Deep Learning based Card-Less Atm using Fingerprint and Face Recognition Techniques

Ayusha Mohite[1], Shruti Gamare[2], Karan More[3], Nita Patil[4]

[1,2,3]*Student, Computer Department, Datta Meghe College of Engineering, Maharashtra, India*
[4]*Professor, Computer Department, Datta Meghe College of Engineering, Maharashtra, India*

Abstract - *The current ATM (Automated Teller Machine) system uses ATM card and PIN (Pin Identification Number) for authentication. This system is likely to be harmed by many security issues such as theft of ATM card, skimming, Lebanese loop etc. So in this paper, we propose a system that uses fingerprint and face recognition authentication (not ATM cards) for accessing user account along 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.*

Keywords: *CNN, Features, ATM, PIN*

1. INTRODUCTION

ATM (Automated Teller Machine) is generally used for withdrawal of money from our Bank account without going to the bank. By means of ATM which is used as an agent through which we can access our bank account remotely by providing atm card details with a proper PIN, one can withdraw, deposit or check the account balance. But in today's ATM technology there is always a chance of stealing money. The money can easily be stolen if one gets the access to ATM card and security pin number rather there is always a chance of losing ATM card and during that period withdrawal of money gets difficult. In addition to it we always have to carry ATM card everywhere we go and only one person can have access to the card which sometimes can get pretty difficult .when members of the same family want to withdraw cash, who are at different locations. In addition, if you are a totally new in area or country and the purse you are carrying in which all of your cash and ATM card are kept gets stolen then undoubtedly it will be the worst situation to survive. To overcome such drawbacks the idea of a card-less ATM which uses fingerprint and face recognition for authorization and authentication of user seems quite useful and reliable. For instance, if two members of the same family are at the different location of a country then both of them can have access to the same account anywhere and anytime they want without carrying an ATM card. In this technology, we take user's fingerprint and face-print as a replacement for ATM card of which data is stored in the separate server to provide a common ground for accessing fingerprint through any bank's ATM and with face recognition we add a double layer of security of which data is stored in particular bank's server. By providing the data of fingerprint and face id of two members for a particular account a single account can be accessed by two persons.

2. LITERATURE SURVEY

Deep learning is a machine learning technique teaches computers to do what comes naturally to humans: learn by example. Deep learning is a main key technology behind driverless cars, allowing them to recognize a stop sign, or to distinguish a pedestrian from a street sign. It is the main key to voice control in devices like TVs, phones, tablets, and hands-free speakers. Deep learning is receiving lots of attention nowadays and for good reasons. It has achieving results that were almost impossible before. In it, a computer model learns to do classification tasks directly from images, text, or sound. These models can achieve state-of-the-art accuracy, sometimes overthrowing human-level performance. Models are trained by using a big set of labeled data and neural network architectures which contain many layers.

Haleh Vafaie et al. [1] provides us a way to improve the usefulness of machine learning techniques for generating classification rules for complex, real-world data.This approach reduces the number of features necessary for texture classification and simultaneously makes improvements in recognition rates. The approach involves the use of genetic algorithms (GA) as a front end to traditional rule induction systems in order to detect and select the best subset of feature to be used by the rule induction system. This technique has been implemented and tested on difficult texture classification problems.

Yi Sun et al.[2] show that the difficulties with face recognition can be well solved with deep learning and using both face verification and identification signals as supervision. The challenge of face recognition is to build effective feature representations for lowering intra-personal variations while enlarging inter-personal differences. The face identification task increases the inter-personal variations by drawing DeepID2 features obtained from various identities apart, while the face verification task lowers the intra-personal variations by pulling DeepID2 features obtained from the same identity together, both of which are essential to face recognition. The learned DeepID2 features can be well generalized to new identities unnoticed in the training data. On the challenging LFW dataset, 99.15% face verification accuracy is maintained. Compared with the previous deep learning result on LFW, the error rate has been drastically reduced by 67%. Deep Learning Face Representation by Joint Identification-Verification reduces intra-personal variations while enlarging inter-personal differences.

