

web-based facial authentication system

Group Members:

Yassine Majdoub

Mahdi Wanna

Aymen Mehrez



Outline:

I. Overview

II. Main Components of the Web-Based Facial Authentication System

III. Functional Flow of the System

IV. Applications

V. Limitations

VI. Conclusion and Future Work

VII. References

I. Overview

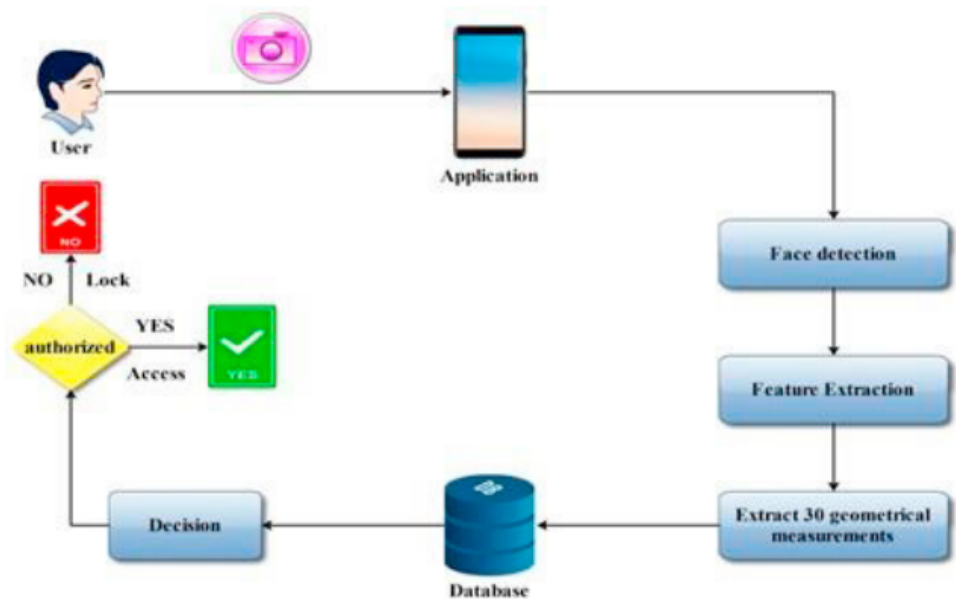
Facial recognition technology has gained widespread popularity as a biometric identification technique in recent years. Using deep learning algorithms, the software analyzes an individual's facial features and stores the data for future use. This technology has become widely used in exam proctoring systems, KYC processing systems, and even in simple mobile devices. One of the key advantages of facial recognition technology is its accuracy, which is higher than that of other biometric techniques. The software identifies approximately 80 distinct nodal points on an individual's face, which serve as endpoints for defining the variables of an individual's face, such as the shape of lips, eyes, length and width of the nose, and depth of eye sockets. In this report, we will explore the main concepts of the web-based facial authentication system, which utilizes facial recognition technology to authenticate users based on their facial features. We will examine the main components, functional flow, and design considerations of this system, as well as potential use cases and future developments.

II. Main components

1. Web-based interface: This is the primary user interface that allows the user to interact with the system. It provides features such as registration, login, and access to the user's profile.
2. Image Capture Module: This module is responsible for capturing the image of the user's face using a webcam. The image is then processed to extract the key facial features for authentication.
3. Facial Detection Module: This module detects the face within the captured image and extracts the key facial features. It uses techniques such as Haar cascades and deep learning algorithms for detecting faces.
4. Facial Recognition Module: This module compares the key facial features extracted from the captured image with those stored in the database for authentication. The facial recognition module uses algorithms such as Eigenface, Fisherface, and Local Binary Patterns Histograms (LBPH) for facial recognition.

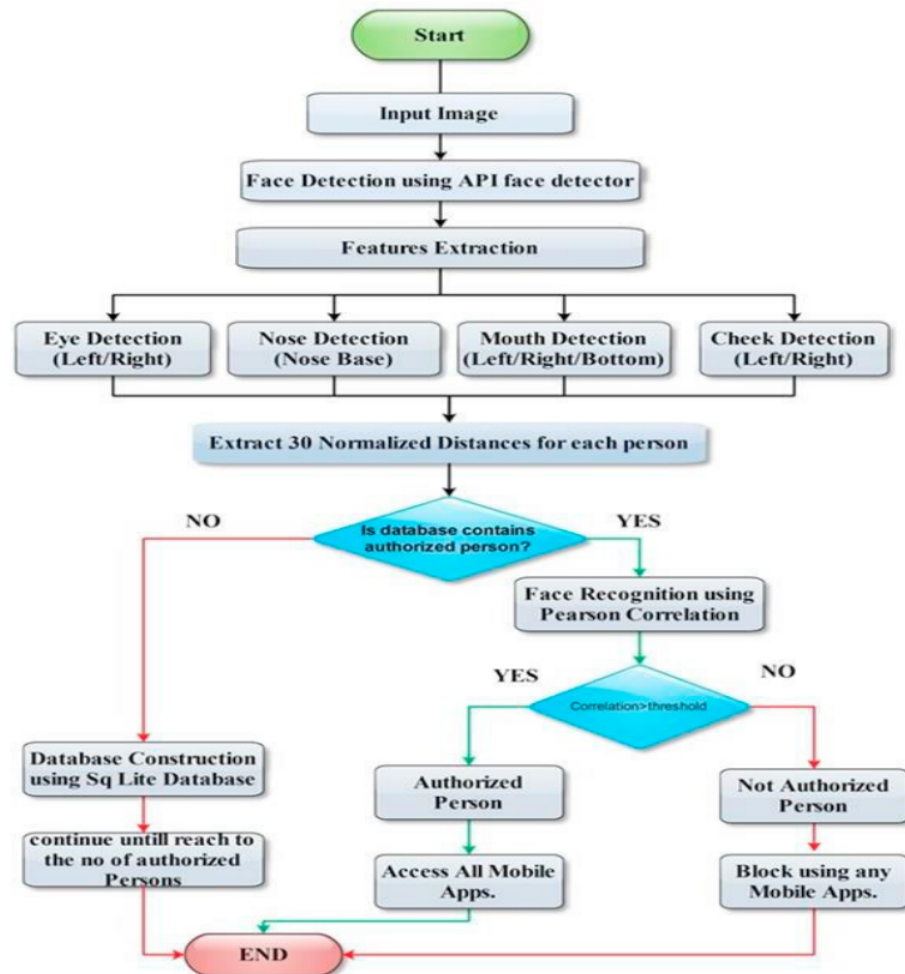
5. Database: The facial authentication system stores the facial features of authorized users in a database. This database is used for comparison during the authentication process.

III. Functional Flow of the System



- 1.Face detection: The system analyzes an image or video frame to locate faces and
2. create a faceprint, which is a set of numerical values that represent unique facial features.
- 3.Face alignment: The system adjusts the position, size, and orientation of the faceprint to a standardized format.
- 4.Feature extraction: The system extracts specific features from the faceprint, such as the distance between the eyes, the shape of the jawline, or the curvature of the lips.
- 5.Database creation: The system stores the faceprints in a database and associates each faceprint with a unique identifier.
- 6.Feature comparison: The system compares the extracted features against a database of known faces to find a match.
- 7.Recognition decision: The system calculates a confidence score based on the degree of similarity between the extracted features and the database of


known faces. If the confidence score exceeds a certain threshold, the system declares a match.



IV. Applications

I. Government use and law enforcement:

a. Security/Counterterrorism: Facial recognition technology can be used to identify potential security threats or individuals who pose a risk to national security. This could include identifying individuals on watchlists or tracking the movements of known terrorists.



b. Immigration: Immigration agencies can use facial recognition technology to verify the identity of individuals entering or leaving the country. This can help prevent individuals from entering the country illegally or using fake identification documents.

c. Law Enforcement: Police departments can use facial recognition technology to identify suspects in criminal investigations. This could include analyzing security footage from a crime scene or matching images from social media to known criminals in a database.

II. Commercial Use:

a. Day Care:

Facial authentication can be used in daycares to ensure that only authorized personnel are allowed to pick up children. The system can be programmed to recognize the faces of parents or guardians and only allow them to access the daycare facilities.

b. Residential Security:

Facial authentication can also be used in residential security systems. Homeowners can use their faces to unlock doors or disarm security systems. This ensures that only authorized individuals are allowed access to the property.

c. Voter Verification:

Facial authentication can be used to verify the identities of voters during elections. This can help prevent voter fraud and ensure that only eligible individuals are allowed to vote.

d. Banking Using ATM:

Facial authentication can be used in banking to enhance the security of ATM transactions. Instead of using a PIN or card, customers can use their faces to access their accounts and withdraw money. This can help prevent card skimming and other types of fraud.

V. Limitations :

1-Accuracy and Bias: Facial recognition algorithms are not always accurate, and their performance can be impacted by several factors, including lighting conditions, facial expressions, and camera angles. Additionally, there are concerns about the potential for algorithmic bias, where certain groups of people may be misidentified more often than others.

2-Privacy Concerns: Facial recognition technology raises significant privacy concerns, as it involves capturing and storing biometric data without individuals' explicit consent. This data could be used for surveillance purposes or shared with other entities, potentially compromising individuals' privacy and civil liberties.

3-Ethical Concerns: There are ethical concerns about the use of facial recognition technology, particularly in law enforcement contexts. There is a risk of false positives or false negatives, which could lead to wrongful arrest or prosecution. Additionally, facial recognition technology could be used to target individuals based on their race, religion, or other characteristics.

4-Technical Limitations: Facial recognition technology has technical limitations, such as difficulty in identifying individuals wearing masks or sunglasses, as well as the inability to recognize faces in low-resolution images or videos.

VI. Conclusion and Future Work

Facial recognition technology is an automated system that identifies and verifies a person's identity based on their facial features. It has gained widespread use in various industries, including security, law enforcement, and marketing. Its usage includes identifying suspects, tracking individuals' movements, and personalizing advertising.

However, facial recognition technology has limitations and concerns, including accuracy and bias issues, privacy concerns, ethical concerns, technical limitations, and social implications. These limitations and concerns pose significant challenges to the technology's future implementation.

There is a growing debate about the use of facial recognition technology, with some advocating for its use in specific contexts and others calling for its ban. To address these concerns, there are calls for more regulation, transparency, and accountability in the development and use of facial recognition technology.

The future implementation of facial recognition technology depends on addressing these limitations and concerns. It is crucial to balance the potential benefits of the technology with its potential negative impacts to ensure that its deployment is ethical, effective, and respects individual rights and freedoms.

VII. References

Rahouma, K. H., & Mahfouz, A. Z. (2021). Design and Implementation of a Face Recognition System Based on API mobile vision and Normalized Features of Still Images. In Proceedings of the 18th International Learning & Technology Conference.