Tunis Business School

End-of-Semester Project

Field of Study: **Information Technology**

Specialization: **Web Service Using Flask**

Topic

Web-Based Facial Authentication System: Theoretical Foundations

---

Presented by
Sinen Frej

Defended on: **May, 2025**

Academic Year: 2024/2025

1 Introduction

This document presents the theoretical foundations of our web-based facial authentication system designed for quiz authentication. The system combines computer vision techniques with efficient similarity search to verify user identity.

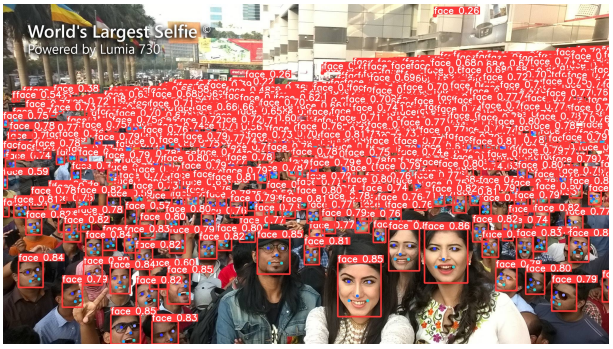
2 Main Components

2.1 Face Detection (YOLO)

For my object detection (a face in my case) I am going to use YOLO object detection systems based on convolutional neural networks fine tuned on many faces ,precisely (YOLOV8-faces) [1],.

this system :

- Uses convolutional neural networks to locate faces in images
- Outputs bounding box coordinates with confidence scores
- Processes images in real-time (optimized for web deployment)



2.2 Face Recognition (InsightFace)

InspireFace is a cross-platform face recognition SDK developed in C/C++, supporting multiple operating systems and various backend types for inference.

- Extracts 512-dimensional face embeddings
- Measures facial geometry: eye distance, nose shape, jawline, etc.
- Normalizes embeddings for illumination and pose variations

2.3 Similarity Search (FAISS)

Faiss ((Facebook AI Similarity Search) [3]is a library for efficient similarity search and clustering of dense vectors. It contains algorithms that search in sets of vectors of any size.

- Efficiently compares query embeddings with database
- Uses cosine similarity metric: $similarity = \frac{A \cdot B}{\|A\|\|B\|}$
- Approximate nearest neighbor search for scalability

3 Functional Flow

After the user grants camera permission, OpenCV's VideoCapture(0) function initializes the video stream. YOLO is then used to detect faces in real time, returning bounding boxes for each detected face. These face regions are sequentially passed to InsightFace, which generates a facial embedding for each. Finally, FAISS performs a nearest-neighbor search in the embedding database, and authentication is determined based on a predefined similarity threshold.

1. User grants camera permission
2. YOLO detects face in video stream
3. InsightFace extracts face embedding
4. FAISS searches for nearest neighbors in database
5. System calculates confidence score:

$$confidence = 1 - \min(distance)$$

6. Authentication decision based on threshold (typically 0.6-0.8)

4 Existing Solutions Analysis

4.1 Advantages

Facial recognition systems offer several compelling advantages. One of the most notable is the ability to provide contactless authentication.

Additionally, facial recognition is generally faster than traditional manual verification methods. Once implemented, it can authenticate individuals in seconds, significantly improving user experience and reducing queues in high-traffic environments such as airports or offices.

Security is another important advantage. Compared to traditional passwords or PIN codes, facial features are more difficult to forge or steal, offering a higher level of protection. This makes the system more resistant to common attacks like credential theft or brute-force access.

Moreover, technologies like FAISS (Facebook AI Similarity Search) have made it possible to scale facial recognition systems efficiently. FAISS allows for high-speed similarity .

4.2 Limitations

Despite their strengths, facial recognition systems face several limitations. Chief among these are privacy concerns surrounding the collection and storage of biometric data. Since facial data is inherently sensitive and uniquely tied to individuals, unauthorized access or misuse of such data could lead to serious ethical and legal issues.

Environmental factors also play a role in the system's performance. Variations in lighting, camera angles, or facial expressions can affect the accuracy of facial recognition, potentially leading to false positives or negatives.

Lastly, while facial recognition is generally secure, it is not immune to advanced spoofing techniques. Sophisticated attacks using high-resolution photos, realistic masks, or AI-generated deepfakes can sometimes fool these systems, highlighting the need for continuous improvement in anti-spoofing measures.

5 Bibliography

References

[1] Redmon, J. *et al.* (2016). "You Only Look Once: Unified, Real-Time Object Detection". CVPR.

[2] Deng, J. *et al.* (2019). "ArcFace: Additive Angular Margin Loss for Deep Face Recognition". CVPR.

[3] Johnson, J. *et al.* (2017). "Billion-scale similarity search with GPUs". arXiv:1702.08734.