Online CAPTCHA replacement through Face Detection

B.E. Project Report - 'B'

Submitted in partial fulfillment of the requirements

For the degree of

Bachelor of Engineering
in
Computer Engineering

by

Mr. Aditya Kakad

Mr. Sumit Bhirud

Mr. Rutwik Chinchole

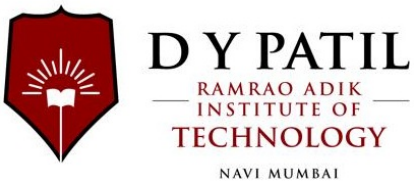
Mr. Aakarsh Raghunath

Supervisor

Dr. Bharti Joshi

Co-Supervisor

Ms. Snehal Mumbaikar



Department of Computer Engineering

Dr. D. Y. Patil Group's

Ramrao Adik Institute Of Technology

Dr. D. Y. Patil Vidyanagar, Sector-7, Nerul, Navi Mumbai-400706.

(Affiliated to University of Mumbai)

April 2019

Ramrao Adik Institute of Technology

(Affiliated to the University of Mumbai)

Dr. D. Y. Patil Vidyanagar, Sector-7, Nerul, Navi Mumbai-400706.

CERTIFICATE

This is to certify that, the project 'B' titled

" Online CAPTCHA replacement through Face Detection "

is a bonafide work done by

Mr. Aditya Kakad
Mr. Sumit Bhirud
Mr. Rutwik Chinchole
Mr. Aakarsh Raghunath

and is submitted in the partial fulfillment of the requirement for the degree of

Bachelor of Engineering
in
Computer Engineering
to the
University of Mumbai

Supervisor	Co-Supervisor
(Dr. Bharti Joshi)	**(Ms. Snehal Mumbaikar)**

Project Co-ordinator	Head of Department	Principal
(Mrs. Smita Bharne)	**(Dr. Leena Ragha)**	**(Dr. Ramesh Vasappanavara)**

Declaration

We declare that this written submission represents my ideas in my own words and where other's ideas or words have been included, we have adequately cited and referenced the original sources. We also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Mr. Aditya Kakad	**15CE8005**	_____
Mr. Sumit Bhirud	**15CE7043**	_____
Mr. Rutwik Chinchole	**15CE7044**	_____
Mr. Aakarsh Raghunath	**15CE7048**	_____

Date : .../.../.....

Project Report Approval for B.E

This is to certify that the project 'B' entitled ***" Online Captcha Replacement Through Face Recognition and Detection "*** is a bonafide work done by ***Mr. Aditya Kakad***, ***Mr. Sumit Bhirud***, ***Mr. Rutwik Chinchole*** and ***Mr. Aakarsh Raghunath*** under the supervision of ***Dr. Bharati Joshi*** and ***Ms. Snehal Mumbaikar***. This dissertation has been approved for the award of ***Bachelor's Degree in Computer Engineering, University of Mumbai***.

Examiners :

1. .....

2. .....

Supervisors :

1. .....

2. .....

Principal :

.....

Date : .../.../.....

Place : .....

Acknowledgement

I take this opportunity to express my profound gratitude and deep regards to my supervisor **Dr. Bharti Joshi** & co-supervisor **Ms. Snehal Mumbaikar** for their exemplary guidance, monitoring and constant encouragement throughout the completion of this report. I am truly grateful to his efforts to improve my technical writing skills. The blessing, help and guidance given by him time to time shall carry me a long way in the journey of life on which I am about to embark.

I take this privilege to express my sincere thanks to **Dr. Ramesh Vasappanavara**, Principal, RAIT for providing the much necessary facilities. I am also thankful to **Dr. Leena Ragha**, Head of Department of Computer Engineering, Project Co-ordinator **Mrs. Smita Bharne** and Project Co-coordinator **Mrs. Bhavana Alte** , Department of Computer Engineering, RAIT, Nerul Navi Mumbai for their generous support.

Last but not the least I would also like to thank all those who have directly or indirectly helped me in completion of this thesis.

Mr. Aditya Kakad
Mr. Sumit Bhirud
Mr. Rutwik Chinchole
Mr. Aakarsh Raghunath

Abstract

The sensitive information stored on the internet should not be easily accessible by any unauthorized personnel, it should be readily available only to the authorized people. Thus integrity, security and confidentiality need to be maintained. There needs to be a security check before any kind of access is granted to any kind of sensitive information. CAPTCHA (Completely Automated Public Turing Test to tell Computers and Humans Apart) is a popular way for authenticating a user. The main goal of any technique is to recognize whether it is a human who is accessing the content or a robot via some recognition techniques. The advancement in recognition technologies has enabled humans to develop bots which can now bypass common authentication techniques which have been in use for a long time. CAPTCHA has been in use since a very long time and has some serious drawbacks. Facial recognition alongside with artificial intelligence can overcome drawbacks like difficulty in solving, ambiguity, and sometimes easy prey for trained bots of CAPTCHA and can easily replace it.

Contents

Abstract **i**

List of Figures **iv**

1 Introduction **1**

1.1 Overview 2

1.2 Objective 2

1.3 Motivation 2

1.4 Problem Definition 2

1.5 Organization of Report 3

2 Literature Survey **4**

2.1 Research Papers Survey 4

2.2 Analysis 6

3 Proposal **7**

3.1 Problem Statement 7

3.2 Proposed Work 7

3.3 Proposed Methodology 8

3.4 Hardware & Software Requirement 12

3.4.1 Hardware Requirements 12

3.4.2 Software Requirements 12

4 Planning & Formulation **13**

4.1 Schedule for Project / Gantt Chart 13

4.2 Detailed Plan of Execution 14

5 Design of System **15**
5.1 System Architecture 15
5.2 Activity Diagram 16

6 Results **17**
6.1 Results & Analysis 17
6.2 Project Outcomes 23

7 Conclusion **24**

8 Future Work **25**

References **26**

Appendices **27**

A Weekly Progress Report **27**

B Paper Publication **29**

C Project Competition **35**

List of Figures

3.1 Visualization of the subset of training data 10
3.2 Training and Validation Loss 11
3.3 Visualization of test predictions. 11

4.1 Schedule 13

5.1 System Architecture 15
5.2 Activity Diagram 16

6.1 Sample e-commerce website 20
6.2 Webcam access 21
6.3 Image captured via webcam 21
6.4 Success 22
6.5 Fallback 22

8.1 Weekly Progress Report 1 27
8.2 Weekly Progress Report 2 28
8.3 Plagiarism Report 34

Chapter 1

Introduction

CAPTCHA means Completely Automated Public Turing Test to tell Computers and Humans Apart. Recognizing both familiar and unfamiliar faces is what humans are good at and that has been established [1][2]. This user identification procedure has received many criticisms, especially from people with disabilities, but also from other people who feel that their everyday work is slowed down by distorted words that are difficult to read. CAPTCHAs based on reading text or other visual-perception tasks prevent blind or visually impaired users from accessing the protected resource. It takes the average person approximately 10 seconds to solve a typical CAPTCHA. The CAPTCHA method can be easily replaced by Facial Recognition proposed in this paper.

For differentiating humans captcha focuses on providing the user with different tests[3]. Various services including web and financial services use Captchas to provide security measures against malicious attacks. OCR (Optical Character Recognition Manual) was used to extract text in AltaVista Captcha with distortions known to reduce incorporated OCR accuracy[4]

CAPTCHA is nearing its end and is in serious need to be replaced. Specialized tests like Handwritten character recognition and image or pattern recognition tests are used to determine is it really a human who needs to access the data[5]. Captcha has various forms and each one has a unique way of identifying. Although CAPTCHA has a series of tests to determine the differences it has some real serious drawbacks which can be overcome by using various efficient alternatives. In this report we propose a technique of using Facial Recognition to detect whether its a human or a robot accessing the content.

1.1 Overview

The process of identification will be carried out through face recognition and detection, in which features of the face will be mapped and identified through the front facing camera/web-camera and after correct verification, access will be given. A Deep Neural network will learn to detect the face from the image capture, and later authenticate from the face of the user by detecting face features. After correct detection of the facial features, the user will be allowed to access the system.

1.2 Objective

This system will be used as a substitute for CAPTCHA technology. Our proposed system will eliminate the language barrier and slow execution of existing system.

1.3 Motivation

This system is based on face recognition and therefore it will become much easier for the elderly to access the website. It will also make the lives of disabled much easier as they will be able to solve the captcha just by showing their faces. Moreover, this system will help to overcome the language barrier. uneducated people will now be able to access the site without much trouble. This system will ensure much efficient completion of the authentication process as it has lesser bugs than the current existing system.

