AI BASED CARDLESS ATM TRANSACTION USING FACE RECOGNITION

Sathish Kumar P
Computer Science and Engineering
Francis Xavier Engineering College
Vannarpettai – Tirunelveli
sathishkumarp.ug19.cs@franciscxavier.ac.in

Rajamanickam R
Computer Science and Engineering
Francis Xavier Engineering College
Vannarpettai – Tirunelveli
rajamanickamr.ug19.cs@franciscxavier.ac.in

Sudhakar S
Computer Science and Engineering
Francis Xavier Engineering College
Vannarpettai – Tirunelveli
sudhakars.ug19.cs@franciscxavier.ac.in

Mrs. Priskilla Angel Rani J
Asst. Professor / Dept. of Computer Science and Engineering
Francis Xavier Engineering College
Vannarpettai – Tirunelveli
priskillaangelranij@francisxavier.ac.in

Dr. R. Ravi
Professor / Dept. of Computer Science and Engineering
Francis Xavier Engineering College
Tirunelveli – Tamil Nadu - India
dr.r.ravi@francisxavier.ac.in

Abstract:
Nowadays we are experiencing a radical increase in skimming in the Automated Teller Machine (ATM) systems. So, actuation in advancement and security of the ATM machines is required. An automated teller machine (ATM) is an electronic telecommunications device that helps customers of banking departments in transactions and transfer of money in their accounts. The customer enters them unique personal identification number (PIN), i.e., stored in the chip of the card. Due to an increase in the installation of ATM and the number of ATM cardholders, the number of cases of fraudulence has also increased radically. The advancement in technology has resulted in an increase in various skimming activities. So, developments are incorporated in the existing systems to make it more secure, convenient and reliable. The employed secured system must have high speed and must be durable. In order to recognise a person's face in a photo or video, face recognition technology is utilised. The fundamental difficulty in face recognition is correctly identifying a person's face even under challenging circumstances, including dim illumination or blurry photos. Face recognition is a major issue because it needs to accurately identify and align facial features such the mouth, nose, eyes, and jawline in order to extract the necessary data for identification. In addition, the use of facial recognition technology raises ethical and privacy problems that have been a problem in recent years. As a result, sophisticated algorithms and methods are required to increase the reliability and accuracy of face recognition systems

Keywords – Face Recognition, 4-digit pin number, Bank details.

I. INTRODUCTION

R. Kabilan, R. Ravi, G. Rajakumar, S. Esther Leethiya Rani, and V. C. Mini Minar (2015) suggested using histogram intersection methods to assess how closely two distributions generated from the LVP's spatial histograms resemble one another and identify the facial image [1].A.Deepika, K.Raja Sundari, and R.Ravi (2014) suggested that the output pixel's value should fall inside the range of its neighbours. Degraded images can be effectively repaired using these filters. As a result, these filters work well for concepts like

picture deconstruction and restoration [2] Edwin Raja S and Ravi R (2020) proposed to use the DMLCA approach to increase the detection accuracy utilising a variety of factors, including detection accuracy based on true positive ratio, precision, and recall [3]. stated that their research concentrates on the dangers of financial botnets for online banking [4]. Muthukumaran Narayanaperumal and Ravi Ramraj (2014) suggested an efficient concept for a hardware architecture that uses four stages for regular pipelining data flow parallelism. Consecutive pixels can be divided into even and odd samples using two-level parallelism, and a separate hardware engine is assigned to each group. Multilevel parallelisms can further improve this strategy [5].R. Kabilan et al. (2019) proposed that the structural, surface morphological, optic, elemental, and electrical research be performed on the manufactured CZTS thin film absorber layer.[6] According to M.D. Amala Dhaya and Dr. R. Ravi (2015) stated that their research concentrates on the dangers of financial botnets for online banking[7] R. Kabilan et al. (2019) proposed that the structural, surface morphological, optic, elemental, and electrical research be performed on the manufactured CZTS thin film absorber layer [8].

