Nat. Volatiles & Essent. Oils, 2022; 9(1): 1859-1872

NVEO
Natural Volatiles &
Essential Oils

FACEPIN: FACE BIOMETRIC AUTHENTICATION SYSTEM FOR ATM USING DEEP LEARNING

Dr. A Kowshika[1] , Dr. P.Sumathi[2] , K S Sandra* , A Santhosh kumar * , R Gokulkrishnan*

Assistant Professor[1] , Head of the Department[2] , Student*

Department of Information Technology, SNS College of Engineering Coimbatore, India.

Abstract: Automated Teller Machines also known as ATM
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 systems today use 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 an automatic teller machine 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 Link will be generated and sent to user to verify the identity of unauthorized 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.

Keywords: Facial recognition, Feature extrqction, Segmentation, CNN algorithm.

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 quick self-serviced transactions, such as cash withdrawal, deposit, and fund transfers. ATMs enable individuals to make banking transactions without the help of an actual teller. Also, customers can avail banking services without having to visit a bank branch. Most ATM transactions can be availed with the use of a debit or credit card. There are some transactions that need no debit or credit card. the utmost utilization rate for ALOHA is 36.8% and therefore the Q value is eighteen .6% [26], [27]. Therefore, the face recognition a part of this study uses PCA and LDA and therefore the Intelligence RFID access control part uses on binary tree search algorithm.

the general design architecture of the system is presented then the precise identity authentication methods. the method for the access system is detailed and final experimental results and conclusions are given..

1.1HISTORY

In 1960, an American named Luther George Simjian invented the Bank graph, a machine that allowed customers to deposit cash and checks into it. The first ATM was set up in June 1967 on a street in Enfield, London at a branch of Barclays bank. A British inventor named John Shepherd-Barron is credited with its invention. The machine allowed customers to withdraw a maximum of GBP10 at a time.

1.2.Types of Automated Teller Machines (ATMs)

Automated Teller Machines (ATMs) are mainly of two types. One is a simple basic unit that allows you to withdraw cash, check balance, change the PIN, get mini statements and receive account updates. The more complex units provide facilities of cash or cheque deposits and line of credit & bill payments. There are also onsite and offsite Automated Teller Machines: the onsite ATMs are within the bank premises, unlike the offsite ones which are present in different nooks and corners of the country to assure that people have basic banking facilities and instant cash withdrawals if they can't go to a bank branch. ATMs can also be categorized based on the labels assigned to them. Some of these labels are listed below-

- Green Label ATMs- Used for agricultural purposes
- Yellow Label ATMs- Used for e-commerce transactions
- Orange Label ATMs- Used for share transactions
- Pink Label ATMs- Specifically for females to help avoid the long queues and waiting time
- White Label ATMs – Introduced by the TATA group, white label ATMs are not owned by a particular bank but entities other than the bank
- Brown Label Banks- Operated by a third party other than a bank

1.3.Uses of an Automated Teller Machine

Automated Teller Machines have revolutionized the banking sector by providing easy access to customers and loading off the burden from bank officials. Some of the uses of an ATM are-

- The most common uses of an Automated Teller Machine include withdrawing money, checking balance, transferring money, or changing the PIN (Personal Identification Number)
- Newer and advanced ATMs also provide options to open/withdraw a Fixed Deposit (FD), or to apply for a personal loan. You can also book railway tickets, pay the insurance premiums, income tax & utility bills, recharge mobile, and deposit cash. Some of these facilities require you to register at the bank branch
- Customers can now do money transactions at their convenience. ATMs today are installed in public spaces, highways, malls, market places, railway/airport stations, hospitals, etc.
- Automated Teller Machines provide 24×7 access anywhere
- ATMs help to avoid the hassle of standing in long queues at the bank even for simpler transactions like withdrawing money. It has also helped in reducing the workload of the bank officials.

1.4.ATM Fraud

Over the last two decades, automated teller machines (ATMs) have become as much a part of the landscape as the phone booths made famous by Superman. As a result of their ubiquity, people casually use these virtual cash dispensers without a second thought. The notion that something could go wrong never crosses their minds. Most ATM scams involve criminal theft of debit card numbers and personal identification numbers (PINs) from the innocent users of these machines. There are several variations of this confidence scheme, but all involve the unknowing cooperation of the cardholders themselves.