1.4 Problem Definition

We all need better version of every small things these days. Captcha technology used to authenticate users have been used for a long time without any changes in the way it works or without any improvements in current execution.

This project tends not just to make some improvements but replace existing captcha verification with more faster and hassle free solution.

We will use face detection to verify human instead of typing certain unpredictable words or selecting some randomized images.

1.5 Organization of Report

Chapter 1 contains the introduction of the project along with Overview, objective, motivation and Problem Definition. Chapter 2 contains the Literature Survey of the research papers with Research Paper Survey and Analysis. Chapter 3 contains the Proposal of the project along with Problem Statement, Proposed work, Proposed Methodology and Hardware and Software required. Chapter 4 contains the Gantt chart of the project. Chapter 5 contains the Design of the system with System Architecture, Activity Diagram and the Algorithm. Chapter 6 contains the Proposed Results and Analysis and Project Outcomes. Chapter 7 and 8 contains the Conclusion and future work.

Chapter 2

Literature Survey

2.1 Research Papers Survey

A CAPTCHA is a program that protects websites against bots by generating and grading tests that humans can pass but current computer programs cannot. The term CAPTCHA (for Completely Automated Public Turing Test To Tell Computers and Humans Apart) was coined in 2000 by Luis von Ahn, Manuel Blum, Nicholas Hopper and John Langford of Carnegie Mellon University.

Facial Key Points (FKPs) Detection is an important and challenging problem in the fields of computer vision and machine learning. It involves predicting the co-ordinates of the FKPs, e.g. nose tip, center of eyes, etc, for a given face.

Nowadays, facial keypoints detection has become a very popular topic and its applications include Snapchat, How old are you, have attracted a large number of users. The objective of facial keypoints detection is to find the facial keypoints in a given face, which is very challenging due to very different facial features from person to person. The idea of deep learning has been applied to this problem, such as neural network and cascaded neural network. And the results of these structures are significantly better than state- of-the-art methods, like feature extraction and dimension reduction algorithms.

Current face or object detection methods via convolutional neural network (such as OverFeat, R-CNN and DenseNet) explicitly extract multi-scale features based on an image pyramid. However, such a strategy increases the computational burden for face detection. DCFs have

shown the ability of scale invariance, which is beneficial for face detection with high speed and promising performance. Experimental results on several popular face detection datasets show the efficiency and the effectiveness of the proposed method for face detection.

2.2 Analysis

The proposed methods as given in table 2.1 have various disadvantages. Two of them proposes a face recognition captcha having multiple faces to choose from and the last paper proposes a system with only 3 keypoints. Our system is similar to the previous one except we use 15 keypoints which makes our system more secure.

Table 2.1: Analysis

Paper Title	**Proposed Method**	**Advantages**	**Challenges**
Face Recognition CAPTCHA	Optimizing sets of parameters on which standard face recognition algorithms fail but humans can succeed	FRC fulfills CAPTCHA design guidelines and is therefore robust against adversarial attacks	Less accuracy due to intensive background noise added inorder to add more security to captcha system.[5]
Design of face detection CAPTCHA for implementing robust security	Image-based clickable CAPTCHA	This methodology avoids the continuing escalation in difficulty caused by improved OCR technology. It also avoids potential language barriers since there is no text used in the CAPTCHA	Black and white images of human face are visually distorted and randomly placed on noisy background is difficult to correctly identify faces.[6]
Face Recognition CAPTCHA Made Difficult	Systematically designed face recognition CAPTCHA	FRC fulfills CAPTCHA design guidelines and is therefore robust against adversarial attacks.	Identifies faces by placing markers on just 3 facial parts (eyes, mouth, nose).[7]

Chapter 3

Proposal

3.1 Problem Statement

To replace the process of online CAPTCHA verification for websites which is used to identify whether the access to the website is by a human or through a bot and to rectify issues with the current captcha technology.

3.2 Proposed Work

A computer program or system intended to distinguish human from bot/machine input, typically as a way of automated extraction of data from websites and thwarting spam. This is done with help of CAPTCHA. An algorithm that cracks CAPTCHAs with 90-99.8 percent accuracy is also claimed. Therefore to improve on the security, process of online CAPTCHA verification for websites need to replace which is used to identify whether the access to the website is by a human or through a bot and to rectify issues with the current captcha technology. The face recognition technique is an alternative solution for this.

Following are steps for our system:

- First we prompt the user for the verification process.
- The user allows the image to be captured from the web camera.
- Once the image is captured, and all the other details are verified, the image is sent to the backend using an API. A RESTful API is used to send the image through the http protocol.
- Once the image is received in the backend (AWS), the face detection process begins.
- First the number of faces in the image is detected.

- If the numbers of faces are greater than 1, prompt is given to the user to capture another image. This is for security reasons that only a single face will be used for authentication.
- On the successful face detection further access granted.
- If the face detection is unsuccessful, user will get prompt for another attempt.
- The number of attempts is restricted to 2 in our system. After this, the regular captcha system will be implemented for the user.
- In case of unavailability of the web camera/front camera, the system will automatically fall back onto the captcha system.

3.3 Proposed Methodology

CNNs use a variation of multilayer perceptrons designed to require minimal preprocessing. They are also known as shift invariant or space invariant artificial neural networks (SIANN), based on their shared-weights architecture and translation invariance characteristics.

Convolutional networks were inspired by biological processes in that the connectivity pattern between neurons resembles the organization of the animal visual cortex. Individual cortical neurons respond to stimuli only in a restricted region of the visual field known as the receptive field. The receptive fields of different neurons partially overlap such that they cover the entire visual field.

CNNs use relatively little pre-processing compared to other image classification algorithms. This means that the network learns the filters that in traditional algorithms were hand-engineered. This independence from prior knowledge and human effort in feature design is a major advantage.

The following algorithms show the main function and the function for sending an image to server.

Algorithm 1 Online captcha replacement by face detection

```
1:  procedure MAIN
2:      if(webcamAccess != granted)
3:      goto 11
4:      elif(webcamAccess == granted)
5:      captureImage()
6:      sendImageToServer()
7:      if(numFaces > 1 or numFaces == 0)
8:      captureImage()
9:      else
10:     grantAccess()
11:     captcha()
```

```
1:  procedure SENDIMAGETOSERVER
2:      Convert the image to RGB colorspace
3:      Convert the RGB image to grayscale
4:      Detect the faces in image
5:      get number of faces
```

PROCESS USED FOR FACE RECOGNITION

The face detection process is having multiple stages as described below.

• Detect Faces Using a Haar Cascade Classifier

We have used OpenCV's implementation of Haar feature-based cascade classifiers to detect human faces in images. OpenCV provides many pre-trained face detectors, stored as XML files.

• Add Eye Detections

A Haar-cascade eye detector can be included in the same way that the face detector was. This allows the image under detection to include eyes as a keypoint for verification.

• **De-noise an Image for Better Face Detection**

Using OpenCV's built in color image denoising functionality called fastNlMeansDenoisingColored -we de-noise this image enough so that all the faces in the image are properly detected. Once we have cleaned the image, we run our trained face detector over the cleaned image to check out its detections.

• **Create a CNN to Recognize Facial keypoints**

We notice that facial key point detection becomes a regression problem at high levels when we include 15 key points, thus we employ a convolutional neural network to recognize the patterns in the images.

• **Compile and Train the Model**

Figure 3.1: Visualization of the subset of training data

Figure 3.1 shows the visualization of training data and after we visualize the data and check that the correct keypoints are being mapped, we start to train the model We first experiment with the choice of optimizer to use. After testing, the best fitting optimizer is the Adam, which we implement. We use the fit method to train the model.

• **Visualize the Loss and Test Predictions**

We plot the training and validation loss data as shown in Figure 3.2 to check where the model starts to overfit or underfit. This would help us to determine the number of epochs and manipulating the dropout layers to avoid over fitting and underfitting the model.

Figure 3.2: Training and Validation Loss

- **Visualize a Subset of the Test Predictions**

Figure 3.3: Visualization of test predictions.

