USER-IDENTIFICATION IN BROWSER APPLICATIONS USING FACE RECOGNITION

A PROJECT REPORT

Submitted by

ABIL VARKICHAN JOSE (VJC15CS005)
AJIN KUMAR P A (VJC15CS009)
ANTONY DADU (VJC15CS022)
BRYANE SUNNY KANIYADAN (VJC15CS039)

to

the APJ Abdul Kalam Technological University
in partial fulfillment for the award of the degree

of

Bachelor Of Technology

In

Computer Science and Engineering

Department of Computer Science and Engineering

Viswajyothi College of Engineering and Technology

Vazhakulam

MAY 2019

USER-IDENTIFICATION IN BROWSER APPLICATIONS USING FACE RECOGNITION

A PROJECT REPORT

Submitted by

ABIL VARKICHAN JOSE (VJC15CS005)
AJIN KUMAR P A (VJC15CS009)
ANTONY DADU (VJC15CS022)
BRYANE SUNNY KANIYADAN (VJC15CS039)

to

the APJ Abdul Kalam Technological University
in partial fulfillment for the award of the degree

of

Bachelor Of Technology

In

Computer Science and Engineering

under the guidance

of

Mr. Andrews Jose
Assistant Professor, CSE Dept.

Department of Computer Science and Engineering

Viswajyothi College of Engineering and Technology

Vazhakulam

MAY 2019

DECLARATION

We undersigned hereby declare that the project report "User-Identification in Browser Aplications Using Face Recognition", submitted for partial fulfillment of the requirements for the award of the Degree of Bachelor of Technology of the APJ Abdul Kalam University is a bonafide work done by us under the supervision of Mr.Andrews Jose. This submission represents any ideas in our own words and where ideas or words of others have been included, we have adequately and accurately cited and referenced the original sources. We also declare that we have adhered to ethics of academic honesty and integrity and have not misrepresented or fabricated any data or idea or fact or source in our submission. We understand that any violation of the above will be a cause for disciplinary action by the institute and/or the University and can also evoke penal action from the sources which have thus not been properly cited or formed the basis for the award of any degree, diploma or similar title of any other University.

Place: **Vazhakulam**
Date:

ABIL VARKICHAN JOSE

AJIN KUMAR

ANTONY DADU

BRYANE SUNNY KANIYADAN

VISWAJYOTHI COLLEGE OF ENGINEERING AND TECHNOLOGY, VAZHAKULAM

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that the project report entitled **"USER-IDENTIFICATION IN BROWSER APPLICATIONS USING FACE RECOGNITION"** submitted by **ABIL VARKICHAN JOSE (VJC15CS005), AJIN KUMAR P A (VJC15CS009), ANTONY DADU (VJC15CS022), BRYANE SUNNY KANIYADAN (VJC15CS039)** to the APJ Abdul Kalam University in partial fulfilment of the requirements for the award of the **Degree of Bachelor of Technology** in **Computer Science and Engineering** is a bonafide record of the project carried out by them under the guidance of supervision. This report in any form has not been submitted to any other University or Institute for any purpose.

Internal Supervisor **External Supervisor**

Project Coordinator **Head of the Department**

VISWAJYOTHI COLLEGE OF ENGINEERING AND TECHNOLOGY, VAZHAKULAM.

Department of Computer Science and Engineering

Vision

Moulding socially responsible and professionally competent Computer Engineers to adapt to the dynamic technological landscape

Mission

1. Foster the principles and practices of computer science to empower life-long learning and build careers in software and hardware development.
2. Impart value education to elevate students to be successful, ethical and effective problem-solvers to serve the needs of the industry, government, society and the scientific community.
3. Promote industry interaction to pursue new technologies in Computer Science and provide excellent infrastructure to engage faculty and students in scholarly research activities.

Program Educational Objectives

Our Graduates

1. Shall have creative aid critical reasoning skills to solve technical problems ethically and responsibly to serve the society.
2. Shall have competency to collaborate as a team member and team leader to address social, technical and engineering challenges.
3. Shall have ability to contribute to the development of the next generation of information technology either through innovative research or through practice in a corporate setting
4. Shall have potential to build start-up companies with the foundations, knowledge and experience they acquired from undergraduate education

Program Outcomes

1. **Engineering knowledge**: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
2. **Problem analysis**: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences

3. **Design / development of solutions**: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

4. **Conduct investigations of complex problems**: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

5. **Modern tool usage**: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations.

6. **The engineer and society:** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

7. **Environment and sustainability:** Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

8. **Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice

9. **Individual and team work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings

10. **Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

11. **Project management and finance**: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and unread in a team, to manage projects and in multidisciplinary environments.

12. **Life-long learning**: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

Program Specific outcomes

1. Ability to integrate theory and practice to construct software systems of varying complexity
2. Able to Apply Computer Science skills, tools and mathematical techniques to analyse, design and model complex systems
3. Ability to design and manage small-scale projects to develop a career in a related industry.

ACKNOWLEDGMENT

First and foremost, I thank God Almighty for his divine grace and blessings in making all these possible. May he continue to lead me in the years. It is my privilege to render my heartfelt thanks and gratitude to our most beloved manager, **Msgr.Dr.Cherian Kanjirakompil** and our Principal **Dr.Josephkunju Paul C** for providing me the opportunity to do this project during the forth year (2018) of my B.Tech degree course. I am deeply thankful for our Head of the Department, **Mr.Amel Austine** for his support encouragement. I would like to express my sincere gratitude to my project guide **Mr.Andrews Jose**, Asst.Professor, Department of Computer Science and Engineering for her motivation, assistance and help for the project. I also express sincere thanks to the project coordinator **Mr.Joe Mathew Jacob**, Asst.Professor, Department of Computer Science and Engineering for his guidance and support. I also thank all the staff members of the Computer Science Department for providing their assistance and support. Last, but not the least, I thank all my friends and family for their valuable feedback from time to time as well as their help and encouragement.

Abil Varkichan Jose
Ajin Kumar
Antony Dadu
Bryane Sunny Kaniyadan

ABSTRACT

Security and data privacy has always been the issue for the users in the real time applications. Latest technologies have been providing different kinds of innovative ideas such as basic form of passwords, codes, gesture identification, biometric authentication, face recognition, etc. to deal with this issue. Face recognition has been one of the most effective methods in this field. Browsers are the doors from the local systems to the outside world of interconnected networks. All the forms of data are sent and received through the browser applications. Even though browsers handle such large amounts of data, the privacy and security provided by these applications are not very effective. Any user logged into the system are able to view the data and activities of the primary users done through the browser applications which can be exploited by the attackers and can cause serious privacy concerns for the users. In this proposed system, face recognition methods are integrated and coupled with the browser applications where the guest users get a different platform for their uses where by doing so, the actual data of the primary users are kept hidden and protected from the unknown users. The browser application detects the user through face recognition methods and performs the user-space division. This system is expected to have effective performance in user identification and data privacy is implemented so that all the activity of the primary user through the browsers gets secured from the guest users using the same browser.

