# “Face Recognition”

# Major Project

# Submitted in the partial fulfillment for the award of the degree of

# Bachelor of Technology

# In

# Computer Science & Engineering

# Submitted to

# 

# RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA,

# (State Technological University of M.P.)

# Submitted By:

# ABHISHEK ANAND (0133CS181005)

# AYUSH ABHISHEK (0133CS181038)

# DEEPALI RAGHUWANSHI (0133CS181047)

# PRIYANSHU MEHTA (0133CS181116)

# SAURAV RAJ (0133CS181151)

# Under the Guidance of

# Prof. RUPALI CHAURE

# 

# SAGARINSTITUTEOFRESEARCH&TECHNOLOGY, BHOPAL (M.P.)

# Department Of Computer Science and Engineering

# MAY - 2022

## DECLARATION

I hereby declare that the work, which is being presented in the major project, entitled " **FACE RECOGNITION**" Submitted in the **Department of Computer Science & Engineering**, **Sagar Institute of Research & Technology, Bhopal** is an authentic record of my own work carried out during the period from Jan - 2022 to May -2022, under the guidance of **“PROF RUPALI CHAURE**”, **Department of Computer Science & Engineering, Sagar Institute of Research & Technology, Bhopal.**

ABHISHEK ANAND (0133CS181005)

Date: 16 April 2022 AYUSH ABHISHEK (0133CS181038)

DEEPALI RAGHUWANSHI (0133CS181047)

Place: Bhopal PRIYANSHU MEHTA (0133CS181116)

SAURAV RAJ (0133CS181151) (0133CS181151)

**CERTIFICATE**

This is to certify that the Major Project “**FACE RECOGNITION**” being Submitted by **ABHISHEK ANAND (0133CS181005),AYUSH ABHISHEK(0133CS181038), DEEPALI RAGHUWANSHI(0133CS181047), PRIYANSHU MEHTA(0133CS181116), SAURAV RAJ(0133CS181151)** in partial fulfillment of the requirement for the award of the degree of **Bachelor of Technology** in **Computer Science and Engineering** to **RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL (M.P.)** during the academic year **2021-22** is a record of bonafide piece of work, carried out by him/her under my supervision and guidance in the **Department of Computer Science and Engineering, Sagar Institute of Research Technology, Bhopal.**

##### 

Prof. Rupali Chaure Dr.Ritu Shrivastava

**CSE Dept. HOD CSE**

**SIRT,Bhopal SIRT,Bhopal**

**Supervisor**

**APPROVAL CERTIFICATE**

The major project entitled “**FACE RECOGNITION**” being submitted by **“ABHISHEK ANAND(0133CS181005), AYUSH ABHISHEK(0133CS181038), DEEPALI RAGHUWANSHI(0133CS181047), PRIYANSHU MEHTA(0133CS181116), SAURAV RAJ(0133CS181151)”** to **RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL (M.P.)** has been examined by us and is hereby approved for the award of degree **“Bachelor of Technology in Computer Science and Engineering”** in the academic year **2021-22**

**(Internal Examiner) (External Examiner)**

Date: Date:

**ACKNOWLEDGEMENT**

This is one of the best moments of my B.Tech. Program to publicly acknowledgment that whohavecontributedinmanydifferentwaystomakemysuccessapartoftheirown.Thecompletion of the Major Project depends upon the co-operation, coordination and combined effects of several resources of knowledge energy.

I heartily thanks to Prof Rupali chaure**,** and guide Prof. Amit Shrivastava who have supported in Major project, faculties of Department of Computer Science & Engineering, for accepting me to work under their Valuable Guidance, Closely Supervised this work over the past few months and offering many innovative ideas and helpful suggestions, which led to the successful completion of this dissertation work.

I am especially thankful Dr.Rajiv Srivastava, Director (SIRT, Bhopal) for his kindco-operationandrenderingmeallpossiblefacilities.

I express my thanks to Dr. Ritu Shrivastava, HOD Computer Science & Engineering dept. **SIRT** Bhopal for kind support.

I am thankful to all staff members of the CSE department and my friends for their timely help co-operation and suggestion during my project work. Lastly but not the least, I must express thanks to my family, without their moral support it was impossible for me to complete this major projectwork.

ABHISHEK ANAND(0133CS181005)

AYUSH ABHISHEK(0133CS181038)

DEEPALI RAGHUWANSHI (0133CS181047)

PRIYANSHU MEHTA (0133CS181116)

SAURAV RAJ (0133CS181151)

|  |  |
| --- | --- |
| **Table of Contents** | **Page No.** |
| Title Page | 1 |
| Declaration Of Student | 2 |
| Certificate | 3 |
| Approval Certificate | 4 |
| Abstract | 5 |
| Acknowledgement | 7 |
| Chapter 1 **Introduction** | 9 |
| 1.1 face recognition | 10 |
| 1.2 face recognition examples |  |
| Chapter 2 **Literature Survey** | 18 |
| 2.1 theory of face recognition | 21 |
| Chapter 3 face recognition processing | 28 |
| 3.1 face recognition process | 29 |
| 3.2 how accurate is face recognition | 30 |
| 3.3 who uses face recognition | 34 |
| Chapter 4 **Objective** | 35 |
| Chapter 5 **Scope** | 36 |
| Chapter 6 **Design** | 37 |
| 6.1 Software Engineering Model Used | 38 |
| 6.2 Use Case Diagram | 39 |
| 6.3 ER – Diagram | 40 |
| 6.4 Data Flow Diagram | 41 |
| 6.5 Sequential Diagram | 42 |
| 6.6 Class Diagram | 43 |
| 6.7 Deployment Diagram | 44 |
| Chapter 7 **Implementation Requirements** | 45 |
| 7.1 Software Requirements | 45 |
| 7.2 Hardware Requirements | 46 |
| Chapter 8 **Test cases and Future Work** | 47 |
| 8.1Test cases | 47 |
| 8.2Future Work | 48 |
| **References** | 49 |
| **Appendix** | 50 |

**ABSTACT**

The project tiled “Face Recognition” is done using the language PYTHON, Deep learning and its cross platform Opens.

Face recognition technology is a biometric technology, which is based on the identification of facial features of a person. People collect the face images, and the recognition equipment automatically processes the images. The paper introduces the related researches of face recognition from different perspectives. The paper describes the development stages and the related technologies of face recognition. We introduce the research of face recognition for real conditions, and we introduce the general evaluation standards and the general databases of face recognition. We give a forward-looking view of face recognition. Face recognition has become the future development direction and has many potential application prospects.

Automatic number plate recognition (ANPR) is an image processing technology which uses number (license) plate to identify the vehicle. The objective is to design an efficient automatic authorized vehicle identification system by using the vehicle number plate. The system is implemented on the entrance for security control of a highly restricted area like military zones or area around top government offices e.g. Parliament, Supreme Court etc. The developed system first detects the vehicle and then captures the vehicle image. Vehicle number plate region is extracted using the image segmentation in an image. Optical character recognition technique is used for the character recognition. The resulting data is then used to compare with the records on a database so as to come up with the specific information like the vehicle owner, place of registration, address, etc. The system is implemented and simulated in Open CV, and it performance is tested on real image. It is observed from the experiment that the developed system successfully detects and recognize the vehicle number plate on real images.

Voice assistants are software agents that can interpret human speech and respond via synthesized voices. Apple's Seri, Amazon's Alexa, Microsoft's Crotona, and Google's Assistant are the most popular voice assistants and are embedded in smart phones or dedicated home speakers. Users can ask their assistants questions, control home automation devices and media playback via voice, and manage other basic tasks such as email, to-do lists, and calendars with verbal commands. This column will explore the basic workings and common features of today's voice assistants. It will also discuss some of the privacy and security issues inherent to voice assistants and some potential future uses for these devices. As voice assistants become more widely used, librarians will want to be familiar with their operation and perhaps consider them as a means to deliver library services and materials.

**CHAPTER – 1**

**INTRODUCTION**

Facial recognition is a way of identifying or confirming an individual's identity using their face. Facial recognition systems can be used to identify people in photos, videos, or in real-time. Facial recognition is a category of biometric security.

Facial recognition is a category of [biometric security](https://www.kaspersky.com/resource-center/definitions/biometrics). Other forms of biometric software include voice recognition, fingerprint recognition, and eye retina or iris recognition. The technology is mostly used for security and law enforcement, though there is increasing interest in other areas of use.

## How does facial recognition work?

Many people are familiar with face recognition technology through the FaceID used to unlock iPhones (however, this is only one application of face recognition). Typically, facial recognition does not rely on a massive database of photos to determine an individual’s identity — it simply identifies and recognizes one person as the sole owner of the device, while limiting access to others.

Beyond unlocking phones, facial recognition works by matching the faces of people walking past special cameras, to images of people on a watch list. The watch lists can contain pictures of anyone, including people who are not suspected of any wrongdoing, and the images can come from anywhere — even from our social media accounts. Facial technology systems can vary, but in general, they tend to operate as follows:

### Step 1: Face detection

The camera detects and locates the image of a face, either alone or in a crowd. The image may show the person looking straight ahead or in profile.

### Step 2: Face analysis

Next, an image of the face is captured and analyzed. Most facial recognition technology relies on 2D rather than 3D images because it can more conveniently match a 2D image with public photos or those in a database. The software reads the geometry of your face. Key factors include the distance between your eyes, the depth of your eye sockets, the distance from forehead to chin, the shape of your cheekbones, and the contour of the lips, ears, and chin. The aim is to identify the facial landmarks that are key to distinguishing your face.

### Step 3: Converting the image to data

The face capture process transforms analog information (a face) into a set of digital information (data) based on the person's facial features. Your face's analysis is essentially turned into a mathematical formula. The numerical code is called a faceprint. In the same way that thumbprints are unique, each person has their own faceprint.

### Step 4: Finding a match

Your faceprint is then compared against a database of other known faces. For example, the FBI has access to up to [650 million photos](https://www.aclu.org/blog/privacy-technology/surveillance-technologies/fbi-has-access-over-640-million-photos-us-through), drawn from various state databases. On Facebook, any photo tagged with a person’s name becomes a part of Facebook's database, which may also be used for facial recognition. If your faceprint matches an image in a facial recognition database, then a determination is made.

Of all the biometric measurements, facial recognition is considered the most natural. Intuitively, this makes sense, since we typically recognize ourselves and others by looking at faces, rather than thumbprints and irises. It is estimated that over half of the world's population is touched by facial recognition technology regularly.

## How facial recognition works

You might be good at recognizing faces. You probably find it a cinch to identify the face of a family member, friend, or acquaintance. You’re familiar with their facial features — their eyes, nose, mouth — and how they come together.

That’s how a facial recognition system works, but on a grand, algorithmic scale. Where you see a face, recognition technology sees data. That data can be stored and accessed. For instance, half of all American adults have their images stored in one or more facial-recognition databases that law enforcement agencies can search, according to a Georgetown University study.

So how does facial recognition work? Technologies vary, but here are the basic steps:

**Step 1**. A picture of your face is captured from a photo or video. Your face might appear alone or in a crowd. Your image may show you looking straight ahead or nearly in profile.

**Step 2**. Facial recognition software reads the geometry of your face. Key factors include the distance between your eyes and the distance from forehead to chin. The software identifies facial landmarks — one system identifies 68 of them — that are key to distinguishing your face. The result: your facial signature.

**Step 3**. Your facial signature — a mathematical formula — is compared to a database of known faces. And consider this: At least 117 million Americans have images of their faces in one or more police databases. According to a May 2018 report, the FBI has had access to 412 million facial images for searches.

**Step 4**. A determination is made. Your faceprint may match that of an image in a facial recognition system database.

## A brief history of facial recognition

You can trace the history of facial recognition to the 1960s. That’s when mathematician and computer scientist Woodrow Wilson Bledsoe first developed a system of measurements that could be used to put photos of faces in different classifications. Because of this work, Bledsoe is known as the unofficial father of facial recognition technology.

Law enforcement agencies soon became interested in Bledsoe’s work. And in the 1970s through the 1990s, agencies developed their own facial recognition systems. These were crude compared to the technology today, but the work on these systems did lead the way to modern facial recognition programs.

Many point to 2001 as a key year for facial recognition technology. That’s when law enforcement officials used facial recognition to help identify people in the crowd at Super Bowl XXXV. That same year, the Pinellas County Sheriff’s Office in Florida created its own facial recognition database.

It wasn’t until the 2010s, though, that computers grew powerful enough to make facial recognition a more standard feature. In 2011, in fact, facial recognition software confirmed the identity of terrorist Osama bin Laden. In 2015, the Baltimore police department used facial recognition to identify those who participated in protests after Freddie Gray was killed by a spinal injury that he suffered while being transported in a police van.

