Model and Approach Used

Face Detection

The system uses **OpenCV Haar Cascade (haarcascade_frontalface_default.xml)** to detect faces in real-time from webcam input. Haar cascades are pre-trained and lightweight, making them suitable for real-time applications on standard hardware.

Face Recognition Model

Face recognition is implemented using **LBPH (Local Binary Patterns Histogram)** provided by opencv-contrib-python.

Why LBPH was chosen:

- Works well for small datasets
- Robust to moderate lighting changes
- Fast and lightweight
- Easy to train and deploy locally
- Does not require GPU or heavy dependencies

Each registered user is assigned a numeric label, and the LBPH model learns facial texture patterns from multiple face samples per user.

Liveness (Spoof Prevention)

A **motion-based liveness detection** technique is used to prevent spoofing attacks with static images.
The system tracks face position changes across consecutive frames and verifies natural head movement before marking attendance.

This prevents basic photo-based spoofing while keeping the system simple and efficient.

Training Process

a. **Face Registration**

   - The user registers by standing in front of a webcam.
   - Approximately **30 grayscale face images** are captured per user.
   - Faces are detected, cropped, resized to a fixed size (200×200), and stored locally.

b. **Label Assignment**

- Each user folder is assigned a unique numeric label.
- A label-to-name mapping is created and saved for later use.

c. **Model Training**

- The LBPH face recognizer is trained using the collected face images and their labels.
- The trained model is saved as a .yml file.
- The label map is persisted to ensure consistent identity mapping during recognition.

d. **Recognition Phase**

- During runtime, the trained model predicts the label and confidence score for detected faces.
- Predictions are accepted only if the confidence score is below a strict threshold and liveness is confirmed.

Accuracy Expectations

Under normal indoor conditions:

- **Face recognition accuracy:** ~85–92%
- **False positives:** Reduced using strict confidence thresholding
- **Liveness detection:** Effective against static photo attacks

Accuracy depends on:

- Lighting conditions
- Camera quality
- Number and diversity of training images
- Proper face alignment during registration

The system is designed for **attendance use cases**, not high-security authentication.

Known Failure Cases

The following limitations are acknowledged:

- Poor lighting or strong backlight may reduce detection accuracy
- High-quality video replay attacks may bypass motion-based liveness detection
- Extreme head pose variations (side profile) may not be recognized
- Performance may degrade with very similar-looking individuals
- Not suitable for large-scale deployments without further optimization

These limitations are documented to demonstrate an understanding of real-world machine learning constraints.