PROJECT REPORT ON
Facial Recognition Attendance Manager

Submitted in partial fulfilment of the requirement of the degree of

Bachelor in Technology
In
Information Technology

By,

Abir Bhattacharya   16500219064
Arkamitra Mukherjee   16500219055
Padma Chhatait   16500219039
Anusweta Das   16500219056
Basudhara Mitra   16500219050

Under the supervision of
Ms. Tuhina Sinha
Assistant Professor of Department of Information Technology

Calcutta Institute of Engineering and Management
Department of Information Technology
Kolkata, West Bengal, India – 700040

<u>Certificate of Approval</u>

This project report is entitled by "Facial Recognition Attendance Manager" prepared by, Abir Bhattacharya, Arkamitra Mukherjee, Padma Chhatait, Anusweta Das and Basudhara Mitra, is approved and certified for the degree of "Bachelor of Technology" in "Information Technology" for which it has been submitted.

(Mr. Samir Biswas)
Head of the Department
Information Technology
Date:

(Mrs. Tuhina Sinha)
Assistant Professor
Information Technology
Date:

Declaration

We hereby declare that the project work being presented in the project proposal entitled "Facial Recognition Attendance Manager" in partial fulfilment of the requirements for the award of the degree of **Bachelor of Technology in Information Technology** at **Calcutta Institute of Engineering and Management** is an authentic work carried out under the guidance of Ms Tuhina Sinha. The matter embodied in this project work has not been submitted elsewhere for the award of any degree of our knowledge and belief.

Date: 23-10-2022

Name of Students
1. Abir Bhattacharya
2. Arkamitra Mukherjee
3. Padma Chhatait
4. Basudhara Mitra
5. Anusweta Das

Signature of Students

    1. _____

    2. _____

    3. _____

    4. _____

    5. _____

Certificate

It is certified that the work contained in the project titled "Facial Recognition Attendance Manager" by Abir Bhattacharya, Arkamitra Mukherjee, Padma Chhatait, Anusweta Das and Basdudhara Mitra, has been successfully carried out under my supervision and that this work has not been submitted elsewhere for a degree.

Signature of Supervisor(s)
Name: Mrs. Tuhina Sinha
Department of Information Technology
Calcutta Institute of Engineering and Management
Date:

Acknowledgement

I am honoured to have the opportunity to express my heartfelt gratitude to all those who have supported me in the successful completion of my final year project on facial recognition attendance management. I would like to begin by expressing my sincerest appreciation to our Project Mentor, Ms Tuhina Sinha, for her invaluable guidance, encouragement, and support throughout the project. Her expertise and insight have been instrumental in helping me navigate through the various challenges and complexities of the project, and I am grateful for their unwavering commitment to my success.

I would also like to extend my deepest appreciation to the faculty members of Calcutta Institute of Engineering and Management for their guidance and support throughout my academic journey. Their teachings have provided me with a strong foundation of knowledge, skills, and values, which have been critical in shaping my perspective and approach to this project.

Finally, I would like to express my appreciation to all those who have contributed to the successful completion of this project, including my classmates, colleagues, and anyone else who has provided support in any form. I am grateful for your invaluable contributions, which have played a significant role in the successful completion of this project. Thank you all for your unwavering support, and I look forward to continued collaboration and learning opportunities in the future.

Contents

Abstract

The attendance system has developed into a clever and effective approach to monitor attendance for a group of people. In the past, maintaining hard copy attendance registers which took time and were prone to mistakes was one of the manual methods used for managing attendance. However, thanks to the technological revolution, attendance management is now more simplified and practical.

Tracking attendance has been made much easier with the development of software tools like Microsoft Excel, Google Sheets, and other spreadsheet programmes. The automatic computations, data validation, and data sorting capabilities of these spreadsheet applications have improved the accuracy and effectiveness of attendance management. Additionally, these software options make it simple to enter, customise, and analyse data, which makes it straightforward for organisations to handle attendance data for a large number of people.

The use of spreadsheet- and database-based attendance systems has replaced manual attendance registers with systems that are more accurate, dependable, and efficient. Automated attendance systems minimise manual data entry and offer real-time access to attendance data, which has decreased administrative costs and increased productivity.

Attendance systems provide benefits to individuals in addition to organisations. For people to register their attendance, examine their attendance history, and get automated notifications, they offer a user-friendly interface. This encourages accountability and gives people the power to own up to their attendance.

Introduction

A facial recognition system is a system which is capable of detecting a human face from a given image or video. It primarily works by detecting facial landmarks on a face and comparing it with the predefined landmarks of an image in the database. [1]

Broadly the Steps of Facial Recognition can be classified into four parts:

1) Representing the Image on a 2D graph: Representing an image on a 2D graph is one of the most fundamental steps in image processing. It is the process of mapping an image's pixel values onto a 2D plane, where each pixel's coordinates represent its location in the image. This representation enables a range of image processing techniques, such as filtering, segmentation, and feature extraction.
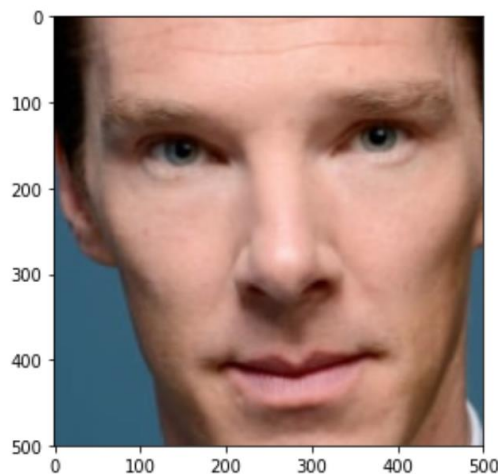

[2] Actual Image

2) Detecting Landmarks: Facial landmarks are typically determined by the help of predefined features such as the nose, eyes, lips, and chin. These features act as reference points that can be located on a face image, allowing for the identification of the position of different facial landmarks. However, identifying these features is completely based on a set of datasets that contain values in the form of a 2D matrix defining how a human facial feature would generally look like. These datasets are usually created by manually annotating a large number of facial images with the corresponding landmarks.
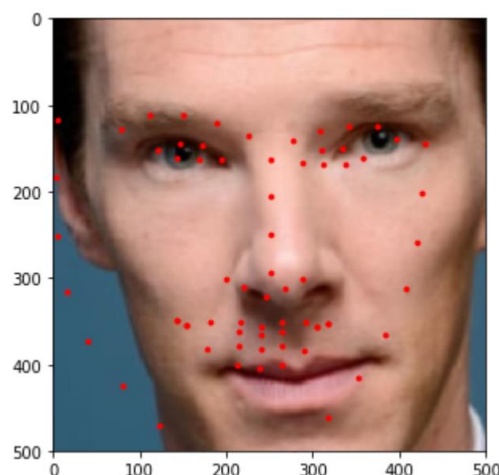
[2] Image with Landmarks