Scalable stacking and learning for building deep architectures Deep Neural Networks (DNNs) has shown remarkable success in pattern recognition tasks. However, parallelizing DNN training across computers has been difficult. Presenting the Deep Stacking Network (DSN), this overcomes the problem of parallelizing learning algorithms for deep architectures. The DNN provides a method of stacking simple processing modules in building deep architectures, with a convex learning problem in each module. Additional fine tuning further improves DSN, while introducing minor non-convexity.In the DNN full learning is batch-mode, making it amenable to parallel training over many machines and thus be scalable over the potentially huge size of the training data. Experimental outcomes on both the MNIST (image) and TIMIT (speech) classification tasks demonstrate that the DSN learning algorithm developed in this work is not only parallelizable in implementation but also attains higher classification accuracy than the Deep Neural Network as proposed by Li Deng et al.[3]

Yann LeCun_et al Reff.[4] in the finding of the papers "Deep learning" shown us that the deep learning discovers intricate structure in large data sets by using the backpropagation algorithm to indicate how the machine should change its internal parameters that are used to compute the representation in each layer from the representation in the previous layer.It allows computational models which are composed of multiple processing her archery to learn representations of data with multiple levels of abstraction. These methods have drastically improved the state-of-the-art in speech recognition, visual object recognition, object detection and many other domains such as drug discovery and genomics. The Deep convolution nets have brought about breakthroughs in processing images, video, speech, and audio, whereas recurrent nets have shone a light on sequential data such as text and speech. It also helps to Reduces the need for feature engineering Quality and accurate results.

David Menotti_et al [5] shown us that the results strongly indicate that spoofing detection systems based on CN can be robust to attacks already known and possibly adapted, with little effort, to image-based attacks that are yet to come.Biometrics systems have significantly improved person identification and authentication, playing an important role in personal, national, and global security. However, these systems might be deceived and, despite the recent advances in spoofing detection, current solutions often rely on domain knowledge, specific biometric reading systems, and attack types. We assume a very little knowledge about biometric spoofing at the sensor to derive spoofing detection systems for iris, face, and fingerprint modalities based on two deep learning approaches. The first approach consists of learning convolutional network architectures for each domain, while the second approach focuses mainly on learning the weights of the network via back-propagation. We consider nine biometric spoofing benchmarks — each one containing real and fake samples of a provided biometric modality and attack type — and learn deep representations for each benchmark by contrasting and combining the two learning approaches. This strategy provides a better comprehension of how these approaches interplay and also creates systems that exceed the best-known results in eight out of the nine benchmarks. It is used to Detects Iris, Face, and Fingerprint Spoofing.

The evolution of fingerprint recognition according to Author Simon A. Cole [10] summarizes the major developments in the history of efforts to use of fingerprint patterns to identify individuals, Jan Purkyne, a Czech physician and anatomist, which noted the presence of friction ridges on human fingertips. He did make the earliest attempt to classify the pattern types by sorting them into nine categories, which today would correspond to the arch, tented arch, and two types of loop, four types of the whorl, and a twinned loop. Galton made his crucial contribution to the development of fingerprint classification. He realized that the classification system lay in reducing, rather than expanding, the number of pattern types, deciding that all fingerprints could broadly be characterized as one of three basic pattern types: arch, loop, or whorl.

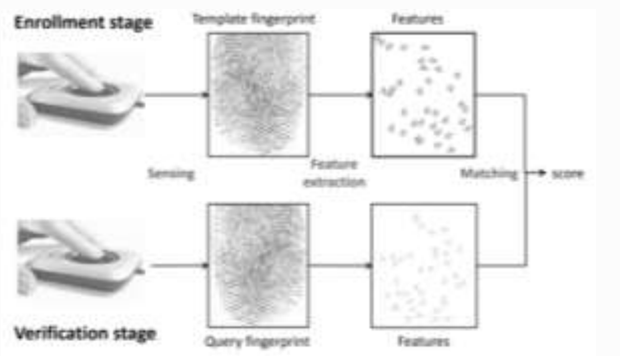

Fig a. The process of Fingerprint recognition

Fingerprint recognition refers to the automated method for identifying or confirming the identity of an individual based on the comparison of two fingerprints. Generally speaking of two types of matching software exist:

1. Minutiae matching relies on recognition of the minutiae points, this is the most widely used technique
2. Pattern matching simply compares the two images to see how similar they are, often used in fingerprint systems to detect duplicates.