Consumers now use facial recognition with their smartphones and other personal devices. Windows Hello and Android’s Trusted Face in 2015 allowed people to log into their devices by simply aiming them at their faces. Apple’s iPhone X unveiled its Face ID facial recognition technology in 2017.

There has been controversy over this technology, with critics saying it is an invasion of privacy. Cities such as San Francisco, Oakland, and Boston have banned governments from using facial recognition. And after Black Lives Matter protests against police brutality in the summer of 2020, several tech giants, including Amazon, Microsoft, and IBM, announced that they would no longer sell their facial recognition technology to law enforcement agencies.

## How accurate is facial recognition?

Critics worry that facial recognition could lead to false identifications. What if a police department uses facial recognition technology to incorrectly identify someone breaking a store window during a riot as a person who was nowhere near the event? How likely is it that this could happen?

That depends. Tests by the National Institute of Standards and Technology say that as of April of 2020, the best face identification algorithm boasted an error rate of just 0.08%. That's a big improvement from 2014, when the best algorithm had an error rate of 4.1%.

Accuracy, though, is higher when identification algorithms are used to match people to clear, static images, such as a passport photo or mugshot, according to a **[story](https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter" \t "_blank)** by the Center for Strategic & International Studies (CSI) in 2020. The story said that facial recognition algorithms can hit accuracy scores as high as 99.97% on the National Institute of Standards and Technology's Facial Recognition Vendor Test when used in this way.

In the real world, though, accuracy rates are usually lower. According to the CSI story, the Facial Recognition Vendor Test found that the error rate for one algorithm rose from 0.1% when faces were matched against high-quality mugshots to 9.3% when matched to pictures of individuals captured in public. Error rates rose especially when subjects were not looking directly at the camera or were partially hidden by shadows or objects.

Aging is another challenge. The Facial Recognition Vendor Test said that middle-tier facial recognition algorithms had error rates that jumped by nearly a factor of 10 when they attempted to match photos of subjects that had been taken 18 years earlier.

## Who uses facial recognition

A lot of people and organizations use facial recognition — and in a lot of different places. Here’s a sampling:

* **U.S. government at airports**. Facial recognition systems can monitor people coming and going in airports. The Department of Homeland Security has used the technology to identify people who have overstayed their visas or may be under criminal investigation. Customs officials at Washington Dulles International Airport made their first arrest using facial recognition in August of 2018, catching an impostor trying to enter the country.
* **Mobile phone makers in products**. Apple first used facial recognition to unlock its iPhone X, and has continued with the technology with the iPhone XS. Face ID authenticates — it makes sure you’re you when you access your phone. Apple says the chance of a random face unlocking your phone is about one in 1 million.
* **Colleges in the classroom**. Facial recognition software can, in essence, take roll. If you decide to cut class, your professor could know. Don’t even think of sending your brainy roommate to take your test.
* **Social media companies on websites**. Facebook uses an algorithm to spot faces when you upload a photo to its platform. The social media company asks if you want to tag people in your photos. If you say yes, it creates a link to their profiles. Facebook can recognize faces with 98 percent accuracy.
* **Businesses at entrances and restricted areas**. Some companies have traded in security badges for facial recognition systems. Beyond security, it could be one way to get some face time with the boss.
* **Religious groups at places of worship**. Churches have used facial recognition to scan their congregations to see who’s present. It’s a good way to track regulars and not-so-regulars, as well as to help tailor donation requests.
* **Retailers in stores**. Retailers can combine surveillance cameras and facial recognition to scan the faces of shoppers. One goal: identifying suspicious characters and potential shoplifters.
* **Airlines at departure gates**. You might be accustomed to having an agent scan your boarding pass at the gate to board your flight. At least one airline scans your face.
* **Marketers and advertisers in campaign**s. Marketers often consider things like gender, age, and ethnicity when targeting groups for a product or idea. Facial recognition can be used to define those audiences even at something like a concert.

## Facial recognition and its use in law enforcement

Facial recognition databases play a significant role in law enforcement today. According to a **[report](https://www.eff.org/pages/face-recognition" \t "_blank)** by the Electronic Frontier Foundation, law enforcement agencies routinely collect mugshots from those who have been arrested and compare them to local, state, and federal facial recognition databases.

Law enforcement agencies can sift through these mugshot databases to identify people in photos taken from a variety of sources: closed-circuit television cameras, traffic cameras, social media, or photos that police officers have taken themselves.

Police officers can also use their smartphones, tablets, or other mobile devices to snap photos of drivers or pedestrians and immediately compare their photo against the faces in one or more facial recognition databases, the Electronic Frontier Foundation says.

And law enforcement has used facial recognition at large events such as concerts, sporting events, or the Olympics to identity people who might be wanted in connection with crimes.

The federal government can use several facial recognition systems. The database it relies on most frequently, though, is the FBIs Next Generation Identification system. This database contains more than 30 million facial records.

## Facial recognition examples

Businesses use facial recognition in a variety of ways today, usually to make it easier for consumers to use their products or services. Here are some examples:

**Traveling**: British Airways uses facial recognition to make it easier for U.S. passengers to board their flights. Passengers can have their faces scanned by a camera to verify their identity. This way, they can board their flights without having to show a passport or boarding pass.

**Apple**: Apple could be considered a pioneer in facial recognition. The tech giant has long allowed consumers to unlock their phones, log into apps, and make purchases just by showing their face to their smartphones and other devices.

**Driving**: Automakers are testing facial recognition technology to help cut down on car theft. Consider Project Mobil: Ford and Intel are testing a project in which a dashboard camera uses facial recognition to identify the primary driver of a car and, perhaps, other authorized drivers. The tech could prevent a car from starting if someone other than a rightful driver is sitting behind the wheel.

**Banking**: Banking giants such as HSBC and Chase already use Apple's FaceID to let customers log into their mobile banking apps. Other financial institutions are testing facial recognition to allow customers to use their phone's cameras to approve online purchases.

**Insurance**: Cigna allows customers in China to file health insurance claims using their photos instead of a written signature. The insurance company says it’s a way to cut down on insurance fraud.

**Even soft drinks**: Coca-Cola has been a longtime user of facial recognition. For instance, the company uses the technology to reward customers for recycling at some of its vending machines in China. It also uses facial recognition to send customers in some countries personalized ads when they use vending machines.

## Facial recognition pros and cons

As a relatively new technology, we're still understanding the pros and cons of facial recognition. But here is a brief list of both the positives and possible negatives of this technology.

### Pros

**Finding missing people**: With facial recognition, law enforcement agencies have been able to track down missing children, sometimes even after they've been missing for years.

**Identifying criminals**: Law enforcement agencies can also use facial recognition to identify criminals or suspects in crimes.

**Making flying safer**: Airports across the globe are using facial recognition to identify criminals and potential threats as they enter airports or try to board flights.

**More efficient shopping?** Retailers can use facial recognition to make it easier for consumers to check out. Instead of forcing customers to pay with cash or credit, retailers can use facial recognition to immediately charge their purchases to their accounts.

### Cons

**A threat to privacy?** Do you want your face saved in a database that law enforcement agencies can tap? Do you want retailers to have a saved image of your face? If you don’t, you're not alone. Many critics worry that facial recognition is one more erosion of personal privacy.

**Mistaken identity**: Facial recognition isn't perfect. What if a law enforcement agency mistakenly identifies you as a criminal suspect when you're filing into your favorite ballpark?

**It can be tricked**: Criminals can trick facial recognition by wearing masks or facial disguises. This could lessen the effectiveness of this tech.

**Aging lowers its effectiveness**: Studies have found that as people age, and their features change, facial recognition has an increasingly difficult time identifying them. Other studies have shown that facial recognition is less effective in identifying people of color and women.

## Reasons to be concerned about your privacy

* longer be private. It could become impossible to remain anonymous.

**How you can help** Privacy matters. Privacy refers to any rights you have to control your personal information and how it’s used — and that can include your faceprint.

So, what are the issues? Here are some:

* **Security**. Your facial data can be collected and stored, often without your permission. It’s possible hackers could access and steal that data.
* **Prevalence**. Facial recognition technology is becoming more widespread. That means your facial signature could end up in a lot of places. You probably won’t know who has access to it.
* **Ownership**. You own your face — the one atop your neck — but your digital images are different. You may have given up your right to ownership when you signed up on a social media network. Or maybe someone tracks down images of you online and sells that data.
* **Safety**. Facial recognition could lead to online harassment and stalking. How? For example, someone takes your picture on a subway or some other public place and uses facial recognition software to find out exactly who you are.
* **Mistaken identity**. Say, for instance, law enforcement uses facial recognition to try to identify someone who robbed a corner store. Facial recognition systems may not be 100 percent accurate. What if the police think the suspect is you?

## Basic freedoms. Government agencies and others could have the ability to track you. What you do and where you go might no protect yourself against facial recognition

Want to protect your privacy in a world in which facial recognition technology is becoming more common? Here are some reasons for hope.

**Tech innovation**: Concerns about facial recognition could spur innovation.

Consider this: Two universities have developed anti-facial recognition glasses to make wearers undetectable.

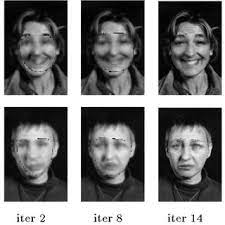
The glasses — the work of researchers at Carnegie Mellon University and the University of North Carolina at Chapel Hill — could be one way to help protect yourself.

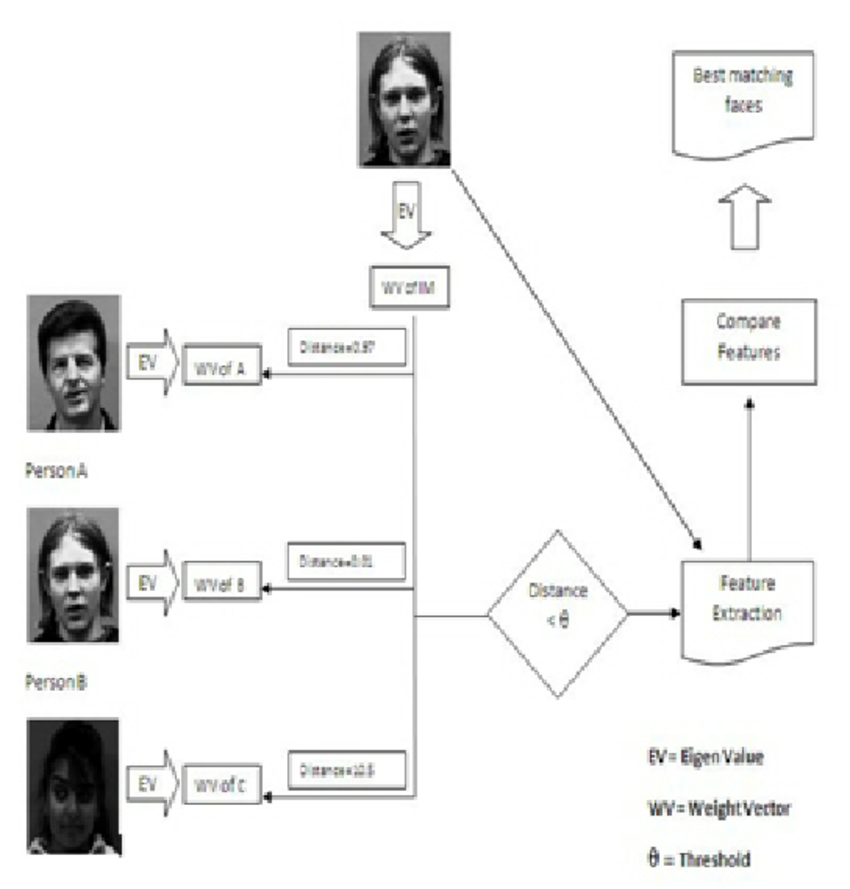
**Social networks**: Changing the way you interact with social media could help protect you from facial recognition-based privacy invasions.

For example, Facebook allows you to opt out of its facial recognition system.

