

FACE RECOGNITION TO IDENTIFY THE CRIMINALS

##### A PROJECT REPORT

Submitted by

##### **KEN BOSTON[REGISTER NO:2114121104126]**

**JANESH KUMAR [REGISTER NO:211421104104]**

***in partial fulfillment for the award of the degree***

***of***

**BACHELOR OF ENGINEERING**

IN

COMPUTER SCIENCE AND ENGINEERING

PANIMALAR ENGINEERING COLLEGE, CHENNAI-600123

ANNA UNIVERSITY: CHENNAI 600 025

OCTOBER 2023

**BONAFIDE CERTIFICATE**

Certified that this project report **“……….TITLE OF THE PROJECT……………..”**

is the bonafide work of “**…………..NAME OF THE CANDIDATE(S)(REG.NO) .…………”** who carried out the project work under my supervision.

**SIGNATURE SIGNATURE**

**Dr.L.JABASHEELA .,M.E.,Ph.D ., << GUIDE NAME>>**

**HEAD OF THE DEPARTMENT SUPERVISOR**

**<<DESIGNATION>>**

DEPARTMENT OF CSE, DEPARTMENT OF CSE,

PANIMALAR ENGINEERING COLLEGE, PANIMALAR ENGINEERING COLLEGE,

NASARATHPETTAI, NASARATHPETTAI,

POONAMALLEE, POONAMALLEE,

CHENNAI-600 123. CHENNAI-600 123.

Certified that the above candidate(s) was/ were examined in the Anna University Project Viva-Voce Examination held on...........................

**INTERNAL EXAMINER EXTERNAL EXAMINER**

**DECLARATION BY THE STUDENT**

We ……......... Name of the Students ( Reg.No)……………… hereby declare that this project report titled “ …………………………………..” , under the guidance of ………………( Guide Name ) ……..is the orginial work done by us and we have not plagiarized or submitted to any other degree in any university by us.

**ACKNOWLEDGEMENT**

We would like to express our deep gratitude to our respected Secretary and Correspondent **Dr.P.CHINNADURAI, M.A., Ph.D.** for his kind words and enthusiastic motivation, which inspired us a lot in completing this project.

We express our sincere thanks to our Directors **Tmt.C.VIJAYARAJESWARI**, **Dr.C.SAKTHI KUMAR,M.E.,Ph.D** and **Dr.SARANYASREE SAKTHI KUMAR B.E.,M.B.A.,Ph.D.,** for providing us with the necessary facilities to undertake this project.

We also express our gratitude to our Principal **Dr.K.Mani, M.E., Ph.D.** who facilitated us in completing the project.

We thank the Head of the CSE Department, **Dr. .JABASHEELA , M.E.,Ph.D.,** for the support extended throughout the project.

We would like to thank my **Project Guide** ……………………… and all the faculty members of the Department of CSE for their advice and encouragement for the successful completion of the project.

**NAME OF THE STUDENTS**

**ABSTRACT**

Facial recognition technology has garnered significant attention as a potential tool for identifying criminals and enhancing public safety. This abstract provides an overview of the ethical and legal considerations associated with the use of facial recognition for criminal identification.

The paper explores the accuracy and bias issues inherent in facial recognition systems, highlighting the potential for false identifications and their disparate impact on various demographic groups. It also examines the profound privacy concerns raised by the collection and analysis of facial data without individuals' consent, as well as the broader implications for civil liberties and personal freedoms.

Furthermore, the abstract discusses the current state of regulatory frameworks governing facial recognition technology, emphasizing the need for comprehensive and transparent regulations to address the technology's risks and ensure its responsible use by law enforcement agencies. It also touches upon the ethical dilemmas faced by society in balancing security needs with individual rights and freedoms.

In conclusion, this abstract highlights the complex ethical and legal landscape surrounding facial recognition technology's application in identifying criminals and underscores the importance of striking a balance between public safety and protecting individual rights and privacy.

