Authentication of credit card using facial recognition

Amit Kumar Sah
Koneti Hemanth Raju
Santhosh Kumar Manish S Prasad

Abstract-The biggest problem faced by credit card users is that they have secure online transactions using credit cards. Credit card fraud is a major risk factor for credit card fraud. Credit cards were stolen and used to purchase large items, which often resulted in significant losses of credit card and business processing services. The security of transactional processes can be easily hacked because of advanced technology. Biometric authentication is considered to be the key to improving security issues. In this paper, a new face-to-face verification process is proposed to improve the security of the online payment system. Test results show that the proposed new process with face-to-face verification can increase security and improve the usability, power, and user satisfaction of the online transaction process.
The project proposes a credit card transaction system that will integrate face detection and face recognition technology using various Open-CV and machine learning techniques, respectively. Before access is granted, the user will need to take a photo of the face in order to access his account, face geometry, eye distance and nose compared. This image will be compared to the image on the bank server for verification, if it exceeds the verification, access will be granted, otherwise it will be rejected.
Keywords- Open-CV, Face Recognition, Security, Verification, Credit Card.

I. INTRODUCTION

India has more than 840.6 million bank card holders and more than 50.3 million credit card holders. It can be expected that a percentage of this nation, given the government's preference for a poor society, would accept the option of a card transaction. From the survey conducted, 29% of consumers prefer card payments, and 42% use digital payments. Although the credit or bank card acceptance rate in the country is still very low, many banks currently offer Rupay cards to customers. Visually, the cards provided by these banks only require a CVV and a pin to gain access. Because there is no complete system, card transactions have their problems. Credit cards and credit card pin codes can be stolen or lost. The proposed solution provides a secure method for credit card authentication using Facial recognition.

Figure 1.1 Credit Card Frauds

Credit cards and Debit cards are widely used around the world. Credit cards quickly become the most common payment method for large purchases. People use credit cards in online transactions in supermarkets. Credit card fraud becomes a major threat to credit card operations. Therefore the need to confirm the process is required in an hour. Credit cards and credit card PINs can be stolen or lost and used illegally by thieves and where obtaining money is difficult because this is an organized crime organization.This project uses the ideas for "Credit Card Verification" based on face recognition in which it submits major applications.

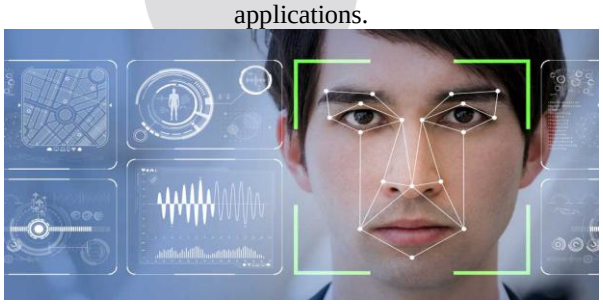


Figure 1.2 Facial Recognition

In the physical world, authenticity is achieved by signing autographs by hand at the point of sale. Without proving valid validation, the following Similar problems can arise fraudulent transactions, long transaction processes including customer insecurity, high transaction costs, etc. Our proposed system is to protect online transactions using face recognition. To help the user

make secure transactions when making the Internet in the system. It helps online shopping websites to make payments more efficient.

Multiple authentication settings include asking the user his username and CVV and verifying his or her identity with a second object such as an OTP message on their registered phone number. But sometimes the SMS on our number is blocked and many such cases happen so a fake transformation occurs. This is a major problem in today's digital world.

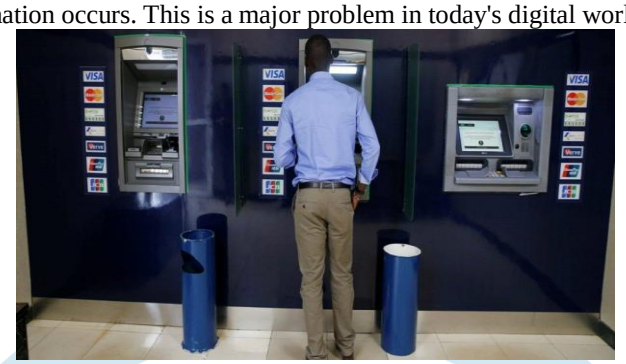


Figure 1.3 ATM

In the proposed system we use a facial verification method to avoid fraud. We also enter card details when making a payment option, when we need to scan the face for the payment to be successful. In the event that a face is different, payment will not be successful and in these ways, we can avoid fraudulent discovery that only the owner will be able to use. And in the future, we can also use biometric in payment mode. The system is expected to provide a high level of authentication (multifactor authentication) that will bring unauthorized access to the minimum barest.

