SIMULATION OF ATM BIOMETRIC AUTHENTICATION SYSTEM USING DEEP LEARNING

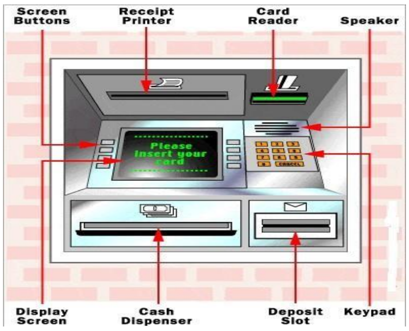
Mrs.V.Sivasakthi M.E[1] , Dr.S.Sujatha[2] ,
[1] vsivasakthi.aamec@gmail.com , [2] sujathaaut@gmail.com ,
[1]Assistant Professor, Anjalai Ammal Mahalingam Engineering College, Kovilvenni,Tamilnadu.
[2] Professor, Anna University (BIT Campus), Tiruchirappalli, Tamilnadu.

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. 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. If this technology becomes widely used, faces would be protected as well as their accounts. Face Verification Click bait Link will be generated and sent to bank account holder to verify the identity of unauthorized user.

I. INTRODUCTION

ATM stands for "Automated Teller Machine". It is a computerized electronic machine that allows bank customers to perform various transactions without the need for a human teller or cashier. ATMs are typically located in public areas such as shopping malls, airports, and banks. ATMs provide a wide range of banking services, including cash withdrawals, deposits, balance inquiries, account transfers, and bill payments. To use an ATM, customers typically need a bank account and an ATM card or debit card that is linked to the account. To withdraw cash, customers insert their card into the machine, enter their Personal Identification Number(PIN),and specify the amount of cash they wish to withdraw. The machine dispenses the cash and issues receipt for the transaction. Similarly, customers can deposit cash or checks by inserting them into the machine and following the instructions on the screen. ATM are available 24/7, making them a convenient way for customers to access their accounts and perform transactions outside of regular banking hours. They have also become an essential part of the global financial system, providing easy and secure access to banking services for millions of people around the world.

Figure1.1AutomatedTellerMachine



\

II.LITERATURE SURVEY

1. **FACE RECOGNITION AS A BIOMETRIC SECURITY FOR SECONDARY PASSWORD FOR ATM USERS,** Lusekelo Kibona and 2015.

In this paper, the author tried to review some mechanisms used in dealing with security threat posed to ATM users and found hat there are potential threats associated with using card based security system so there is a need to add up another secondary security after the primary stage has been passed and that secondary stage is facial recognition security system as explained in an algorithm developed in this paper.

2. **FINGERPRINT BASED BIOMETRIC ATM AUTHENTICATION SYSTEM**, Dhiraj Sunehra and 2014.

The prominent biometric methods that may be used for authentication include fingerprint, palm print,hand print, face recognition, speech recognition, dental and eye biometrics. In this paper, a microcontroller based prototype of ATM cashbox access system using fingerprint sensor module is implemented. The necessary software is written in Embedded 'C' and the system is tested.

3. **DEEP LEARNING BASED CARD-LESS ATM USING FINGERPRINT AND FACE RECOGNITION TECHNIQUES,** Ayusha Mohite, Shruti Gamare, Karan More, Nita Patil 2019.

We propose a system that uses fingerprint and face recognition authentication (not ATM cards) for accessing user accountalong with PIN which is more secure and reliable than the existing system. Here we are using the CNN model for face recognition and Minutiae feature extraction for fingerprint recognition.

4. **USABILITY AND BIOMETRIC VERIFICATION AT THE ATM INTERFACE,** Lynne Coventry, Antonella De Angeli and Graham Johnson and 2003.

Biometric techniques in general and focus upon the usability phases and issues, associated with iris verification technology at the Automated Teller Machine (ATM) user interface. The paper concludes with a review of some of the major research issues encountered, and an outline of future work in the area.

5. **ENHANCED ATM SECURITY SYSTEM USING BIOMETRIC,** S,Selina Oko,Jane Oruh and 2012.

The existing security of the ATM (Automated Teller Machine) system has been improved by integrating the fingerprint of the user into the bank's database as to further authenticate it. This was achieved by modelling and building an ATM simulator that will mimic a typical ATM system. The end result is an enhanced biometric authenticated ATM system that ensures greater security and increased customer's confidence in the banking sector.

