International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 07 | July - 2022 Impact Factor: 7.185 ISSN: 2582-3930

CREDIT CARD FRAUD DETECTION AND PREVENTION BY FACE RECOGNITION

[1] Mohammed Sadiq, [2] Sindhu

[1] Assistant Professor, Department of Master of Computer Application, BIET, Davangere
[2]Student, Department of MCA, BIET, Davangere

***Abstract*—Internet banking is now becoming the most commonly used form of banking transactions. Confidentiality can be compromised in the process of electronic purchases. We therefore introduced a new approach to prevent theft during online transactions in order to protect information through a two-step mechanism of authentication. The primary step of authentication is OTP verification. If the OTP has been checked, the face should be recognized. The details are collected and the authorization for both true and fraudulent transactions is submitted to the bank. The new credit card scanning device has beneficial characteristics such as certain health, user-friendliness, etc. The purpose of the application is to reduce credit card fraud by knowledge of the Face System. Customers get the most accessible and highly efficient electronic banking program.**

***Index Terms*—Authentication, Credit card scanning, face recognize, Local Binary Patterns (LBP), Open-CV, RSA, transaction, verification, webcam.**

I. INTRODUCTION

As a result of rapid advances in science and technology, potential technologies are being set up with solid protection. But there's always a justification to crack this security system on the other side. While automation enhancement has had a positive overall effect, numerous financial institutions, such as banks and applications such as ATM, are still subject to theft and fraud. The new ATM configuration uses a card anda PIN to maximize security in the case of counterfeit cards, or due to arbitrarily issued PINs, duplicate cards and various other challenges. To solve, a hybrid interface consisting of traditional features coupled with new features such as facial recognition and a one-time password is used. Database stores information about the user's account data, photographs of his / her face and a mobile number that will significantly boost protection. The primary thing the customer has to do is tap the ATM card. The live image is taken automatically through a webcam mounted on the ATM, which is compared to the images saved in the database. If it matches, an OTP willbe 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 tran When this fits, an OTP will be sent to the appropriate registered mobile phone. The customer must put this randomly generated code in the text box. When customers put a legitimate OTP, they will continue with the transaction. The segment can continue. So,the combination of a face-recognition algorithm and an OTP significantly decreases the risks of theft plus frees the user from the extra burden of recalling complicated passwords.

II. PROPOSED MODEL

The purpose of the project is to create a framework thatuses face recognition to authenticate a legitimate person. First, the customer will enter the details of the credit card and the information will be checked in the bank database.

After the verification process, OTP is produced and sent tothe customer. If the OTP has been checked, the user will be asked for face authentication. The webcam face picture will be collected and forwarded to the bank servers for authentication in encrypted form. The image would be decrypted in the database and used for authentication purposes. The RSA algorithm is used for image encryption and decryption. The Python language is used for scripting and manipulating the Open-CV library file that is embedded into Python. After that, the LBP algorithm is used to authenticate the face. Unless the identity suits the picture stored in the database, the user's credit card cap will be reviewed and, if it satisfies the criteria, the user will be able to make a charge or the charge will be cancelled.

- RSA- RSA algorithm is used for encryption and decryption purpose. It makes use of two keys Public key and Private key. The public key is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key.
- Open-CV- Open-CV (Open Computer Vision) is a library mainly aimed at real-time computer vision. It provides great support for face detection and face-recognition techniques using Python.
- LBP- LBP is a type of algorithm used for classification in computer vision. It has been found to be a powerful feature extraction and classification purposes

III. LITERATURE SURVEY

Mohsin Karovaliya [1] is proposed this system is to make traditional ATM model more safe. We also put forward a new concept that will improve the overall transaction experience; reliability and comfort at the ATM. Features such as face recognition and One-Time Password (OTP) are used for improving account security and user privacy. Face popularity generation allows the gadget to identify each and every person uniquely hence making face as a key. This completely eliminates the probabilities of fraud because of theft and duplicity of the ATM cards. Furthermore, the randomly generated OTP frees the person from remembering PINs as it itself acts as a PIN.

