*FACE RECOGNITION SYSTEM FOR NET BANKING*

1st Anvesh Duddu Dept. Of Computer Science and Engineering Hindustan Institute of Technology and Science Chennai, India [anvesh81255@gmail.com](mailto:anvesh81255@gmail.com)

2nd Sairam Eruvuri Dept. Of Computer Science and Engineering Hindustan Institute of Technology and Science Chennai, India [sairameruvuri@gmail.com](mailto:sairameruvuri@gmail.com)

3rd Ranjana P Dept. Of Computer Science and Engineering Hindustan Institute of Technology and Science Chennai, India [pranjana@hindustanuniv.ac.in](mailto:pranjana@hindustanuniv.ac.in)

**Abstract**: The recent advancements in technology have led to a surge in online transactions via online shopping, internet banking, payment gateways, etc. Security is the most prevailing issue during these transactions. Due to such issues people are not interested to use online transactions, so we propose our system which secures online transactions using two-step verification. The first step in this process is OTP verification followed by facial recognition to complete online transaction. The system uses a web interface to interact with a user. The interface is used to get payment details from the user. After the OTP verification, the user is authenticated using facial recognition using system webcam. The system uses webcam in order to verify the user by comparing the real time captured image of the user against the images associated with the users’ account.

**I. INTRODUCTION**

Online payments are being widely used worldwide. People are switching over to online transaction like online shopping, online bill payment, etc as it reduces the problem of carrying cash. Online payments can be used anywhere and big transactions can be easily done using user account. Banking companies make sure that funds moves to the merchant's account accurately and on time. It makes sure that customers don’t need to

make any efforts and can go cashless. But the fundamental problem faced during online transactions is lack of security. Online

payments scam is a wide-ranging term for theft and scam committed using or involving a card details, such as a credit card or debit card, as a fraudulent source of funds in a online transaction.

With increased online transactions, the risk of frauds has been increased. Card details and their pins can be stolen, OTP can be stolen. It becomes quite easy to make fraudulent transactions in such situations. The motivation behind this project is the massive increase in frauds. The victims of Online payments scam suffers too much and if the fraud is done due to customer’s mistake then bank never takes up the responsibility of their loss. Today's fraud detection systems are designed to prevent these losses. The proposed system with facial recognition can help to secure the overall online banking system. Among all the biometric techniques, face recognition is one of the most challenging as well as the reliable one, being more user-friendly and due to ease of use, it is more in use nowadays.

Face authentication is the way of authenticating based on the physiological or chemical traits of a person. These traits will be unique for each individual. As they can never be stolen or replicated, they prevent dictionary attacks (It is a way of trying hundreds and sometimes even millions of combinations as in a dictionary so as to find the correct one), phishing attacks (fraudulent acts that try to acquire our personal information by gaining faith in us) etc. While making online payments transaction from one user account to another user, the online banking is always concerned about the hackers and fraudulent persons.

**II. RELATED WORK**

2.1 **Techniques for securing online transactions**

The existing methods of securing online transactions are account associated password, card verification value (CVV) and one-time password (OTP). OTP is a combination of alphabets and numbers which is sent to the account holders’ registered phone number via SMS or via e-mail. Any card holder who doesn’t have any of the 2 mentioned above will not be able to follow through with the online transaction. It is generally believed that OTP is secure and safe. However, it is not robust to attacks like impersonation, phishing, and malware-based replay attacks.

2.2 **Techniques for biometrics Biometric**

Technology is used for authentication of a card holder. The various biometric techniques are using voice, face, palm and fingerprints. voice recognition analyses countless patterns and elements, 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, and 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 in facial recognition include PCA [2], SVM [2], LDA [3]. Principle component analysis (PCA) is used to decrease the dimensionality of data to reduce the number of parameters in images, which are high dimensional correlated data.

**III. PROPOSED WORK**

As now-a-days world is moving toward the cashless payment modes with different security systems (pins, passwords, internet banking, etc.) as well as different platforms (Paytm, phonepe, gpay, etc.) it is difficult for people to remember lots of payment modes credentials (usernames, passwords, etc.). we propose idea with which we can make a payment system for the people where they can store all their credential once and make a payment to another person within seamless time. We have to deal a lot with our payment modes during the payment or pay out from waiting in long queues, waiting for the change money, which is quiet delay in the process. Our proposed work solves the problem of managing multiple payment modes by replacing all of them by one which makes the transaction process fast, secure and more convenient. It is a hassle-free payment system.

