Real-Time Secure Clickbait and Biometric ATM User Authentication and Multiple Bank Transaction System

Savitha. U,Harishankari.M, Mathivadhanii. R, Sowjanya. B

Department O Electronics and Communication Engineering

Veltech Hightech Dr. Rangarajan Dr. Sakunthala engineering college, Avadi, Chennai.

muralikrishnank1971@gmaiil.com

misspacer26@gmail.com

sabithabalaji.2001@gmail.com

ABSTRACT

The usage of ATM's has increased in huge numbers. As technology continues to develop rapidly, conventional ATMs are assailable to theft. It is no secret that computer vision is advancing rapidly in today's world. As biometric identification techniques have advanced over the past few years, including fingerprinting, retina scanning, and facial recognition, the past few years have seen an increase in the number of security measures at ATMs to increase security. Specifically, this project aims to give a computer vision method to solve the security risk associated with accessing ATMs. This proposes an ATM security model that uses electronic facial recognition using Deep Convolutional Neural Network. where faces would be protected as well as their accounts. Face Verification Clickbait Link will be generated and sent to the bank account holder to verify the identity of the unauthorized user through some dedicated artificial intelligent agents, for remote certification. As the biometric features cannot be cloned, this proposal will make it possible for the account holder to be the only individual who has access to their account. By using a real-time data set, fraud stemming from ATM card theft is eliminated.

Keywords: (i)assailable (ii) deep convolutional neural network (iii) click bait link (iv) cloned

INTRODUCTION

Automated Teller Machines, popularly referred to as ATMs, are one of the most useful advancements in the banking sector. ATMs allow banking customers to avail of quick self-serviced transactions. ATMs enable individuals to make banking transactions without the help of an actual teller. The most common uses of an Automated Teller Machine include withdrawing money, checking balance, transferring money, or changing the PIN (Personal Identification Number). Nowadays, crimes at ATMs have become an alarming issue. Security for the customer's account is not guaranteed by PIN. Most ATM scams involve criminal theft of debit card numbers and personal identification numbers (PINs) from innocent users of these machines. Some of the theft methods which is involved in ATMs are skimming, shimming, cash out, etc. As this is an alarming issue for our growing demand for ATMs, measures to reduce the risk level are being discussed and brought into

action lately with the help of IOT (Internet of Things) and Deep learning. This is been implemented with the help of face recognition to secure

ATMs. Face-Based ATM Login Process The ATMs which are equipped with Face recognition technology can recognize the human face during a transaction. Face-based card holder authentication can be used as primary or as a secondary authentication measure along with ATM PIN. Face verification is embedded with security features to prevent fraud, including liveness-detection technology that detects and blocks the use of photographs, videos or masks during the verification process.

