Multifactor Authentication over Credit Card Fraud Detection and Prevention

Ashwini. M. Zinjurde, Vilas. B. Kamble

***Abstract**: Online banking becomes most used method for banking transaction now days. Now the trend is turning towards digitization and so is the population going towards the same thing. People often go to the credit/debit card, Net Banking, etc. online methods. Confidentiality may be hacked during online transactions. To reduced, fraud online activities so, as to secure the data by a two-step authentication method. The primary step of authentication is to verifying OTP. Once the OTP is verified, face recognition will be done. The data is analyzed and the results for both the valid and invalid transactions are sent to the Bank. A new card scanning system has important factor such as most safety, user-friendliness, etc. The application's importance is to mitigate credit card fraud through Face device awareness. The customers get both most usable and highly secure online banking application.*

***Keywords:** Credit Card, Fraud Detection, OTP, Online Banking System.*

I. INTRODUCTION

Due to rapid development in science and technology, upcoming innovations are being built-up with strong security. But on other side is also becoming reason to break this security structure. Though enhancement in automation has made a positive impact overall, but various financial institutions like banks and applications like ATM are still subjected to thefts and frauds. The existing ATM model uses a card and a PIN which gives rise to increase in vulnerability in the form of stolen cards, or due to randomly allotted PINs, duplicity of cards and various other threats. To overcome, hybrid model which is consists of conventional features along with additional features like face recognition and one-time password is used. Database holds information about a user's account details, images of his/her face and a mobile number which will improve security to a large extent. Primary thing by the user is to swipe the ATM card. A live image is captured automatically through a webcam installed on the ATM, which is compared with the images stored in the database. If it matches, an OTP will be sent to the corresponding registered mobile number. This randomly generated code has to be put by the customer in the text box. If the customers put valid OTP, the transaction can proceed. Therefore, the combination of face recognition algorithm and an OTP drastically reduces the chances of fraud plus frees a user from an extra burden of remembering complex passwords.

II. PROPOSED MODEL

The aim of the research is to develop a technique which uses face recognition to verify a valid user. Firstly, the user has to enter the credit card details and then the details will be verified with the bank database. After the verification process, OTP will be generated and sent to the user. Once the OTP is verified user will be requested for face authentication. Using webcam face image will be captured and in features form image will be sent for authentication to the bank database. At the database the image will be trained by our CNN and further, it will be use for the authentication purpose. Python language is used for programming and for processing the image Open-CV libraries are used that is integrated in Python. After that LBP algorithm is used for face feature extraction. If the face is matched with the images to read in the database then the user’s credit card limit will be checked and if it fulfills the requirement, the user is allowed for transaction or else the transaction will be aborted. The limitation to be resolved by this research is to showing a work with the below characteristics:1)To obtains input real time face image from open compute vision library of machine learning and image processing. A real time image is containing face features of human at current moment and output in the form of recognition.2)To execute in real-time application uses open-CV library functionality with CNN algorithmic solution.3)This allows customer to modify their face features like nose, mouth ,eyes etc and the customer can view controlled face image in anytime.4)For the execution time accuracy in the face recognition able regulations model creation process must be completely spontaneous. This feature is to invent the system absolute replacement to existing face evaluation methods.

III. LITERATURE SURVEY

Mohsin Karovaliya, et.al [1] The point of this paper is to make conventional ATM model increasingly protected. We additionally set forward another idea that will improve the general exchange understanding; unwavering quality and solace at the ATM. Highlights, for example, face acknowledgment and One-Time Password (OTP) are utilized for improving record security and client protection.

Revised Manuscript Received on July 30, 2020.
***** Correspondence Author

Ashwini. M. Zinjurde*, Department of CSE, PESCOE,Aurangabad,India. E-mail: ashwini.zinjurde1994@gmail.com

Dr. Vilas. B. Kamble, Department of CSE, PESCOE, Aurangabad, India. E-mail: vbkamble@yahoo.com

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

Face prevalence age permits the device to distinguish every single individual particularly consequently making face as a key. This totally takes out the probabilities of extortion in light of burglary and guile of the ATM cards.