According to A.N. Marana et al. [13], Ridges can divide into two ridges (bifurcation). Ridge terminations and bifurcations are considered minutiae Ridge Extraction:- The first step in ridge-based fingerprint matching is the extraction of the fingerprint ridges. Straight Line Extraction:-The second step in the matcher is the extraction of the straight lines that approximate the fingerprint ridges. As proposed by Hong-Ren Su & al [14] a new pore extraction approach based on deep learning, which is specifically, designed and trained a CNN model to recognize pores in a small image block. The advantage of the feature learning capability of CNN's, the proposed method was able to achieve a pore detection rate of 88.6%. Conventional automated fingerprint identification systems (AFIS) utilize the level 1 and 2 features for fingerprint matching. With the current development of fingerprint sensor technology, high-resolution fingerprint images (≥1000 dpi) are more accessible now. With these images, finer fingerprint features (level 3 features) can be extracted and used for fingerprint matching to further enhance the recognition accuracy of AFIS. They also introduced the idea of using AFMM in high-resolution fingerprint matching, which uses the scores of matching ridge pattern, minutiae, and pores. The full testing set of DBI was used for fingerprint recognition performance evaluation. It consists of 1480 high-resolution partial fingerprint images from 148 subjects with10 samples per subject. Experimental results showed that the proposed method yields recognition accuracy comparable to the state-of-the-art methods. As this work demonstrated the potential of using deep learning for pore.

According to Yani Wang & al [12], the CNN model which has seven hidden layer, the activation function of each layer is a sigmoid function. The automatic fingerprint identification method, CNN algorithm, not only improves the recognition rate but also saves processing time. Based on our proposed algorithm, the experiments in this paper are divided into three steps: first: It Pre-process the original image, such as enhancement binarization, denoising and thinning; then Extract the entire feature points from the pre-processed image and fuzz them, the image size remains unchanged at 492*442 and then Input the fuzzy image into CNN for training and recognition; obtain the recognition rate.

A fingerprint segmentation method based on CNN trained with non-overlapping fingerprint image patches. The proposed solution by Author Branka Stojanović et al. [14] consists mainly of four steps: which includes Pre-processing, Sample creation, Processing & Region mask Creation. The fingerprint image is preprocessed to ensure that it is of proper size and acceptable quality; the image is divided into non-overlapping image segments (blocks) of size 16×16 pixels; then the image blocks (segments) are used as input for a previously trained CNN; and the results are merged into a region mask and a smoothing filter is applied to the result. This indicates that this method, unlike the Fourier coefficients based, can be applied to real latent images. In their previous work, they proposed two ROI segmentation methods based on Neural Networks (NN): trained with pixel values of image segments and trained with the Fourier coefficients computed over non-overlapping image segments.

Facial recognition is a type of biometric software which maps an individual's facial features mathematically and stores the data as a face-print. The software uses deep learning algorithms to compare a live capture or digital image to the stored face-print in order to confirm an individual's identity.

Earlier face recognition was not that efficient of what it is today. It used to recognize face considering specific subjective markers including lip thickness and hair color in order to identify faces automatically.

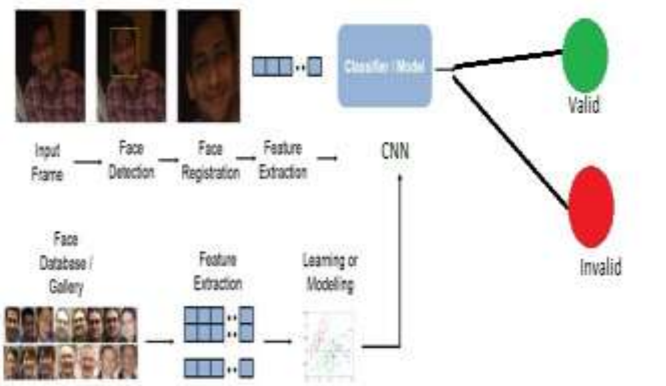

Fig b. The process of Face recognition

However, this previous technology had its limitations it was only able to handle a limited dataset. Performing recognition with large data what somewhat difficult.

Nowadays because of the CNN, it is possible for a computer to deal with the large dataset .not only it is possible to compare but it gets better for the system to increase its performance and train itself through the large data. The more the data the more the training and better the accuracy.

Convolutional neural network (CNN) is a part of machine learning which is a part of artificial intelligence. Convolutional neural networks, like neural networks, are neurons with learnable weights and biases. Each neuron gets several inputs, takes a weighted sum over them, forward it through an activation function and responds with an output. The overall network has a loss function in which all the tips and tricks that we developed for neural networks still apply on Convolutional neural networks.

A CNN is a feed-forward network with the ability to extract topological properties from the input picture. It obtains features from the raw picture and then a classifier classifies extracted features. Convolutional neural networks are invariance to distortions and simple geometric transformations like scaling, rotation, translation and squeezing. CNN combine three architectural ideas to make sure some degree of the scale, shift, and distortion invariance: local receptive fields, shared weights, and spatial or temporal sub-sampling. The network is generally trained as a standard neural network by backpropagation.