ATM fraud is described as a fraudulent activity where the criminal uses the ATM card of another person to withdraw money instantly from that account. This is done by using the PIN. The other type of ATM fraud is stealing from the machine in the ATM by breaking in.

- **Skimming:** This type of ATM scam involves a skimmer device that criminals place on top of or within the card slot. To record your PIN number, the criminals may use a hidden camera or an overlay that covers the original PIN pad. Using the card numbers and PIN's they record; thieves create duplicate cards to withdraw money from consumers' accounts. Unlike losing your debit card or having it stolen, you won't

realize anything is amiss until unauthorized transactions take place. Take a look at these so you know how to detect ATM skimmers.

- **Shimming:** This is the latest update to skimming. Instead of reading your card number, criminals place a shimming device deep inside the ATM to record your card's chip information. The end result is the same as skimming because thieves use the stolen chip data to create "cloned" versions of your debit card.
- **Cash-out:** This scam targets multiple accounts from the same financial institution. Armed with a hacked bank employee's credentials, the criminal alters account balances and withdrawal limits. Using stolen debit card numbers captured from a separate skimming attack, they can "cash out" the ATM until it's out of money.
- **Jackpotting:** While there are multiple types of jackpotting attacks, typically, these incidents involve gaining physical access to the inside of the machine. The criminals may replace hardware or install malicious software giving them control of the cash dispensing function. Jackpotting is similar to a cash out scam, but it does not require the criminal to have any customer account details or stolen debit card information.

1.5.Problem Identified

Nowadays, crimes at ATMs have become an alarming issue. Security for the customer's account is not guaranteed by PIN. Many people, who aren't familiar with the concept of PIN are unlikely to memorize and recognize it. There are many people who mistrust PIN, such as, if they have lost their card, they would feel unsafe that their account could be accessed by others and they would lose all their money.

1.6.AI with IoT

Individually, the Internet of Things (IoT) and Artificial Intelligence (AI) are powerful technologies. When you combine AI and IoT, you get AIoT—the artificial intelligence of things. You can think of internet of things devices as the digital nervous system while artificial intelligence is the brain of a system. To fully understand AIoT, you must start with the internet of things. When "things" such as wearable devices, refrigerators, digital assistants, sensors and other equipment are connected to the internet, can be recognized by other devices and collect and process data, you have the internet of things.

Artificial intelligence is when a system can complete a set of tasks or learn from data in a way that seems intelligent. Therefore, when artificial intelligence is added to the internet of things it means that those devices can analyze data and make decisions and act on that data without involvement by humans. These are "smart" devices, and they help drive efficiency and effectiveness. The intelligence of AIoT enables data analytics that is then used to optimize a system and generate higher performance and business insights and create data that helps to make better decisions and that the system can learn from.

1.6.1Real-World Examples of AI Embedded IoT Devices

- **Traffic Management**

Traffic is a real problem in urban areas and there is a consistent need for efficient traffic management to avoid congestion. Traffic management can be difficult if it has to be done by humans as it would only lead to chaos and confusion. AIoT, however, is a smart solution to this problem. Real-time traffic can now be managed efficiently using drones that can monitor large areas and transmit the traffic data which can then be analyzed using AI for final decision making like adjusting traffic lights without human intervention.

- **Self- Driving Cars**

Self-driving cars are another use case of IoT devices embedded with AI. Tesla's self-driving cars are the best example. With the help of installed sensors and the power of AI, this car has the ability to make human-like decisions by determining the conditions of the surroundings. For example, they can determine the optimal speed, weather and road conditions to make effective decisions.

- **Smart Homes**

IoT blended with AI has also led to the emergence of smart homes concept. Smart homes have all the devices connected to each other with the help of IoT and these devices also possess the ability to make smart decisions with the help of AI. Smart homes tend to make our lives easier by giving us the power to control our devices even remotely. For example, we can pre-decide the time of switching on the television or making a call to the fire department in-case of fire. We can also turn our appliances on or off as required even when we are away from our homes.

- **Body Sensors**

Maintaining a good health is a big challenge for people today. Due to busy schedules, visiting doctors every now and then for regular checkups is also difficult for a huge chunk of population but this problem can also be solved with the help of wearable devices such as fitness trackers that help in tracking blood sugar levels, heartbeat, cholesterol levels and much more thereby helping in health management. These sensors can also be used by construction companies to detect the posture of their laborers in order to avoid any kind injuries while working

- **Robots for Manufacturing Industries**

Manufacturing Industries also make use of robots for manufacturing processes and these robots are nothing but another kind of AI embedded IoT devices. They help in enhancing the manufacturing processes by saving time and cost of processing. An example is the use of robots by eye wear manufacturers for manufacturing lenses with a great precision.