For each training image, there are two landmarks per eyebrow (four total), three per eye (six total), four for the mouth, and one for the tip of the nose. The above Figure 3.3 shows visualization of predictions on test data

3.4 Hardware & Software Requirement

3.4.1 Hardware Requirements

- System with Windows 7 and above
- Webcam
- Storage of 2GB
- Minimum RAM of 1GB

3.4.2 Software Requirements

- python 3.6+
- node.js
- browser capable of running javascript
- jupyter notebook
- Amazon Elastic Compute Cloud (EC2)

Chapter 4

Planning & Formulation

4.1 Schedule for Project / Gantt Chart

The Figure 4.1 displays schedule of project through gantt chart

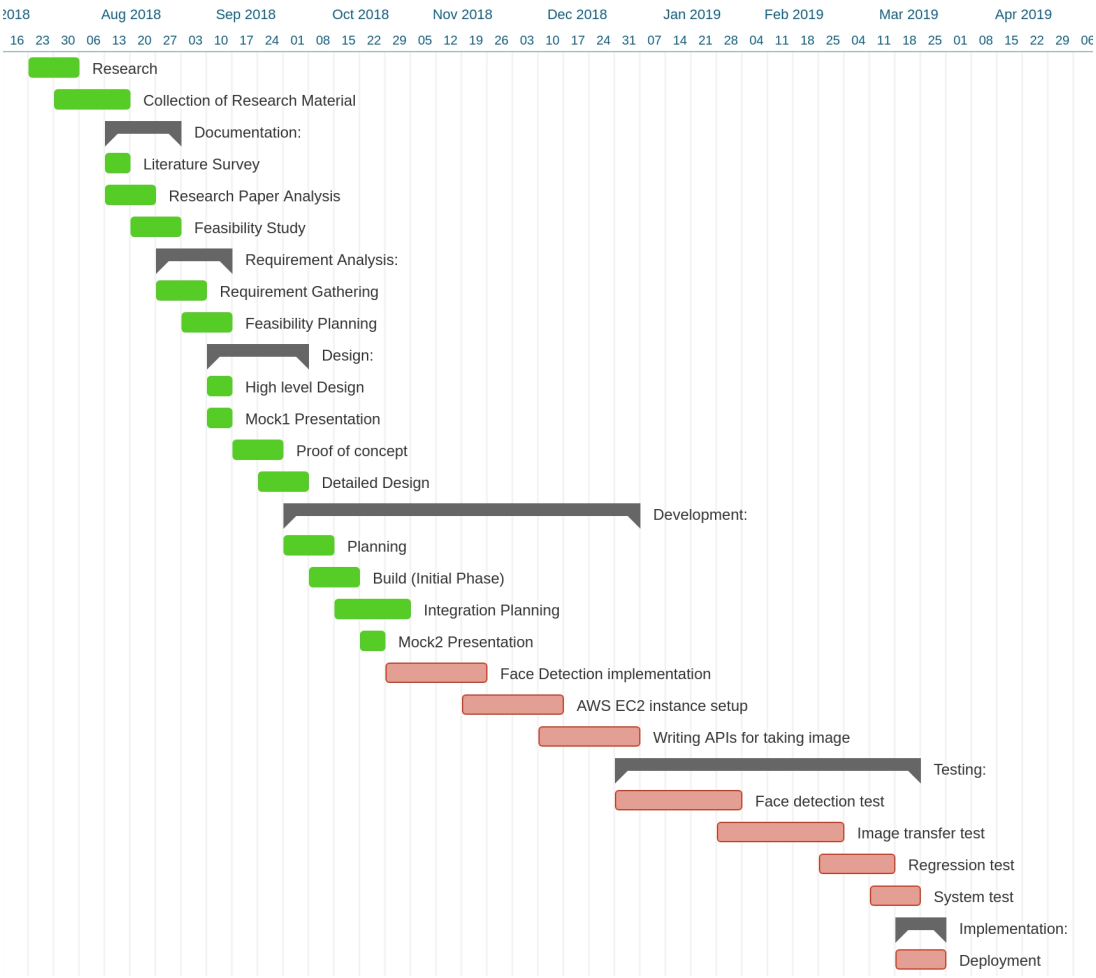


Figure 4.1: Schedule

4.2 Detailed Plan of Execution

The work plan and time schedule for the proposed project is given below. Approximately 6 months are required.

Step 1. Analysis Phase: (August 2018 to October 2018).

-Analysis of various previous modules is done to add or combine new features to the system.

Step 2. Requirement Analysis Phase: (September 2018)

-The hardware and software requirements for the system were analyzed.

Step 3. Designing Phase: (September 2018 to October 2018).

- Designing the sub modules.

Step 4. Coding and Testing Phase: (October 2018 to February 2019)

-Implementation of detailed proposal along with the testing of the modules.

Step 5. Document writing or report writing: (March 2019)

-Detailed report writing.

Chapter 5

Design of System

5.1 System Architecture

The entire system is hosted on Amazon Web Services EC2 (Elastic Compute Cloud). Figure 5.1 shows the system architecture of our face detection system.

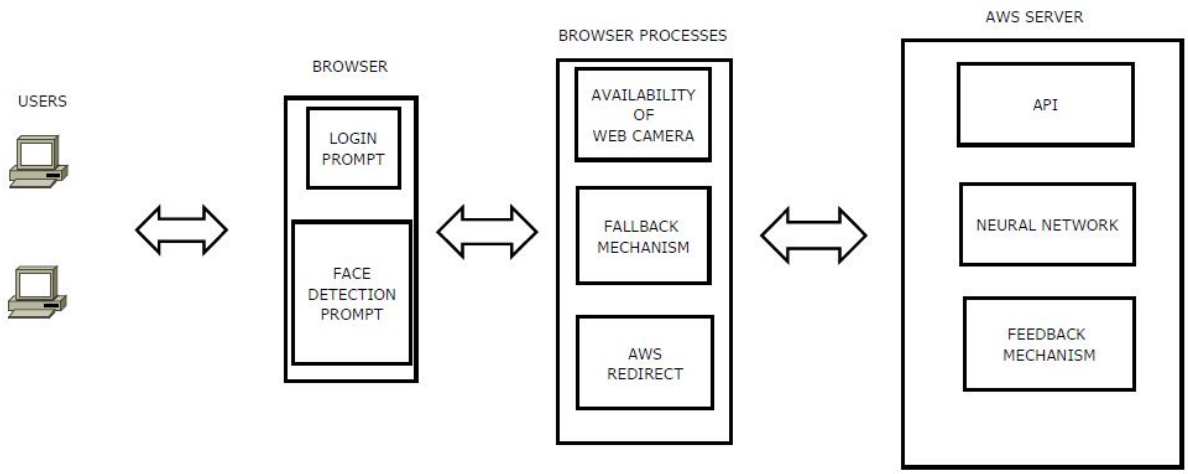


Figure 5.1: System Architecture

The system architecture in Figure 5.1 gives the conceptual model that defines the structure and behaviour of our system. It shows how the flow of the system works, along with the representation of the system. The system is structured to have 2 dependent nodes, the front end node, which takes care of capturing and bundling the image in an API and sending this image to the AWS backend. It also takes the response from the backend if the image key points were detected or not. Furthermore, if the keypoints were not detected, after a fixed set of 2 tries, the system will fall back to the original CAPTCHA implementation.

The backend is responsible to process the image and map the keypoints after capturing the API sent through the API. The backend is stored on AWS EC2 instance which allows scalability of the system if required.

5.2 Activity Diagram

The activity diagram gives the dynamic aspects of the system. Figure 5.2 displays activity diagram of this system. It shows the steps one will go through using our face detection system. The activity diagram in Figure 5.2 explains the flow and change of states as the image(data) flows through the system. It gives the activity that is being performed in every step of the system. The first thing the system does is checks if the user has access to a webcam, if he does, then the system proceeds to the next step, that is capturing the image. If the user does not have a webcam, the system falls back to captcha. After the image is captured, it is sent for processing to the backend, and the appropriate result is sent back to the backend.

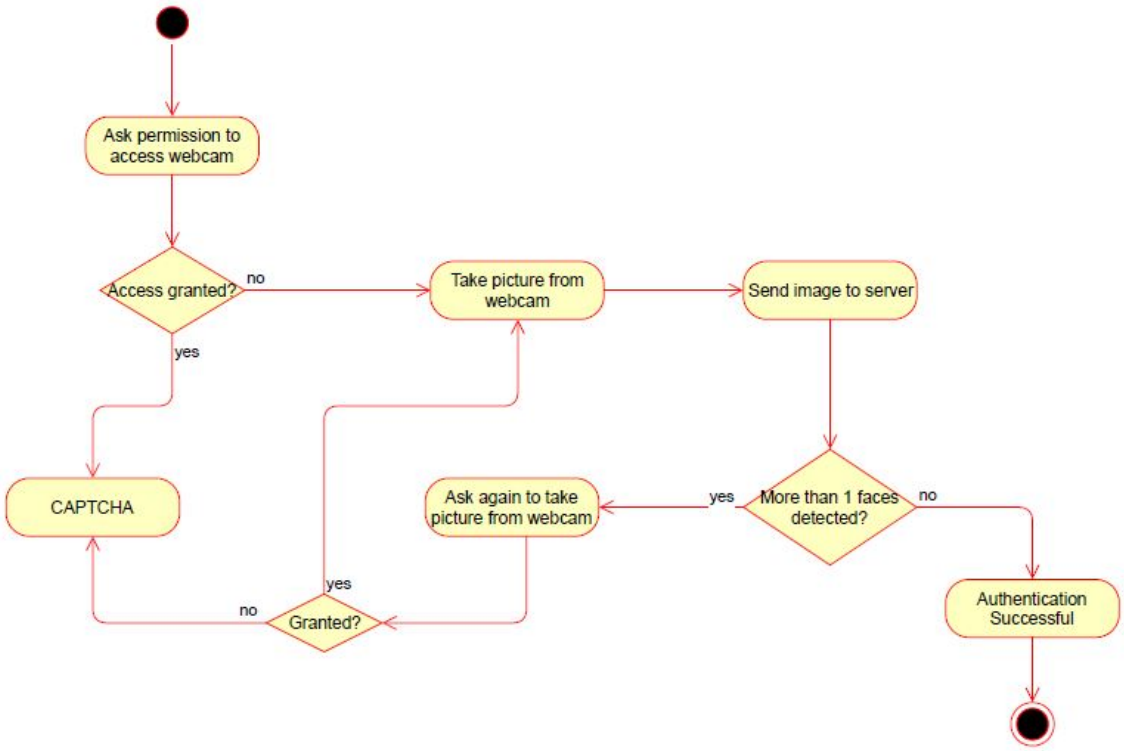


Figure 5.2: Activity Diagram

Chapter 6

Results

6.1 Results & Analysis

After performing initial tests on both the systems, using a timer function, we were able to determine a result from the time consumed for the entire process. The concluding results showed that the captcha standalone system was unreliable in terms of efficiency with respect to time. From an accuracy stand point, the CAPTCHA system was vulnerable to bots. Bots were able to figure out the various captchas and go through the security clearance without hinderance.

We conducted numerous tests on different environment. The environment variables included the lighting of the environment, the light on the face (visibility), background lighting, and internet connection. We identified that these were the variables that affected the accuracy and the success rate of the model, and fluctuating these conditions caused fluctuations in the accuracy of face detection. The Table 6.1 notes those test results for particular condition and Table 6.2 compares traditional captcha with our face recognition system.

Table 6.1: Tests and Results

Sr. No.	Environment	Result
1	Optimal : Well lit, face clearly visible, no background light, Strong internet connection.	No of tests : 15 Successful : 14 Successful in 1st attempt : 12 Successful in 2nd attempt : 2 Not successful : 1 Success percentage : 93.33
2	Good : Fairly lit, face visible, no background light, mid range internet connection.	No of tests : 15 Successful : 12 Successful in 1st attempt : 11 Successful in 2nd attempt : 1 Not successful : 3 Success percentage : 80
3	Strained : Dimly lit, face visible (low light), background lights, fair internet connection.	No of tests : 15 Successful : 8 Successful in 1st attempt : 3 Successful in 2nd attempt : 5 Not successful : 7 Success percentage : 53.33
4	Bad : Poorly lit, face blurred or blackened due to poor lighting, extreme background light, fluctuating internet connection.	No of tests : 15 Successful : 2 Successful in 1st attempt : 0 Successful in 2nd attempt : 2 Not successful : 13 Success percentage : 13.33

Table 6.2: Analysis of systems

Sr. No.	Parameters	CAPTCHA	FACE DETECTION
1.	Speed	15-42 Seconds	4-9 Seconds
2.	Accuracy	Takes attempts anywhere from 1-6	Maximum of 2 attempts
3.	Security	Provides security but vulnerable to bots	Provides more security as it is difficult to read images
2.	Optimization	No possible way for optimization	Additional image inputs will improve the accuracy of the system.
2.	Efficiency	50-90	Approximately 94

Figure 6.1 shows a sample furniture website. After the user clicks 'Buy Now' , he will be redirected to the payment page, when the image capture prompt will appear. After the user gives access through this prompt, he will be able to capture the image as shown in Figure 6.2. The user will fill the appropriate details required and will have a preview of the image he has captured which is shown in Figure 6.3. If the image captured is not as per the wish of the user, he can capture it again using the 'Take Snapshot' button in Figure 6.2. If all the keypoints are detected properly, the user will then be successfully redirected to the Thank you page in Figure 6.4, from which he will be able to go back to the shopping website. If the image keypoints were not detected, the system will allow the user to recapture and retry the process for a total of 2 times. After failing to detect the keypoints after 2 tries, the system will fallback to the original CAPTCHA implementation as shown in Figure 6.5.

