

Credit Card Validation and Face Verification

Prof. Mahendra Shinde¹, Omkar Garudkar², Sarthak Gond³, Kunal Patil⁴, Nikhil Ghule⁵

¹Professor, Dept of Computer Engineering, MIT (Maharashtra Institute of Technology) polytechnic, Pune, Maharashtra, India

^{2,3,4,5}Diploma in Computer Engineering, Dept of Computer Engineering, MIT (Maharashtra Institute of Technology) polytechnic, Pune, Maharashtra, India

Abstract - The number of personnel using online transactions methods has made tremendous growth over the last few years so we need a safe place to complete the same. We suggest using biometric authentication to verify and validate online transactions. Cutting a multi-step process into a one-step process, therefore, saves consumer time. Simplify the function of manually entering the details of the card intended for OCR to enable devices to detect visual signals using a webcam. Device users are ordinary people who are often frustrated with online interactions due to the extra time taken out. The current authorization system includes OTP that is prone to hard retrieval. We also created a type of blank bone in python that will mimic the system billing process and mimic the OTP system billing process. We used that to test whether people liked this new way of verifying payments and getting a user feedback on how to improve the project. We propose a project that can make payments that run online without unnecessary obstacles. Credit card companies have no security other than OTP (one-time-password) and CVV. if this program does its job without any problem, credit card and debit card companies can use this program to reduce the fraud of online transactions.

Keywords - Credit card, Face recognize, webcam, transaction, face verification, fingerprint authentication, Rapid API (Lambda face recognition and face detection), Google Cloud Vision API.

1. INTRODUCTION:

While using e-commerce sites we all face some issues regarding OTP production (One time Password), the most common of all, outdated OTP, previous OTP generation, OTP theft, and more.

Due to the growing number of credit card/debit card holders and the simplicity of online transactions, there are a large number of users who prefer online transactions. Also, banks play an important role to ensure transactions and customers can withdraw money according to their needs. This also enhances the 'Digital India' motto.

Although credit/debit card companies offer CVV security and Banks offer OTP security, there is still a lot of potential for fraud to occur at large prices. Therefore this may create a situation that creates insecurity while performing online transactions.

So, we have developed a system that tries to end this situation. We used a two-way authentication model

That uses fingerprint authentication and facial verification using a single learning network and a siamese network.

2. LITERATURE REVIEW:

There are many systems that have been developed in engineering colleges by students for doing online transactions. The developed systems are fine but there is a lack of security.

The existing systems are:

- i) Multimodal Biometric System in Secure e-Transaction in Smart Phone.
- ii) Survey on Online Transaction using Face Recognition.
- iii) Two-way Credit Card Authentication with Face Recognition Using Webcam.

i) Multimodal Biometric System in Secure e-Transaction in Smart Phone:

In this multimodal biometric system they are using two type of biometric like face recognition and voice recognition. They are using credit/debit cards for e-transaction on e-commerce site. During the e-transaction they used smart phones and give the features of smart phone where they save transaction.

The voice recognition system is useful system but there are drawbacks like Background Noise Interference and Lack of Accuracy and Misinterpretation.

ii) Survey on Online Transaction using Face Recognition:

In this existing system, they use a well-known biometric surface. They used an LBPH algorithm that uses cryptography to scan users' faces.

In this system, there are some drawbacks like those of the system that require high costs. And at the end of the transaction OTP is provided so these programs can create a room for online transaction fraud.

iii) Two-way Credit Card Authentication With Face Recognition Using Webcam:

The program uses two methods to verify online transactions using OpenCV and LBP algorithm. By gaining facial recognition. This face recognition system is good but there is a flaw in the system provided by OTP after successful OTP verification then goes to deal with the facial recognition system. So this OTP security still has a lot of potential for fraud.

3. PROPOSED MODEL:

We propose a system that uses facial recognition and fingerprint authentication to assure the user of safe and effective transactions.

In today's fast-paced world where the need for competent technology in a competitive market is growing. We aim to develop a system that overcomes minor hardware shortcomings with good software. Literacy in India is low so internet users are low but with the use of fingerprint recognition and OCR (Optical Character recognition), the volume of illiterate users will increase as this system will increase usability. Security is a major concern due to the high level of cell phone theft which is why the current OTP system (One Time Password) leaves room for improvement. Reversible software is compatible with low-resolution cameras.

We used python language for programming and we used Django (Web-Framework) to design and improve our E-commerce site. We used OCR (Optical Character Recognition) to obtain credit/debit card details and auto-complete them accordingly. We used the Lambda API for face detection.

1) Optical Character Recognition:

Credit card/debit card identification using Tesseract OCR where we take a picture of our credit/debit card in front of the webcam automatically scans the credit/debit card and completes all required details such as the cardholder's name, card number, and expiration date.

