



Web-Based Facial Authentication System

**INFORMATION ASSURANCE
AND SECURITY**

Prepared By :

- Yosr Boussarsar
- Islem Hamzaoui
- Eya Essid
- Eya Trabelsi
- Wadii Selman

TABLE OF CONTENT

1. INTRODUCTION	3
2. SYSTEM'S COMPONENTS	4
3. DATA EXCHANGE	5
4. WORKING FLOWS	7
5. USERS AND THEIR ROLES	9
6. MAIN FUNCTIONS	10
7. AUTHENTICATION DIAGRAM	13
8. CONCLUSION	14



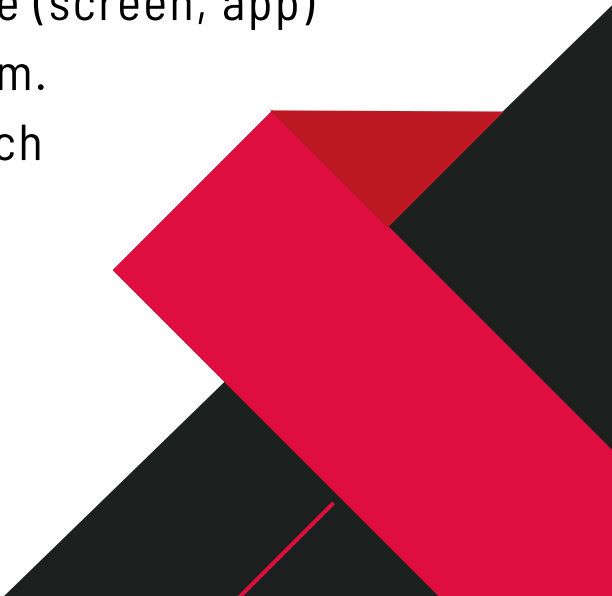
INTRODUCTION

A web-based facial authentication system offers a **secure** and **convenient** method for users to authenticate their identities using facial recognition technology.


This report outlines the **design, components, working flows, roles, functions, and data exchanged** within such a system.