Contents

LIST OF FIGURES i

LIST OF TABLES ii

LIST OF ABBREVIATIONS iii

1 INTRODUCTION 1

1.1 Problem Definition 2

1.2 Objective 2

1.3 Scope 3

2 LITERATURE SURVEY 4

2.1 Advanced 2D Face Recognition by Feature Extraction and Optimized Multilayer Architecture 4

2.2 Improved Face Recognition Method using Local Binary Pattern Method 7

2.3 Face Recognition System for Access Control using PCA 9

2.4 Idle Lock based Privacy Preserving Secured Web Browser 12

3 USER-IDENTIFICATION IN BROWSER APPLICATIONS USING FACE RECOGNITION 14

3.1 System Design 15

3.1.1 System Architecture 15

3.1.2 System Requirements 15

3.1.3 Face Detection and Recognition Module 16

3.1.4 Browser Module 17

3.2 Implementation Details 17

3.2.1 Face Recognition 17
3.2.2 Browser 18

4 RESULTS AND DISCUSSION **20**

5 CONCLUSIONS **22**

REFERENCES **iv**

APPENDIX **v**

A Sample Code for Face Recognition **v**

B Sample Code for Browser Main Window **vi**

C Screenshots **viii**

List of Figures

2.1 Proposed Flow Chart 5
2.2 Neural Network 6
2.3 Euclidien Distance Comparison for eigenfaces and fisherfaces showing the percentage reduction 8
2.4 Recognition of input image using PCA 10
2.5 System Design 11
2.6 Architecture of accessing exiting browser 12
2.7 Architecture of Secured Web Browser 13
2.8 Working Model of PPSWB 13

3.1 Proposed Architecture 15

C.1 Add User viii
C.2 Found User ix
C.3 Browser ix
C.4 No user found x

List of Tables

4.1 Face Detection Time 20

List of Abbreviations

API Application Programming Interface

CEF Chromium Embedded Framework

FRR False Rejection Rat

ICA Independent Component Analysis

JDK Java Development Kit

LBP Local Binary Pattern

LDA Linear Discriminant Analysis

PCA Principle Component Analysis

www World Wide Web

Chapter 1

INTRODUCTION

A web browser is a software application for accessing information on the World Wide Web (www). As a client/server model, the browser is the client run on a computer that contacts the Web server and requests information. The Web server sends the information back to the Web browser which displays the results on the computer or other Internet-enabled device that supports a browser. Browser security is the application of Internet security to web browsers in order to protect networked data and computer systems from breaches of privacy or malware. While browsing, browser loads the content from a website controlled by someone else, which may or may not be trustworthy. It downloads their content on to the computer, runs that trusted or untrusted code and it has to do this constantly, without exposing the computer or the user to unnecessary risks. Face is most commonly used biometric to recognize people. Face recognition has received substantial attention from researchers due to human activities found in various applications of security like airport, criminal detection, face tracking, forensic etc. Compared to other biometric traits like palm print, Iris, finger print etc., face biometrics can be non-intrusive. They can be taken even without user's knowledge and further can be used for security based applications like criminal detection, face tracking, airport security, and forensic surveillance systems. Face recognition involves capturing face image from a video or from a surveillance camera. They are compared with the stored database. Face biometrics involves training known images, classify them with known classes and then they are stored in the database. When a test image is given to the system it is classified and compared with stored database.

1.1 Problem Definition

Security and data privacy has always been the issue for the users in the real time applications. All the forms of data are sent and received through the browser applications. Most browsers store the credentials inorder to make the log in effortless and the latest browsers have all the informations of a user stored, in the form of bookmarks, histories, saved passwords, autofill informations, etc. Any user logged into the system can view the data and track activities of the primary users done through the browser applications. All these are accessible for that unknown person until the main user always keeps logging out from his browser and again logs in when needed, which is a troublesome activity. So, its better that each user other than the primary user gets a new session for the browser activities so that all the details of the primary users get hidden from the guest users. Even if one's email account is accessed by any other person, all the details can me altered or misused since that is the basic key used everywhere in the internet for any activity.

1.2 Objective

The objective of this project is two-fold. The initial goal is to develop a browser to which real time face recognition can be integrated and then implementing the user detection and identification. By integrating and coupling face recognition methods, primary users can be authenticated, so that only he gets complete access to all his informations. So, authentication is the pivotal factor in determining the privacy. Security should be provided from the physical access of an attacker. Therefore, it is neccessary that the browser application provides increased privacy to the user and his contents where when an other user arrives, he is provided with another instance of the browser or session where no information of the primary user is visible. These faces are detected through the webcams present in each systems. These are the basic objectives which meets the above mentioned problem statement.

1.3 Scope

As discussed in the problem definition, In reality, everyone has details about themselves that they would like to keep private, whether it's from the other members of their household or any other unknown person or from advertisers who seek to learn everything about them in order to create an advertising profile, or from network monitoring which leads to false assumptions about their intentions. The proposed system provides security and maintains the privacy of users and their data in the browsers through face recognition methods. An automatic guest session is provided if a new user other than the primary user comes infront of the system by using the webcams. This browser session provides a form of icognito modes prevailing in the modern browsers but no details of the primary user is visible. If the primary user is recognised then he gets access to his information. The guest seesion ends once the window is closed. If ever there is an attacker trying to intrude into the primary user's privacy thorugh the saved data, it becomes impossible since his face cannot be identified. The scope of this system varies from large scale (including big marketing enterprises, banking sectors, etc.) to small scale systems like personal computers, single log in systems, etc.

Chapter 2

LITERATURE SURVEY

2.1 Advanced 2D Face Recognition by Feature Extraction and Optimized Multilayer Architecture

Facial recognition has most significant real-life requests like investigation and access control. It is associated through the issue of appropriately verifying face pictures and transmit them person in a database. Most of the face detector techniques could be classified into feature based methods and image based also. Feature based techniques adds low-level analysis, feature analysis, etc. Facial recognition is a system capable of verifying and identifying a human after 3D images. By evaluating selected facial unique features from the image and face dataset. Design from transformation method given vector dimensional illustration of individual face in a prepared set of images, Principle component analysis inclines to search a dimensional sub-space whose normal vector features correspond to the maximum variance direction in the real image space. The PCA algorithm evaluates the feature extraction, data, i.e. Eigen Values and vectors of the scatter matrix. Face recognition is a design recognition mission performed exactly on faces. It can be described as categorizing a facial either "known" or "unknown", after comparing it with deposits known individuals. It is also necessary to need a system that has the capability of knowledge to recognize indefinite faces. Computational representations of facial recognition must statement various difficult issues. The novel technique is compared with well settled facial recognition methods, name

component analysis and eigen values and vector. This algorithm is called PCA and ICA (Independent Component Analysis). In research work, this novel approach is implemented to detect the face in minimum time and evaluate the better accuracy based on Back Propagation Neural Networks.

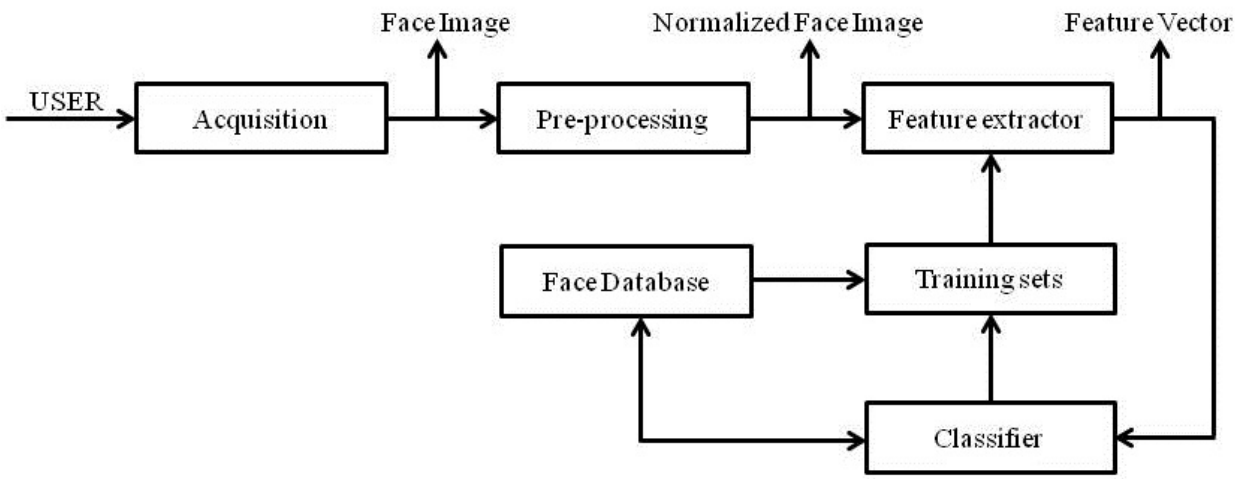

Figure 2.1: Proposed Flow Chart

Image Acquisition converts the image uploaded from the database to grey scale image in order to reduce the size of the image. The noise in the grey scale image is identified and it is reduced to maintain the quality.

