Chapter- 1

Introduction

**Chapter-1**

**Introduction**

* 1. **Overview**

Artificial intelligence and Machine Learning have gained increasing popularity in recent years due to their ability to handle tasks that would otherwise take too much computational power, and due to their versatility, the wide range of problems they have been shown to solve. One of the most well known ask that machine learning has made possible is face recognition. Face recognition technology has been used for a variety of applications including automatic tagging in Facebook photos, Snapchat lenses that overlay dog ears on someone’s head, and security and surveillance, with the more recent capacity to track individuals moving throughout a closed space as they cross in front of security cameras.

Facial recognition systems rely on unique facial features as and additional layer of security to identify and distinguish people whether they’re new faces or old ones in database.We set out to apply this technique to the field of internet security, along with Captchas, I m not a robot check boxes, security questions, two factor authentication, and many others. Facial recognition has the potential to be a much simpler approach to security than remembering additional security in formation or connecting other accounts and devices.

* 1. **Problem Statement**

However, there’s an obvious issue with using facial recognition to login to your account. Anyone with you picture can login to it too. Furthermore, if any one hacks the site, then you may gain access the database of face data and be able to relate user accounts to actual faces, then do some reverse processing to label those faces with real names rather than whatever alias may have been their username. And is facial recognition even accurate enough to avoid false positives and log someone into the wrong account? Can someone just sit in front of a camera long enough to get sneak past a sitessecurity?

Apple has provided a solution to solve this photo trick by relying on dual cameras and an array of projected infrared dots to detect depth in its new facial recognition system. However, such a solution is limited to devices with expensive hardware upgrades and can’t be applied to lower cost applications. Higher costs often limit to the improvements, complicate manufacturing, and raise the price for consumers.

* 1. **Objectives**
* To Study the various face detection techniques.
* To design an efficient face detection algorithm.
* To implement designed algorithm using OpenCV.
* To test the implemented algorithm in various conditions with sufficient number of datasets.
  1. **Scope**

To address the issues of impersonation, we propose a system that would use a video stream, rather than a still image, to check that the correct person is logging in. if our facial recognition detects a video frame without the correct matching face, the login step will fail. However, such a system could be spoofed by simply holding a video up to the camera, so we will also ask the user to perform some random gesture to ensure it’s a real person in front of the camera. Our solution is pure software-based, requiring no additional hardware expenses, and can be applied to a wide range of applications including building security, unlocking cell phones ,and website logins. The reliability and ease of use of our system will be reliant on the accuracy of the facial recognition and the set of facial gestures available to use.

Chapter- 2

Literature Survey

**Chapter-2**

**Literature Survey**

**2.1 Literature Study**

The task of face recognition has been actively researched in recent years. This paper provides an up-to-date review of major human face recognition research. We first present an overview of face recognition and its applications. Then, a literature review of the most recent face recognition techniques is presented. Description and limitations of face databases which are used to test the performance of these face recognition algorithms are given. A brief summary of the face recognition vendor test (FRVT) 2002, a large scale evaluation of automatic face recognition technology, and its conclusions are also given. Finally, we give a summary of the research results.

A formal method of classifying faces was first proposed in a formal method. The author proposed collecting facial profiles as curves, finding their norm, and then classifying other profiles by their deviations from the norm. This classification is multi-modal, i.e. resulting in a vector of independent measures that could be compared with other vectors in a database. Progress has advanced to the point that face recognition systems are being demonstrated in real-world settings. The rapid development of face recognition is due to a combination of factors: active development of algorithms, the availability of a large databases of facial images, and a method for evaluating the performance of face recognition algorithms. In the literatures, face recognition problem can be formulated as: given static (still) or video images of a scene, identify or verify one or more persons in the scene by comparing with faces stored in a database.

* 1. **Data Mining**

**2.2.1 Eigenface**

Eigenface is one of the most thoroughly investigated approaches to face recognition. It is also known as Karhunen- Loève expansion, eigen picture, eigenvector, and principal component. References used principal component analysis to efficiently represent pictures of faces. They argued that any face images could be approximately reconstructed by a small collection of weights for each face and a standard face picture (eigenpicture). The weights describing each face are obtained by projecting the face image onto the eigen picture. Reference used eigenfaces, which was motivated by the technique of Kirby and Sirovich, for face detection and identification.

**2.2.2 Neural Networks**

The attractiveness of using neural networks could be due to its non linearity in the network. Hence, the feature extraction step may be more efficient than the linear Karhunen-Loèvemethods. One of the first artificial neural networks (ANN) techniques used for face recognition is a single layer adaptive network called WISARD which contains a separate network for each stored individual .

