Multimodal Biometric ATM Substantiation Using Face and Fingerprint Acknowledgement

Dr. S.M. Uma[1], Ms. S. Abikayil Aarthi[2,] Ms. N. Dhamayandhi[3], Ms. M. Kavitha[4]
[1]*Professor, Kings College of Engineering, Punalkulam*
[2,3,4] *Assistant Professor, Kings College of Engineering, Punalkulam*

***Abstract*—With the growing demand for enhanced security measures in the banking sector, the utilization of biometric authentication systems has gained prominence. Automated Teller Machines also known as ATM's are widely used nowadays by each and everyone. There is an urgent need for improving security in banking region. Due to tremendous increase in the number of criminals and their activities, the ATM has become insecure. ATM system today uses no more than an access card and PIN for identity verification. The recent progress in biometric identification techniques, including finger printing, retina scanning, and facial recognition has made a great effort to rescue the unsafe situation at the ATM. This project proposes and automatic teller machines security model that would combine a physical access card and electronic facial recognition using Deep Convolutional Neural Network. If this technology becomes widely used, faces would be protected as well as their accounts. Face verification linkwill be generated and sent to user to verify the identity ofunauthorized user through some dedicated artificial intelligent agents, for remote certification. However, it obvious that man's biometric features cannot be replicated, this proposal will go a long way to solve the problem of Account safety making it possible for the actual account owner alone have access to his accounts.**

***Index Terms*—ATM security, biometric authentication, facial recognition, deep convolutional neural network, account safety**

I. INTRODUCTION

Automated Teller Machines, or ATMs for short, are one of the most helpful innovations in the banking industry. They enable customers to quickly complete self-servicedtransactions, including cash withdrawals, deposits, and fund transfers. They also allow people to access banking services without physically visiting a bank branch. The majority of ATM transactions require the use of a debit or credit card, though some do not [26], [27]. As a result, the face recognition portion of this study employs PCA and LDA and, consequently, the Intelligence RFID The binary tree search algorithm is used by the access control portion. The system's overall architecture is shown first, followed by the specific identity authentication techniques. The access system's methodology is described in detail, along with the outcomes and conclusions of the final experiment. technologies present a viable way to deal with worriesabout ATM security and stop fraud. The project's goal is to implement an effective and safe authentication system that safeguards customers' financial interests and fosters confidence in banking offerings.

II. LITERATURE SURVEY

1. Title: Futuristic Banking: Streamlining ATM Transactions with Fingerprint and Contactless Authentication
Authors: A. Essaki Muthu; A. Justin Diraviam
Description:
Although there have historically been security concerns with card-based transactions, automated teller machines (ATMs) are a major component of modern banking. This study suggests fingerprint technology and Near-Field Communication (NFC) card emulation as safe substitutes for ATM cash transactions. NFC Card Emulation makes it possible to send and receive secure data across short distances, which is perfect when managing sensitive data. Fingerprint technology is suggested as an extra security measure to boost security during authentication. Physical cards or NFC tags are not necessary for user authentication when fingerprint sensors are used. This connection provides an even higher degree of protection for the authentication procedure than the existing card-based method used

in ATMs. By doing away with real cards, the technology improves security and reduces dangers like ATM manipulation and magnetic strip damage.With the increasingeffectiveness and security of authentication, ATM transactions are assured of a high degree of protection. By combining NFC Card Emulation with fingerprint technology,this innovative approach improves ATM security and offers consumers a smooth and secure banking experience.
Advantage: Enhanced Easily Accessible
Disadvantage: Technical malfunctions.

