Credit Card Transaction Based on Face Recognition Technology

Dhikhi T¹, Ajay Rana², Anurag Thakur³, Karan Kapoor⁴

¹Assistant Professor, SRM Institute of Science and Technology, Chennai, India
²,³,⁴Department of Computer Science and Engineering, SRM Institute of Science and Technology Chennai, India
tdhikhi@gmail.com¹, ajay.rana6288@gmail.com², anuragthakur532@gmail.com³
karan98kpop@gmail.com⁴

Abstract— This paper proposes a method for credit card transaction system which will make use of face recognition and face detection technology, using Haar Cascade and GLCM algorithm. The main problem faced by credit card users is attack to lot of privacy issues such as credit card. This generally happens when users give their credit card number to unknown people or when the card is lost. So, we are proposing a system that will reduce the risk of credit card frauds. The system we are proposing will match the image of user’s face with dataset of respective user. A database will be maintained for authentication purpose. If the image matches, that means user is genuine and he will be allowed to proceed otherwise, the user will be denied to do the transaction.

Keywords— Haar Cascade, GLCM Algorithm, Administrator, Face detection, Face recognition.

1. INTRODUCTION

In the current scenario, credit card and debit card are becoming the most common type of payment mode. All the credit card related task is managed by credit card processor. Companies using credit card processing makes sure that transactions are processed correctly and on time. Many companies prefer online transaction because it benefits their business. Funds are transferred into account on time without putting much effort.

Since people are comfortable with cashless transactions, the demand of credit card is increasing rapidly. The main problem faced by the credit card users is to have a secure online transaction. Credit card fraud is a big challenge. The proposed solution will make use of face detection and face recognition technology for making credit card transaction system secured and much better.

2. RELATED WORK

One of the existing systems deals with securing payment process between the card issuer and the card reader terminal and it is thus ensures that card number is not known to any other entity, other than the two end points [1]. There is another system that suggests, a detection model must be available to capture the possible anomalous transaction [2]. There is a number of challenges like concept drift, class imbalance and verification latency in credit card fraud detection [3]. Machine learning can also be used for detecting credit card fraudulent transaction using a real world dataset [4][5]. Deep learning presents a programming resolution to the matter of mastercard fraud detection that produces use of historic client knowledge in addition as real time group action details that area unit recorded at a similar time of group
action [6]. There is another system that makes use of two random forests to train the behavior features of normal and abnormal transactions. The system compares the two forests which differs in classifier and analyze their performance on credit card transaction [7][8]. One of the existing system makes use of Boat algorithm for detecting fraud transaction [9]. There is another system which analyze the periodic behavior of the time of a transaction using the Von Mises Distribution [10].

3. COMPONENTS OF SYSTEM

A. Haar Cascade

Haar Cascade, a machine learning object detection algorithm rule accustomed establish objects in a picture or video and supported the idea of options planned by Paul Viola and Archangel Jones. It’s renowned for having the ability to observe (identify) faces and parts pictures. A Haar Cascade is largely a classifier that is employed to observe the thing that it’s been trained for, from the supply. The Haar Cascade is by superimposing the positive image over a collection of negative pictures. The coaching is mostly done on a server and on numerous stages. Higher results are obtained by victimization top quality pictures and increasing the quantity of stages that the classifier is trained.

The algorithmic rule has four stages: Haar Feature Choice, making Integral pictures, Adaboost coaching, Cascading Classifiers. In general, 3 types of options are utilized in that the worth of a 2 rectangular options is that the distinction total of the pixels at intervals 2 rectangular regions. These regions have same form and size and are horizontally or vertically adjacent. Wherever as within the 3 rectangular options are computed by taking the total of 2 outside parallelograms then ablated with the total in an exceedingly center rectangle. Moreover, within the four rectangles feature computes the distinction between diagonal pairs of rectangles.

![Haar Cascade](image)

Fig. 1: Haar Cascade

B. Face recognition

It’s a engineering being employed in various form of applications that identifies human faces in digital pictures. Face detection jointly refers to the psychological method by that humans find and commit to faces in an exceedingly visual scene. Face Detection is that the 1st and essential step for face recognition, and it’s accustomed observe faces within the pictures. It’s a vicinity of object detection and might be use in several areas like security, bio-metrics, enforcement, diversion, personal safety, etc. It’s
accustomed observe faces in real time for police investigation and chase of person or objects. It’s wide utilized in cameras to spot multiple appearances within the frame Ex- Mobile cameras and DSLR’s.

First, an image of your face is captured from a photograph or video. Your face may seem alone or in an exceedingly crowd. Your image could show you wanting straight ahead or nearly in profile. After that, identity verification package reads the pure mathematics of your face. Key factors embody the space between your eyes and also the distance from forehead to chin. The package identifies facial landmark, one system identifies sixty eight of them, that are key to identifying your face. The result: your facial signature. Then your facial signature and a mathematical formula is compared to an information of far-farmed faces. And at last a determination is created. Your faceprint could match that of a picture in an exceedingly identity verification system information.