Top of Form

TABLE OF CONTENTS

| **CHAPTER NO.** | **TITLE** | **PAGE NO.** |
| --- | --- | --- |
|  | **ABSTRACT** | iii |
|  | **LIST OF TABLES** | vii |
|  | **LIST OF FIGURES** | viii |
|  | **LIST OF SYMBOLS, ABBREVIATIONS** | ix |
| **1.** | **INTRODUCTION** |  |
|  | 1.1 Organization Profile ( optional) |  |
|  | 1.2 Problem Definition |  |
| **2.** | **LITERATURE SURVEY** |  |
| **3.** | **SYSTEM ANALYSIS** |  |
|  | 2.1 Existing System |  |
|  | 2.2 Proposed system |  |
|  | 2.3 Feasibility Study |  |
|  | 2.4 Hardware Environment |  |
|  | 2.5 Software Environment |  |
| **4.** | **SYSTEM DESIGN** |  |
|  | 4.1. ER diagram |  |
|  | 4.2 Data dictionary |  |
|  | 4.3 Table Normalization |  |
|  | 4.4 Data Flow Diagram |  |
|  | 4.5 UML Diagrams |  |
| **5.** | **SYSTEM ARCHITECTURE** |  |
|  | 5.1 Architecture Overview  5.2 Module Design Specification (Description of the Modules) |  |
|  | 5.2 Algorithms |  |
| **6.** | **SYSTEM IMPLEMENTATION** |  |
|  | 6.1 Client-side coding (sample) |  |
|  | 6.2 Server-side coding(sample) |  |
| **7.** | **SYSTEM TESTING** |  |
|  | 7.1 Unit Testing |  |
|  | 7.2 Integration Testing |  |
|  | 7.3 Test Cases & Reports |  |
| **8.** | **CONCLUSION** |  |
|  | 8.1 Conclusion and Future Enhancements |  |
|  | **APPENDICES** |  |
|  | A.1 Sample Screens |  |
|  | A.2 Publications  A.3 Plagiarism Report |  |
|  | **REFERENCES** |  |

INTRODUCTION:

Face recognition technology has emerged as a powerful tool in the field of law enforcement and public security. One of its crucial applications is the identification of criminals, aiding in the apprehension of suspects, and maintaining public safety. Traditional methods of identifying criminals often rely on eyewitness accounts, fingerprinting, and manual surveillance. While these methods have proven effective, they are not without limitations. Face recognition systems offer a more technologically advanced and efficient means of criminal identification.

The primary objective of a face recognition system in the context of identifying criminals is to analyze and match the facial features of individuals against a database of known criminals or suspects. This process involves the capture of facial images through various sources, including surveillance cameras, social media, and official records. These images are then subjected to advanced computer algorithms that extract and analyze unique facial characteristics, such as the arrangement of facial landmarks, skin texture, and facial expressions.

PROBLEM DEFINITION:

The problem of developing and implementing a face recognition system for identifying criminals is multifaceted and encompasses several key challenges and considerations:

1. **Accuracy and Reliability:**
   * The system must achieve a high level of accuracy in identifying criminals to minimize false positives and negatives.
   * Variations in lighting, pose, and image quality can affect the system's reliability, especially in real-world surveillance scenarios.
2. **Database Size and Management:**
   * Maintaining a comprehensive database of known criminals, including up-to-date images and profiles, requires robust data management capabilities.
   * Efficient indexing and retrieval of relevant data from large criminal databases are critical.
3. **Privacy and Civil Liberties:**
   * Balancing the need for criminal identification with privacy concerns is a significant challenge.
   * Ensuring that individuals' rights are respected and that data is handled in compliance with privacy regulations is essential.
4. **Bias and Fairness:**
   * Addressing potential biases in face recognition algorithms, especially concerning race, gender, and age, is crucial to prevent discriminatory outcomes.
   * Developing and using fair and unbiased algorithms is an ongoing challenge.
5. **Real-time Processing:**
   * In applications like surveillance, the system must process facial data in real-time to identify criminals quickly.
   * Achieving high-speed processing while maintaining accuracy is a technical challenge.
6. **Data Security and Access Control:**
   * Safeguarding the facial data and the system itself from unauthorized access and cyberattacks is paramount.
   * Implementing robust access control measures and encryption to protect sensitive information is vital.
7. **Ethical Considerations:**
   * Ensuring that the use of face recognition technology for criminal identification aligns with ethical standards and principles is essential.
   * Transparency, accountability, and public trust must be maintained.
8. **Legal Framework and Compliance:**
   * Developing a legal framework and ensuring compliance with existing laws and regulations related to biometrics and data privacy is necessary.
   * Adhering to legal requirements regarding data retention, consent, and lawful surveillance practices is critical.
9. **Algorithm Development and Training:**
   * Continuously improving the accuracy and robustness of face recognition algorithms through research, development, and training is an ongoing challenge.
   * Staying up-to-date with advancements in deep learning and computer vision is essential.
10. **Human Rights and Due Process:**
    * Ensuring that the use of face recognition technology does not infringe upon human rights, such as the right to a fair trial and due process, is a significant concern.
    * Proper legal procedures must be followed when using facial recognition in criminal investigations.
11. **Public Perception and Acceptance:**
    * Gaining public acceptance and trust in the technology is essential for its successful deployment.
    * Clear communication about its benefits, limitations, and safeguards is necessary to build public confidence.