Besides, the haphazardly produced OTP liberates the individual from recalling PINs as, it itself goes about as a PIN.

Rupinder Saini , et.al [2] This paper manages differentiate concerning assorted biometric frameworks actually by utilizing characterizing their points of interest and hindrances. A short creation is by and large offered with respect to regularly utilized biometrics, comprehensive of, Face, Iris, Fingerprint, Finger Vein, Lips, and Voice. The complexity guidelines posting added is controlled to precision, size of format, cost, wellbeing stage, and long time balance. Khyati Chaudhary, et.al [3] proposed In current situation while the timeframe misrepresentation comes into a conversation, charge card extortion snaps to mind up to this point. With the phenomenal development in MasterCard exchanges, charge card misrepresentation has expanding unnecessarily as of late. Misrepresentation identification comprises of following of the spending conduct of clients/customers in the event that you need to self-control, location, or evasion of unwanted direct. As financial assessment card will turn into the most winning method of charge for each online notwithstanding normal buy, extortion relate with it are additionally quickening. Extortion location is engaged with not, at this point least complex catching the fake occasions, yet also shooting of such exercises as fast as suitable. Anissa Lintang Ramadhani, et.al [4] has included Face is the most paramount a piece of the edge in genuine life that makes it a basic variable. on this examinations, we use face catch method that fused in Ry-UJI mechanical. The robot is determined to have the guide of a recognized voice order searching for somebody and when somebody's face has been resolved, face notoriety is whole. This content will apply the human face acknowledgment gadget the use of the Eigen-face approach. Eigen-face is one of the facial acknowledgment procedures based absolutely at the key issue assessment (PCA) set of rules. PCA included a scientific system to infer an immovable of highlights for face notoriety. Face acknowledgment level starts with face recognition strategy the use of course classifier technique, face pre-processes, gain and teach the face identified and in this way the face prevalence anani. S. R, et.al [5] states MasterCard bears unmistakable utilization of charge technique, so it's far went with in numerous situations. As we probably am aware, over the span of on line exchanges there are numerous odds to take the private data through the assailants or programmers. Along these lines, we support a fresh out of the box new technique to avoid false all through online exchanges and to comfortable the realities by methods for a stage confirmation system. The data is handled and the affirmation is dispatched to the bank for each the genuine and invalid exchanges. Another methodology of Visa filtering has useful properties in expressions of cost money related reserve funds and time execution. M. Eckhardt et.al [6] Marking recordings for influence substance, for example, outward appearance is dreary and tedious. Scientists regularly invest noteworthy measures of energy commenting on test information, or basically come up short on the time required to name their information. Hence we have created VidL, an open source video marking framework that can saddle the conveyed human intensity of the web. Markus Schedl et.al [7] The reason for this patterns and study article is twofold. We first distinguish and shed light on what we accept are the most squeezing difficulties MRS research is confronting, from both scholarly and industry viewpoints. We survey the best in class towards explaining these difficulties and examine its constraints. Second, we detail conceivable future headings and dreams we examine for the further advancement of the field. Oluwatobi Olabiyiet.al [8] The proposed framework joins camera-based information on the driving condition and the driver themselves, notwithstanding conventional vehicle elements. It at that point utilizes a profound bidirectional repetitive neural system (DBRNN) to become familiar with the connection between's tangible sources of info and looming driver conduct accomplishing precise and high skyline activity forecast. The proposed framework performs better than other existing frameworks on driver activity forecast assignments and can precisely foresee key driver activities including speeding up, slowing down, path change and turning at terms of 5sec before the activity is executed by the driver. Sheena C V et.al [9] States that Key-outline extraction from video information is a functioning examination issue in video object acknowledgment and data recovery. Key-outline alludes to the picture outline in the video grouping which is agent and ready to mirror the rundown of a video content. By utilizing the key-outline it can communicate the primary substance of video information unmistakably and lessen the measure of memory required for video information preparing and multifaceted nature significantly.