Rupinder Saini [2] introducing this system affords contrast concerning diverse biometric systems in reality by using defining their advantages and disadvantages. A short creationis generally offered regarding normally used biometrics, inclusive of, Face, Iris, Fingerprint, Finger Vein, Lips, Voice. The contrast standards listing added is restrained to accuracy, size of template, cost, safety stage, and long time balance.

Khyati Chaudhary [3] proposed in present state of affairs whilst the time period fraud comes into a discussion, credit card fraud clicks to mind thus far. With the extraordinary growth in credit card transactions, credit card fraud has increasing excessively in recent years. Fraud detection consists of tracking of the spending behavior of customers/ clients if you want to willpower, detection, or avoidance of undesirable conduct. As credit score card will become the most winning mode of charge for each online in addition to regular purchase, fraud relate with it are also accelerating. Fraud detection is involved with no longer simplest capturing the fraudulent events, but additionally shooting of such activities as quick as viable.

Anissa Lintang Ramadhani [4] has proposed added Face is the most memorable a part of the frame in actual life that makes it an critical variable. on this studies, we use face apprehend technique that incorporated in Ry-UJI robotic. The robot is diagnosed with the aid of a detected voice command looking for someone and when someone's face has been determined, face reputation is entire. This text will apply the human face recognition device the usage of the Eigen-face approach. Eigen-face is one of the facial recognition strategies based totally at the fundamental issue evaluation (PCA) set of rules. PCA involved a mathematical procedure to derive a hard and fast of features for face reputation. Face recognition level begins with face detection technique the usage of cascade classifier method, face preprocess, acquire and educate the face detected and subsequently the face popularity.

Janani. S. R [5] states credit card affords prominent use of charge method, so it's far accompanied in many scenarios. As we know, in the course of on line transactions there are many chances to steal the private information through the attackers or hackers. So, we endorse a brand new method to keep away from fraudulent all through online transactions and to cozy the facts by means of a step verification procedure. The information is processed and the acknowledgement is dispatched to the bank for each the legitimate and invalid transactions. a new approach of credit card scanning has beneficial attributes in phrases of cost financial savings and time performance.

IV. EXISTING SYSTEM APPROACH

Fraud is one of the big legal problems in the credit score card industry. The main goals are, first of all, to recognize the unusual forms of credit score card fraud and, secondly, to test the different methods used to detect fraud [4]. The sub- purpose is to provide, evaluate and analyze recently published findings in the detection of credit score card fraud. This article describes specific terminology for credit score card fraud and highlights important facts and figures in this field. Based on the nature of theft encountered by banks or credit card companies, a variety of steps can be implemented and enforced. The recommendations made on this paper may have valuable characteristics in terms of price reductions and time efficiency. The importance of the use of the methods examined right here lies in the minimization of credit report card theft. However, there are still legal issues when good credit report card consumers are misclassified as dishonest. In addition to the ethical nature of dishonest actions, there has been a growing interest in banking ethics for some time. A critical venture to help businesses and Political institutions, along with banks, must take measures to deter and resolve theft quickly and correctly.

V. METHODOLOGY USED

A. Image Processing

Every image is formation of RGB shades. Every captured picture has some noise, unwanted background. Therefore thereis 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 implemen-tation 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 destinyeffects.

C. Convolutional Neural Networks

In proposed work we are using CNN which takes face images as a input. After getting images from opencv python it will processed using image processing techniques for feature evaluation. We extract different features from those images using Har-cascade. By using a series of mathematical functions we are going to identify the unique faces. Every layer in CNN has capability to find out weights of images by using matrix evaluations which converts input to output with valu- able functions. Layers of CNN used to identify matched face from extracted images and give prediction by preserving high accuracy 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 extract different features of face images like pixel weight matrix calculations by using feature kernels. Perform mathematical convolutions on image, where every function uses a unique filter. This outcome will be in different feature maps. At the end, we will collect all of these feature maps and draft them as the destination output matrix of the convolution layer.