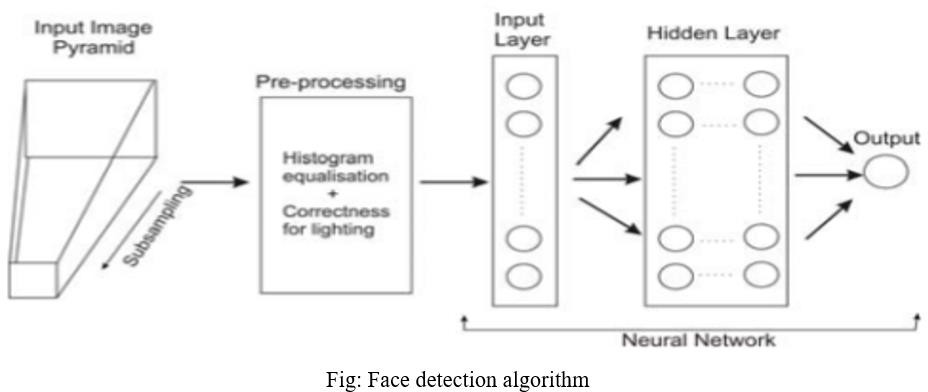
It’s smart in general to be careful about what you share on social networks. Posting too much personal information, including photos, could lead to identity theft. For instance, you might share your dog’s name or your high school mascot. Those details might give an identity thief a clue to the answers to your security questions for your bank or credit card accounts.

**The Internet of things**: It’s also a good idea to consider the so-called Internet of Things — those devices in your home that connect to the internet. IoT devices that use face recognition include iPads, Xboxes, and video systems.





.

****Facial recognition software **reads the geometry of your face**. Key factors include the distance between your eyes and the distance from forehead to chin. The software identifies facial landmarks — one system identifies 68 of them — that are key to distinguishing your face. The result: your facial signature.

**CHAPTER - 2**

# LITERATURE SURVEY

A **facial recognition system** is a technology capable of matching a [human face](https://en.wikipedia.org/wiki/Human_face" \o "Human face) from a [digital image](https://en.wikipedia.org/wiki/Digital_image" \o "Digital image) or a [video frame](https://en.wikipedia.org/wiki/Film_frame" \o "Film frame) against a [database](https://en.wikipedia.org/wiki/Database" \o "Database) of faces, typically employed to [authenticate](https://en.wikipedia.org/wiki/Authenticate" \o "Authenticate) users through [ID verification services](https://en.wikipedia.org/wiki/ID_verification_service" \o "ID verification service), works by pinpointing and measuring facial features from a given image.[[1]](https://en.wikipedia.org/wiki/Facial_recognition_system" \l "cite_note-1)

Development began on similar systems in the 1960s, beginning as a form of computer [application](https://en.wikipedia.org/wiki/Application_software" \o "Application software). Since their inception, facial recognition systems have seen wider uses in recent times on [smartphones](https://en.wikipedia.org/wiki/Smartphone" \o "Smartphone) and in other forms of technology, such as [robotics](https://en.wikipedia.org/wiki/Robotics" \o "Robotics). Because computerized facial recognition involves the measurement of a human's physiological characteristics, facial recognition systems are categorized as [biometrics](https://en.wikipedia.org/wiki/Biometrics" \o "Biometrics). Although the accuracy of facial recognition systems as a biometric technology is lower than [iris recognition](https://en.wikipedia.org/wiki/Iris_recognition" \o "Iris recognition) and [fingerprint](https://en.wikipedia.org/wiki/Fingerprint" \o "Fingerprint) recognition, it is widely adopted due to its contactless process.[[2]](https://en.wikipedia.org/wiki/Facial_recognition_system" \l "cite_note-2) Facial recognition systems have been deployed in advanced [human–computer interaction](https://en.wikipedia.org/wiki/Human%E2%80%93computer_interaction" \o "Human–computer interaction), [video surveillance](https://en.wikipedia.org/wiki/Video_surveillance" \o "Video surveillance) and automatic [indexing](https://en.wikipedia.org/wiki/Search_engine_indexing" \o "Search engine indexing) of images.[[3]](https://en.wikipedia.org/wiki/Facial_recognition_system" \l "cite_note-:8-3)

Facial recognition systems are employed throughout the world today by governments and private companies.[[4]](https://en.wikipedia.org/wiki/Facial_recognition_system" \l "cite_note-4) Their effectiveness varies, and some systems have previously been scrapped because of their ineffectiveness. The use of facial recognition systems has also raised controversy, with claims that the systems violate citizens' privacy, commonly make incorrect identifications, encourage [gender norms](https://en.wikipedia.org/wiki/Gender_role" \o "Gender role) and [racial profiling](https://en.wikipedia.org/wiki/Racial_profiling" \o "Racial profiling), and do not protect important biometric data. These claims have led to the ban of facial recognition systems in several cities in the [United States](https://en.wikipedia.org/wiki/United_States" \o "United States).[[5]](https://en.wikipedia.org/wiki/Facial_recognition_system" \l "cite_note-:10-5) As a result of growing societal concerns, [Meta](https://en.wikipedia.org/wiki/Meta_Platforms" \o "Meta Platforms) announced[[6]](https://en.wikipedia.org/wiki/Facial_recognition_system" \l "cite_note-6) that it plans to shut down [Facebook facial recognition system](https://en.wikipedia.org/wiki/DeepFace" \o "DeepFace), deleting the face scan data of more than one billion users.[[7]](https://en.wikipedia.org/wiki/Facial_recognition_system" \l "cite_note-7) This change will represent one of the largest shifts in facial recognition usage in the technology's history.

As one of the most successful applications of image analysis and understanding, face recognition has recently received significant attention, especially during the past several years. At least two reasons account for this trend: the first is the wide range of commercial and law enforcement applications, and the second is the availability of feasible technologies after 30 years of research. Even though current machine recognition systems have reached a certain level of maturity, their success is limited by the conditions imposed by many real applications. For example, recognition of face images acquired in an outdoor environment with changes in illumination and/or pose remains a largely unsolved problem. In other words, current systems are still far away from the capability of the human perception system. This paper provides an up-to-date critical survey of still- and video-based face recognition research. There are two underlying motivations for us to write this survey paper: the first is to provide an up-to-date review of the existing literature, and the second is to offer some insights into the studies of machine recognition of faces. To provide a comprehensive survey, we not only categorize existing recognition techniques but also present detailed descriptions of representative methods within each category. In addition, relevant topics such as psychophysical studies, system evaluation, and issues of illumination and pose variation are covered. Categories and Subject Descriptors: I.5.4 [Pattern Recognition]: Applications General Terms: Algorithms Additional Key Words and Phrases: Face recognition, person identification An earlier version of this paper appeared as “Face Recognition: A Literature Survey,” Technical Report CARTR-948, Center for Automation Research, University of Maryland, College Park, MD, 2000. Authors’ addresses: W. Zhao, Vision Technologies Lab, Sarnoff Corporation, Princeton, NJ 08543-5300; email: wzhao@sarnoff.com; R. Chellappa and A. Rosenfeld, Center for Automation Research, University of Maryland, College Park, MD 20742-3275; email: {rama,ar}@cfar.umd.edu; P. J. Phillips, National Institute of Standards and Technology, Gaithersburg, MD 20899; email: jonathon@nist.gov. Permission to make digital/hard copy of part or all of this work for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial advantage, the copyright notice, the title of the publication, and its date appear, and notice is given that copying is by permission of ACM, Inc. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or a fee. c 2003 ACM 0360-0300/03/1200-0399 $5.00 ACM Computing Surveys, Vol. 35, No. 4, December 2003, pp. 399–458. 400 Zhao et al. 1. INTRODUCTION As one of the most successful applications of image analysis and understanding, face recognition has recently received significant attention, especially during the past few years. This is evidenced by the emergence of face recognition conferences such as the International Conference on Audioand Video-Based Authentication (AVBPA) since 1997 and the International Conference on Automatic Face and Gesture Recognition (AFGR) since 1995, systematic empirical evaluations of face recognition techniques (FRT), including the FERET [Phillips et al. 1998b, 2000; Rizvi et al. 1998], FRVT 2000 [Blackburn et al. 2001], FRVT 2002 [Phillips et al. 2003], and XM2VTS [Messer et al. 1999] protocols, and many commercially available systems (Table II). There are at least two reasons for this trend; the first is the wide range of commercial and law enforcement applications and the second is the availability of feasible technologies after 30 years of research. In addition, the problem of machine recognition of human faces continues to attract researchers from disciplines such as image processing, pattern recognition, neural networks, computer vision, computer graphics, and psychology. The strong need for user-friendly systems that can secure our assets and protect our privacy without losing our identity in a sea of numbers is obvious. At present, one needs a PIN to get cash from an ATM, a password for a computer, a dozen others to access the internet, and so on. Although very reliable methods of biometric personal identification exist, for Table I. Typical Applications of Face Recognition Areas Specific applications Video game, virtual reality, training programs Entertainment Human-robot-interaction, human-computer-interaction Drivers’ licenses, entitlement programs Smart cards Immigration, national ID, passports, voter registration Welfare fraud TV Parental control, personal device logon, desktop logon Information security Application security, database security, file encryption Intranet security, internet access, medical records Secure trading terminals Law enforcement Advanced video surveillance, CCTV control and surveillance Portal control, postevent analysis Shoplifting, suspect tracking and investigation example, fingerprint analysis and retinal or iris scans, these methods rely on the cooperation of the participants, whereas a personal identification system based on analysis of frontal or profile images of the face is often effective without the participant’s cooperation or knowledge. Some of the advantages/disadvantages of different biometrics are described in Phillips et al. [1998]. Table I lists some of the applications of face recognition. Commercial and law enforcement applications of FRT range from static, controlled-format photographs to uncontrolled video images, posing a wide range of technical challenges and requiring an equally wide range of techniques from image processing, analysis, understanding, and pattern recognition. One can broadly classify FRT systems into two groups depending on whether they make use of static images or of video. Within these groups, significant differences exist, depending on the specific application. The differences are in terms of image quality, amount of background clutter (posing challenges to segmentation algorithms), variability of the images of a particular individual that must be recognized, availability of a well-defined recognition or matching criterion, and the nature, type, and amount of input from a user. A list of some commercial systems is given in Table II. A general statement of the problem of machine recognition of faces can be formulated as follows: given still or video images of a scene, identify or verify one or more persons in the scene using a stored database of faces. Available ACM Computing Surveys, Vol. 35, No. 4, December 2003. Face Recognition: A Literature Survey 401 Table II. Available Commercial Face Recognition Systems (Some of these Web sites may have changed or been removed.) [The identification of any company, commercial product, or trade name does not imply endorsement or recommendation by the National Institute of Standards and Technology or any of the authors or their institutions.] Commercial products Websites FaceIt from Visionics http://www.FaceIt.com Viisage Technology http://www.viisage.com FaceVACS from Plettac http://www.plettac-electronics.com FaceKey Corp. http://www.facekey.com Cognitec Systems http://www.cognitec-systems.de Keyware Technologies http://www.keywareusa.com/ Passfaces from ID-arts http://www.id-arts.com/ ImageWare Sofware http://www.iwsinc.com/ Eyematic Interfaces Inc. http://www.eyematic.com/ BioID sensor fusion http://www.bioid.com Visionsphere Technologies http://www.visionspheretech.com/menu.htm Biometric Systems, Inc. http://www.biometrica.com/ FaceSnap Recoder http://www.facesnap.de/htdocs/english/index2.html SpotIt for face composite http://spotit.itc.it/SpotIt.html

