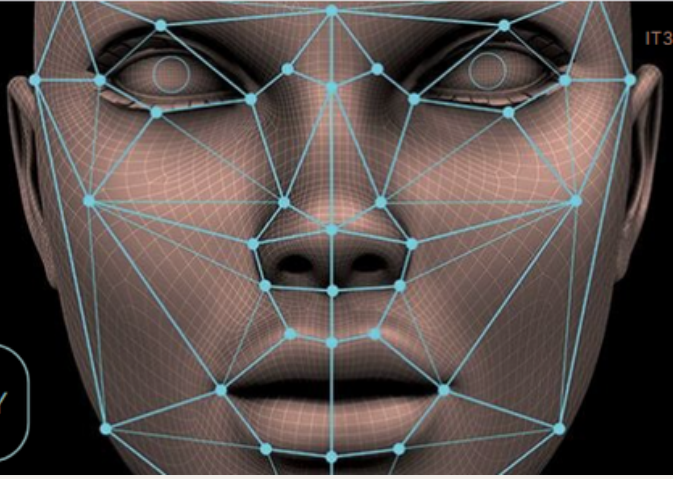
21/03/2024

IT360: INFORMATION INSURANCE AND SECURITY

Journey To The Future



FOR VERIFIED USERS ONLY

Introducing

3 E Y E S

Web-Based Facial Authentication System

Realized by:

Sarra Ibn El Haj - Ju.Fin/IT

Becher Zribi- Ju.Fin/IT

Amine Maaloul - Ju.BA/IT

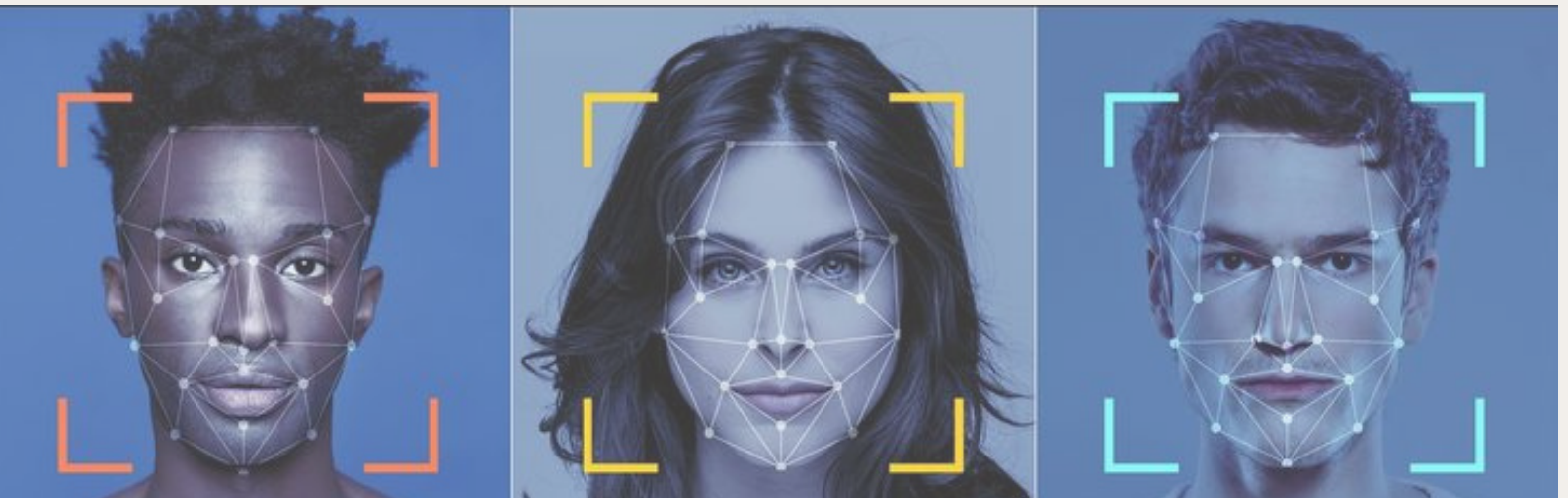
Raouf Lakhoues - Ju.BA/IT

Report Summary

- Introduction
- Deep Dive into the Main Components of a Web-Based Facial Authentication System
- Functional Flow
- Deep Dive into Technical Aspects of Web-Based Facial Authentication
- Security Protocols
- Standard Requirements and Standards
- Conclusion

Introduction

Ever wished you could ditch passwords entirely? Web-based facial recognition is here to help! This tech lets you log in to websites and apps with just a quick glance at your webcam. With facial recognition, users can log in to web applications without the hassle of entering their email-password or other user credentials. This authentication system is fast, convenient, and doesn't require any special hardware; most devices already have a webcam. Facial recognition technology uses artificial intelligence to create a unique map of a user's facial details, which is then stored as a hash to protect user privacy.