Alexandre Schaefer et.al [10] Suggested that utilizing enthusiastic film cuts is one of the most famous and powerful techniques for feeling elicitation. The fundamental objective of the current investigation was to create and test the adequacy of another and far reaching set of enthusiastic film portions. Fifty film specialists were approached to recollect explicit film scenes that evoked dread, outrage, bitterness, sicken, delight, delicacy, just as genuinely impartial scenes. For every feeling, the 10 most habitually referenced scenes were chosen and cut into film cuts.

Next, 364 members saw the film cuts in singular research center meetings and appraised each film on various measurements. Results indicated that the film cuts were compelling with respect to a few measures, for example, enthusiastic discreteness, excitement, positive and negative impacts.

IV. EXISTING SYSTEM APPROACH

Fraud is one of the significant good issues inside the financial assessment card industry. The essential points are, most importantly, to recognize the remarkable kinds of FICO assessment card misrepresentation, and, besides, to check elective methods which have been utilized in extortion location [4]. The sub-reason for existing is to give, assess and break down of late distributed discoveries in FICO rating card misrepresentation location.

This article characterizes normal terms in FICO assessment card misrepresentation and features key insights and figures around there. Depending at the kind of extortion looked by banks or Master Card gatherings; various measures might be followed and applied.

The recommendations made on this paper are potentially to have helpful qualities as far as value investment funds and time execution. The noteworthiness of the utilization of the procedures looked into directly here is inside the minimization of FICO rating card extortion. however there are as yet moral issues when appropriate financial assessment card clients are misclassified as deceitful. some time, there has been a solid enthusiasm inside the morals of banking notwithstanding the moral multifaceted nature of false direct. A basic dare to support organizations and money related foundations alongside banks are to find a way to forestall misrepresentation and to address it effectually and effectively.

a) Existing approaches to real time face recognition based on LBP classifier:

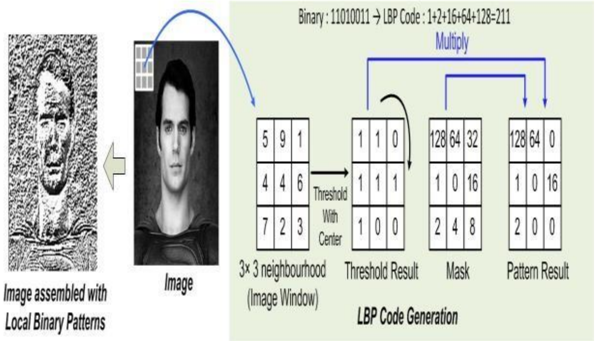


Fig.1 Block Diagram of Existing System

In existing ways to deal with continuous face acknowledgment dependent on LBP classifier. Such framework get perceived face pictures by acknowledgment framework is face discovery which checks whether human face is available in the caught picture or not. For this we use HAAR Cascade classifier which removes the highlights from the caught picture. For include extraction we apply diverse haar highlights like edge highlights, line highlights. On the off chance that face is identified, at that point and afterward just subsequent stage that is face acknowledgment begins in any case procedure will be ended.

The overall structure of existing system is illustrated in Figure 1. The system is comprised of LBP networks fails to achieve above 80 % accuracy while working with real time face images. So there is need of strong system which will work on real time face recognition with high accuracy.

V. METHODOLOGY USED

A. Image Processing:-

Every image is formation of RGB shades. Every captured picture has some noise, unwanted background. Therefore there is want of manner the ones captured image before assign to our recognition module. Pre-processing unit made is up of noise removal, grey image conversion, binary picture conversion of enter pix after that characteristic extraction carried out on those samples. In future extraction five steps implemented wherein finding the eccentricity. Next elongations of pix are evaluated via calculating pixel segmentation as well as rotation of enter photographs.

B. Tensor-flow: -

Machine getting to know is a complex area. The implementation in machine gaining knowledge of and introduction of models is a lot tough and difficult than it was, way to gadget mastering technology and frameworks. Inclusive of Google's Tensor drift that makes our challenge simple. it is procedure of obtaining records, training models, serving predictions, and refining destiny effects.