III.PROPOSED SYSTEM

- Existing ATM authentication method is the use of password-PINs and OTP.
- QR cash withdrawals were enabled so customers could ditch their ATM cards and simply scan a QR-code on ATMs using the QRapp to withdraw cash.
- ATM security system architecture that incorporates both the finger print and GSM technology into the existing PIN-based authentication process.
- The algorithms used in the existing system for biometric authentication are Artificial Neural Networks(ANNs),Fuzzy Expert Systems(FESs),and Support Vector Machines(SVMs).

DEMERITS

- The accuracy of the existing system is80 to 90 percent.
- Face detection and loading training data processes just a little bit slow.
- I tcan only detect face from a limited distance.
- It cannot repeat live video to recognize missed faces.
- This method is not very secure and prone to increase in criminal activities.

Proposed work

- This paper proposes an automatic teller machine security model that would combine a physical access card and electronic facial recognition using Deep Convolutional Neural Network.
- When the stored image and the captured image is does not match, it results in unauthorized user.
- Face Verification Link will be generated and sent to account holder to verify the identity of unauthorized user.

III. SYSTEM ARCHITECTURE

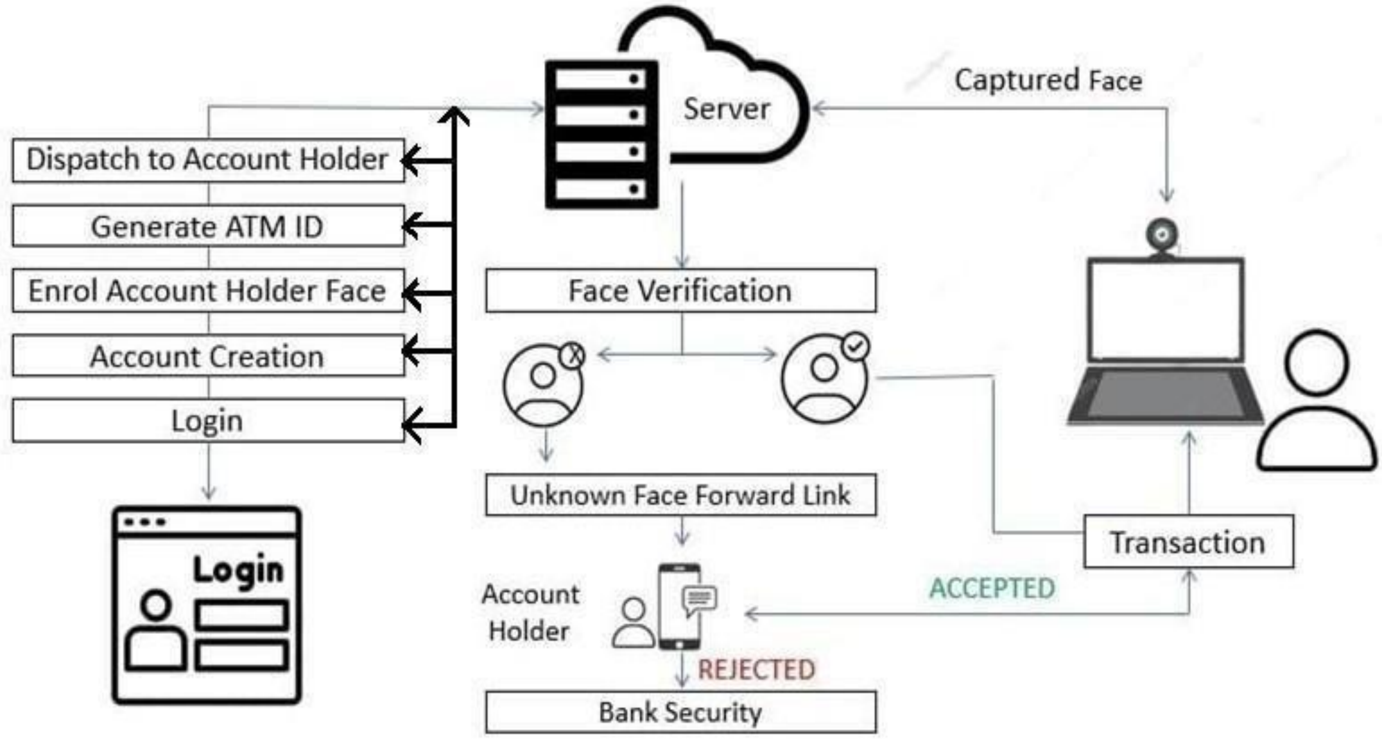


Figure2.1 SystemArchitecture

The system architecture below illustrates how a user utilizes the ATM simulation to perform a transaction. At first, the user must enter the login page by using admin credentials.

After entering the admin credentials, it verifies those credentials, which are stored in the database. If it matches, it goes to an account creation page. After entering the login page, the user can create an account on the account creation page by using the user credentials like username, mail ID, phone number, address, etc.

After creating an account, the user must enroll their face, which gets stored in the database to generate an ATM ID and send it to the account holder's email. All those user credentials are stored in the database.

While performing the transaction process at that time, it lively captures your face and goes to face verification. In this process, it verifies your face by comparing your captured face with the stored face in the database.

If it matches, the user can proceed with the transaction process; if it does not, it sends an unknown face-forward link to the account holder's phone number. When the user clicks the link, it goes to a webpage where it captures an unknown face. The user has the option to accept or reject it.

If the user clicks accept, the transaction process will proceed further; if not, it will get out of the transaction process or block the transaction.

IV CNN ALGORITHM

There are three types of layers that make up the CNN which are the convolutional layers, pooling layers, and fully-connected (FC) layers. When these layers are stacked, a CNN architecture will be formed. In addition to these three layers, there are two more important parameters which are the dropout layer and the activation function which are defined below.

1. Convolutional Layer:

This layer is the first layer that is used to extract the various features from the input images. In this layer, the mathematical operation of convolution is performed between the input image and a filter of a particular size MxM. By sliding the filter over the input image, the dot product is taken between the filter and the parts of the input image with respect to the size of the filter (MxM). The output is termed as the Feature map which gives us information about the image such as the corners and edges. Later, this feature map is fed to other layers to learn several other features of the input image.

2. Pooling Layer:

In most cases, a Convolutional Layer is followed by a Pooling Layer. The primary aim of this layer is to decrease the size of the convolved feature map to reduce the computational costs. This is performed by decreasing the connections between layers and independently operates on each feature map. Depending upon method used, there are several types of Pooling operations. In Max Pooling, the largest element is taken from feature map. Average Pooling calculates the average of the elements in a predefined sized Image section. The total sum of the elements in the predefined section is computed in Sum Pooling. The Pooling Layer usually serves as a bridge between the Convolutional Layer and the FC Layer

3. Fully Connected Layer:

The Fully Connected (FC) layer consists of the weights and biases along with the neurons and is used to connect the neurons between two different layers. These layers are usually placed before the output layer and form the last few layers of a CNN Architecture.In this, the input image from the previous layers is flattened and fed to the FC layer. The flattened vector then undergoes few more FC layers where the mathematical functions operations usually take place. In this stage, the classification process begins to take place.

4. Dropout:

Usually, when all the features are connected to the FC layer, it can cause over fitting in the training dataset. Over fitting occurs when a particular model works so well on the training data causing a negative impact in the model’s performance when used on a new data. To overcome this problem, a dropout layer is utilized wherein a few neurons are dropped from the neural network during training process resulting in reduced size of the model. On passing a dropout of 0.3, 30% of the nodes are dropped out randomly from the neural network.

5. Activation Functions:

Finally, one of the most important parameters of the CNN model is the activation function. They are used to learn and approximate any kind of continuous and complex relationship between variables of the network. In simple words, it decides which information of the model should fire in the forward direction and which ones should not at the end of the network. It adds non-linearity to the network. There are several commonly used activation functions such as the ReLU, Soft Max, tanH and the Sigmoid functions. Each of these functions have a specific usage. For a binary classification DCNN model, sigmoid and Soft Max functions are preferred a for a multi-class classification, generally Soft Max us used. 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

VI.MODULES

1. ATM Simulator

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.

2. FACE RECOGNITION MODULE

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.