Pre-processing applies segmentation for edge detection based on threshold values.

Feature Extraction uses independent component analysis (ICA) which is found to be more effective strategy.

Optimization Reduces the feature data using genetic algorithms which are computer programs that simulates the procedures of natural evolution in arranging to solve complex and to model evolutionary systems. The genetic optimization approach is designed to solve the difficult problems like Complexity, cost, energy and Time consumptions.

Classification reduces the features using back propogation neural network. It evaluates the performance parameters i.e false acceptance rate, false rejection Rate and Accuracy and compare the existing performance parameters i.e accuracy.
In edge detection the single edges in the gray scale image are detected. It uses a multi-stage technique to detect a wide range of edges in images.

In FRR (False Rejection Rate), the quantity of the probability that the biometric traits secure system will incorrectly reject an access attempt is measured. An organization's FRR typically is stated as the ratio of the amount of false rejections divided by the amount of documentation attempts.

The back propagation neural network is the classification technique used to classify the face recognition training state data set. The information is transferred between hidden layers to the output layer. Hidden layer checks the backup information and then transfers the information in the next layer. Activation functions are used to filter the information.

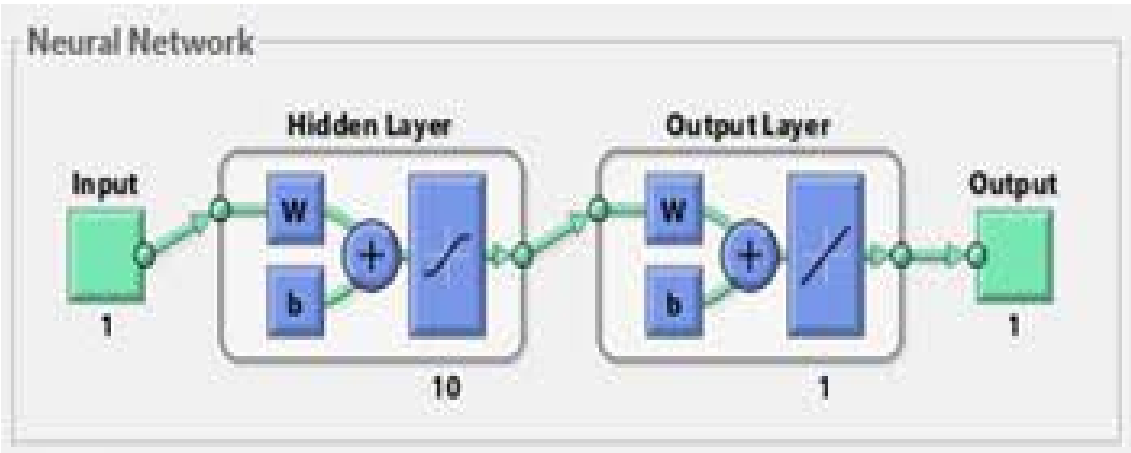

Figure 2.2: Neural Network

2.2 Improved Face Recognition Method using Local Binary Pattern Method

Face recognition is becoming the key security feature in every aspect of computational security. It is regarded as a secure biometrics and effortless identification.Here two methods are discussed based on Yale database. The entire process is divided into two phases: face detection and face recognition. The image is used after converting it to grayscale image since it reduces complexities in calculations. For face detection, the Viola Jones algorithm is used. It is an algorithm which covers the first face of face recognition, the face identification. Though it is an old method, it is used here because it is computationally efficient and lighter to execute in all devices including mobile devices. The four steps in this process are Face. X8 down sampler, color segmentation, followed by post processing and template matching.

Now after face detection, face identification should be done which can be performed by some face recognition algorithm, Some of them are Eigenfaces and fisher faces. The Eigenfaces method is widely used where it calculates the Eigenvector which is actually the eigenfaces. These inputs are then calculated as a coordinate system. It also does some dimensionality reduction by utilizing principal component analysis. This is greatly advantageous in the case where scattering of images is minimum.

In fisher faces method, it utilizes both Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA). LDA has the advantage of minimizing the variation besides maximizing class seperation.

The disadvantages of this method is that it can't detect faces in challenging conditions. The algorithms proposed will have less complexity computationally, but lacks efficiency since it won't meet the defined standards. In the case of low light images, the faces won't be identified properly. The absence of neural networks or any kind of machine learning algorithms provide limited accuracy and limits the system to expand its capability. The total performance of face recognition system improves if a large number of training images are used.

The Local Binary Pattern (LBP) is a technique of face detection and recognition using both shape and texture information of a face image. It is very effective for image textures. The human face area is segmented into small regions to measure local binary pattern histogram which is used to recognize image. The local binary patterns are used to select the target region of the image and form a matrix for feature selection.

Face recognition using eigenfaces have some initialization stages like preparing a training set and calculating eigenfaces from the set of images.

Fisherfaces method is another popular method for face recognition which uses both Principle Component Analysis (PCA) and Linear Discriminant Analysis (LDA) to produce the projection matrix. It is similar to the eigenfaces method. The fisherfaces method has an advantage of using within class information which minimizes variation within class besides maximizing class separation.

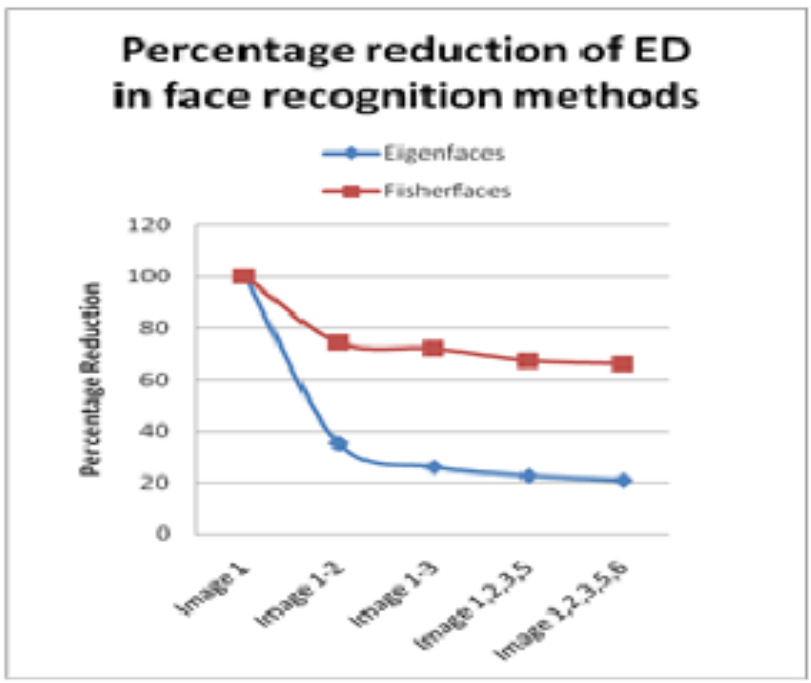

Figure 2.3: Euclidien Distance Comparison for eigenfaces and fisherfaces showing the percentage reduction

2.3 Face Recognition System for Access Control using PCA

Security of computer systems is an important region that needs to be looked at. Hence, a very important part of a system is established using a face recognition system. When compared to other biometric security systems like fingerprint, voice etc. the face recognition system provides better universality, usability and security. Thus face recognition can be considered as one of the best methods to provide security to the computer systems. It is affected by noise and has a better response rate. Like all the other face recognition processes, here also there are the basic four steps which include image acquisition, pre-processing, feature extraction and classification. For feature extraction PCA (Principal Component Analysis) algorithm is used. The PCA algorithm includes the two phases the training phase and the classification phase. In the two phases the eigen spaces are trained and then used for classification. A value is set for face identification. Accordingly, the eigen vector values are compared and if the distance is close to face class the face is detected.

Principal Component Analysis (PCA) is used in pattern recognition and a method of projection to a subspace. It is used to re-express the data in lower dimension basis vector and hence the redundancy of the data is minimal with less loss of orginal data. Any particular face can be represented as eigenfaces in terms of a coordinate system. PCA can outperform LDA (Linear Discriminant Analysis) if the training data set is small. PCA is a more suitable algorithm for access control since it gives faster response of recognition compared to LDA. PCA also has the advantage of simple computerization.