2) Face Detection:

We used a webcam to find the users you are dealing with. With the help of lambda API and Google cloud view for better face recognition and discovery The Lambda API is usable and easy to use, the lambda API is mainly used to test all types of photos and videos, such as face detection and recognition.

3) Face recognition:

We are using lambda API because lambda API is free to use and gives proper and accurate face recognition. Users

can easily register. It has proven to provide powerful feature extraction API. It's fixable to use.

4) Liveness Detection:

Liveness Detection is a very useful tool that helps to determine whether the acquired face is real or fake. This module is very important for recognition systems as these can be manipulated by using a valid user image and authorizing access to fraudulent users. Since our standard cameras have no depth view they cannot distinguish between a 3D photo of a live face and a 2D face photo.

4. SYSYTEM ARCHITECTURE:

In modern life, credit/debit cards are used all over the world. These days people also choose to use a credit/debit card to do a large number of online transactions. But that leaves some bad things as one of the most common scams. According to a very recent survey, India ranks third in the world, with India being the most targeted country in the world. There are about 2500 online fraud scams registered in the last two years in India. Traditional credit/debit card security is CVV and OTP (One Time Password) authentication. But this protection is built using fingerprint authentication and face recognition. In the proposed program we used the Lambda API, an algorithm for face detection and face recognition. The user must place a credit/debit card in front of the camera and the required information is automatically filled in the form. In card verification, we use the google cloud vision API, then fingerprint authentication is required after facial recognition of authorized users, the webcam will turn on face scanning for users to verify faces, and the user's name and the image will be stored on the database server.

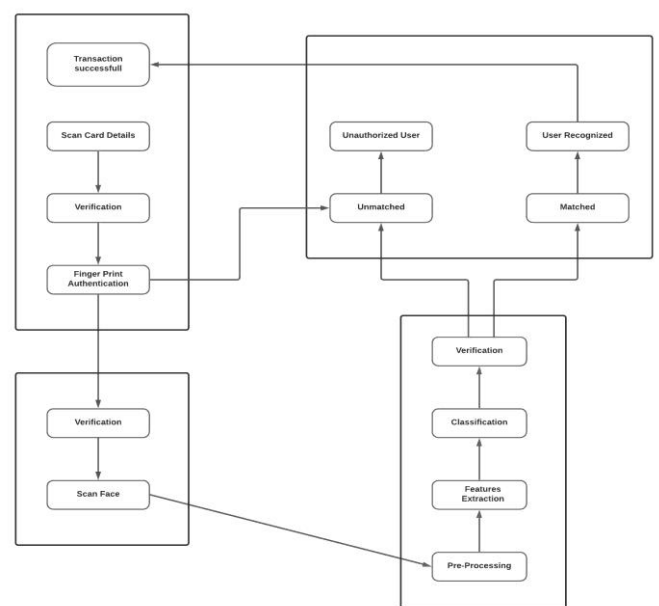
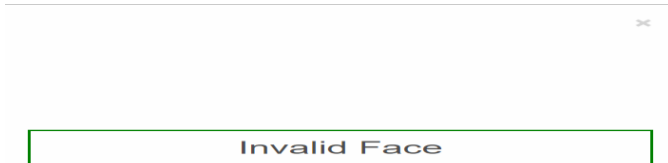


Fig 2 Architecture Diagram for application.



H. This is a screenshot where the program gives a warning as "Invalid Face" due to the fact that the face which was scanned is either fake or unauthorized.



I. This is the screenshot where the face get scanned and Recognized using webcam and using Rapid API (Lambda Face Detection and Face recognition Algorithm).



J. This is the screenshot where the users face detected and recognized successfully



K. The transaction get completed.



6. CONCLUSIONS:

We have developed a security model for credit card verification and face verification using webcam and fingerprint authentication to provide high security that helps reduce online transaction fraud. The proposed system is integrated with a two-way security module, fingerprint verification, and facial recognition that can only be accessed by an authorized user to protect users from online transactions. This program will help to promote online transactions.

7. REFERENCES:

- [1] Amit Kumar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (6), 2015, 5080-5084 "Multimodal Biometric System in Secure e-Transaction in Smart Phone" <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.736.5642&rep=rep1&type=pdf>
- [2] International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified Vol. 6, Issue 2, February 2017, Namita Jain, Vikrant Mukkawar, Mahesh Jadhav, Prof. Shruti Sekra. "Survey on Online Transaction using Face Recognition" <https://ijarcce.com/upload/2017/february-17/IJARCCCE%2039.pdf>

- [3] International Journal of Engineering Trends and Technology (IJETT) – Volume 67 Issue 5- May 2019
Asma Shaikh, Aditi Mhadgut, Apurva Prasad, Bhagyashree Shinde, Rohan Pandita. “Two-way Credit Card Authentication with Face recognition using webcam” <https://ijettjournal.org/Volume-67/Issue-5/IJETT-V67I5P227.pdf>