C. Convolutional Neural Networks:

In proposed work we are utilizing CNN which takes face pictures as info. In the wake of getting pictures from open-cv python it will prepared utilizing picture handling methods for highlight assessment. We separate various highlights from those pictures utilizing Har-course. By utilizing a progression of numerical capacities we will recognize the one of kind countenances. Each layer in CNN has capacity to discover loads of pictures by utilizing lattice assessments which changes over contribution to yield with significant capacities. Layers of CNN used to distinguish coordinated face from removed pictures and give expectation by saving high precision and less time.

- Step 1- Input face image
- Step 2- Face extraction
- Step 3- Image processing by using open-cv
- Step 4- Feature Extraction from images
- Step 5- Model generation
- Step 6- face recognition

Four main layer working approach of CNN explained below:-

a. Convolutional Layer:

We are going to remove various highlights of face pictures like pixel weight lattice figurings by utilizing highlight parts. Perform numerical convolutions on picture, where each capacity utilizes an interesting channel. This result will be in various component maps. Toward the end, we will gather these component guides and draft them as the goal yield grid of the convolution layer.

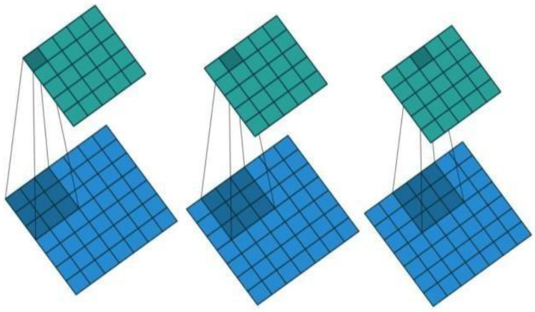


Fig.2 Convolutional Layer

b. Pooling:

The statement of pooling is to continually diminish the dimensionality to limits the quantity of components and count in the system. This constrains the hour of preparing and keeps up over fitting issue. The maximum Pooling separates out the biggest pixel esteem out of a component. While pooling normal is determined for the normal pixel esteem that must be assessed

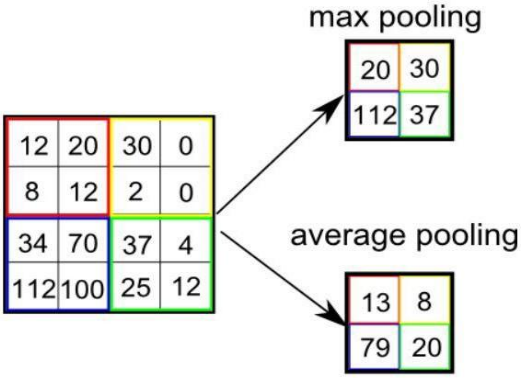


Fig.3. Pooling Layer

c. Flattening:

By and large here we put the pooled highlight into a solitary segment as an example contribution for additional layer (change the 3D framework information to 1D grid information)

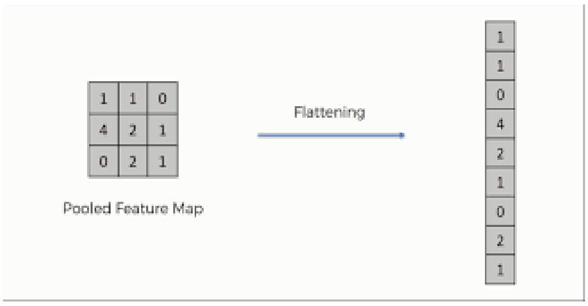


Fig.4 Flattening Matrix

d. Fully Connection:

A fully connection layer has full associations of neurons to all the nodes, in the previous layer. The combination of more neurons to assesses precisely.