In face recognition, PCA is used to calculate the eigenfaces and finding the vectors that accounts for the distribution of face images within the entire image space. There are two phases in the PCA algorithm - training phase and classification phase. In the training phase, the eigenspace is established from training samples and the training images are mapped to eigenspace for classification. During the classification phase, an appropriate classifier is used to classify when input is projected to the same eigenspace.

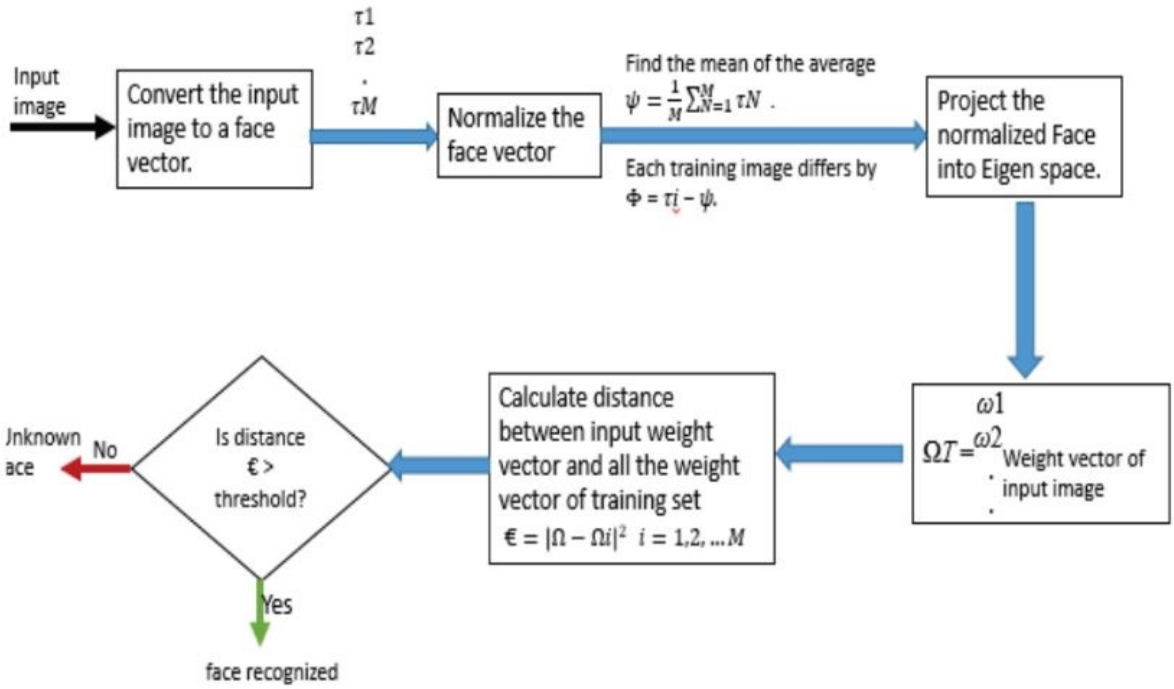

Figure 2.4: Recognition of input image using PCA

In the system design stage the process starts via a webcam which detects motion which is written using MATLAB. When a motion is detected, that particular frame is sent to the face detection module which also uses MATLAB. The processed face is compared with all the faces in the database. If found, then a signal is passed to Arduino UNO microcontroller. If the correct person's face has been identified the when that particular signal is acquired by the Arduino UNO microcontroller, a light starts to blink indicating that the correct user was identified. The software development part as mentioned above has been mainly done using MATLAB and Computer Vision Toolbox and Statistical and Image acquisition Toolbox has been used. These toolboxes provide functions such as webcam access, image processing etc. Under controlled conditions the face recognition system provides very high accurate result rate.

Figure 2.5: System Design

The face detection module achieved a higher correct detection rate and was able to recognize multiple faces in the same frame. Thus the system was able to distinguish between recognized and unrecognized faces and the microcontroller connected to other systems took appropriate action in each of the scenarios. The System gave accurate results when the background conditions were set under controlled parameters rather than uncontrolled ones. The accuracy rate of the system was directly proportional to the number of training image and as the variation in head position decreased, the accuracy rate increased. Therefore, to attain maximum accuracy rate of the system, all parameters were set in controlled conditions. Thus, the system could be used for the security applications.

PCA was a reliable algorithm to be used in face recognition security system if the parameters were set in the controlled conditions. Using Arduino UNO microcontroller gave the advantage of easy progaramming and also an economical control. The main disadvantage is the low capacity processor that are not capable of running long time and hence not suitable for continuous system.

2.4 Idle Lock based Privacy Preserving Secured Web Browser

Web browsers are becoming an effective tool for internet users in these days. So browser privacy and browser security is a must concern for the users. The developers need to build the softwares with a strong unbreakable security feature, otherwise attackers can easily attack personal details. There is a web browser called Turtle Mini, which is of small size compared to other browsers like google chrome, mozilla firefox etc. This browser provides a idle lock based security feature.ie, this browser will automatically lock if the browser become idle for a time that the user already set. If the browser is locked,then we have to enter a 4 digit passcode to use the browser again. The idle time of the browser is determined by continuously monitoring the keyboard and mouse.

The issues with the normal browsers is that a guest user other than the actual or primary user can see the personal details of the primary user and also have the access to all the credentials of that user. By using the details any anonymous user can act as the primary user and communicate.

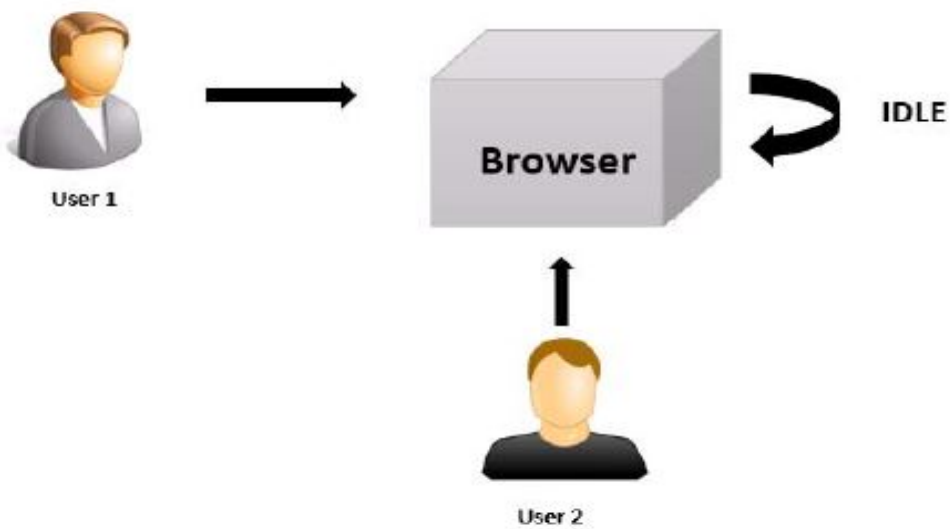

Figure 2.6: Architecture of accessing exiting browser

The main turtle mini objective is Privacy Preserving Secured Web Browser (PPSWB). The browser will lock itself when the browser is not in use. The user needs to enter a four digit pincode to access and use the password. The browser continuously monitors the keyboard and mouse and detects the idleness. This also provides an option for the primary user to use the browser without a lock. If the browser becomes idle then the timer will start and lock the browser if it exceeds. User have to again enter the pin if the browser is locked.

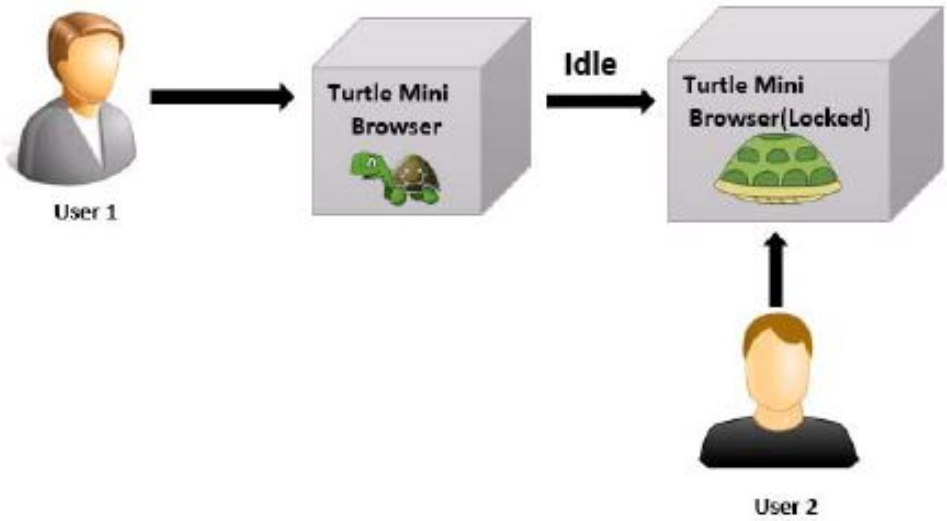

Figure 2.7: Architecture of Secured Web Browser

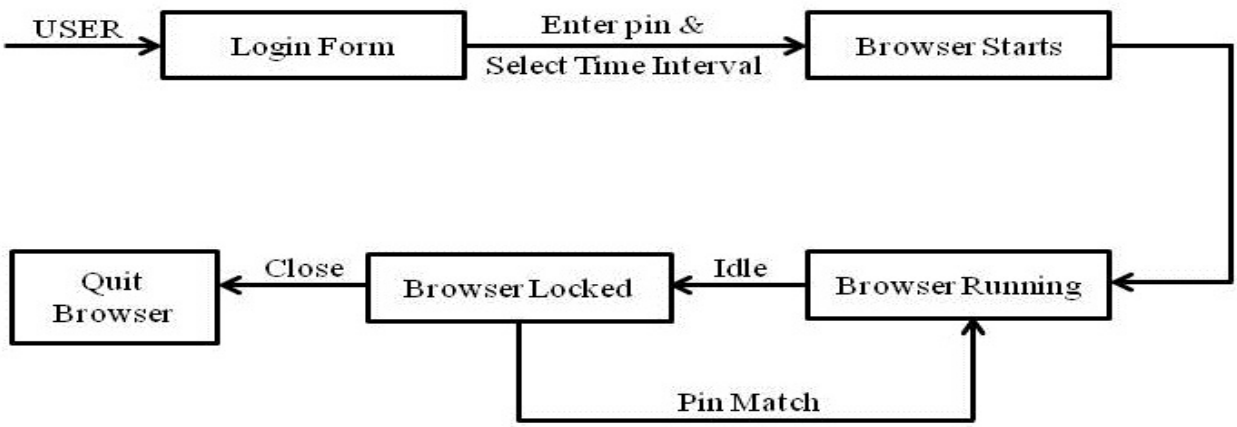

Figure 2.8: Working Model of PPSWB

Chapter 3

USER-IDENTIFICATION IN BROWSER APPLICATIONS USING FACE RECOGNITION

A browser which solves the prime concern of security issue, a physical data breach attack by another physically present user in a web browser environment. The normal culture of human to live the hassle-free life has made him save all the passwords for the websites he visit. Also additional effortless attempt is aided by the signed in stage for social networking websites which gives one click access to one's personal space. So there should be some browser which enforces such a security which restricts an intruder from any data from web browsers. A web browser can be made by integrating the most effortless and the most secure biometric feature available in the modern world is face recognition.

The very novelty of this system is that it is effortless to the user and keeping his data safe to an environment where only access to the browser is given only to the person authorized to do so. The system recognises the owners face in real time by utilising the webcam of the system.

The entire face recognition part can be defined as two phases: face detection and face identification. The systems used are of high accuracy and the major priority was to deliver perfect images for security assurance.

3.1 System Design

3.1.1 System Architecture

The image of the primary users is stored in the database for matching in realtime. The image of the user infront of the system is captured using the webcams and then given as input to the face recognition system which includes face detection and then the comparison is done with the image in the face database for any matching and if database result of the matching is true value, then the primary user gets access to his data and credentials stored in the browser and if the matching gives a false value, then the guest user gets a browsing session where all the primary user data is hidden and the guest user gets a fresh session. This proposed architecture includes integration of the face recognition system into the browser which provides secure browsers through user-identification using face recognition.

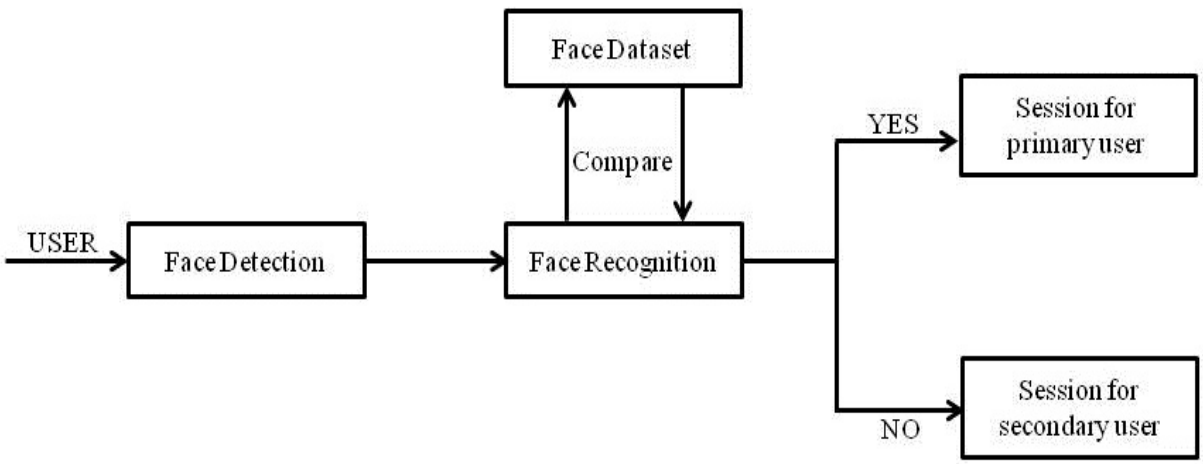

Figure 3.1: Proposed Architecture

3.1.2 System Requirements

The basic requirements for the proposed system is the hardwares required for capturing images and softwares for its processing and producing the required output. A linux operating system is used for the smooth functioning and efficient performance of the proposed system implementation. The hardware requirements consists of a laptop with a quadcore

processor and 4GB RAM or more with a webcam of 2MP or more for capturing images with high quality and better resolution. A preferable GPU is required for faster processing of the images and thereby giving a faster output results. The coding and execution of algorithm is done using softwares that provide platforms for running codes in Python language. CEF(Chromium Embedded Framework) python is utilized when coding the browser and during the implementation of the proposed system. A PyQt is used to interface the face recognition system and the browser. The face data sets are stored in a cloud backup application for proper generation of results.

3.1.3 Face Detection and Recognition Module

The algorithm used here recognizes and manipulates faces from Python or from the command line with simple face recognition library. The algorithm is built using dlib's state-of-the-art face recognition built with deep learning and CNN. The model has an accuracy of 80-85%. This also provides a simple "face_recognition" command line tool that enables face recognition on a folder of images from the command line. The main feature of the algorithm is that it finds all the faces that appear in the picture by getting the location of each persons eyes, nose, mouth and chin and then it recognizes who appears in each photo.

The tools used are very minimal which includes Python 3.3+ idle for coding the algorithm. The dlib is installed with python bindings. Then, the "face_recognition" module is installed from the pypi. When "face_recognition" module is installed, a simple command-line program called "face_recognition" is received that can be used to recognize faces in a photograph or folder full for photographs. A single image is given as input and the model is trained and the image is stored as a pickled value in the databse. This value is compared with the input image and the recognition is carried out. Then, the command "face_recognition" is run by passing stored value of the pickled image.The entire process is proposed to provide maximum accuracy and timely completion of the recognition procedure. The face landmarks and similiarities can be efficiently judged from this model since this considers the unchangeable attributes, especially the distance margins in face. This causes the recognition to be possible at even worse conditions of light and face input shapes.

3.1.4 Browser Module

A basic browser is created with the help of an open-source code CEF Python which provides python bindings for chromium embedded frameworks and for a good visualization GUI toolkit PyQt5 is used. CEF focuses on facilitating embedded browser use cases in third-party applications. A basic browser is thus created initially using CEF Python and PyQt5. Qt is set of cross-platform C++ libraries. It is used to implement the latest aspects of modern applications. Including it with CEF Python code, PyQt provides basic GUI on the Chromium based web-browser. PyQt5 is a comprehensive set of Python codes and enables Python to be used as an alternative application development language to C++ on all supported platforms. PyQt5 may also be embedded in C++ based applications to allow users of those applications to configure or enhance the functionality of those applications.

The CEF Python is made available by installing pypi/cefpython3 package using pip tool and PyQt5 is made available by installing pip3 install PyQt5.

3.2 Implementation Details

3.2.1 Face Recognition

In the very first stage of the project, it had to be decided that which face recognition algorithm had to be used. Many different face recognition methods were tried which included artificial neural network. Voila Jones, etc. We had to run these algorithms using different data sets. All these algorithms had accuracy issues in different light conditions or camera resolutions. After testing various algorithms, dlib's state-of-the-art face recognition was fixed which was built with deep learning and CNN which showed 80-85% of accuracy. Python had inbuilt face recognition modules and these modules had to be imported to our project. These face recognition modules required only a single image for data training which had been the novelty of this algorithm. This algorithm used the concepts of CNN (Convolutional Neural Network) and deep learning. The proposed algorithm fetches a single image as training set. This single image is used to train the entire model. We are having an inbuilt model representation for this "face_recognition" python module. This single image is represented

as numpy arrays in concepts of CNN matrices . This identifiers are a found from applying pickle function to this. This stream of character value is stored for comparison. Then when we provide an input image , it is converted and represented in just the similar way stated above. Thus it becomes easy in case of recognition part. The new pickled value obtained about the input image is compared to the previously existing image and then they are matched and face is recognized. The matrix representation uses Maximum margin object detection, especially the distance measures between both eyes, pupils, nose, face contour points, just as the case of 64 point mark, the face counters and counter parts are marked with points and they form the features of this image. All these points will have greater similarity since they are always independent and at the same time unchangeable for a person's face even in conditions of low light. That yield to the accuracy of this model. There are no near misses for this classifier model. The response time is reduced to a greater extent since we have easy pickling and matrix representation. The pickled stream is easy to compare and represent . So the time involved in the entire process reduces to minimum.

3.2.2 Browser

In the next stage, the basic browser had to be coded. Since security and privacy features had to be implemented, elements of security like new-tab, history, auto-save, bookmarks, session-timeout, etc. So, it was hard to code and implement a full-fledged browser with these features. So, the alternative way to work upon basic framework and modify the browser with these features. CEF (Chromium embedded framework) Python along with PyQt(v5) was used for developing the browser. Since all basic browsers use C++ language, CEF Python enabled this by giving various C++ libraries. Next phase, the face recognition algorithm had to be integrated into the browser. The face recognition was set up as an application which had to be called from the browser. Using PyQt, the frame for capturing the image of the users was called and the captured image was given as input to the face recognition algorithm. The browser has a camera button for capturing the image for face recognition. For saving a user to the data base, a new user button is added to the browser, through which we can capture the new image and store it to the database. All the images of the new user are added to the folder named 'Faces' with image name given which is given during

adding the new user. 'faces.db' , a databse file is also created at the time when the new user is added. For implementing the face recognition module, files were imported from OpenCV which is a library of programming functions. This integration stage was rather easy to implement since we have dependent python programs for both face recognition and browser. So here we just need to call an external library from the face recognition engine. This is rather an easy task, it is done by the call 'import face_recognition'. The default prebuilt model is being imported to the browser environment. We just need to configure the camera handler program for capturing the image. In browser we have pop-up dialogues for face recognition and utilities. It is being done based on the database file 'faces.db'. Corresponding recognition works on them. New domain data is added, that is username and passwords, auto-fill is also residing in the same database. The interfacing application utilising PyQt works similarly by providing a recognizer dialog of captured face, messages for every actions with proper timer being set.

Chapter 4

RESULTS AND DISCUSSION

The work done to build a browser in which integrates a face recognition module and have corresponding sessions with respect to those faces recognized can be integrated. This ensures privacy protection in each sessions. So these browser should be efficiently integrate the python module. Normally browsers are coded in language C++ or efficient languages. Python is rarest of them but with JDK, JavaScript JSON calls are inefficient to call python module. So we coded a browser in python with all the basic features to integrate the face recognition module and to call them efficiently within time bound. Time responsiveness is a key factor in deciding how well a calling . This is done with the module Chromium Embedded Framework. CEF python has features added up. Providing multiple tabs, auto-fills etc. can be attributed to be done with CEF Python. Pyqt is used to interface this application just as a desktop python application. By this we get the interface of a proper browser just as the one we use in our day to day basis.

Table 4.1: Face Detection Time

Sample test case	Time taken
Camera capturing	0.98 sec
Recognition dialog display	1.12 sec
Browser session loading	0.90 sec
Idle session timeout	600 sec
Domain addition	0.60 sec

The accuracy of the face recognition system is around 80-85% . So the privacy protection is done at the maximum level with an easy error free procedure. This too runs as a background back-end application in appearance, or can be seen as part of the browser. Enough data abstraction is done for the end user since he can navigate through these with buttons. Efficient calls can be made within the browser so as to avoid computational and time constraints. The features such as password saving based on domain is provided for each user. Also at the time of adding a user, his all basic details including Name, Last name , email address, mobile phone number, preferable username is collected. At a time of form filling , these data can be provided as auto-fill details. The fields are compared with the ones stored in local database corresponding to face database file, and these are compared with the web page text field and efficiently supported. A website supporting both these can be instantiated with 'www.facebook.com'. This website is an example of substituting both the username and passwords along with providing autofill in a single page. We can also use these features in similar other pages. The performance of the browser is not affected by the face recognition which runs in the background. It works flawlessly at times required. We also provide an idle session timeout especially targeted to protect users privacy if he walks away without log out. A sample time mouse idle is captured to provide session timeout. The log out needs re authentication to log in back.

Chapter 5

CONCLUSIONS

Face is most commonly used biometric character used to recognize people and has universal acceptance. The proposed system builds an effective face and gesture recognition system that can perform in real-time scenarios in browser application. The proposed face recognition system is expected to have higher accuracy in comparison with other contemporary algorithms. This system can provide security for browsers by integrating face recognition system into the browser. Every primary user gets privilege to hide the personal details and data including various credentials like saved passwords, transactions pins, mails, etc. These credentials are very important in maintaining online privacy which can be utilized by the attackers to communicate as the primary users or use those data to intrude into the primary users' privacy. By providing the secondary browsing sessions, secondary users get a different browsing place idle from all the existing and stored data. This proposed system is expected to have give more security oriented browsers with more privacy being provided.

Future Work

Browser with auto face detection and device independent browsers can be considered on the road-map as a future work. This will be considered as a very useful feature for further future use. This will indeed decrease the identification typing signing in time and add maximum local protection to the user using the system Additional local caches can be provided just as users can switch sessions in real time and resume their work.

REFERENCES

[1] Hsu, R.-L., Abdel-Mottaleb, M., and Jain, A. K. Face Detection In Color Images.Ieee Trans. Pattern Analysis and Machine Intelligence 24, 5, 696–706, 2002

[2] S. Guo, S. Chen, Y. Li, "Face recognition based on convolutional neural network and support vector machine", IEEE International Conference on Information and Automation, 2017.

[3] P. Viola and M. J. Jones, "Robust real-time face detection," Int. J. Comput. Vis., vol. 57, no. 2, pp. 137- 154,2004.

[4] P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman, "Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection," IEEE Trans. Pattern Anal. Mach. Intel!. , vol. 19, no. 7, pp. 7ll- 720, Jul. 1997.

[5] David Tarkowski IMAQMOTION - Image acquisition motion detection.http://www.mathworks.com/MATLABcentral/fileexch ange/5470.

[6] Barrett, R ; Maglio, P.P. ; Kellem, D.C; "Web Browser Intelligence: opening up the Web",Compcon '97. Proceedings, IEEE,1997-26 Feb 1997, pp-122 - 123.

[7] Shinjo.Y; FeiGuo ;Kaneko,N. ; Matsuyama, T., "A distributed web browser as a platform for running collaborative aapplications",Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2011 7th International Conference, Oct. 2011, pp 278 – 286.

[8] Taivalsaari, A., Mikkonen, T. ; Ingalls, D. ; Palacz, K., "Web Browser as an Application Platform", Software Engineering and Advanced Applications, 2008. SEAA '08. 34th Euromicro Conference, Sept. 2008, pp 293 – 302.

Appendix A

Sample Code for Face Recognition

```
import face_recognition

from FaceDB import FaceDB
class FaceRecognitionUtil:
 def recognize(self, filename):
  users = FaceDB.get_instance().get_all_user()
  print(users)
  for user in users:
   known_image = face_recognition.load_image_file(user)
   unknown_image = face_recognition.load_image_file(filename)
   if len(face_recognition.face_encodings(unknown_image)) != 0:
   biden_encoding = face_recognition.face_encodings(known_image)[0]
   unknown_encoding = face_recognition.face_encodings(unknown_image)[0]
   results = face_recognition.compare_faces([biden_encoding],
                                            unknown_encoding)
   if results[0]:
     return FaceDB.get_instance().get_user(user)
  return None
```

Appendix B

Sample Code for Browser Main Window

```
import ctypes
import os
import platform
import sys

from cefpython3 import cefpython as cef
from PyQt5.QtGui import *
from PyQt5.QtCore import *
from PyQt5.QtWidgets import *
import Utils
from CefApplication import CefApplication
from MainWindow import MainWindow

def main():
    check_versions()
    sys.excepthook = cef.ExceptHook
    settings = {}
    if Utils.MAC:
```

```
        settings["external_message_pump"] = True
    cef.Initialize(settings)
    app = CefApplication(sys.argv)
    main_window = MainWindow()
    main_window.show()
    main_window.activateWindow()
    main_window.raise_()
    app.exec_()
    if not cef.GetAppSetting("external_message_pump"):
        app.stopTimer()
    del main_window
    del app
    cef.Shutdown()

if __name__ == '__main__':
    main()
```

