CARD-LESS ATM USING FINGERPRINT AND FACE RECOGNITION TECHNIQUES

[*1] Dr. P. Sreenivasulu, [2]M.Susmitha, [3]M.Chitra , [4]CH. V. Navya Sree, [5]CH. Mounika

[*1]Dr. P. Sreenivasulu Professor of ECE Department, NECG

[2]M. Susmitha student of ECE Department NECG

[3]M. Chitra student of ECE Department NECG

[4]Ch. V. Navya Sree student of ECE Department NECG

[5]Ch. Mounika student of ECE Department NECG

ABSTRACT

In the field of biometric security, this study presents a Card-less ATM system leveraging fingerprint and face recognition techniques with a focus on Convolutional Neural Networks (CNN) and deep learning, implemented in the MATLAB domain. The methodology involves the acquisition of a dataset comprising fingerprint and face samples, followed by their training through a CNN model. During testing, both fingerprint and face images must belong to the same individual for authentication success, and a message box displays, granting access for transactions. In the case of a mismatch between the provided images or when they correspond to different individuals, the system responds with an "Authentication failed. Please try again." message. The system's accuracy relies on the efficient pre-processing of images, including resizing, ensuring reliable recognition and reducing false positives. This research contributes to enhancing ATM security by combining multiple biometric modalities to verify the user's identity, ultimately improving the accuracy and reliability of the authentication process.

Keywords: Fingerprint and face dataset, preprocessing, Splitting, Validation Security systems, Convolutional neural networks, Deep Learning, classification and Accuracy.

I. INTRODUCTION

An automatic teller system (ATM) is an electronic banking outlet that permits customers to entire primary transactions without visiting branch. ATMs are convenient, These ATM allows customer to perform cash withdraw, deposit and balance checking. Fees are generally charged for the use of ATM cards bank where the account is located, all those charges will be avoided if we do not use ATM cards. If any transaction or withdrawals should be made the we should visit the bank that holds the account. Anyone with a ATM card (Debit or Credit) can withdraw cash with the pin which is set by the person who holds the account. Generally, ATM's will be located by the bank in public places like Traffic areas, shopping mall, Stores like grocery and convenience, Airport, Railway station, Bus stop, Fuel station, Restaurant etc. The ATM card comes with a plastic card and the chip inside of it where we can swipe inside the ATM machine and in recent times many ATM cards also coming with the WIFI option where we don't want to swipe the card for paying bills. But in current situation there is a threat of stollen of ATM cards. The money can be withdrawal if somebody gets the ATM pin with the card. If we want to withdraw cash, we always need to carry ATM card with us.

II. LITERATURE SURVEY

Dileep Kumar [1] provides a way that using Biometric fingerprints in payment system is much safe and secure and very easy to use and even without using any password or secret codes to remember as compare with previous system like debit card payment system. In biometric algorithm, several data points on the fingerprint'sdata scientifically measured and stored. The Algorithm measures 40+ data points of fingerprint. Fingerprints basically consist of ridges and furrows. Techniques to match finger-print can be done in two categories: Those are minutiae based and other is correlation based. First it checks the minutiae points in finger and then it maps their relative minute points in the finger. It is too difficult to extract the finger-prints minutiae points so accurately when the scanned fingerprint quality is too low quality. Correlation-based techniques require the precise location of a registration point and are affected by image translation and rotation.

Yi Sun et al.[2] describes how difficult to recognize face is resolved using “Deep Learning” technique by verifying and identifying the face. The major task for recognizing face we should build a most efficient representation of the feature to lower an intrapersonal variation for increasing the inner variation. The detection of face is increased using DeepID2 captured from the different identifications in the face, So they connected to third and the fourth layer of the CNN to the

DeepID2. Then they achieved 99.15% accuracy in the verification of face. As they Compared it with the previous approach of “Deep Learning” the rate of error is decreased to 67%.

