pan's system addresses these limitations by introducing a two-factor authentication process. First, users present an RFID card for identification. Then, the system captures a live facial image and utilizes FNNs to analyze the facial features for verification. FNNs, a type of artificial neural network, are adept at handling imprecise data, making them suitable for facial recognition tasks despite potential variations in lighting, pose, or facial expressions. Pan's research highlights the potential benefits of integrating FNN-based face recognition with RFID technology for access control systems. This combined approach offers enhanced security compared to traditional methods and could be applicable in various settings requiring strict access control, such as secure facilities, data centers, or high-value storage areas.

Li, Shan, et.al,.[2] and Gao propose a novel approach to address this issue. They frame the problem of face recognition under pose variations as a regression task. By viewing facial representations through this lens, they introduce a regressor that leverages a "coupled bias-variance tradeoff." This approach aims to strike a balance between the bias and variance of the regression model for different facial poses. The authors argue that controlling variance, which can be high due to pose differences, is crucial for accurate recognition. Ridge regression and lasso regression, two established techniques, are explored within this framework to achieve the desired bias-variance tradeoff. Experimental results on benchmark face databases demonstrate that the proposed method significantly improves recognition performance compared to traditional approaches. This research sheds light on the importance of considering the statistical properties of pose variations in face recognition and paves the way for further exploration of regression-based techniques for robust cross-pose face recognition.

H.S. Bhatt, et.al,.[3] tackle a growing challenge in face recognition: identifying individuals who have undergone facial surgery. Traditional face recognition algorithms often struggle when presented with pre- and post-surgery images of the same person due to significant changes in facial features. The authors propose a novel approach using a multi objective evolutionary algorithm. This algorithm works by dividing the face image into smaller regions, or "granules," at various levels of detail. It then analyzes these granules using feature extraction techniques and assigns weights to each region based on its importance for identification. The algorithm essentially "evolves" by optimizing these feature extractors and weight assignments simultaneously, aiming to achieve the best possible recognition accuracy even with surgically altered faces. Experimental results on a database of surgically altered faces demonstrate that the proposed multi objective evolutionary algorithm outperforms existing algorithms and even a commercial face recognition system. This research holds promise for improving the robustness of face recognition technology in scenarios where facial modifications might be used to evade identification.

Mohamed El Amine Ouis, et.al,.[4]explore the potential of facial recognition technology for access control systems. Traditional methods like key cards or PINs have limitations - they can be lost, stolen, or even guessed. This research investigates a more secure approach: using automated face recognition to verify a user's identity. The authors propose a system that utilizes cameras to capture a user's face and then employs algorithms to compare it against a pre-existing database of authorized individuals. This real-

time verification process offers several advantages. It eliminates the need for physical tokens like cards, reducing the risk of loss or theft. Additionally, facial recognition is inherently unique to each individual, potentially offering a more secure authentication method compared to PINs. The paper likely delves into the specific algorithms used for face detection and recognition, potentially including techniques like Principal Component Analysis (PCA) or Linear Discriminant Analysis (LDA). The authors also likely discuss the system's implementation details, such as camera placement and computational requirements.

Ding, Xu, et.al,.[5] propose a novel approach using a multi-task learning framework. This framework tackles two tasks simultaneously: (1) face detection and (2) pose-invariant face recognition. By learning these tasks together, the system can extract more robust facial features that are less affected by pose variations. Here's how it might work: The system first attempts to locate the face within the image using face detection techniques. Then, it analyzes the detected face to estimate its pose (frontal, tilted, etc.). Crucially, this pose information is used not only to account for the pose variation but also to guide the feature extraction process. This joint learning approach helps the system identify features that are most discriminative for recognizing individuals regardless of their head orientation.

3. EXISTING SYSTEM

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. A QR code scanner is required to detect code and decrypt information in stored in QR code. Scanner need to be installed in the ATM machine to take input credentials from the user. We will provide extra feature to an existing system, so traditional withdrawing option is also there. On other end, ATM machine will scan the QR code generated by 'Get Note'- android application and decrypt it with the key stored in the database. After decryption ATM will get required credentials such as card number, amount, pin, cvv number on card etc. It will authenticate all the details with the banks database. After successful authentication, cash will be dispensed by the ATM machine. 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.

4. 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. The proposed methodology for the project involves leveraging face recognition technology to enhance ATM transaction security and mitigate unauthorized access. The motivation behind this project stems from the increasing need for robust security measures in financial transactions, particularly at ATMs, where traditional methods like PINs and passwords are susceptible to breaches. By integrating deep learning-based Convolutional Neural Network (CNN) algorithms, the system aims to detect and capture images of unknown individuals attempting to access an ATM using an ATM card that isn't linked to their account. Upon detection, an image of the unknown person is generated and forwarded to the ATM account holder's email for verification. The account holder then has the option to either accept or reject the link associated with the image. In the event of rejection, a complaint is automatically sent to cybercrime and bank sectors for further investigation. This innovative approach not only bolsters ATM security by employing biometric authentication but also facilitates swift action against potential security threats through automated reporting and verification processes.