Face perception is an important part of the capability of human perception system and is a routine task for humans, while building a similar computer system is still an on-going research area. The earliest work on face recognition can be traced back at least to the 1950s in psychology [Bruner and Tagiuri 1954] and to the 1960s in the engineering literature [Bledsoe 1964]. Some of the earliest studies include work on facial expression of emotions by Darwin [1972] (see also Ekman [1998]) and on facial profile-based biometrics by Galton [1888]). But research on automatic machine recognition of faces really started in the 1970s [Kelly 1970] and after the seminal work of Kanade [1973]. Over the past 30 years extensive research has been conducted by psychophysicists, neuroscientists, and engineers on various aspects of face recognition by humans and machines. Psychophysicists and neuroscientists have been concerned with issues such as whether face perception is a dedicated process (this issue is still being debated in the psychology community [Biederman and Kalocsai 1998; Ellis 1986; Gauthier et al. 1999; Gauthier and Logothetis 2000]) and whether it is done holistically or by local feature analysis. Many of the hypotheses and theories put forward by researchers in these disciplines have been based on rather small sets of images. Nevertheless, many of the ACM Computing Surveys, Vol. 35, No. 4, December 2003. 402 Zhao et al. findings have important consequences for engineers who design algorithms and systems for machine recognition of human faces. Section 2 will present a concise review of these findings. Barring a few exceptions that use range data [Gordon 1991], the face recognition problem has been formulated as recognizing three-dimensional (3D) objects from two-dimensional (2D) images.1 Earlier approaches treated it as a 2D pattern recognition problem. As a result, during the early and mid-1970s, typical pattern classification techniques, which use measured attributes of features (e.g., the distances between important points) in faces or face profiles, were used [Bledsoe 1964; Kanade 1973; Kelly 1970]. During the 1980s, work on face recognition remained largely dormant. Since the early 1990s, research interest in FRT has grown significantly. One can attribute this to several reasons: an increase in interest in commercial opportunities; the availability of real-time hardware; and the increasing importance of surveillance-related applications. Over the past 15 years, research has focused on how to make face recognition systems fully automatic by tackling problems such as localization of a face in a given image or video clip and extraction of features such as eyes, mouth, etc. Meanwhile, significant advances have been made in the design of classifiers for successful face recognition. Among appearance-based holistic approaches, eigenfaces [Kirby and Sirovich 1990; Turk and Pentland 1991] and Fisherfaces [Belhumeur et al. 1997; Etemad and Chellappa 1997; Zhao et al. 1998] have proved to be effective in experiments with large databases. Feature-based graph matching approaches [Wiskott et al. 1997] have also been quite successful. Compared to holistic approaches, feature-based methods are less sensitive to variations in illumination and viewpoint and to inaccuracy in face local1There have been recent advances on 3D face recognition in situations where range data acquired through structured light can be matched reliably [Bronstein et al. 2003]. ization. However, the feature extraction techniques needed for this type of approach are still not reliable or accurate enough [Cox et al. 1996]. For example, most eye localization techniques assume some geometric and textural models and do not work if the eye is closed. Section 3 will present a review of still-image-based face recognition. During the past 5 to 8 years, much research has been concentrated on videobased face recognition. The still image problem has several inherent advantages and disadvantages. For applications such as drivers’ licenses, due to the controlled nature of the image acquisition process, the segmentation problem is rather easy. However, if only a static picture of an airport scene is available, automatic location and segmentation of a face could pose serious challenges to any segmentation algorithm. On the other hand, if a video sequence is available, segmentation of a moving person can be more easily accomplished using motion as a cue. But the small size and low image quality of faces captured from video can significantly increase the difficulty in recognition. Videobased face recognition is reviewed in Section 4. As we propose new algorithms and build more systems, measuring the performance of new systems and of existing systems becomes very important. Systematic data collection and evaulation of face recognition systems is reviewed in Section 5. Recognizing a 3D object from its 2D images poses many challenges. The illumination and pose problems are two prominent issues for appearance- or image-based approaches. Many approaches have been proposed to handle these issues, with the majority of them exploring domain knowledge. Details of these approaches are discussed in Section 6. In 1995, a review paper [Chellappa et al. 1995] gave a thorough survey of FRT at that time. (An earlier survey [Samal and Iyengar 1992] appeared in 1992.) At that time, video-based face recognition was still in a nascent stage. During the past 8 years, face recognition has received increased attention and has advanced ACM Computing Surveys, Vol. 35, No. 4, December 2003. Face Recognition: A Literature Survey 403 technically. Many commercial systems for still face recognition are now available. Recently, significant research efforts have been focused on video-based face modeling/tracking, recognition, and system integration. New datasets have been created and evaluations of recognition techniques using these databases have been carried out. It is not an overstatement to say that face recognition has become one of the most active applications of pattern recognition, image analysis and understanding. In this paper we provide a critical review of current developments in face recognition. This paper is organized as follows: in Section 2 we briefly review issues that are relevant from a psychophysical point of view. Section 3 provides a detailed review of recent developments in face recognition techniques using still images. In Section 4 face recognition techniques based on video are reviewed. Data collection and performance evaluation of face recognition algorithms are addressed in Section 5 with descriptions of representative protocols. In Section 6 we discuss two important problems in face recognition that can be mathematically studied, lack of robustness to illumination and pose variations, and we review proposed methods of overcoming these limitations. Finally, a summary and conclusions are presented in Section 7. 2. PSYCHOPHYSICS/NEUROSCIENCE ISSUES RELEVANT TO FACE RECOGNITION Human recognition processes utilize a broad spectrum of stimuli, obtained from many, if not all, of the senses (visual, auditory, olfactory, tactile, etc.). In many situations, contextual knowledge is also applied, for example, surroundings play an important role in recognizing faces in relation to where they are supposed to be located. It is futile to even attempt to develop a system using existing technology, which will mimic the remarkable face recognition ability of humans. However, the human brain has its limitations in the total number of persons that it can accurately “remember.” A key advantage of a computer system is its capacity to handle large numbers of face images. In most applications the images are available only in the form of single or multiple views of 2D intensity data, so that the inputs to computer face recognition algorithms are visual only. For this reason, the literature reviewed in this section is restricted to studies of human visual perception of faces. Many studies in psychology and neuroscience have direct relevance to engineers interested in designing algorithms or systems for machine recognition of faces. For example, findings in psychology [Bruce 1988; Shepherd et al. 1981] about the relative importance of different facial features have been noted in the engineering literature [Etemad and Chellappa 1997]. On the other hand, machine systems provide tools for conducting studies in psychology and neuroscience [Hancock et al. 1998; Kalocsai et al. 1998]. For example, a possible engineering explanation of the bottom lighting effects studied in Johnston et al. [1992] is as follows: when the actual lighting direction is opposite to the usually assumed direction, a shape-from-shading algorithm recovers incorrect structural information and hence makes recognition of faces harder. A detailed review of relevant studies in psychophysics and neuroscience is beyond the scope of this paper. We only summarize findings that are potentially relevant to the design of face recognition systems. For details the reader is referred to the papers cited below. Issues that are of potential interest to designers are2: —Is face recognition a dedicated process? [Biederman and Kalocsai 1998; Ellis 1986; Gauthier et al. 1999; Gauthier and Logothetis 2000]: It is traditionally believed that face recognition is a dedicated process different from other object recognition tasks. Evidence for the existence of a dedicated face processing system comes from several sources [Ellis 1986]. (a) Faces are more easily remembered by humans than other 2Readers should be aware of the existence of diverse opinions on some of these issues. The opinions given here do not necessarily represent our views. ACM Computing Surveys, Vol. 35, No. 4, December 2003. 404 Zhao et al. objects when presented in an upright orientation. (b) Prosopagnosia patients are unable to recognize previously familiar faces, but usually have no other profound agnosia. They recognize people by their voices, hair color, dress, etc. It should be noted that prosopagnosia patients recognize whether a given object is a face or not, but then have difficulty in identifying the face. Seven differences between face recognition and object recognition can be summarized [Biederman and Kalocsai 1998] based on empirical evidence: (1) configural effects (related to the choice of different types of machine recognition systems), (2) expertise, (3) differences verbalizable, (4) sensitivity to contrast polarity and illumination direction (related to the illumination problem in machine recognition systems), (5) metric variation, (6) Rotation in depth (related to the pose variation problem in machine recognition systems), and (7) rotation in plane/inverted face. Contrary to the traditionally held belief, some recent findings in human neuropsychology and neuroimaging suggest that face recognition may not be unique. According to [Gauthier and Logothetis 2000], recent neuroimaging studies in humans indicate that level of categorization and expertise interact to produce the specification for faces in the middle fusiform gyrus.3 Hence it is possible that the encoding scheme used for faces may also be employed for other classes with similar properties. (On recognition of familiar vs. unfamiliar faces see Section 7.) —Is face perception the result of holistic or feature analysis? [Bruce 1988; Bruce et al. 1998]: Both holistic and feature information are crucial for the perception and recognition of faces. Studies suggest the possibility of global descriptions serving as a front end for finer, feature-based perception. If dominant features are present, holistic descrip3The fusiform gyrus or occipitotemporal gyrus, located on the ventromedial surface of the temporal and occipital lobes, is thought to be critical for face recognition. tions may not be used. For example, in face recall studies, humans quickly focus on odd features such as big ears, a crooked nose, a staring eye, etc. One of the strongest pieces of evidence to support the view that face recognition involves more configural/holistic processing than other object recognition has been the face inversion effect in which an inverted face is much harder to recognize than a normal face (first demonstrated in [Yin 1969]). An excellent example is given in [Bartlett and Searcy 1993] using the “Thatcher illusion” [Thompson 1980]. In this illusion, the eyes and mouth of an expressing face are excised and inverted, and the result looks grotesque in an upright face; however, when shown inverted, the face looks fairly normal in appearance, and the inversion of the internal features is not readily noticed. —Ranking of significance of facial features [Bruce 1988; Shepherd et al. 1981]: Hair, face outline, eyes, and mouth (not necessarily in this order) have been determined to be important for perceiving and remembering faces [Shepherd et al. 1981]. Several studies have shown that the nose plays an insignificant role; this may be due to the fact that almost all of these studies have been done using frontal images. In face recognition using profiles (which may be important in mugshot matching applications, where profiles can be extracted from side views), a distinctive nose shape could be more important than the eyes or mouth [Bruce 1988]. Another outcome of some studies is that both external and internal features are important in the recognition of previously presented but otherwise unfamiliar faces, but internal features are more dominant in the recognition of familiar faces. It has also been found that the upper part of the face is more useful for face recognition than the lower part [Shepherd et al. 1981]. The role of aesthetic attributes such as beauty, attractiveness, and/or pleasantness has also been studied, with the conclusion that ACM Computing Surveys, Vol. 35, No. 4, December 2003. Face Recognition: A Literature Survey 405 the more attractive the faces are, the better is their recognition rate; the least attractive faces come next, followed by the midrange faces, in terms of ease of being recognized. —Caricatures [Brennan 1985; Bruce 1988; Perkins 1975]: A caricature can be formally defined [Perkins 1975] as “a symbol that exaggerates measurements relative to any measure which varies from one person to another.” Thus the length of a nose is a measure that varies from person to person, and could be useful as a symbol in caricaturing someone, but not the number of ears. A standard caricature algorithm [Brennan 1985] can be applied to different qualities of image data (line drawings and photographs). Caricatures of line drawings do not contain as much information as photographs, but they manage to capture the important characteristics of a face; experiments based on nonordinary faces comparing the usefulness of linedrawing caricatures and unexaggerated line drawings decidedly favor the former [Bruce 1988]. —Distinctiveness [Bruce et al. 1994]: Studies show that distinctive faces are better retained in memory and are recognized better and faster than typical faces. However, if a decision has to be made as to whether an object is a face or not, it takes longer to recognize an atypical face than a typical face. This may be explained by different mechanisms being used for detection and for identification. —The role of spatial frequency analysis [Ginsburg 1978; Harmon 1973; Sergent 1986]: Earlier studies [Ginsburg 1978; Harmon 1973] concluded that information in low spatial frequency bands plays a dominant role in face recognition. Recent studies [Sergent 1986] have shown that, depending on the specific recognition task, the low, bandpass and high-frequency components may play different roles. For example gender classification can be successfully accomplished using low-frequency components only, while identification requires the use of high-frequency components [Sergent 1986]. Low-frequency components contribute to global description, while high-frequency components contribute to the finer details needed in identification. —Viewpoint-invariant recognition? [Biederman 1987; Hill et al. 1997; Tarr and Bulthoff 1995]: Much work in visual object recognition (e.g. [Biederman 1987]) has been cast within a theoretical framework introduced in [Marr 1982] in which different views of objects are analyzed in a way which allows access to (largely) viewpointinvariant descriptions. Recently, there has been some debate about whether object recognition is viewpoint-invariant or not [Tarr and Bulthoff 1995]. Some experiments suggest that memory for faces is highly viewpoint-dependent. Generalization even from one profile viewpoint to another is poor, though generalization from one three-quarter view to the other is very good [Hill et al. 1997]. —Effect of lighting change [Bruce et al. 1998; Hill and Bruce 1996; Johnston et al. 1992]: It has long been informally observed that photographic negatives of faces are difficult to recognize. However, relatively little work has explored why it is so difficult to recognize negative images of faces. In [Johnston et al. 1992], experiments were conducted to explore whether difficulties with negative images and inverted images of faces arise because each of these manipulations reverses the apparent direction of lighting, rendering a top-lit image of a face apparently lit from below. It was demonstrated in [Johnston et al. 1992] that bottom lighting does indeed make it harder to identity familiar faces. In [Hill and Bruce 1996], the importance of top lighting for face recognition was demonstrated using a different task: matching surface images of faces to determine whether they were identical. —Movement and face recognition [O’Toole et al. 2002; Bruce et al. 1998; Knight and Johnston 1997]: A recent study [Knight ACM Computing Surveys, Vol. 35, No. 4, December 2003. 