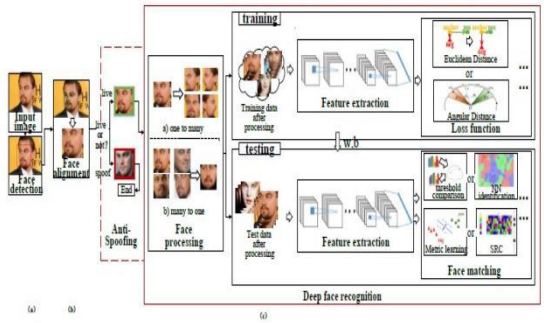
LITERATURE SURVEY

One of the most widely used information systems is the ATM, and entries made on the ATM keypad frequently include the PIN of an ATM user. The PIN is a private piece of customer data used to verify a transaction. In order to meet the security criterion of secrecy, the banking system primarily operates under the trust assumption that the PIN is protected and kept secret by both the system and the customer. To increase user security by adding the secondary stage of prevention to the existing system ATM theft control by detecting the face is used where the detection of the subject results in acceptance or rejection. Furtherly using the GSM module OTP is generated. And when the network coverage is low, the iBeacon module works as Bluetooth Low Energy (BLE) and acts as a transmitter to detect and track smartphones [1]. Here the detection process is performed by facial detection. When a person enters the ATM and appears before the camera with a mask or anything that would cover their face, then a voice play will instruct them to remove them. If they continue to wear them, through RS-232 the image of that person will be sent to Arduino UNO [2]. To enhance the safety measures in ATMs, the usage of vibration Sensors are used to monitor the ATM when an unknown person tries to withdraw cash or tries to break in. when these are observed, the door will be locked and the message of the breaking into the ATM will be notified to the officials. IR Sensor to monitor the person moving IN/OUT. Also, IoT MODEM sends data and control through the server it performs Emergency Lock through the server [3]. As the misusage of biometric details has increased, the usage of specialized forms of detection namely, multi-spectral imaging (MSI) sensors is used to reduce the vulnerability of fingerprint sensors to spoof attacks. Fingerprint verification is done using the Arduino UNO code using the library files. [4]. The system is developed using a microcontroller, whenever the person accesses the ATM, it asks for the iris recognition and PIN number before the transaction. As iris recognition is told to be one of the safest biometric security methods. If the user puts in the wrong PIN number, the door of the ATM will be locked automatically and the nearest police station will get an alert message via GSM modem [5].

PROPOSED METHOD

This study suggests a multi-modal security paradigm for automated teller machines that makes use of electronic

facial recognition powered by a Deep Convolutional Neural Network. Artificial intelligence (AI) is a subset of machine learning, which itself is a subset of deep learning. Deep learning makes it possible for us to attain higher accuracy than conventional machine learning techniques when it comes to face recognition. With face detector and alignment, deep FR system. To locate faces, a face detector is utilized first. The faces are secondly positioned according to normalized canonical coordinates. Third, the FR module is put into practice. Face anti-spoofing in the FR module recognizes Face processing is used to handle variations before training and testing, such as poses and ages. Different architectures and loss functions are used to extract discriminative deep features when training. Face-matching methods are then used to do feature classification after the deep features of testing data are extracted.



With face detector and alignment, deep FR system. To locate faces, a face detector is utilized first. The faces are secondly positioned according to normalized canonical coordinates. Third, the FR module is put into practice. Face anti-spoofing in the FR module recognizes Face processing is used to handle variations before training and testing, such as poses and ages. Different architectures and loss functions are used to extract discriminative deep features when training. Face-matching methods are then used to do feature classification after the deep features of testing data are extracted.

If it is an unauthorized user when the stored image and the taken image don't match. Face Verification Links will be created and sent to users in order to confirm the identity of unauthorized users via special artificial intelligence agents for remote certification, which will either properly authorize the transaction or alert the banking security system to a security breach. Fast and Accurate Predictions are produced as a result of the short reaction time. The identification stage moves quickly and precisely. As a result, there are fewer efforts at fraud.

BLOCK DIAGRAM

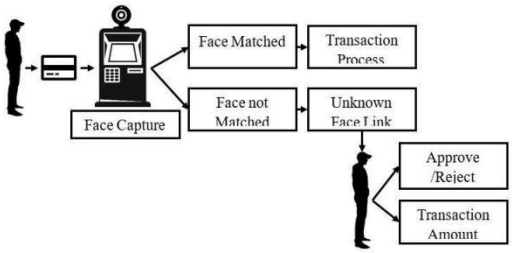


Fig:02

This ATM Security model block diagram is further defined by the shown modules;

1. ATM Simulator
2. Face Recognition Module
    2.1. Face Enrolment
    2.2. Face identification
3. Unknown face detection

4. Transaction process

1. ATM Simulator:

ATM Test systems could be following an Era of advanced testing software designed that will be utilized for XFS technology, which is also referred to as Open-Architecture or Advanced Function ATMs. ATM Simulator is an advanced internet-based solution that enables the virtualized version of any ATM to be utilized for testing purposes. ATM Simulator is a tool that creates pretend ATMs that look and work just like real ones. It uses special technology to make sure the simulation is accurate and also makes it easier and faster to test things like face recognition.

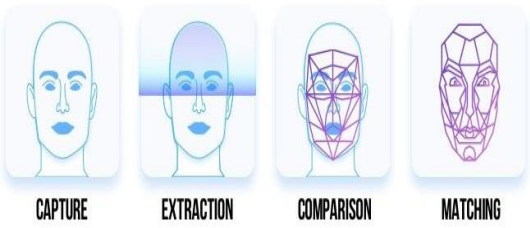


Fig:03

2. Face Recognition Module

2.1. Face Enrolment:

This unit starts by saving some pictures of people's faces who are receiving money from a bank. These models are used to check and save other different poses, like looking up or down, coming nearer or going farther away, and turning right or left.