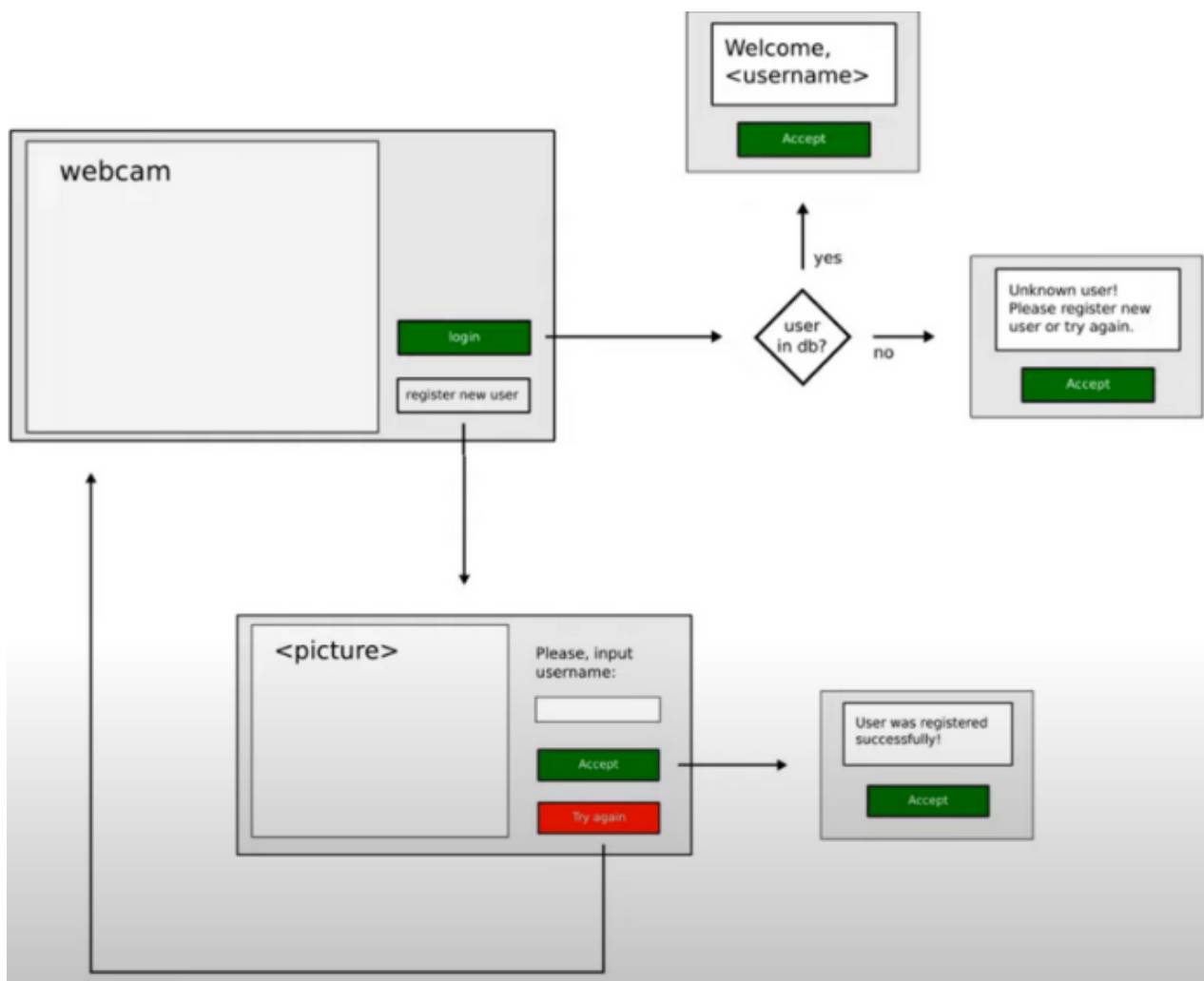
SYSTEM'S COMPONENTS

- **Capture Device:** This could be a **webcam**, **smartphone camera**, or **specialized facial recognition scanner**. It captures the user's face image.
 - **Facial Recognition Engine:** This software component analyzes the captured image. It extracts facial features like distance between eyes, lip shape, and nose bridge. It compares these **features** against a **database** of enrolled faces.
 - **Database:** This secure storage system holds templates (mathematical representations) of enrolled users' facial features.
 - **Secure Communication Channel:** This **encrypted pathway** transmits data between components. It ensures data privacy and security.
 - **Authentication Server:** This central server manages user **enrollment**, **authentication requests**, and **communication** with other components.
 - **User Interface:** This is the interface (screen, app) where users interact with the system. It can be a physical keypad or a touch screen for entering **PINs** or **confirmations**.
- 

DATA EXCHANGE

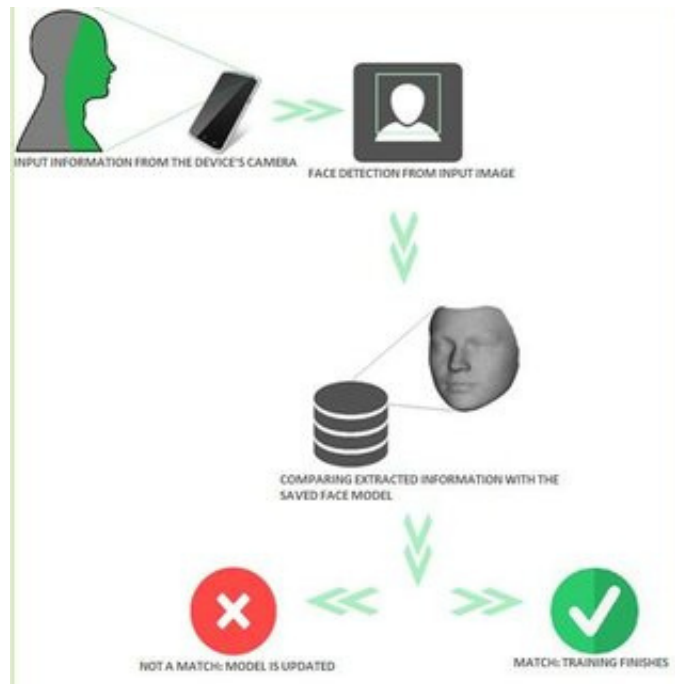
- **Enrollment:** User's facial image and a unique identifier (**ID number**, **username**) are captured and stored in the **database**.
 - **Authentication:** User's face is captured. The facial recognition engine extracts **features** and sends them to the **server**. The server retrieves the user's template from the database and compares it.
 - **Success/Failure:** The server sends a **success** or **failure** message to the user interface based on the comparison result.
- 