LITERATURE SURVEY:

Face recognition using Eigenfaces and artificial neural networks (ANNs) is a classic approach in the field of computer vision and pattern recognition. This technique combines dimensionality reduction with machine learning to recognize faces from images. Here's an overview of how this approach works:

1. **Data Collection and Preprocessing:**
   * Gather a dataset of face images with a sufficient number of individuals.
   * Preprocess the images to ensure they are aligned, have consistent lighting, and are of the same size. Common preprocessing steps include resizing, grayscale conversion, and histogram equalization.
2. **Eigenfaces for Dimensionality Reduction:**
   * Principal Component Analysis (PCA) is applied to the preprocessed face images to reduce the dimensionality of the data.
   * PCA identifies the principal components (eigenfaces) that capture the most significant variations in the face images. These eigenfaces are essentially the eigenvectors of the covariance matrix of the face image dataset.
   * By retaining a subset of the top eigenfaces, you reduce the dimensionality of the data while preserving the most important facial features.
3. **Feature Extraction:**
   * Project each face image onto the subspace spanned by the selected eigenfaces. This process extracts a feature vector for each face.
   * The feature vector for each face can be thought of as its representation in the eigenface space.

The Chicago Face Database (CFD) is a widely used stimulus set of faces and associated norming data for research in psychology, cognitive science, and neuroscience. It is a valuable resource for researchers studying various aspects of face perception, emotion recognition, and social cognition. The CFD provides a diverse collection of facial images, along with detailed information about the faces and norming procedures. Here are some key details about the Chicago Face Database:

**Contents of the Chicago Face Database:**

1. **Face Images:** The CFD contains high-quality photographs of faces. These faces are posed by individuals from different racial and ethnic backgrounds, covering a range of ages and genders. The database includes both neutral expressions and expressions depicting various emotions, making it suitable for emotion recognition studies.
2. **Norming Data:** One of the strengths of the CFD is the extensive norming data associated with each face. This norming data includes information about how participants (often a large group of individuals) perceive and evaluate the faces. It typically includes ratings for factors such as perceived attractiveness, emotional expressions, trustworthiness, and age.
3. **Demographic Information:** The CFD provides demographic information about the faces, including the gender, age, and ethnicity of the individuals depicted in the photographs.

Public policies aimed at combating criminal assets in Mexico, particularly in the northern border states, face several challenges and opportunities. The northern border states of Mexico, such as Tamaulipas, Nuevo León, Chihuahua, and Baja California, have been historically affected by organized crime and drug trafficking. Addressing the issue of criminal assets in this region is crucial for reducing the power and influence of criminal organizations. Here are some of the challenges and opportunities associated with these policies:

**Challenges:**

1. **Lack of Resources:** Many northern border states in Mexico have limited financial resources and capacity to combat criminal assets effectively. Adequate funding and resources are essential for conducting investigations, asset forfeiture proceedings, and ensuring the proper management of seized assets.
2. **Corruption and Intimidation:** Corruption remains a significant challenge in Mexico, and criminal organizations often intimidate or co-opt law enforcement officials, making it difficult to investigate and seize criminal assets without external interference.
3. **Complex Legal Framework:** The legal framework for asset forfeiture and seizure can be complex and challenging to navigate. Inconsistent or outdated laws may hinder the efficient disposal and management of seized assets.
4. **International Implications:** The proximity of the northern border states to the United States

Top of Form

SYSTEM ANALYSIS:

System analysis for a face recognition system designed to identify criminals involves a thorough examination of the system's requirements, components, functionality, and constraints. Below is an overview of the system analysis process:

**1. System Requirements:**

* Define the specific objectives of the face recognition system, including the identification of criminals.
* Gather requirements from law enforcement agencies, security experts, and other stakeholders.
* Specify the desired accuracy, response time, and scalability of the system.
* Identify legal and ethical requirements, including compliance with data privacy regulations.

