**First Deliverable: Main concepts explanation**

Isra Mariem Thabti , Hiba Abdelli BA/IT

# Web-Based Facial Authentication System

We choose to work on facial recognition technology because of its immense potential to revolutionize various aspects of security, access control, and user authentication.

## Exploring the Evolution, Applications, and Ethical Considerations of Facial Recognition Technology:

Facial recognition technology is an emerging field in computer vision and artificial intelligence that enables machines to identify and verify individuals based on their facial features. It works by analyzing patterns, contours, and unique characteristics of a person's face, such as the distance between the eyes, the shape of the nose, and the contour of the jawline.

This technology has gained significant attention due to its wide range of potential applications, including security and surveillance, access control, authentication systems, and personalized user experiences. With advancements in deep learning and neural networks, facial recognition algorithms have become increasingly accurate and efficient, capable of handling various challenges such as changes in lighting conditions, facial expressions, and occlusions.

However, along with its benefits, facial recognition technology also raises concerns regarding privacy, security, and ethical considerations. Issues such as data protection, algorithmic bias, and the potential for misuse have sparked debates and led to calls for regulation and oversight.

Despite these challenges, facial recognition technology continues to evolve and find new applications in diverse fields, shaping the future of security, commerce, healthcare, and beyond. As researchers and developers work to address its limitations and mitigate risks, facial recognition holds promise as a powerful tool for enhancing convenience, efficiency, and security in our increasingly digital world.

## Protocol Explanation :

**Evaluation Protocols:** These protocols define how the performance of a facial recognition system is measured.

- **Data Sets:** The type and size of facial image datasets used for testing.
- **Metrics:** Accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR) etc. used to measure performance.
- **Scenarios:** Controlled lighting vs. variations in lighting, facial expressions etc.

**Security Protocols:** These protocols focus on securing the sensitive facial data used by the system. This might involve:

- **Data Encryption:** Storing facial data in a scrambled format to prevent unauthorized access.
- **Access Control:** Limiting who can access and use facial recognition data.
- **Audit Trails:** Tracking how facial data is used to ensure accountability.

## Standard Requirements :

**Face Detection**: Utilize an accurate face detection algorithm to detect faces in live video streams.

Consideration : handling varying lighting conditions, angles, and facial expressions.

**Image Capture**: Capture high-quality images of detected faces from the live video feed.

Consideration : Ensuring images are clear, well-aligned, and suitable for facial recognition.

**Facial Recognition**: Use a reliable facial recognition algorithm to compare captured face images with those stored in the database.

Recognition is guaranteed using **the geometry of the face** such as the distance between eyes, depth of eye sockets, distance from forehead to chin, the shape of cheekbones, lips, ears, chin,

nose, etc . A faceprint is sorted and compared to saved ones in the database .

**Database Management**: Securely store face images in the database, ensuring proper encryption and access controls.

**Authentication Decision**: Determine authentication decisions based on the similarity scores and percentage of accuracy or distance metrics calculated during facial recognition.

Consideration : Setting a threshold for similarity scores to determine acceptable matches for authentication.

**Logging and Auditing**: Log authentication attempts, including timestamps, user identifiers, and authentication results, for auditing purposes.

Consideration : Implement error logging to record any failures or exceptions encountered during the authentication process.

**Security Measures**: Encrypt sensitive data such as captured face images and authentication logs to protect user privacy.

**Functional Flow :**

1. **Face Detection during Live Video**:
    - Continuously capture frames from the live video feed.
    - Pass each frame through the face detection algorithm to detect any faces present.
2. **Image Capture of User's Face**:
    - When a face is detected, capture the corresponding frame containing the detected face (Preprocess the captured face image if necessary e.g., resizing, alignment).
3. **Facial Recognition and Comparison**:
    - Retrieve stored face images from the database.
    - Compare the captured face image with the stored images using the facial recognition algorithm.
    - Calculate similarity scores or distance metrics
4. **Authentication Decision**:
    - Determine if the similarity score exceeds the predefined threshold for authentication.
    - Grant access if a match is found above the threshold; otherwise, deny access.
5. **Error Handling**:
    - Handle  errors or exceptions encountered during the face detection, image capture, or facial recognition processes.
6. **Security Considerations**:
    - Ensure all components of the system adhere to security best practices, including encryption, access controls, and secure communication protocols.

With a potential to enhance security measures and streamline user verification processes , our system aims to make a significant contribution being extended to specific context that will be discovered and featured in the next deliverables .