e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 13, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 7, Issue 13, April 2024 ||

International Conference on Intelligent Computing & Information Technology (ICIT-24)

Organized by

Erode Sengunthar Engineering College, Erode, Tamilnadu, India

Face Biometric Authentication System for Atm Using Deep Learning

Ms.K. Indhumathi[1], R. Karpagajothi[2], K. Nivethitha[3], A. Swetha[4]

Assistant Professor, Dept. of CSE, Shree Venkateshwara Hi Tech Engineering College, Gobichettipalayam, Tamil Nadu, India[1]

Student, Dept. of CSE, Shree Venkateshwara Hi Tech Engineering College, Gobichettipalayam, Tamil Nadu, India[2,3,4]

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.

KEYWORDS: Biometric Authentication, Automated Teller Machine (ATM), Deep Learning, Convolutional Neural Networks (CNNs), Facial Recognition, Security, Fraud Prevention, Identity Verification, Financial Transactions, Machine Learning, Authentication Technology.

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. 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.

A) FACE DETCTION

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.

B) PREDICTIVE ANALYSIS

Validation and Testing: Validate the trained model using cross-validation techniques and evaluate its performance on a separate test dataset. Measure metrics such as accuracy, precision, recall, and F1- score to assess the model's effectiveness in authentication tasks.Predictive Analysis: Once the model is trained and validated, deploy it to the ATM system for real-time authentication. When a user attempts to access the ATM, capture their facial image and input it into the model. The model then predicts whether the authentication attempt is successful or not based on learned patterns from the training data.Continuous Learning: Continuously update the deep learning model using feedback from

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 7, Issue 13, April 2024 ||

International Conference on Intelligent Computing & Information Technology (ICIT-24)

Organized by

Erode Sengunthar Engineering College, Erode, Tamilnadu, India

real-world authentication attempts. Incorporate mechanisms for online learning to adapt the model to evolving trends and mitigate performance degradation over time.Security and Privacy Considerations: Implement robust security measures to protect the biometric data and ensure user privacy. Use encryption techniques to safeguard data transmission and storage, and comply with regulations such as GDPR and CCPA

C) 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).

II. RELATED WORK

"Facial Recognition for ATM Security Using Convolutional Neural Networks" by Saraf et al. In this work, the authors present a CNN-based facial recognition system designed specifically for ATM security. They evaluate the system's performance on real-world ATM authentication tasks and demonstrate its effectiveness in preventing unauthorized access."Deep Learning-Based ATM Security System Using Facial Recognition" by Liu et al. This paper proposes an ATM security system that employs deep learning for facial recognition. The authors develop a CNN model trained on a large dataset of facial images to authenticate users at ATMs, enhancing security and user convenience. "Enhancing ATM Security Using Deep Learning- Based Face Recognition" by Sharma et al. This study investigates the use of deep learning-based face recognition for enhancing ATM security. The authors develop a robust authentication system based on CNNs, addressing challenges such as illumination variations and occlusions in facial images."Face Recognition for ATM Security: A Survey" by Gupta et al. This survey paper provides an overview of face recognition techniques used in ATM security systems. It covers traditional methods as well as recent advancements in deep learning- based approaches, discussing their strengths and limitations in the context of ATM authentication.

III. EXISTING 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 QR app 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 Gaussian Mixture Models (GMMs), Artificial Neural Networks (ANNs), Fuzzy Expert Systems (FESs), and Support Vector Machines (SVMs). 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

IV. PROPOSED SYSTEM

This project proposes an automatic teller machine multi modal security model that would combine a physical access card and electronic facialrecognition 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 antispoofing 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.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 7, Issue 13, April 2024 ||

International Conference on Intelligent Computing & Information Technology (ICIT-24)

Organized by

Erode Sengunthar Engineering College, Erode, Tamilnadu, India

V. ABOUT THE CNN ALGORITHM

One of the most popular types of deep neural networks is known as convolutional neural networks (CNN or ConvNet). A CNN convolves learned features with input data, and uses 2D convolutional layers, making this architecture well suited to processing 2D data, such as images. CNNs eliminate the need for manual feature extraction, so you do not need to identify features used to classify images. The CNN works by extracting features directly from images. The relevant features are not pretrained; they are learned while the network trains on a collection of images. This automated feature extraction makes deep learning models highly accurate for computer vision tasks such as object classification. 4 CNNs learn to detect different features of an image using tens or hundreds of hidden layers. Every hidden layer increases the complexity of the learned image features. For example, the first hidden layer could learn how to detect edges, and the last learns how to detect more complex shapes specifically catered to the shape of the object we are trying to recognize. Deep learning is a specialized form of machine learning. A machine learning workflow starts with relevant features being manually extracted from images. The features are then used to create a model that categorizes the objects in the image. With a deep learning workflow, relevant features are automatically extracted from images. In addition, deep learning performs “end-to-end learning” – where a network is given raw data and a task to perform, such as classification, and it learns how to do this automatically.