**2. Data Collection and Database:**

* Determine the sources of facial data, such as surveillance cameras, social media, and criminal records.
* Define the criteria for collecting and updating facial images of known criminals.
* Establish procedures for securely storing and managing the database, including access control and encryption.

**3. Hardware and Software Components:**

* Identify the necessary hardware components, such as cameras, servers, and storage systems.
* Choose appropriate software tools and libraries for facial recognition, image processing, and database management.
* Ensure that the system can handle real-time processing and high-resolution images, if required.

**4. Data Preprocessing:**

* Analyze the quality of facial images, addressing issues like lighting, pose variations, and image resolution.
* Develop preprocessing algorithms to standardize and enhance facial images for accurate recognition.

**5. Face Recognition Algorithm:**

* Select or design a face recognition algorithm, considering factors like accuracy, speed, and robustness.
* Evaluate and fine-tune the algorithm using a diverse dataset of known criminals and non-criminals.
* Implement measures to mitigate biases and fairness concerns in the algorithm.

**6. Real-Time Processing:**

* Ensure that the system can process facial data in real-time, especially in surveillance applications.
* Optimize algorithms for efficient real-time performance.
* Consider the hardware requirements, such as GPUs or specialized processors, for real-time processing.

**7. Privacy and Security:**

* Address privacy concerns by implementing strict access controls and encryption for the database.
* Develop protocols for obtaining consent and handling sensitive facial data.
* Protect the system from cyberattacks and unauthorized access.

EXISTING SYSTEMS:

Now, let’s understand how FRS works.

1. **Detection:** Detection begins with the extraction of the face out of the image fed into the system. Subsequently, various features on the human face are marked. Certain features of the face do not change with age or size. These include the distance between the eyes, the depth of the eye socket, and the shape of the nose. There are around 80 such features called ‘landmarks.’ The measurements of these landmarks are then put together to create a code. This code is called a ‘faceprint,’ and it is unique to every person.
2. **Matching:** This faceprint is then matched with the prints stored in the system. At this stage, the image goes through several layers of technology to ensure accuracy. Since most of our databases are currently 2D photos, the database images need to be processed by a layer of technology. This processing usually involves pulling out the facial landmarks to resemble their 3D counterparts. If the subject image is low resolution, it must be encoded and decoded to produce details with the desired resolution. The algorithms need to consider the differences in lighting, facial expression, and angles.
3. **Identification:** The goal of this step depends on what the facial recognition software is used for — surveillance or [authentication](https://www.spiceworks.com/it-security/identity-access-management/articles/what-is-multi-factor-authentication/). This step should ideally produce a 1:1 match for the subject. This may be done in multiple ways, a quick pass to narrow down the options, then enable the more complex layers to take over. Some companies analyze skin texture along with facial recognition algorithms to increase accuracy.