There are two main approaches namely as Zeiler & Fergus style networks and e recent Inception type networks. Author Florian Schroff et al. [6] Despite significant recent advances in the field of face recognition, implementing face verification and recognition efficiently at scale presents serious difficulties to current approaches. In this paper, they have presented a system, called FaceNet, that directly learns a mapping from face images to a compact Euclidean space where distances directly correspond to a measure of face similarity. Once this space has been produced, tasks such as face recognition, verification and clustering can be easily implemented using standard techniques with FaceNet embedding as feature vectors. The method uses a deep convolutional network trained to directly optimize the embedding itself, rather than an intermediate bottleneck layer as in previous deep learning approaches. To train, they use triplets of roughly aligned matching / non-matching face patches generated using a novel online triplet mining method.

Adrian Rhesa Septian Seswanto [7] Face Recognition starts with extracting the coordinates of features such as the width of eyes, the width of mouth, pupil, and compare the result with its measurements stored in the database and returns the closest record (facial metrics). Nowadays, there are a lot of face recognition techniques and algorithms found and developed in the world. Facial recognition becomes an interesting research topic. It is proven by a numerous number of published papers related to facial recognition including facial feature extraction, facial algorithm improvements, and facial recognition implementations. Main purposes of this research are to get best facial recognition algorithm (Eigenface and Fisherface) provided by the Open CV 2.4.8 by comparing the ROC (Receiver Operating Characteristics) curve and implement it in attendance system as the main case study. Based on experiments, the ROC curve proves that using the current training set, the Eigenface achieves a better result than Fisherface. Eigenface tested inside the Attendance System returns between 70% to 90% similarity for genuine face images.

This system uses eye blinking recognition for more security by detecting the movements of the eyeball and number of eye blinking for improving the face recognition for screen unlock. For eye detection, our system uses Haar Feature-based Cascade Classifier.

Chung-Hua Chu [8] In recently, eye blink recognition, and face recognition are very popular and promising techniques. In some cases, people can use the photos and face masks to hack mobile security systems, so we propose an eye blinking detection, which finds eyes through the proportion of human face. The proposed method detects the movements of an eyeball and the number of eye blinking to improve face recognition for screen unlock on the mobile devices. Experimental results show that our method is efficient and robust for the screen unlocks on the mobile devices.

Hazem M EI-Bakry [9] Automatic recognition of human faces is a significant problem in the development and application of pattern recognition. Simple technique is introduced for the identification of human faces in cluttered scenes based on neural nets. In the detection phase, neural nets are used to test whether a window of 20/spl times/20 pixels contains a face or not. A major difficulty in the learning process comes from the large databases required for face/nonface images. This problem is solved by dividing these data into two groups. Such a division results in a reduction of computational complexity and thus it decreasing the time and memory needed during the testing of an image. Feature measurements are made through Fourier descriptors for the recognition phase. For training and recognition of ten human faces, such features are used as input to the neural classifier. Simulation results for the proposed algorithm shows a good performance during testing.

In our system, we use the MNN method for extracting the features of the face. It uses the classifier to extract features which accept the input of the 20×20 pixel region of Grayscale image and it generates output region ranging from 1 to -1 for signifying the presence or absence of a face.

3. METHODOLOGY

The System Cardless ATM uses fingerprint recognition and face recognition instead of ATM card for authenticating of the user. The user information is stored into the database while the user opens an account in the bank. The information such as name, email id, mobile number, fingerprints, and face-print is registered into the database. The cardless ATM uses the fingerprint recognition and faces recognition technique for authentication and authorization. Here we have implemented using the real-time database. The face recognition uses CNN model for classification and the fingerprint recognition uses minutiae feature for extraction. Only 4 chances are provided for the user for fingerprint recognition if it doesn't match sends an alert message is sent to the bank server. Then the user needs to visit the bank resolve the issues. Accuracy percentage to be mapped between both the recognition is 70% + for authentication. If the user is valid he/she can withdraw /deposit cash.

Deep learning is part of machine learning methods based on learning data representations, as opposed to task-specific algorithms. Learning can be supervised, semi-supervised or unsupervised [15]. Deep learning models are vaguely inspired by information processing and communication patterns in biological nervous systems yet have various differences from the structural and functional properties of biological brains(especially human brains), which make them incompatible with neuroscience evidence[16].

3.1 Facial Recognition:

Facial recognition is the category of biometric software that maps an individual's facial features mathematically and stores the data as a face-print. The software uses deep learning algorithms to compare a live capture or digital image to the stored face-print in order to verify an individual's identity.

