



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

An Access Monitoring System Utilising AI Facial Recognition. Facetrack By Charles Gill



This project develops a **facial recognition access monitoring system** that logs entries and exits by comparing live-captured faces against a known database.

Aims:

- Build a reliable, contactless recognition system.
- Monitor presence using face biometrics.

Objectives:

- Capture and align faces via webcam.
- Generate 128D face embeddings.
- Compare identities using cosine similarity.
- Record recognised individuals with timestamps.

The system begins by using **Haar cascades** to detect faces in the webcam feed based on edge and texture patterns. This is done via the **OpenCV** library.



Once a face is located, **RetinaFace** refines the detection and identifies five key landmarks: the eyes, nose, and mouth corners.

These landmarks help align the face for consistency.

The aligned face is then passed to **DeepFace**,



which extracts a **128-dimensional vector** — a unique biometric signature used for matching against stored profiles.

RetinaFace detects facial landmarks using feature pyramids.

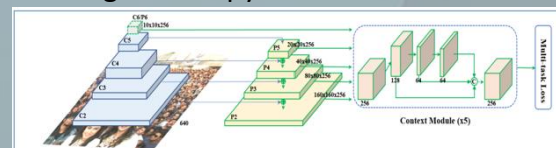


Figure 2. An overview of the proposed single-stage dense face localisation approach. RetinaFace is designed based on the feature pyramids with independent context modules. Following the context modules, we calculate a multi-task loss for each anchor.

DeepFace then converts the aligned face into a **128D vector**, stored in a database.

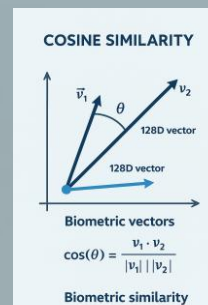


Figure: Matching via Cosine Similarity

During monitoring, a new face is encoded and compared to stored vectors using **cosine similarity** to find the closest match.

This project successfully demonstrates a working facial recognition system for access monitoring, using real-time face detection.

While the system proved accurate under controlled conditions, several limitations were identified.

Recognition performance was sensitive to lighting, face angles, and motion blur. High-quality biometric capture was essential.

Despite these challenges, the system performed well in practice, offering a contactless, efficient, and user-friendly alternative to traditional access logs. It lays the foundation for future enhancements and improved handling of lookalike errors.