DEEP LEARNING CONVENTIONAL NEURAL NETWORK-BASED FACE BIOMETRIC VALIDATION SYSTEM FOR ATM

[1]C.Rathnakumar, [2]R.Kavin Kumar, [3]S.Prasath
[1]Associate Professor, MCA Department, Paavai Engineering College, Namakkal, Tamil Nadu
II MCA, Paavai Engineering College, Namakkal, Tamil Nadu

Abstract :Automated Teller Machines (ATMs) have become a ubiquitous part of modern life, used by individuals from all walks of life. However, the increasing number of criminals and their activities have made ATM security a pressing concern. Currently, ATM systems rely on access cards and Personal Identification Numbers (PINs) for identity verification, which can be vulnerable to exploitation. To address this issue, there have been significant advancements in biometric identification techniques such as fingerprinting, retina scanning, and facial recognition.To improve ATM security, this paper proposes a model that combines a physical access card with electronic facial recognition technology utilizing Convolutional Neural Networks . The integration of these two technologies would ensure that both the face and account of the user are protected from unauthorized access. In addition, to remotely verify the identity of an unauthorized user, a Face Verification Link will be generated and sent to the account owner through dedicated Artificial Intelligence agents.This proposal recognizes that human biometric features are difficult to replicate and seeks to provide a solution to the problem of account safety by ensuring that only the rightful account owner has access to their accounts.

Keywords: ATM, Biometrics, CNN, Face Recognition

I. INTRODUCTION

One of the most useful developments in the banking industry is the Automated Teller Machine, or ATM. ATMs permit banking clients to profit fast self-overhauled exchanges, like money withdrawal, store, and asset moves. People can conduct financial transactions without the assistance of a real teller thanks to ATMs. Likewise, clients can benefit banking administrations without visiting a bank office. Most ATM exchanges can be profited with the utilization of a charge or Mastercard. Some transactions do not require a credit or debit card. ATM Fakeness happening in the general public has become exceptionally normal these days. Skimming and Catching of the ATM gadgets have been planned by numerous Robbers. Shoulder Surfing Attack: unauthorized use of ATM cards by someone other than the owner. As a result, the creation of such a system to safeguard customers from fraud and other security breaches is urgently required. Face recognition is a tool for users to verify the card owner and can be used to secure ATM transactions. Banks face a significant issue in the form of financial fraud, and the current secure information stored on the magnetic tape of ATM cards is highly susceptible to theft or loss. By involving face acknowledgment as a device for validating clients in ATMs can be affirmed as the card proprietor. Process for logging into an ATM with a Face-Based ID ATMs with face recognition technology are able to recognize a person's face during a transaction. ATMs will automatically warn cardholders to exercise caution whenever "Shoulder Surfers" attempt to peek over the cardholder's shoulder to obtain his PIN when the cardholder enters it. In the event that the client wears a veil or shades, the ATM will won't serve him until the covers are eliminated.
Touchless: Passwords don't need to be remembered. Just taking a gander at the ATM camera will login the card holder in a split second. There is no need for physical contact.
Secure: Since your face serves as your

password, you won't have to worry about it being lost or stolen. In addition, the card holder's access to the account and transaction pages is locked by the face recognition engine when the card holder moves away from the ATM's camera and another face appears. Along with the ATM PIN, face-based cardholder authentication can be used as a primary or secondary authentication method. Fake cards, stolen PINs, and even the stolen card itself can't be used to commit ATM fraud with face-based authentication. Liveness-detection technology, which identifies and blocks the use of photographs, videos, or masks during the verification process, is one of the security features embedded in face verification to prevent fraud. This proposed work aims to improve banking security by proposing a partnership between a Face Recognition System and an unknown face forwarder URL for authentication. The system is proposed to prevent a variety of criminal acts and unauthorized access in order to increase ATM security. To Forestall unapproved access utilizing Face check Connection. To forestall robbery and other crimes

II. RELATED WORK

The following steps using for Face Recognition

(a) Register the Face:

Registering a few frontal faces of Bank Beneficiary templates is the first step in this module. These layouts then, at that point, become the reference for assessing and enlisting the formats for different stances: shifting up/down, drawing nearer/further, and turning left/right.

(b) Capturing Face image:

The ATM should have cameras set up to record relevant video. Webcam is used here to interface the computer and camera.

(c)Frame Removal: Outlines are extricated from video input. The video must be broken up into a series of images that are then processed further. The speed at which a video should be separated into pictures relies upon the execution of people. We can conclude that 20 to 30 frames are typically taken per second and sent to the subsequent phases.

(d)Pre-processing: Face Picture pre-handling are the means taken to organize pictures before they are utilized by model preparation and deduction. The next steps are as follows:

Thusly, in this module, Area Proposition Organization (RPN) produces returns for money invested by sliding windowson the component map through secures with various scales and different viewpoint proportions. Face location and division strategy in light of further developed RPN. RoIAlign faithfully preserves the exact spatial locations, and RPN is used to generate RoIs. These are liable for giving a predefined set of bouncing boxes of various sizes and proportions that will be utilized for reference while first foreseeing object areas for the RPN.