3) Generating Blueprint of Face: After the facial landmarks are identified and located on an image, the next step in facial recognition is to generate a blueprint of the face. The blueprint is created by connecting the dots of the facial landmarks using mathematical algorithms. The resulting structure is unique for each individual, except for identical twins in some cases. The blueprint of the face is commonly referred to as a facial template or face print. It contains important information about the geometry of the face, including the distance between different facial features and the angles at which they are positioned. This information is used to create a digital representation of the face, which is then compared to a database of face prints to identify the person. The accuracy of the facial recognition process heavily relies on the quality of the faceprint. Therefore, it is crucial to ensure that the facial landmarks are correctly identified, and the blueprint is accurately generated. Factors such as lighting conditions, facial expressions, and occlusions, such as glasses or hats, can affect the accuracy of the face print.
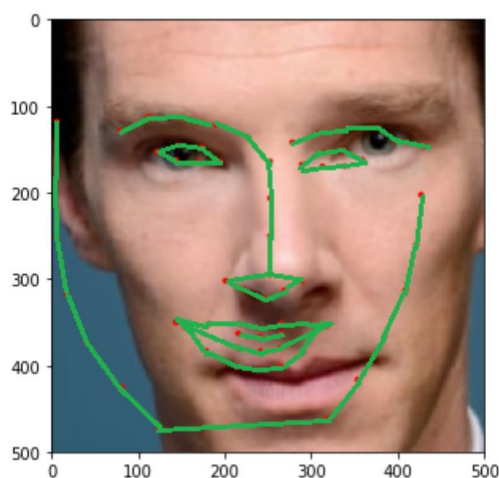
[2] Blueprint of the Image

4) Comparison: The final step in facial recognition is comparing the generated facial template with the faceprints stored in the database. The faceprint obtained from the new image is compared with all the other faceprints in the database to find the closest match possible. The process involves calculating the distance between the facial template and the faceprints in the database and selecting the one with the smallest distance.

The accuracy of the facial recognition process depends on the quality of the facial templates and the size and diversity of the database. A larger and more diverse database increases the chances of finding a match and improving the accuracy of the process. In most cases, a matching accuracy of more than 70-80% is considered reliable and is used as a threshold for positive identification.

Aims and Objective

The project aims to create a system that can automate the process of taking attendance in a classroom. This system will provide a more efficient way for teachers to take attendance, reducing the time and effort required to complete this task. The following are the objectives of the project:

1. Login portion for the Teacher who is going to give attendance to students of a particular department:

The first objective is to create a login system for teachers. This will allow only authorized teachers to access the attendance system. Teachers will be able to log in using their unique credentials, such as their department id and password. Once logged in, they will have access to the attendance system.

2. Uploading of the Image of the class taken during the class:

The second objective is to allow the teacher to upload an image of the classroom taken during the class. This image will be used to detect the faces of the students present in the class. The teacher can use any camera device such as a phone camera or any other camera. Once the image is uploaded, the system will start processing it.

3. Detecting all the faces present in the class:

The third objective is to detect all the faces present in the uploaded image. The system will use machine learning algorithms such as Eigen Vectors to detect the faces. The system will be designed to handle multiple faces in the image. For the purpose of the project we will be using the face-api-js api[3] which is built using Eigen Vector detection of faces.

4. Identifying the student's faces who belong to that class:

The fourth objective is to identify the faces of students who belong to that particular class. The system will compare the detected faces with the images of students in the database to identify which students are present in the class. If the system identifies a student, it will mark them as present in the attendance.

5. Submitting the attendance for those student in the database:

The final objective is to upload the student's present status along with the name of the class and date. The server will be taking the data and adding them accordingly in the database.

In conclusion, the attendance system will provide an efficient way for teachers to take attendance in the classroom. It will reduce the time and effort required to complete this task and provide accurate attendance data. The system will be designed to handle multiple classes, and the data can be used for administrative purposes. Overall, this project will be a valuable addition to the education system, making the attendance process more efficient and effective.

Literature Review

Facial recognition is a way of identifying or confirming an individual's identity using their face. It is a category of biometric security. The technology is mostly used for security and law enforcement, though there is increasing interest in other areas of use. The technology is used for a variety of purposes. These include:

1. Unlocking phones

Facial recognition technology has become increasingly prevalent in recent years, with its applications ranging from security and law enforcement to personal device authentication. One such application is the use of facial recognition technology to unlock mobile devices such as smartphones. Apple, one of the leading technology companies, has integrated facial recognition technology into their latest iPhone models, providing a new level of security for users. The face recognition technology used in Apple's iPhones relies on a complex algorithm that analyses the unique features of a person's face, such as the distance between their eyes and the shape of their nose. This algorithm creates a mathematical model of the user's face, which is then stored on the device as a reference for future authentication attempts. When the user attempts to unlock their phone, the device's camera captures an image of their face and compares it to the stored reference model to determine if the user is authorized to access the device. Apple claims that the chance of a random face unlocking an iPhone is about one in 1 million, making the technology highly secure. However, some experts have expressed concerns about the potential for false positives or false negatives, which could lead to unauthorized access or denied access for legitimate users. Despite these concerns, facial recognition technology has become an increasingly popular method of authentication for mobile devices. It offers a fast and convenient way for users to unlock their devices without the need for a password or PIN code. Additionally, it provides a higher level of security than traditional methods, as it is much more difficult for someone to impersonate another person's face than it is to guess a password or PIN code. [6]

2. Law enforcement

Facial recognition technology has become a controversial topic, particularly when it comes to its use by law enforcement agencies. The technology has been adopted by many police departments around the world, claiming that it can help them to identify and apprehend criminals. However, there are growing concerns over the accuracy and potential misuse of the technology. According to a report by NBC, facial recognition technology is becoming increasingly popular among law enforcement agencies in the United States. The report suggests that over 50% of American adults are already in a law enforcement facial recognition database, with the technology being used for a variety of purposes such as identifying

suspects in criminal investigations, tracking missing persons, and monitoring public gatherings. The use of facial recognition technology by law enforcement agencies is not limited to the United States. Many countries around the world have also adopted this technology, including China, which has one of the most extensive surveillance systems in the world. In China, facial recognition technology is used for a range of purposes, including monitoring public gatherings, tracking individuals, and identifying suspects in criminal investigations. Despite its growing popularity, the use of facial recognition technology by law enforcement agencies has been met with criticism from civil rights groups and privacy advocates. Concerns have been raised about the accuracy of the technology, particularly when it comes to identifying individuals from ethnic minority groups. There have also been concerns about the potential misuse of the technology, including its use for mass surveillance and the infringement of individuals' privacy rights.