**2.2.3 Graph Matching**

Graph matching is another approach to face recognition. Reference presented a dynamic link structure for distortion invariant object recognition which employed elastic graph matching to find the closest stored graph. Dynamic link architecture is an extension to classical artificial neural networks. Memorized objects are represented by sparse graphs, whose vertices are labelled with a multiresolutiondescription in terms of a local power spectrum and whose edges are labelled with geometrical distance vectors.

**2.2.4 Hidden Markov Models (HMMs)**

Stochastic modelling of nonstationary vector time series based on (HMM) has been very successful for speech applications. Reference applied this method to human face recognition. Faces were intuitively divided into regions such as the eyes, nose, mouth, etc., which can be associated with the states of a hidden Markov model. Since HMMs require a one-dimensional observation sequence and images are two-dimensional, the images should be converted into either 1D temporal sequences or 1D spatial sequences.

**2.2.5 Geometrical Feature Matching**

Geometrical feature matching techniques are based on the computation of a set of geometrical features from the picture of a face. The fact that face recognition is possible even at coarse resolution as low as 8x6 pixels when the single facial features are hardly revealed in detail, implies that the overall geometrical configuration of the face features is sufficient for recognition. The overall configuration can be described by a vector representing the position and size of the main facial features, such as eyes and eyebrows, nose, mouth, and the shape of face outline.

Chapter- 3

Problem Identification and Problem Solution

**Chapter-3**

**Problem Identification and Problem Solution**

**3.1 Problem Identification**

There are two main obstacles encountered when we were doing our design. First is the delayed schedule due to heavy course load. Since in the winter quarter, all of our team members were very busy, we spent not much time on the project. But later we caught up the progress during holidays and other quarters. The second obstacle is frame rate limitation. Since the camera we use cannot detect fast motions due to video frame processing rate and CPU limitation, some fast facial motions are hard to be detected, so we had to perform the gesture slowly which takes more time or increase video frame processing rate if we had a better device.

**3.2 Proposed Solution**

The solution for the two obstacles stated above are: for the delay because of the rainy quarter we worked extra hours and late nights for the completion of the project .the second solution i.e for the frame rate limitation we increases the video frame rate if possible and if not we would perform the gesture slowly .

Chapter- 4

Implementation

**Chapter-4**

**Implementation**

* 1. **Requirements**
     1. **Functional Requirements**

The functional requirements of our project describe features our system must have to be successful. Users need to be able to create accounts and store their facial data for the site to identify them later. The site needs to be able to identify users with facial recognition, which requires some form of video camera. The site must be able to stop impersonation, distinguishing between real people and fake copies. And finally, the site needs to be able to recognize faces and gestures to log users into the correct accounts.

**4.1.2 Non-functional Requirements**

The non-functional requirements describe features that improve the sites performance, or would otherwise benefit the system. A secure API for storing and using face data to identify users andlearn new faces would be ideal to avoid the risk of losing identifiable information in the event of a site hack. Since we imagine nobody wants to sit in front of a camera for minutes on end trying to access an account, the site should be able to identify users quickly, and provide a quick login experience. Since Software programs often require continuous debugging efforts as new features are added and new issues are discovered, the source code should be clear and easy to follow, relying on software tools to simplify the implementation.

## 4.2 Use Cases

The use case represents the list of actions and event steps which define the interactions among users, websites, and the API.

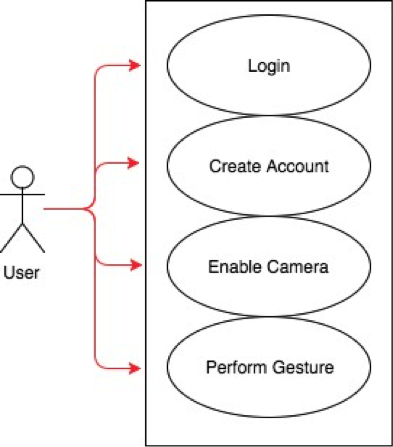


Figure 4.1: Use case diagram of the user

**4.3 Activity Diagram**

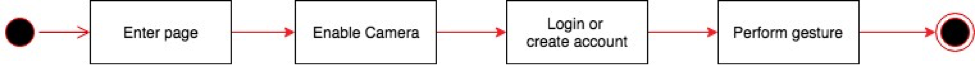


Figure 4.2: High level view of user operations

As a user, after he/she enters the index page of the website, he/she may attempt to log into by enabling the camera or create an account. The user needs to wait for the system response after the system finishes recording. After that, the user should perform given gestures from the server.