Face Authentication: 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. 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.

3. UNKNOWN FACE FORWARDER MECHANISM

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, whicheither authorizes the transaction appropriately or signals a security-violation alert to the banking security system.

4. TRANSACTION MODULE

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. C.EXPERIMENTAL RESULT: 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. 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 encourage into 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

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

REFERENCES

JOURNAL REFERENCES:

[1] 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.

[2] I. Cohen, N. Sebe, A. Garg, L. S. Chen, and T. S. Huang, "Facial expression recognition from video sequences: temporal and static modeling," Computer Vision Image Understanding, vol. 91, no. 1-2, pp. 160-187, 2003.

[3] 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.

[4] A. Had, S. Benouar, M. Kedir-Talha, F. Abtahi, M. Attari, and F. Seoane,``Full impedance cardiography measurement device using raspberryPI3 and system-on-chip biomedical instrumentation solutions," IEEE J.Biomed. Health Informat., vol. 22, no. 6, pp. 1883-1894, Nov. 2018.

[5] B. Heisele, P. Ho, and T. Poggio, "Face recognition with support vector machines: Global versus component-based approach," in Proc. of Eighth International Conference on Computer Vision (ICCV'01), Vancouver, Canada, Jul 2001, pp. 688–694.

[6] C. Huang, H. Ai, B. Wu, and S. Lao. Boosting nested cascade detectorsfor multi-view face detection. ICPR 2004, pp. 415–418.

[7] M. Karovaliya, S. Karedia, S. Oza, and D. Kalbande, "EnhancedSecurity for ATM Machine with OTP and Facial RecognitionFeatures," Procedia Computer Science, vol. 45, pp. 390-396,2015.

[8] J. Liang, H. Zhao, X. Li, and H. Zhao, ``Face recognition system basedon deep residualnetwork," in Proc. 3rd Workshop Adv. Res. Technol. Ind.(WARTIA), Nov. 2017.

[9] A. Li, S. Shan, and W. Gao, ``Coupled bias-variance tradeoff for cross-poseface recognition," IEEE Trans. Image Process., vol. 21, no. 1, pp. 305-315,Jan. 2012.

[10] X. Pan, ``Research and implementation of access control system basedon 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.

[11] K. J. Peter, G. Nagarajan, G. G. S. Glory, V. V. S. Devi, S.Arguman, and K. S. Kannan, "Improving ATM security via facerecognition," in Electronics Computer Technology (ICECT),2011 3rd International Conference on, 2011, pp. 373-376.

[12]S.Pravinthraja and K.Umamaheswari, "Multimodal Biometricsfor Improving Automatic Teller Machine Security," BonfringInternational Journal of Advances in Image Processing, vol. 1,pp. 19-25, 2011.

[13] R.Rasu,P.Kumar,"Security for ATM Terminal Using Various Recognition Systems," International Journal of Engineering and Innovative Technology (IJEIT), vol. 2, 2012.

[14] T. Sharma and S. L. Aarthy, ``An automatic attendance monitoring systemusing RFID and IOT using cloud," in Proc. Online Int. Conf. Green Eng.Technol. (IC-GET), Nov. 2016, pp. 1-4.

[15] E. Spinella, "Biometric Scanning Technologies: Finger, Facialand Retinal Scanning," SANS Institute, San Francisco, CA, vol.28, 2003.

[16] J. K. Suhr, S. Eum, H. G. Jung, G. Li, G. Kim, and J. Kim, "Recognizability assessment of facial images for automated teller machine applications," Pattern Recognition, vol. 45, pp. 1899-1914, 2012.

[17] I. Taleb, M. E. Amine Ouis, and M. O. Mammar, ``Access control usingautomated face recognition: Based on the PCA & LDA algorithms," inProc. 4th Int. Symp.ISKO-Maghreb, Concepts Tools Knowl. Manage.(ISKO-Maghreb), Nov. 2014, pp. 1-5.

[18] S. Thorat, S. Nayak, and J. P. Dandale, "Facial recognition technology: An analysis with scope in India," arXiv preprint arXiv:1005.4263, 2010.

WEB REFERENCES:

[1] GitHub,https://github.com/opencv

[2]MDN Web Docs,https://developer.mozilla.org/