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

Mahendra P [1], Shaheershah T S [1], Aishwariya K [2]

[1]*Student, Department of Computer science and Engineering, Adithya institute of technology, Coimbatore, Anna University, Tamil Nadu, India.*

[2]*Supervisor, Department of Computer science and Engineering, Adithya institute of technology, Coimbatore, Anna University, Tamil Nadu, India.*

Corresponding Author: patnammahendra707@gmail.com

Abstract: - ATM or Automated Teller Machines are widely used by people nowadays. Performing cash withdrawal transaction with ATM is increasing day by day. ATM is very important device throughout the world. The existing conventional ATM is vulnerable to crimes because of the rapid technology development. A total of 270,000 reports have been reported regarding debit card fraud and this was the most reported form of identity theft in 2021. A secure and efficient ATM is needed to increase the overall experience, usability, and convenience of the transaction at the ATM. In today's w kl, orld, the area of computer vision is advancing at a breakneck pace. 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. Specifically, the goal of this project is to give a computer vision method to solve the security risk associated with accessing ATM machines. This project proposes an automatic teller machine security model that uses electronic facial recognition using Deep Convolutional Neural Network (DCNN). If this technology becomes widely used, faces would be protected as well as their accounts. Face Verification Clickbait Link will be generated and sent to bank account holder 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. This eliminates the possibility of fraud resulting from ATM card theft and copying. The experimental results on real-time datasets demonstrate the superior performance of the proposed approach over state-of-the-art deep learning techniques in terms of both learning efficiency and matching accuracy. By using this real time dataset, the proposed system achieves the highest accuracy with 97.93%.

Key Words: - ***Shimming, Cash-'out, DCNN algorithm ,Central neural networks, general public license, Face detection.***

I. 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.

Manuscript revised May 11, 2023; accepted May 12, 2023. Date of publication May 14, 2023.

This paper available online at www.ijprse.com

ISSN (Online): 2582-7898; SJIF: 5.59

Fig.1. ATM

II. HISTORY

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.

2.1 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.

2.2 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.

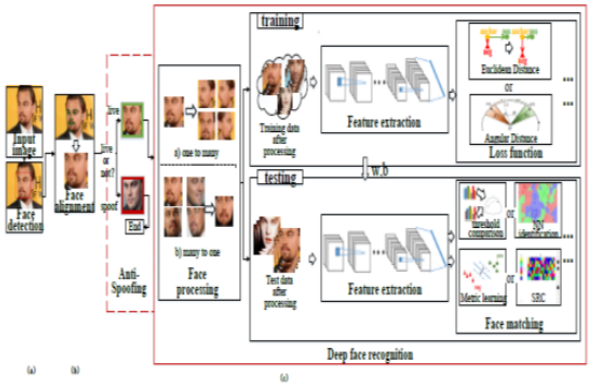


Fig.2. Facial Biometric Authentication System using Deep Learning Techniques

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.

2.3 CNN Face Recognition Step

Filters=32: This number indicates how many filters we are using to look at the image pixels during the convolution step. Some filters may catch sharp edges, some filters may catch color variations some filters may catch outlines, etc. In the end, we get important information from the images. In the first layer the number of filters=32 is commonly used, then increasing the power of 2. Like in the next layer it is 64, in the next layer, it is 128 so on and so forth.

Kernel size= (5,5): This indicates the size of the sliding window during convolution, in this case study we are using 5X5 pixels sliding window.

Strides= (1, 1): How fast or slow should the sliding window move during convolution. We are using the lowest setting of

1X1 pixels. Means slide the convolution window of 5X5 (kernal_size) by 1 pixel in the x-axis and 1 pixel in the y-axis until the whole image is scanned.

Input shape= (64,64,3): Images are nothing but matrix of RGB color codes. during our data pre-processing we have compressed the images to 64X64, hence the expected shape is 64X64X3. Means 3 arrays of 64X64, one for RGB colors each.

Kernel_initializer='uniform': When the Neurons start their computation, some algorithm has to decide the value for each weight. This parameter specifies that. You can choose different values for it like 'normal' or 'glorot_uniform'.

Activation='relu': This specifies the activation function for the calculations inside each neuron. You can choose values like 'relu', 'tanh', 'sigmoid', etc.

Optimizer='adam': This parameter helps to find the optimum values of each weight in the neural network. 'adam' is one of the most useful optimizers, another one is 'rmsprop'

Batch_size=10: This specifies how many rows will be passed to the Network in one go after which the SSE calculation will begin and the neural network will start adjusting its weights based on the errors. When all the rows are passed in the batches of 10 rows each as specified in this parameter, then we call that 1-epoch. Or one full data cycle. This is also known as mini-batch gradient descent. Hence a proper value must be chosen using hyperparameter tuning.