- **Face Detection**

Face detectors are another important use case of AIoT. Face detection becomes important for crime investigation departments and even in offices for detecting the faces of employees for the purpose of attendance. Another interesting area where face detectors are being used currently are shopping malls and other public places to keep a check on whether people are wearing masks or not and punishing the defaulters accordingly.

- **Retail Analytics**

Management of staff in retail outlets is an important task because both over staffing and under staffing can lead to inefficient operations. With the use of sensors and AI, however, people entering the outlets and their movement inside the outlet can be observed in order to estimate the time they will take to reach the checkout line. The staff at the counter can then be increased or decreased accordingly to reduce the checkout time and increase productivity. The captured data can also be used later for determining the peak hours and formulate management strategies well in advance.

- **Smart Buildings**

Another area of intersection of IoT and AI is smart office buildings. So, not only homes but a whole building can also have AIoT installed for better operational efficiency and management cost. Some companies for example, install a network of AIoT devices in their buildings and these devices can detect the presence of personnel and

adjust the temperatures accordingly or turn off appliances where no one is present thereby increasing energy efficiency which ultimately leads to lower costs.

1.6.2.IoT and Machine Learning

IoT is the data “supplier”, while machine learning is the data “miner”. To make the data supplied by IoT work, it needs to be refined. Dozens of IoT sensors and external factors are producing a myriad of data points. The “miner’s” task here is to identify correlations between them, extract meaningful insight from these variables and transport it to the storage for further analysis.

1.6.3.Deep Learning

Deep learning attempts to mimic the human brain—albeit far from matching its ability—enabling systems to cluster data and make predictions with incredible accuracy. Deep learning is a subset of machine learning, which is essentially a neural network with three or more layers. These neural networks attempt to simulate the behavior of the human brain—albeit far from matching its ability—allowing it to “learn” from large amounts of data. While a neural network with a single layer can still make approximate predictions, additional hidden layers can help to optimize and refine for accuracy.

Deep learning drives many artificial intelligence (AI) applications and services that improve automation, performing analytical and physical tasks without human intervention. Deep learning technology lies behind everyday products and services (such as digital assistants, voice-enabled TV remotes, and credit card fraud detection) as well as emerging technologies (such as self-driving cars).

1.7.Scope of the Project

Face recognition can be used to secure ATM transaction and is used as a tool for authenticating users to confirm the card owner.

Financial fraud is a very important problem for Banks and current secure information in the ATM card magnetic tape are very vulnerable to theft or loss. By using face recognition as a tool for authenticating users in ATMs can be confirmed as the card owner. Face Based ATM login Process the ATMs which are equipped with Face recognition technology can recognize the human face during a transaction. When there are “Shoulder Surfers" who try to peek over the cardholder’s shoulder to obtain his PIN when the cardholder enters it, the ATMs will automatically remind the cardholder to be cautious. If the user wears a mask or sunglasses, the ATM will refuse to serve him until the covers are removed.

Touchless - There is no need for remembering your passwords. Only looking at the ATM camera will login the card holder instantly. No physical contact is needed.

Secure - Since your face is your password, there is no need to worry for your password being forgotten or stolen. In addition, the face recognition engine locks access to the account and transaction pages for the card holder as the card holder moves away from the camera of the ATM and another face appears

Face based card holder authentication can be used as primary or as a secondary authentication measure along with ATM PIN. Face based authentication prevents ATM fraud by the use of fake card and stolen PIN or stolen card itself. 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.

II.SYSTEM ANALYSIS

Existing System

- **Existing ATM authentication method is the use of password-PINs and OTP.**

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.

- **QR cash withdrawals were enabled so customers could ditch their ATM cards and simply scan a QR-code on ATMs using the QR app to withdraw cash.**

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.

- **ATM security system architecture that incorporates both the finger print and GSM technology into the existing PIN-based authentication process.**

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.