Before access is granted, the user will need to take a photo of the face in order to access his account, face geometry, eye distance and nose compared. This image will be compared to the image on the bank server for verification, if it exceeds the verification, access will be granted, otherwise it will be rejected. In case of unauthorized access, a bank security warning message will be sent.

II. Existing Systems

Multiple authentication settings include asking the user his username and CVV and verifying his or her identity with a second object such as an OTP message on their registered phone number. But sometimes the SMS on our number is blocked and many such cases happen so a fake transformation occurs. This is a major problem in today's digital world. In general, online banking sites and mobile applications are designed for security and banks continue to put renewed security agreements in place. Existing system issues:

- 2-Way authentication contains card and OTP details only.
- Poor level of security.
- It is easy for hackers to get into an account.
- Hackers can hold a SIM card.
- If a SIM card is made, the bank server will assume that the criminal is a real user. Prone to unauthorized access by perceived third parties.

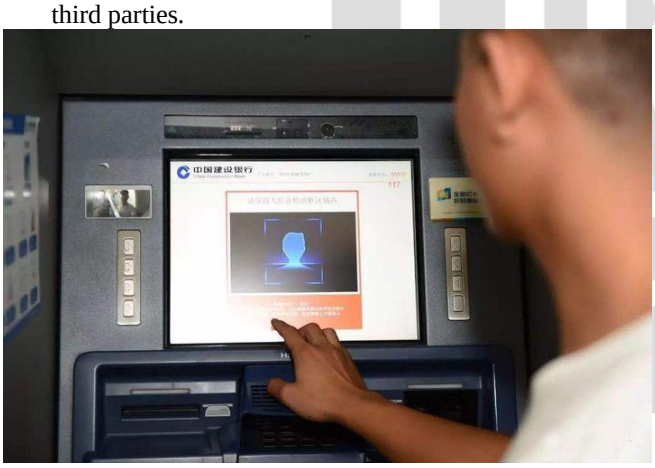
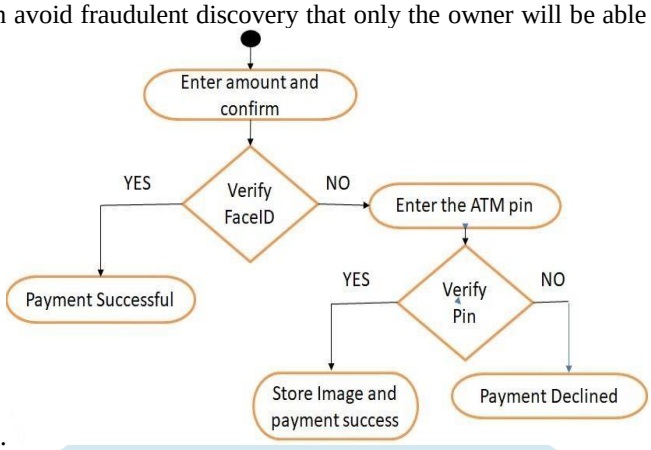


Figure 2.1 Face Recognition in ATMs

III. Proposed System

In the proposed system we use a facial verification method to avoid fraud. We also enter card details when making a payment option, when we need to scan the face for the payment to be successful. In the event that a face is different, payment will not be

successful and in these ways, we can avoid fraudulent discovery that only the owner will be able to use. And in the future, we can also use biometric in payment_mode.



The system is expected to provide a high level of authentication (multifactor authentication) that will bring unauthorized access to the minimum barest. Before access is granted, the user will need to take a photo of the face in order to access his account, face geometry, eye distance and nose compared. This image will be compared to the image on the bank server for verification, if it exceeds the verification, access will be granted, otherwise it will be rejected. In case of unauthorized access, a bank security warning message will be sent. And the customer was informed about the problem.