[3] The “Deep Neural Network” provides us a method of stacking to process a modules with simple way for building the deep architectures, with a convex learning problem in each of the module. For fine tuning the further process improves the Deep Stack Network. In the Deep Neural Network training is in the batch-mode,

makes it to the parallel training on many of the machines and it is also scalable with the huge sizes for training those datasets. The results of the Experiment on MNIST which is the Image datasets and TIMIT which is the speech datasets classification displays the Deep Stack Network technology introduced and this kind it is not only parallelizable in the implementation also it shows the high level of accuracy in classification than the “Deep Neural Network” which is proposed by Li Deng et al.

Yann LeCun et al Reff.[4] mentions that "Deep learning" describes the complete structure in the huge amount of datasets by using a algorithm which is backpropagation algorithm which shows how a machine should change its parameters where it is used to calculate each layer from its previous ones. It allows the conventional models which are made of multiple processing to learn the representations of datasets with abstraction of multiple levels. This models has increased the accuracy in recognizing the voice and detecting object in video. The Deep CNN will process audio, video and images also the recurrent networks will process in text and also the speech.

Haleh Vafaie et al. [5] describes us how to use “Machine Learning” Techniques for creating the classification rules for the complex and also the Real-World data. This technique reduce total number of the features which is more necessary for the classification of texture and at the same time it makes the improvements in the rate for recognition. It uses GA-Genetic Algorithm as Frontend for the traditional rule induction system for the detectionof the best subset of feature which will be used by the “Rule Induction System”.

III. PROPOSED SYSTEM

We propose a new method of withdrawing money where it will be a completely cardless system Using our face and finger-print of the account holder we can withdraw cash with safer and faster. While the user opens the account on the same time the account holders face and finger-print will be scanned and those data will be stored in the separate database. As the population is more the processing speed will become slow if the system needs to check each and everyone’s face and finger-print. So first we enter the account holder name, pin and mobile number, then the system compares scanned face and finger-print in the ATM with the stored face and finger-print of the account holder in the database. Here we are using Convolutional Neural Network for the detection of face and the finger-print.

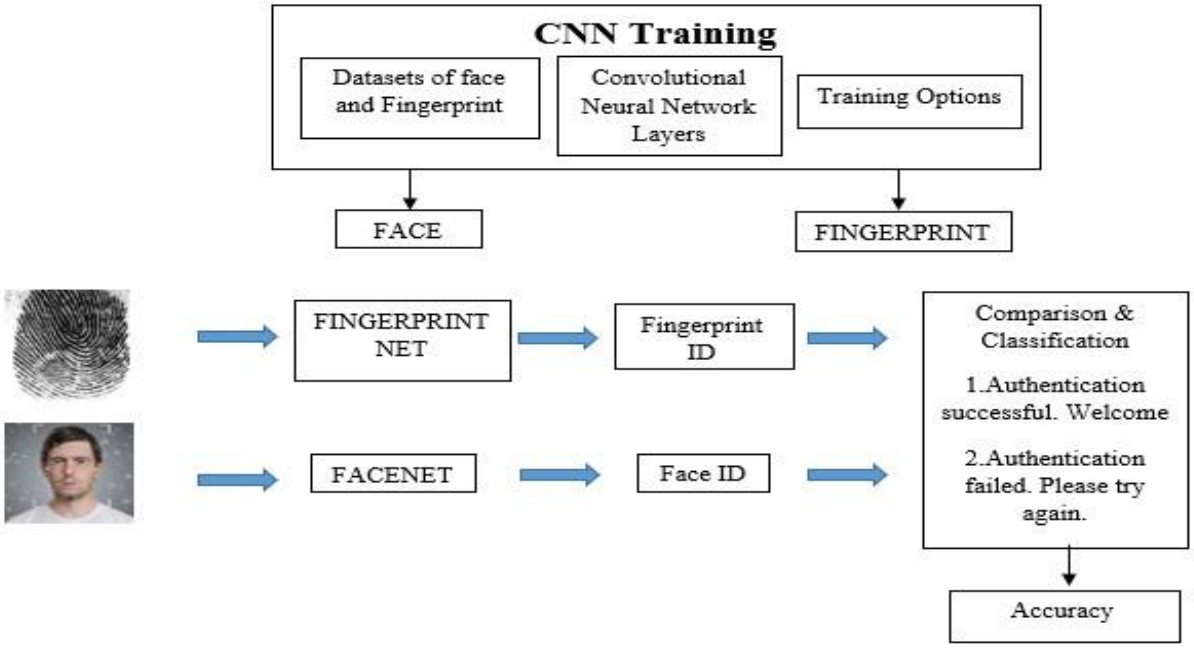
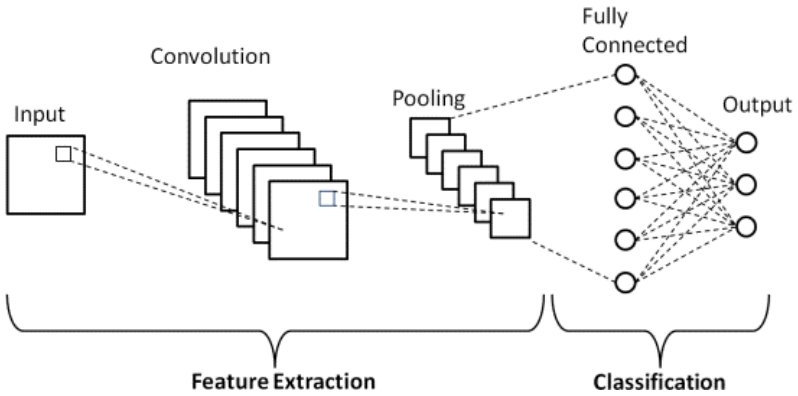