406 Zhao et al. and Johnston 1997] showed that famous faces are easier to recognize when shown in moving sequences than in still photographs. This observation has been extended to show that movement helps in the recognition of familiar faces shown under a range of different types of degradations—negated, inverted, or thresholded [Bruce et al. 1998]. Even more interesting is the observation that there seems to be a benefit due to movement even if the information content is equated in the moving and static comparison conditions. However, experiments with unfamiliar faces suggest no additional benefit from viewing animated rather than static sequences. —Facial expressions [Bruce 1988]: Based on neurophysiological studies, it seems that analysis of facial expressions is accomplished in parallel to face recognition. Some prosopagnosic patients, who have difficulties in identifying familiar faces, nevertheless seem to recognize expressions due to emotions. Patients who suffer from “organic brain syndrome” suffer from poor expression analysis but perform face recognition quite well.4 Similarly, separation of face recognition and “focused visual processing” tasks (e.g., looking for someone with a thick mustache) have been claimed. 3. FACE RECOGNITION FROM STILL IMAGES As illustrated in Figure 1, the problem of automatic face recognition involves three key steps/subtasks: (1) detection and rough normalization of faces, (2) feature extraction and accurate normalization of faces, (3) identification and/or verification. Sometimes, different subtasks are not totally separated. For example, the facial features (eyes, nose, mouth) used for face recognition are often used in face detection. Face detection and feature extraction can be achieved simultaneously, as indi4From a machine recognition point of view, dramatic facial expressions may affect face recognition performance if only one photograph is available. cated in Figure 1. Depending on the nature of the application, for example, the sizes of the training and testing databases, clutter and variability of the background, noise, occlusion, and speed requirements, some of the subtasks can be very challenging. Though fully automatic face recognition systems must perform all three subtasks, research on each subtask is critical. This is not only because the techniques used for the individual subtasks need to be improved, but also because they are critical in many different applications (Figure 1). For example, face detection is needed to initialize face tracking, and extraction of facial features is needed for recognizing human emotion, which is in turn essential in human-computer interaction (HCI) systems. Isolating the subtasks makes it easier to assess and advance the state of the art of the component techniques. Earlier face detection techniques could only handle single or a few well-separated frontal faces in images with simple backgrounds, while state-of-the-art algorithms can detect faces and their poses in cluttered backgrounds [Gu et al. 2001; Heisele et al. 2001; Schneiderman and Kanade 2000; Viola and Jones 2001]. Extensive research on the subtasks has been carried out and relevant surveys have appeared on, for example, the subtask of face detection [Hjelmas and Low 2001; Yang et al. 2002]. In this section we survey the state of the art of face recognition in the engineering literature. For the sake of completeness, in Section 3.1 we provide a highlighted summary of research on face segmentation/detection and feature extraction. Section 3.2 contains detailed reviews of recent work on intensity image-based face recognition and categorizes methods of recognition from intensity images. Section 3.3 summarizes the status of face recognition and discusses open research issues. 3.1. Key Steps Prior to Recognition: Face Detection and Feature Extraction The first step in any automatic face recognition systems is the detection of faces in images. Here we only provide a summary on this topic and highlight a few ACM Computing Surveys, Vol. 35, No. 4, December 2003. Face Recognition: A Literature Survey 407 very recent methods. After a face has been detected, the task of feature extraction is to obtain features that are fed into a face classification system. Depending on the type of classification system, features can be local features such as lines or fiducial points, or facial features such as eyes, nose, and mouth. Face detection may also employ features, in which case features are extracted simultaneously with face detection. Feature extraction is also a key to animation and recognition of facial expressions. Without considering feature locations, face detection is declared successful if the presence and rough location of a face has been correctly identified. However, without accurate face and feature location, noticeable degradation in recognition performance is observed [Martinez 2002; Zhao 1999]. The close relationship between feature extraction and face recognition motivates us to review a few feature extraction methods that are used in the recognition approaches to be reviewed in Section 3.2. Hence, this section also serves as an introduction to the next section. 3.1.1. Segmentation/Detection: Summary. Up to the mid-1990s, most work on segmentation was focused on single-face segmentation from a simple or complex background. These approaches included using a whole-face template, a deformable feature-based template, skin color, and a neural network. Significant advances have been made in recent years in achieving automatic face detection under various conditions. Compared to feature-based methods and template-matching methods, appearanceor image-based methods [Rowley et al. 1998; Sung and Poggio 1997] that train machine systems on large numbers of samples have achieved the best results. This may not be surprising since face objects are complicated, very similar to each other, and different from nonface objects. Through extensive training, computers can be quite good at detecting faces. More recently, detection of faces under rotation in depth has been studied. One approach is based on training on multipleview samples [Gu et al. 2001; Schneiderman and Kanade 2000]. Compared to invariant-feature-based methods [Wiskott et al. 1997], multiview-based methods of face detection and recognition seem to be able to achieve better results when the angle of out-of-plane rotation is large (35◦). In the psychology community, a similar debate exists on whether face recognition is viewpoint-invariant or not. Studies in both disciplines seem to support the idea that for small angles, face perception is view-independent, while for large angles, it is view-dependent. In a detection problem, two statistics are important: true positives (also referred to as detection rate) and false positives (reported detections in nonface regions). An ideal system would have very high true positive and very low false positive rates. In practice, these two requirements are conflicting. Treating face detection as a two-class classification problem helps to reduce false positives dramatically [Rowley et al. 1998; Sung and Poggio 1997] while maintaining true positives. This is achieved by retraining systems with falsepositive samples that are generated by previously trained systems. 3.1.2. Feature Extraction: Summary and Methods 3.1.2.1. Summary. The importance of facial features for face recognition cannot be overstated. Many face recognition systems need facial features in addition to the holistic face, as suggested by studies in psychology. It is well known that even holistic matching methods, for example, eigenfaces [Turk and Pentland 1991] and Fisherfaces [Belhumeur et al. 1997], need accurate locations of key facial features such as eyes, nose, and mouth to normalize the detected face [Martinez 2002; Yang et al. 2002]. Three types of feature extraction methods can be distinguished: (1) generic methods based on edges, lines, and curves; (2) feature-template-based methods that are used to detect facial features such as eyes; (3) structural matching methods ACM Computing Surveys, Vol. 35, No. 4, December 2003. 408 Zhao et al. that take into consideration geometrical constraints on the features. Early approaches focused on individual features; for example, a template-based approach was described in [Hallinan 1991] to detect and recognize the human eye in a frontal face. These methods have difficulty when the appearances of the features change significantly, for example, closed eyes, eyes with glasses, open mouth. To detect the features more reliably, recent approaches have used structural matching methods, for example, the Active Shape Model [Cootes et al. 1995]. Compared to earlier methods, these recent statistical methods are much more robust in terms of handling variations in image intensity and feature shape. An even more challenging situation for feature extraction is feature “restoration,” which tries to recover features that are invisible due to large variations in head pose. The best solution here might be to hallucinate the missing features either by using the bilateral symmetry of the face or using learned information. For example, a view-based statistical method claims to be able to handle even profile views in which many local features are invisible [Cootes et al. 2000]. 3.1.2.2. Methods. A template-based approach to detecting the eyes and mouth in real images was presented in [Yuille et al. 1992]. This method is based on matching a predefined parameterized template to an image that contains a face region. Two templates are used for matching the eyes and mouth respectively. An energy function is defined that links edges, peaks and valleys in the image intensity to the corresponding properties in the template, and this energy function is minimized by iteratively changing the parameters of the template to fit the image. Compared to this model, which is manually designed, the statistical shape model (Active Shape Model, ASM) proposed in [Cootes et al. 1995] offers more flexibility and robustness. The advantages of using the so-called analysis through synthesis approach come from the fact that the solution is constrained by a flexible statistical model. To account for texture variation, the ASM model has been expanded to statistical appearance models including a Flexible Appearance Model (FAM) [Lanitis et al. 1995] and an Active Appearance Model (AAM) [Cootes et al. 2001]. In [Cootes et al. 2001], the proposed AAM combined a model of shape variation (i.e., ASM) with a model of the appearance variation of shape-normalized (shape-free) textures. A training set of 400 images of faces, each manually labeled with 68 landmark points, and approximately 10,000 intensity values sampled from facial regions were used. The shape model (mean shape, orthogonal mapping matrix Ps and projection vector bs) is generated by representing each set of landmarks as a vector and applying principalcomponent analysis (PCA) to the data. Then, after each sample image is warped so that its landmarks match the mean shape, texture information can be sampled from this shape-free face patch. Applying PCA to this data leads to a shapefree texture model (mean texture, Pg and bg ). To explore the correlation between the shape and texture variations, a third PCA is applied to the concatenated vectors (bs and bg ) to obtain the combined model in which one vector c of appearance parameters controls both the shape and texture of the model. To match a given image and the model, an optimal vector of parameters (displacement parameters between the face region and the model, parameters for linear intensity adjustment, and the appearance parameters c) are searched by minimizing the difference between the synthetic image and the given one. After matching, a best-fitting model is constructed that gives the locations of all the facial features and can be used to reconstruct the original images. Figure 2 illustrates the optimization/search procedure for fitting the model to the image. To speed up the search procedure, an efficient method is proposed that exploits the similarities among optimizations. This allows the direct method to find and apply directions of rapid convergence which are learned off-line. ACM Computing Surveys, Vol. 35, No. 4, December 2003. Face Recognition: A Literature Survey 409 Fig. 2. Multiresolution search from a displaced position using a face model. (Courtesy of T. Cootes, K. Walker, and C. Taylor.) 3.2. Recognition from Intensity Images Many methods of face recognition have been proposed during the past 30 years. Face recognition is such a challenging yet interesting problem that it has attracted researchers who have different backgrounds: psychology, pattern recognition, neural networks, computer vision, and computer graphics. It is due to this fact that the literature on face recognition is vast and diverse. Often, a single system involves techniques motivated by different principles. The usage of a mixture of techniques makes it difficult to classify these systems based purely on what types of techniques they use for feature representation or classification. To have a clear and high-level categorization, we instead follow a guideline suggested by the psychological study of how humans use holistic and local features. Specifically, we have the following categorization: (1) Holistic matching methods. These methods use the whole face region as the raw input to a recognition system. One of the most widely used representations of the face region is eigenpictures [Kirby and Sirovich 1990; Sirovich and Kirby 1987], which are based on principal component analysis. (2) Feature-based (structural) matching methods. Typically, in these methods, local features such as the eyes, nose, and mouth are first extracted and their locations and local statistics (geometric and/or appearance) are fed into a structural classifier. (3) Hybrid methods. Just as the human perception system uses both local features and the whole face region to recognize a face, a machine recognition system should use both. One can argue that these methods could potentially offer the best of the two types of methods. Within each of these categories, further classification is possible (Table III). Using principal-component analysis (PCA), many face recognition techniques have been developed: eigenfaces [Turk and Pentland 1991], which use a nearestneighbor classifier; feature-line-based methods, which replace the point-to-point distance with the distance between a point and the feature line linking two stored sample points [Li and Lu 1999]; Fisherfaces [Belhumeur et al. 1997; Liu and Wechsler 2001; Swets and Weng 1996b; Zhao et al. 1998] which use linear/Fisher discriminant analysis (FLD/LDA) [Fisher 1938]; Bayesian methods, which use a probabilistic distance metric [Moghaddam and Pentland 1997]; and SVM methods, which use a support vector machine as the classifier [Phillips 1998]. Utilizing higherorder statistics, independent-component ACM Computing Surveys, Vol. 35, No. 4, December 2003. 410 Zhao et al. Table III. Categorization of Still Face Recognition Techniques Approach Representative work Holistic methods Principal-component analysis (PCA) Eigenfaces Direct application of PCA [Craw and Cameron 1996; Kirby and Sirovich 1990; Turk and Pentland 1991] Probabilistic eigenfaces Two-class problem with prob. measure [Moghaddam and Pentland 1997] Fisherfaces/subspace LDA FLD on eigenspace [Belhumeur et al. 1997; Swets and Weng 1996b; Zhao et al. 1998] SVM Two-class problem based on SVM [Phillips 1998] Evolution pursuit Enhanced GA learning [Liu and Wechsler 2000a] Feature lines Point-to-line distance based [Li and Lu 1999] ICA ICA-based feature analysis [Bartlett et al. 1998] Other representations LDA/FLD LDA/FLD on raw image [Etemad and Chellappa 1997] PDBNN Probabilistic decision based NN [Lin et al. 1997] Feature-based methods Pure geometry methods Earlier methods [Kanade 1973; Kelly 1970]; recent methods [Cox et al. 1996; Manjunath et al. 1992] Dynamic link architecture Graph matching methods [Okada et al. 1998; Wiskott et al. 1997] Hidden Markov model HMM methods [Nefian and Hayes 1998; Samaria 1994; Samaria and Young 1994] Convolution Neural Network SOM learning based CNN methods [Lawrence et al. 1997] Hybrid methods Modular eigenfaces Eigenfaces and eigenmodules [Pentland et al. 1994] Hybrid LFA Local feature method [Penev and Atick 1996] Shape-normalized Flexible appearance models [Lanitis et al. 1995] Component-based Face region and components [Huang et al. 2003] analysis (ICA) is argued to have more representative power than PCA, and hence may provide better recognition performance than PCA [Bartlett et al. 1998]. Being able to offer potentially greater generalization through learning, neural networks/learning methods have also been applied to face recognition. One example is the Probabilistic Decision-Based Neural Network (PDBNN) method [Lin et al. 1997] and the other is the evolution pursuit (EP) method [Liu and Wechsler 2000a]. Most earlier methods belong to the category of structural matching methods, using the width of the head, the distances between the eyes and from the eyes to the mouth, etc. [Kelly 1970], or the distances and angles between eye corners, mouth extrema, nostrils, and chin top [Kanade 1973]. More recently, a mixture-distance based approach using manually extracted distances was reported [Cox et al. 1996]. Without finding the exact locations of facial features, Hidden Markov Model- (HMM-) based methods use strips of pixels that cover the forehead, eye, nose, mouth, and chin [Nefian and Hayes 1998; Samaria 1994; Samaria and Young 1994]. [Nefian and Hayes 1998] reported better performance than Samaria [1994] by using the KL projection coefficients instead of the strips of raw pixels. One of the most successful systems in this category is the graph matching system [Okada et al. 1998; Wiskott et al. 1997], which is based on the Dynamic Link Architecture (DLA) [Buhmann et al. 1990; Lades et al. 1993]. Using an unsupervised learning method based on a self-organizing map (SOM), a system based on a convolutional neural network (CNN) has been developed [Lawrence et al. 1997]. In the hybrid method category, we will briefly review the modular eigenface method [Pentland et al. 1994], a hybrid representation based on PCA and local feature analysis (LFA) [Penev and Atick 1996], a flexible appearance model-based method [Lanitis et al. 1995], and a recent development [Huang et al. 2003] along this direction. In [Pentland et al. 1994], ACM Computing Surveys, Vol. 35, No. 4, December