3. Airports and border control

Facial recognition technology is becoming increasingly popular at airports around the world. With the rise in air travel, there has been a growing need to streamline the airport experience and make it more efficient. Facial recognition technology offers a solution to this problem, allowing airports to speed up the check-in and security processes while also improving security. One of the most significant developments in the use of facial recognition technology at airports is the introduction of biometric passports. These passports contain a microchip that stores the holder's biometric data, including their facial image. This data can then be used to verify the traveller's identity at automated e-Passport control points, which are now present at many airports worldwide. The use of facial recognition technology at airports has several benefits. For travellers, it means that they can avoid long queues and reach their gates faster. It also provides a more seamless and convenient experience, reducing stress and anxiety levels associated with travel. For airports, it means that they can process travellers more quickly and efficiently, allowing them to handle higher volumes of passengers. Facial recognition technology also offers improved security at airports. By using facial recognition to verify travellers' identities, airports can more accurately screen for individuals who may pose a security risk. This can help to prevent potential threats and improve overall safety and security for all travellers. However, the use of facial recognition technology at airports has also been met with criticism from privacy advocates. Concerns have been raised about the potential misuse of biometric data, including the risk of data breaches and the possibility of facial recognition being used for surveillance purposes. [8]

4. Banking

Biometric online banking using facial recognition is rapidly gaining popularity as a secure and convenient way for customers to access their accounts and authorize

transactions. With traditional authentication methods such as passwords and one-time passwords becoming increasingly vulnerable to hacking and phishing attacks, facial recognition offers a more secure alternative. By using facial recognition, customers can simply look at their smartphone or computer to authenticate themselves, without the need for complex passwords that can be easily compromised. This makes the online banking experience more convenient, faster, and more secure, as there are no passwords for hackers to steal or crack. Moreover, facial recognition technology has the capability of detecting and preventing fraudulent activity by identifying whether the source of a biometric sample is a live human being or a fake representation. This technique, known as 'live less' detection, helps to prevent fraudsters from using stolen biometric data to impersonate someone else. The adoption of facial recognition technology in online banking has the potential to make debit cards and signatures obsolete. Facial recognition is a more secure and reliable way of verifying identities, and it is much harder for fraudsters to replicate or steal someone's facial features compared to a signature or a physical card. This could lead to a reduction in fraud, making online banking more secure for customers and the banking industry as a whole. However, despite the many benefits of facial recognition in online banking, there are also concerns about privacy and security. Some people are uncomfortable with the idea of their biometric data being stored and shared with third parties. There is also the possibility of facial recognition systems being hacked, leading to the theft of biometric data and potential identity theft.

Previous works on facial recognition system:
- Amazon Web Services (AWS). It uses deep learning algorithms to analyse images and videos, and can detect objects, scenes, and faces in them. It can also analyse and recognize text within images. Amazon Rekognition can be used to automate various tasks such as identifying and tagging images and videos, facial recognition, analysing live video streams for security purposes, and more. It also provides an API that developers can use to integrate image and video analysis into their own applications. The service is designed to be scalable and can handle large volumes of image and video analysis requests in real-time. It is also customizable, allowing users to fine-tune the algorithms to better suit their specific needs. While Amazon Rekognition has many potential applications, it has also faced criticism from some quarters over concerns about privacy and the accuracy of its facial recognition capabilities. [9]
- Apple's phone unlocking technology with face recognition is called Face ID. It was first introduced on the iPhone X in 2017 and has since been included on all new iPhones, including the latest models. Face ID uses a combination of hardware and software to capture and analyse a user's face in order to unlock their device. The technology uses a TrueDepth camera system which includes a dot projector, infrared camera, and flood

illuminator. When the user looks at their iPhone, the dot projector creates a pattern of 30,000 invisible dots on their face. The infrared camera then captures an image of this pattern, which is sent to the iPhone's Secure Enclave for processing. The system compares the captured image to the user's enrolled facial data and if it matches, the iPhone is unlocked. Apple's Face ID technology is designed with security and privacy in mind. The facial data used for Face ID is stored in the iPhone's Secure Enclave, which is a special area of the device's processor that is isolated from the rest of the system. The data is encrypted and never leaves the device, making it more difficult for hackers or other unauthorized parties to gain access to it. Overall, Face ID has been well-received by users and reviewers for its ease of use and security features. However, some concerns have been raised about the technology's accuracy, particularly when it comes to recognizing certain facial features or in low-light conditions.

- British Airways has implemented facial recognition technology at selected airports in the United States to enable passengers to board flights without showing their passport or boarding pass. The technology uses cameras to capture passengers' faces and compare them against a digital image stored in a secure database. This allows for fast and secure identification of passengers, while also reducing the time needed for traditional check-in procedures. To use the facial recognition technology, passengers simply need to approach the camera at the boarding gate, which will scan their face and compare it to their passport and booking details. If the system recognizes the passenger's face, they will be granted access to the plane without the need for additional identification checks. This technology offers several benefits to passengers and airlines. Firstly, it provides a faster and more convenient boarding process, as passengers can simply walk up to the boarding gate without needing to present any additional documentation. Secondly, it enhances security, as the system can quickly and accurately verify the identity of each passenger. Lastly, it reduces the need for physical contact and handling of documents, which is especially important during the COVID-19 pandemic. It's worth noting that passengers who do not wish to use facial recognition can still opt to show their passport or boarding pass as usual. Additionally, facial recognition technology is only being used for the boarding process, and passengers will still need to show their passports or other identification documents at check-in and security checkpoints. Overall, the implementation of facial recognition technology by British Airways demonstrates the potential for advanced technologies to enhance passenger experience and improve security in the aviation industry. [10]
- Facebook's facial recognition technology was first introduced in the United States in 2010 with the launch of its Tag Suggestions tool. This tool uses facial recognition algorithms to automatically suggest tags for people in