Figure 1: Workflow of Proposed System.

IV. IMPLEMENTATION



The project is implementing a card-less ATM system using face and fingerprint recognition techniques involves utilizing Convolutional Neural Networks (CNNs) and MATLAB. The system first captures the user's face and finger print data through high-resolution cameras and scanners. These inputs are preprocessed to enhance quality and remove noise. A CNN, trained on a large Dataset of facial and fingerprint images, then extracts features and performs recognition. MATLAB's deep learning toolbox can be used to design and train the CNN model. Once the user is authenticated by matching the live inputs to the stored database, the ATM grants access. This approach ensures high security and convenience by eliminating the need for physical cards..

Convolutional Neural Network

The word 'Convolution" in the Convolution Neural Network describes a type linear operation using a mathematical function Here two functions will be multiplied to produce another function which displays how shape of a function is changed by another function. Here Images will be represented in the matrix form and it will be multiplied to give output they will be known as extracted features of a image.

Figure 2: CNN Architecture

The above figure describes a simple CNN architecture.

1. Input Layer
2. Convolution Layer
3. Pooling Layer.
4. Fully Connected Layer.
5. Output Layer.

Datasets

Datasets of the fingerprint is taken from the Kaggle website and those data were undergone for the training andtesting and the face images were matched with the set of fingerprints and then the data is passed in the CNN model.

Data Pre-processing

Pre-processing is the step in analyzing any dataset, which includes removing unwanted images to clean the dataset for training purposes. And also added some of the missing data in the dataset.

First, we stored 200 face images which belongs to 5 classes 180 face images passed for training and 20 face images passed for testing.

Then we stored 200 Finger-print images which belongs to 5 classes 180 Finger-print images passed for training and 20 Finger-print images passed for testing.

Methodology

For Binary Images, The pixels of image value ranges between 0 to 255. (Zero means complete black, 255 means

complete white. The greyscale ranges between 0 and 1.

For Colored Image, there will be three layers those are a red layer, a green layer, and a blue layer. Each colors have its unique value ranges between 0 -255.

First, we should import all the necessary libraries. Then stored datasets path will be set and here the images are resized with height=150 and width=150. The datasets are stored in three classes and we have just confirmed that the images belong to same class or not.

Once The datasets of Face and Finger-print is passed into training and testing those datasets were normalized into 0 or 1. The image will be in matrix format with the values of 0 and 1.