IV. METHODOLOGY

The main purpose of the project Face recognition. Where the system takes a user's image and checks if the image is the same as the image in the database if it matches what was done allowed otherwise rejected. The face recognition process involves a lot of work behind the scenes where many algorithms are involved in face recognition. The three main steps in the system are

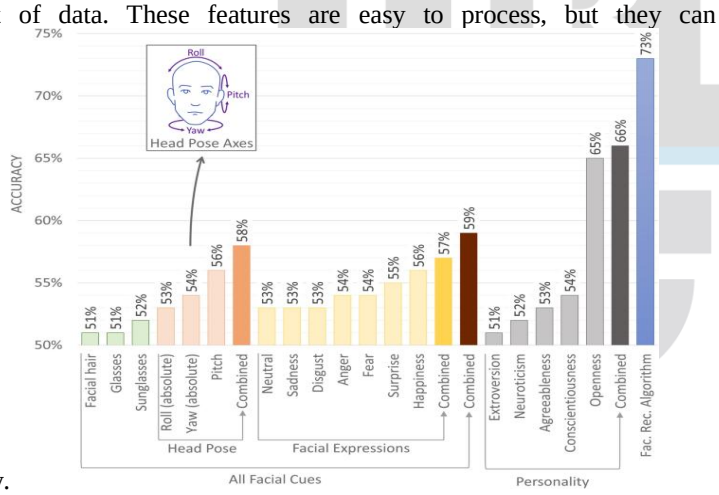
- Face detection
- Feature extraction
- Face recognition.

A. Face detection

Face detection is the first and most important step in face recognition, and it is used to find faces in photos. It is part of the acquisition of an object and can be used in many areas such as security, biometric, law enforcement, entertainment, personal security, etc. It is used to detect faces in real time of observation and tracking of people or objects. It is widely used in cameras to identify multiple appearances in the Ex-Mobile camera and DSLR frameworks. Facebook also uses a face recognition algorithm to find faces in photos and get to know them

B. Feature release

Feature extraction is part of a size reduction process, in which, the original set of raw data is separated and downgraded into control groups. So when you want to process it will be easy. The most important feature of these big data sets is that they have a great value for flexibility. These mutations require a lot of computer resources to process them. Feature extracting therefore helps to obtain the best feature in those big data sets by selecting and incorporating flexible features, therefore, effectively reducing the amount of data. These features are easy to process, but they can still explain the actual details set accurately and initially.



C. Face Recognition

Make face matching face to face with one or more known faces in the configured database. This is the final phase of the project. The project was implemented using a local binary pattern algorithm. Here the actual face matching occurs against the image in the database. After this step, we get the final result, even if the program finds the same face in the database.

D. Face Recognition Process

There are many ways to get a face, with the help of these methods, we can see the face with high accuracy. These processes have similar face detection methods such as OpenCV, Neural Networks, Matlab, etc. Face detection works to find more faces in an image. First the image is imported by providing an image location. Image is converted from RGB

to Grayscale because it's easy to see faces on grayscale.

Figure 4.1 Converting from RGB to Grey

After that, image manipulation is applied, in which size, cropping, blurring, and sharpening of images are done as needed. The next step is to split the image, which is used to find a line or to separate multiple objects in one image so that the editor can quickly see the objects and faces in the image.

E**. Haar Cascade**

Haar Cascade, the discovery of a machine-generated object that is often designed to create objects in an image or video and supports the idea of options developed by Paul Viola and Archangel Jones. It is known for its ability to view (identify) images and parts of images. Haar Cascade is primarily a separator used to detect what we have been trained for, from dedication. Haar Cascade by providing a good image over a collection of negative images. Training is mostly done on the server and in many stages. Higher results are achieved by the concentration of high quality images and the increase in the number of segments in the training separator. The next step is to use the Haar-Like feature algorithm, suggested by Viola and Jones to find the face. This algorithm is used to determine the location of a person's face in a frame or image. All human faces share certain areas of the human face such as the eye area is darker than its neighbors' pixels and the area of the nose shines brighter than the eye area.

A haar-like algorithm is also used to select a feature or to remove an element of an object from an image, with the help of edge detection, line detection, intermediate detection of eyes, nose, mouth, etc. in the image. It is used to select the most important elements in an image and to extract these features to determine the face.

These common features can be compared using Haar Features. A few common facial features:

a. The eye area is darker than the upper cheeks.
b. The nasal bridge region is brighter than the eyes.

Composition of structures that form comparable facial features:

a. Location and size: eyes, mouth, nose bridge
b. Price: gradients oriented to pixel dynamics.

