ISSN No. 0976-5697

Volume 11, Special Issue I, May 2020

International Journal of Advanced Research in Computer Science

CONFERENCE PAPER

Available Online at www.ijarcs.info

SECURED ONLINE CREDIT CARD TRANSACTION USING FACIAL RECOGNITION AS AN AUTHENTICATION PROCESS

Devraj Yadav P
School of Computing and Information Technology REVA University, Bangalore, India
devrajyadavdeva9666@gmail.co

Sheelavathy K V ,Assistant Professor School of Computing and Information Technology REVA University, Bangalore,
sheelakv@reva.edu.in

Chermanna MT
School of Computing and Information Technology REVA University, Bangalore, India
ronithchermanna@gmail.com

Boya Harinath
School of Computing and Information Technology
REVA University, Bangalore, India
boyaharinath1608@gmail.com

Deepak J
School of Computing and Information Technology
REVA University, Bangalore, India
bhuriyuj@gmail.com

Abstract—Face Recognition is a biometric technology that is best and comes to mind during identifying and verifying a identity of a person. Subsisting authentication phases of Online transaction is not as secure, since it can be accessed by a third party if he is adequate, which is same with biometric dactyl gram scanners. Thus genuine time face recognition is something which cannot be hacked without the notice of the accommodation provider. Integrating face recognition as an authentication process makes online transaction more secure. Since there are sundry online payment mode today authentic time face recognition will be a better reliable mode of authentication. We have made utilization of python and library open-cv which has three face recognition algorithms, faces of customers are trained into the machine and stored into the database and accessed when needed. Out of the three algorithms fisher face and Eigen face have less precision and withal depends on background effulgence. Thus LBPH (local binary pattern histogram) is utilized as it gives a higher precision and works on dim light as well. After validating and verifying rest of the customer information authentication is done where the images captured is compared with database and verified for the right utilizer and thus authentication is done. Thus this project aims on implementing the above conception for the betterment in the on demand system.

Keywords—Computer Vision (CV), Local Binary Pattern Histogram (LBPH), Hans Peter Luhn Credit Card algorithm.

I. INTRODUCTION

The Online transaction implifies, any electronic payment system that sanctions customers of a financial institution to conduct financial transactions through the financial institution's internet-enabled website or app.

Though online banking is slow in progress as not sizably voluminous no of people incline to utilize it. Online banking is the future, thus making it more secure would be the aim as the day passes. Authentication is a paramount issue in system control in computer predicated communication.

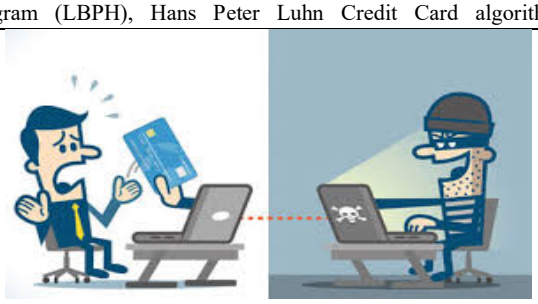


Fig. 1. Fraud by a capable hacker with traditional authentication

Subsisting authentication process does not ensure the identity of the precise utilizer. One efficient way of surmounted this quandary is to verify on biometric substructure.

Since dactylogram scanners though gives good precision cannot be trusted sometimes and retina scanners are not cost efficient, genuine time face apperception becomes an efficient way for the authentication.

Face Apperception can be defined as such, this technology is an application of image processing which is utilized for recognise and probing a face where now we will be implementing for verification. Face apperception is a non-invasive identification system and more expeditious than other systems since multiple faces can be analysed concurrently.

We will be making utilization of python coding laungage along with the python library open computer vision which contains sundry algorithms in hand out of which three of them are face apperception algorithms.

Despite three algorithms two of which are fisher face and eigen face one of the best but depends mainly on light intricacy never gave the precision we needed, thus we stuck on to LBPH (local binary pattern histogram). This gives better precision along with working on dim light.

The number of identity fraud cases incremented 16 percent between 2015 and 2016, according to Javelin Strategy & Research. Fraud Mazuma doubled up to 1.7billion doubling till 2019.Thus a safer more reliable authentication is needed.