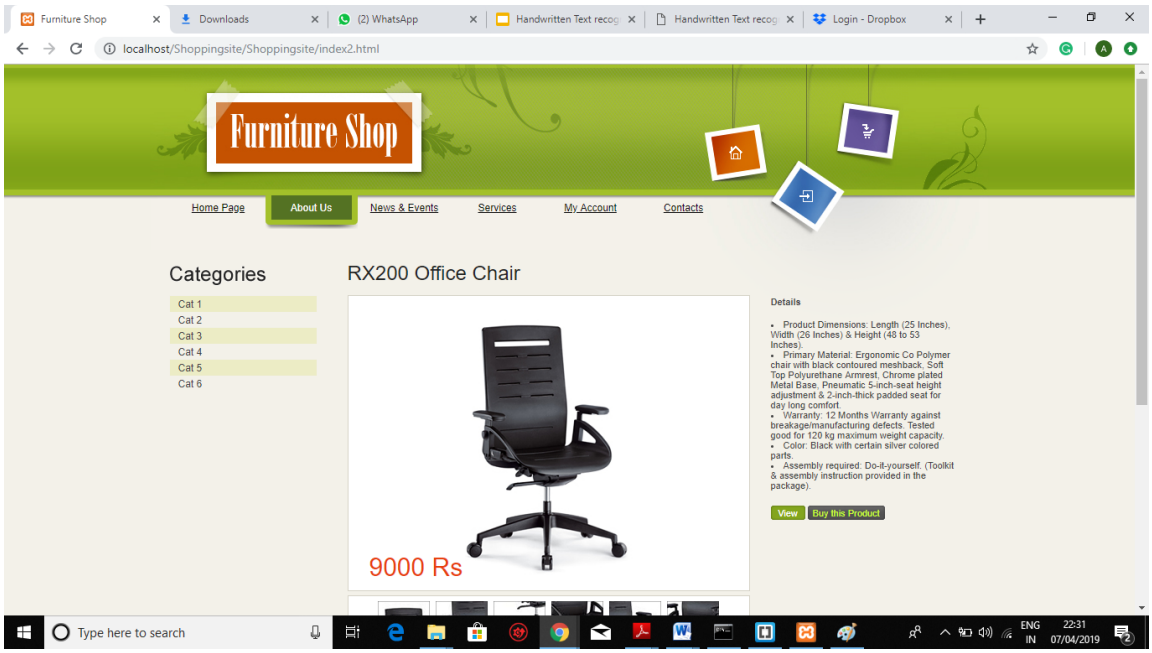


Figure 6.1: Sample e-commerce website

Figure 6.2: Webcam access

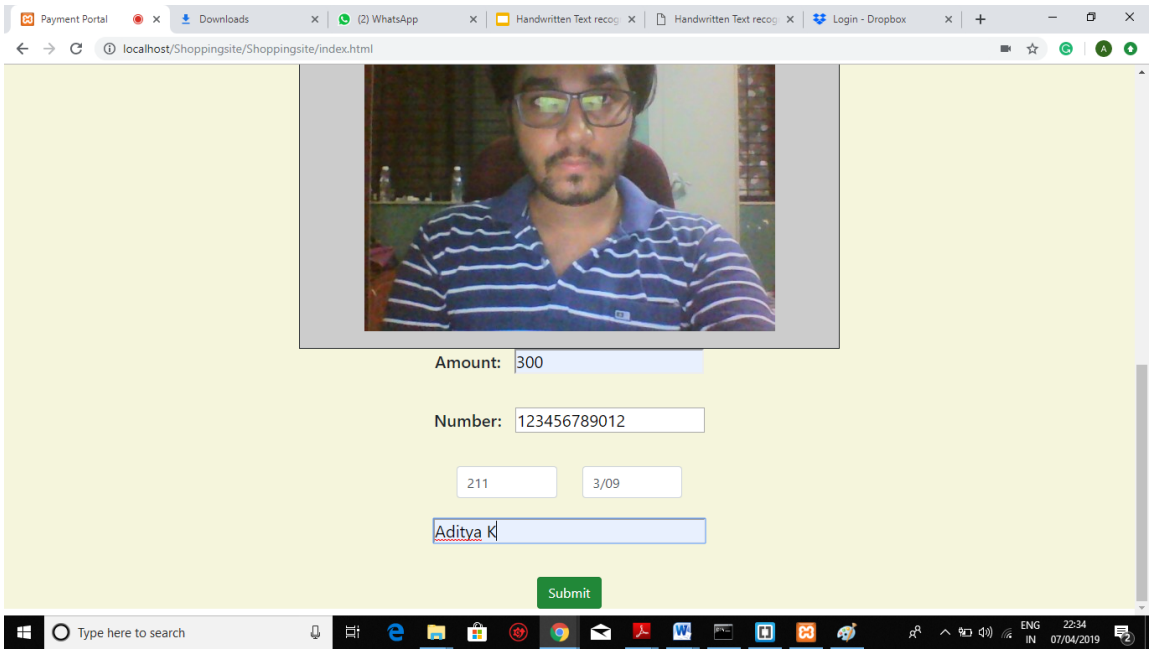


Figure 6.3: Image captured via webcam

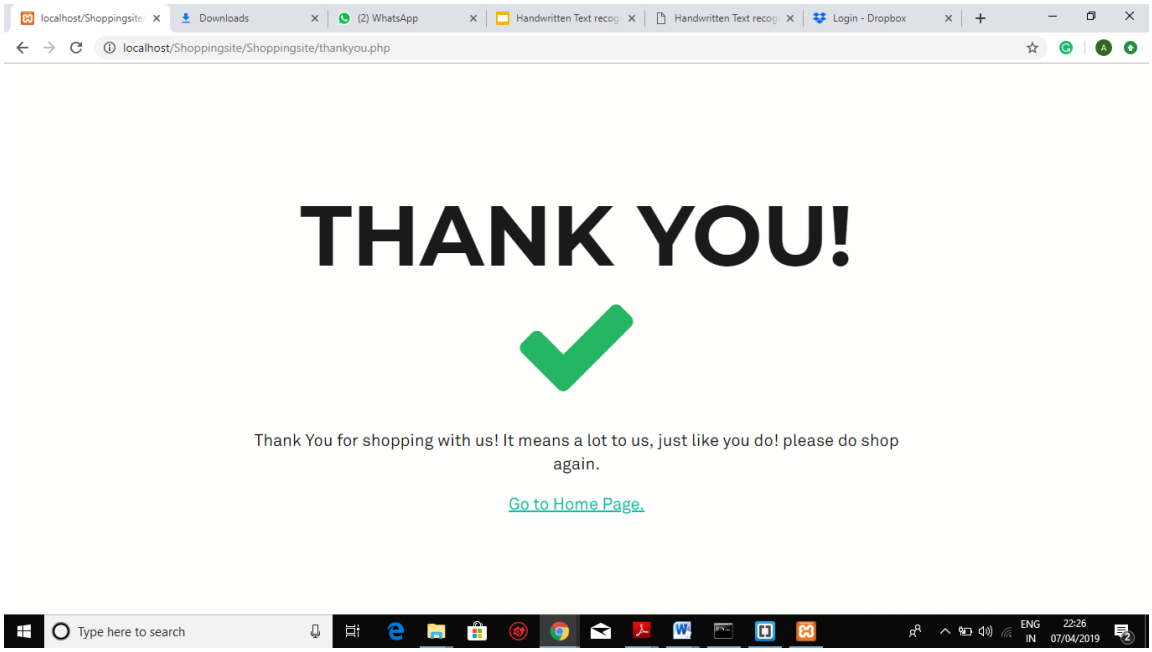


Figure 6.4: Success

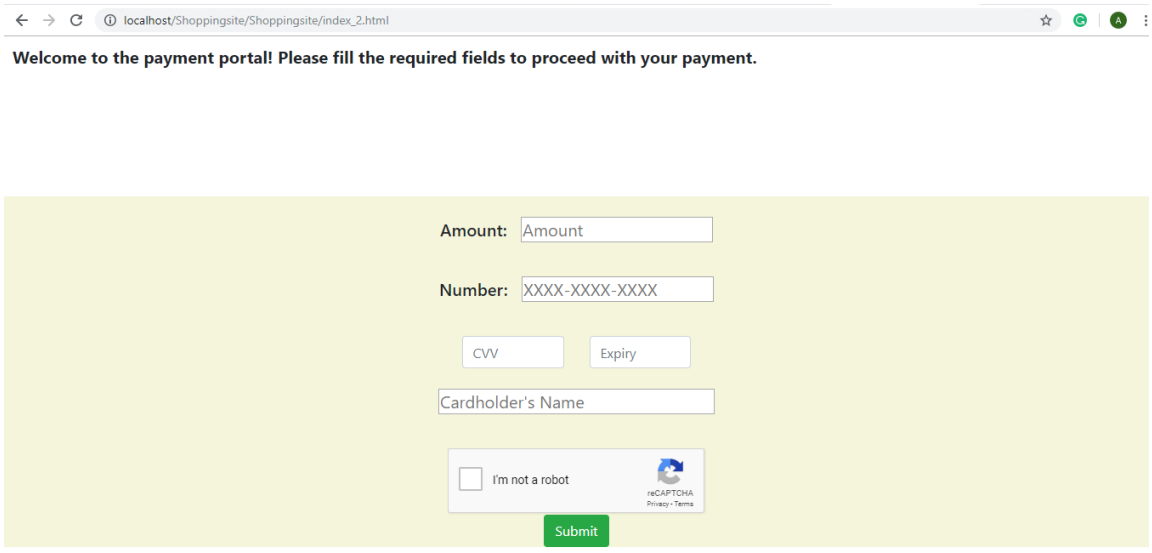


Figure 6.5: Fallback

6.2 Project Outcomes

The traditional captcha system is replaced by more secure face detection system. System will fallback to captcha if conditions required for face detection are not met. Several benefits and uses are highlighted below.

• For authentication purposes :

This system can be used for any secure authentication purposes with the base of the system being facial keypoint detection.

• Attendance System :

Besides using this online, it can be used as a biometric system for attendance which can be used in : a) Schools b) Offices

• Security System:

Face detection can be used for secure access to buildings/houses to authentic users, and can also be used as traffic camera security system.

Chapter 7

Conclusion

After conducting various tests in controlled environments, the results gathered showed that it was highly beneficial to use Face Detection in most of the cases. It provided with faster results and better accuracy and security, as it is difficult to bypass a face detection system through conventional bot development. Our system would be highly beneficial for people who are not able to solve a CAPTCHA due to unfortunate literacy incapability, and also for people suffering a language barrier on the internet.

Chapter 8

Future Work

This system can further be enhanced by using IRIS scanning as a feature. After detecting the face, the system will be able to recognise the features of the iris and give access based on this authentication. Since the features of the iris are unique, it will be a much secure detection feature.