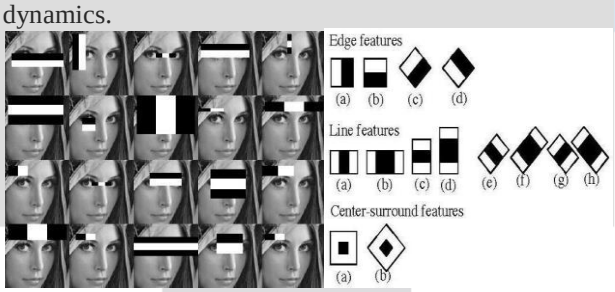


Figure 4.2 Haar cascade Feature Extraction

The next step is to provide the x, y, w, h links that form a rectangular box in the image to show the surface of the face or we can say that to indicate the area of interest in the image. After this, it can form a rectangular box in the area of interest where it finds the face. Many other discovery techniques are used together to find discovery such as smile, eye recognition, blink detection, etc.

F. Local Binary Patterns Histogram

It was first described in 1994 (LBP) and has since been found to be a powerful factor in texture separation. It has also been identified that when LBP is combined with histograms of mean definition gradients (HOG), it improves the performance of large-scale acquisition of other data sets. Using LBP compiled with histograms we can represent face images with a simple data vector.

Local Binary Pattern is an algorithm based on the composition of an object. However, unlike other text-based algorithms that typically use a global boundary value, this algorithm reflects the local representation of texture. LBP is defined as a set of binary comparisons of large pixels between center pixels and eight round pixels. Local Binary Pattern makes this comparison using the following formula:

$$LBP(x_c, y_c) = \sum_{n=0}^{7} s(i_n - i_c)2^n$$

When ic is equal to the value of the center pixel ($xxcc$, $yycc$), the value of eight round pixels. Icon
used to specify local features in facial images and works using a basic LBP operator. Face Feature released matrix initially in size 3 x 3, values are compared to the average pixel value, then a binary pattern code is generated and the LBP code is obtained by converting binary code into a single decimal.

The first computational step for LBPH is to create an intermediate image that defines the original image in a better way, by highlighting facial features. To do so, the algorithm uses the concept of a quick window, depending on the parameter and neighbor parameters.

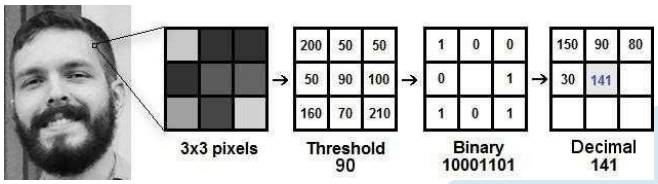


Figure 4.3 LBPH operation

Now, using the image generated in the last step can use the Grid X and Grid Y parameters to split the image into multiple grids, as can be seen in the following image.

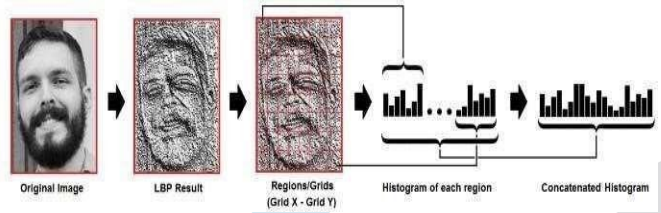
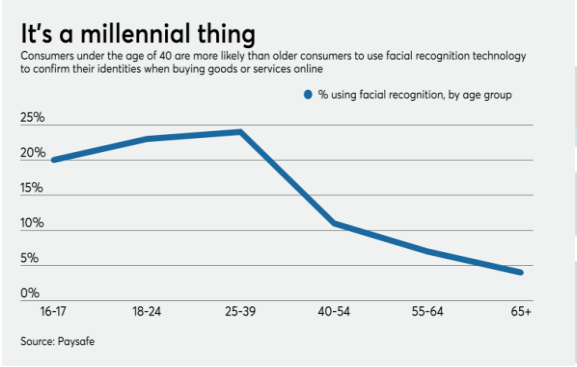


Figure 4.4 Obtaining Histogram

So Find an image similar to the input image and just need to compare the two histograms and replace the image with the nearest histogram. We can use a variety of methods to compare histograms (calculate the distance between two histograms), for example, Euclidean distance, square-chi, total value, etc..

V. EXPERIMENTAL RESULTS

1. In our project, we explain three different cases of how our project will work will be explained in a better way, Our project is designed using Tkinter-python for UI.
2. If the login credentials match then it shows a pop-up message saying successfully enrolled. Then enrollment page will open.
3. This page will capture the face of the user and store it in the database. It captures 5 images of the customer to get the trained image
4. The next step will display the withdraw page.