Epochs=10: The same activity of adjusting weights continues for 10 times, as specified by this parameter.

2.4 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.

2.5 Motivation

ATM Fraudulence occurring in the society has become very common nowadays. Skimming and Trapping of the ATM devices have been designed by many Burglars. Unauthorized usage of ATM cards by person other than the owner Shoulder Surfing Attack. Thus, there is a dire need for development of such system which would serve to protect the consumers from fraud and other breaches of security.

2.6 Scope

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.

2.7 Objective Aim

The objective of this project is to proposes the alliance of Face Recognition System for authentication process, unknown face forwarder URL and enhancing the security in the banking region. To provide more security in the ATM, the system is proposed to avoid various types of criminal activities and unauthorized access. To Prevent unauthorized access using Face verification Link. To prevent theft and other criminal activities.

III. METHODOLOGY

ATM Simulator is a Next Generation testing application for XFS-based ATMs (also known as Advanced Function or OpenArchitecture 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.

IV. Related Works

4.1 Face Recognition Module

Face Enrolment: 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.

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

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

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.

V. Face Detection

Therefore, in this module, Region Proposal Network (RPN) generates RoIs by sliding windowson 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 RoIAlign 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.

- Face Image Segmentation Using Region Growing (Rg) Method The region growing methodology and recent related work of region growing are described here. RG is a simple image segmentation method based on the seeds of region. It is also classified as a pixel-based image segmentation method since it involves the selection of initial seed points. This approach to segmentation examines the neighbouring pixels of initial “seed points” and determines whether the pixel neighbours should be added to the region or not based on certain conditions. In a normal region growing technique, the neighbour pixels are examined by using only the “intensity” constraint. A threshold level for intensity value is set and those neighbour pixels that satisfy this threshold is selected for the region growing.
- RPN A Region Proposal Network, or RPN, is a fully Convolutional network that simultaneously predicts object bounds and objectless scores at each position. The RPN is trained end-to-end to generate high-quality region proposals. It works on the feature map (output of CNN), and each feature (point) of this map is called Anchor Point. For each anchor point, we place 9 anchor boxes (the combinations of different sizes and ratios) over the image. These anchor boxes are cantered at the point in the image which is corresponding to the anchor point of the feature map.

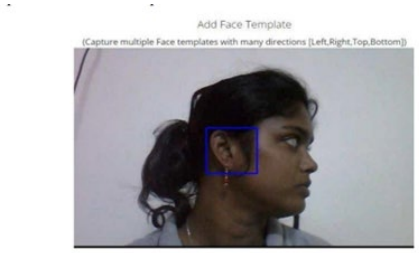
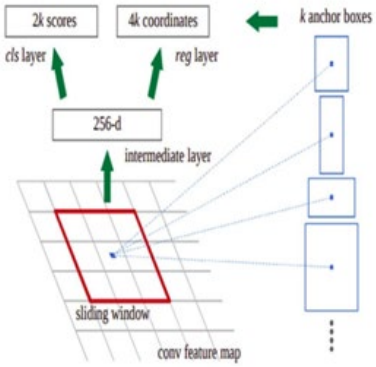


Fig.2. Facial Features

Training of RPN. To know that for each location of the feature map we have 9 anchor boxes, so the total number is very big, but not all of them are relevant. If an anchor box having an object or part of the object within it then can refer it as a foreground, and if the anchor box doesn't have an object within it then we can refer it as **background.** So, for training, assign a label to each anchor box, based on its Intersection over Union (IoU) with



- given ground truth. We basically assign either of the three (1, -1, 0) labels to each anchor box.
- Label = 1 (Foreground): An anchor can have label 1 in following conditions, If the anchor has the highest IoU with ground truth. If the IoU with ground truth is greater than 0.7. (IoU>0.7).
- Label = -1 (Background): An anchor is assigned with -1 if IoU < 0.3.
- Label = 0: If it doesn't fall under either of the above conditions, these types of anchors don't contribute to the training, they are ignored.

After assigning the labels, it creates the mini-batch of 256 randomly picked anchor boxes, all of these anchor boxes are picked from the same image.

- The ratio of the number of positive and negative anchor boxes should be 1:1 in the mini-batch, but if there are less than 128 positive anchor boxes then we pad the mini-batch with negative anchor boxes.
- Now the RPN can be trained end-to-end by backpropagation and stochastic gradient descent (SGD).
- The processing steps are Select the initial seed point
- Append the neighbouring pixels—intensity threshold
- Check threshold of the neighbouring pixel
- Thresholds satisfy-selected for growing the region.
- Process is iterated to end of all regions.