Then the input image will be multiplied with the Feature Detector which is the random value produced in the CNN and then values will be stored in a matrix form and that matrix is called as Feature Map.

Once all the Input Image values are multiplied and stored in the Feature Map. This Feature Map values goes under the process of Max Pooling.

After Max Pooling that values is called as Pooled Feature Map. In the next process Flattening. Here all the valuesare stored in sequential order and then Flattened values are passed in the Fully Connected Layer.

Here we have selected Epoch=40 and then the model provides the Training and Validation Accuracy, Training and Validation Loss. Finally, the Image will be classified for which class it belongs to in the three classes.

Application

Once during testing, both fingerprint and face images must belong to the same individual for authentication success, and a message box displays, granting access for transactions. In the case of a mismatch between the provided images or when they correspond to different individuals, the system responds with an "Authentication failed. Please try again." Message. This research contributes to enhancing ATM security by combining multiple biometric modalities to verify the user's identity, ultimately improving the accuracy and reliability of the authentication process.

V. DIFFERENCES

Feature	Proposed Method	Existing Method
Authentication Method	Biometric (Fingerprint and Face Recognition)	Card and PIN
Security Level	Higher due to unique biometric data	Moderate; susceptible to card skimming, PIN theft, and cloning
Speed of Transaction	Faster; quick biometric scan	Slower; involves inserting card and entering PIN
Risk of Fraud	Lower; difficult to replicate biometric data	Higher; cards can be stolen or cloned, and PINs can be observed
User Experience	Enhanced; seamless and user-friendly	Standard; can be cumbersome with card handling

VI. RESULTS

Face Recognition

We used 200 face images which belonged to 5 classes and here 180 images used for training purpose and 20 images used for validation purpose. These images are considered as datasets and it is passed in the CNN model and the total number of epochs, we used is 40. The results for detecting face are 100%.

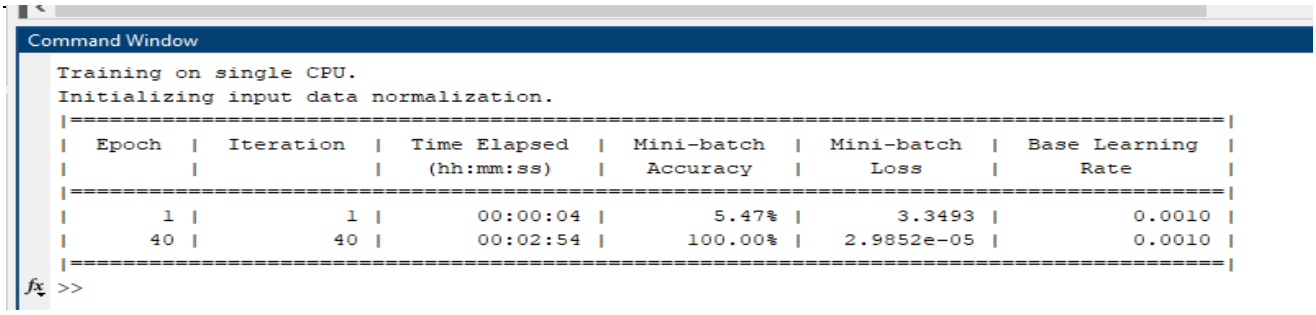


Figure 3: Training and Validation Accuracy and loss

From the above table we can observe the Training and Validation Accuracy, Training and Validation Loss.

Finger-Print Recognition

We used 200 finger-print images which belonged to 5 classes and here 180 images used for training purpose and 20 images used for validation purpose. These images are considered as datasets and it is passed in the CNN model and the total number of epochs, we used is 40. The results for detecting finger-print are 100%.