5. When the customer clicks on the withdraw button he will go into this page to verify the face. The customer has to click on the Verify Face Id button and the system captures the image and then tries to match with the stored images in the database. If it matches it will show the message as "Match-Id is verified". The below figure will show that the message popup is displayed.
6. On the next page, it will ask for an account password as two-factor verification. If the customer gives the password correctly then it will go to the next page. The account password page will look like below:
7. On the next page, it will display the box containing 4 options. To withdraw, to deposit, to sent amount to another account.
8. We can see that the balance inquiry button, when the customer clicks on this button he can see the balance in his account. In the same way, the customer can also select the withdraw button to withdraw the amount of money.

VI. Conclusion and Future Work

The purpose of Our proposed project on credit card authentication using face recognition is to reduce credit card frauds that may occur during an online payment process. It should be flexible so that people can easily use it without any hesitation. The webcam plays an important role in the system. It is reliable and user-friendly. Using this technique solves the issues by integrating face Recognition, this system
cannot still identify people with a similar face. his problem is overcome by using OTP. The comparison of the real-time image with the images stored in the database would be reliable. This system should not be made wait a long time for a user.

The proposed system gives a method for online transaction security using facial recognition. The system can be developed to automate the process. Some future enhancements for the proposed system can be:

1. Improving the system for banking transactions.

2. To add some more features to make the transaction secure.
3. More efficient Object Detection Neural network.
4. To implement the system in a banking and online transaction section web is mot more convenient so develop the app for this application.

Acknowledgements

It gives us great pleasure in presenting the preliminary paper “Authentication of Credit Card using Facial Recognition”. We would like to take the great opportunity to thank our internal guide Mr. Santhosh Kumar for giving us all the help and guidance we needed. We are really grateful to him for their kind support. His valuable suggestions are very helpful. We are also grateful to Dr. Suresh L, Head of Information Science Department, RNS Institute of Technology, Bangalore for his indispensable support for encouraging us to write this paper.

References

[1] Credit Card Fraud Detection Using Computer Vision and Its Performance. Authors: - Abhinav Srivast/ava, Amlan Kundu, Shamik Sural, Arun Majumdar.
[2] Convolutional Neural Network Approach for Vision-Based Student Recognition System.Authors: Nusrat Mubin Ara, Md. Saiful Islam
[3] Fast and Efficient Implementation of Convolutional Neural Networks Authors: Abhinav Podili, Chi Zhang, Viktor Prasanna. Elissa, "Title of paper if known," unpublished.
[4] R.S. Choras, “Facial feature detection for face authentication," in the Proceeding of IEEE Conference on Cybernetics and Intelligent Systems., 2013.
[5] Facial Expression Recognition via Deep Learning. Authors: Abir Fathalla, Gary Thung, Ali Douai.
[6] Farhadi, A., Hejrati, M., Sadeghi, M.A., Young, P., Rashtchian, C., Hockenmaier, J., Forsyth, D.: Every picture tells a story: Generating sentences from images. In: Computer Vision{ECCV 2010. Springer (2010)
[7] Berg, A.C., Berg, T.L., Daume III, H., Dodge, J., Goyal, A., Han, X., Mensch, A., Mitchell, M., Sood, A., Stratos, K., et al.: Understanding and predicting importance in images. In: Computer Vision and Pattern Recognition (CVPR), 2012 IEEE Conference on, IEEE (2012) 3562–3569.
[8] A Survey on Hidden Markov Model for Credit Card Fraud Detection. Author Name: - Anshul Singh, Devesh Narayan.
[9] Enhanced security for ATMs with OTP and Facial recognition features. Mohsin Karovaliya a , Saifali Karediab , Sharad Ozac , Dr.D.R.Kalbande

AUTHORS PROFILE

Mr. Amit Kumar Sah, currently a final year student, Dept. of ISE RNSIT College, Bangalore , Karnataka, India.

Mr. Koneti Hemanth Raju, currently a final year student, Dept. of ISE RNSIT College , Bangalore, Karnataka ,India.

Mr.Manish S Prasad, currently a final year student, Dept. of ISE RNSIT college, Bangalore, Karnataka, India.

Mr.Santosh Kumar, currently working as Assistant Professor, Dept. of Information Science RNSIT, Bangalore, Karnataka, India.