**4.4 Architecture Diagram**

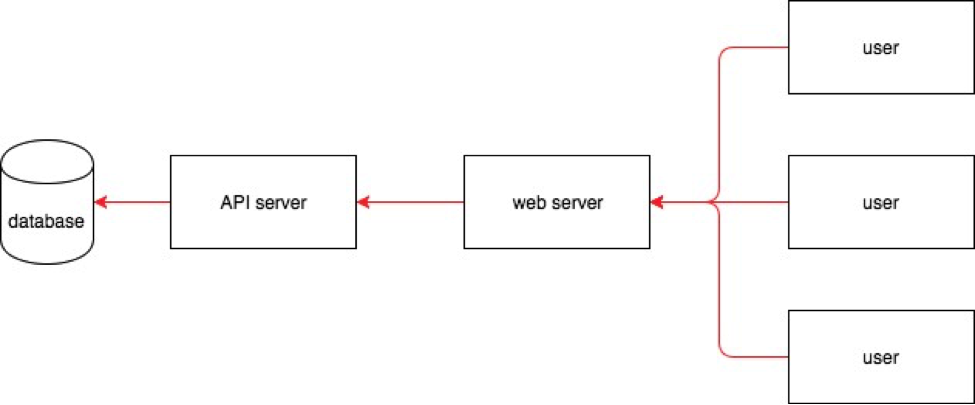


Figure 4.3: Architecture diagram of the system

Since all data will be stored in our database, Wedecide to build an advanced data-centric architecture for our design to make the data more accessible and manageable for users. In addition, considering security and management of APIs, we choose to have a three-tier architecture because if the protect data security and improve manageability of different APIs. In our design, users post requests to the web server and the server will call different APIs depending on the requests from users. Multiple users can login to the system at same time from different places.

Chapter – 5

Result Analysis

**Chapter-5**

**Result Analysis**

**5.1 Testing and Performance Evaluation**

### 5.1.1 White Box

For the white box testing, we tested each portion of the code to ensure that they function as intended. We designed a series of varied test cases to use on the system to verify that all of the constraints are met in any situation. The test cases asserted the system’s ability to maintain its functions in standard use situations, as well as potential edge cases.

* + - * **Login and Registration**

We tested regular login and registration function. We first tested to register with a conflict username, and the system showed a warning. We then login with username and incorrect password, and the system also provided awarning.

* + - * **Facial Detection and Recognition**

We tested our facial detection and recognition part using different faces. The system was able to detect all faces appeared on the screen and successfully authenticated the correct user.

* + - * **Gesture Recognition**

We tested gesture recognition by performing requested gestures assigned by the system. The system successfully recognized the gestures.

* + - * **Image Impersonation**

The last test was to test image impersonation. Face recognition test can be passed byusing photos if the camera is not good enough to detect image depth. Our design solves this problem because it requires the person to perform gestures. We tested that although a different person holding the picture can pass the face recognition part, the gesture testing cannot be passed.

### 

### 5.1.2 Black Box

Black box testing enlists the help of individuals not involved with the development of our application, which include classmates and friends. They understand what the system is designed to do, but not how it is done. The testers then used the system to sign up and login, as if they are real users of the system.

Chapter- 6

Conclusion and Future Scope

**Chapter-6**

**Conclusion and Future Scope**

## 6.1 Conclusion

Since the face recognition algorithmwe use is more than 99% accurate, the site only needs to compare the user’s face to one stored image, rather than against a million different faces like Face- book, and our implementation checks the user’s identity over several frames, we believe that face recognition is a secure, reliable, and simple method of authentication. in the future, there may not even be need for passwords or even captcha checks to stop bots.

if we separated the database of face information from the site’s data and trained our own neural network, our implementation would be much more secure. just like signing in with your Google account doesn’t give your password away to the whatever site, logging in with your face shouldn’t give any site access to the associated data either.lastly, if we improved the set of gestures our site can detect, we could speed up the process substantially compared to only detecting blinks. Making the authentication process quick and seamless requires making the gestures simple and unobtrusive, which we have found to be the largest hurdle we would need to solve for our design to be competitive.

## Future Scope

**6.2.1 Recognize more gestures**

We plan to add more gestures into our system such as waving hands and opening mouth. The increasing number of random gestures will make the user harder to predict the move, and thus improve the security of the system..

**6.2.2 Test with more people and a larger image set**

We plan to test with more people and get a more precise result of how accurate our system is on recognizing users’ faces and gestures. We will also improve the accuracy of the system by training and testing with a larger image set.

**6.2.3 Store and encrypt face data in a separate database**

The photos of the users in the database have a potential security issue. To solve that, we plan to store and encrypt the photos of the user in a separate database so that even if the database is being hacked, the photos will not leak.

* + 1. **Replace users photo with face encoding**

To bring the security of our system to the next level, we could only store the characteristics of the user’s face in the data base instead of the photo. Even if the face encoding data is leaked, the hacker cannot recover user’s face.

**6.2.5 Remove the need for password in our implementation**

When our system reaches really high accuracy, we could remove process of entering the password during login. User’s account can be verified with facial recognition as the single security check.