2. Title: ATM Assisting Device for Secure Transactions usingGSM Technology
Authors: Kalirajan K; Suganya D N
Description:
Hackers frequently target automated teller machines (ATMs) in an attempt to gain personal identification numbers (PINs) and card information from users by using skimmers. A unique ATM security system that uses a vibrator to create a temporary password is presented as a solution to this problem. Every time the money is withdrawn,the consumer must input this temporary password on top of their regular PIN. It is assured that the temporary password is distinct and difficult to duplicate by employing vibrator to generate it. A hacker cannot access the cash without providing the temporary password, which is only good for a short period of time, even if they manage to get their hands on it together with the customer's regular PIN. Additionally, the suggested system is made to recognize and notify the owner in the case that something is stolen. The device will trigger a warning and automatically close the shutter if the temporary password is entered wrong more than once. This will alert the owner to the attempted theft and stop the criminal from getting to the cash. The suggested approach includes a system to notify the police in the event of theft, significantly enhancing security. The cash is kept safe until the authorities come because once the shutter is closed, only authorized individuals, like the police, may open it.
Advantage: Monitoring Transactions in Real Time
Disadvantage: possibility of mobile network
Problems
. 3. Title: Third Generation Security System for Face
Detection in ATM Machine Using Computer Vision
Authors: S Sridevi; K.M. Monica
Description:
A procedure is suggested for identifying illegal users of an ATM. By honing their characteristics and storing the information, some assumptions are made, one of which is the identification context. Not everyone, though, will be a suspect. suspicious behavior on distant ATMs and to lower the possibility of fraudulent activities, including taking out cash with someone else's card, Various video survey and image processing have been discussed in relation to surveillance methods. Preprocessing, categorization, feature extraction, and related video processing techniques are covered along with other operations.
Advantage: Improving the security system's overall dependability and lowering the possibility of false positives or negatives.
Disadvantage: accuracy issues.
4. Title: Smart ATM Card for Multiple Bank Accounts Authors: Darwin Nesakumar A; Arthi S; Avulu Lahari

Description:
This paper's primary goal is to employ RFID technology to combine several bank accounts and user accounts onto a single smart card. To generate an OTP, a formula-based authentication method is employed, whereby operators and alphabets are substituted for integers. During registration, registered phone numbers will receive an OTP. We have included the user's biometric, or fingerprint, which is used for every transaction, to bolster security. By registering their bank credentials, customers may now complete their transactions without having to carry around numerous ATM cards or remember different pin numbers. This ensures security and authenticity through the use of biometric authentication.
Advantage: Easy Access to Several ATMs
Disadvantage: T e c h n i c a l Compatibility
5. Title: Machine Learning Model using Times SeriesAnalytics for rediction of ATM Transactions
Authors: Puspa Setia Pratiwi; Chandra Prasetyo Utomo
Description:
Banking locations that enable customers to do routine financial operations swiftly and automatically without the assistance of bankers are known as automated teller machines, or ATMs. Transaction

behavior performed by users at ATMs is frequently unpredictable. Therefore, in order to give banks the chance to reduce operational expenses, the banking industry is highly urged to develop an intelligent cash management system. To make a forecast, transaction patterns from customers are required. The purpose of this project is to use time series methods and machine learning techniques to forecast transaction values at ATMs. The purpose of this research is to develop a machine learning model that uses four algorithms—Linear Regression, Prophet, ARIMA, and LSTM algorithms—to estimate the value of ATM transactions. The dataset that is being used is the ATM transaction data XYZ Bank. There are around 11.588 rows and 10 columns in this dataset. The Coefficient of Determination (R2) is 0.72, the Mean Absolute Error (MAE) is 20,686.91, and the Mean Squared Error (MSE) is 710,590,544.24. These are the results of the computations using the best evaluation model identified in the LSTM technique.

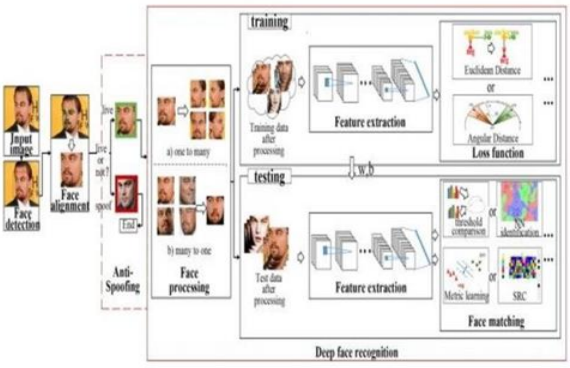
Advantage: Banks can save money overall by cutting back on needless expenses related to maintenance, cash replenishment, and operational inefficiencies.