DATA EXCHANGE



WORKING FLOWS

The web-based facial authentication system typically consists of the following flows:




1. User Registration Flow: In this flow, a new user registers on the system by providing necessary details such as **name**, **email**, and creating a **password**.

2. Facial enrollment: The user is then prompted to take a photo of their face using their **webcam** (User's face image is captured from **multiple angles** for increased accuracy) or upload an existing photo. The system then extracts facial features from the photo and stores them in the user's profile.


WORKING FLOW

3. Authentication Flow: In this flow, a user who wants to authenticate themselves logs in to the system using their email and a photo of their face or upload an existing one. The system then extracts **facial features** from the new photo and compares them with the stored facial features of the user. If the features **match**, the user is authenticated and **granted access** to the system.

4. Administration Flow: In this flow, system administrators can manage user accounts, **set up** authentication **policies**, and monitor system activity. They can also configure the system to integrate with other applications or services.



USERS' ROLES


- **Enrolled User:** Individuals who have their facial data stored in the system for authentication purposes.
 - **System Administrator:** Manages user enrollment, system configuration, and access control and ensures the security and performance of the system.
 - **Developer:** A person who develops and maintains the system, integrates it with other applications or services and ensures its security and performance.
- 

MAIN FUNCTIONS

User Enrollment (Performed by the web user):

- Step 1: User provides identification and creates a PIN/password (for backup or multi-factor authentication).
- Step 2: User's face image is captured from multiple angles (optional for increased accuracy).
- Step 3: The system extracts facial features and creates a template.
- Step 4: The template and user ID are securely stored in the database.

User Authentication:

- Step 1: User initiates authentication (e.g., unlocking phone, accessing app).
 - Step 2: User's face is captured by the device.
 - Step 3: The facial recognition engine extracts features from the captured image.
 - Step 4: The extracted features are securely sent to the authentication server.
 - Step 5: The server retrieves the user's template from the database based on the user ID associated with the request.
 - Step 6: The server compares the received features with the user's template using a predefined algorithm.
- 

MAIN FUNCTIONS

==> On successful match:

- The server sends a success message to the user interface, granting access.
- Session Management: The system creates a session for the user, tracking their activity and automatically logging them out after inactivity or upon request.
- Access Control: The system verifies the user's role and permissions based on their identity and grants access to authorized resources.

==> On failed match:

- The server sends a failure message to the user interface, denying access.



MAIN FUNCTIONS


Facial Recognition:

- Step 1: Preprocessing - Enhances image quality by adjusting lighting, reducing noise, and normalizing orientation.
- Step 2: Face Detection - Locates the presence and position of a face within the image.
- Step 3: Feature Extraction - Identifies and extracts distinct facial features.
- Step 4: Feature Comparison - Compares the extracted features against a database of enrolled users' facial templates.

Password Reset (Optional):

- This function allows users to reset a forgotten PIN or password associated with their account for backup or multi-factor authentication purposes.

Two-Factor Authentication (MFA) (Optional):

- This function adds an extra layer of security by requiring a second verification factor after successful facial recognition.
- 

AUTHENTICATION DIAGRAM

Web Administration
and Monitoring



Face Recognition API



Web camera



Server and Database



RFID reader device



CONCLUSION

In conclusion, the web-based facial authentication system smoothly combines conventional authentication techniques with facial recognition technology.

Together, the system's components provide both security and user comfort.

Users may rapidly register and authenticate themselves thanks to the enrollment and authentication procedures.

Overall, this system provides a secure and user-friendly authentication solution for online platforms.