II. STEP'S TO BE FOLLOWED

1. Firstly during the account engenderment process in the financial institution the customer's face data is trained into the system.
2. In the API when user needs to make a transaction firstly they enter the unique user credentials that are assigned to them.
3. After the verification of the credentials the card details are entered.
4. To verify the card Luhn algorithm is implemented.
5.The next phase is to verify the user based on face recognition after which the transaction process is done

III. PROPOSED METHODOLOGY

Fig. 2. Data Gathering and Train the Recognizer

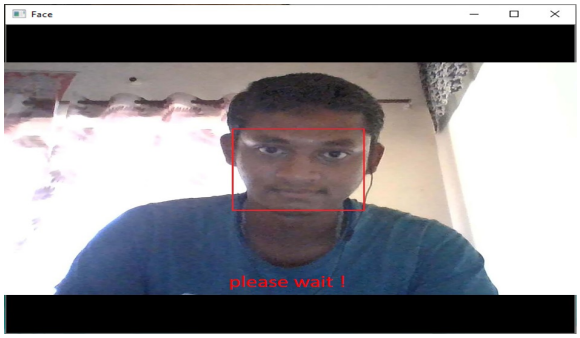


Fig. 3. Recognition

IV. MODULES IDENTIFIED

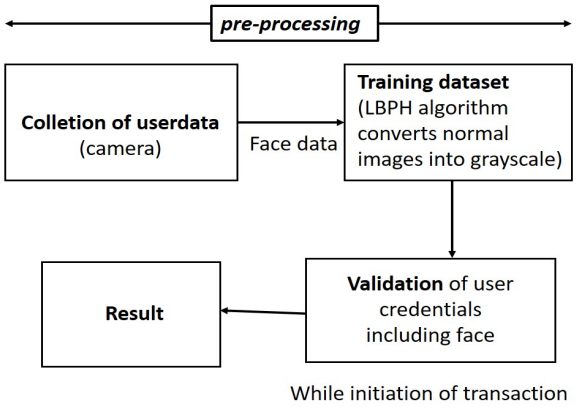


Fig. 4. Modules

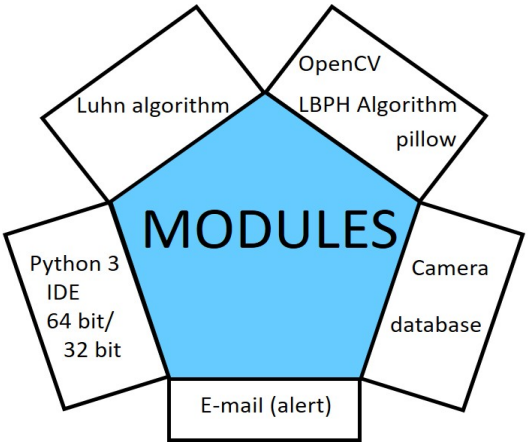


Fig. 5. Tools and Packages

A. IDLE (3.6.7python shell): An integrated development environment for Python IDLE of version 3.6.7 has been bundled with the default implementation of the language since 1.5.2b1. Which we have made use for our code.

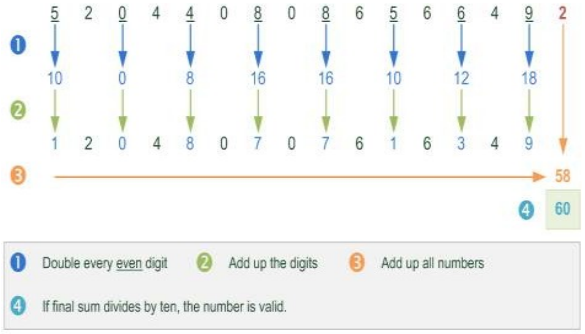
B. Open-CV(LBPHalgorithm): Open computer vision is a library of programming functions. Here python is made utilization of to access this library. For which we utilize the training function as well and LBPH is one of the face apperception algorithm in this librarry.

C. Luhn algorithm: An algorithm to check the validity of the users credit card.

D. Camera,Database: Not just to train additionally to authenticate validity camera or webcam can be utilized. A database of required recollection to store the trained data.

V. METHODOLOGY

At the commencement when the customer has opened his account his face is trained into the system using Python and that data is store in the system. Adscititiously a unique id and a pin password is supplementally given to each customer, by entering which along with facial authentication transaction proceeds, else an electronic mail is sent to customer if any authentication failure occurs to attest if it is the utilizer himself or not. If not then the accommodation provider is notified and required measures are taken.



After the authentication of the utilizer the Credit card is then validated utilizing Luhn's algorithm withal kenned as the modulus 10, designated after the engenderer himself Hans Peter Luhn. This public domain algorithm is widely in utilization today. It is designated in ISO/IEC 7812-1. It is not intended to be a cryptographically secure hash function; it was designed to bulwark against contingent errors, not malignant attacks. Whenever there is mistyped or otherwise erroneous numbers most of the institutions make utilization of this algorithm due to its simple methodology.

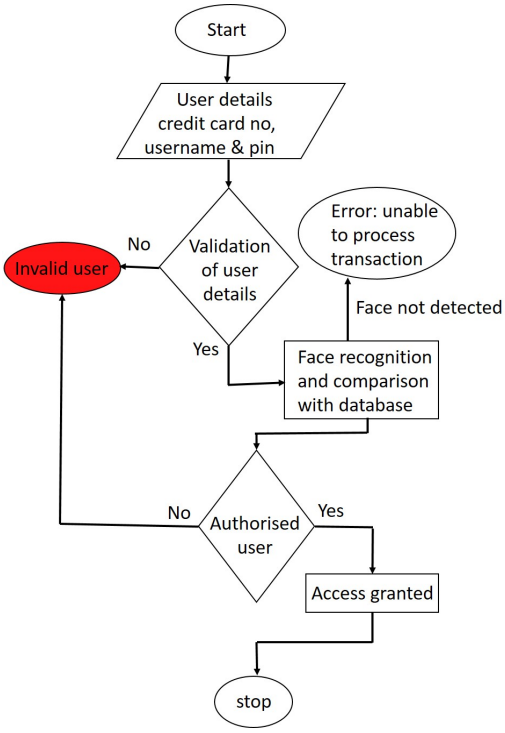


Fig. 6. Methodology Flow Chart

Fig. 7. Pictorial Hans Peter Luhn algorithm

As in the above figure From the rightmost digit, which is the check digit, and moving left, double the value of every second digit. The odd placed digit is not doubled, the first digit doubled is immediately to the left of the check odd placed digit. If the result of this doubling operation is more preponderant than 9 (e.g., 8 × 2 = 16), then integrate the digits of the result (e.g., 17: 1 + 7= 8, 18: 1 + 8 = 9) or, alternatively, the same final result can be found by subtracting 9 from that result (e.g., 16: 16 − 9 = 7, 18: 18 − 9 = 9).Taking the sum of all the digits.,If the total modulo 10 is equipollent to 0 (if the total ends in zero) then the entered card number is right according to Lunh's algorithm.

Thus later after validating card utilizer face authentication is done for which the Open Source Computer Vision library containing LBPH(Local Binary Pattern Histogram) a face apperception algorithm is utilized for authentication.

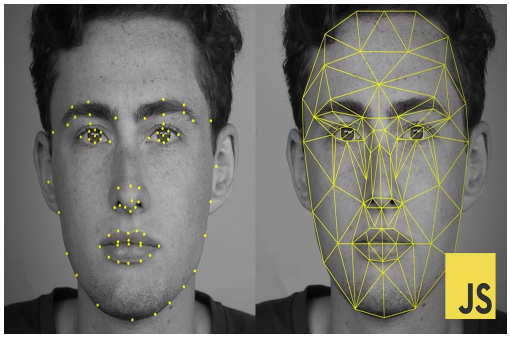


Fig. 8. LBPH recognition

Fig. 9. LBPH binary pattern matrix form

The LBPH Face Recognizer Process As in Fig:8 Takes a 3×3 window and move it across one image. At each move (each local part of the picture), compare the pixel at the center, with its circumventing pixels. Denote the neighbors with intensity value less than or identically tantamount to the center pixel by 1 and the rest by 0. After you read these 0/1 values under the 3×3 window in a clockwise order, you will have a binary pattern like 11100011 that is local to a particular area of the picture. When you culminate doing this on the whole image, you will have a list of local binary patterns.

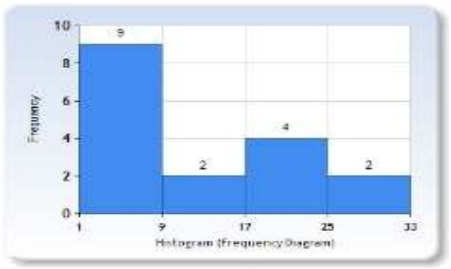


FIG. 10. HISTOGRAM SAMPLE.

Now, after you get a list of local binary patterns, you convert each one into a decimal number utilizing binary to decimal conversion (as shown in above image) and then you make a histogram of all of those decimal values. A sample histogram looks akin to this: In the cessation, you will have one histogram for each face in the training data set. That signifies that if there were 100 images in the training data set then LBPH will extract 100 histograms after training and store them for later apperception. Recollect, the algorithm additionally keeps track of which histogram belongs to which person.

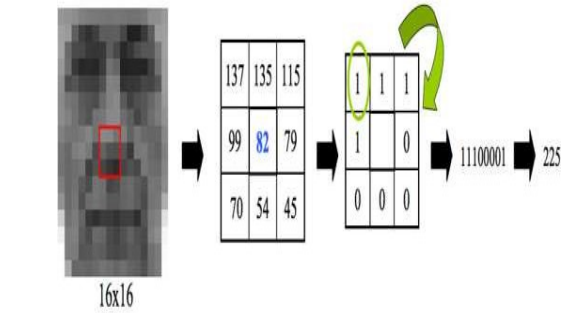
VI. OBJECTIVE

Driven by current developments in human-centered computing, an automatic system for facial apperception has emerging applications in secured access and mobile banking areas.

Moreover, mobile contrivances present a vital role in our lives as they are utilized widely in personal and professional atmospheres. This brings up the conception of facial apperception systems utilizing mobile contrivances which can be more reliable and can avail to build the trust with clients and online banking systems

VII. RESULTS AND DISCUSSION

1) First user credentials are created and data is trained into the system as in Fig.2



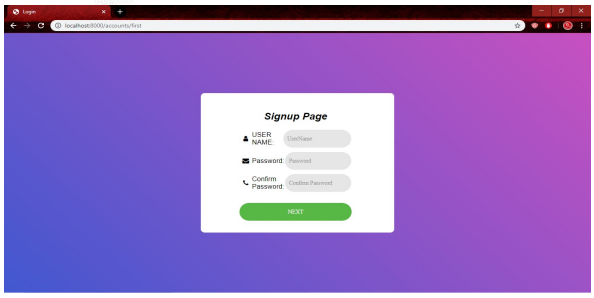


Fig. 11. Signup Page

2) On the user application login credentials will be taken to verify the user and then the card detail are entered as in below.

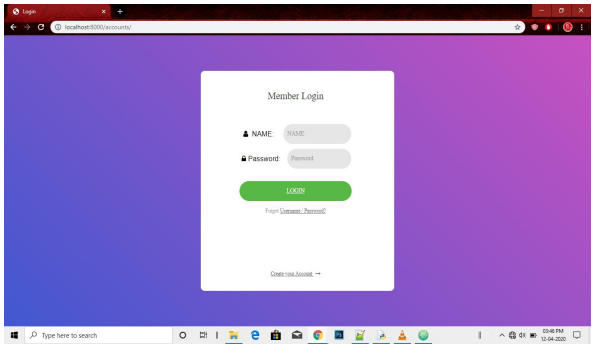


Fig. 12. Login page

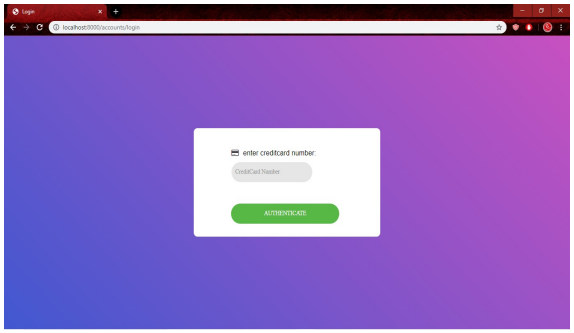


Fig. 13. Card details authentication page

3) After the validation of user details and card face authentication is done which on success continues user transaction. With reference to Fig:3

4) If not an email is sent to user about the failed attempt of transaction to verify it was him and not a third party.

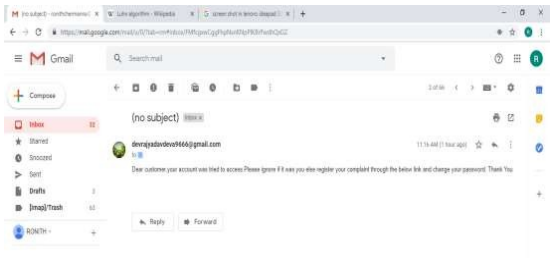


Fig. 14. Warning Mail

VIII. CONCLUSION & FUTURE SCOPE

Purpose of Our proposed project on credit card authentication utilizing face apperception is abbreviating credit card frauds that may occur during an online payment process. It will be flexible, reliable, precise so that people can facilely utilize it without any hesitation. The web cam plays a consequential role in the system which may be superseded by any other camera on application to scan . Utilizing this technique solves the subsisting issues by integrating face Apperception ,this system still lacks the faculty to identify people with homogeneous face.This quandary is overcome by utilizing OTP. The comparison of the authentic time image with the images stored in the database should be made reliable.This application should not be made time consuming for a utilizer.

In future the successful implementation will bring up better versions of face recognition software. Which intern may bring it up in other required fields further developing the field of image processing.

IX.ACKNOWLEDGEMENT

The prosperous implementation of this project required an abundance of guidance and assistance from many people directly or indirectly and we are prodigiously privileged to have get this along the completion of our project.

We respect and sincerely thank Assistant Professor Sheelavathy K V for her support and guidance which made us complete the project duty.

X. REFERENCES:

[1] Biometric Face Recognition Payment System ; Dr.C.S.Mala ,Surekha.R.Gondkar,Saurab. B; International Journal of Engineering Research & Technology (IJERT);Year: 2018 Volume: 6

[2] Survey on Online Transaction using Face Recognition; Prof. Shruti Sekra, Namita Jain, Vikrant Mukkawar, Mahesh Jadhav;International Journal of Advanced Research in Computer and Communication Engineering;year:2017

[3] A robust and secure authentication mechanism in online banking ;Hridya Venugopal , N Viswanath;2016 Online International Conference on Green Engineering and Technologies (IC-GET)

[4] Credit Card Transaction Using Face Recognition Authentication ; Akshay Prakash, G Mahesh, Maram Gowri, Muzameel Ahmed; International Journal of Innovative Research in Computer and Communication Engineering; Year: 2016

[5] Facial Verification Technology for Use In Atm Transactions; Aru, Okereke Eze, Ihekweaba Gozie; American Journal of Engineering Research (AJER*)*; Year: 2013

[6] A proposed technique of online face authentication to be used for the user identification ;
Dibyendu Ghoshal ; 2012 International Conference on Computer Communication and Informatics ; Year: 2012 ; Pages: 1 – 5

[7] Online biometric authentication using facial thermograms; MadasuHanmandl Shantaram Vasikarla;2012 IEEE Applied Imagery Pattern Recognition Workshop(AIPR)

[8] The application and of face recognition in authentication system for distance education Qianqian Zhao ; Mali Ye; 2010 International Conference on Networking and Digital Society;Year: 2010 Volume: 1

[9] Personal Based Authentication by Face Recognition; Yung-Wei Kao ; Hui- Zhen Gu ; shyan;MingYuan; 2008 Fourth International Conference on Networked Computing and Advanced Information Management;Year :2008 Volume: 2