5. SYSTEM ARCHITECTURE

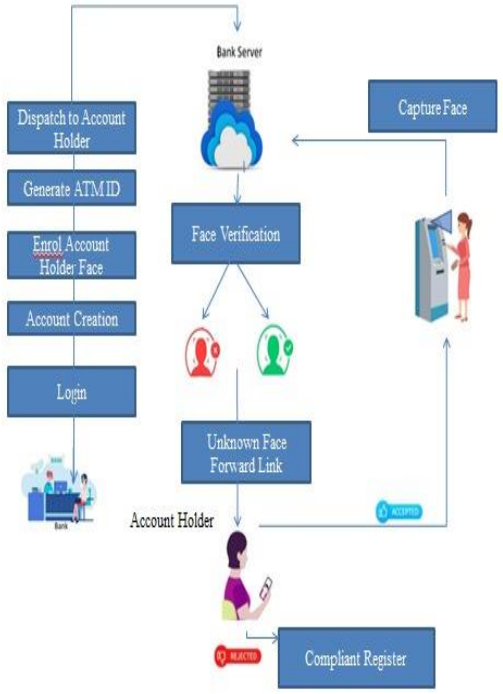

Fig -2 System Architecture

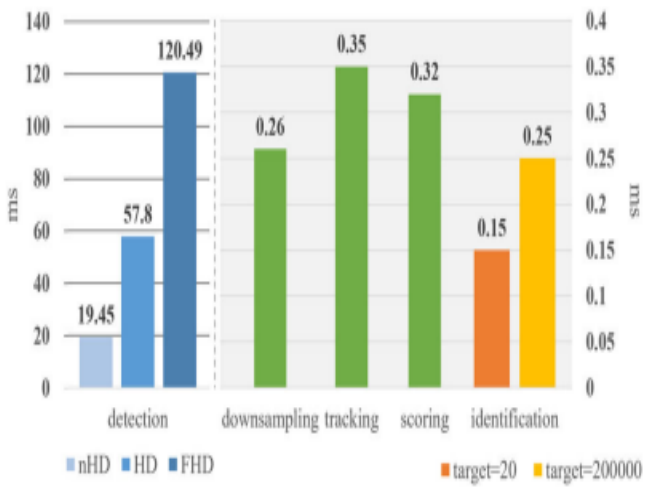

Fig -3 Comparison of processing latency

5.1 CRIME PREVENTION

The marriage of deep learning and real-time, high-precision criminal face recognition in ATMs presents a significant leap forward in crime prevention. This technology discourages criminal activity at its source. The potential for real-time identification of known criminals deters them from even attempting illegal transactions at the ATM. Furthermore, the system can trigger immediate alerts to authorities upon recognizing a suspicious face, allowing for swift apprehension before a crime occurs. By preventing unauthorized access through facial recognition, fraudulent transactions plummet, protecting both financial institutions and users. This enhanced security can also foster greater user confidence, encouraging wider ATM usage. However, it's vital to acknowledge the need for continuous improvement and responsible implementation to address potential biases and privacy concerns. Overall, this deep learning-powered approach has the potential to create a safer and more secure environment for everyone involved.

5.2 DOWN SAMPLING

While deep learning excels at recognizing facial patterns, processing high-resolution images in real-time for ATM security can be sluggish. Down-sampling techniques bridge this gap. By strategically reducing the image size (number of pixels), down-sampling allows the deep learning model to process information faster, crucial for real-time identification. Additionally, it minimizes memory consumption, beneficial for resource-constrained ATM environments. However, there's a trade-off: down-sampling can discard valuable details, potentially impacting recognition accuracy. Common down-sampling techniques include pooling layers within the deep learning architecture itself, or simply resizing the image beforehand. Finding the right balance between processing speed and information preservation is key for achieving real-time, high-precision criminal face recognition in ATMs.

Fig- 4 Down Sampling

5.3 FACE RECOGNITION

Deep learning acts as the brain behind real-time, high-precision criminal face recognition for ATM security. Convolutional Neural Networks (CNNs) are the star players here. Imagine them as a team analyzing faces piece by piece. Early layers identify basic shapes like edges and eyes, while later layers combine this information to recognize more complex features like a unique nose structure or wrinkle patterns. This intricate feature extraction allows for robust identification even under challenging conditions like different lighting, poses, or expressions. Deep learning's secret weapon? Massive amounts of data. By training on a vast database of labeled faces, the system learns to distinguish subtle variations and generalize this knowledge to identify even unseen criminals. The real-time aspect is crucial. Deep learning models are constantly being optimized for speed, allowing for near-instantaneous analysis of live facial images captured at the ATM and comparison against the criminal database. However, it's important to remember that this technology is still under development.