**RERERENCES**

[1] Zhang, Xiaozheng, and YongshengGao. "Face recognition across pose: A review" Pattern Recognition, vol 42, no. 11, pp. 2876-2896, 2009.

[2] Tolba, A. S., A. H. El-Baz, and A. A. El-Harby. "Face recognition: A literature review." International Journal of Signal Processing, vol 2, no. 2, pp. 88-103, 2006.

[3] Dantcheva, Antitza, PetrosElia, and Arun Ross. "What else does your biometric data reveal? A survey on soft biometrics." IEEE Transactions on Information Forensics and Security, vol 11, no. 3, pp. 441-467, 2016.

[4] Papakostas, George A. "Over 50 Years of Image Moments and Moment Invariants." Moments and Moment Invariants-Theory and Applications, pp. 3-32, 2014.

[5] Zafeiriou, Stefanos, Cha Zhang, and Zhengyou Zhang. "A survey on face detection in the wild: past, present and future." Computer Vision and Image Understanding, vol. 138 pp. 1-24, 2015.

[6] Jin, Jing, Bin Xu, Xiaoliang Liu, Yuanqing Wang, Liqun Cao, Lei Han, Biye Zhou, and Minggao Li. "A face detection and location method based on Feature Binding." Signal Processing: Image Communication, vol. 36, pp. 179-189, 2015.

[7] Hatem, Hiyam, ZouBeiji, and RaedMajeed. "A Survey of Feature Base Methods for Human Face Detection."International Journal of Control and Automation, vol. 8, no. 5, pp. 61-78, 2015.

[8] Rizvi, QaimMehdi, Bal Gopal Agarwal, and Rizwan Beg. "A Review on Face Detection Methods.", 2011.

[9] Yang, Ming-Hsuan, David J. Kriegman, and Narendra Ahuja. "Detecting

faces in images: A survey."IEEE Transactions on pattern analysis and machine intelligence, vol. 24, no. 1, pp. 34-58, 2002.

[10] Kouzani, Abbas Z., Fangpo He, and Karl Sammut. "Common sense knowledge-based facedetection."IEEE International Conference on Intelligent Engineering Systems ( INES'97), pp. 215-220, 1997.

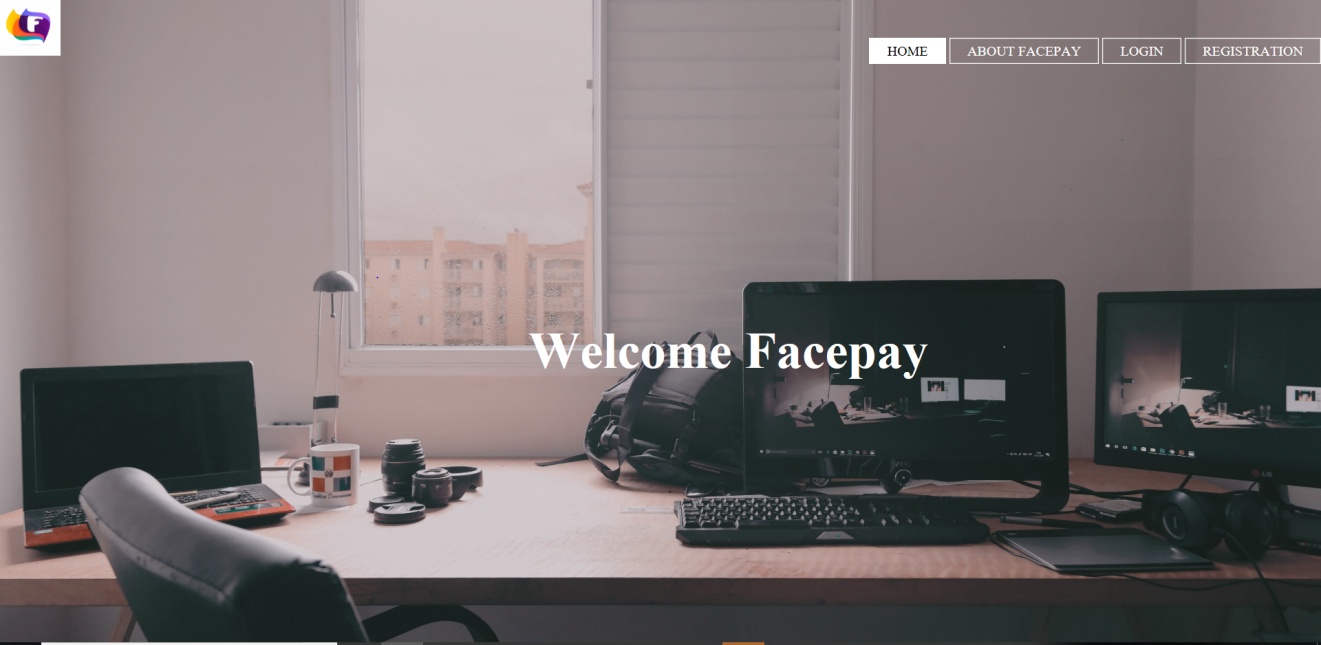
Appendix-A

Research Paper

Appendix-B

Screenshots

1. The main page -The Welcome page from where the user can navigate to Login page , Registration Page or About Us page.

Figure 1 :Main Page

**2.**The Registration Page- The user have to Fill his details like name , contact number, Email for registration.(User has 2 options for Password i.e Email and face Detection ).