(i) Face Image Segmentation Using the Region Growing (RG) Method This section discusses the region growing method and recent related research.

RG is a straightforward technique for segmenting images based on region seeds. It is likewise delegated a pixel-based picture division strategy since it includes the determination of introductory seed focuses. Based on a set of conditions, this method of segmentation looks at the pixels that are adjacent to the initial "seed points" and decides whether or not those pixels should be added to the region. The "intensity" constraint is all that is used to examine the neighboring pixels in a conventional method for growing a region. A limit level for power esteem is set and those neighbor pixels that fulfill this edge is chosen for the district developing.

(ii)RPN A Region Proposal Network, or RPN, is a fully convolutional network that predicts both object bounds and objectless scores at each position simultaneously. The RPN receives comprehensive training to produce high-quality region proposals. Each feature (point) in the CNN output is referred to as an Anchor Point, and it operates on the feature map.

III. FEATURE EXTRACTION

The face image is fed into the feature extraction module following face detection to identify the most important characteristics that will be used for classification. The eyes, nose, and mouth information from each pose is automatically extracted, and its relationship to the frontal face templates is used to calculate the effects of the variation.

Face Image Features

(i) Head

- Forehead height is the separation

between the tops of the eyebrows and the tops of the forehead.

- Middle Face Height: the distance between the nose tip and the top of the eyebrows.
- Lower Face Height: the distance between the chin's base and the tip of the nose.
- Jaw Shape: A number used to categorise various jaw shapes. If you utilise face shape recognition, you can replace this number; for details, see (this) notebook.

(ii) Eye

- Left Eye Region
- Right Eye Region
- Eye to Eye Distance: The separation between the eyes' closest points
- Eye to Eyebrow Distance: Which side of the face is more directed towards the screen determines the distance between the eye and the eyebrow (left or right).
- The distance between the eyebrows, measured horizontally.
- Eyebrow Shape Detector 1: To distinguish between (Straight | Non-straight) eyebrow shapes, measure the angle between three places (eyebrow left edge, eyebrow centre, and eyebrow right edge).
- Eyebrow Shape Detector 2: This indicator uses a number to distinguish between (Curved | Angled) eyebrow shapes.
- Eyebrow Slope
- Eye Slope Detector 1: A technique for determining the eye's slope. it is the angle between the centre and edge points of the eye. Three different types of eye slopes—upward, downward, and straight—are represented by this detector.
- Eye Slope Detector 2: This tool helps determine the angle of the eye. it is the difference between the eye's centre and edge points on the Y axis. This detector is not a'mathematical' slope; rather, it is a number that can be divided into three different eye slopes (Upward, Downward, Straight).

(iii)

- Length of nose
- Nose Width: the width of the nose's lowest portion
- Nose Arch: The angle at which the nose's lower border curves (a longer nose has a wider curve, a smaller angle).

(iv)

- Upper Lip Height
- Lower Lip Height

IV. FACE IDENTIFICATION AND VERIFICATION

During the enrollment process, DCNN algorithms were developed to automatically recognise and reject inappropriate face photos. This will guarantee appropriate enrollment and, as a result, the optimum performance.By adding the convolved grid of a vector-valued input to the kernel with a bank of filters to a specific layer, the CNN generates feature maps. The activations of the convolved feature maps are then computed using a non-linear rectified linear unit (ReLU). Local response normalisation, or LRN, is used to normalise the new feature map that the ReLU produced. Spatial pooling (maximum or average pooling) is used to further compute the result of the normalisation. Then, some unneeded weights are initialised to zero using the dropout regularisation approach, and this process often happens within the fully linked layers before to the classification layer. In the fully connected layer, classification of picture labels is done using the softmax activation function. The face detection module receives the facial image after it has been taken by the ATM Camera. This module finds areas of an image where people are most likely to be present. Following face recognition using the Region Proposal Network (RPN), the feature extraction module uses the face image as input to identify the most important features that will be used for classification. A very brief feature vector that accurately depicts the facial image is created by the module. The face image's retrieved features are compared with those kept in the face database in this case using DCNN and a pattern classifier. After that, the face image is categorised as known or unknown. If the image face is recognised, the appropriate Card Holder is found, and the next step is taken.

V. RESULT & CONCLUSION

The much-needed and much awaited answer to the issue of unauthorised transactions is provided by biometrics as a method of identifying and validating account owners at the

Automated Teller Machines. The goal of this research is to propose a solution to the dreaded problem of fraudulent transactions made feasible only by the account holder being physically present or remotely present at an automated teller machine using biometrics and an unknown face forwarder. As a result, it ends instances of unauthorised transactions at ATM locations without the genuine owner's awareness.

The strength of using a biometric feature for identification is increased when another is utilised at the authentication level.The ATM security architecture takes into account the potential proxy usage of the already in place security instruments (such as ATM Cards) and data (such as PINs). It involves the owner of the bank account in all accessible and available transactions in real time.

REFERENCES

[1] 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.

[2] 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.

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

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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