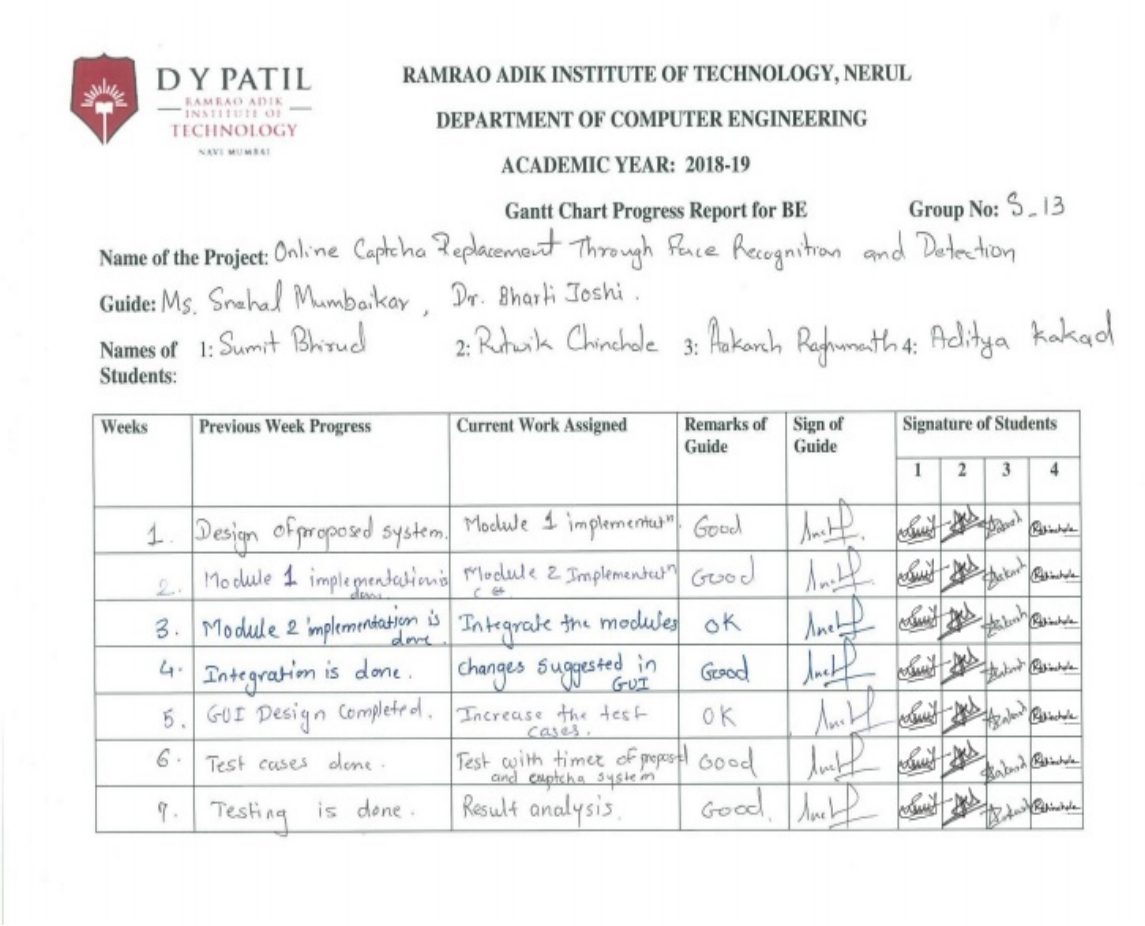
Iris Recognition is one of the important biometric recognition systems that identify people based on their eyes and iris.

Iris recognition is a method of biometric authentication, based on extraction features of the iris of an individual's eyes. Each individual has a unique iris; the variation even exists between identical twins and between the left and right eye of the same person.

Appendices

Appendix A

Weekly Progress Report



D Y PATIL
RAMRAO ADIK INSTITUTE OF TECHNOLOGY
NAVI MUMBAI

RAMRAO ADIK INSTITUTE OF TECHNOLOGY, NERUL

DEPARTMENT OF COMPUTER ENGINEERING

ACADEMIC YEAR: 2018-19

Gantt Chart Progress Report for BE **Group No:** S_13

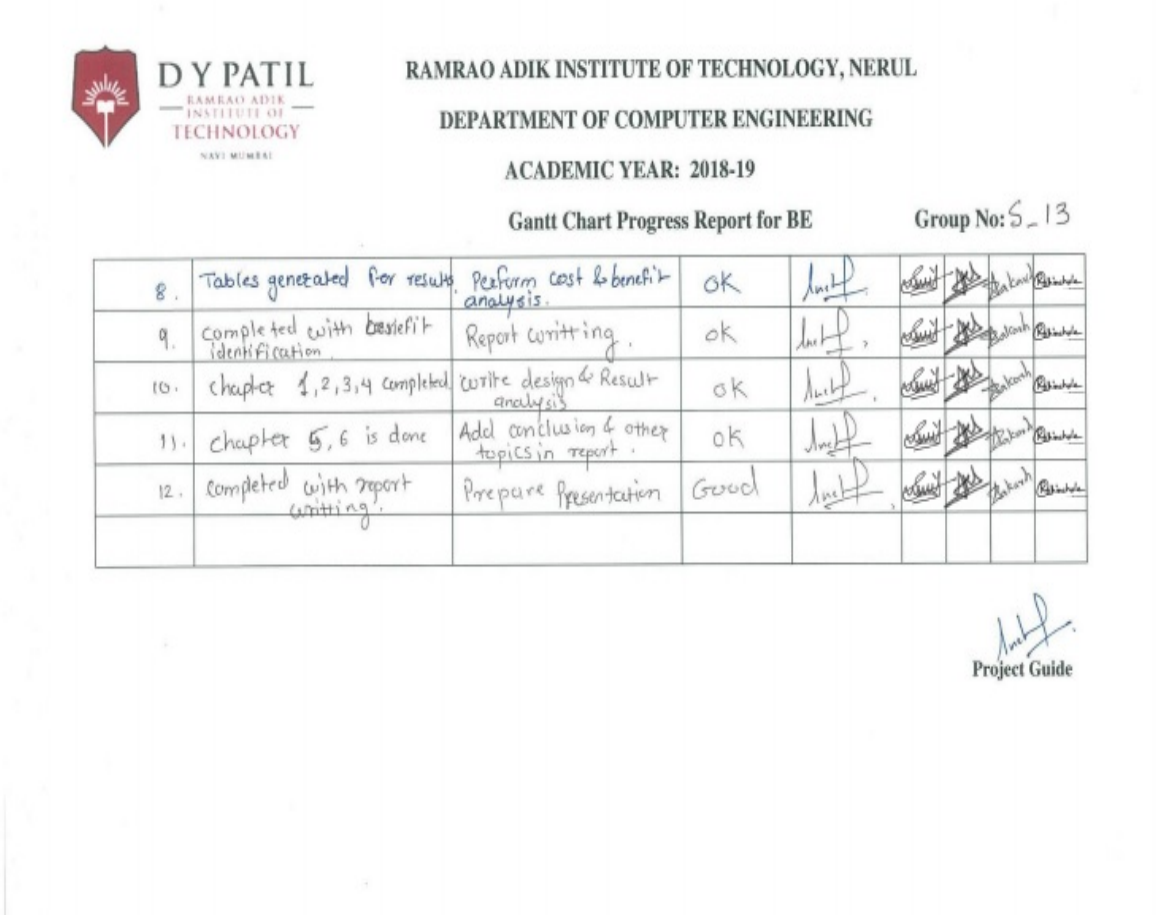
Name of the Project: Online Captcha Replacement Through Face Recognition and Detection

Guide: Ms. Snehal Mumbaikar , Dr. Bharti Joshi .

Names of Students: 1: Sumit Bhirud 2: Rutuja Chinchole 3: Aakarsh Raghunath 4: Aditya Kakad

Weeks	Previous Week Progress	Current Work Assigned	Remarks of Guide	Sign of Guide	Signature of Students			
					1	2	3	4
1.	Design of proposed system.	Module 1 implementation	Good					
2.	Module 1 implementation is done.	Module 2 Implementation	Good					
3.	Module 2 implementation is done.	Integrate the modules	OK					
4.	Integration is done.	Changes suggested in GUI	Good					
5.	GUI Design Completed.	Increase the test cases.	OK					
6.	Test cases done.	Test with timer of proposed and captcha system	Good					
7.	Testing is done.	Result analysis.	Good.					

Figure 8.1: Weekly Progress Report 1



D Y PATIL
RAMRAO ADIK INSTITUTE OF TECHNOLOGY
NAVI MUMBAI

RAMRAO ADIK INSTITUTE OF TECHNOLOGY, NERUL

DEPARTMENT OF COMPUTER ENGINEERING

ACADEMIC YEAR: 2018-19

Gantt Chart Progress Report for BE **Group No:** S_13

8.	Tables generated for result.	Perform cost & benefit analysis.	OK					
9.	completed with benefit identification.	Report writting.	ok					
10.	chapter 1,2,3,4 completed.	write design & Result analysis	ok					
11.	chapter 5, 6 is done	Add conclusion & other topics in report.	ok					
12.	completed with report writting.	Prepare Presentation	Good					

Project Guide

Figure 8.2: Weekly Progress Report 2

Appendix B

Paper Publication

The research paper is communicated to 2nd International conference on intelligent communication and computational techniques (ICCT 2019).

Online CAPTCHA replacement through Face Detection

Rutwik Chinchole, Aditya Kakad, Sumit Bhirud, Aakarsh Raghunath and Ms. Snehal Mumbaikar
University of Mumbai

Abstract – **The sensitive information stored on the internet should not be easily accessible by any unauthorized personnel, it should be readily available only to the authorized people. Thus integrity, security and confidentiality need to be maintained. There needs to be a security check before any kind of access is granted to any kind of sensitive information. CAPTCHA (Completely Automated Public Turing Test to tell Computers and Humans Apart) is a popular way for authenticating a user. The main goal of any technique is to recognize whether it is a human who is accessing the content or a robot via some recognition techniques. The advancement in recognition technologies has enabled humans to develop bots which can now bypass common authentication techniques which have been in use for a long time. CAPTCHA has been in use since a very long time and has some serious drawbacks. Facial recognition alongside with artificial intelligence can overcome drawbacks like difficulty in solving, ambiguity, and sometimes easy prey for trained bots of CAPTCHA and can easily replace it.**

Index Terms – CAPTCHA, RESTful API, Face Detection, Key points, Accuracy.