Disadvantage: Model Intricacy

III. PROBLEM STATEMENT

1. Existing System

The current ATM authentication mechanism involves the usage of OTP and password-PINs.Currently, all that is needed for identity verification on ATMs is an access card, which typically contains a magnetic stripe (magstripe) and a set Personal Identification Number (PIN). In some additional situations, a chip and PIN are used, often accompanied by a magstripe for identifying reasons in case the chip fails.Customers may now withdraw cash from ATMs by merely scanning a QR code with the QR app, eliminating the need for their ATM cards.To read a QR code and extract its contained data, you need a QR code scanner. In order for the ATM to accept user credentials, a scanner must be installed. We'll add more features to an established system; therefore the conventional withdrawal option is also available. The ATM will, on the other hand, scan the QR code produced by the Android software "Get Note" and use the database-stored key to decrypt it. The ATM will get the necessary information after decryption, including the card number, amount, pin, and CVV number on the card. It will use the bank's database to authenticate every detail. The ATM will dispense cash upon successful authentication. An ATM security system design that combines the current PIN-based authentication method with both fingerprint and GSM technologies. In order to identify a customer during an ATM transaction, PIN verification and fingerprint recognition are combined. Fingerprint is validated using efficient minutiae feature extraction method. In order to ensure security when using a swipe machine for transactions, Through the use of GSM technology, the customer will confirm the transaction by sending an approval message. GPS will be used to determine the position in both situations. The card will be immediately banned by the system and the client will receive a notice with further details if someone else attempts to use it.Fuzzy Expert Systems (FESs), Support Vector Machines (SVMs), Artificial Neural Networks (ANNs), and Gaussian Mixture Models (GMMs) are the algorithms employed in the current biometric identification system.PCA and LDA. Biometrics measures an individual's distinct physical or behavioral traits in order to identify or verify their identification. Physical biometrics like as fingerprints, hand or palm geometry, and features of the retina, iris, or face are commonly used. It is possible to establish identification with biometrics. A fresh gauge that claims to be a component of a certain entity is checked against the information kept about that entity. The claim that the individual is who they say they are is considered validated if the measures agree. A well- known biometric database including samples of both faces and voices, as well as the similarity ratings of five face and three speech biometric experts, was used to train and test the algorithms.



Disadvantages

- The system's precision is not perfect.
- A little bit delayed in the loading of training data and face detection operations.
- Its range for facial detection is restricted.
- It is unable to identify faces that are missing in live video.
- There is still some physical labor required of the training set management and teacher.
- A number of issues, including noisy data, intraclass differences, limited degrees of freedom, non-universality, spoof attacks, and unacceptable error rates, must be addressed by unimodal biometric systems.
- This approach is not particularly safe and is likely to lead to a rise in illegal activity.

To detect codes, a QR code scanner is necessary. It is recommended to have a mobile phone with an installed app. Proposed System

This study suggests a multi-modal security architecture for automated teller machines that combines electronic face recognition with a physical access card using Deep Convolutional Neural Network. Deep Learning-Based Facial Biometric Authentication System Artificial intelligence (AI) is a subset of machine learning, which is a subset of deep learning. Compared to conventional machine learning techniques, deep learning allows us to attain higher accuracy in face recognition.

