International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

Secure Online Payment with Facial Recognition using CNN

Ritika Patil[1], Shubhada Patil[2], Shruti Sagar[3], Shruti Sancheti [4], Prof. Sheetal More[5]

[1,2,3,4]Student, Dept. of Computer Engineering, Sinhgad College of Engineering, Maharahtra, India
[5]Professor, Dept. of Computer Engineering, Sinhgad College of Engineering, Maharahtra, India

---

Abstract - *The recent advancements in technology have led to a surge in online transactions via online shopping, internet banking, payment gateways, etc. Security is one of the major issues during these transactions. Due to such issues people are hesitant to use online transactions, so we propose our system which secures online transactions using two-step verification. The first step is OTP verification followed by facial recognition. The system uses an online interface in order to interact with a user. The interface is used to get card details from the particular user. After the OTP verification, the user will be authenticated using facial recognition. The system uses a CNN in order to verify the user by comparing the real time captured image of the user against the images associated with the users account.*

***Key Words*: CNN, online payment, security, image verification, face recognition, credit card**

1. INTRODUCTION

Today's advanced technology allows hackers to get personal details of users and so some people are reluctant to use online transactions. This makes security a key factor during online payments. We propose a system to enhance the security of online transactions by providing a two-step verification process-OTP verification followed by Facial Recognition.

The system will focus on reducing attacks, which makes the transactions vulnerable, like lost or stolen cards, account takeover, counterfeit cards, fraudulent application, multiple imprint, and collusive merchants. In account takeover, a card holder unknowingly gives personal details to a fraudster and the fraudster then issues a new card using these details. In counterfeit, a card is cloned and used by a fraudster. In multiple imprints, as single transactions is recorded multiple times. In collusive merchants, employees work with the fraudsters. The system succeeds in reducing all these frauds by capturing and verifying a real time image of the card holders.

Authentication with the help of biometrics is gaining popularity due to its uniqueness for every person. The different biometric technologies are fingerprint, hand geometry, iris, face and palm. We are using face recognition is the most popular due to its usability, collectability and acceptability [8]. There are many techniques used for facial recognition like SVM [2], PCA [2], LDA [3], and CNN. The system uses CNN for facial recognition because it has shown better results [1] for face recognition. The system has a web user interface. It is compatible with all operating systems and all types of browsers. The user must have a camera connected to the machine in order to capture a real time image. It also requires that the user have a good internet connection to access the UI.

2. RELATED WORK

2.1 Techniques for securing online transactions

The current methods of securing online transactions include account associated password, CVV and OTP. One Time Password (OTP) is a set of alphanumeric characters which is sent to the account holders registered phone number through SMS or e-mails. The person who does not have access to these will not be able to follow through with the online transaction. Although it seems like OTP is secure and safe, it is not robust to attacks like impersonation, phishing, and malware based replay attacks.

2.2 Techniques for biometrics

Biometrics technology is used for authentication of an authorized user. The different biometric techniques include voice, face [9], palm and fingerprint. Voice recognition measures a users voice patterns, speaking style and pitch. Fingerprint identification uses patterns of the rides and valleys present in fingerprints scanned beforehand. Palm identification uses palm prints and other physical traits for unique identification of user's palm. Face recognition captures and stores the facial features of an individual and stores them for identification process.

2.3 Techniques for face recognition

The different techniques used for face recognition include PCA [2], LDA [3], SVM [2] and CNN. Principle component analysis (PCA) is used to reduce the dimensionality of data to reduce the number of parameters in images, which are high dimensional correlated data. It is based on Eigen values and Eigen vectors. Linear Discriminant Analysis (LDA) is based on linear projection of image space to lower dimension space by maximizing between-class scatter and minimizing the within-class scatter [3]. Support Vector Machine (SVM) is used for binary classification. An SVM based classifier is used in face recognition to predict the similarity and dissimilarity between two images [2]. Convolutional Neural Networks is a

deep neural network architecture which is used to extract features from images. CNNs can be used as classifiers or simply feature extraction. CNNs have show better accuracy with facial recognition as compared to the other techniques.

3. LITERATURE SURVEY

3.1 FaceNet (2015 IEEE): A Unified Embedding for Face Recognition and Clustering

In this paper is presented a system, called FaceNet [1]. FaceNet learns how to directly map face images to a compact Euclidean space. The distances between the generated vectors give the similarity between the faces. The created space can be used for different tasks such as face recognition, verification and clustering using standard techniques with FaceNet embeddings as feature vectors. We extend this concept to apply it to secure online transactions.