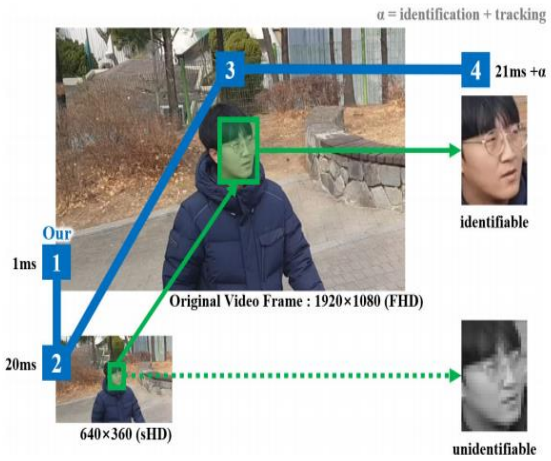

Fig -5 Face Recognition

6.RESULTS

Fig -6 User Details

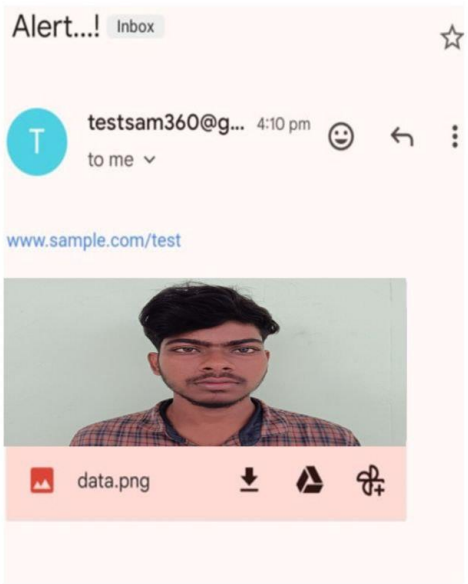

Fig -7 Alert Message

7.CONCLUSION

The implementation of a face recognition-based ATM transaction security system, coupled with the capability to detect and capture unknown persons attempting to misuse ATM cards, is a proactive solution addressing growing concerns of financial fraud and unauthorized access. Motivated by the imperative to enhance security measures in banking transactions, the project harnesses deep learning, specifically CNN algorithms, to accurately identify individuals during ATM interactions. By integrating face recognition technology, potential threats are mitigated through immediate detection of unfamiliar faces attempting to access accounts. Furthermore, the incorporation of an automated notification system, linking captured images of unknown persons to account holders' emails, empowers users to validate transactions and promptly report suspicious activities. This approach not only fortifies security but also fosters a collaborative effort between users and banking institutions in combating cybercrime. Ultimately, the project's two-pronged approach ensures heightened security and instills confidence among ATM users, contributing to a safer banking environment.

8.REFERENCES

[1] 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.

[2] Li, S. Shan, andW. Gao, ``Coupled bias-variance tradeoff for cross-pose face recognition," IEEE Trans. ImageProcess., vol. 21, no. 1, pp. 305-315, Jan. 2012.

[3] H. S. Bhatt, S. Bharadwaj, R. Singh, and M.Vatsa, ``Recognizing surgically altered face images using multi objective evolutionary algorithm," IEEE Trans. Inf. Forensics Security, vol. 8, no. 1, pp. 89-100, Jan. 2013.

[4] Taleb, M. E. Amine Ouis, and M. O. Mammar, ``Access control using automated face recognition: Based on the PCA & LDA algorithms," in Proc. 4th Int. Symp. ISKO-Maghreb, Concepts Tools Knowl. Manage. (ISKO- Maghreb), Nov. 2014, pp. 1-5.

[5] 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.

[6] J. Yang, Z. Lei, D. Yi, and S. Li, ``Person-specific face antispoofong with subject domain adaptation," IEEE Trans. Inf. Forensics Security, vol. 10, no. 4, pp. 797-809, Apr. 2015.

[7] T.R.Lekhaa, “Secured credit card transaction using web cam” International Research Journal of Engineering and Technology, April 2016.

[8] J. Liang, H. Zhao, X. Li, and H. Zhao, ``Face recognition system based on deep residual network," in Proc. 3rd Workshop Adv. Res. Technol. Ind. (WARTIA), Nov. 2017, p. 5.

[9] Wazwaz, A. O. Herbawi, M. J. Teeti, and S. Y. Hmeed, ``Raspberry Pi and computers-based face detectionand recognition system," in Proc. 4th Int. Conf. Comput. Technol. Appl. (ICCTA), May 2018, pp. 171-174.

[10] Had, S. Benouar, M. Kedir-Talha, F. Abtahi, M. Attari, and F. Seoane, ``Full impedance cardiography measurement device using raspberry PI3 and system-on-chip biomedical instrumentation solutions," IEEE J. Biomed. Health Informat., vol. 22, no. 6, pp. 1883-1894, Nov. 2018.

[11] A.Kowshika,” Least mobility high power (LMHP) dynamic routing for QoS development in Manet” WirelessPersonal Communications, Springer US, March 2019.