****

**CHAPTER-3**

**FACE REGCONITION PROCESS**

**Step 1**. A picture of your face is captured from a photo or video. Your face might appear alone or in a crowd. Your image may show you looking straight ahead or nearly in profile.

**Step 2**. Facial recognition software reads the geometry of your face. Key factors include the distance between your eyes and the distance from forehead to chin. The software identifies facial landmarks — one system identifies 68 of them — that are key to distinguishing your face. The result: your facial signature.

**Step 3**. Your facial signature — a mathematical formula — is compared to a database of known faces. And consider this: At least 117 million Americans have images of their faces in one or more police databases. According to a May 2018 report, the FBI has had access to 412 million facial images for searches.

## A brief history of facial recognition

You can trace the history of facial recognition to the 1960s. That’s when mathematician and computer scientist Woodrow Wilson Bledsoe first developed a system of measurements that could be used to put photos of faces in different classifications. Because of this work, Bledsoe is known as the unofficial father of facial recognition technology.

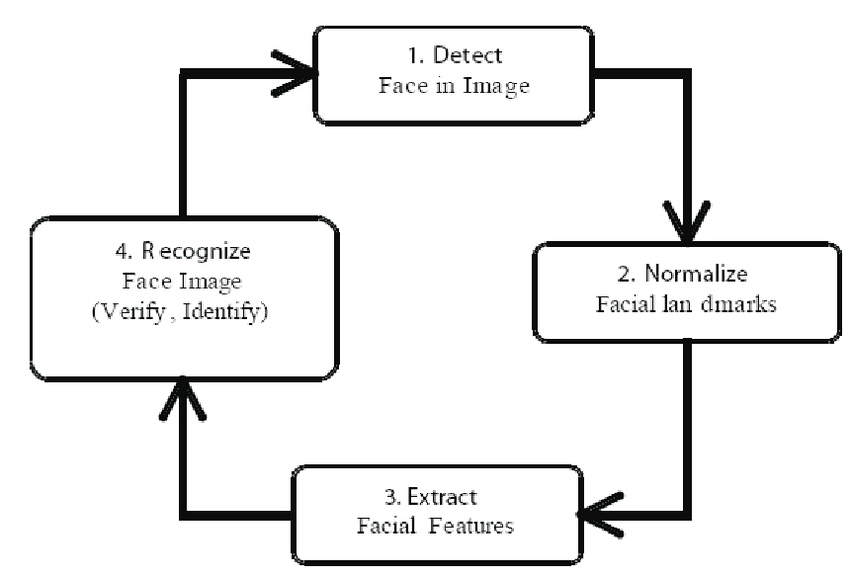
Law enforcement agencies soon became interested in Bledsoe’s work. And in the 1970s through the 1990s, agencies developed their own facial recognition systems. These were crude compared to the technology today, but the work on these systems did lead the way to modern facial recognition programs.

Many point to 2001 as a key year for facial recognition technology. That’s when law enforcement officials used facial recognition to help identify people in the crowd at Super Bowl XXXV. That same year, the Pinellas County Sheriff’s Office in Florida created its own facial recognition database.

It wasn’t until the 2010s, though, that computers grew powerful enough to make facial recognition a more standard feature. In 2011, in fact, facial recognition software confirmed the identity of terrorist Osama bin Laden. In 2015, the Baltimore police department used facial recognition to identify those who participated in protests after Freddie Gray was killed by a spinal injury that he suffered while being transported in a police van.

Consumers now use facial recognition with their smartphones and other personal devices. Windows Hello and Android’s Trusted Face in 2015 allowed people to log into their devices by simply aiming them at their faces. Apple’s iPhone X unveiled its Face ID facial recognition technology in 2017.

There has been controversy over this technology, with critics saying it is an invasion of privacy. Cities such as San Francisco, Oakland, and Boston have banned governments from using facial recognition. And after Black Lives Matter protests against police brutality in the summer of 2020, several tech giants, including Amazon, Microsoft, and IBM, announced that they would no longer sell their facial recognition technology to law enforcement agencies.



## How accurate is facial recognition?

Critics worry that facial recognition could lead to false identifications. What if a police department uses facial recognition technology to incorrectly identify someone breaking a store window during a riot as a person who was nowhere near the event? How likely is it that this could happen?

That depends. Tests by the National Institute of Standards and Technology say that as of April of 2020, the best face identification algorithm boasted an error rate of just 0.08%. That's a big improvement from 2014, when the best algorithm had an error rate of 4.1%.

Accuracy, though, is higher when identification algorithms are used to match people to clear, static images, such as a passport photo or mugshot, according to a **[story](https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter" \t "_blank)** by the Center for Strategic & International Studies (CSI) in 2020. The story said that facial recognition algorithms can hit accuracy scores as high as 99.97% on the National Institute of Standards and Technology's Facial Recognition Vendor Test when used in this way.

In the real world, though, accuracy rates are usually lower. According to the CSI story, the Facial Recognition Vendor Test found that the error rate for one algorithm rose from 0.1% when faces were matched against high-quality mugshots to 9.3% when matched to pictures of individuals captured in public. Error rates rose especially when subjects were not looking directly at the camera or were partially hidden by shadows or objects.

Aging is another challenge. The Facial Recognition Vendor Test said that middle-tier facial recognition algorithms had error rates that jumped by nearly a factor of 10 when they attempted to match photos of subjects that had been taken 18 years earlier.

## Who uses facial recognition

A lot of people and organizations use facial recognition — and in a lot of different places. Here’s a sampling:

* **U.S. government at airports**. Facial recognition systems can monitor people coming and going in airports. The Department of Homeland Security has used the technology to identify people who have overstayed their visas or may be under criminal investigation. Customs officials at Washington Dulles International Airport made their first arrest using facial recognition in August of 2018, catching an impostor trying to enter the country.
* **Mobile phone makers in products**. Apple first used facial recognition to unlock its iPhone X, and has continued with the technology with the iPhone XS. Face ID authenticates — it makes sure you’re you when you access your phone. Apple says the chance of a random face unlocking your phone is about one in 1 million.
* **Colleges in the classroom**. Facial recognition software can, in essence, take roll. If you decide to cut class, your professor could know. Don’t even think of sending your brainy roommate to take your test.
* **Social media companies on websites**. Facebook uses an algorithm to spot faces when you upload a photo to its platform. The social media company asks if you want to tag people in your photos. If you say yes, it creates a link to their profiles. Facebook can recognize faces with 98 percent accuracy.
* **Businesses at entrances and restricted areas**. Some companies have traded in security badges for facial recognition systems. Beyond security, it could be one way to get some face time with the boss.
* **Religious groups at places of worship**. Churches have used facial recognition to scan their congregations to see who’s present. It’s a good way to track regulars and not-so-regulars, as well as to help tailor donation requests.
* **Retailers in stores**. Retailers can combine surveillance cameras and facial recognition to scan the faces of shoppers. One goal: identifying suspicious characters and potential shoplifters.
* **Airlines at departure gates**. You might be accustomed to having an agent scan your boarding pass at the gate to board your flight. At least one airline scans your face.
* **Marketers and advertisers in campaign**s. Marketers often consider things like gender, age, and ethnicity when targeting groups for a product or idea. Facial recognition can be used to define those audiences even at something like a concert.

## Facial recognition and its use in law enforcement

Facial recognition databases play a significant role in law enforcement today. According to a **[report](https://www.eff.org/pages/face-recognition" \t "_blank)** by the Electronic Frontier Foundation, law enforcement agencies routinely collect mugshots from those who have been arrested and compare them to local, state, and federal facial recognition databases.

Law enforcement agencies can sift through these mugshot databases to identify people in photos taken from a variety of sources: closed-circuit television cameras, traffic cameras, social media, or photos that police officers have taken themselves.

Police officers can also use their smartphones, tablets, or other mobile devices to snap photos of drivers or pedestrians and immediately compare their photo against the faces in one or more facial recognition databases, the Electronic Frontier Foundation says.

And law enforcement has used facial recognition at large events such as concerts, sporting events, or the Olympics to identity people who might be wanted in connection with crimes.

The federal government can use several facial recognition systems. The database it relies on most frequently, though, is the FBIs Next Generation Identification system. This database contains more than 30 million facial records.

## Facial recognition examples

Businesses use facial recognition in a variety of ways today, usually to make it easier for consumers to use their products or services. Here are some examples:

**Traveling**: British Airways uses facial recognition to make it easier for U.S. passengers to board their flights. Passengers can have their faces scanned by a camera to verify their identity. This way, they can board their flights without having to show a passport or boarding pass.

**Apple**: Apple could be considered a pioneer in facial recognition. The tech giant has long allowed consumers to unlock their phones, log into apps, and make purchases just by showing their face to their smartphones and other devices.

**Driving**: Automakers are testing facial recognition technology to help cut down on car theft. Consider Project Mobil: Ford and Intel are testing a project in which a dashboard camera uses facial recognition to identify the primary driver of a car and, perhaps, other authorized drivers. The tech could prevent a car from starting if someone other than a rightful driver is sitting behind the wheel.

**Banking**: Banking giants such as HSBC and Chase already use Apple's FaceID to let customers log into their mobile banking apps. Other financial institutions are testing facial recognition to allow customers to use their phone's cameras to approve online purchases.

**Insurance**: Cigna allows customers in China to file health insurance claims using their photos instead of a written signature. The insurance company says it’s a way to cut down on insurance fraud.

**Even soft drinks**: Coca-Cola has been a longtime user of facial recognition. For instance, the company uses the technology to reward customers for recycling at some of its vending machines in China. It also uses facial recognition to send customers in some countries personalized ads when they use vending machines.

## Facial recognition pros and cons

As a relatively new technology, we're still understanding the pros and cons of facial recognition. But here is a brief list of both the positives and possible negatives of this technology.

### Pros

**Finding missing people**: With facial recognition, law enforcement agencies have been able to track down missing children, sometimes even after they've been missing for years.

**Identifying criminals**: Law enforcement agencies can also use facial recognition to identify criminals or suspects in crimes.

**Making flying safer**: Airports across the globe are using facial recognition to identify criminals and potential threats as they enter airports or try to board flights.

**More efficient shopping?** Retailers can use facial recognition to make it easier for consumers to check out. Instead of forcing customers to pay with cash or credit, retailers can use facial recognition to immediately charge their purchases to their accounts.

### Cons

**A threat to privacy?** Do you want your face saved in a database that law enforcement agencies can tap? Do you want retailers to have a saved image of your face? If you don’t, you're not alone. Many critics worry that facial recognition is one more erosion of personal privacy.

**Mistaken identity**: Facial recognition isn't perfect. What if a law enforcement agency mistakenly identifies you as a criminal suspect when you're filing into your favorite ballpark?

**It can be tricked**: Criminals can trick facial recognition by wearing masks or facial disguises. This could lessen the effectiveness of this tech.