Cash withdrawals via ATMs are still a common practise today, although they can encounter a number of problems. We suggest using card-less transactions to address issues like skimming and card cloning brought on by the use of cards. The system demands that ATMs be used, and those ATMs must have software installed that allows users to verify their identities using a reference number, login ID, and password. Mysql-created databases served as record sheets for each account user, storing information such as user ids, passwords, account balances, reference numbers, and withdrawal amounts among other things.

The system's fundamental operation is to use a mobile application that has been installed for cash withdrawals, sign in, and generate a reference number of the user's choosing that includes the amount to be withheld together. Once generated by the user, this reference number would be good for about a half-hour, depending on the bank's preference. The user must then proceed to the ATM, sign in using their user name, password, and a code that will flash in their mobile application, and then finish the transaction. For each user, this code is modified minute by minute in the application. The user will be approved if the user id, password, and code are for entering the reference number. The ATM will dispense the cash if the reference number is also a match.

As a result, the system will offer three levels of protection, starting with a password or lock on the mobile app to confirm the user's identity. The user will login to the ATM machine using their user ID, password, and the code that is present in the mobile app at the second stage of authentication. The user would then complete the final step of authentication by keying in the reference number into the ATM. So, the suggested approach totally abolishes the use of ATM cards and resolves related issues. As the reference number is produced by the user each time a transaction is made, the security is further increased. Moreover, this resolves the issues brought on by OTP sharing.

A. History:

The debut of Automated Teller Machine (ATM) dates back to 1967. The first machine was installed in Barclays' Enfield Town in London. In Europe at that time, banks were already searching for ways to make cash withdrawal services to be made available to general public after working hours. This is when John Shepherd-Barron thought about vending machines which sold chocolate bars and the idea struck as to why a similar mechanism wasn't being used to withdraw cash. This is the revolutionary idea which changed the face of retail banking. The Personal Identification Number (PIN) was introduced much later in 1970. James Goodfellow was the person behind the concept of PIN which could be stored on cards. This was one of the most important moments in the history of ATM since it meant that the humans could be identified and

verified by machines without the need of human intervention.

B. Existing Problems:

In recent past, the banking frauds have been on a constant rise. The fraudsters aim at looting money through online banking methods and also target transactions via debit, credit and ATM cards. ATM card frauds have been present since the time ATMs were invented but the number and types of fraud cases have increased drastically. The fraudsters are robbing the people of their hard-earned money via these methods. There are two things which are required to access the account of an individual- card issued by the bank and the PIN. With the rise of cybercrime various means have been developed to intercept the user's PIN and the card details stored in the magnetic strip. Fake cards can then easily be created and funds can be withdrawn from the account of the unsuspecting individual. In such times it is essential to be well informed about such frauds and dedicate the research towards overcoming these problems.

• **Card Skimming:** This is one of the most popular and common technique. Skimming essentially refers to stealing or duplicacy of the data present in the electronic card which ultimately enables the criminal to forge the ATM card. During this process the customer can use their card normally and won't be notified of any suspicious activity till the time the amount has been withdrawn and the account has been defrauded. This cloning technique is responsible for maximum number of frauds taking place. Here the card details are stolen by placing a foreign device in the ATM machine. The PIN is also then captured and eventually the card is cloned.

• **Eavesdropping:** Similar to its contextual meaning, eavesdropping is a technique via which the card data is stolen by a foreign device placed by the criminal on the card. This can be achieved via methods like wire trap, reading the card reader functionality or having a magnetic reader installed within the reader. The principle of this method is the use of proper card reading functionality.

• **Cash shimming:** In Card Shimming method, the data is targeted which is present on the chip of the ATM card. Here, a foreign material is placed between the ATM card and the card reader present in the ATM machine. By using this method, the fraudster can capture the data of multiple cards. Also, the attacks can be carried out in multiple ways like capturing the data equivalent magnetic strip or relay etc.