Our system which protects online transactions using two-step authentication. The first step is otp followed by facial recognition. As mentioned in the proposed system the user interface will be more customers friendly which will be developed by using the languages like HTML4, CSS, SCSS, PHP, and JavaScript. Every customer will be allotted with their own account login credentials with which the customer should login to his/her account.

**IV.SYSTEM ARCHITECTURE**

If the user is new to the application, one should register so that it helps the user to login easily. After login customer will choose the payee to whom he wants to do the transaction. After entering the details of Payee, customer goes for facial recognition, if the facial recognition is successful then he needed to get verified through otp verification. If facial reorganization or otp verification is failed then he will be redirected to transaction page.

**Face Detection**

First stage was creating a face detection system using Haarcascade classifier. Although, These are trained Haar-cascades, OpenCV has a robust set of Haar-cascades that was used for the project. Using face-cascades alone caused random objects to be identified and eye cascades were incorporated to obtain stable face detection. Face and eye classifier objects are created using classifier class in OpenCV through the cv2.CascadeClassifier() and loading predict identity

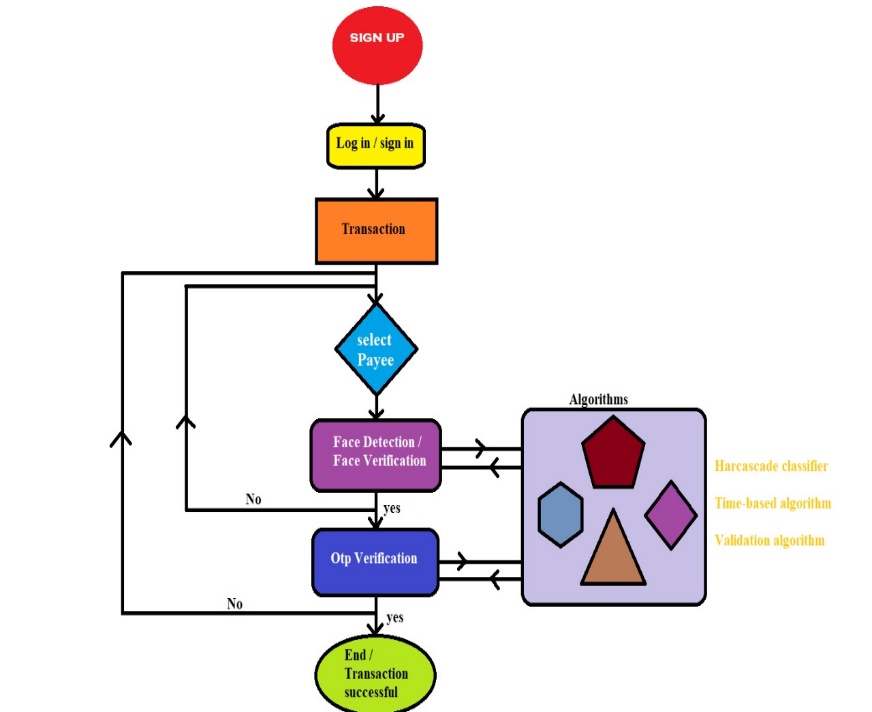


Figure (Architecture of proposed system face recognition for net banking)

**Face Recognition Process**

The algorithm works in real time through a webcam and recognize person in real time if they blinked. In layman’s terms, the program work as following steps:

1.Detect faces in each frame generated by the webcam.

2.For each detected face, detect eyes.

3.For each detected eye, detect if eyes are open or closed.

4.If at some point it was detected that the eyes were open then closed then open, we conclude the person has blinked and the program recognize user.

**Training the classifiers**

OpenCV enables the creation of python scripts to store features extracted from datasets using the Face Recognizer class. The stored images are converted to grayscale and saved with IDs in two lists with same indexes.