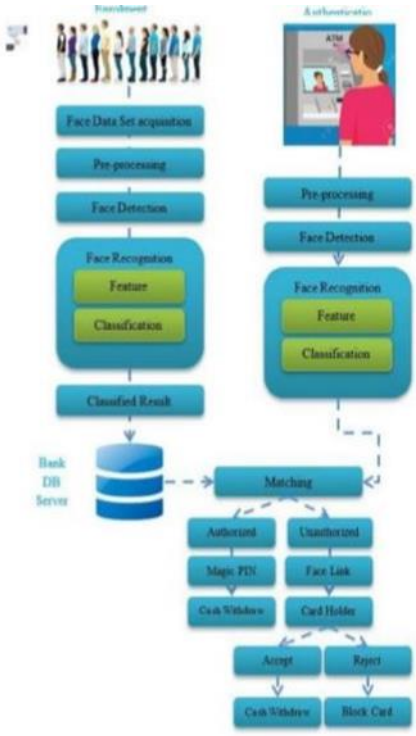
Deep FR system with alignment and a face detection. First, faces are localized using a face detector. Second, using normalized canonical coordinates, the faces are aligned. The FR module is put into use third. The face antispoofing feature in the FR module finds Face processing is used to address variances before, regardless of whether the face is real or artificial tests and training, such as ages and positions; After the deep features of the testing data are retrieved, face matching techniques are employed to perform feature classification. Various architectures and loss functions are utilized to extract discriminative deep features during training.

Unidentified Face Verification Link Producer He isan unauthorized user if there is a discrepancy between the taken image and the saved image. In order to verify the identity of an unauthorized user, a Face Verification Link will be generated and sent to them. This will allow for remote certification, which will either authorize the transaction as intended or notify the banking security systemof a security breach.

Advantages

- The fact that each user's face ID is distinct and cannot be used by another person is one of the benefits.
- It can be applied to lessen efforts at fraud and to stopstealing and other illegal actions.
- A reliable and safe facial authentication platform
- Establish lifestyle infrastructure that is secure and safe.
- Using the Face Verification Link, prevent unwantedaccess; • Quick and precise prediction

IV. SYSTEM ARCHITECTURE



V. SYSTEM SPECIFICATION

1. HARDWARE SPECIFICATION

Processors: Intel® Core™ i5 processor 4300M at 2.60 GHz or 2.59 GHz (1 socket, 2 cores, 2 threads per core), 8 GB of DRAM

Disk space: 320 GB

Operating systems: Windows® 10, macOS*, and Linux*

2. SOFTWARE SPECIFICATION

Server Side: Python 3.7.4(64-bit) or (32-bit) Client Side : HTML, CSS, Bootstrap

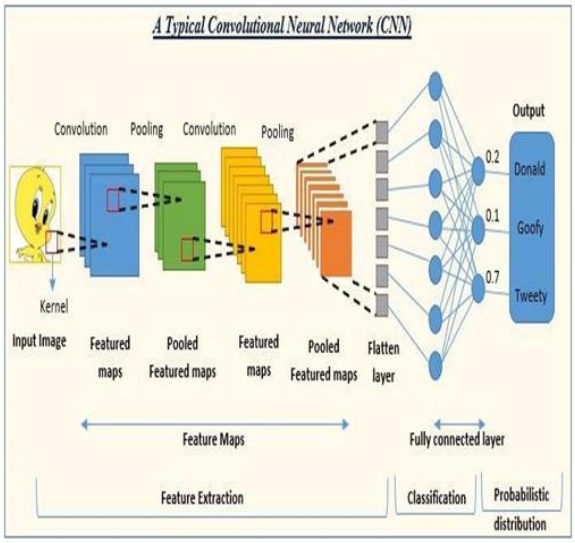
IDE : Flask 1.1.1

Back end : MySQL 5. Server : WampServer 2i

OS : Windows 10 64 –bit or Ubuntu 18.04LTS —Bionic Beaver‖

VI. ALGORITHM

For picture identification and classification applications, onepopular kind of deep learning model is the Convolutional Neural Network (CNN) method. CNNs are made up of several layers of linked neurons and are modeled after how the human brain processes images. Convolutional layers are used to extract features from the input pictures, and then fully connected layers are used for classification and pooling layers to lower dimensionality. Because CNNs can learn hierarchical representations directly from raw data, they have shown outstanding performance in a variety of applications, including as object identification, facial recognition, and medical picture analysis.

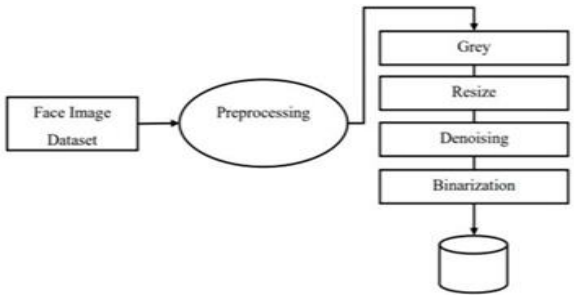


VII. SYSTEM IMPLEMENTATION

1. PROJECT DESCRIPTION

Module List

1. ATM Simulator
2. Face Recognition Module



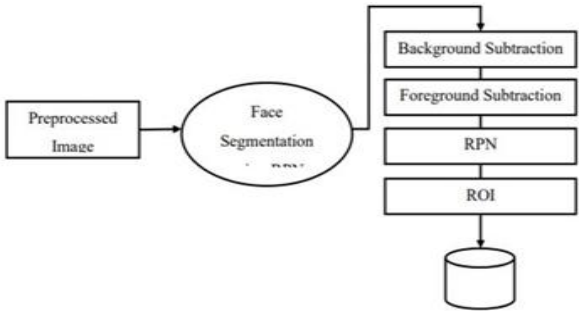
- Face Enrollment
- Face Authentication

3. Prediction

4. Unknown Face Forwarder Mechanism.

1. ATM Simulator

An Next Generation testing tool for XFS-based ATMs is called ATM Simulator (also known as Advanced Function or Open-Architecture ATMs). A virtualized replica of any ATM may be used for ATM testing



thanks to a web technology called ATM Simulator.ATM Simulator combines automation for quicker, more effective testing of face authentication and unknown face forwarder technique with virtualization to deliver realistic ATM simulation.

2.Face Recognition Module

Face Enrollment

The first step in this module is to register a few Bank Beneficiary templates' front faces. The templates for theother poses—tilting up or down, moving closer or farther, and turning left or right—are then evaluated and registered using these as a reference.

Face Image Acquisition

ATMs should have cameras installed in order to record pertinent footage. Webcam is employed here, and the computer and camera are interfaced.

Frame Extraction

From the input video, frames are extracted. The video has to be split up into a series of pictures that are processed further. The implementation of persons determines the rate at which a video has to be split

into pictures. From there, we may infer that typically 20–30 frames per second are captured and forwarded on to the following stages.

Pre-processing

The actions done to prepare photos before they are utilized for model training and inference are known as face image pre-processing. The actions to be performed are:

- RGB to greyscale picture conversion
- Resize the picture
- Denoise (remove noise)

To get rid of extraneous noise, smooth our photograph. We use Gaussian blur for this.

Binarization

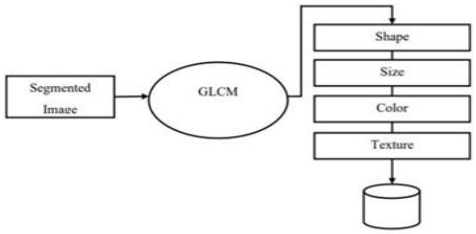
Binarization is the process of transforming a grayscale image to black and white. This reduces the image's information from 256 shades of grey to just two: black and white, or a binary image.

Face Detection

Therefore, in this module, Region Proposal Network (RPN) generates RoIs by sliding windows on the feature mapthrough anchors with different scales and different aspect ratios. Face detection and segmentation method based on improved RPN. RPN is used to generate RoIs, and RoI Align faithfully preserves the exact spatial locations. These are responsible for providing a predefined set of bounding boxes of different sizes and ratios that are going to be used for reference when first predicting object locations for the RPN.

Feature Extraction

Following face detection, the feature extraction module receives the face picture as input in order to identify the salient characteristics that will be employed in the classification. The eyes, nose, and mouth are automatically retrieved from each posture, and the variation's consequences are then computed based on how the variation relates to the frontal face templates.



Face Classification

During the enrollment process, DCNN algorithms were developed to automatically identify and reject incorrect face photos. This will guarantee accurate enrollment and, thus, optimal performance.

Face Identification

The face detection module receives the image once the ATM camera has captured the face. This module identifies the areas of a picture that are probably inhabited by people. Following the employment of Region Proposal Network (RPN) for face recognition, the face picture is sent into the feature extraction module in order to identify the salient characteristics that will be employed in the classification process. The module creates a very brief feature vector that suffices to depict the picture of the face.Here, the extracted characteristics of the face picture are compared with those kept in the face database using DCNN and a pattern classifier. After that, the facial picture is categorized as recognized or unknown. Assuming that the image's face is known, the matching Card Holder is recognized and moves forward.

3. Prediction

This module uses test Live Camera Captured Classified file and trained classified result to match. The prediction accuracy is shown based on the difference, which is calculated using the Hamming Distance.

Unknown Face Forwarder

In order to verify the identity of an unauthorized user, anUnknown Face Verification Link will be generated and sent to the card holder. This will allow for remote certification, which will either authorize the transaction appropriately or alert the banking security system to a security breach.

VIII. CONCLUSION

Face biometrics provides the much-needed and eagerly awaited solution to the issue of illicit transactions byidentifying and authenticating account owners at automated teller machines. In this project, we have created a method to address the widely-feared problem of fraudulent transactions using biometrics and an Unknown Face Forwarder on Automated Teller Machines, which can only be used when the account holder is in close physical proximity. As a result,instances of illicit transactions

at ATMs without the genuine owner's knowledge are eliminated. The security of using a biometric characteristic for identification is increased when another is utilized for authentication. The ATM security
design takes into account the potential for proxy use of the current security technologies (such ATM card) and data (such a PIN) into the current ATM security systems.

IX. FUTURE ENHANCEMENT

By creating a unique deep feature representation approach, the recognition performance should be significantly improved in the future.

REFERENCE

[1] Arjun Kumar V ―ATM Security Using Face Recognition‖, International Journal of Current Engineering and Scientific Research (IJCESR) IN 2018.

[2] P. A. D. Gujar, N. B. Sawant, T. L. Hake, A. A. Shete, and S. M. Deshmukh, ―Face recognition open CV based ATM security system, ‖ Int. J. Res. Appl. Sci. Eng. Technol., vol. 10, no. 5, pp. 1114–1119, 2022.

[3] J. J. Patoliya and M. M. Desai, ―Face detection-based ATM security system using embedded Linux platform, ‖ in 2017 2nd International Conference for Convergence in Technology (I2CT), 2017.

[4] M. Karovaliya, S. Karedia, S. Oza, and D. R. Kalbande, ―Enhanced security for ATM machine with OTP and facial recognition features, ‖ Procedia Comput. Sci., vol. 45, pp. 390–396, 2015.

[5] S. Sasipriya, P. M. Kumar, and S. Shenbagadevi, Face recognition based new generation ATM system.

[6] M. Karovaliya and S. Karedia, Sharad Oza Enhanced Security for ATM Machine with Otp and Facial Recognition Features. 2015.

[7] T. Kwon and S. Na, ―Stegano PIN: Two-Faced Human- Machine Interface for Practical Enforcement of PIN Entry Security, ‖ IEEE TRANSACTIONS ON HUMAN MACHINE SYSTEMS, vol. 46, no. 1, pp. 1–8, 2015.

[8] V. Hiremath and A. Mayakar, Face recognition using Eigenface approach. ―Enhanced Principal Component Analysis Recognition Performance.

[9] Selvakumar, Logesh, M. Vishnu, Maniraj, and P. Kumar, ―Face biometric authentication system for ATM using deep learning, ‖ in 2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC), 2022, pp. 647–655.

[10] A. Kowshika, P. Sumathi, K. S. Sandra, A. Santhosh kumar, and R. Gokul krishnan, ―Facepin: Face biometric authentication system for ATM using deep learning, ‖ NVEO, pp. 1859–1872, 2022.