<FACE RECOGNITION SYSTEM>

Submitted for

Artificial Intelligence and Machine Learning CSET2301

Submitted by:

(<E23CSEU2326>) NAME- KRITIKA

(<E23CSEU2316>) NAME- KHUSHI

Submitted to

MR. SHWETANG DUBEY

Jan-Apr 2025

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

BENNETT UNIVERSITY

THE TIMES GROUP

CERTIFICATE

Candidate's Declaration

I hereby declare that the work presented in this report entitled "Face Recognition SYSTEMS" in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science and Engineering** submitted in the department of Computer Science & Engineering and Information Technology, Bennett University of Information Technology Greater Noida is authentic record of my own work carried out over a period from January 2025 to April 2025 under the supervision of **MR. SHWETANG DUBEY** . The matter embodied in the report has not been submitted for the award of any other degree or diploma.

(<E23CSEU2326>) NAME- KRITIKA

(<E23CSEU2316>) NAME- KHUSHI

This is to certify that the above statement made by the candidate is true to the best of my knowledge.

MR. SHWETANG DUBEY

Computer Science & Engineering

Dated: 24-04-2025

ACKNOWLEDGEMENT

I would like to thank and express our gratitude to our Project supervisor MR. Tarandeep Singh for the opportunity that he provided us with this

wonderful project “Face Recognition System”. The outcome would not

be possible without his guidance. This project taught me many new things and

helped to strengthen concepts of Machine Learning. Next, I would like to

express my special thanks to the Lab Assistant for cordially contacting us and

helping us with finishing this project within the specified time. Lastly, I would

I like to thank my friends and parents for their help and support.

(<E23CSEU2326>) NAME- KRITIKA

(<E23CSEU2316>) NAME- KHUSHI

INDEX

ABSTRACT

Face recognition systems are a subset of biometric authentication technologies designed to identify or verify individuals based on their facial features. These systems analyse facial images captured via cameras and extract key facial characteristics, such as the distance between eyes, nose shape, and overall facial structure, to create a unique facial profile. This profile is then compared to a pre-existing database to identify or verify the individual.

Several algorithms are used in face recognition, including classical methods like Principal Component Analysis (PCA) for feature extraction (Eigenfaces), Linear Discriminant Analysis (LDA) (Fisher faces), and more advanced deep learning-based approaches such as Convolutional Neural Networks (CNNs). CNNs have significantly improved recognition accuracy and robustness, enabling the system to handle various challenges like facial expression changes, lighting variations, and partial occlusions.

Face recognition systems are widely used in various sectors, including security (e.g., surveillance cameras), mobile devices (for unlocking phones), and online platforms (for user verification). They offer advantages in terms of contactless authentication, efficiency, and convenience. However, concerns regarding privacy, data security, and the potential for misuse of the technology remain critical. Despite these challenges, face recognition continues to evolve and play an essential role in modern identity verification and surveillance systems.

INTRODUCTION

Face recognition is a biometric technology that identifies or verifies individuals based on their unique facial features. Unlike traditional identification methods such as passwords or PINs, face recognition offers a contactless and convenient way to authenticate users. The primary aim of this system is to capture facial images, analyze distinctive facial characteristics, and match these features with a pre-existing database to establish identity. Over the years, advancements in machine learning and computer vision have significantly improved the accuracy and speed of face recognition systems.

Face recognition has diverse applications across multiple industries. In security, it is used for surveillance, providing automated monitoring to detect unauthorized access in restricted areas. Mobile devices, such as smartphones and laptops, have adopted facial recognition for user authentication, offering a more secure and user-friendly alternative to passwords. Additionally, social media platforms use face recognition to tag users in photos, enhancing the user experience.

The face recognition process typically involves three major stages: face detection, feature extraction, and face matching. Face detection locates faces within an image, feature extraction identifies and quantifies facial features, and face matching compares the extracted features with those in a database for recognition. Although technology is rapidly advancing, challenges such as dealing with changes in lighting, facial expressions, or partial occlusions still pose hurdles to achieving perfect accuracy. Nonetheless, face recognition remains a powerful tool with widespread use in modern technology.