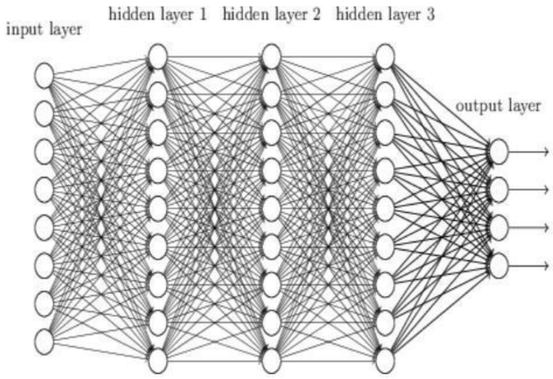


Fig.5 Fully Connected Layer

D. Machine Learning:-

Machine Learning which is a part of AI trains the system to learn automatically and experiences to improvise without being explicitly programmed. Local Binary sample Histogram is a popular and simple surface administrator which names the pixels of a picture by methods for threesholding the area of each pixel and considers the final product as a parallel range. Open source PC vision is a library of programming capacities which are essentially focused on continuous PC vision.

VI. PROPOSED SYSTEM APPROACH

In a proposed framework, we have proposed constant facial acknowledgment based Master Card confirmation and misrepresentation anticipation framework. In a proposed framework, we will conquer existing downsides and give continuous extortion recognition instrument dependent on AI and open-CV python.

We will design following sub modules:

1. **Data Training: -** In this face administrator of MasterCard framework can catch various face pictures of clients and register them into the framework. In the wake of getting face dataset it train the face model for every single client. In preparing stage we have utilized CNN and LBPH for extricating face highlights for making face model. In the wake of making face model we are taking ongoing face picture while login into charge card validation framework. Are taking real time face image while login into credit card authentication system.

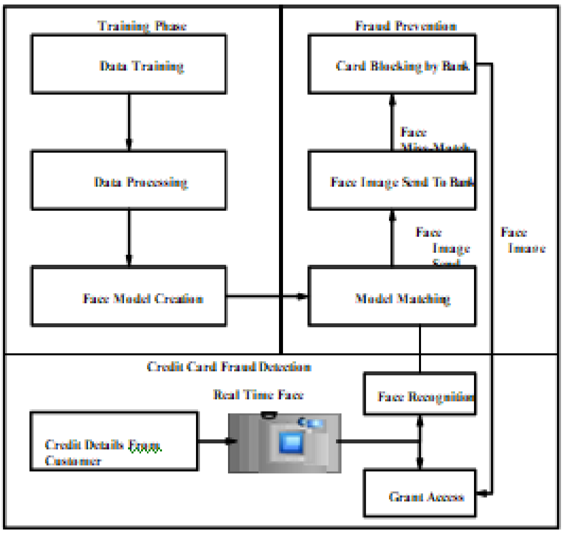


Fig 6. Block Diagram of Proposed System

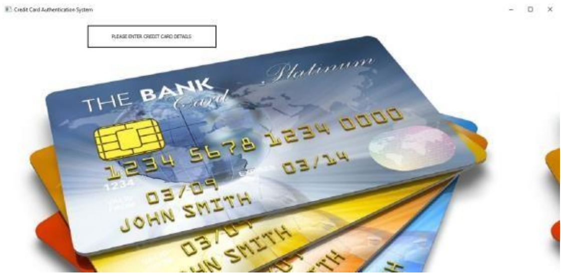
2. **Face feature extraction:** - Utilizing open PC vision library. We are going to catch ongoing face pictures of clients. In the wake of getting faces we are sending these pictures for highlight extraction and picture handling. Facial factor assessment is the technique of getting face parts like eyes, nose, mouth, and so on from continuous face pictures. Facial factor assessment is a lot of fundamental for the introduction of preparing strategies like face location and face acknowledgment.
3. **Fraud Prevention & Detection**: - After face discovery on the off chance that client is legitimate client; at that point get to give to client in any case card
4. **Obstructed by bank**. Which are primary assignment to separate veritable client and unlawful clients. By utilizing ongoing face acknowledgment we are attempting to give physical level security to charge card verification structure.

VII. RESULT AND DISCUSSION

In multifactor authentication system we have been implemented greatly trained model that can accurately analyze real time customers. In this system we used tensor-flow machine learning framework and predefined libraries.

a) Customer home page:

In which credit card system is made up of multifactor authentication mechanism. We try to ensure users confidentiality of account and provide multifactor authentication facility.