2.1.1. Face Image Acquisition:

We should put cameras in ATMs to record important video. A camera and a computer are connected together, and a special camera called a webcam is being used.

2.1.1.1. Frame Extraction:

Frames are extracted from the video input source. The footage necessitates segmentation into a series of frames that undergo subsequent analysis. The optimal frequency for segmenting a video into frames is contingent upon the idiosyncratic approach of the operator. Based on the available evidence, it can be inferred that typically 20 to 30 frames per second are captured and subsequently transmitted to subsequent phases.

2.1.2. Pre-processing:

Pre-processing of facial images involves a series of measures implemented to prepare the images for utilization in model training and inference. The actions to be executed encompass the following procedural measures: observe the image. The conversion from color space represented in the Red, Green, and Blue (RGB) color model to the Greyscale color space is a necessary transformation that can be accomplished through various image processing techniques. The action of properly adjusting the dimensions of an image in order to conform to particular specifications or requirements in a precise and accurate manner is commonly referred to as resizing an image.

2.1.3. Face Detection:

In this manner, in this module, Locale Proposition Arrange (RPN) produces RoIs by sliding windows on the included outline through grapples with diverse scales and diverse angle proportions. Confront location and division strategy based on moved forward RPN. RPN is utilized to produce RoIs, and RoI Adjust loyally jam the precise

spatial areas. These are mindful of giving a predefined set of bounding boxes of diverse sizes and ratios that are planning to be utilized for reference when to begin with, foreseeing question areas for the RPN.

2.1.4. Feature Extraction:

Upon the detection of facial features, the extracted image is subsequently forwarded as input to the feature extraction component in order to identify the salient characteristics that will be utilized for categorical differentiation. In the process, every posture's facial features, encompassing the eyes, nose, and mouth, are automatically extracted. Subsequently, these features are employed in the computation of the variations' impacts, by means of their association with the frontal face templates.

2.1.5. Face Classification

Deep convolutional neural network (DCNN) algorithms were developed with the objective of automatizing the identification and elimination of inadequate facial images in the enrolment phase. Assuring adequate enrolment will thereby guarantee optimal performance.

2.2. Face Identification

The face image obtained from the ATM camera is directed to the face detection module. This particular module is capable of identifying human image regions with a high degree of likelihood. Once the RPN has completed face detection, the face image is provided to the feature extraction module for the identification of significant attributes that will be employed for categorization. The feature vector created by the module is concise yet sufficient in accurately depicting the facial image.

In this case, a DCNN is utilized alongside a pattern classifier to compare a facial image's distinctive features with those already saved in the face database. Afterward, the facial image is categorized as either recognized or unrecognized. Once the face in the image is recognized, the system is able to determine the corresponding Card Holder and proceed to the next step.

3. Unknown face detection

After obtaining the face that is being captured by the camera for processing, testing, or detection the face that was captured will be examined. As the approved face is been extracted and saved as a separate form of the pattern by the CNN, the process will commence by comparing it with previously sorted and captured by a camera in real-time. Hamming Distance measures how different two things are. This tells us how accurate our predictions are while being compared. Once the captured face is told to be an unknown one or a non-registered one, Obscure Confront Confirmation Interface (OCCI) will be created and sent to the cardholder to confirm the character of the unauthorized client through the registered way of making it an authenticated transaction for further certification, or where it processes signals for it as a security-violation caution and stops the transaction process and keeps the money secure.

4. Transaction process:

4.1. Money withdrawal:

When the face matches with the previously registered one, the transaction occurs with no errors and as a result, the entered amount will be ejected. If the face is not the registered one, the user needs to identify the face and accept the requested face, and they can input the required withdrawal amount within the designated bank account balance is imperative to effectively conclude the transaction.

4.2 Collection of cash:

Upon inputting the designated sum, the automated teller machine (ATM) will dispense said amount, and subsequently enable the recipient to retrieve the funds accordingly.

RESULT AND ANALYSIS:

Finding the performance of our system is done using sensing ability, specific points out, and the accuracy of Data in the datasets are divided into two classes non-pedestrian (the negative class) and pedestrian (the positive class). Sensing ability, specific point-outs, and accuracy are calculated using the True positive (TP), true negative (TN), false negative (FN), and false positive (FP). Here TP is the number of positive cases that are classified as positive.

$$Sensitivity = \frac{TP}{TP + FN}$$

$$Specificity = \frac{TN}{TN + FP}$$

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

FP is defined as the number of negative cases that are classified as positive. TN is the number of negative cases classified as negative and FN is the number of positive cases classified as negative.

Fig:04

As is said that during the initial registration process, the face of the cardholder is scanned for a brief time of a few seconds where the DCNN creates its own pattern for the face. Which usually works like marking points all over our faces at equal distances. After the facial point placements, those points are placed in a way that only the system knows the group and forms the face on which it was placed. This is where the usage of a convolutional network is used so that the level of theft can be reduced drastically as it's unknown to us the point formation.

Fig: 4.1

Fig: 4.2

Fig: 4.3

Fig: 4.4

The above-shown figures show us how a face is being separated using the facial point separation and how the dataset has our picture after feature extraction and face image accusation.

Fig:05

Now the dataset is already filled with its own type of image accusation and feature extraction. Hence during the capturing of the face while the money transaction, if the extracted features don't match up an alert to the registered user will be sent respectively.

6. CONCLUSION:

Biometrics when being used in identifying and authenticating account owners at the Automated Teller Machines it gives the needed and much-anticipated solution to the problem of illegal transactions. Here, we have developed to provide a solution to the much-anticipated solution for the issue of fraudulent transactions through Automated Teller Machine by biometrics and Unknown Face Forwarder that can be made possible only when the account holder is physically or far present. Thus, it eliminates cases of illegal transactions at ATM points without the knowledge of the owner. Using a biometric feature for identification is strong and it is further safe when another is used at the authentication level. The ATM security design incorporates the possible maximum usage of the existing security tools (such as ATM Cards) and information (such as a PIN) into the existing ATM security mechanisms. It involves, on a real-time basis, the bank account owner in all the available and permissible transactions.

REFERENCE:

[1] R.S. Ramya, G. Nivetha, R.S. Saranya, S. shanmathi, U.Pavithra, ''ATM theft control system by iris recognition technique'', International Research Journal of Modernization in Engineering Technology and Science, 2021.

[2] P. Visalakshi, D. V. Sai Teja, K. Muni Kira, ''IoT-based ATM monitoring using cloud data with sensors'', International Journal of Advance Research, Ideas and Innovations in Technology, 2019.

[3] Nagarjuna Telagam, Sunita Panda, Nehru Kandasamy, Menakadevi Nanjundan, ''Smart Sensor Network Based Atm Management System using Lab view'', International Journal Engineering and Advanced Technology (IJEAT), June 2019.

[4] C. Bhosale, P. Dere and C.K. Jadhav ''ATM security using face and fingerprint recognition'', International Journal of

Research in Engineering Technology and Science, 2018.

[5] V. Manoj, Mouli Sankar. R, S. Sasipriya, U. Devi, ‘‘Multi Authentication ATM Theft Prevention Using iBeacon’’, International Research Journal of Engineering and Technology (IRJET),2019.

[6] T. Sangeetha, M. Kumaraguru, S. Akshay M. Kanishka “Biometric-based Fingerprint Verification System for ATM machines”, JPCS conference series, 2021.

[7] A. Gokul, B. Tharik salman, R. Vasudevan, Y. vasanth, Dr. S.M Uma “Biometric-based security ATM transaction incorporating GSM module”, IRJET 2021.

[8] Selvakumar. R A Logesh.S, Maha Vishnu S; Maniraj S; Praveen kumar. A “Face biometric authentication ATM system using deep learning”, 2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC), 2022.

[9] Priyabrata Pattanaik, Mihir Narayan Mohanty, “ATM security improvement using biometrics”, International Journal of Advanced Research in Engineering and Technology (IJARET), 2020

[10] S Gokul, S Kukan, K Meenakshi, S Vishnu Priyan, J Rolant Gini, M.E. Harikumar, “Biometric based smart ATM using RFID”, Third international conference on smart system and inventive technology, 2020