**Known face dataset encoding**

In my case, the algorithm is able to recognize maximum user. I selected around 10 pictures of each. algorithm process and encode our database of known faces. Now that we know the encodings for each person we want to recognize, we can try to identify and recognize faces through a webcam

**Face liveness detection**

To detect an open-closed-open eye pattern at some point. I trained a Convolutional Neural Network to classify whether an eye is closed or open. The chosen model is the LeNet-5 which has been trained on the closed eyes in the wild (CEW) dataset. It is composed of around 8000 eye images in 20\*20 scale size.

Each time we detect an eye, we predict its status using our model, and we keep track of the eyes status for each person. Therefore, it becomes really easy to detect an eye blinking, which tries to find a closed-open-closed pattern in the eyes status history.

We have reached 94% of accuracy

**Face recognition of living people**

We almost have all the elements to set up our “real”-face recognition algorithm. We just need a way to detect faces and eyes in real-time. we used OpenCV already-trained Haar-cascade classifier to perform these tasks.

The code used for detecting and recognizing real faces. It takes in arguments:

* model: our open/closed eyes classifier
* video\_capture: a stream video
* face\_detector: a Haar-cascade face classifier. We used haarcascade\_frontalface\_alt.xml
* open\_eyes\_detector: a Haar-cascade open eye classifier. We used haarcascade\_eye\_tree\_eyeglasses.xml
* left\_eye\_detector: a Haar-cascade left eye classifier. We used haarcascade\_lefteye\_2splits.xml which can detect open or closed eyes.
* right\_eye\_detector: a Haar-cascade right eye classifier. we used haarcascade\_righteye\_2splits.xml which can detect open or closed eyes.
* data: a dictionary of known encodings and known names
* eyes\_detected: a dictionary containing for each name the eyes status history.

We grab a frame from the webcam stream and we resize it to speed up computations. we detect faces from the frame, then we encode them into a 128-d vector. we compare this vector with the known face encodings and we determine the person’s name by counting the number of matches. The one with the biggest number of matches is selected. we try to detect eyes into face boxes. First, we try to detect open eyes with the open\_eye\_detector. If the detector succeeds, then ‘1’ is added to the eye status history meaning the eyes are open since the open\_eye\_detector cannot detect closed eyes. Otherwise, if the first classifier has failed, (maybe because eyes are closed or simply because it did not recognize eyes) then the left\_eye and right\_eye detectors are used. The face is separated into left and right side for the respective detectors to be classified.The eye part ​is extracted​ and the trained model predicts whether the eyes are closed. If one closed eye ​is detected, then both eyes ​are predicted to be closed and a ‘0’ is added to the eyes status history. Otherwise it’s concluded that the eyes are open. Finally the isBlinking() function is used to detect eye blinking and if the person has blinked ​the face is recognized and complete the transaction

**V. CONCLUSION**

Our proposed project- Face Recognition for net banking will help in reducing the online banking frauds that may occur during an transaction process. It will provide a two-step verification i.e. OTP verification and face authentication of the user for securing the online payment. Because of this any registered user can easily trust on it and confidently make payments over the Internet in seamless time. Although this system will provide more security and will help in reducing the online banking scams but still it

needs a lot of improvement as the frauds will use clone or similar faces. Also, the rate of comparison of the real time recognition image with the image stored in database should be fast enough so that the user does not have to wait for a long period of time while doing transaction. Having dealt with all the issues this system will provide a better security and seamless transaction. This will definitely improve scope of online transaction

**VI. REFERENCES**

[1] Prof. Pavan Sharma1, Priyanshu2, Vikas Tiwari3 “ A Mobile Payment System Based on Face Recognition”, Apr 2019

[2]. Asma haikh1, Aditi Mhadgut2, Apurva Prasad3, Bagyashree Shinde4, Rohan Pandita5” CREDIT CARD AUTHENTICATION WITH FACE RECOGNITION USING WEBCAM”, DECEMBER 2018

[3] Tison Varghese, Vidya Nambiar, Pushkar Dandekar and Gayatri Hegde” Authentication of Credit Card Using Facial Recognition”, April 2018

[4] Wakil Ghori “Security Issues on Online Transaction of Digital Banking”, February 2017

[5] Ms.Amani Gorre1 ,Mr. Dinesh Bejjanki2 , Ms.Lavanya Dimki3 ,Ms.Kavya Kasthuri4 “Analysis of Face Recognition Security Features and Customer Friendly Interface in Internet Banking System” , 2019