photos that are uploaded to Facebook. When a user uploads a photo, Facebook's Tag Suggestions tool scans the photo and creates a digital representation of each person's face in the image. The tool then compares these digital representations to previously tagged photos in the user's profile, as well as photos in other users' profiles, to identify potential matches. If the tool finds a potential match, it suggests a tag for the person in the photo. To protect users' privacy, Facebook has implemented several safeguards and controls around its facial recognition technology. For example, the tool is only available to users who have opted in to facial recognition, and users can turn off the feature at any time in their privacy settings. Facebook also requires users to explicitly confirm the suggested tags before they are applied to the photo. While Facebook's facial recognition technology has been praised for its convenience and ease of use, it has also been criticized for potential privacy violations. In 2019, Facebook reached a $5 billion settlement with the US Federal Trade Commission over privacy violations, including the use of facial recognition without proper user consent. Despite these concerns, Facebook continues to use facial recognition technology in various ways, such as to help prevent identity theft and to improve accessibility for visually impaired users. However, the company has faced increasing pressure from regulators and privacy advocates to provide more transparency and control over its use of facial recognition.

- Google Photos is a photo-sharing and storage service that allows users to store, organize, and share their digital photos and videos. One of the key features of Google Photos is its facial recognition technology, which is used to automatically tag and sort photos based on the people recognized in them. When a user uploads a photo to Google Photos, the service uses facial recognition algorithms to identify any people in the photo. The service then creates a unique digital representation of each person's face, known as a faceprint. Google Photos then scans the user's library of photos to look for other images that include the same people and applies the appropriate tags to each photo. This allows users to easily find and organize photos of specific people, without the need to manually tag each photo themselves. Additionally, Google Photos can automatically create albums and collages based on shared events or themes, such as vacations or birthdays, by using its facial recognition technology to group together photos of the same people. To protect users' privacy, Google has implemented several measures around its use of facial recognition in Google Photos. Firstly, users must opt-in to facial recognition when they first set up their account, and can turn off the feature at any time. Secondly, Google Photos uses encryption to protect users' photos and faceprints from unauthorized access. Finally, Google allows users to easily delete their faceprint from the service if they no longer wish to use the facial

recognition feature. Despite these safeguards, concerns have been raised about the potential for misuse of facial recognition technology, including its potential impact on privacy and civil liberties. As a result, some governments have introduced regulations to limit the use of facial recognition in certain contexts, such as law enforcement.

- Snapchat is a popular social media platform that allows users to share photos and videos with their friends and followers. One of the key features of Snapchat is its facial recognition technology, which is used to create interactive filters and lenses that users can apply to their photos and videos. Snapchat's facial recognition technology works by analyzing the user's face in real-time using the camera on their smartphone or tablet. The technology is able to detect key facial features, such as the eyes, nose, and mouth, and use this information to track the user's movements and expressions. Snapchat's filters and lenses are created by third-party developers who use the company's Lens Studio tool to design and code their creations. These filters and lenses can range from simple effects, such as adding bunny ears or a flower crown to the user's head, to more complex animations that respond to the user's movements and expressions. Brands and organizations can also create their own custom filters and lenses to promote their products or services. For example, a fast food restaurant might create a filter that adds a burger and fries to the user's photo, while a music festival might create a lens that superimposes virtual stage lights and fireworks onto the user's video. Snapchat's facial recognition technology has been praised for its ability to create fun and engaging experiences for users, while also providing a powerful marketing tool for brands and organizations. However, there are also concerns about the potential misuse of facial recognition technology, including its impact on privacy and the potential for bias or discrimination. As a result, Snapchat and other social media platforms have faced increasing scrutiny from regulators and privacy advocates in recent years. [5]

How Facial Recognition Attendance System is Different from previous works:

- All the previous facial recognition systems were able to recognize one face at a time but this system can recognize multiple faces at a time.
- Teacher needs to click a picture of a class and using this system each face will be matched from database and if matched that particular student will be marked as present and if any student doesn't belong to that particular class (i.e. checked from database) then it'll also identify that.
- For all the previous facial recognition system a particular software needs to be installed in system but for this no need to install any additional software. It works on any modern browser, one only needs to locally download the repository.

- The software can be accessed from only a few computers which reduces the chances of student's putting their attendances even if they get hold of the credentials.

Methodology

Facial Recognition Attendance Management is capable of identifying individual faces from an image including a group of people with different faces. In this way we can generate a list of student present in a class by taking images of the class from 2-3 angles. Once the list of students is generated their attendances can be allotted in a databases by making a POST API call.

For the working of this system no other software is needed to be installed because the entire process can be implemented on a website.

Thus Technologies which will be required for this project are:

1. Mongo DB (For recording student attendances persistently)
2. Node.js (For making the APIs needed for this project)
3. HTML (For frontend scripting of the website)
4. CSS (For styling the frontend)
5. Vanilla JavaScript (For making the API calls)

Other open source services used:

1. face-api.js by Vincent Muhler [3]
2. Cloudinary [4]

Data Flow Diagrams

Level Zero:

Level One:

User Credentials

Login_db

Details for verifying user credentials

Checking Login Credentials
0.1

Wait

API Models being loaded
0.2

Loaded

Choosing Image File
0.3

Uploaded Image

Detecting Faces in the Image
0.4

Detected Faces

Detecting Facial Features
0.5

Blueprint of Face

Student_images

Comparing Blueprint of the faces generated with existing blueprint of the faces
0.6

Students whose Blueprints match

Marking Attendance of Students
0.7

Attendance Report

Entity Relationship Diagram
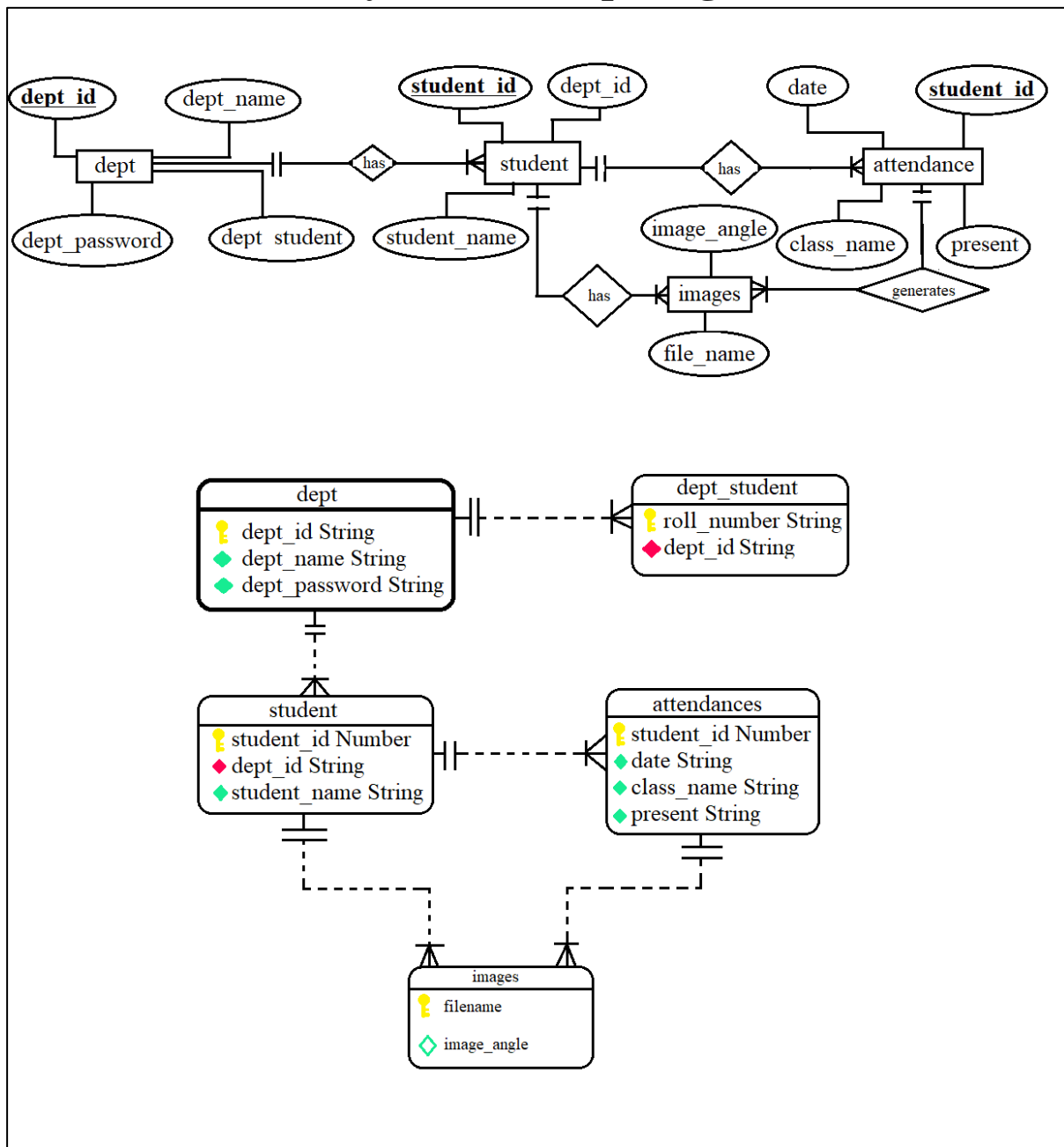
Result and Analysis

First teachers have to open our web application. After opening it a "**Loading**" page will be shown. It may take few times to load the models for our application.
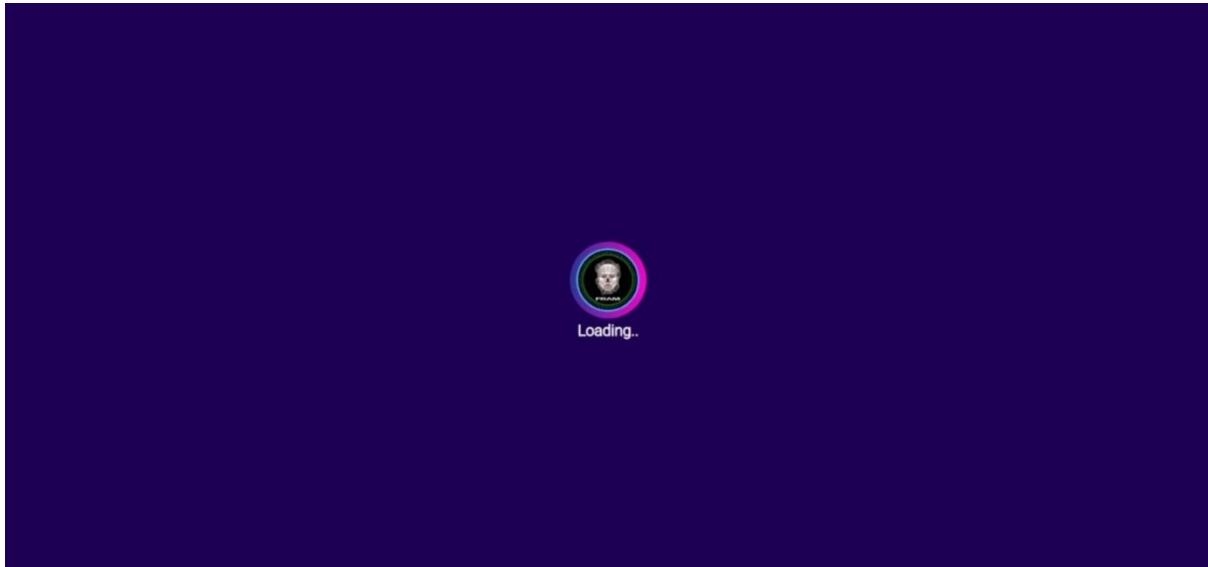
After the page is loaded a new page will appear where teachers have to login in our application with the necessary credentials.
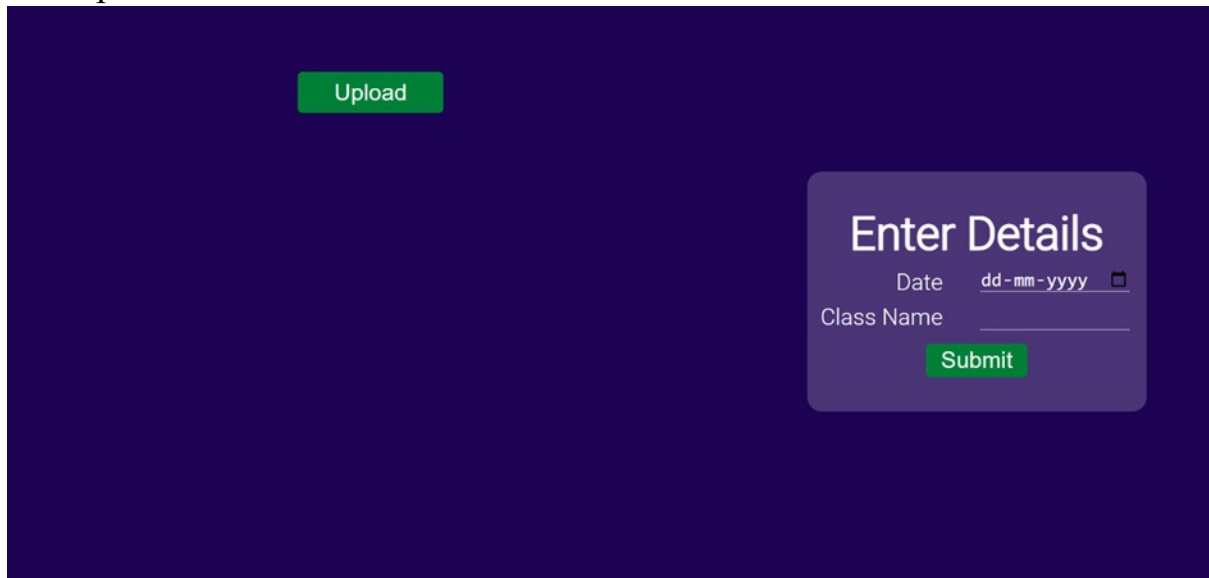
The login credentials are already present in the database. Teachers have to login with that credentials only. If the teacher gives the right Department ID and password then the page will redirect to the next page where teachers can upload the photo of classroom to mark the attendance.