C. **GLCM Algorithmic rule**

It stands for Gray-level Co-occurrence matrix. The GLCM perform characterize the feel of a picture by calculative however usually pairs of pel with specific values and in an exceedingly specified spatial relationship occur in a picture, making a GLCM. A GLCM may be a matrix wherever the quantity of rows and columns is up to the quantity of grey levels, G, within the image.

The matrix components $P(i, j | \Delta x, \Delta y)$ is that the frequency with that 2 pixels, separated by a pel distance $(\Delta x, \Delta y)$, occur at intervals a given neighborhood, one with intensity ‘i’ and also the different with intensity ‘j’. The matrix components $P(i, j | d, \theta)$ contains the second order applied math likelihood values for changes between grey levels ‘i’ and ‘j’ at a selected displacement distance $d$ and at a selected angle $(\theta)$. Employing a sizeable amount of intensity levels $G$ implies storing a great deal of temporary information, i.e. a $G \times G$ matrix for every combination of $(\Delta x, \Delta y)$ or $(d, \theta)$.

![Fig. 2: GLCM Algorithm](image)

**4. PROPOSED SYSTEM**

The aim of the project is to implement a system, that uses face recognition and detection technique to authenticate the individual, in order to perform a successful and a secured transaction. This system will help in reducing credit card frauds. The aim is to make the transaction system fully automatic, that provides a reliable mode of online transaction process. In the proposed system, user gets authenticated by the system by matching the features of user image to the features stored in administrator. If the features matches, the transaction will be done successfully if not the user will be denied and transaction will not proceed.
5. MODULE DESCRIPTION

Module 1 (Admin Module)- Administrator register to the system using administrator login and password provided by the administrator is compared to the password stored in the system for the authentication purpose. This module is responsible for making changes in the system and get users registered to our system.

In this, face image is cropped from the given image (input) the features are extracted and stored in the database using Gray Level Co-occurrence Matrix.

Fig. 3: Flow Chart for the system
Module 2 (User Module)- Here user authentication process is done. Only the authenticated user is allowed to proceed.

In this module, the password given by the user is compared to the password stored in the database. If it matches, user will be allowed proceed i.e. user will be allowed to do the transaction. If not he or she will be denied from doing the payment.

6. RESULT AND DISCUSSION

A. The given screenshot displays the web page where admin can login to the system.
B. This screenshot displays the face detection and feature extraction process, done by data stored in database.

C. The user login to the system using the credential given at the time of registration.

D. This image shows the payment details. Here the details entered by user is matched with the details stored in database.
E. This image shows the process of comparing the user image with the image stored in database, that is the original image for user authentication.

F. If the user is genuine, he will be allowed to do the transaction. This image shows the payment confirmation.
7. CONCLUSION

Our proposed project has been designed for the purpose of reducing the credit card frauds that may occur during online payment transaction. There is no need of specialized hardware for installing this system. It just need a computer and a camera for construction. The system is reliable and efficient mode of transaction process.

The camera plays a crucial role in the working of our project, therefore the image quality and also the performance of the camera must be tested time to time.

8. FUTURE WORK

Since we have proposed a modular approach we can improve different modules until we reach an acceptable identification and authentication rate. The comparison of the input image and the image stored in database should be fast and reliable enough.

9. REFERENCES

[1]. Method for secure credit card transaction, Nader Nassar, Grant Miller, International Conference, 2013.
[2]. Credit card fraud detection based on transaction behaviour, John Richard, Larry A. Vea, TENCON, 2017.
[3]. Credit fraud card detection, Andrea, Giacoma, Olivier Cealen, IEEE International Conference, 2018.
[4]. Credit card fraudulent Transaction Detection, IEEE International Conference, 2018.
[5]. Credit card fraud detection using machine learning, John williams, 7th IEEE International Conference, 2017.
[6]. Deep learning detecting fraud in credit card transaction, Abhimanyu Roy, Loreto Alonzi, Peter Beling, System and information, 2018.
[7]. Credit card fraud detection system, V. Filippov, System and information, 2008.
[8]. Random forest for credit card fraud detection, Lutao Zheng, Shuo Wang, IEEE 15th International conference, 2018.
[9]. Boat adaptive credit card fraud detection System, KK Sherly, IEEE International conference, 2010.
[10]. Detecting credit card fraud using periodic features, Alejandro, Bjorn, IEEE International Conference, 2015.
[11]. MN BORHAN,"Design Of The High Speed And Reliable Source Coupled Logic Multiplexer", Journal of VLSI Circuits And Systems 1 (01), 18-22, 2019
[12]. Mv Ngo Tien HoA, "High Speed And Reliable Double Edge Triggered D- Flip-Flop For Memory Applications", Journal of VLSI Circuits And Systems, 1 (01), 13-17, 2019