PROBLEM STATEMENT

Face recognition technology has gained significant attention due to its potential to enhance security and user experience across various applications, including surveillance, authentication, and identity verification. However, despite its growing use, there are several challenges and limitations that hinder its widespread adoption and effectiveness.

One of the primary issues is the system's performance in real-world scenarios, where faces may be captured under varying lighting conditions, different angles, and occlusions (e.g., glasses, hats, or facial hair). These factors can significantly affect the accuracy and reliability of the system, leading to false positives or false negatives in identifying or verifying individuals. Additionally, face recognition systems may struggle with the "age factor," as faces change over time due to aging or health conditions, leading to inconsistencies in recognition.

Another critical problem is the challenge of large-scale face databases, where the system may need to identify or verify individuals from a vast pool of candidates. As the number of faces increases, the computational complexity of the recognition process also rises, making it harder to maintain efficiency and accuracy.

Moreover, there are concerns regarding privacy, security, and ethical issues related to the use of face recognition systems, particularly in public surveillance and unauthorized data collection. These challenges must be addressed to improve the robustness, reliability, and fairness of face recognition technology in real-world applications.

METHODOLOGY

To build an effective face recognition system, various methodologies are employed, which can be categorized into different stages: data collection, preprocessing, feature extraction, and recognition. Below is an overview of the methodology:

1. Data Collection:

The foundation of any face recognition system lies in the collection of quality data. The system requires a large dataset of facial images for training and testing. This data includes images of various individuals captured under different lighting conditions, angles, and expressions. Datasets may include labeled images, which allow the system to learn the unique features of each face. Common datasets used for face recognition include LFW (Labeled Faces in the Wild), YALE, and FERET.

2. Face Detection:

The first step in the process is detecting faces within the image. This is typically done using algorithms such as the Viola-Jones face detection method or more modern deep learning-based approaches like Single Shot Multibox Detector (SSD) or Faster R-CNN. Face detection identifies the regions in an image where faces are located, and it is critical to ensure that only the face is considered for recognition, excluding other elements like background objects.

3. Preprocessing:

After face detection, the next step is preprocessing, which ensures that the image is in a suitable format for feature extraction. This step involves:

- Normalization: Resizing the image to a standard dimension and ensuring the face is centered.
- Gray-Scaling: Converting the image to grayscale to reduce computational complexity and focus on the essential features.
- Noise Reduction: Removing any irrelevant noise or distortion that could affect the accuracy of the system.

4. Feature Extraction:

The goal of feature extraction is to identify and extract relevant facial features from the detected face. Various techniques can be used for this purpose:

- Principal Component Analysis (PCA): PCA reduces the dimensionality of the face image while preserving the important features that differentiate faces. This method is often referred to as Eigenfaces.
- Local Binary Patterns (LBP): This method captures the texture of a face by considering the local patterns and is particularly useful in situations with variations in lighting.
- Deep Learning-Based Feature Extraction (CNNs): Convolutional Neural Networks (CNNs) are increasingly used for feature extraction. CNNs can learn hierarchical features from raw pixel data, offering a robust and scalable approach to face recognition.

5. Face Matching/Recognition:

After extracting facial features, the system matches the features against a database of stored faces. Two common methods for matching faces are:

- Euclidean Distance: This simple approach calculates the distance between feature vectors and classifies faces based on the smallest distance.
- Support Vector Machines (SVM): SVM can be used as a classifier to distinguish between different faces by learning from the feature vectors.
- Deep Learning Models (e.g., CNNs): Deep learning models can be trained to directly map the extracted features to specific identities, providing end-to-end learning from raw image data to identity prediction.

6. Post-Processing & Decision Making:

Once the system identifies a face, post-processing techniques are applied to refine the recognition results. This may include filtering based on confidence scores, where the system only accepts recognition results above a certain confidence threshold to reduce false positives. In the case of identity verification, the system compares the input face to a stored identity and confirms whether they match.

7. Evaluation:

To evaluate the performance of the face recognition system, various metrics are used, such as:

- Accuracy: The percentage of correct face identifications and verifications.
- Precision & Recall: Precision measures how many of the identified faces are correct, while recall measures how many of the actual faces were identified.

- F1-Score: A balance between precision and recall to provide a single metric of performance.
- False Positive Rate (FPR) & False Negative Rate (FNR): Measures of incorrect classifications in the system.

8. Optimization:

To improve the performance of the system, various optimization techniques can be employed, including:

- Hyperparameter Tuning: Optimizing model parameters to achieve better results.
- Ensemble Methods: Combining multiple classifiers to improve accuracy and robustness.
- Data Augmentation: Using techniques like image flipping, rotation, and zooming to increase the dataset size and make the system more robust.

9. Deployment:

Once the system is trained and evaluated, it is deployed for real-world applications. Depending on the use case, it can be integrated into security systems, mobile devices, or social media platforms. The deployment stage also includes ensuring the system is scalable and can handle real-time processing.

💻 Hardware and Software Requirements

🔧 Hardware Requirements

1. **Processor (CPU):**
   - **Minimum:** Intel i5 (4-core)
   - **Recommended:** Intel i7/i9

     Face recognition and video processing benefit from multi-core CPUs for faster computation.
2. **RAM:**
   - **Minimum:** 8 GB
   - **Recommended:** 16 GB or higher

     Adequate memory is essential for handling real-time image processing and database operations.
3. **Graphics Processing Unit (GPU):**
   - **Optional but Recommended:** NVIDIA GTX 1050 Ti or better

     For accelerating any potential deep learning upgrades in future versions (like emotion detection, advanced embeddings).
4. **Storage:**
   - **Minimum:** 50 GB of free disk space

- **Recommended:** SSD with at least 100 GB free
  Required for storing face image datasets, student records, attendance logs, and libraries.

5. **Camera:**
   - **Required:** Integrated or USB HD Webcam (720p minimum, 1080p recommended)
     Used for real-time face detection and recognition.
6. **Internet Connection:**
   - **Optional:** Required for installing dependencies and updates via pip.
     Not mandatory for offline use once the system is installed.

💻 Software Requirements

1. **Operating System:**
   - **Compatible:** Windows 10/11, macOS, or any modern Linux distro
     The project is tested and verified on Windows using PowerShell.
2. **Programming Language:**
   - **Primary:** Python 3.x
     All scripts and modules including face recognition, database handling, and the Flask web app are written in Python.
3. **Python Libraries and Frameworks:**
   - OpenCV: Real-time webcam capture and face detection

- face_recognition: For Dlib-based facial embedding and recognition
- Flask: Web-based dashboard for attendance viewing
- SQLite3: Lightweight relational database used for students and attendance
- Pandas, NumPy: For data operations and future analytics

4. **Development Tools / IDEs:**
   - **Recommended:**
     - Visual Studio Code (VS Code) – primary IDE
     - Jupyter Notebook – for prototyping
     - SQLite Browser – for database inspection

5. **Database:**
   - **Type:** SQLite (default, file-based)

     Lightweight and ideal for local offline usage of the attendance system.

6. **Web Framework & UI:**
   - **Backend:** Flask (Python)
   - **Frontend:** HTML, CSS (simple Bootstrap-style layout)

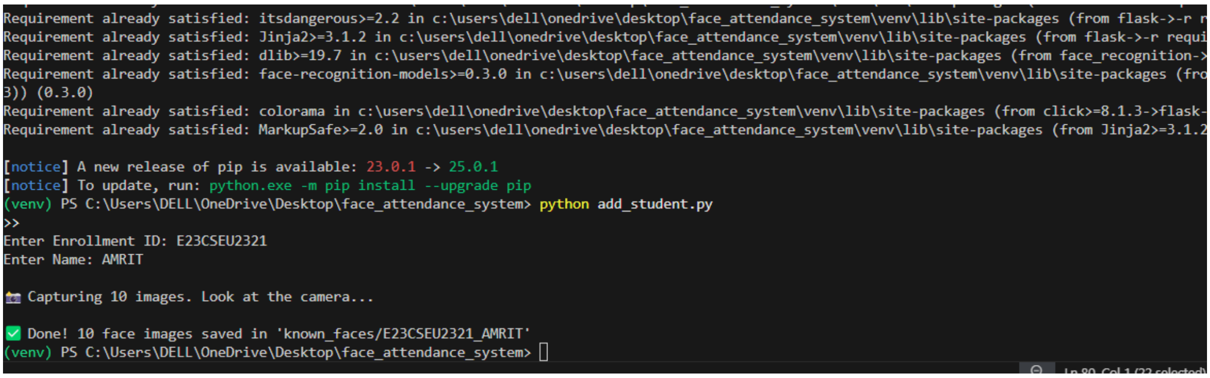
CONCLUSIONS

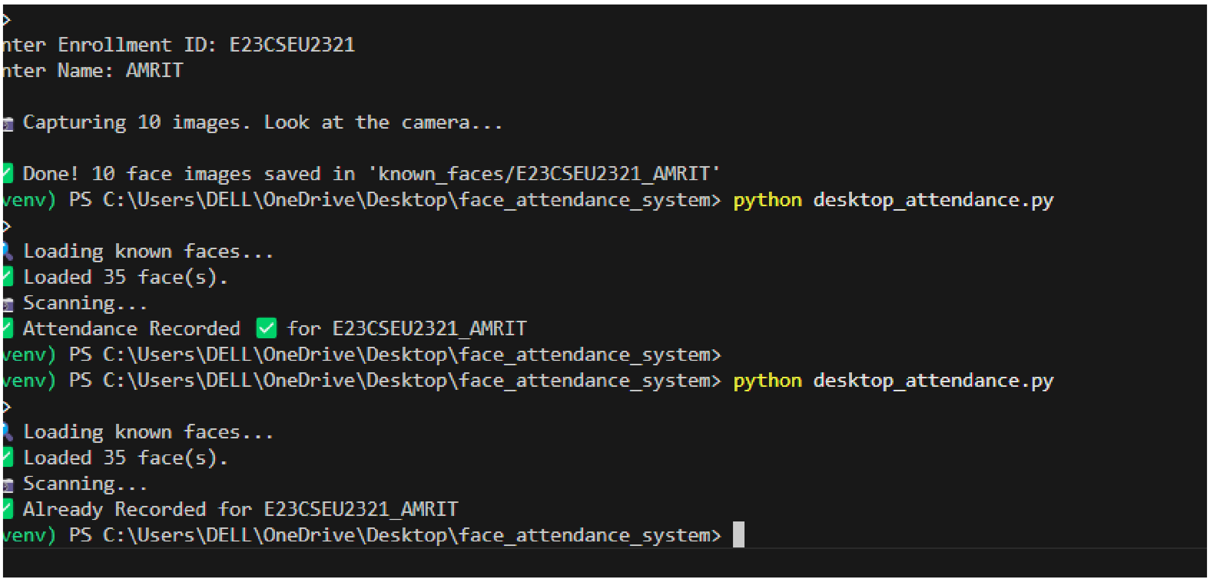
In conclusion, face recognition systems have become a powerful and indispensable technology in various applications, ranging from security and surveillance to personalized user experiences. With advancements in machine learning and deep learning, particularly the use of Convolutional Neural Networks (CNNs), these systems have significantly improved in accuracy and efficiency. The combination of traditional methods, such as PCA and newer techniques like deep learning, has enabled the development of robust face recognition systems that can handle challenges like varying lighting, poses, and facial expressions.

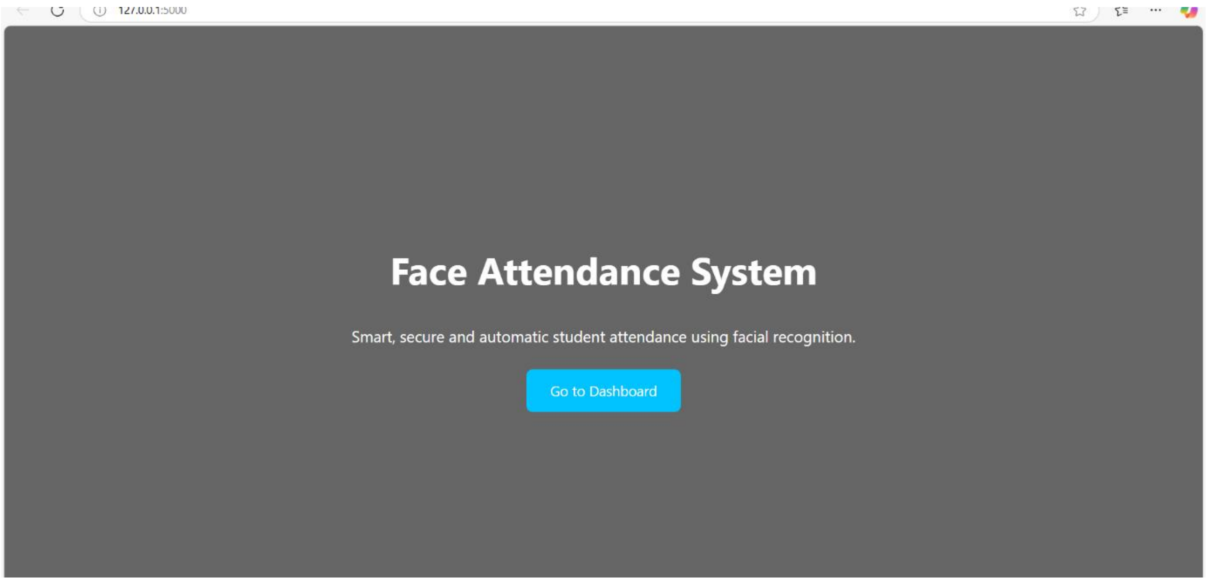
Despite the success of these technologies, challenges still persist in areas such as real-time processing, handling occlusions, and improving robustness in unconstrained environments. The future of face recognition systems lies in addressing these challenges while ensuring privacy and security concerns are managed effectively.

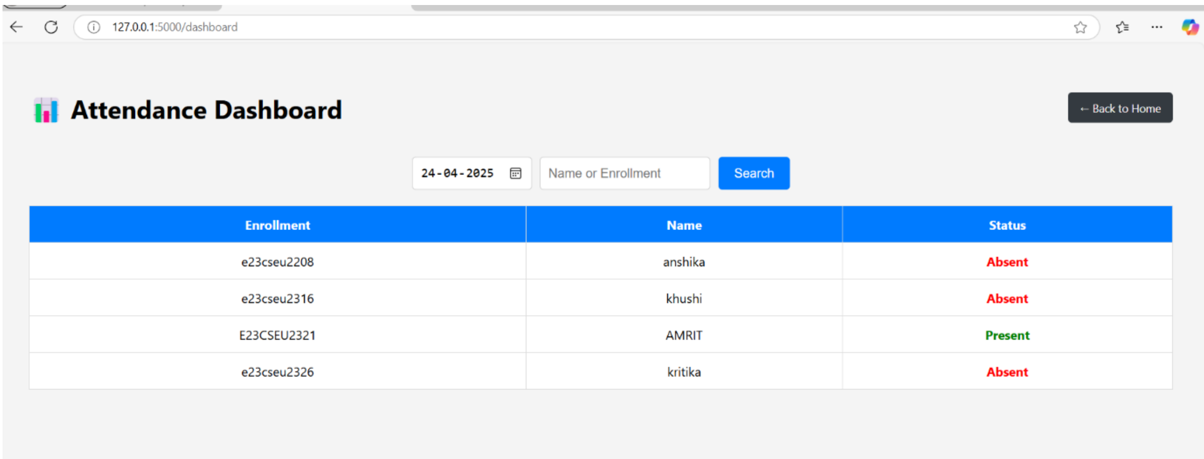
By integrating advanced algorithms with cutting-edge hardware, face recognition systems will continue to evolve, becoming more accurate, efficient, and scalable. The continued refinement of these systems promises a future where face recognition plays an even more significant role in enhancing user interactions, improving security, and contributing to numerous industries such as retail, healthcare, and law enforcement.

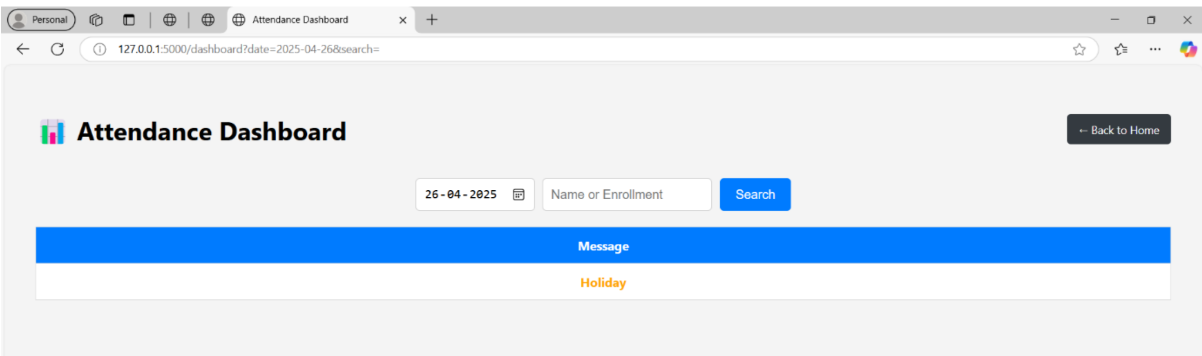
RESULT


Requirement already satisfied: itsdangerous>=2.2 in c:\users\dell\onedrive\desktop\face_attendance_system\venv\lib\site-packages (from flask->-r r
Requirement already satisfied: Jinja2>=3.1.2 in c:\users\dell\onedrive\desktop\face_attendance_system\venv\lib\site-packages (from flask->-r requi
Requirement already satisfied: dlib>=19.7 in c:\users\dell\onedrive\desktop\face_attendance_system\venv\lib\site-packages (from face_recognition->
Requirement already satisfied: face-recognition-models>=0.3.0 in c:\users\dell\onedrive\desktop\face_attendance_system\venv\lib\site-packages (fro
3)) (0.3.0)
Requirement already satisfied: colorama in c:\users\dell\onedrive\desktop\face_attendance_system\venv\lib\site-packages (from click>=8.1.3->flask-
Requirement already satisfied: MarkupSafe>=2.0 in c:\users\dell\onedrive\desktop\face_attendance_system\venv\lib\site-packages (from Jinja2>=3.1.2
[notice] A new release of pip is available: 23.0.1 -> 25.0.1
[notice] To update, run: python.exe -m pip install --upgrade pip
(venv) PS C:\Users\DELL\OneDrive\Desktop\face_attendance_system> python add_student.py
>>
Enter Enrollment ID: E23CSEU2321
Enter Name: AMRIT
Capturing 10 images. Look at the camera...
Done! 10 face images saved in 'known_faces/E23CSEU2321_AMRIT'
(venv) PS C:\Users\DELL\OneDrive\Desktop\face_attendance_system>


nter Enrollment ID: E23CSEU2321
nter Name: AMRIT
Capturing 10 images. Look at the camera...
Done! 10 face images saved in 'known_faces/E23CSEU2321_AMRIT'
venv) PS C:\Users\DELL\OneDrive\Desktop\face_attendance_system> python desktop_attendance.py
Loading known faces...
Loaded 35 face(s).
Scanning...
Attendance Recorded for E23CSEU2321_AMRIT
venv) PS C:\Users\DELL\OneDrive\Desktop\face_attendance_system>
venv) PS C:\Users\DELL\OneDrive\Desktop\face_attendance_system> python desktop_attendance.py
Loading known faces...
Loaded 35 face(s).
Scanning...
Already Recorded for E23CSEU2321_AMRIT
venv) PS C:\Users\DELL\OneDrive\Desktop\face_attendance_system>


127.0.0.1:5000
Face Attendance System
Smart, secure and automatic student attendance using facial recognition.
Go to Dashboard


127.0.0.1:5000/dashboard
Attendance Dashboard
← Back to Home
24-04-2025
Name or Enrollment
Search
Enrollment
Name
Status
e23cseu2208
anshika
Absent
e23cseu2316
khushi
Absent
E23CSEU2321
AMRIT
Present
e23cseu2326
kritika
Absent


Personal
Attendance Dashboard
127.0.0.1:5000/dashboard?date=2025-04-26&search=
Attendance Dashboard
← Back to Home
26-04-2025
Name or Enrollment
Search
Message
Holiday

Future Work

The field of face recognition technology continues to evolve rapidly, with ongoing advancements aimed at improving accuracy, efficiency, and applicability. Several areas of future work in face recognition systems include:

1. Improved Robustness to Real-World Variations:
   - Despite significant progress, face recognition systems still struggle with variations in lighting, facial expressions, and occlusions (e.g., glasses, masks, or scarves). Future work will focus on enhancing models to become more resilient to these challenges. One promising approach is the use of Generative Adversarial Networks (GANs) for data augmentation, enabling the system to handle a broader range of scenarios.
2. Real-Time Face Recognition:
   - Processing speed is critical for applications like surveillance and interactive systems. Future work will focus on optimizing algorithms for faster real-time processing without compromising accuracy. Edge computing and hardware acceleration (such as improved GPUs and specialized AI chips) will play a key role in reducing latency and enabling real-time performance.
3. Handling Low-Quality Images:
   - Face recognition systems often face difficulties with low-resolution or noisy images. Developing advanced techniques for image super-resolution and noise reduction will improve the accuracy of face recognition in such scenarios, making the technology more widely applicable.
4. Privacy and Security Concerns:
   - With the widespread adoption of face recognition technology, privacy and ethical concerns have become more pressing. Future research will explore methods to

anonymize data and protect user privacy, such as using federated learning and differential privacy to train models without exposing sensitive data.

5. Cross-Domain Face Recognition:
   - Face recognition systems typically perform well within a single environment or dataset, but cross-domain recognition (e.g., transferring a model trained on a specific dataset to another domain or environment) remains a challenge. Researchers will explore domain adaptation techniques to improve performance across diverse datasets and conditions.
6. Integration with Other Modalities:
   - To enhance the accuracy and usability of face recognition systems, integrating face recognition with other biometric modalities (e.g., voice, iris recognition, or fingerprint scanning) could create multi-factor authentication systems that are more secure and versatile. Hybrid systems can increase reliability, particularly in high-security settings.
7. Ethical and Bias Reduction:
   - Addressing the bias inherent in some face recognition models, particularly in recognizing faces from underrepresented groups, is crucial for the future. Researchers will continue to work on making face recognition systems more inclusive and fair by mitigating biases related to gender, race, and age.
8. Deep Learning and AI Advances:
   - As deep learning models and architectures continue to improve, future systems will likely benefit from innovations in neural networks, such as transformers and self-supervised learning, which could offer more efficient and accurate face recognition models without requiring vast amounts of labelled data.

GitHub Link of my Complete Project

Code

https://github.com/kritika038/Face_attendance_system

README

https://github.com/kritika038/Face_attendance_system/blob/main/README.md