If the teachers give wrong Department ID and password then it will redirect to another page where there is a warning that she/he has given the wrong login credentials.
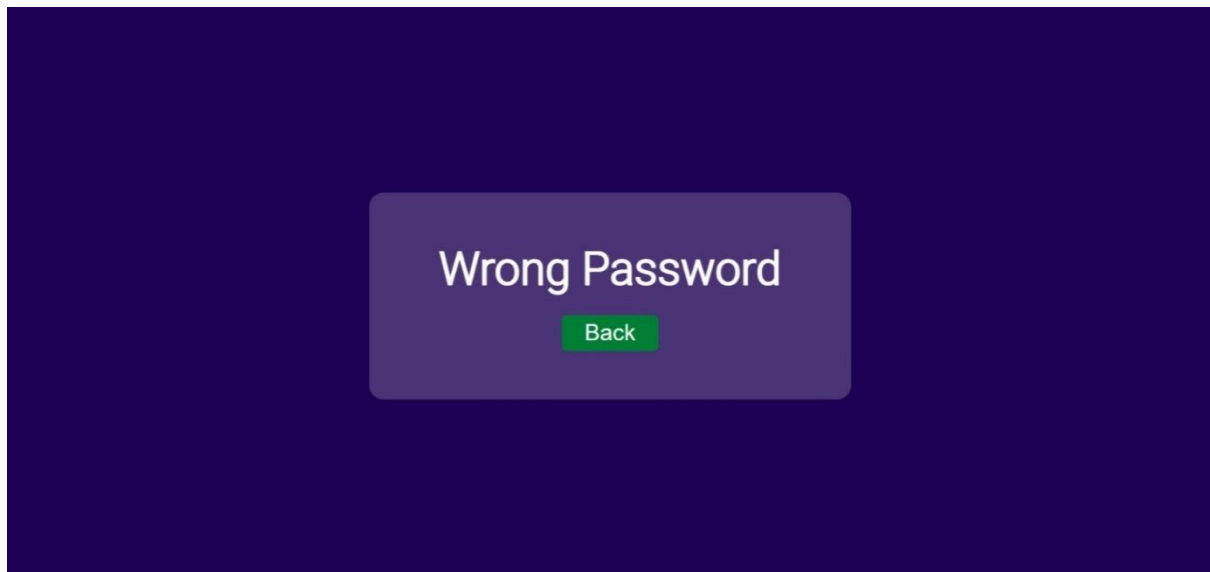
After giving wrong ID and password this above page will appear. Teachers have to click on the back button and it will again redirect to the login page and give the right credentials and go to the upload photo page.

After successful log in teacher needs to upload the class image by clicking on the "upload" button.

And the students who belong to that class and present in that image, their face will be identified. Then teacher needs to enter the class name and the date of the class took place. Then teacher needs to click on the "submit" button.

Request failed..try again later
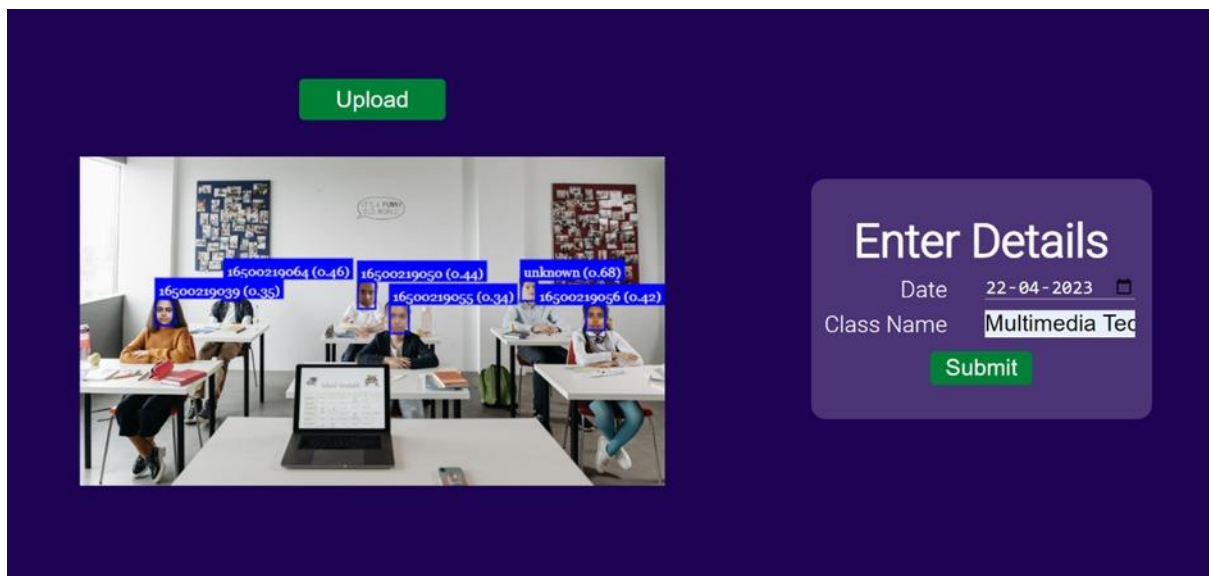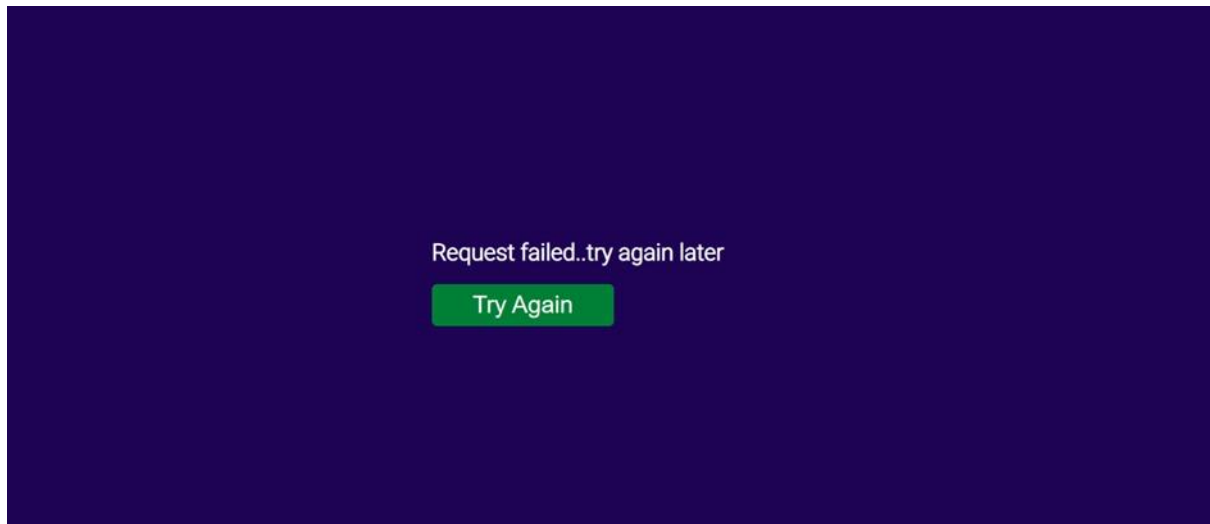
Try Again