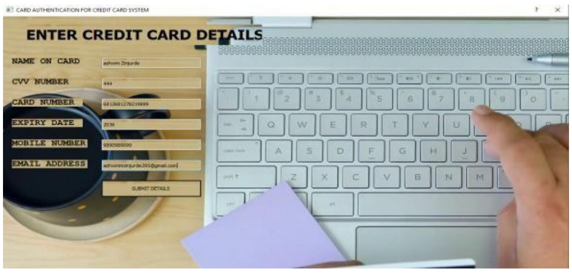
Credit Card Authentication System

PLEASE ENTER CREDIT CARD DETAILS

Fig.7 Customer home page

b) First factor authentication:

In which customer feels its credit card details if all verified correctly then customer get enters into second factor.



CARD AUTHENTICATION FOR CREDIT CARD SYSTEM

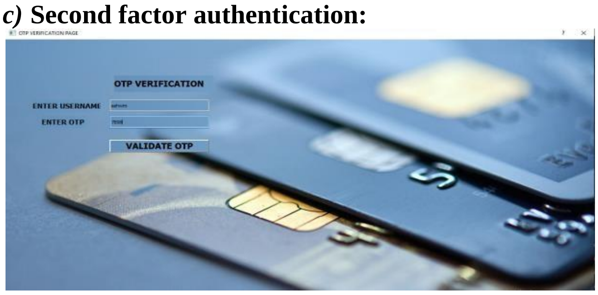
ENTER CREDIT CARD DETAILS

NAME ON CARD: ashwini Zirpurde
CVV NUMBER: 444
CARD NUMBER: [illegible]
EXPIRY DATE: [illegible]
MOBILE NUMBER: [illegible]
EMAIL ADDRESS: ashwinizirpurde295@gmail.com

SUBMIT DETAILS

Fig.8. First factor authentication (card details)

c) Second factor authentication:



OTP VERIFICATION PAGE

OTP VERIFICATION

ENTER USERNAME: ashwini
ENTER OTP: [illegible]

VALIDATE OTP

Fig.9. Second factor authentication (OTP Verification)

d) Third factor authentication (face recognition):

Last and most important aspect of our implementation is real time face recognition. In which customer's real time face verified by using camera. After face verified successfully then and only then customer get its account else it's session terminated and security alert will send to actual user.

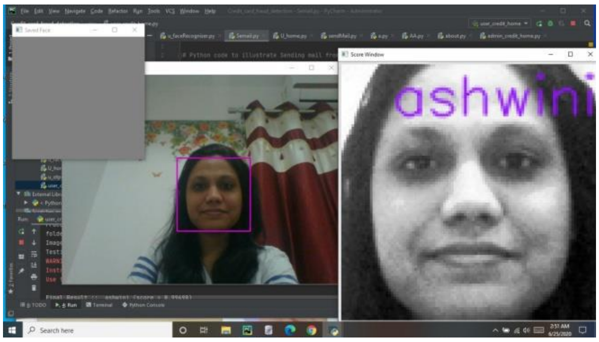


Fig 10. Third factor authentication (Face recognition)

i) Training Model

In credit card fraud detection system we have utilized tensor flow for training and validating purpose to creates models dataset. . In which 1000 image samples per customer were trained for creating of face model. Finally plot files obtained as an result of our trained model.

ii) Testing Model

In final phase of data testing in which real time face images matched by our training model with higher percent of accuracy. After matching correct customer faces results display on console and customer gets its account access. Finally we have been used alert generation for any suspicious activity done with card. The alert email sends to respective customer.

In our experimental setup, In table 1 describe current system modules and respective obtained outcomes.