VI. 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.

- Face Features

1) Forehead Height: distance between the top edge of eyebrows and the top edge of forehead.
2) Middle Face Height: distance between the top edge of eyebrows and nose tip.
3) Lower Face Height: distance between nose tip and the baseline of chin.
4) Jaw Shape: A number to differentiate between jaw shapes. this number can be replaced if you use Face Shape Recognition, see (this) notebook.
5) Left Eye Area
6) Right Eye Area
7) Eye to Eye Distance: distance between eyes (closest edges)
8) Eye to Eyebrow Distance: distance between eye and eyebrow (left or right is determined by which side of the face is more directed to the -screen-)
Eyebrows Distance: horizontal distance between eyebrows

Eyebrow Shape Detector 1: The angle between 3 points (eyebrow left edge, eyebrow center, eyebrow right edge), to differentiate between (Straight | non-straight) eyebrow shapes
11) Eyebrow Shape Detector 2: A number to differentiate between (Curved | Angled) eyebrow shapes.
12) Eyebrow Slope.
13) Eye Slope Detector 1: A method to calculate the slope of the eye. it's the slope of the line between eye's center point and eye's edge point. this detector is used to represent 3 types of eye slope (Upward, Downward, Straight).
14) Eye Slope Detector 2: Another method to calculate the slope of the eye. it's the difference on Y-axis between eye's

center point and eye's edge point. this detector isn't a 'mathematical' slope, but a number that can be clustered into 3 types of eye slope (Upward, Downward, Straight).

15) Nose Length

16) Nose Width: width of the lower part of the nose .17) Nose Arch: Angle of the curve of the lower

edge of the nose (longer nose = larger curve = smaller angle) .

18) Upper Lip Height.

19) Lower Lip Height

- Gray Level Co-occurrence Matrix GLCM is a second-order statistical texture analysis method. It examines the spatial relationship among pixels and defines how frequently a combination of pixels are present in an image in a given direction Θ and distance d. Each image is quantized into 16 gray levels (0–15) and 4 GLCMs (M) each for Θ = 0, 45, 90, and 135 degrees with d = 1 are obtained. From each GLCM, five features (Eq. 13.30–13.34) are extracted. Thus, there are 20 features for each image. Each feature is normalized to range between 0 to 1 before passing to the classifiers, and each classifier receives the same set of features. The features we extracted can be grouped into three categories. The first category is the first order statistics, which includes maximum intensity, minimum intensity, mean, median, 10th percentile, 90th percentile, standard deviation, variance of intensity value, energy, entropy, and others. These features characterize the Gray level intensity of the tumour region.

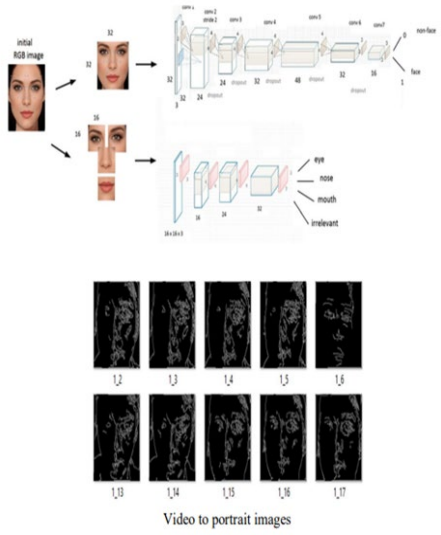


Fig.3. Video to Portrait Images

VII. Face Identification And Verification

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 The CNN creates feature maps by summing up the convolved grid of a vector-valued input to the kernel with a bank of filters to a given layer. Then a non-linear rectified linear unit (ReLU) is used for computing the activations of the convolved feature maps. The new feature map obtained from the ReLU is normalized using local response normalization (LRN). The output from the normalization is further computed with the use of a spatial pooling strategy (maximum or average pooling). Then, the use of dropout regularization scheme is used to initialize some unused weights to zero and this activity most often takes place within the fully connected layers before the classification layer. Finally, the use of softmax activation function is used for classifying image labels within the fully connected layer. 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

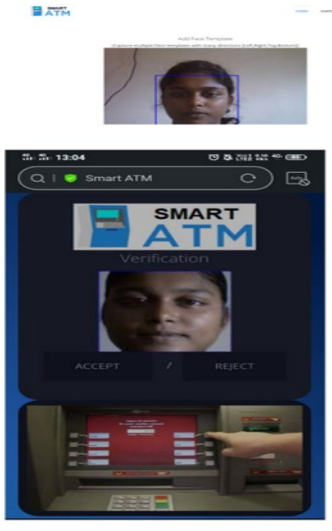


Fig.4. Smart ATM

Future Scope:

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

VIII. RESULT

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.

IX. CONCLUSION

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.

Fig.5. Smart ATM Dashboard

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]. 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.

[7]. 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.

[8]. 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.

[9]. 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.

[10]. 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.