3.2 When Face Recognition Meets with Deep Learning (2015 IEEE)

The paper [4] aims to provide a common ground to all students and researchers alike by conducting an evaluation of easily reproducible face recognition systems based on CNNs. It uses public database LFW (Labelled Faces in the Wild) to train CNNs instead of a personal database. It proposes three CNN architectures which are the first reported architectures trained using LFW data. We use the LFW dataset to train our network as well as a personal database to test it.

3.3 Building Recognition System Based on Deep Learning (2016 IEEE)

Deep learning architectures use a multiple convolution layers and activation functions which are cascaded. The most important aspect is the setup-the number of layers and the number of neurons in each layer, the selection of activation functions and optimization algorithm. It [5] uses GPU implementation of CNN. The CNN is trained in a supervised way in order to achieve very good results. We extend this system in order to use it for the secure online transactions.

3.4 An Efficient Scheme for Face Detection (2015 IEEE)

This work [6] is based on skin colour, contour drawing and feature extraction to provide an efficient and simple way to detect human faces in images. The features under consideration are mouth, eyes, and nose. The results are with good accuracy, great speed and simple computations.

3.5 Gender and Age Classification of Human Faces (2017 IEEE)

This paper [10] introduces an approach to classify gender and age from images of human faces which is an essential part of our method for autonomous detection of anomalous human behaviour. This paper is a continuous study from previous research on heterogeneous data in which images as supporting evidence is used. A method for image classification based on a pre-trained deep model for feature extraction and representation followed by a Support Vector Machine classifier is presented. We use CNN in place of SVM.

3.6 Credit Card Transaction Using Face Recognition Authentication (2015 ICIIBMS)

This paper [8] is based on a credit card transaction system which integrates face recognition and face detection technology using Haar Cascade and GLCM algorithms. The training data set includes the extracted features from the images and is stored in administrator database, which is then used for the authentication. We use CNN instead to increase efficiency and reduce complexity of system.

4. SYSTEM ARCHITECTURE

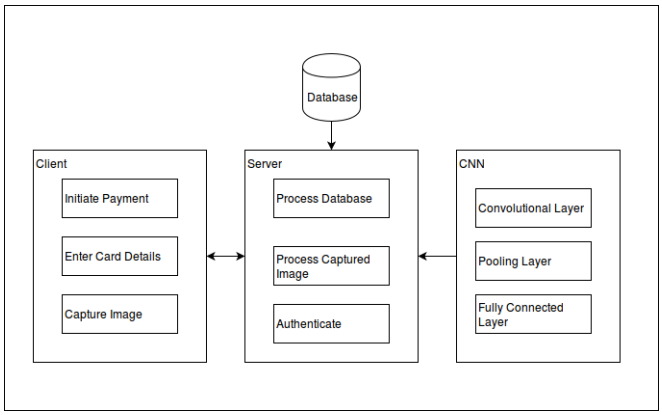

Fig -1: System Architecture

The system has the following components-Database, Client, Server and CNN. The database is divided into training and testing dataset. The training dataset, LFW, is used to train the CNN component while the testing dataset, a dataset of personal faces, is used to test its accuracy. The Server includes the modules used to interact with the database. They are also used to process the images received from the CNN. The Client side has the initiate payment, get card details and capture image modules. The capture image module is used to capture the image of the user and send it to the server side. The CNN consists of the convoluted layer which is used to extract the features of the user, the pooling layer which is used to reduce image size and the fully connected layer to give the probability of the user being the actual user. The system works as follows. A user initiates

payment by entering the card details in the displayed web page. The details are sent to server side and are authenticated. The user is then redirected to OTP web page. After entering a valid OTP, the user is redirected to the capture image web page where a real time image of user is captured and sent to server side. The image is processed via the CNN and authenticates the user against the image of the user stored in database at the server side.

4. METHODOLOGY

Convolutional Neural Network is being used for facial recognition and authentication of the user. A CNN is a deep learning algorithm and is found to be efficient in analysing images because CNNs use relatively little pre-processing compared to other image classification algorithms [4]. A CNN consists of an input and an output layer and hidden layers. A deep CNN architecture has a series of hidden layers one after the other where the output of one hidden layer is sent as input to the next hidden layer. The different layers present in the hidden layers are convolutional layer, pooling layer and normalization layers, and activation functions.

The system uses the inception v3 model [7] for CNN architecture. The inception model includes multiple inception blocks, each of which consist of a combination of Convolutional layers, pooling layers and activations which are concatenated together.

A Siamese network is used in our system. The Siamese network uses two CNNs, with the same weights and bias. One CNN gets its input image from the database and the other CNNs input is the real time captured image of the user. The model uses the triplet loss function to find the difference between the outputs of both the CNNs. This difference is used for training the complete model using back propagation.

A CNN takes an input image at its input layer. It extracts various features of the input and sends it to the following layer, which is usually a convolutional layer.