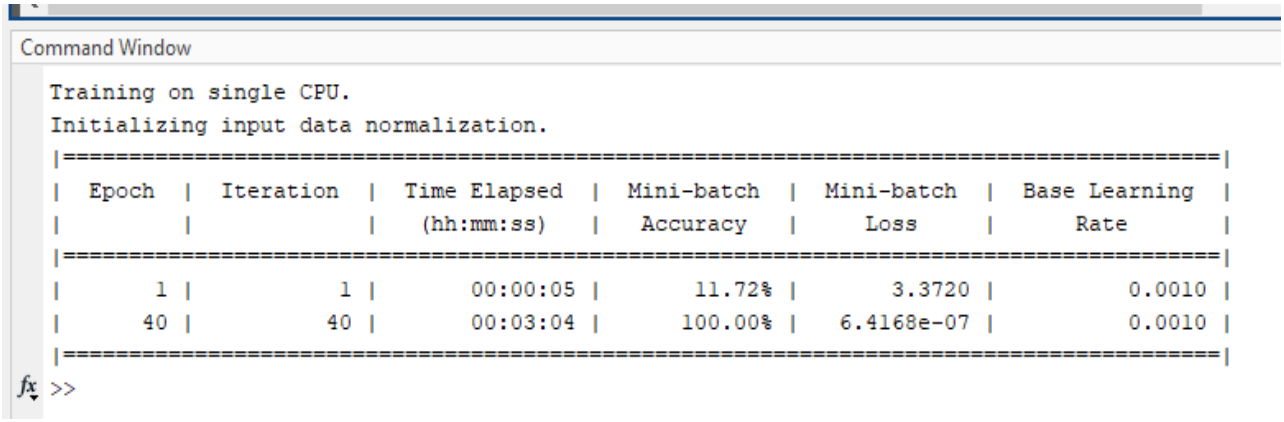


Figure 4: Training and Validation Accuracy and loss

From the above table we can observe the Training and Validation Accuracy, Training and Validation Loss.

VII. CONCLUSION

The implementation of a card-less ATM system that employs fingerprint and face recognition techniques is a promising advancement in financial technology. This project involves the collection and preprocessing of fingerprint and face datasets, followed by their careful separation into training and validation sets. The security aspects of this system are enhanced by employing state-of-the-art convolutional neural networks (CNN) and deep learning algorithms. The classification process utilizes the CNN model to compare the provided fingerprint and face data with the stored data, leading to a binary authentication outcome. When the provided data matches the stored data (belonging to the same person), authentication is successful, and the user is welcomed to access the ATM. Conversely, if the data does not match, authentication fails, prompting the user to try again. This project aims to provide a secure and convenient alternative to traditional card-based ATM access and showcases the potential of advanced biometric technologies to enhance financial services.

VIII. FUTURE SCOPE

1. Enhanced Security Measures:

➢ Multimodal Biometrics: Integrating additional biometric modalities such as iris recognition, voice recognition, and vein pattern recognition to further strengthen security.

➢ Advanced Anti-Spoofing Techniques: Developing and incorporating sophisticated anti-spoofing algorithms to detect and prevent fraudulent attempts using fake fingerprints or photos.

2. Machine Learning and AI Improvements:

➢ Continuous Learning: Implementing systems that continuously learn and adapt to new data, improving accuracy and robustness of the biometric recognition models over time.

➢ Federated Learning: Utilizing federated learning approaches to enhance the system's capability to learn from a distributed dataset without compromising user privacy.

IX. REFERENCES

[1] Dileep Kumar, Dr.Yeonseung Ryu, Dr.Dongseop Kwon. A Survey on Biometric Fingerprints: TheCardless Payment System, Auguest 2008.

[2] Yi Sun, Yuheng Chen, Xiaogang Wang, Xiaoou Tang. Deep Learning Face Representation by Joint Identification-Verification, June 2014.

[3] Li Deng, Dong Yu, and John Platt, "Scalable stacking and learning for building deep architectures", IEEE, 2012.

[4] Yann LeCun, Yoshua Bengio, and Geoffrey Hinton, "Deep learning", 27 May 2015.Université de Montréal,2009 International Society for Music Information Retrieval.

[5] Haleh Vafaie and Kenneth De Jong, "Genetic Algorithms as a Tool for Feature Selection in Machine Learning", IEEE, Nov. 1992.