1. INTRODUCTION

CAPTCHA means Completely Automated Public Turing Test to tell Computers and Humans Apart. Recognizing both familiar and unfamiliar faces is what humans are good at and that has been established [1], [2]. The CAPTCHA method can be easily replaced by Facial Recognition proposed in this paper.

For differentiating humans captcha focuses on providing the user with different tests[3]. Various services including web and financial services use Captchas to provide security measures against malicious attacks. OCR (Optical Character Recognition Manual) was used to extract text in AltaVista Captcha with distortions known to reduce incorporated OCR accuracy[4]

CAPTCHA is nearing its end and is in serious need to be replaced. Specialized tests like Handwritten character recognition and image or pattern recognition tests are used to determine is it really a human who needs to access the data[5]. Captcha has various forms and each one has a unique way of identifying. Although CAPTCHA has a series of tests to determine the differences it has some real serious drawbacks which can be overcome by using various efficient alternatives. In this paper we propose a technique of using Facial Recognition to detect whether it's a human or a robot accessing the content.

2. CURRENT SYSTEM AND LIMITATIONS

CAPTCHA is a system which can date back to the twentieth century, One question was needed to be answered by Alan Turing - Can Human thinking be mimicked by computer? The goal of any CAPTCHA system is to make challenges and ask questions such that the computers won't be able to pass them but humans can easily get through with it. Various types of Captcha were evolved during its usage and each one introduced some new challenges along with various limitations which can be seen below[7].

Sr. No	Existing Systems	Limitations
1	Honeypot	The form can be mistakenly filled by a human. Once a bot figures out that the form does not need to be filled, it will learn and overcome.
2	TextCAPTCHA	It asks a simple question, which can easily be answered by an NLP bot, rendering it extremely unsafe.
3	Reject Submission	If the form is small and the user has enabled auto-fill extension on the browser, this form will always reject the input.
4	Math Question	NLP bots can easily solve the math problem with the advancement in IBM Watson.

Table 1. Existing system limitations

3. PROPOSED WORK

A computer program or system intended to distinguish human from bot/machine input, typically as a way of automated extraction of data from websites and thwarting spam. This is done with help of CAPTCHA. An algorithm that cracks CAPTCHAs with 90-99.8 percent accuracy is also claimed. Therefore to improve on the security, process of online CAPTCHA verification for websites need to replace which is used to identify whether the access to the website is by a human or through a bot and to rectify issues with the current captcha technology. The face recognition technique is an alternative solution for this[6].

4. PROPOSED SYSTEM FLOW

The image in Figure 1 shows the simple system architecture the proposed face detection system employees, with the entire system stored on aws for wide availability.

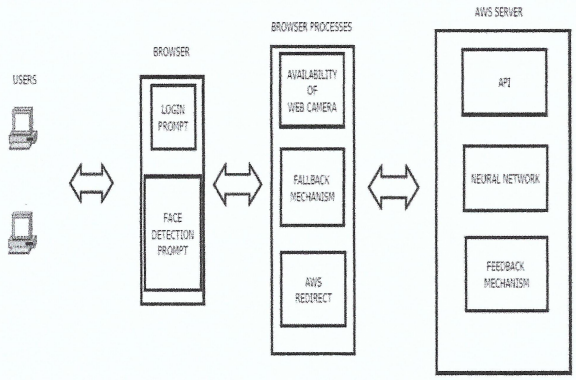


Figure 1. System Architecture

1. First we prompt the user for the verification process.
2. The user allows the image to be captured from the web camera.
3. Once the image is captured, and all the other details are verified, the image is sent to the backend using an API. The RESTful API is used to send the image through the http protocol.
4. Once the image is received in the backend (AWS), the face detection code starts to implement.
5. First the number of faces in the image is detected.
6. If the numbers of faces are greater than 1, prompt is given to the user to capture another image. This is for security reasons that only a single face will be used for authentication.
7. On the successful face detection further access granted.
8. If the face detection is unsuccessful, user will get prompt for another attempt.
9. The number of attempts is restricted to 2 in our system. After this, the regular captcha system will be implemented for the user.
10. In case of unavailability of the web camera/front camera, the system will automatically fall back onto the captcha system.

5. PROCESS USED FOR FACE RECOGNITION

The face detection process is having multiple stages as described below.

5.1 Detect Faces Using a Haar Cascade Classifier

- We have used OpenCV's implementation of Haar feature-based cascade classifiers to detect human faces in images. OpenCV provides many pre-trained face detectors, stored as XML files.

5.2 Add Eye Detections

- A Haar-cascade eye detector can be included in the same way that the face detector was. This allows the image under detection to include eyes as a keypoint for verification.

5.3 De-noise an Image for Better Face Detection

- Using OpenCV's built in color image de-noising functionality called fastNlMeansDenoisingColored -we de-noise this image enough so that all the faces in the image are properly detected. Once we have cleaned the image, we run our trained face detector over the cleaned image to check out its detections.

5.4 Create a CNN to Recognize Facial Keypoints

- We notice that facial key point detection becomes a regression problem at high levels when we include 15 key points, thus we employ a convolutional neural network to recognize the patterns in the images.

- We need to train a regressor, and for that, we need a training set of images, a set of facial images and keypoint pairs to train on. We use this dataset from Kaggle.

Figure 2. Visualization of the subset of training data.

5.5 Compile and Train the Model

- Figure 2 shows the visualization of training data and after we visualize the data and check that the correct keypoints are being mapped, we start to train the model
- We first experiment with the choice of optimizer to use. After testing, the best fitting optimizer is the Adam, which we implement. We use the 'fit' method to train the model.

5.6 Visualize the Loss and Test Predictions

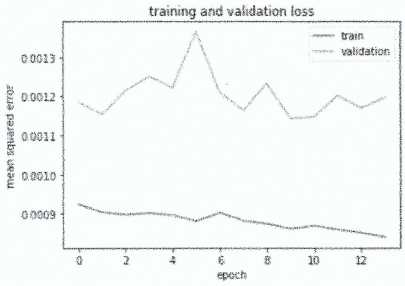


Figure 3. Training and Validation Loss

- We plot the training and validation loss data as shown in Figure 3 to check where the model starts to overfit or underfit.
- This would help us to determine the number of epochs and manipulating the dropout layers to avoid over fitting and underfitting the model.

5.7 Visualize a Subset of the Test Predictions

- For each training image, there are two landmarks per eyebrow (four total), three per eye (six total), four for the mouth, and one for the tip of the nose.
- The below Figure 4 shows visualization of predictions on test data

Figure 4: Visualization of test predictions.

6. RESULTS AND ANALYSIS

After performing initial tests on both the systems, using a timer function, we were able to determine a result from the time consumed for the entire process. The concluding results showed that the captcha standalone system was unreliable in terms of efficiency with respect to time. From an accuracy stand point, the CAPTCHA system was vulnerable to bots. Bots were able to figure out the various captchas and go through the security clearance without hinderance.

We conducted numerous tests on different environment. The environment variables included the lighting of the environment, the light on the face (visibility), background lighting, and internet connection. We identified that these were the variables that affected the accuracy and the success rate of the model, and fluctuating these conditions caused fluctuations in the accuracy of face detetction.

Sr. No	Environment	Result
1	Optimal : Well lit, face clearly visible, no background light, Strong internet connection.	No of tests : 15 Successful : 14 Successful in 1st attempt : 12 Successful in 2nd attempt : 2 Not successful : 1 Success percentage : 93.33
2	Good : Fairly lit, face visible, no background light, mid range internet connection.	No of tests : 15 Successful : 12 Successful in 1st attempt : 11 Successful in 2nd attempt : 1 Not successful : 3 Success percentage : 80
3	Strained : Dimly lit, face visible (low light), background	No of tests : 15 Successful : 8

	lights, fair internet connection.	Successful in 1st attempt : 3 Successful in 2nd attempt : 5 Not successful : 7 Success percentage : 53.33
4	Bad : Poorly lit, face blurred or blackened due to poor lighting, extreme background light, fluctuating internet connection.	No of tests : 15 Successful : 2 Successful in 1st attempt : 0 Successful in 2nd attempt : 2 Not successful : 13 Success percentage : 13. 33

Table 2. Tests and Results

Sr No.	Parameters	CAPTCHA	FACE DETECTION
1.	Speed	**15-42 Seconds**	**4-9 Seconds**
2.	Accuracy	**Takes attempts anywhere from 1-6.**	**Maximum of 2 attempts.**
3.	Security	**Provides security but vulnerable to bots.**	**Provides more security as it is difficult to read images**
4.	Optimization	**No possible way for optimization**	**Additional image inputs will improve the accuracy of the system.**
5.	Efficiency	**50-90%**	**Approximately 94%**

Table 3. Analysis of the systems

The tests to determine the accuracy of the system were based on variables that influenced the face detection. The main variable which we figured out were environment lighting, how well the face was lit, and how good the internet connection sustained. The best case scenario took the accuracy up to 94%, with access provided in as little as 4 seconds. In a fairly lit environment, the accuracy dropped a little but still gave a high percentage of 80, with time required anywhere from 4 to 10 seconds. This was faster than the CAPTCHA systems in place.

7. CONCLUSION

After conducting various tests in controlled environments, the results gathered showed that it was highly beneficial to use Face Detection in most of the cases. It provided with faster results and better accuracy and security, as it is difficult to bypass a face detection system through conventional bot development. Our system would be highly beneficial for people who are not able to solve a CAPTCHA due to unfortunate literacy incapability, and also for people suffering a language barrier on the internet.

8. REFERENCES

[1] H. Lamba, A. Sarkar, M. Vatsa, R. Singh, and A. Noore. Face recognition for look-alikes: A preliminary study. In Proceedings of the International Joint Conference on Biometrics, pages 1–6, 2011.

[2] P.Sinha,B.Balas,Y.Ostrovsky,andR.Russell.Facerecognition by humans: Nineteen results all computer vision researchers should know about. Proceedings of the IEEE, 94(11):1948 –1962, 2006.

[3] The official captcha site. http://www.captcha.net.

[4] K. Kluever. Evaluating the usability and security of a video captcha. Master's thesis, Rochester Institute of Technology, 2008.

[5] A. Rusu and V. Govindaraju. Handwritten captcha: Using the difference in the abilities of humans and machines in reading handwritten words. In Proceedings of the 9th International Workshop on Frontiers in Handwriting Recognition, pages 226–231, 2004.

[6] L. von Ahn, B. Maurer, C. McMillen, D. Abraham, and M. Blum. recaptcha: Human-based character recognition via web security measures. Science, 321:1465–1468, 2008

[7] May, Matt (2005-11-23). "Inaccessibility of CAPTCHA". W3C. Retrieved 2015-04-27.

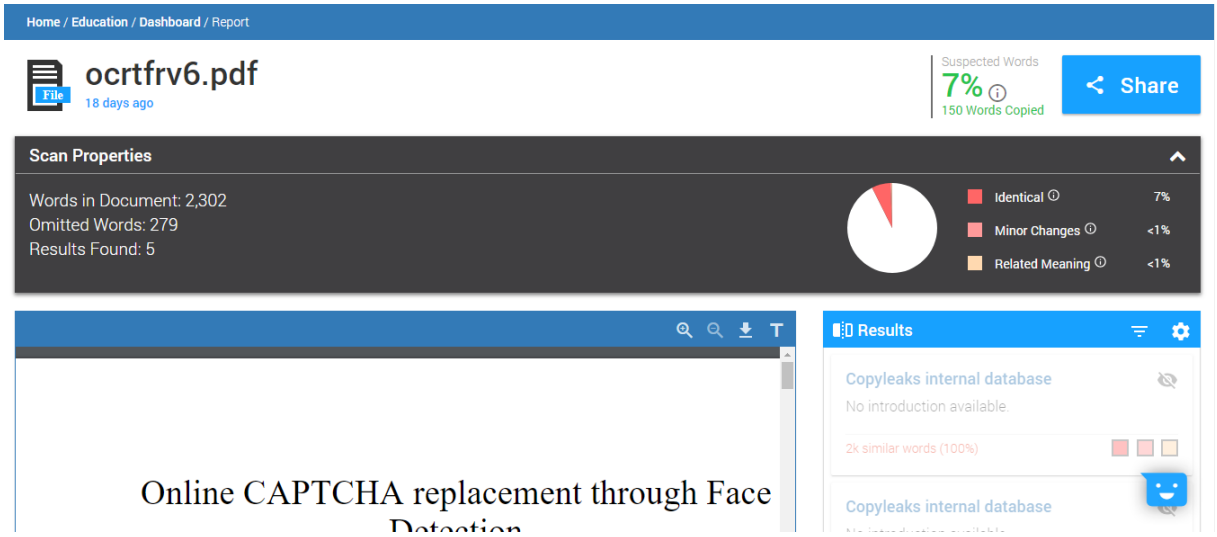


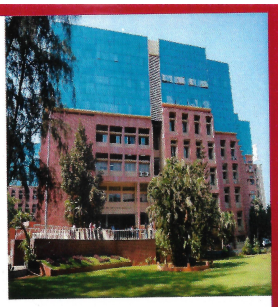
Figure 8.3: Plagiarism Report

Appendix C

Project Competition

Participated in Srijan a national level project competition organized by Ramrao Adik Institute of Technology, Nerul on April 3rd, 2019.

D Y PATIL
RAMRAO ADIK INSTITUTE OF TECHNOLOGY
NAVI MUMBAI



National Level Project Competition

Srijan-2019

Certificate of Participation

This is to certify that Mr./~~Ms.~~ SUMIT BHIRUD has participated and presented the project titled ONLINE CAPTCHA REPLACEMENT USING FACE DETECTION in *"National Level Project Competition Srijan-2019"* conducted under **Technovate-2019**.

This competition was organized by Ramrao Adik Institute of Technology on April 3rd, 2019.

Dr. Leena Ragha
Coordinator

Dr. Ramesh Vasappanavara, PhD.
Principal, RAIT

www.rait.ac.in

D Y PATIL
RAMRAO ADIK INSTITUTE OF TECHNOLOGY
NAVI MUMBAI

National Level Project Competition
Srijan-2019

Certificate of Participation

This is to certify that Mr./~~Ms.~~ ADITYA KAKAD
has participated and presented the project titled ONLINE CAPTCHA REPLACEMENT THROUGH FACE DETECTION
in *"National Level Project Competition Srijan-2019"* conducted under **Technovate-2019**.

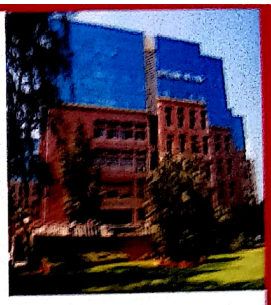
This competition was organized by Ramrao Adik Institute of Technology on April 3rd, 2019.

Dr. Leena Ragha
Coordinator

Dr. Ramesh Vasappanavara, PhD.
Principal, RAIT

www.rait.ac.in

D Y PATIL
RAMRAO ADIK INSTITUTE OF TECHNOLOGY
NAVI MUMBAI



National Level Project Competition

Srijan-2019

Certificate of Participation

This is to certify that Mr./Ms. AAKARSH RAGHUNATH has participated and presented the project titled ONLINE CAPTCHA REPLACEMENT THROUGH FACE DETECTION in *"National Level Project Competition Srijan-2019"* conducted under **Technovate-2019.**

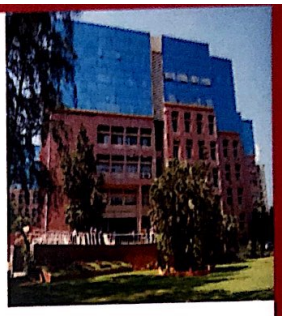
This competition was organized by Ramrao Adik Institute of Technology on April 3rd, 2019.

Dr. Leena Ragha
Coordinator

Dr. Ramesh Vasappanavara, PhD.
Principal, RAIT

www.rait.ac.in

D Y PATIL
RAMRAO ADIK INSTITUTE OF TECHNOLOGY
NAVI MUMBAI



National Level Project Competition

Srijan-2019

Certificate of Participation

This is to certify that Mr./~~Ms.~~ RUTWIK CHINCHOLE has participated and presented the project titled ONLINE CAPTCHA REPLACEMENT THROUGH FACE DETECTION in *"National Level Project Competition Srijan-2019"* conducted under **Technovate-2019**.

This competition was organized by Ramrao Adik Institute of Technology on April 3rd, 2019.

Dr. Leena Ragha
Coordinator

Dr. Ramesh Vasappanavara, PhD.
Principal, RAIT

www.rait.ac.in