If the teacher doesn't enter either of the class date or subject name then an error message will be shown to them. Teacher needs to click on the "Try Again" button to get back to the upload page to enter the details correctly.

If every input field is filled correctly then the attendance will be marked for those students who are present and it will get saved in the database. Then teacher can log out by clicking on the "log out" button, which will redirect the user back to the home page.
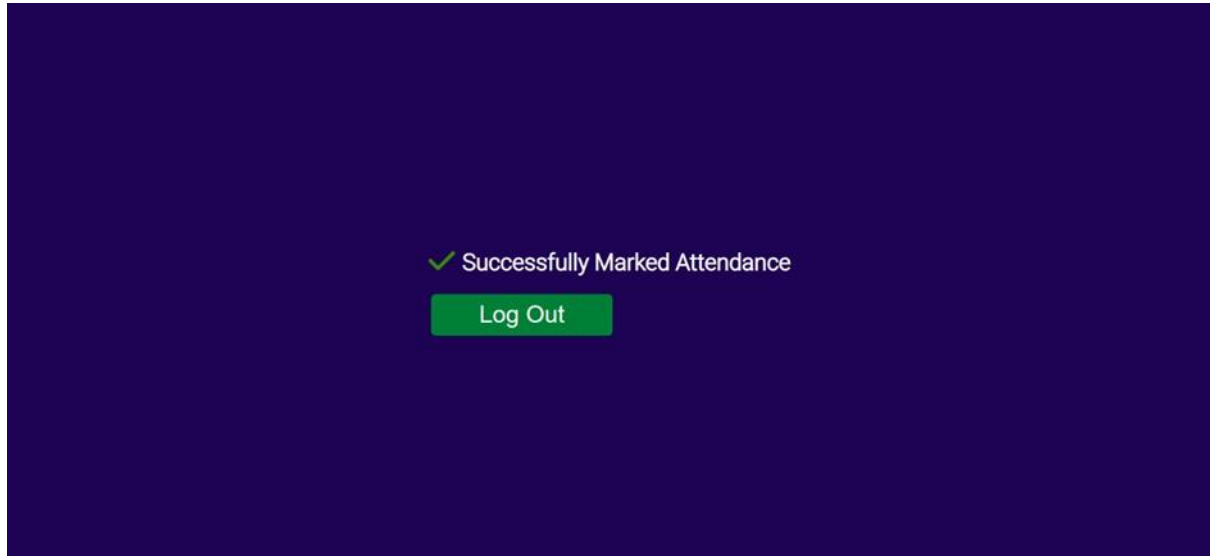
These are the database snapshots where the respective student's attendance is marked.

Discussion

All existing attendance systems that use Face Recognition techniques have one thing in common which is to detect faces individually and mark their attendances. However that process is time consuming as it leads to students standing in a queue generally for getting attendance and takes away time from their classes. Our system captures the entire class in a single snap and allots attendances thus it is not time consuming.

In normal attendance system which is followed in most classes, a teacher marks attendances on pen and paper which takes 10 - 15 minutes from a class. Our attendance system will require just a minute to click an image of the entire class. The entire process is created with safety in mind where a teacher can upload attendances by accessing this portal through a certain IP Address which is one of the department's faculty computer or any other such administrative computers. As a result of which if someone gets their hands on the credentials they still can't upload attendances.

It is a common practices in many classes where a student's attendance is marked even though that student isn't present when some other individual says "Yes Ma'am" or "Present Ma'am" when that absent student's name is called. Such kind of malpractices can't be done in our Attendance System.

We currently went with the 5 angle approach, where an individual's face is captured from 5 different angles. Thus there is there is no dataset images present where an individual's face might not get detected when he or she is wearing a hat, sunglasses or have beards.

Conclusion

Face recognition is an emerging technology that can provide many benefits. This application is completely based on web therefore no installation is required separately on the computer. Unlike other systems which require installation of the software in the local computer.

Our Facial Recognition Attendance Manager will help the teachers to save their time. On average a professor would take 10 minutes for taking attendance. That would mean 5 minutes of less study in a class. If there are 4 subjects taught in a day that would mean approximately 40 minutes in a day wasted. Compared to our system which would take much less time for completion of taking attendance of the entire class.

Other System available in the market would detect one face at a time and register their attendance. Our system is going to take an image of the entire class and save the time.