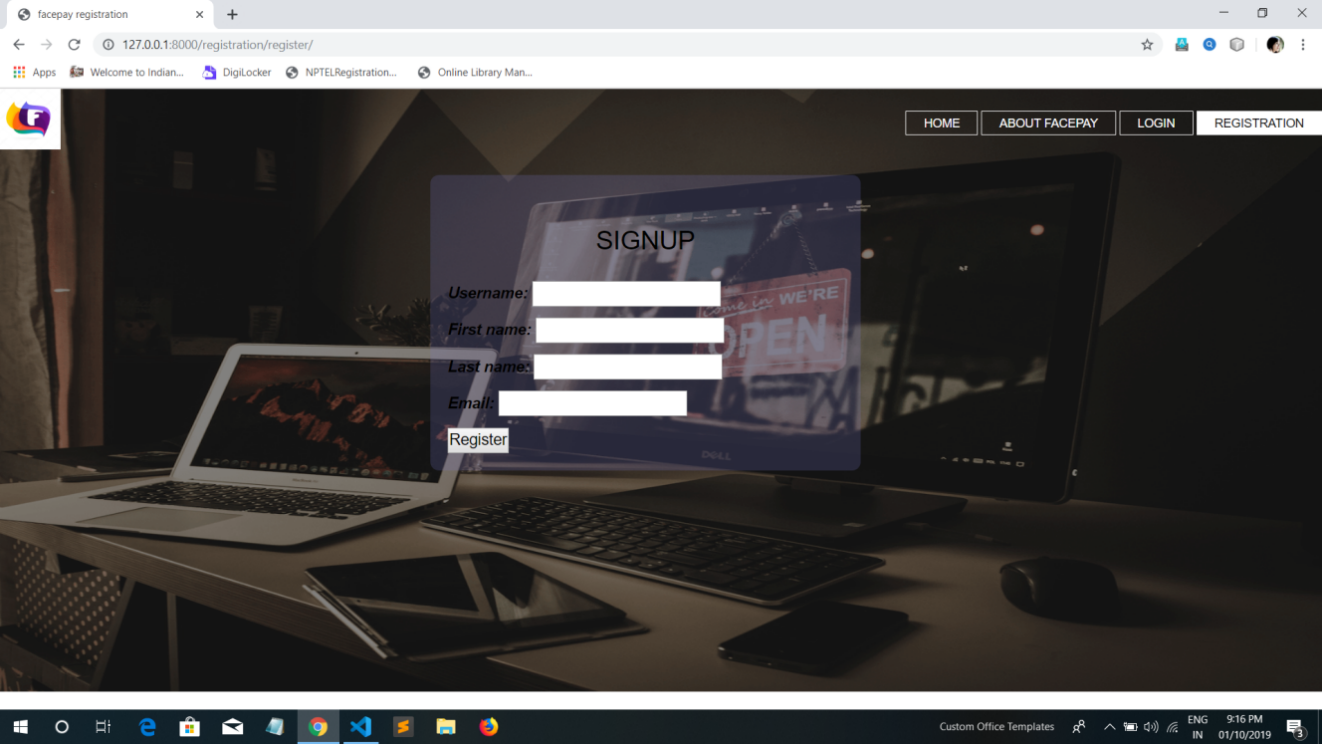


Figure 2 :Registration Page

**3.**Login Page- Login requires the user’s email and password.

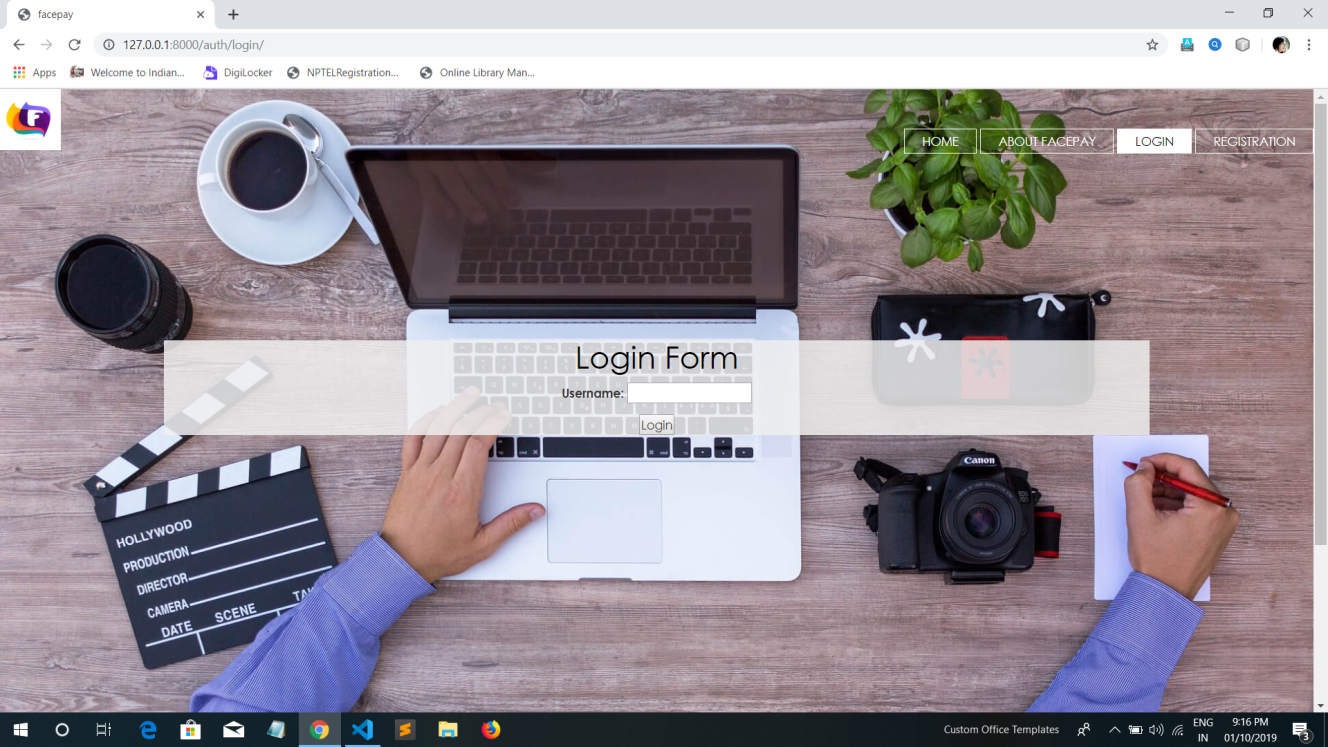


Figure 3 : Login Page