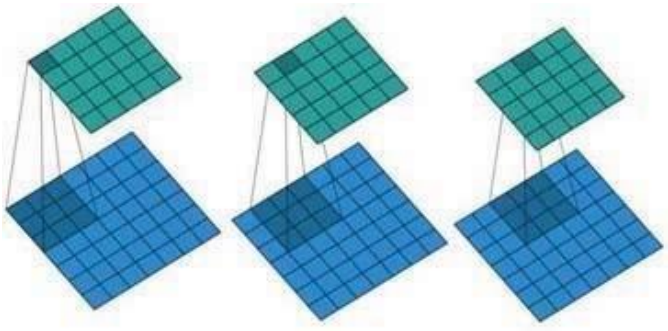

Fig. 1. Convolutional Layer

b) Pooling

The expression of pooling is to constantly decrease the dimensionality to limits the number of factors and calculationin the network. This limits the time of training and maintains over fitting problem. The max Pooling extracts out the largest pixel value out of a feature. While pooling averageis calculated for the average pixel value that has to be evaluated.Pooling layer operates on each feature map independently.

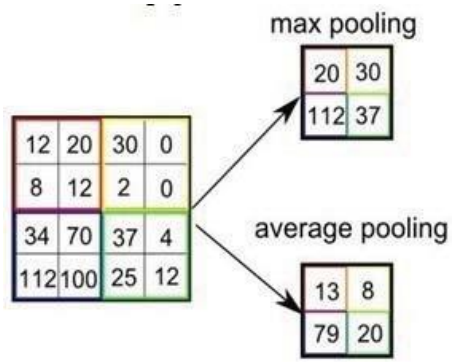

Fig. 2. Pooling layer

c) Flattening

Generally here we put the pooled feature into a single column as a sample input for further layer (transform the 3D matrix data to 1D matrix data)

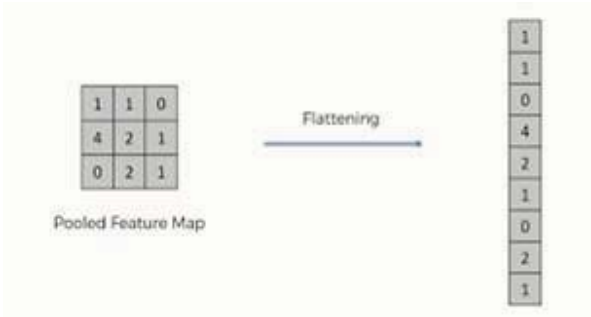

Fig. 3. Flattening Matrix

d) Fully Connection

A fully connected layer has full connections of neutrons to all the nodes in the previous layer. The fusion of more neurons to evaluates accurately.

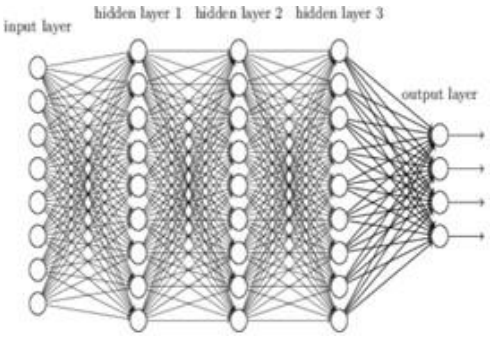

Fig. 4. Fully Connected Layer

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 common and easy-to-use texture operator that marks the pixels of an image by thresholding the vicinity of each pixel and considering the end result to be a binary set. Open Source Computer Vision is a library of programming functions that are mainly designed for real-time machine vision.

VI. PROPOSED SYSTEM APPROACH

In a proposed system, we have proposed real time facial recognition based credit card verification and fraud prevention system.

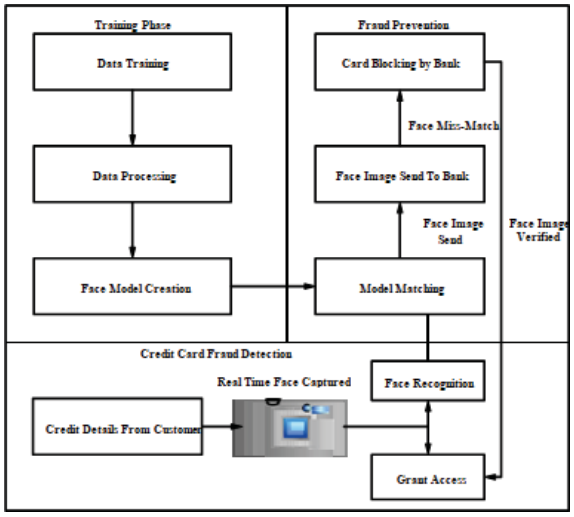

Fig. 5. Block Diagram of Proposed System

In a proposed system, we are going to overcome existing drawbacks and provide real time fraud detection mechanism based on machine learning and open-CV python.
We are going to invent following sub modules:

1. Data Training: - In this face admin of credit card system can capture multiple face images of customers and register them into the system. After getting face dataset it train the face model for each and every customer. In training phase we have used CNN and LBPH for extracting face features for creating face model. After creating face model we are taking real time face image while login into credit card authentication system.

