



# FACE RECOGNITION SYSTEM USING OPEN CV

MOHD VIKAR<sup>1</sup> UMAR

HASAN<sup>2</sup> MAAZ AHMAD<sup>3</sup>

ABU SEHEL<sup>4</sup>

DR PRAVEEN KUMAR<sup>5</sup> MRS MANSI

AGGARWAL<sup>6</sup>

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

RISHI INSTITITUE OF ENGINEERING AND TECHNOLOGY, MEERUT UP

&

DELHI INSTITUTE OF ENGINEERING AND TECHNOLOGY, MEERUT UP

## ABSTRACT

Identifying a person with an image has been popularised through the mass media. However, it is less robust to fingerprint or retina scanning. This report describes the face detection and recognition mini-project undertaken for the visual perception and autonomy module at Plymouth university. It reports the technologies available in the Open-Computer-Vision (OpenCV) library and methodology to implement them using Python.

For face detection, Haar-Cascades were used and for face recognition Eigenfaces, Fisherfaces and Local binary pattern histograms were used. The methodology is described including flow charts for each stage of the system. Next, the results are shown including plots and screenshots followed by a discussion of encountered challenges. The report is concluded with the authors' opinion on the project and possible applications.

In this report, we use two approaches for detecting a face and track it continuously. Basically video sequences provide more information than a still image. Whereas the Viola Jones algorithm is used to detect the face based on the Haar features. We have modified the algorithm to make it work, a bit more efficient than what it was.

**Keywords: Python, Open CV, Face Recognition**

## INTRODUCTION

In recent years, face recognition has gained significant attention in various fields, such as security, surveillance, and human-computer interaction, due to its capability to identify and verify human identities. In this project, we will be designing and implementing an efficient Face Recognition System in Python that can detect and authenticate a person via their facial features.

Face recognition technology has gone from being a futuristic idea to becoming a reality today. With advances in machine learning technology, the technology has advanced to the point where it is now possible to accurately recognize and identify an individual based solely on their facial features. In this project report, we will explain how to build a face recognition system in Python.

Face recognition system is a biometric technology which has been developed to recognize and identify human faces based on their facial features. The system uses various algorithms and techniques to capture, analyze, and compare different facial features to identify an individual. The purpose of this project is to design and develop a face recognition system in Python using OpenCV, a Python library that provides computer vision and machine learning tools.

## OBJECTIVE

The objective of this project is to create a facial recognition system using advanced machine learning algorithms and computer vision techniques. The system will detect human faces from images and videos, extract their facial features, and recognize the person based on their previously saved data.

This project is to build a face recognition system using Python that can accurately identify individuals based on their facial features. We will use various Python libraries such as

OpenCV, NumPy, and dlib to build the system. The project will include capturing images of individuals, training the system on these images, and then testing the system to see how accurate it can recognize individuals.

## GOAL

The goal of face detection is to locate and identify human faces within digital images or video frames. Face detection algorithms analyze the visual information to determine the presence and location of faces in an image or video. The primary objective is to accurately detect the facial regions, usually represented by rectangles or bounding boxes, in order to perform various tasks such as face recognition, facial expression analysis, age estimation, gender classification, and more.

**The purpose of face detection can vary depending on the application. Some common use cases include:**

**Face recognition:** After detecting a face, further analysis can be performed to identify the person by comparing their facial features with a database of known individuals.

**Biometric systems:** Face detection is a crucial step in biometric authentication systems, where the goal is to match a detected face with the enrolled data of a specific individual for access control or identity verification purposes.

**Surveillance and security:** Face detection plays a vital role in surveillance systems, helping to identify individuals in crowds or monitor specific individuals of interest.

**Emotion detection:** By detecting faces, it becomes possible to analyze facial expressions and infer emotional states, enabling applications such as sentiment analysis or human-computer interaction.

**Augmented reality and image processing:** Face detection is essential in various interactive applications, including applying digital masks or filters to detected faces, or for other image processing tasks like facial feature tracking or gaze estimation.

Overall, the goal of face detection is to enable computers to automatically locate and understand human faces, providing a foundation for a wide range of applications that rely on facial information.

## THE HISTORY OF FACE RECOGNITION

The history of face recognition can be traced back several decades, with advancements in technology and research leading to its development. Here's an overview of the key milestones and advancements in the history of face recognition:

**1960s-1970s:** The early stages of face recognition research began in the 1960s and 1970s. The initial focus was on manual analysis of photographs and subjective identification by humans.

**1980s:** The introduction of computer-based face recognition systems marked a significant step forward. Researchers started developing algorithms to automatically detect and analyze facial features. One notable method was the Eigenfaces approach proposed by Sirovich and Kirby in 1987, which used principal component analysis (PCA) for facial feature extraction.

**1990s:** In the 1990s, face recognition gained further attention and progress. Researchers explored different techniques, including local feature-based methods such as the active appearance model (AAM) and elastic bunch graph matching (EBGM). These approaches focused on capturing the variations in facial appearance caused by changes in expression, pose, and lighting conditions.

**2000s:** The 2000s saw advancements in face recognition driven by the availability of large datasets and more powerful computing capabilities. Discriminative models, such as Support Vector Machines (SVM) and Neural Networks, gained popularity for face recognition tasks. Additionally, the introduction of 3D face recognition techniques using depth sensors provided a more robust representation of facial geometry.

**2010s:** Deep learning revolutionized the field of face recognition in the 2010s. Convolutional Neural Networks (CNN) emerged as a powerful tool for feature extraction, enabling significant improvements in accuracy and robustness. Notable breakthroughs, such as the DeepFace system by Facebook and the FaceNet system by Google, showcased the potential of deep learning for face recognition.

**Recent developments:** In recent years, face recognition has continued to evolve and be integrated into various applications. Mobile devices and social media platforms commonly use face recognition for user authentication and tagging photos. However, ethical concerns surrounding privacy, bias, and potential misuse of facial recognition technology have also gained attention, leading to discussions and debates about its responsible deployment.

Overall, the history of face recognition has witnessed a progression from manual analysis to automated algorithms, from feature-based methods to deep learning approaches, and from limited applications to widespread use in various domains. Ongoing research and advancements continue to enhance the accuracy, speed, and ethical considerations of face recognition systems.

## ADVANTAGES OF FACE DETECTION:

**Automation:** Face detection automates the process of locating and identifying human faces in images or video frames, eliminating the need for manual effort and enabling efficient analysis of large datasets.

**Versatility:** Face detection can be applied to a wide range of applications, including face recognition, surveillance, biometric authentication, emotion analysis, augmented reality, and more. It provides a foundational technology for numerous use cases.

**User Authentication:** Face detection can be used for secure user authentication. By matching a detected face with stored biometric data, it enables convenient and reliable identity verification without the need for physical tokens or passwords.

**Improved Security:** In security and surveillance systems, face detection helps identify individuals in real-time, aiding in the prevention and investigation of criminal activities. It can be used in airports, public spaces, and other high-security areas.

**Enhanced User Experience:** Face detection enables various interactive applications, such as applying filters or digital masks to faces in real-time, enhancing user experience in gaming, social media, and virtual communication platforms.

## Disadvantages of Face Detection:

**Privacy Concerns:** The use of face detection raises privacy concerns, as it involves capturing and analyzing individuals' facial data. There are debates surrounding the potential misuse or abuse of this technology and the need for proper regulation to protect individuals' privacy rights.

**Biased Results:** Face detection algorithms may exhibit bias, leading to inaccurate or unfair outcomes. Bias can occur due to factors like imbalanced training data, variations in demographics, or inherent limitations of the algorithms. This can result in the misidentification or exclusion of certain individuals, particularly from underrepresented groups.

**Sensitivity to Image Quality:** The accuracy of face detection algorithms can be affected by factors such as lighting conditions, image resolution, pose variations, occlusions, and image quality. In challenging conditions, the performance of face detection may degrade, leading to false positives or missed detections.

**Computational Requirements:** Efficient face detection often requires substantial computational resources, especially when dealing with real-time video streams or large-scale datasets. This can limit its practical application in resource-constrained devices or systems.

**Ethical Considerations:** Face detection technology raises ethical considerations regarding consent, data security, and potential societal implications. Its deployment should be accompanied by responsible practices, transparency, and safeguards to prevent misuse or discrimination.

It's important to consider these advantages and disadvantages when implementing face detection systems, ensuring they are used ethically, responsibly, and with appropriate safeguards to protect privacy and mitigate biases.

## CONTROVERSIES ON FACE DETECTION

Face detection and facial recognition technologies have been at the center of several controversies due to their potential privacy implications, biases, and ethical concerns. Here are some notable controversies surrounding these technologies:

**Privacy Concerns:** The use of face detection and facial recognition raises significant privacy concerns. The collection and storage of individuals' biometric data without their explicit consent can infringe upon privacy rights. There have been instances where facial recognition data has been misused or accessed without proper authorization, highlighting the need for stringent privacy regulations and safeguards.

**Surveillance and Mass Monitoring:** The widespread deployment of face detection and facial recognition in surveillance systems has sparked debates about mass monitoring and its impact on civil liberties. Critics argue that extensive surveillance infringes upon individuals' rights to privacy, freedom of movement, and freedom of expression, creating a potential for abuse by governments and law enforcement agencies.

**Biases and Discrimination:** Face detection and facial recognition algorithms can exhibit biases, leading to inaccurate results and potential discrimination. These biases can arise due to imbalanced training data, inadequate representation of certain demographics, or algorithmic limitations. Such biases can disproportionately impact marginalized groups, leading to false identifications, increased scrutiny, or exclusion.

**Misidentification and False Positives:** Facial recognition systems are not infallible and can produce false identifications or false positives. Instances of misidentifications have been reported, where innocent individuals have been wrongfully targeted or implicated based on flawed facial recognition matches. Such cases raise concerns about the reliability and consequences of relying solely on this technology for identification and decision-making.

**Inadequate Regulation:** There is ongoing debate regarding the need for comprehensive and robust regulations surrounding face detection and facial recognition technologies. Some argue that existing legal frameworks are insufficient to address the potential risks and ethical considerations associated with these technologies, emphasizing the need for clear guidelines, transparency, and accountability in their deployment.

**Public Backlash and Bans:** In response to the controversies and concerns surrounding face detection and facial recognition, some cities, organizations, and even countries have implemented partial or complete bans on the technology. These bans aim to protect privacy, prevent potential misuse, and allow for a more informed and thoughtful approach to its deployment.

Addressing the controversies surrounding face detection and facial recognition requires a multidisciplinary approach involving policymakers, researchers, industry stakeholders, and the public. Striking a balance between innovation, security, privacy, and ethical considerations is crucial to ensure responsible and beneficial use of these technologies.

## METHODOLOGY

The methodology for face detection typically involves a combination of image processing techniques, pattern recognition algorithms, and machine learning approaches. Here is a general overview of the common steps involved in face detection:

**Preprocessing:** The input image or video frame is preprocessed to enhance its quality and improve the effectiveness of subsequent steps. Preprocessing steps may include resizing, noise reduction, contrast enhancement, and normalization.

**Feature Extraction:** Various features are extracted from the preprocessed image to represent facial characteristics. Commonly used features include color information, texture, gradients, and shape descriptors. These features provide distinctive information to distinguish faces from the background or other objects.

**Detection Algorithm:** A detection algorithm is applied to the extracted features to locate potential face regions within the image. Different algorithms can be employed, such as Viola-Jones, Histogram of Oriented Gradients (HOG), or Convolutional Neural Networks (CNNs). These algorithms utilize specific criteria or learned patterns to identify areas likely to contain faces.

**Face Localization:** Once potential face regions are identified by the detection algorithm, further analysis is performed to precisely localize the facial regions. This can be achieved using techniques like geometric constraints, template matching, or shape modeling.

**Post-processing:** The detected face regions may undergo post-processing steps to refine the results and remove false detections. Techniques such as non-maximum suppression, region merging, or size filtering can be employed to eliminate redundant or erroneous detections.

**Validation and Verification:** In some cases, additional validation or verification steps are performed to confirm the presence of actual faces and filter out non-face objects or false positives. This can involve using machine learning models or rule-based methods to assess facial characteristics, symmetry, or other criteria.

**Output and Application:** The final output of the face detection process is typically represented by bounding boxes or masks around the detected facial regions. These results can then be utilized for various applications, such as face recognition, emotion analysis, or further processing.

## Tools & Technologies:

The following tools and technologies will be used for this project:

**Python:** The programming language we will be using for the project.

**OpenCV & Dlib:** Python libraries for computer vision and machine learning.

**Deep Learning Frameworks:** Advanced deep learning frameworks such as TensorFlow or Keras can be used for the project.

**Camera:** A Camera to capture images and live video feed for real-time facerecognition.

**Dataset:** A dataset of images and videos containing multiple individuals for training and testing.

## CONCLUSION

In conclusion, face detection is a crucial technology that has evolved significantly over the years. It enables the automated identification and localization of human faces within images or video frames, laying the foundation for numerous applications such as face recognition, biometric authentication, surveillance, emotion analysis, and augmented reality.

The advantages of face detection include automation, versatility, improved security, user authentication, and enhanced user experience. It automates the process of locating and analyzing faces, making it efficient for large datasets. It can be applied to various domains and provides a convenient and reliable means of authentication. Additionally, it enhances user experiences in interactive applications by enabling real-time manipulation of facial features.

However, face detection also poses certain challenges and controversies. Privacy concerns arise due to the collection and storage of biometric data without consent. Biases in algorithms and the potential for misidentification can lead to discriminatory outcomes. Inadequate

regulation and the use of facial recognition in surveillance systems have raised concerns about mass monitoring and infringement of civil liberties.

To address these issues, responsible deployment and the consideration of ethical implications are crucial. Striking a balance between innovation, security, privacy, and fairness is essential. Robust privacy regulations, transparency in algorithmic decision-making, and the mitigation of biases are important factors to ensure the responsible and beneficial use of face detection technology.

Despite the controversies, face detection continues to advance, driven by advancements in image processing, pattern recognition, and deep learning techniques. As technology progresses, it is essential to approach face detection with a holistic perspective, emphasizing ethical considerations, privacy protection, and the promotion of fairness and inclusivity in its application.

## REFERENCES

1. "Computer Vision: Algorithms and Applications" by Richard Szeliski - 2010
2. "Deep Learning" by Ian Goodfellow, Yoshua Bengio, and Aaron Courville -2016
3. "Face Recognition: A Literature Survey" by Zhifei Zhang – 2016
4. "Face Detection and Recognition: Theory and Practice" by Asit Kumar Datta, Madhura Datta, and Pradipta Kumar Banerjee - 2016
5. "Deep Face Recognition" by Yandong Wen, Zhifeng Li, and Yu Qiao - 2016
6. "Advances in Face Detection and Facial Image Analysis" edited by Lijun Yin, Abdenour Hadid, and Marios Savvides - 2016