1. About Facepay Page- It is A short description of the Facepay.



Figure 4 : About Facepay page 1

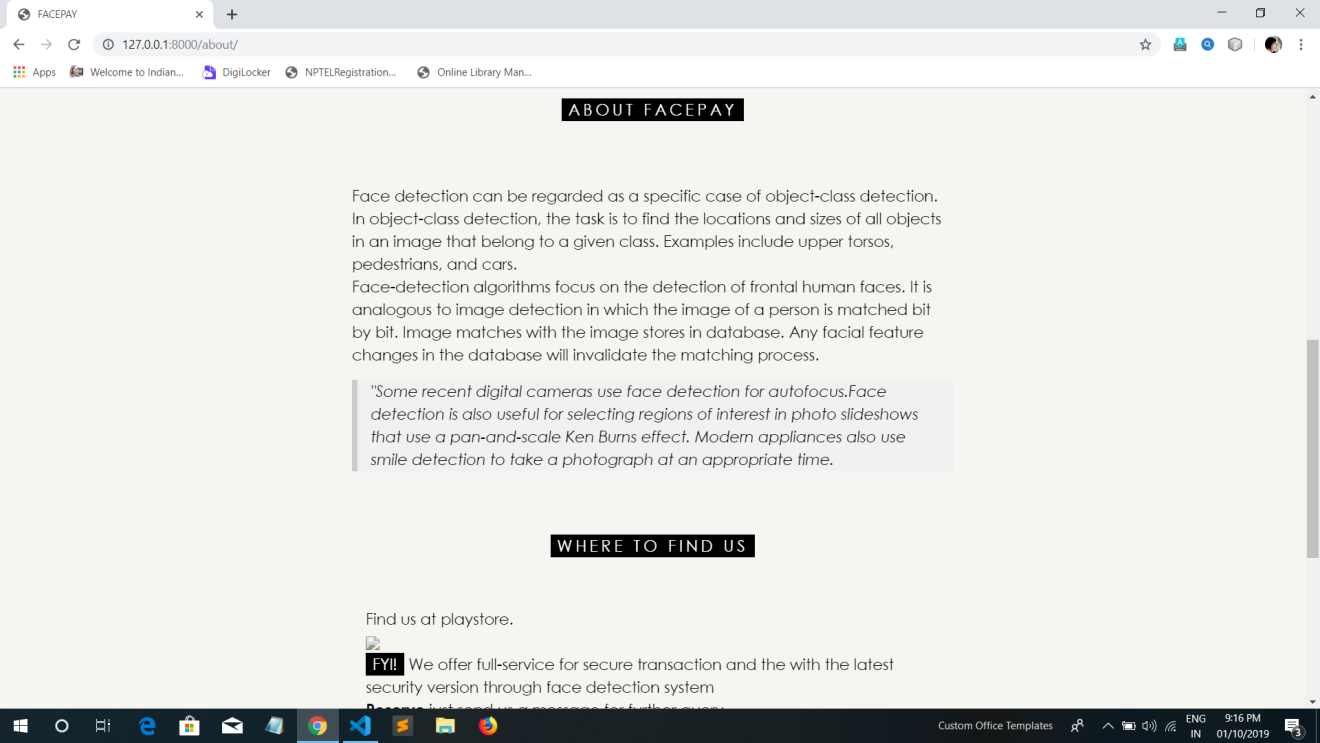


Figure 5 :About Facepay page 2

1. Transaction Page – This page is made for future uses the implementation and execution will be done in future.

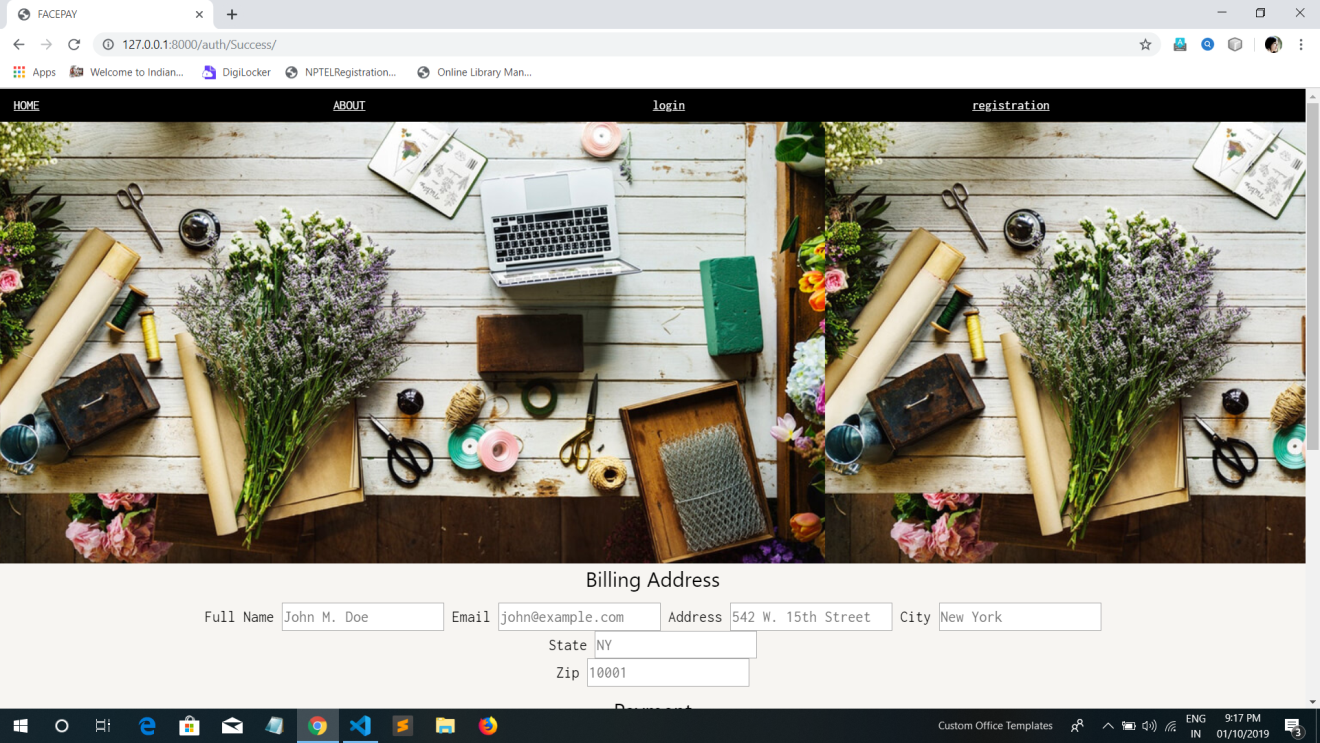


Figure 6 : Transaction page 1

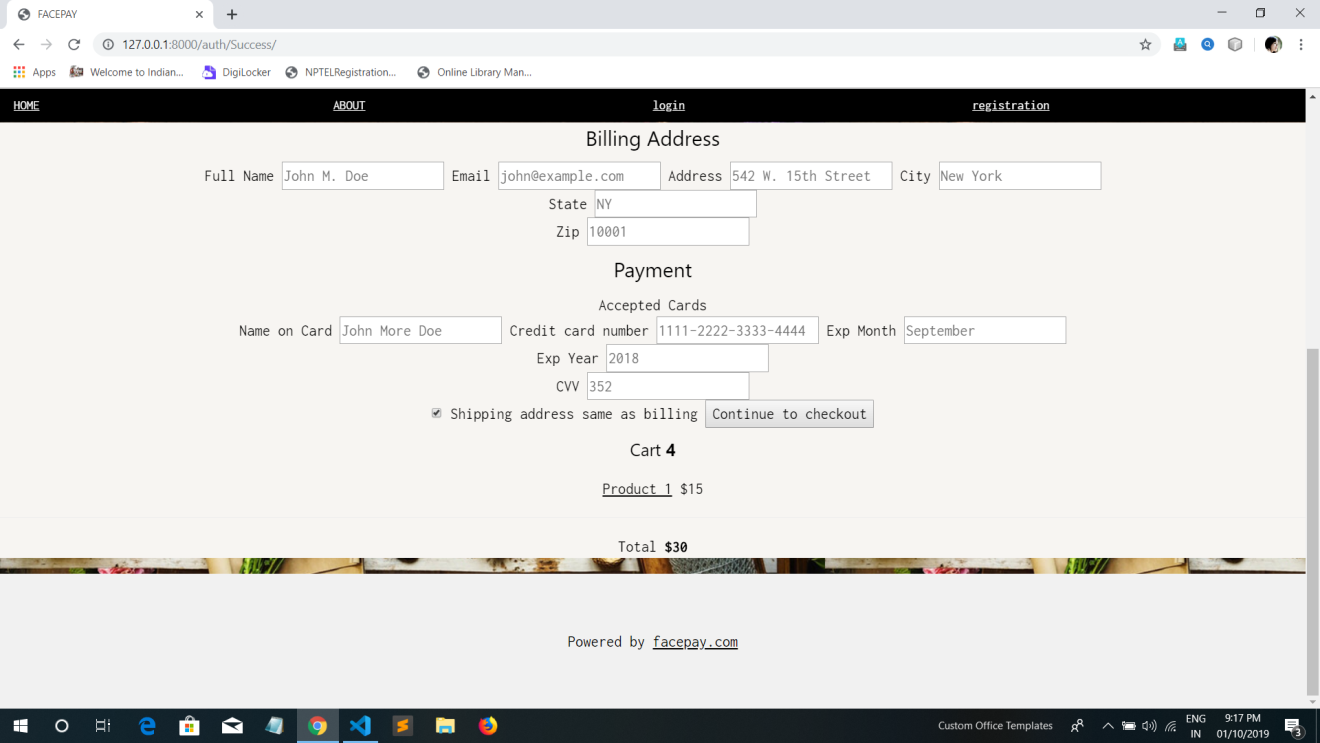


Figure 7 : Transaction Page 2