2. Face feature extraction: - Using open computer vision library. We are going to capture real time face images of customers. After getting faces we are forwarding these images for feature extraction and image processing. Facial factor evaluation is the procedure of getting face parts like eyes, nose, mouth, etc. from real time face images. Facial factor evaluation is very much essential for the initialization of processing techniques like face detection and face recognition.

3. Fraud Prevention Detection: - After face detection if customer is legal customer then access grant to customer otherwise card blocked by bank. Which are main task to differentiate genuine customer and illegal customers. By using real time face recognition we are trying to provide physical level security to credit card authentication framework.

VII. RESULTS AND DISCUSSION

TABLE I
COMPARISON TABLE FOR FACIAL RECOGNITION

Sr. No	Comparison Parameter		
	LBPH	*CNN*	*Final Accuracy*
1	78	83	87

In our proposed credit card fraud fraud detection system, mainly shows result of 3 different parameter for comaparision like LBPH,CNN and final accuracy.In following table 1, we seen that value of LBPH is 78,CNN is 83 and final accuracy is 87.

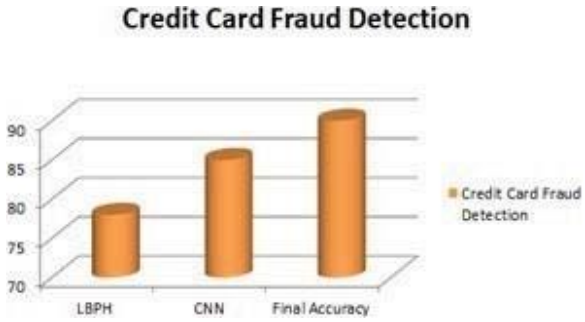

Fig. 6. Comparision graph for facial recognition

As per our implementation need we are worked on real time face images catured 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 opencv-python and machine learning. In which we have taken facial image sample of ccustomer 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 opencv-python images can tranform from one classifierto other. But only using LBPH we cant getting expected

accuracy it get nearly about 78 percent accuracy while working with real time face images. The second approach used to recognize real time face images is CNN. In which we already trainned 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 unathenticated person tries to login using credit card details that time they failed to prove facial reacognition. Then we get intimation about wrong attempts through registred email and card get temporarly blocked.

VIII. CONCLUTION AND FUTURE WORK

We are creating a credit card fraud monitoring system focused on face-to-face identification in real time, with a viewto ensuring the safety of consumers and avoiding abuse of credit cards as a whole. The proposed application is contrasted with the facial recognition assist and the study unit. For future practice, the audio and physical level features of the retina and thumb will have multi-level protection

ACKNOWLEDGMENT

This work is supported in a credit card fraud detection and prevention by face recognition of any state in india. Authors are thankful to Faculty PESCOE,Aurangabad for providing the facility to carry out the research work.

REFERENCES

[1] Mohsin Karovaliya, "Enhanced security for ATM machine with OTP and Facial recognition features," International Conference on Advanced Computing Technologies and Applications (ICACTA2015),may 2015
[2] Rupinder Saini , "comparison of various biometric methods," IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI) 2016
[3] Khyati Chaudhary , "A review of Fraud Detection Techniques: Credit Card," International Journal of Computer Applications (0975 – 8887) Volume 45– No.1, May 2012
[4] Anissa Lintang Ramadhani , "Human Face Recognition Application Using PCA and Eigenface Approach," 2017 Second International Conference on Informatics and Computing (ICIC),NOV 2017
[5] Janani.S.R. , "secured credit card transactions using webcam," International Research Journal of Engineering and Technology (IRJET) 2019