VI. INPUT DATASET

Authorized User Images: Collect facial images of individuals who are authorized to use the ATM. These images should cover a variety of poses, expressions, lighting conditions, and occlusions to ensure robustness of the system. Ensure that the images are of high quality and accurately represent the authorized users.Non-Authorized User Images: Collect facial images of individuals who are not authorized to use the ATM. These images should also cover a range of variations to ensure the system can distinguish between authorized and unauthorized users effectively.Data Augmentation: Augment the dataset by applying transformations such as rotation, scaling, cropping, and flipping to increase the diversity of the images. This helps improve the robustness of the deep learning model to variations in facial appearance.Data Labeling: Label each image in the dataset as either an authorized user or a non-authorized user. This labeling is crucial for training the deep learning model in a supervised manner.Dataset Splitting: Split the dataset into training, validation, and testing sets. The training set is used to train the model, the validation set is used to tune hyperparameters and monitor for overfitting, and the testing set is used to evaluate the final performance of the trained model. Preprocessing: Preprocess the images to standardize their size, color, and orientation. This ensures consistency in the input data and facilitates training of the deep learning model.

VII. PREPROCESSING

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,Resizeimage,Removenoise(Denoise),Sm ooth 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.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 7, Issue 13, April 2024 ||

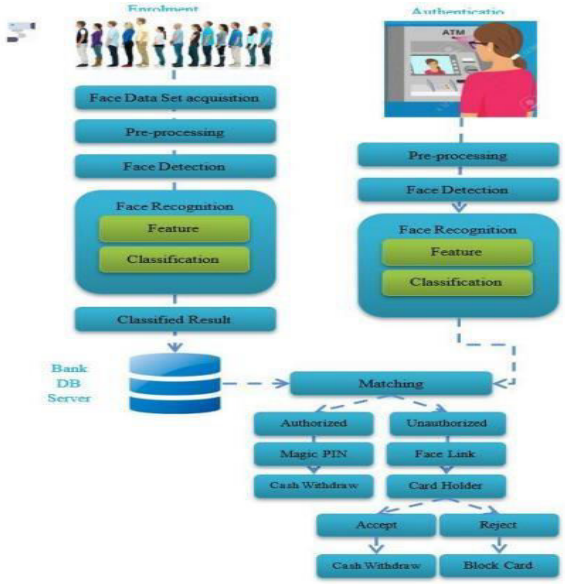
International Conference on Intelligent Computing & Information Technology (ICIT-24)

Organized by

Erode Sengunthar Engineering College, Erode, Tamilnadu, India

VIII. DOCUMENT TERM MATRIX CONSTRUCTION

Represent each document as a vector in a high- dimensionalspace,where eachdimensioncorresponds to a unique term in the vocabulary. Organize the document representations into a matrix format, where rows represent documents and columns represent terms. Each cell in the matrix contains the corresponding value representing the frequency, TF-IDF score, or embedding of a term in a document.



ARCHITECTURE DIAGRAM

IX. RESULT

Here, we count some results obtained by knowledge distillation in the field of target detection. The datasets VOC07+12 and MSCOCO. VOC and COCO are commonly used for target detection and image segmentation.VOC 07+12 has 20 object categories, COCO contains 164K images, and COCO has 80 object categories, which are challenging and authoritative. The detection network is the classical two-stage algorithm FasterRCNN, where the teacher-student backbone network is either a resnet101-resnet50 combination or a RetinaNet101-RetinaNet50 combination. We summarize the results of knowledge distillation for target detection over the past 5 years, and we compare the advantages and disadvantages of each distillation method from a fair perspective. From the table below, we can clearly see that knowledge distillation can significantly raise the performance of minimodels without changing the structure of the network, and knowledge distillation can make a great contribution to the deployment of future projects. From the data in the tables, we can find that there are three types of knowledge that can be used for knowledge distillation, feature-based, response-based, and relationshipbased knowledge.

In our perception, the images are background except for the detected objects, and the computation of background features wastes a lot of computational resources and seriously affects the detection performance, but [40], [43] found that background features are also helpful for detection performance, and in addition, current knowledge distillation methods ignore the role of categories outside the dataset for target detection, and arbitrarily discarding background features is an unwise choice. The intermediate layer features utilized in knowledge distillation want to prefer the student feature maps to be as similar as possible to the teacher feature maps by calculating a distance between the feature maps and adding the distance values to the loss function and then using backpropagation to improve the degree of similarity between teacher feature maps and student feature maps. Response-based knowledge is for students to imitate the soft output of the teacher's network, using additional information about the similarities within and between classes, which is the simplest and most efficient way to handle this, but this would be missing the supervisory information in the middle layer, which is not a very significant performance gain for the student network. The most

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 7, Issue 13, April 2024 ||

International Conference on Intelligent Computing & Information Technology (ICIT-24)

Organized by

Erode Sengunthar Engineering College, Erode, Tamilnadu, India

commonly used in current knowledge distillation is the combination of featurebased and response-based knowledge [25], [38], [40], [50], [53], [73]. Relationship-based knowledge [41], [43], [74], [75], [76], [77]is an extension of response-based knowledge and feature-based knowledge, and it studies the relationship between different layers and samples more comprehensively and deeply.

X. CONCLUSION AND FUTURE WORK

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

REFERENCES

1. 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.
2. 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.
3. 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.
4. Taleb, M. E. Amine Ouis, and M. O. Mammar,
5. ``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.
6. 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.
7. 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.
8. T.R.Lekhaa, “Secured credit card transaction using web cam” International Research Journal of Engineering and Technology, April 2016.
9. 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.
10. 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.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com