The Convolutional Layer performs most of the computations in the CNN architecture. Each convolutional layer takes an input image. The image has several parameters like size of image, number and size of the filter being used. The filter is used to extract the useful features from the input images. It is usually an odd square matrix which traverses along the height and width of the input image. The output of one convolutional layer acts as input to the following layer.

The Pooling Layer is used to reduce the number of parameters of the input image to make computations more efficient. There are several activations that can be used in the Pooling Layer. The system uses max pool function to reduce the parameters and the output generated is sent as input to the next layer.

The Output Layer is a fully connected layer where every neuron of previous layer is connected to every neuron of current layer. The fully connected layer first uses the flatten function to flatten the input image. This is then sent as input to an activation function such as sigmoid function to predict the output class of the image. The system uses CNN to encode the images and then find the difference between the flattened encoded images to see if they are match. The encoded images match if the difference is less than a learned threshold.

Back propagation is used in order to train the CNN and reduce the errors present in the network. The system uses the triplet loss function to adjust the weights and bias in each layer.

5. RESULTS

The training of the CNN on our personal dataset of faces resulted in an accuracy of 80-85%. The system is able to correctly identify the users, on which the network has been trained, and authenticate them in the real time application.

6. CONCLUSION

The system enhances the security of online transactions by successfully recognizing and authenticating authorized users. The system can be used as a payment gateway for any application which requires online payments. These include ecommerce websites, internet and mobile banking. The system can be accessed on any operating system using any web browser. For future work, iris identification can be added to the system for further enhancing the security of the transactions.

ACKNOWLEDGEMENT

We would like to thank our guide, Prof. S.V. More, for her constant support and guidance. We would also like to express our deep gratitude to the principal, Dr. S.D. Lokhande, for his continuous efforts in creating a competitive environment in our college. We would like to convey our heartfelt thanks to our H.O.D., Prof. Wankhade, for giving us the opportunity to embark upon this topic. We also wish to thank all the staff members of the Department of Computer Engineering for helping us directly or indirectly in completing the work successfully.

REFERENCES

[1] Florian Schroff, Dmitry Kalenichenko,and James Philbin, “FaceNet: A Unified Embedding for Face Recognition and Clustering”, IEEE, 2015.

[2] Muzammil Abdulrahman, Alaa Eleyan, “Facial expression recognition using Support Vector Machines”,

23nd Signal Processing and Communications Applications Conference (SIU), IEEE, 2015.

[3] Yuan Wei, "Face Recognition Method Based on Improved LDA", 9th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC), IEEE, vol. 2, pp. 456 - 459, 2017.

[4] Guosheng Hu, Yongxin Yang, Dong Yi,et. al.,When Face Recognition Meets with Deep Learning: an Evaluation of Convolutional Neural Networks for Face Recognition, IEEE International Conference on Computer Vision Workshop, 2015.

[5] Pavol Bezak, "Building Recognition System Based on Deep Learning", IEEE, vol. 6, no. 1, pp. 212-217, 2016.

[6] Mohamed Heshmat, Moheb Girgis,et al, "An Efficient Scheme for Face Detection Based on Contours and Feature Skin Recognition", IEEE, 2015.

[7] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S., et. al., "Going deeper with convolutions", CoRR, abs/1409.4842, 2014.

[8] Gittipat Jetsiktat, Sasipa Panthuwadeethorn, Suphakant Phimoltares, "Enhancing User Authentication of Online Credit Card Payment using Face Image Comparison with MPEG7-Edge Histogram Descriptor",International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS), IEEE, 2015.

[9] Adrian Rhesa Septian Siswanto, Anto Satriyo Nugroho, Maulahikmah Galinium, "Implementation of Face Recognition Algorithm for Biometrics Based Time Attendance System", International Conference on ICT for Smart Society (ICISS), IEEE, 2014.

[10] Xiaofeng Wang, Azliza Mohd Ali, Plamen Angelov, "Gender and Age Classification of Human Faces for Automatic Detection of Anomalous Human Behaviour",IEEE, 2017.

[11] W. Mohamed and M. Heshmat, M. Girgis, S. Elaw, A new method for face recognition using variance estimation and feature extraction, International Journal of Emerging Trends and Technology in Computer Science (IJETTCS), vol. 2, no. 2, pp. 134-141, 2013.

[12] R.S. Choras, "Facial feature detection for face authentication", in the Proceeding of IEEE Conference on Cybernetics and Intelligent Systems., 2013, pp.112-116, 2015.

[13] I. Aldasouqi and M. Hassan, Smart human face detection system, International Journal of Computers, vol. 5, no. 2, pp. 210-216, 2015.

[14] A K. Jain, P. Flynn, A. A. Ross, Handbook of Biometrics, New York: Springer, 2010.