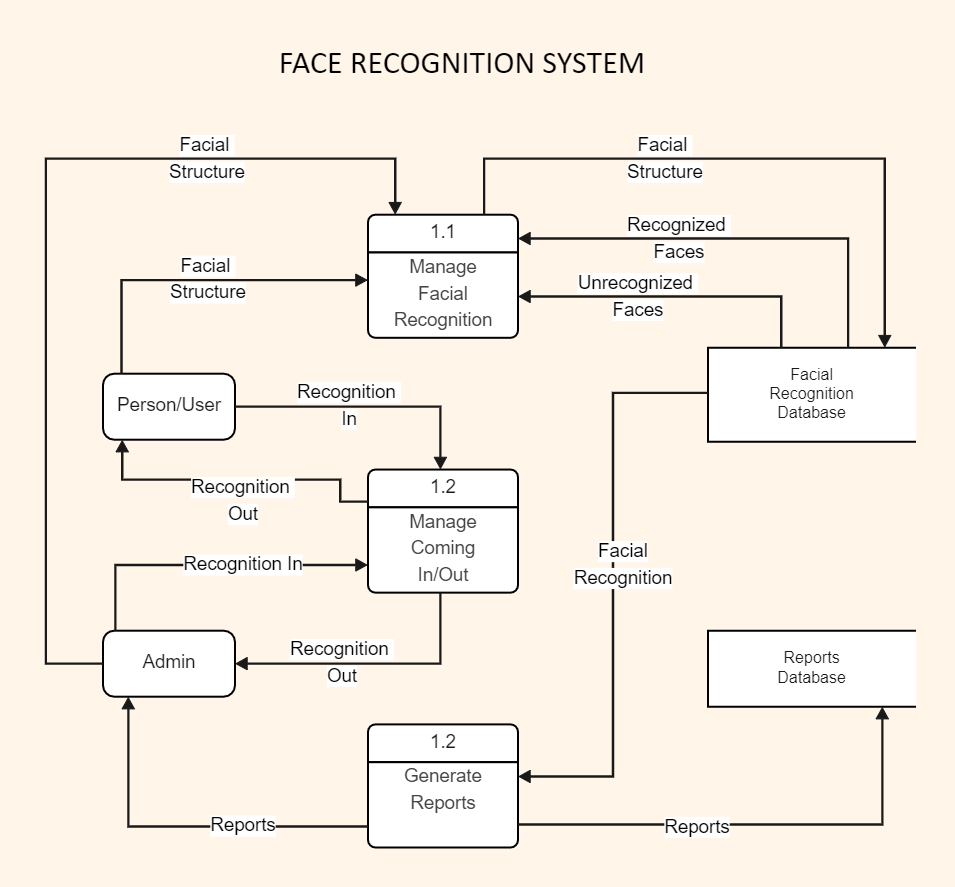
Each facial recognition software provider focuses on different aspects of the technology layers to provide almost-flawless service. For example, one software may focus on correcting lighting conditions while another can focus on skin texture analysis.

PROPOSED SYSTEM:

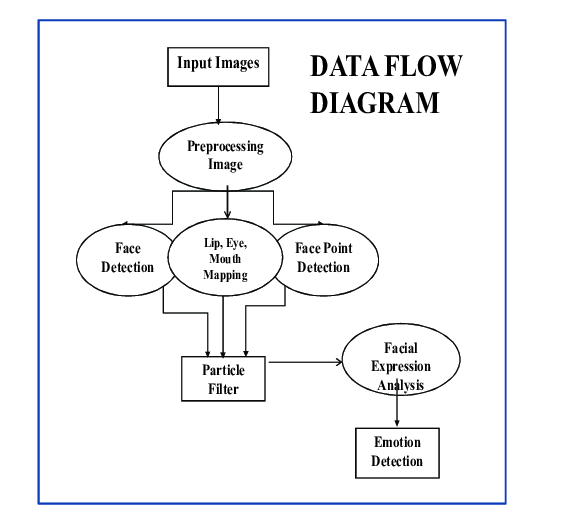
Open face recognition provides an uncertain challenge to criminal face identification. Thus, this recognition has many uses, from security to entertainment. Even if other biometric characteristics like iris and fingerprints are reliable, a person must be present to use them. Therefore, there are better tools for thieves to use for authentication. Anyone can recognize a criminal in an image using face recognition technology in conjunction with a criminal database containing the individual's personal information. In addition to needing great accuracy, a criminal recognition system also needs to be flexible to numerous variations in illumination, occlusion, maturity level, postures, etc. We use the Haar cascade and Histograms of oriented gradients (HOG) recognition learning systems discussed and contrasted in this study. We assessed models, and HOG outperformed the criminal recognition system. We also go through several practical uses for this criminal recognition.