C. Motivation:

Keeping the above-mentioned problems in mind, we wanted to devise a solution which would enable customers to use their cards without any fear in a secure environment. This was the motivation behind this project. Some measures which have been included to boost the safety of ATM cards involve chip enabled cards which are used to verify whether the card is fake or genuine. Other methods like CNN (Convolutional neural network), have been implemented for debit and credit card purchasing methods but for ATM services such a method is still not available which is what motivated us to develop something which could omit the contact of the ATM card with the machine altogether. Many ideas have been proposed to solve the issues related to banking frauds. face recognition techniques have been a topic of research for a long time. This includes authentication using face recognition, secondary 4-digit pin number. In the author has proposed the use of image recognition to verify the identity of the user. The system requires that the dataset images be installed in all ATMs. In the author proposes to provide three tier security system involving the use of CNN and OTP verification. Encryption techniques to provide secure exchange of data over cloud have been discussed.

II. LITERATURE REVIEW

1. Resolution Invariant Face Recognition using a Distillation Approach (IEEE 2020).

In this study, they suggest employing both HR and LR pictures to train a network under the supervision of a fixed network that has already been trained on HR face photos. By dividing the Soft max weights between the two networks and minimising the KL-divergence between the output Soft max probabilities of the pretrained (i.e., Teacher) and trainable (i.e., Student) networks, the advice is provided.

2. Advanced ATM System Using Iris Scanner (IEEE 2019).

The biometric scanners used in the offered design, such as the iris scanner and the two-way check with the fingerprint scanner, give it a distinctive quality. The system can access the subsequent stages for the transaction since the iris scanner is the primary security check. The ATM card's inbuilt fingerprint scanner serves as the system's secondary security check. Only when the cardholder's inputted data matches what is in the database is the transaction process considered successful. It is appropriate for usage since it uses less energy. Comparing the proposed modified approach to the other current categorization and affirmation procedures for ATMs, it is practical and inexpensive.

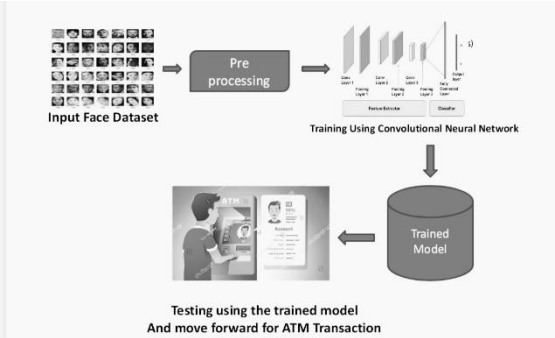
3. A Constraint-based Biometric Scheme on ATM and Swiping Machine (IEEE 2016).

Biometric process for a single little debit? and "What may be the greatest loss if one's card is used fraudulently?" We suggest a restriction on ATM transactions employing biometrics as a solution to enhance system performance and address the stated problems. The suggestion is broken up into two sections. By imposing a restriction on the amount of cash that may be withdrawn and the number of transactions, the first portion addresses the sensor performance issue. If one seeks to withdraw several little amounts OR needs to withdraw a large amount, they must first produce their biometric.

III. PROCESS OF (CNN) TECHNIQUE

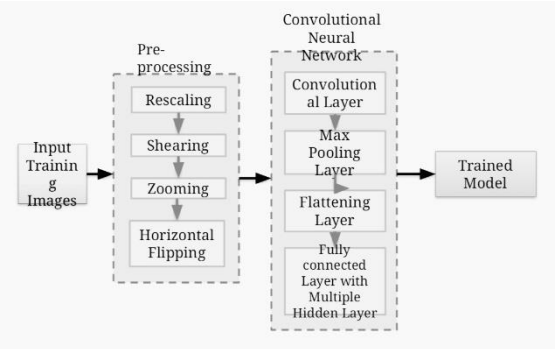
In the beginning of our project, we will gather user face images. We will take 50 pictures of each user's face, and each of those 50 pictures will be kept in a separate folder. The user faces that have been gathered are used for training and validation purposes. After data collection, pre-processing methods like zooming, shearing, rescaling, and horizontal flipping are used on the user's face photos. We next feed these pre-processed data into our convolutional neural network model. Convolutional neural networks are used for the training process, and the trained model is saved as a file for testing.

Proposed System Architecture:



To get the 97% accuracy in our project, we shall train the image data more than 100 times. Using the trained model, we can classify the users' faces in real time after training. A 97% accurate result will likewise be obtained when testing an image using our trained model. Following the prediction of the user's image and receipt of their banking information, the machine next requests the user's four-digit secret pin in order to complete the transaction. In the event that their face and 4-digit pin number match, they are able to conduct transactions; otherwise, they are unable to do so.

Training Model:



IV. CONCLUSION AND FUTURE SCOPE

A. Conclusion:

By doing away with card swiping, the suggested solution intends to address the issues of card cloning at numerous locations, including ATM machines, shopping centres, retail stores, etc. It enables the user to create a reference number based on their needs. The exchange of data is safe when encryption software like bcrypt is used. Also, there will be three layers of protection provided by the checks being made to confirm the user's identity: authentication at the time of signing in to the website, via the password and the code flashing on the smartphone screen, and through the reference number. The degree of vulnerability is diminished by the reference number expiring after a set period. This essay aims to address the problem of banking frauds and assaults, which can be developed and improved a lot further.

B. Future Scope:

There is always room for improvement because no suggested solution can be considered to be perfect for the vulnerability of the banking system to assaults. This system, like all others, has benefits and problems of its own.

It is possible to enhance the cryptography method being utilised here. Moreover, a mobile application might be developed in place of a website to make this system more portable and to make signing in repeatedly easier. The creation of a mobile application as well as modifications to ATMs are necessary for the proposed idea to be implemented properly. The biggest problem that will prevent the system from functioning correctly is the slow internet. So, adjustments might be made to get rid of the issue. Hence, even though the concept tries to

There are several factors that must be taken into account for the system to operate successfully and efficiently, including the card cloning issue.

V. REFERENCE

[1] D. R. Kabilan, R. Ravi, G. Rajakumar, S. Esther Leethiya Rani and V. C Mini Minar, “A combined face recognition approach based on LPD and LVP”, ARPN Journal of Engineering and Applied Sciences, vol. 10, no. 6, pp. 2577-2581, 2015.

[2] A.Deepika, K.Raja Sundari, and R.Ravi, “Image Decomposition and Restoration for Blurred Images Using Filtering Techniques”, International Journal of Advanced Research in Computer Engineering & Technology, vol. 3, no. 3, pp. 631-635, 2014.

[3] Edwin Raja S and Ravi R, “A performance analysis of Software Defined Network based prevention on phishing attack in cyberspace using a deep machine learning ith CANTINA approach(DMLCA)”, Computer Communications, vol. 152, pp.0-6, 2020.

[4] Muthukumaran Narayanaperumal and Ravi Ramraj, “Simulation Based VLSI Implementation of Fast Efficient Lossless Image Compression System Using Adjusted Binary Code &Golumb Rice Code”, International Journal of Computer, Information, Systems and Control Engineering, vol. 8 no. 9, pp.1603-1606, 2014.

[5] Yesubai Rubavathi Charles and Ravi Ramraj, “A novel local mesh color texture pattern for image retrieval system”, International Journal of Electronics and Communications (AEÜ), vol.70, pp. 225-233, 2016.

[6] R. Kabilan, Dr. R. Ravi, G. Rajakumar, S. Esther Leethiya Rani and V. C Mini Minar, “A combined face recognition approach based on LPD and LVP”, ARPN Journal of Engineering and Applied Sciences, vol. 10, no. 6, pp. 2577-2581, 2015.

[7] M.D. Amala Dhaya, and Dr. R. Ravi, “Financial Botnets - Online Threat for Financial Banking”, International Journal of Advanced Research Trends in Engineering and Technology, vol. 2, no. 8, pp.23-27, 2015+

[8] R. Kabilan et al. (2019) proposed that the structural, surface morphological, optic, elemental, and electrical research be performed on the manufactured CZTS thin film absorber layer.