1. Face Detection Process – The user’s face is being detected by the webcam

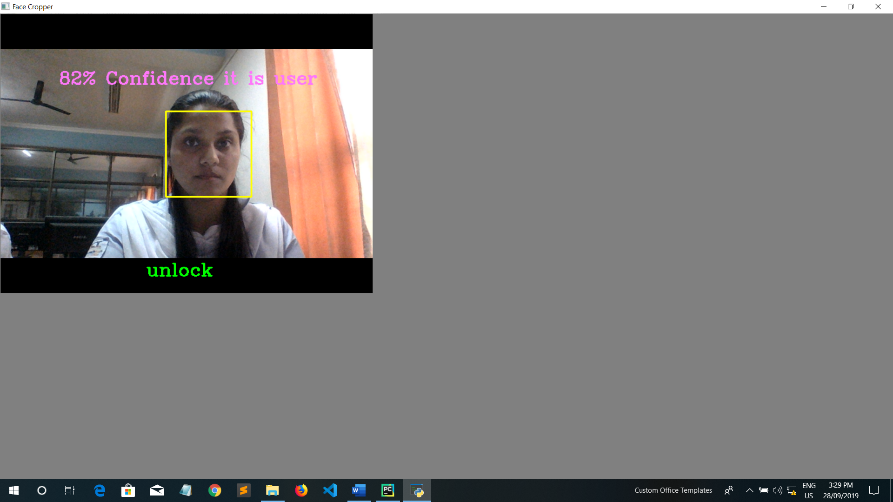


Figure 8 : Face Detection Process



Figure 9 : Face Detection Conceptual Model