Thus our system is a unique and easy to use and fast way of collecting attendances.

Future Scope

The following are the future scopes related to this project
1. Using of more face recognition algorithms for getting more accurate results.
2. Using of 8 angle face detection approach so that we can detect faces even if someone is having a beard, hat or sunglasses.
3. Encrypting the credentials.

Appendix

Image Dataset

The database consists of five sets of images each having five sample images. The five sets of images are of five people and the five samples are images of different sides of each face. The sides are front, left, right, front-left and front-right. The images are sourced manually. All images are in RGB colour-space and stored in the JPEG format.

padma_1[11]

padma_2[12]

padma_3[13]

padma_4[14]

padma_5[15]

arkamitra_1[16]

arkamitra_2[17]

arkamitra_3[18]

arkamitra_4[19]

arkamitra_5[20]

anusweta_1[21]

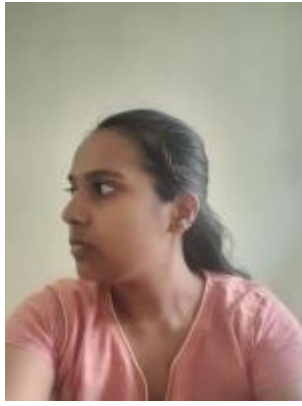anusweta_2[22]

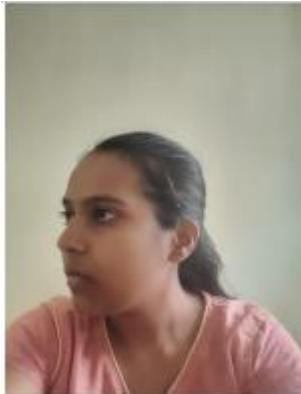anusweta_3[23]
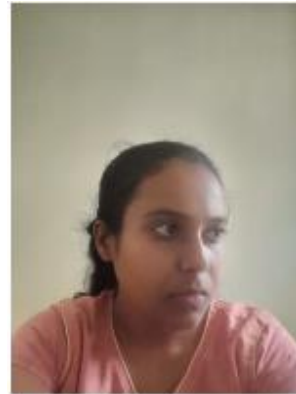

anusweta_4[24]

anusweta_5[25]

basudhara_1[26]

basudhara_2[27]

basudhara_3[28]

basudhara_4[29]

basudhara_5[30]

abir_1[31]

abir_2[32]

abir_3[33]

abir_4[34]

abir_5[35]

References

[1]https://en.wikipedia.org/wiki/Facial_recognition_system

[2]https://medium.com/ml-everything/how-facial-recognition-works-part-2-faciallandmarks-72f1b0e2a33a

[3]https://justadudewhohacks.github.io/face-api.js/docs/index.html

[4]https://cloudinary.com/

[5]https://www.kaspersky.com/resource-center/definitions/what-is-facial-recognition

[6]https://support.apple.com/en-in/HT208108

[7]http://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policingtool-america-n1004251

[8]https://www.kaspersky.com/resource-center/definitions/what-is-facial-recognition

[9]https://docs.aws.amazon.com/rekognition/index.html

[10]https://mediacentre.britishairways.com/pressrelease/details/

[11]https://res.cloudinary.com/dvzh3aj7y/image/upload/v1680198582/LabelledImages/16500219039/1.jpg

[12]https://res.cloudinary.com/dvzh3aj7y/image/upload/v1680198581/LabelledImages/16500219039/5.jpg

[13]https://res.cloudinary.com/dvzh3aj7y/image/upload/v1680198581/LabelledImages/16500219039/2.jpg

[14]https://res.cloudinary.com/dvzh3aj7y/image/upload/v1680198581/LabelledImages/16500219039/3.jpg

[15]https://res.cloudinary.com/dvzh3aj7y/image/upload/v1680198581/LabelledImages/16500219039/4.jpg

[16]https://res.cloudinary.com/dvzh3aj7y/image/upload/v1680197957/LabelledImages/16500219055/4.jpg

[17]https://res.cloudinary.com/dvzh3aj7y/image/upload/v1680197957/LabelledImages/16500219055/3.jpg

[18]https://res.cloudinary.com/dvzh3aj7y/image/upload/v1680197957/LabelledImages/16500219055/1.jpg

[19]https://res.cloudinary.com/dvzh3aj7y/image/upload/v1680197957/LabelledImages/16500219055/2.jpg

[20]https://res.cloudinary.com/dvzh3aj7y/image/upload/v1680197957/LabelledImages/16500219055/5.jpg

[21]https://res.cloudinary.com/dvzh3aj7y/image/upload/v1680197569/LabelledImages/16500219056/4.jpg

[22]https://res.cloudinary.com/dvzh3aj7y/image/upload/v1680197569/LabelledImages/16500219056/1.jpg

[23]https://res.cloudinary.com/dvzh3aj7y/image/upload/v1680197569/LabelledImages/16500219056/2.jpg

[24]https://res.cloudinary.com/dvzh3aj7y/image/upload/v1680197569/LabelledImages/16500219056/5.jpg

[25]https://res.cloudinary.com/dvzh3aj7y/image/upload/v1680197569/LabelledImages/16500219056/3.jpg

[26]https://res.cloudinary.com/dvzh3aj7y/image/upload/v1680163649/LabelledImages/16500219050/1.jpg

[27]https://res.cloudinary.com/dvzh3aj7y/image/upload/v1680163649/LabelledImages/16500219050/2.jpg

[28]https://res.cloudinary.com/dvzh3aj7y/image/upload/v1680163649/LabelledImages/16500219050/3.jpg

[29]https://res.cloudinary.com/dvzh3aj7y/image/upload/v1680163649/LabelledImages/16500219050/4.jpg

[30]https://res.cloudinary.com/dvzh3aj7y/image/upload/v1680163649/LabelledImages/16500219050/5.jpg

[31]https://res.cloudinary.com/dvzh3aj7y/image/upload/v1680106543/LabelledImages/16500219064/2.jpg

[32]https://res.cloudinary.com/dvzh3aj7y/image/upload/v1680106543/LabelledImages/16500219064/1.jpg

[33]https://res.cloudinary.com/dvzh3aj7y/image/upload/v1680106543/LabelledImages/16500219064/5.jpg

[34]https://res.cloudinary.com/dvzh3aj7y/image/upload/v1680106544/LabelledImages/16500219064/3.jpg

[35]https://res.cloudinary.com/dvzh3aj7y/image/upload/v1680106543/LabelledImages/16500219064/4.jpg