- **The algorithms used in the existing system for biometric authentication are Gaussian Mixture Models (GMMs), Artificial Neural Networks (ANNs), Fuzzy Expert Systems (FESs), and Support Vector Machines (SVMs). LDA, PCA.**

Biometrics measure the unique physical or behavioral characteristics of an individual as a means to recognize or authenticate their identity. Common physical biometrics include fingerprints, hand or palm geometry, and retina, iris, or facial characteristics. Biometrics may be used for identity establishment. A new measurement that purports to belong to a particular entity is compared against the data stored in relation to that entity. If the measurements match, the assertion that the person is whom they say they are is regarded as being authenticated. The algorithms were trained and tested using a well-known biometric database which contains samples of face and speech and similarity scores of five face and three speech biometric experts.

Disadvantages

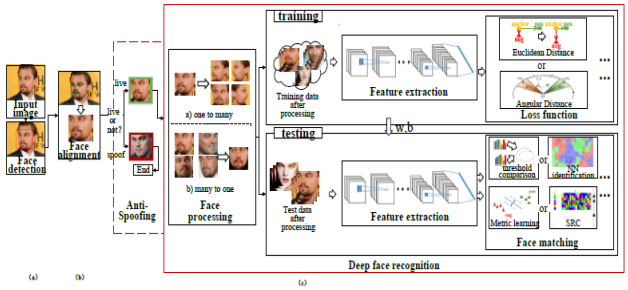
- The accuracy of the system is not 100%.
- Face detection and loading training data processes just a little bit slow.
- It can only detect face from a limited distance.
- It cannot repeat live video to recognize missed faces.
- The instructor and training Set manager still have to do some work manually.
- Unimodal biometric systems have to contend with a variety of problems such as noisy data, intraclass variations, restricted degrees of freedom, non-universality, spoof attacks, and unacceptable error rates.
- This method is not very secure and prone to increase in criminal activities.
- QR code scanner is required to detect code
- Should carry the mobile phone with app installed on it

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.

- **Facial Biometric Authentication System using Deep Learning Techniques**

Deep learning is a subset of machine learning, which, in turn, is a subset of artificial intelligence (AI). When it comes to Face recognition, deep learning enables us to achieve greater accuracy than traditional machine learning methods.



Deep FR system with face detector and alignment. First, a face detector is used to localize faces. Second, the faces are aligned to normalized canonical coordinates. Third, the FR module is implemented. In FR module, face anti-spoofing recognizes Whether the face is live or spoofed; face processing is used to handle variations before training and testing, e.g. poses, ages; Different architectures and loss functions are used to extract discriminative deep feature when training; face matching methods are used to do feature classification after the deep features of testing data are extracted.

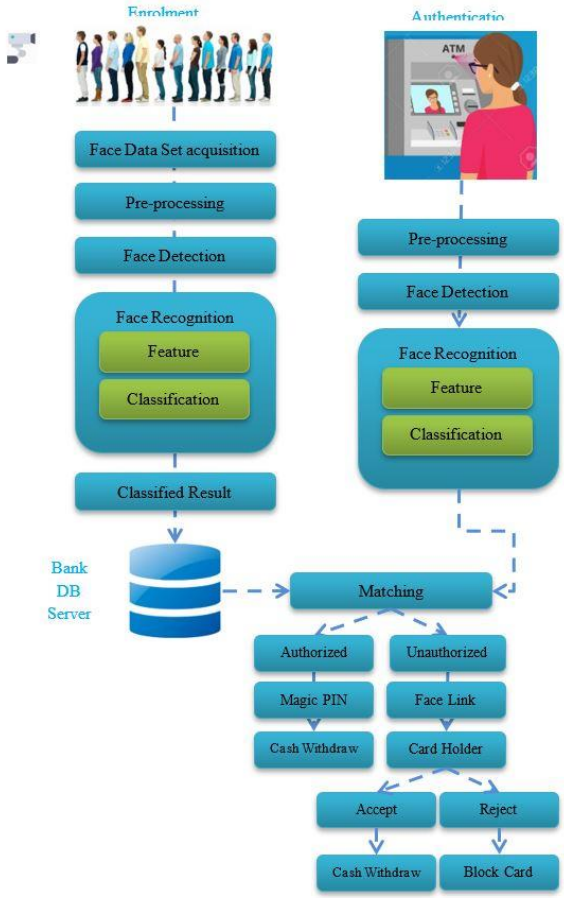
- **Unknow Face Verification Link Generator** –