Appendix C

Screenshots

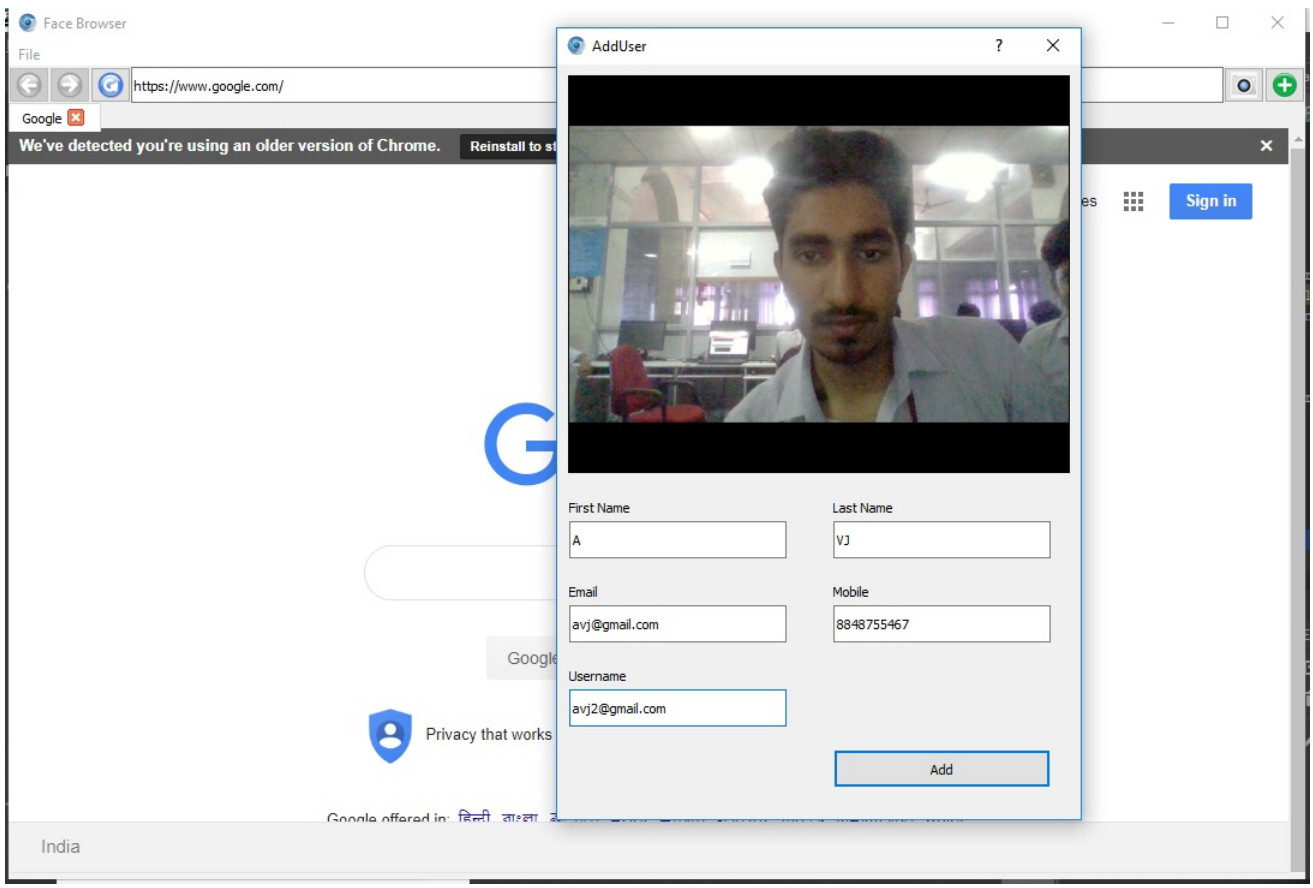

Figure C.1: Add User

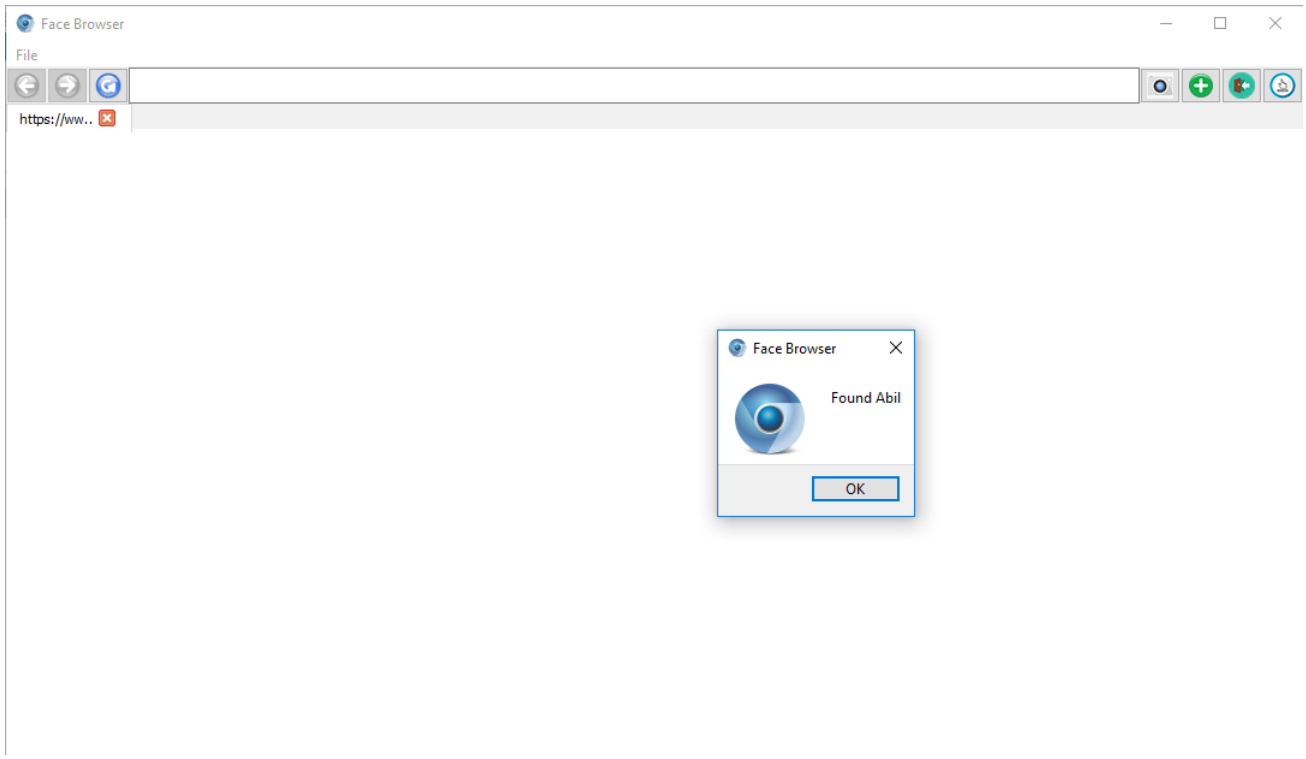

Figure C.2: Found User

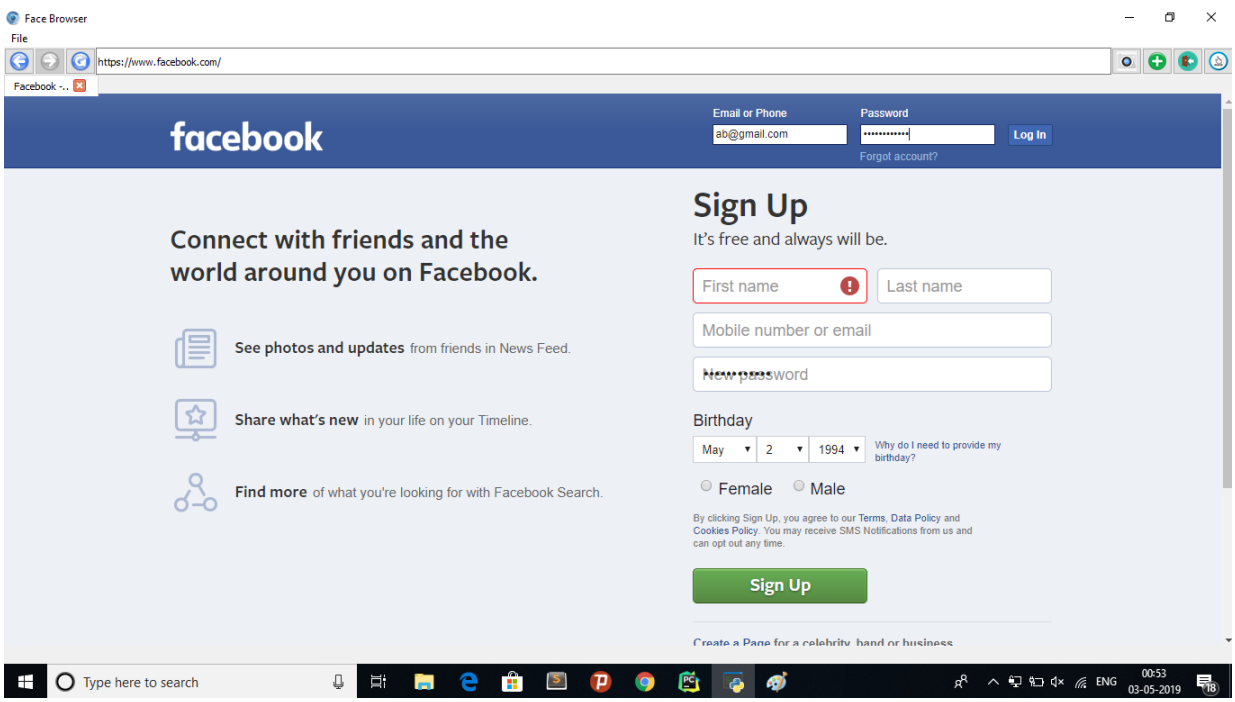

Figure C.3: Browser

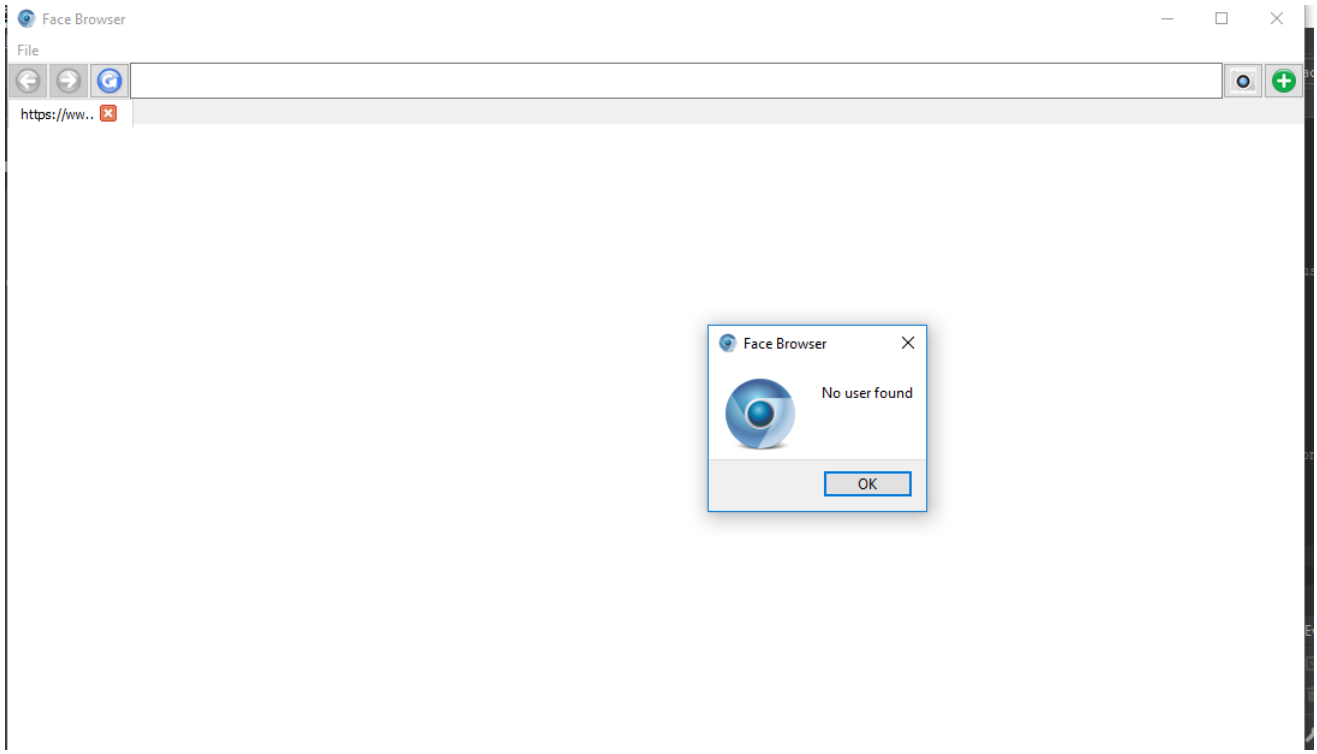

Figure C.4: No user found