How a simple facial recognition application works:

The software identifies 75-80 nodal points on the human face. In this context, nodal points are endpoints used to measure variable of a person's face, such as length or width of nose, the depth of eye and the shape of cheekbones. The system captures data for nodal points on a digital image of an individual's face and stores the resulting data as a face-print. The faceprint is then used as a basis for comparison with data captured from faces in an image or video.

3.2 Fingerprint Recognition:

Fingerprint recognition refers to the automated method of identifying the identity of an individual based on the comparison of two fingerprints. Fingerprint recognition is one of the most popular biometrics, and it is the most widely used biometric solution for authentication on computerized systems. The reason for fingerprint recognition being so popular is the ease of acquisition, established use and acceptance when compared to other biometric systems, and the fact that there are many sources of this biometric on each individual.

The three basic patterns of fingerprint ridges are the arch, the loop, and the whorl. An arch is a pattern where the ridge enters one side of the finger, then rises in the center forming an arch, and exits on the other side of the finger. a loop that enters one side of the finger, then forms a curve, and exits on the same side of the finger from which it entered. Loops are the most common pattern in fingerprints. A whorl is the pattern which forms ridges form circularly around a central point. Minutiae refers to specific points in a fingerprints, these are the small details in a fingerprint that are important for fingerprint recognition. There are mainly three types of minutiae features: the ridge ending, the bifurcation, and the dot. The ridge ending is indicated by the name, the spot where a ridge ends. A bifurcation is a spot where a ridge splits into two ridges. Spot is that fingerprint ridge that is significantly shorter than other ridge. This detail is stored into the database and used for verification and validation of a user while he/she tries to access the account.

When the user gives its fingerprint as input its minutiae features are extracted and mapped to the database to find whether the person has right to accesses the particular account or not. If the match is found the can easily withdraw/deposit cash.

4. CONCLUSION

This paper concludes that the conventional ATM system needs to be replaced with Biometric systems where the transaction process becomes easier, reliable, secure, and eliminating the need for carrying any kind of swipe cards. The fingerprint is one of many forms of biometrics used to identify individuals and verify their identity. It is based on the characteristics of the user's fingerprint, like stability, reliability, etc. Fingerprint and face-print allow the recognition of a registered person through quantifiable physiological characteristics that verify the identity of an individual. This system would be able to provide a user-friendly inexpensive experience unleashing the security aspects of the proposed biometric ATM systems.

REFERENCES

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

2) Yi Sun, Yuheng Chen, Xiaogang Wang, and 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) David Menotti, Giovani Chiachia, Allan Pinto, William Robson Schwartz, Helio Pedrini, Alexandre Xavier and Anderson Rocha, "Deep Representations for Iris, Face, and Fingerprint Spoofing Detection", IEEE, January 27th, 2015.

6) Florian Schroff, Dmitry Kalenichenko, James Philbin: Submitted on 12 Mar 2015 (v1), last revised 17 Jun 2015 (this version, v3).Also published, in Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition 2015

7) International Conference ICT For Smart Society(ICISS) 2014

8) Chung-Hua Chu, Yu-Kai Feng: Published Year 01 March 2018 Study of eye blinking to improve face recognition for screen unlock on mobile devices DO - 10.5370/JEET.2018.13.2.953.

9) El-Bakry H.M. (2005) Human Face Detection Using New High-Speed Modular Neural Networks. In: Duch W., Kacprzyk J., Oja E., Zadrożny S. (eds) Artificial Neural Networks: Biological Inspirations – ICANN 2005. ICANN 2005. Lecture Notes in Computer Science, vol 3696. Springer, Berlin, Heidelberg.

10) Cole S.A. History of Fingerprint Pattern Recognition. In: Ratha N., Bolle R. (eds) Automatic Fingerprint Recognition Systems. Springer, New York, NY, 2004.

11) Bhavesh Pandya, Georgina Cosma, Ali A. Alani, Aboozar Taherkhani, Vinayak Bharadi, T.M McGinnity, "Fingerprint classification using a deep convolutional neural network", Information Management (ICIM) 2018 4th International Conference on, pp. 86-91, 2017.

12) 9th International Congress on Image and Signal Processing, Biomedical Engineering and Informatics (CISP-BMEI) 2016.

13) Bhavesh Pandya, Georgina Cosma, Ali A. Alani, Aboozar Taherkhani, Vinayak Bharadi, T.M McGinnity, "Fingerprint classification using a deep convolutional neural network", Information Management (ICIM) 2018 4th International Conference on, pp. 86-91, 2016.

14) XVIII Brazilian Symposium on Computer Graphics and Image Processing (SIBGRAPI'05) 2005.

15) www.Meddataquest.com

16) Wikipedia