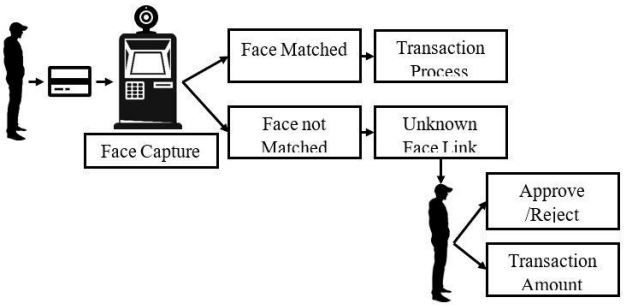
When the stored image and the captured image don't match, it means that he is an unauthorized user. Face Verification Link will be generated and sent to user to verify the identity of unauthorized user through some dedicated artificial intelligent agents, for remote certification, which either authorizes the transaction appropriately or signals a security-violation alert to the banking security system.

Advantages

- The advantages can be found as that the face-id is unique for everybody; it cannot be used by anybody other than the user.
- It can be used to reduce fraudulent attempts.
- To prevent theft and other criminal activities.
- Secure facial authentication platform that users can trust
- Provide safe and secure lifestyle infrastructure
- Prevent unauthorized access using Face verification Link.
- Fast and Accurate Prediction

System Flow





Block Diagram

Problem Description

Financial fraud is a very important problem for Banks and current secure information in the ATM card magnetic tape are very vulnerable to theft or loss. By using face recognition as a tool for authenticating users in ATMs can be confirmed as the card owner. Face Based ATM login Process the ATMs which are equipped with Face recognition technology can recognize the human face during a transaction. When there are “Shoulder Surfers" who try to peek over the cardholder’s shoulder to obtain his PIN when the cardholder enters it, the ATMs will automatically remind the cardholder to be cautious. If the user wears a mask or sunglasses, the ATM will refuse to serve him until the covers are removed.

The use of facial recognition enables to deliver more advanced transactions at its ATMs because facial recognition provides an extra layer of security for both the cardholder and the bank. Bank customers can use their Debit/Credit card at the ATM to access their accounts, rather than being limited to only those accounts associated with their ATM card. With facial recognition, Bank can now guarantee its customers the most rigorous security along with the convenience of open banking.

The process used by the bank is to capture the facial images of their customers in the bank branch and then store the images in a secure biometric database. When the customer taps their ID card or inserts their bank card at the ATM, Deep Face activates biometric software supplied by DL Model. The system captures multiple facial images and determines the best image to be used for recognition. In the event that none are deemed to be suitable, the customer will be prompted to move closer, step back, remove their hat or sunglasses or whatever is needed to capture a suitable image. The captured image is sent to the biometric processing system where it is compared to the customer's image stored in the bank's ID database. Once verified, the customer can access their accounts and perform authorized transactions. It's not Verified, ATM Camera to capture the user facial image. Internet-friendly mobile communication device, which is accessible on 24/7 bases, is required for the bank account owner to handle the remote certification. Dedicated intelligent agents for intelligent monitoring of initiated transactions and real-time feedbacks (alerts) to appropriate banking security points. Robust Internet and GSM networks are needed to enable multimedia messaging services (MMS) for certification and authorization processes. There are numerous anti-fraud measures built into the system to add to its security. One such measure is the support of an infra-red lens to capture additional facial details to prevent fraud attempts.

This ATM Security Model consists of this module

1. ATM Simulator
2. Face Recognition Module

2.1. Face Enrollment

2.2. Face Authentication

2.3. Unknow Face Forwarder Mechanism.

4. Transaction Model
5. Performance Analysis

Block Description

1.ATM Simulator

ATM Simulator is a Next Generation testing application for XFS-based ATMs (also known as Advanced Function or Open-Architecture ATMs). ATM Simulator is a web technology to allow ATM testing with a virtualized version of any ATM.ATM Simulator uses virtualization to provide with realistic ATM simulation, coupled with automation for faster, more efficient testing for face authentication and unknown Face Forwarder Technique.

1.Face Recognition Module

2**.1. Face Enrollment**

This module begins by registering a few frontal face of Bank Beneficiary templates. These templates then become the reference for evaluating and registering the templates for the other poses: tilting up/down, moving closer/further, and turning left/right.

2.1.1. Face Image Acquisition

Cameras should be deployed in ATM to capture relevant video. Computer and camera are interfaced and here webcam is used.

2.1.1.1. Frame Extraction

Frames are extracted from video input. The video must be divided into sequence of images which are further processed. The speed at which a video must be divided into images depends on the implementation of individuals. From we can say that, mostly 20-30 frames are taken per second which are sent to the next phases.

2.1.2. Pre-processing

Face Image pre-processing are the steps taken to format images before they are used by model training and inference. The steps to be taken are:

- Read image
- RGB to Grey Scale conversion
- Resize image

Original size (360, 480, 3) — (width, height, no. RGB channels)
Resized (220, 220, 3)

- Remove noise (Denoise)

smooth our image to remove unwanted noise. We do this using gaussian blur.

- Binarization

Image binarization is the process of taking a grayscale image and converting it to black-and-white, essentially reducing the information contained within the image from 256 shades of grey to 2: black and white, a binary image.

2.1.3. Face Detection

Therefore, in this module, Region Proposal Network (RPN) generates RoIs by sliding windows on the feature map through 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.

2.1.4. Feature Extraction

After the face detection, face image is given as input to the feature extraction module to find the key features that will be used for classification. With each pose, the facial information including eyes, nose and mouth is automatically extracted and is then used to calculate the effects of the variation using its relation to the frontal face templates.

2.1.5. Face Classification

DCNN algorithms were created to automatically detect and reject improper face images during the enrolment process. This will ensure proper enrolment and therefore the best possible performance

2.2. Face Identification

After capturing the face image from the ATM Camera, the image is given to face detection module. This module detects the image regions which are likely to be human. After the face detection using Region Proposal Network (RPN), face image is given as input to the feature extraction module to find the key features that will be used for classification. The module composes a very short feature vector that is well enough to represent the face image.

Here, it is done with DCNN with the help of a pattern classifier, the extracted features of face image are compared with the ones stored in the face database. The face image is then classified as either known or unknown. If the image face is known, corresponding Card Holder is identified and proceed further.

3.Prediction

In this module the matching process is done with trained classified result and test Live Camera Captured Classified file. Hamming Distance is used to calculate the difference according to the result the prediction accuracy will be displayed.

4.Unknow Face Forwarder

Unknown Face Verification Link will be generated and sent to card holder to verify the identity of unauthorized user through some dedicated artificial intelligent agents, for remote certification, which either authorizes the transaction appropriately or signals a security-violation alert to the banking security system.

5.Transaction Module

5.1. Enter the Withdrawal Money

In this section, you have to enter your withdrawal amount and press enter.
But make sure your withdrawal amount does not exceed your balance in the account otherwise transaction will fail.

5.2. Collect the Cash

In this section, you have to collect your money from the lower slot of the machine. Take your money before 30 seconds.

6.Performance Analysis

In this module we able to find the performance of our system using SENSITIVITY, SPECIFICITY AND ACCURACY of Data in the datasets are divided into two classes not pedestrian (the negative class) and pedestrian (the positive class). Sensitivity, specificity, and accuracy are calculated using the True positive (TP), true negative (TN), false negative (FN), and false positive (FP). TP is the number of positive cases that are classified as positive. FP is 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.

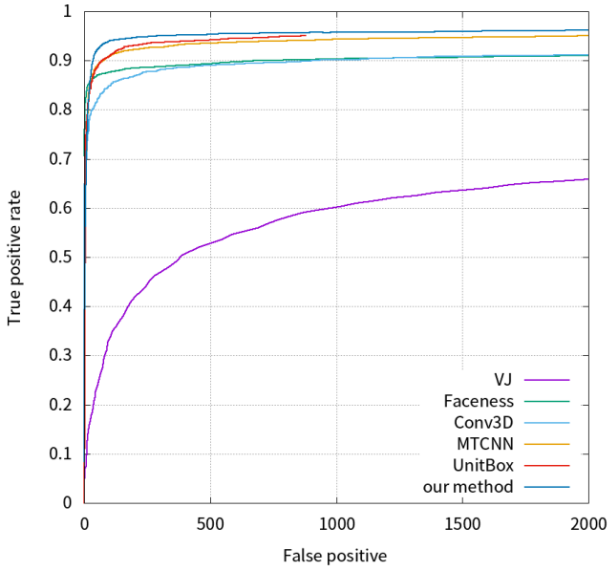
$$Sensitivity = \frac{TP}{TP + FN}$$

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

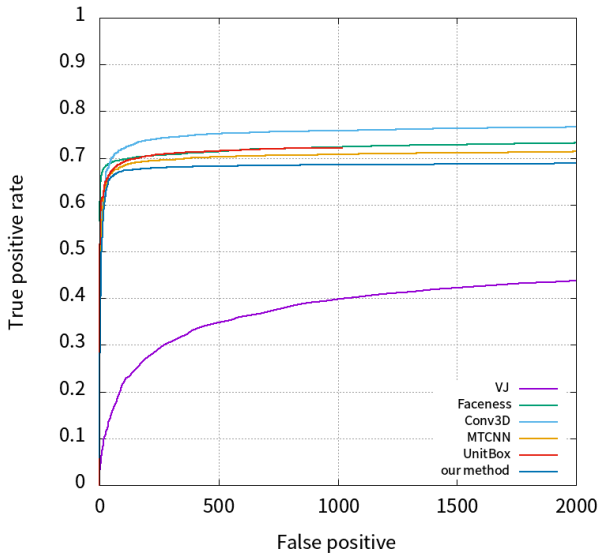
$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Results and Discussion

To evaluate the performance of our method, we compare our method against the state-of-the-art methods in FDDB. The evaluation indicators include: recall rate is used to evaluate the proportion of the detected face to the total face of the sample mark; false positive is the number of errors in the detected face. These two indicators are expressed by the ROC (Receiver Operating Characteristic) curve.



1.a. Discontinuous ROC Curves



1.b. Continuous ROC Curves

The results are shown in FIGURE. 1(a) and FIGURE.1(b). The ROC curve detection results show that the traditional face detection method VJ recall rate is only 66.6%, the detection method based on deep learning has been greatly improved. Our method achieves state-of-the-art performance in terms of both the discrete ROC curve and continuous ROC curve. Our discrete ROC curve is superior to the MTCNN. We also obtain the best true positive rate of the discrete ROC curve at 2000 false positives (96.1%). In addition, the possible influencing factor is that our method is not very effective in detecting the side face. The ROC curve does not clearly indicate which method is better, so another indicator AUC is used to illustrate the pros and cons of the method. AUC represents the area proportion under the ROC curve and the value is between 0 and 1. The higher the AUC value is, the better the method performance will be. Then test on the WIDER FACE dataset, WIDER FACE is a more challenging benchmark than FDDB in face detection. It is very encouraging to see that our model consistently achieves the competitive performance across the three subsets. It has higher robustness for faces with large occlusion and Angle change, which is basically consistent with the evaluation results in the FDDB dataset.

System Specification

4.1 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*
-

4.2 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 18.04 LTS “Bionic Beaver”

Conclusion

Biometrics as means of identifying and authenticating account owners at the Automated Teller Machines gives the needed and much anticipated solution to the problem of illegal transactions. In this project, we have developed to proffer a solution to the much-dreaded 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 the ATM points without the knowledge of the authentic owner. Using a biometric feature for identification is strong and it is further fortified when another is used at authentication level. The ATM security design incorporates the possible proxy usage of the existing security tools (such as ATM Card) and information (such as PIN) into the existing ATM security mechanisms. It involves, on real-time basis, the bank account owner in all the available and accessible transactions.

Future Enhancement

In the future, the recognition performance should be further boosted by designing novel deep feature representation schemes.

REFERENCES

[1] 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.

[2] I. 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.

[3] 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.

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

[5] A. 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.
[6] T.R.Lekhaa, “Secured credit card transaction using web cam” International Research Journal of Engineering and Technology, April 2016.
[7] A. Li, S. Shan, andW. Gao, ``Coupled bias-variance tradeoff for cross-pose face recognition,'' IEEE Trans. Image Process., vol. 21, no. 1, pp. 305-315, Jan. 2012.
[8] 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.
[9] 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.
[10] A.Kowshika,” Least mobility high power (LMHP) dynamic routing for QoS development in Manet” Wireless Personal Communications, Springer US, March 2019.
[11]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.
[12] T. Sharma and S. L. Aarthy, ``An automatic attendance monitoring system using RFID and IOT using cloud,'' in Proc. Online Int. Conf. Green Eng. Technol. (IC-GET), Nov. 2016, pp. 1-4.
[13] A.KOWSHIKA, “A PACKET FORWARDING MECHANISM FOR MANET USING MODRP IN DYNAMIC SOURCE ROUTING (DSR)”, IEEE, OCT 2010.