Table 1: Modules of System

Sr. No.	No Input Sample's	Output Generated
1	Customer card details	OTP verification
2	Input OTP	Face recognition
3	Real time face image	Account access

a) Comparative study:

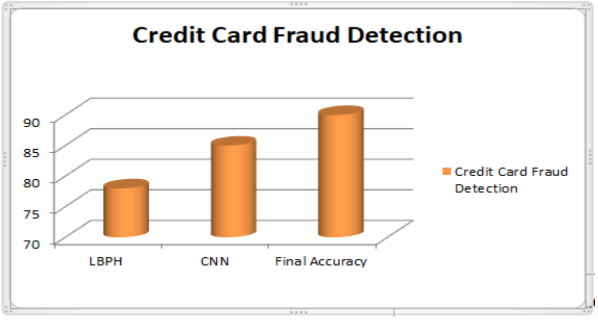


Fig 11. Comparison graph for facial recognition

As per our implementation need we are worked on real time face images captured from system camera while customer proves its identity. Physical level authentication consists of retina scan, thumb scan and face scan. The last and main level of authentication is physical level authentication check. Among all above security factors we are used facial scan using real time face recognition using open cv-python and machine learning. In which we have taken facial image sample of customer and prove its identity by using our machine learning trained model. The LBPH is used to recognize real time face image using har cascade classifier and frontal face xml files. Using open cv-python images can transform from one classifier to other. But only using LBPH we can't getting expected accuracy it get nearly about 78 percent accuracy while working with real time face images. These approach used to recognize real time face images is CNN.

In which we already trained customers face images to create train model for our neural network. By using CNN approach we get nearly about 85 percent accuracy. After that we combine both classifiers LBPH and CNN trained model to accurately recognize faces and grant customers. If unauthenticated person tries to login using credit card details that time they failed to prove facial recognition. Then we get intimation about wrong attempts through registered email and card get temporarily blocked.

VIII. CONCLUSION

We have developed multifactor based credit card fraud detection system with a view to be on the whole depend to users safety an prevent misuse of credit cards. The proposed implementation is based on facial recognition with the assist of other authentication factors such as OTP verification. In future work taking audio and physical level features of retina and thumb to give multi-level security.

REFERENCES

1. Mohsin Karovaliya, "**Enhanced security for ATM machine with OTP and Facial recognition features**" , 1877-0509 © 2015 The Authors. Published by ElsevierB.V.
2. Rupinder Saini ,"**comparison of various biometric methods"** , Vol 2- I-1 2014.
3. Khyati Chaudhary, "**A review of Fraud Detection Techniques: Credit Card**" , Volume 45– No.1, May2012.
4. Anissa Lintang Ramadhani, "**Human Face Recognition Application Using PCA and Eigenface Approach"** , All content following this page was uploaded by Eri Prasetyo on 15 February2019.
5. Janani.S.R., "**secured credit card transactions using webcam**" , 2016, IRJET.
6. M. Eckhardt and R. Picard. , "A more effective way to label affective expressions" . In Affective Computing and Intelligent Interaction and Workshops, 2009. ACII 2009. 3rd International Conference on, pages 1–2. IEEE,2009.
7. M.Schedl,H.Zamani,C.-W.Chen,Y.Deldjoo,andM.Elahi,''Current challenges and visions in music recommender systems research,''Int. J. Multimedia Inf. Retr., vol. 7, no. 2, pp. 95–116, 2018.
8. O. Olabiyi, E. Martinson, V. Chintalapudi, and R. Guo. (2017). ''Driver actionpredictionusingdeep(bidirectional)recurrentneuralnetwork.'' [Online]. Available:https://arxiv.org/abs/1706.02257
9. C. V. Sheena and N. K. Narayanan, ''Key-frame extraction by analysis of histograms of video frames using statistical methods,'' Procedia Comput. Sci., vol. 70 pp. 36–40, Jan.2015.
10. A. Schaefer, F. Nils, X. Sanchez, and P. Philippot, ''Assessing the effectivenessofalargedatabaseofemotion-elicitingfilms:Anewtool for emotion researchers,'' Cognition Emotion, vol. 24, no. 7, pp. 1153–1172,2

AUTHORS PROFILE

Ashwini. M. Zinjurde
Mtech Student Department of Computer Science & Engineering PESCOE ,Aurangabad

Dr. Vilas. B. Kamble
Associate Professor Department of Computer Science & Engineering CSI Life membership CSI LM 00112518 ISTE LM 42747 PESCOE , Aurangabad