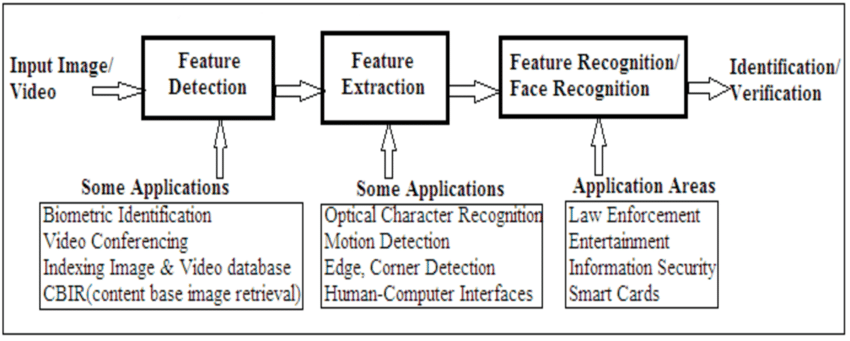
**Aging lowers its effectiveness**: Studies have found that as people age, and their features change, facial recognition has an increasingly difficult time identifying them. Other studies have shown that facial recognition is less effective in identifying people of color and women.

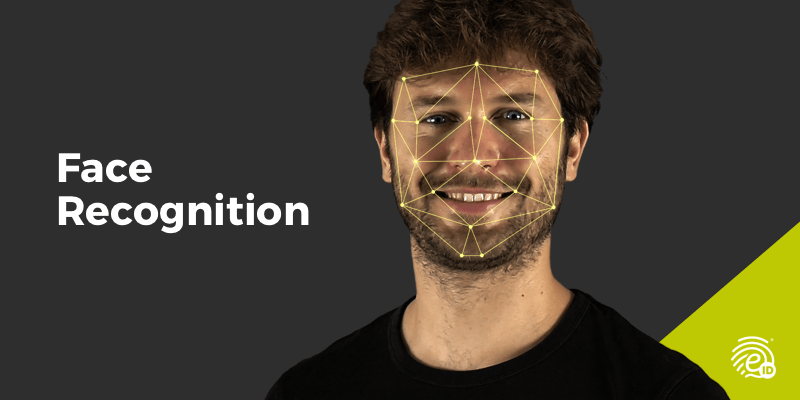
## Reasons to be concerned about your privacy

Privacy matters. Privacy refers to any rights you have to control your personal information and how it’s used — and that can include your faceprint.

So, what are the issues? Here are some:

* **Security**. Your facial data can be collected and stored, often without your permission. It’s possible hackers could access and steal that data.
* **Prevalence**. Facial recognition technology is becoming more widespread. That means your facial signature could end up in a lot of places. You probably won’t know who has access to it.
* **Ownership**. You own your face — the one atop your neck — but your digital images are different. You may have given up your right to ownership when you signed up on a social media network. Or maybe someone tracks down images of you online and sells that data.
* **Safety**. Facial recognition could lead to online harassment and stalking. How? For example, someone takes your picture on a subway or some other public place and uses facial recognition software to find out exactly who you are.
* **Mistaken identity**. Say, for instance, law enforcement uses facial recognition to try to identify someone who robbed a corner store. Facial recognition systems may not be 100 percent accurate. What if the police think the suspect is you?
* **Basic freedoms**. Government agencies and others could have the ability to track you. What you do and where you go might no longer be private. It could become impossible to remain anonymous.

****

****

**CHAPTER - 4**

**OBJECTIVE**

The objective of face recognition is, from the incoming image, **to find a series of data of the same face in a set of training images in a database**. The great difficulty is ensuring that this process is carried out in real-time, something that is not available to all biometric facial recognition software providers

**CHAPTER – 5**

**SCOPE**

This system can be deployed for **verification and attendance tracking at various government offices and corporates**. For access control verification and identification of authentic users it can also be installed in bank lockers and vaults. For identification of criminals the system can be used by police force also.

**This system can be effectively used in ATM's ,identifying duplicate voters, passport and visa verification, driving license verification, in defense, competitive and other exams, in governments and private sectors**.

Facial recognition is a way of using software **to determine the similarity between two face images in order to evaluate a claim**. The technology is used for a variety of purposes, from signing a user into their phone to searching for a particular person in a database of photos.

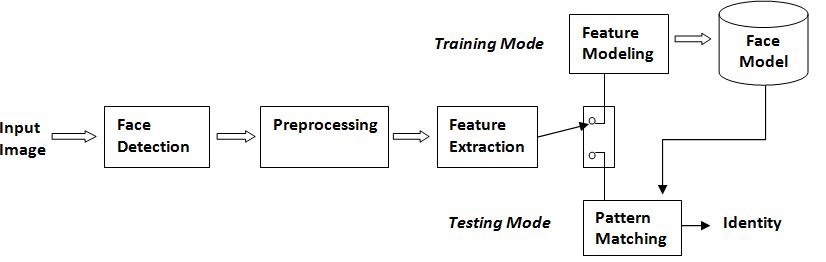
[[](https://www.google.com/search?sxsrf=ALiCzsZGYjczy72Cpeiuj7A1J7ZghpLdjQ:1651343897036%26q=What+is+the+future+scope+of+face+detection?%26tbm=isch%26source=iu%26ictx=1%26vet=1%26fir=1dGkaYD1yRo5VM,YGqx5R_9qBlnaM,_%26usg=AI4_-kSvedRZ9vrhoGIir4PMCBy02xLorA%26sa=X%26ved=2ahUKEwig34mzt7z3AhUGUGwGHUzoC9wQ9QF6BAgVEAE#imgrc=1dGkaYD1yRo5VM)](https://www.google.com/search?sxsrf=ALiCzsZGYjczy72Cpeiuj7A1J7ZghpLdjQ:1651343897036&q=What+is+the+future+scope+of+face+detection?&tbm=isch&source=iu&ictx=1&vet=1&fir=1dGkaYD1yRo5VM%252CYGqx5R_9qBlnaM%252C_&usg=AI4_-kSvedRZ9vrhoGIir4PMCBy02xLorA&sa=X&ved=2ahUKEwig34mzt7z3AhUGUGwGHUzoC9wQ9QF6BAgVEAE" \l "imgrc=1dGkaYD1yRo5VM)

**CHAPTER -6**

**DESIGN**

**6.1 SOFTWARE ENGINEERNG MODEL USED**

ITERATIVE WATERFALL MODEL



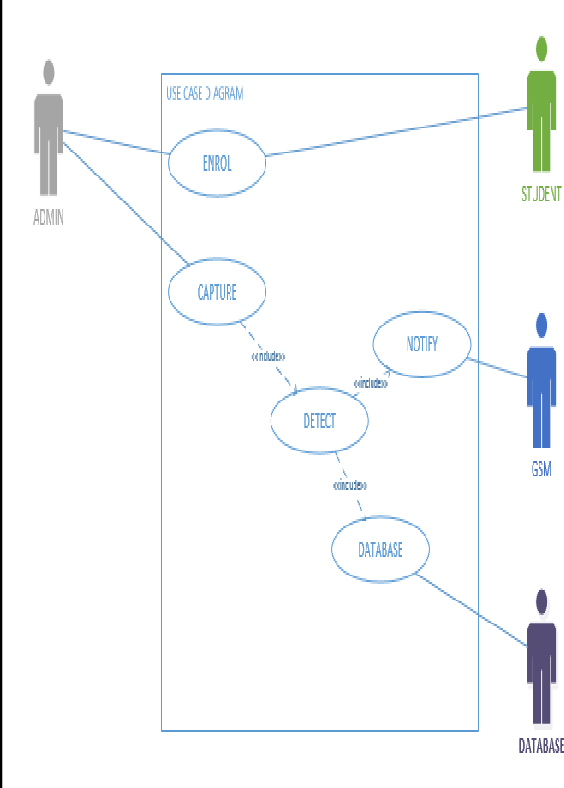
The Iterative waterfall model can be thought of as incorporating the necessary changes to the classical waterfall model to make it usable in practical software development projects. It is almost the same as the classical waterfall model except some changes are made to increase the efficiency of the software development.

The iterative waterfall model provides feedback paths from every phase to its preceding phases, which is the main difference from the classical waterfall model.

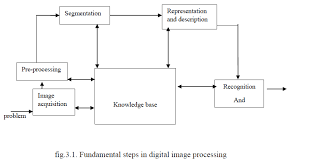
When errors are detected at some later phase, these feedback paths allow correcting errors committed by programmers during some phase. The feedback paths allow the phase to be reworked in which errors are committed and these changes are reflected in the later phases. But, there is no feedback path to the stage – feasibility study, because once a project has been taken, does not give up the project easily.

It is good to detect errors in the same phase in which they are committed. It reduces the effort and time required to correct the errors.

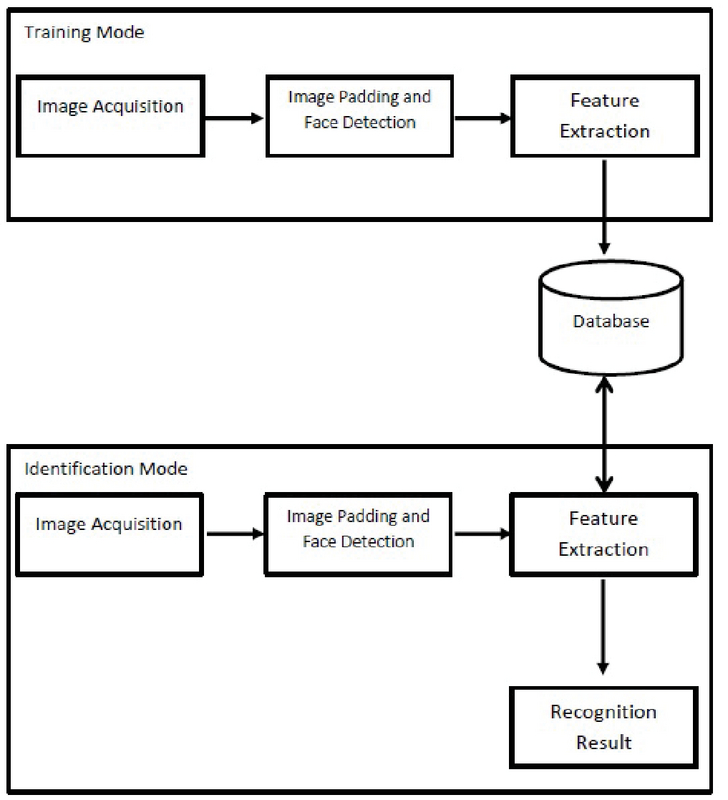
**6.2 USE CASE DIAGRAM**

****

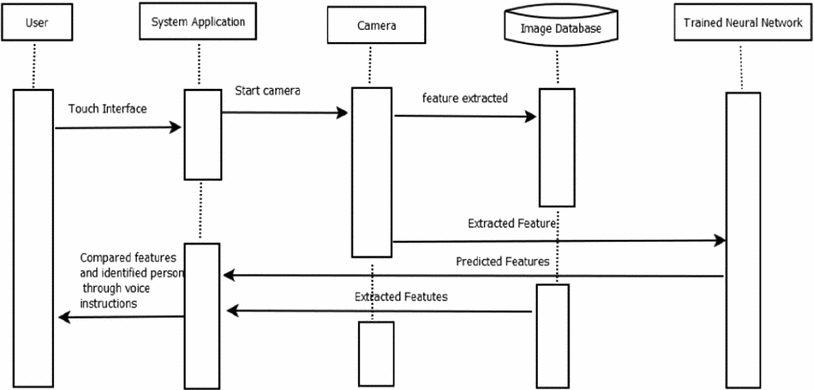
**6.3 ER – DIAGRAM**

****

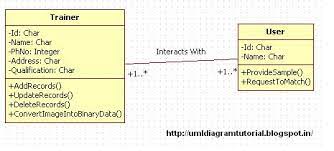
**6.4 DATA FLOW DIGRAM**

****

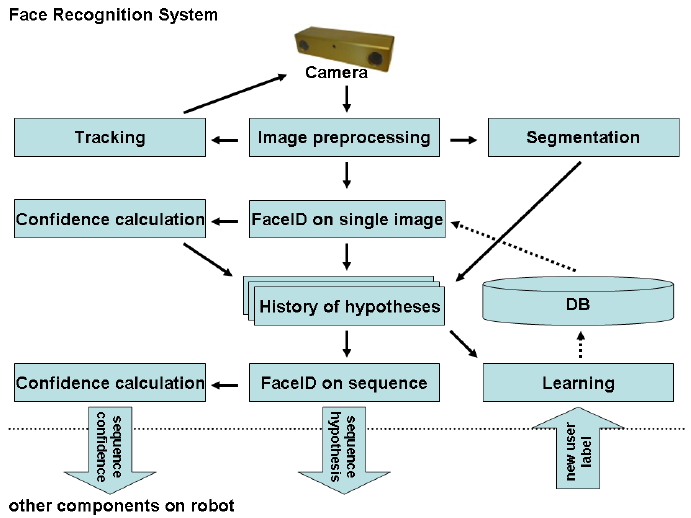
**6.5 SEQUENCE DIGRAM**



**6.6 CLASS DIAGRAM**

****

**6.7 DEPLOYMENT DIAGRAM**

****

**CHAPTER – 7**

**IMPLEMENTATION REQUIREMENT**

**7.1 Software Requirement**

* 4 GB RAM (Minimum)
* 80 GB HDD.
* Dual Core processor.
* CDROM (installation only). VGA resolution monitor.
* Microsoft Windows 98/2000/NT with service pack 6 / XP with service pack 2/ Windows 7 with service pack 2.
* SQL Server 2008 R2.