SYSTEM DESIGN:

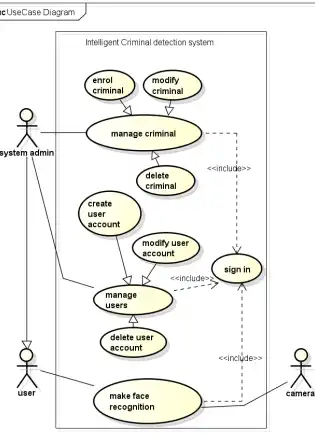
ER DIAGRAM



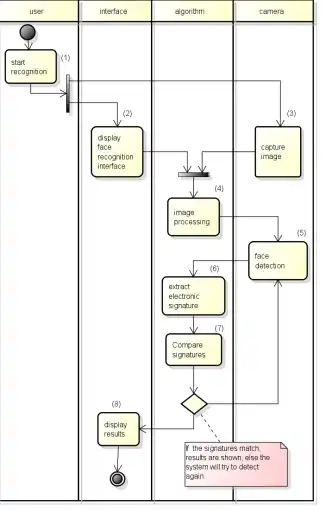
DATAFLOW DIAGRAM:



USE CASE DIAGRAM

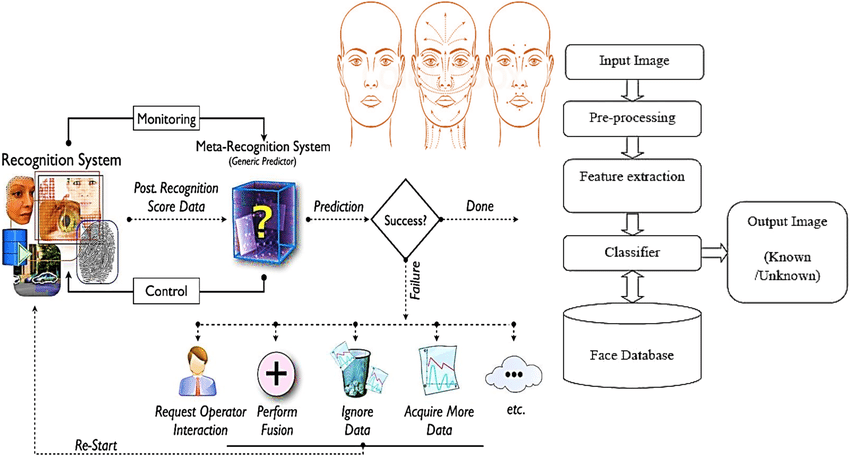


ACTIVITY DIAGRAM:



SYSTEM ARCHITECTURE:

ARCHITECTURE DIAGRAM:



SYSTEM IMPLEMENTATION:

**import** cv2

**import** numpy **as** np

**import** face\_recognition

**import** cv2

**import** numpy as np

**import** face\_recognition

img\_bgr =

face\_recognition.load\_image\_file('student\_images/modi.jpg')

img\_rgb = cv2.cvtColor(img\_bgr,cv2.COLOR\_BGR2RGB)

cv2.imshow('bgr', img\_bgr)

cv2.imshow('rgb', img\_rgb)

cv2.waitKey

img\_modi=face\_recognition.load\_image\_file('student\_images/modi.jpg')

img\_modi\_rgb = cv2.cvtColor(img\_modi,cv2.COLOR\_BGR2RGB)

#--------- Detecting Face -------

face = face\_recognition.face\_locations(img\_modi\_rgb)[0]

**copy** = img\_modi\_rgb.copy()

# ------ Drawing bounding boxes around Faces------------------------

cv2.rectangle(**copy**, (face[3], face[0]),(face[1], face[2]), (255,0,255), 2)

cv2.imshow('copy', **copy**)

cv2.imshow('MODI',img\_modi\_rgb)

cv2.waitKey(0)

img\_modi = face\_recognition.load\_image\_file('student\_images/modi.jpg')

img\_modi = cv2.cvtColor(img\_modi,cv2.COLOR\_BGR2RGB)

#------to find the face location

face = face\_recognition.face\_locations(img\_modi)[0]

#--Converting image into encodings

train\_encode = face\_recognition.face\_encodings(img\_modi)[0]

#----- lets test an image

test = face\_recognition.load\_image\_file('student\_images/modi2.jpg')

test = cv2.cvtColor(test, cv2.COLOR\_BGR2RGB)

test\_encode = face\_recognition.face\_encodings(test)[0]

print(face\_recognition.compare\_faces([train\_encode],test\_encode))

cv2.rectangle(img\_modi, (face[3], face[0]),(face[1], face[2]), (255,0,255), 1)

cv2.imshow('img\_modi', img\_modi)

cv2.waitKey(0)

SYSTEM TESTING: