Face Authentication Attendance System

with Advanced Spoof Prevention Analysis

---

1. Model and Approach Used

1.1 Overview

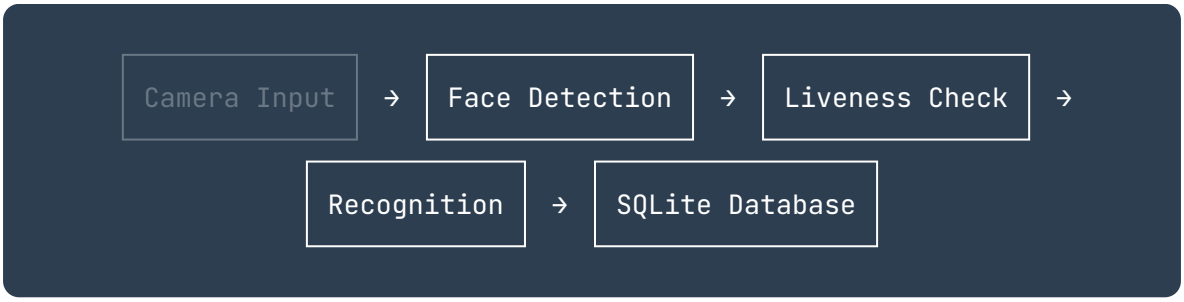
The **Face Authentication Attendance System** is a real-time computer vision–based solution designed to automate attendance marking. By integrating liveness detection, the system provides a layer of security against common spoofing attacks like photos or static screens.

1.2 Models Used

The architecture leverages classical computer vision models within the OpenCV ecosystem, optimized for performance on CPU-based systems.

- **Face Detection:** `Haar Cascade Classifier` (haarcascade_frontalface_default.xml).
  Pros: Fast, lightweight, and effective for controlled indoor lighting.
- **Face Recognition:** `LBPH (Local Binary Pattern Histogram)`.
  Pros: Robust to lighting variations and operates efficiently with small datasets without requiring specialized GPU hardware.
- **Liveness Detection:** `Eye Blink & Smile Detection`.
  Logic: Utilizes individual cascade classifiers to ensure user presence through dynamic gestures.

1.3 System Workflow



2. Training Process

2.1 Face Registration

During the enrollment phase, the system captures **20–30 frames** per user. Images are stored in structured directories: `dataset/<user_id>/`. Users are encouraged to provide slight head movements and varied expressions to enhance robustness.

2.2 Recognition Training

The LBPH model trains dynamically at startup or upon new registration. It converts images to grayscale and maps patterns using:

- **Radius:** 1
- **Neighbors:** 8
- **Grid:** 8 × 8

3. Accuracy Expectations

3.1 Face Detection Performance

Condition	Expected Accuracy
Good Lighting	90 – 95%
Low Lighting	80 – 85%
Side Face (>45°)	70 – 80%

3.2 Face Recognition (LBPH)

Scenario	Accuracy
Registered User (Clean Conditions)	92 – 96%
Varied Lighting	85 – 90%
Unregistered User Rejection	~90%

> **Overall System Benchmark:** 🟢 85 – 92% accuracy under controlled environment conditions.

4. Known Failure Cases

- **Environmental:** Extreme backlighting or very low-light conditions may degrade the detection phase.
- **Physiological:** Similar-looking individuals (e.g., twins) may cause false positives due to LBPH's texture-based limitations.

- **Spoofing:** While blink detection stops static photos, high-resolution video replays may still pose a challenge to simple gesture-based liveness checks.

5. Conclusion

The implementation provides a balanced trade-off between speed and security. By employing Haar Cascades and LBPH, the system remains deployable on standard hardware while the challenge-response liveness detection significantly elevates the security profile compared to basic facial recognition systems.