**7.2 Hardware Requirement**

* 4 GB RAM (Minimum)
* 80 GB HDD.
* Dual Core processor.
* CDROM (installation only). VGA resolution monitor.
* Microsoft Windows 98/2000/NT with service pack 6 / XP with service pack 2/ Windows 7 with service pack 2.
* SQL Server 2008 R2.

**CHAPTER - 8**

**CONCLUSION AND FUTURE WORK**

**8.1 CONCLUSION**

The computational models, which were implemented in this project, were chosen after extensive research, and the successful testing results confirm that the choices made by the researcher were reliable.The system with manual face detection and automatic face recognition did not have a recognition accuracy over 90%, due to the limited number of eigenfaces that were used for the PCA transform. This system was tested under very robust conditions in this experimental study and it is envisaged that real-world performance will be far more accurate.The fully automated frontal view face detection system displayed virtually perfect accuracy and in the researcher's opinion further work need not be conducted in this area. The fully automated face detection and recognition system was not robust enough to achieve a high recognition accuracy. The only reason for this was the face recognition subsystem did not display even a slight degree of invariance to scale, rotation or shift errors of the segmented face image. This was one of the system requirements identified in section 2.3. However, if some sort of further processing, such as an eye detection technique, was implemented to further normalise the segmented face image, performance will increase to levels comparable to the manual face detection and recognition system. Implementing an eye detection technique would be a minor extension to the implemented system and would not require a great deal of additional research.All other implemented systems displayed commendable results and reflect well on the deformable template and Principal Component Analysis strategies.The most suitable real-world applications for face detection and recognition systems are for mugshot matching and surveillance. There are better techniques such as iris or retina recognition and face recognition using the thermal spectrum for user access and user verification applications since these need a very high degree of accuracy.The real-time automated pose invariant face detection and recognition system proposed in chapter seven would be ideal for crowd surveillance applications. If such a system were widely implemented its potential for locating and tracking suspects for law enforcement agencies is immense. The implemented fully automated face detection and recognition system (with an eye detection system) could be used for simple surveillance applications such as ATM user security, while the implemented manual face detection and automated recognition system is ideal of mugshot matching. Since controlled conditions are present when mugshots are gathered, the frontal view face recognition scheme should display a recognition accuracy far better than the results, which were obtained in this study, which was conducted under adverse conditions. Department of ECE Page 48 Furthermore, many of the test subjects did not present an expressionless, frontal view to the system. They would probably be more compliant when a 6'5'' policeman is taking their mugshot! In mugshot matching applications, perfect recognition accuracy or an exact match is not a requirement. If a face recognition system can reduce the number of images that a human operator has to search through for a match from 10000 to even a 100, it would be of incredible practical use in law enforcement. The automated vision systems implemented in this thesis did not even approach the performance, nor were they as robust as a human's innate face recognition system. However, they give an insight into what the future may hold in computer vision.

CHAPTER 9

TEST CASES

**9.1 FUTURE WORK**

## Future uses of facial recognition

Some industries have been harder hit than others by the COVID-19 pandemic and this has meant that they have had to adapt much quicker and pivot to the use of new technologies in order to prepare for the world opening up again.

Events – both on a local and global scale – has been one of the most impacted industries as restrictions on numbers, social distancing, mandatory masks and other safety precautions have meant that organisers have had to rethink the way events are managed. Many events over the past 18 months have been conducted virtually, however, as we start to open up and international travel starts again, event organisers are turning to facial recognition as a way of managing access, check-in, visitor experience and safety.

[NEC worked with the Ladies Professional Golf Association (LPGA)](https://www.lpga.com/news/2017-nec-introduces-facial-recognition-software-at-ana-inspiration" \t "_blank) at the 2017 ANA Inspiration at Mission Hills Country Club.  Credentialed media covering the LPGA major championship passed through NEC’s NeoFace Watch face recognition solution before being allowed access to the ANA Inspiration Media Center, enabling secure entry to the facility.

Event organisers are also turning to facial recognition used in conjunction with an app to allow people to register for an event. When attending the event, facial recognition can then be used for admittance and allocation of seats without having to produce a ticket.

The automobile industry is another that is investing in facial recognition technology. Last year, about $6 billion was lost to motor vehicle theft in the US alone. Obviously, there is a need for a new, reliable safety measure that would keep car owners at peace even when they’re not around their car. Face recognition is already helping to provide that extra layer of safety and help reduce thefts.

Face recognition in automobiles works on a simple and non-obtrusive principle. After a driver enrols into the system, the system “remembers” them. Each time they enter the vehicle again, the system “recognises” them and gives them access to predefined functionalities such as permission to start the car.

Car owners can also set up permissions or restrictions for other people such as family members. For example, they could set up certain restrictions on their children learning to drive such as a time or speed limit or deny access without an adult present. If an unauthorised person enters the car, the system can notify the owner or block the car from starting. This helps prevent theft and gives owners better control of their cars.

[Hyundai is one of the companies leading the way](https://tech.hyundaimotorgroup.com/article/in-car-biometric-technology-for-human-interaction/" \t "_blank) when it comes to biometric integration. In 2018, they introduced the world’s first fingerprint system that locks the doors and starts the engine, through its Chinese Santa Fe.

Using iris recognition, their Driver State Warning System (DSW) is a feature that delivers a warning when the driver is not focusing on driving, and it takes a step forward from the current system that only recognises the direction of the face or when the eyes are closed, providing a safer driving environment.

DSW’s facial recognition technology identifies drivers through facial features such as eyes, nose, mouth, and ears. In addition, the system analyses the pupil and facial movement, then combines with driving information such as the speed of the car and steering angle, to offer safer driving. It detects the risk of lane departure and intrusion caused by driver carelessness in advance and calls the driver’s attention with cluster warning lights, alarm sounds, and vibrations.

## summery

Facial recognition is here to stay and rather than seeing facial recognition as a threat to our personal privacy, we should instead be embracing the many benefits that faciaSummal recognition provides.

Whilst there are isolated cases of facial recognition being used inappropriately, there are now thousands of use cases that show that, when deployed appropriately and with the consent of people using the software, facial recognition is helping to create a safer environment, providing outstanding security and enhancing customer experiences across a wide range of settings.

**REFERENCES**

• Adelson, E. H., and Bergen, J. R. (1986) The Extraction of Spatio-Temporal Energy in

• Human and Machine Vision, Proceedings of Workshop on Motion: Representation and

• Analysis (pp. 151-155) Charleston, SC; May 7-9 • AAFPRS(1997). A newsletter from the American Academy of Facial Plastic and Reconstructive Surgery. Third Quarter 1997, Vol. 11, No. 3. Page 3.

• Baron, R. J. (1981). Mechanisms of human facial recognition. International Journal of Man Machine Studies, 15:137-178

• Beymer, D. and Poggio, T. (1995) Face Recognition From One Example View, A.I. Memo No. 1536, C.B.C.L. Paper No. 121. MIT

• Bichsel, M. (1991). Strategies of Robust Objects Recognition for Automatic Identification of Human Faces. PhD thesis, , Eidgenossischen Technischen Hochschule, Zurich.

• Brennan, S. E. (1982) The caricature generator. M.S. Thesis. MIT.

• Brunelli, R. and Poggio, T. (1993), Face Recognition: Features versus Templates. IEEE Transactions on Pattern Analysis and Machine Intelligence, 15(10):1042-1052

• Craw, I., Ellis, H., and Lishman, J.R. (1987). Automatic extraction of face features. Pattern Recognition Letters, 5:183-187, February.

• Deffenbacher K.A., Johanson J., and O'Toole A.J. (1998) Facial ageing, attractiveness, and distinctiveness. Perception. 27(10):1233-1243

• Dunteman, G.H. (1989) Principal Component Analysis. Sage Publications.

• Frank, H. and Althoen, S. (1994). Statistics: Concepts and applications. Cambridge University Press. p.110

• Gauthier, I., Behrmann, M. and Tarr, M. (1999). Can face recognition really be dissociated from object recognition? Journal of Cognitive Neuroscience, in press

. • Goldstein, A.J., Harmon, L.D., and Lesk, A.B. (1971). Identification of human faces. In Proc. IEEE, Vol. 59, page 748

• de Haan, M., Johnson, M.H. and Maurer D. (1998) Recognition of individual faces and average face prototypes by 1- and 3- month-old infants. Centre for Brain and Cognitive

• Development, Department of Psychology, Birkbeck College.

• Hadamard, J. (1923) Lectures on the Cauchy Problem in Linear Partial Differential Equations , Yale University Press Department of ECE Page 50

• Haralick, R.M. and Shapiro, L.G.. (1992) Computer and Robot Vision, Volume I. Addison-Wesley

• Haxby, J.V., Ungerleider, L.G., Horwitz, B., Maisog, J.M., Rapoport, S.I., and Grady, C.L. (1996). Face encoding and recognition in the human brain. Proc. Nat. Acad. Sci. 93: 922 - 927.

• Heisele, B. and Poggio, T. (1999) Face Detection. Artificial Intelligence Laboratory. MIT.

• Jang., J., Sun, C., and Mizutani, E. (1997) Neuro-Fuzzy and Soft Computing. Prentice Hall.

• Johnson, R.A., and Wichern, D.W. (1992) Applied Multivariate Statistical Analysis. Prentice Hall. p356-395

**APPENDIX**

FACE DETECTION:

To detect Face FDetect = vision.CascadeObjectDetector; %Read the input image I = imread('HarryPotter.jpg'); %Returns Bounding Box values based on number of objects BB = step(FDetect,I); figure, imshow(I); hold on for i = 1:size(BB,1) rectangle('Position',BB(i,:),'LineWidth',5,'LineStyle','- ','EdgeColor','r'); end title('Face Detection'); hold off; The step(Detector,I) returns Bounding Box value that contains [x,y,Height,Width] of the objects of interest. clear all clc %Detect objects using Viola-Jones Algorithm %

BB = 52 38 73 73 379 84 71 71 198 57 72 72 %

NOSE DETECTION:

%To detect nose NoseDetect= vision.CascadeObjectDetector('Nose','MergeThreshold',16); BB=step(NoseDetect,I); figure, imshow(I); hold on for i = 1:size(BB,1) rectangle('Position',BB(i,:),'LineWidth',4,'LineStyle','- ','EdgeColor','b'); end title('Nose Detection'); hold off; EXPLANATION: To denote the object of interest as 'nose', the argument 'Nose' is passed. vision.CascadeObjectDetector('Nose','MergeThreshold',16); The default syntax for Nose detection : vision.CascadeObjectDetector('Nose'); Based on the input image, we can modify the default values of the parameters passed to vision.CascaseObjectDetector. Here the default value for 'MergeThreshold' is 4. When default value for 'MergeThreshold' is used, the result is not correct. Here there are more than one detection on Hermione. To avoid multiple detection around an object, the 'MergeThreshold' value can be overridden

MOUTH DETECTION:

%To detect Mouth MouthDetect = vision.CascadeObjectDetector('Mouth','MergeThreshold',16); BB=step(MouthDetect,I); figure, imshow(I); hold on for i = 1:size(BB,1) rectangle('Position',BB(i,:),'LineWidth',4,'LineStyle','- ','EdgeColor','r'); end title('Mouth Detection'); hold off;

EYE DETECTION:

%To detect Eyes EyeDetect = vision.CascadeObjectDetector('EyePairBig'); %Read the input Image I = imread('harry\_potter.jpg'); BB=step(EyeDetect,I); figure,imshow(I); rectangle('Position',BB,'LineWidth',4,'LineStyle','-','EdgeColor','b'); title('Eyes Detection'); Eyes=imcrop(I,BB); figure,imshow(Eyes);