Deep Dive into the Main Components of a Web-Based Facial Authentication System

❶ Client-Side

1. **Webcam Capture:** This component utilizes the user's webcam to capture their facial image or video stream in real-time. Modern web browsers provide APIs for accessing the webcam with user permission.
2. **Facial Feature Extraction:**

- Some implementations perform basic facial feature extraction on the client-side using JavaScript libraries like OpenCV.js or through WebAssembly.
- These libraries can detect facial landmarks (eyes, nose, mouth) and extract relevant features for comparison.
- This can reduce the amount of data sent to the server, improving efficiency.

3. **Secure Communication:** The extracted features (or the entire image, depending on the approach) are securely transmitted to the server. This is typically done using HTTPS protocol, which encrypts the data in transit, protecting it from eavesdropping.

Deep Dive into the Main Components of a Web-Based Facial Authentication System

❷ Server-Side

1. **Data Reception:** The server receives the facial data (features or image) from the client.
2. **Facial Template Storage:** During user enrollment, the server securely stores the user's facial template in a database. This template is a mathematical representation of the user's face, extracted from their enrolment images using facial recognition algorithms.

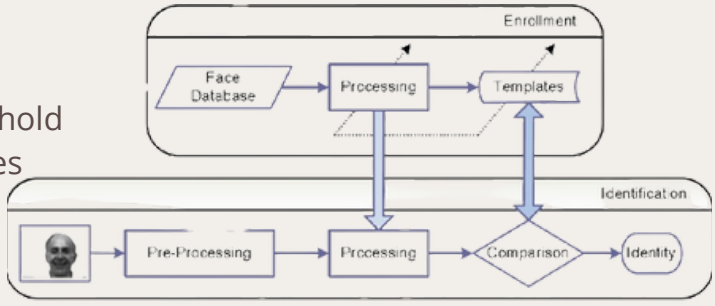
- For enhanced privacy, this template is often hashed using cryptographic techniques. Hashing transforms the data into a fixed-length value that cannot be easily reversed to obtain the original image.

3. **Facial Recognition Engine:** The core of the system is the facial recognition engine. It utilizes machine learning algorithms, typically deep learning models based on Convolutional Neural Networks (CNNs) trained on massive datasets of faces.

- The engine receives the newly captured facial data (from the login attempt) and compares it with the user's stored template. The comparison involves calculating a similarity score between the two representations.

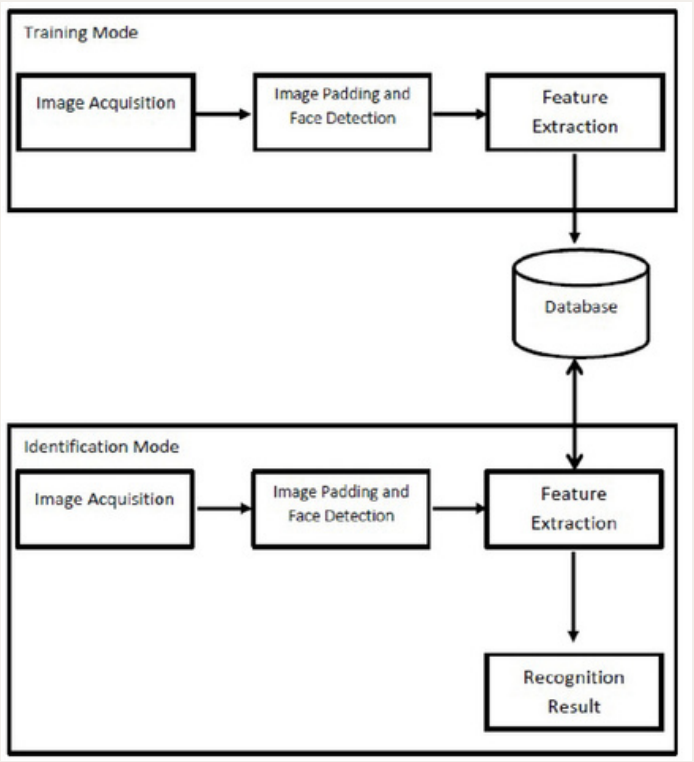
4. **Access Control:** Based on the similarity score returned by the facial recognition engine, the system makes an access control decision.

- If the score is above a predefined threshold (indicating a high degree of similarity), the system grants access to the user.
- Conversely, if the score falls below the threshold (indicating a low similarity), the system denies access, potentially prompting the user to try again or use an alternative authentication method



Functional Flow

1. User grants camera permission on the web application.
2. The webcam captures an image of the user's face.
3. Facial detection algorithms locate and isolate the face within the image.
4. Facial recognition techniques extract facial features and convert them into a faceprint.
5. The system compares the generated faceprint with the existing faceprints in the database.
6. An authentication result is produced, indicating whether the detected face matches any stored faceprints.
7. The authentication outcome is communicated to the web application for further processing or access control.



Deep Dive into Technical Aspects of a Web-Based Facial Authentication System

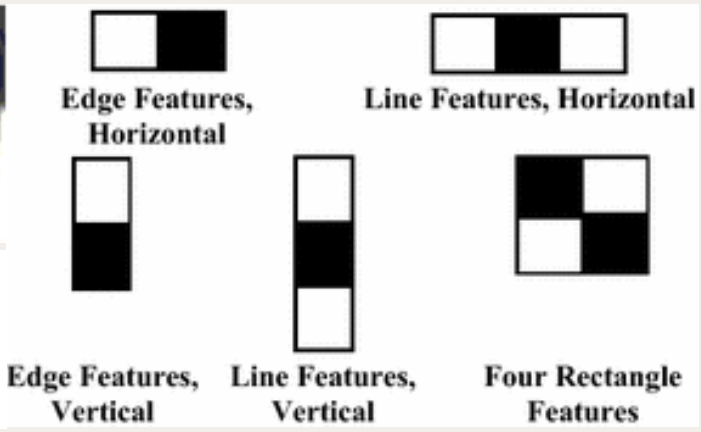
Facial detection and recognition are the core functionalities of a web-based facial authentication system.

❶ Face Detection

Locates the presence and position of human faces within an image or video stream.

1. **Viola-Jones Algorithm**: This is a classic and efficient method for face detection. It uses Haar features, which are simple image filters that can identify basic facial components like eyes, nose, and mouth. While effective for frontal faces, it might struggle with variations in pose or occlusion (e.g., someone wearing glasses).

$$f(x,y) = \sum_i p_b(i) - \sum_i p_w(i)$$



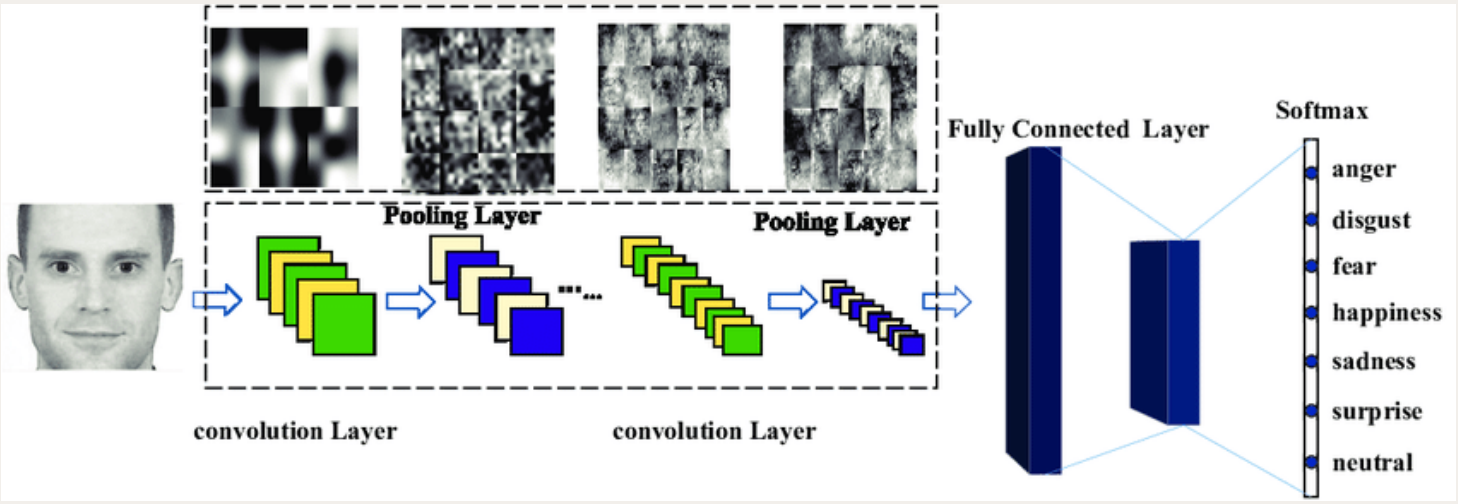
Deep Dive into Technical Aspects of a Web-Based Facial Authentication System

Facial detection and recognition are the core functionalities of a web-based facial authentication system.

❶ Face Detection

Locates the presence and position of human faces within an image or video stream.

2.**Convolutional Neural Networks (CNNs)**: Deep learning-based CNNs have become the dominant approach for face detection. These algorithms are trained on massive datasets of facial images and can achieve very high accuracy in detecting faces under various conditions, including pose variations, partial occlusions, and different lighting scenarios.



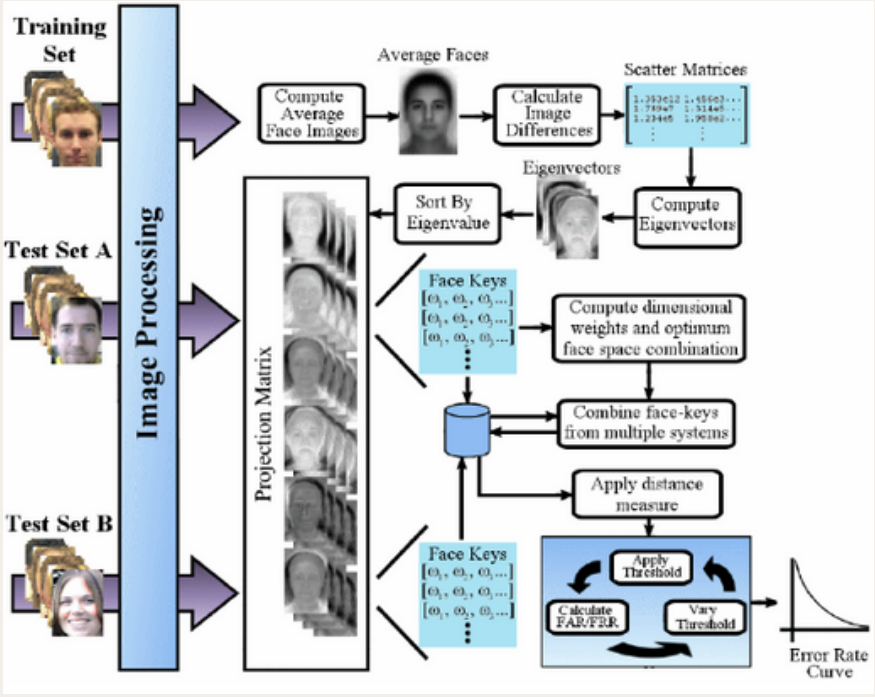
Deep Dive into Technical Aspects of a Web-Based Facial Authentication System

Facial detection and recognition are the core functionalities of a web-based facial authentication system.

❷ Face Recognition

Recognizes and identifies an individual based on their facial characteristics.

1. **Eigenfaces**: This technique, also known as Principal Component Analysis (PCA), creates a set of basis vectors (eigenfaces) that capture the most significant variations in a collection of facial images. A user's face can be represented as a linear combination of these eigenfaces.



Deep Dive into Technical Aspects of a Web-Based Facial Authentication System

Facial detection and recognition are the core functionalities of a web-based facial authentication system.

❷ Face Recognition

Recognizes and identifies an individual based on their facial characteristics.

1. Eigenfaces:

Let $X = \{x_1, x_2, \ldots, x_n\}$ be a random vector with observations $x_i \in R^d$.

1. Compute the mean μ

$$\mu = \frac{1}{n}\sum_{i=1}^{n} x_i$$

2. Compute the the Covariance Matrix S

$$S = \frac{1}{n}\sum_{i=1}^{n}(x_i - \mu)(x_i - \mu)^T,$$

3. Compute the eigenvalues λ_i and eigenvectors v_i of S

$$Sv_i = \lambda_i v_i, i = 1, 2, \ldots, n$$

4. Order the eigenvectors descending by their eigenvalue. The k principal components are the eigenvectors corresponding to the k largest eigenvalues.

The k principal components of the observed vector x are then given by:

$$y = W^T(x - \mu)$$

where $W = (v_1, v_2, \ldots, v_k)$.

The reconstruction from the PCA basis is given by:

$$x = Wy + \mu$$

where $W = (v_1, v_2, \ldots, v_k)$.

The Eigenfaces method then performs face recognition by:

- Projecting all training samples into the PCA subspace.
- Projecting the query image into the PCA subspace.
- Finding the nearest neighbor between the projected training images and the projected query image.

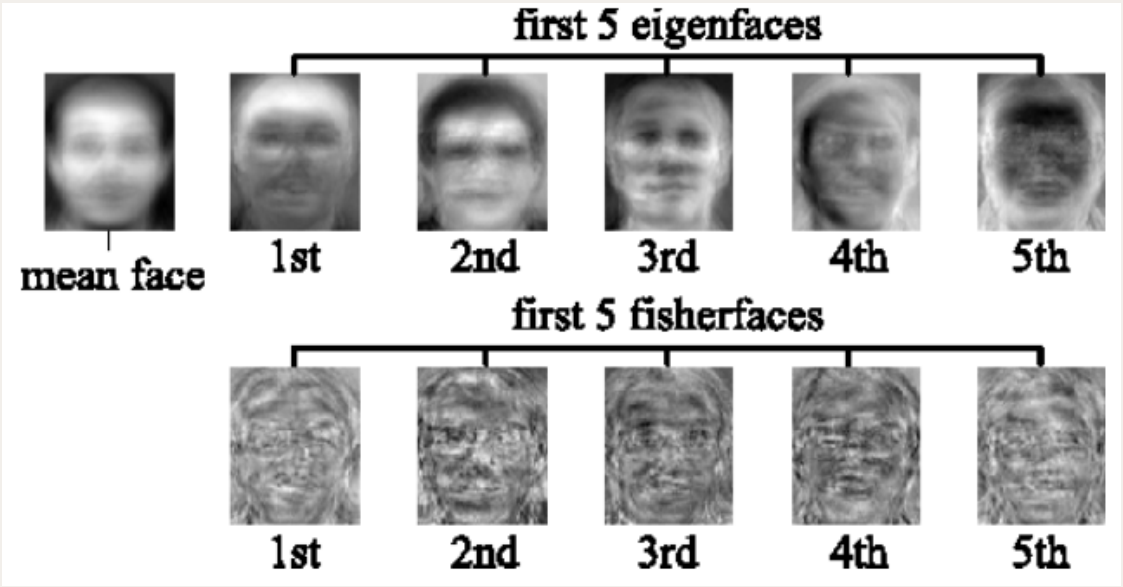
Deep Dive into Technical Aspects of a Web-Based Facial Authentication System

Facial detection and recognition are the core functionalities of a web-based facial authentication system.

❷ Face Recognition

Recognizes and identifies an individual based on their facial characteristics.

2.**Fisherfaces**: This method builds upon eigenfaces, focusing on maximizing the separation between different classes (individual users) in the facial data. This allows for more efficient discrimination between users during face recognition.



Deep Dive into Technical Aspects of a Web-Based Facial Authentication System

Facial detection and recognition are the core functionalities of a web-based facial authentication system.

❷ Face Recognition

Recognizes and identifies an individual based on their facial characteristics.

2.**Fisherfaces**:

Let X be a random vector with samples drawn from c classes:

$$\begin{aligned} X &= \{X_1, X_2, \ldots, X_c\} \\ X_i &= \{x_1, x_2, \ldots, x_n\} \end{aligned}$$

The scatter matrices S_B and S_{W} are calculated as:

$$\begin{aligned} S_B &= \sum_{i=1}^{c} N_i (\mu_i - \mu)(\mu_i - \mu)^T \\ S_W &= \sum_{i=1}^{c} \sum_{x_j \in X_i} (x_j - \mu_i)(x_j - \mu_i)^T \end{aligned}$$

, where μ is the total mean:

$$\mu = \frac{1}{N} \sum_{i=1}^{N} x_i$$

And μ_i is the mean of class $i \in \{1, \ldots, c\}$:

$$\mu_i = \frac{1}{|X_i|} \sum_{x_j \in X_i} x_j$$

Fisher's classic algorithm now looks for a projection W, that maximizes the class separability criterion:

$$W_{opt} = \arg\max_W \frac{|W^T S_B W|}{|W^T S_W W|}$$

Following [23], a solution for this optimization problem is given by solving the General Eigenvalue Problem:

$$\begin{aligned} S_B v_i &= \lambda_i S_w v_i \\ S_W^{-1} S_B v_i &= \lambda_i v_i \end{aligned}$$

The optimization problem can then be rewritten as:

$$\begin{aligned} W_{pca} &= \arg\max_W |W^T S_T W| \\ W_{fld} &= \arg\max_W \frac{|W^T W_{pca}^T S_B W_{pca} W|}{|W^T W_{pca}^T S_W W_{pca} W|} \end{aligned}$$

The transformation matrix W, that projects a sample into the $(c-1)$-dimensional space is then given by:

$$W = W_{fld}^T W_{pca}^T$$

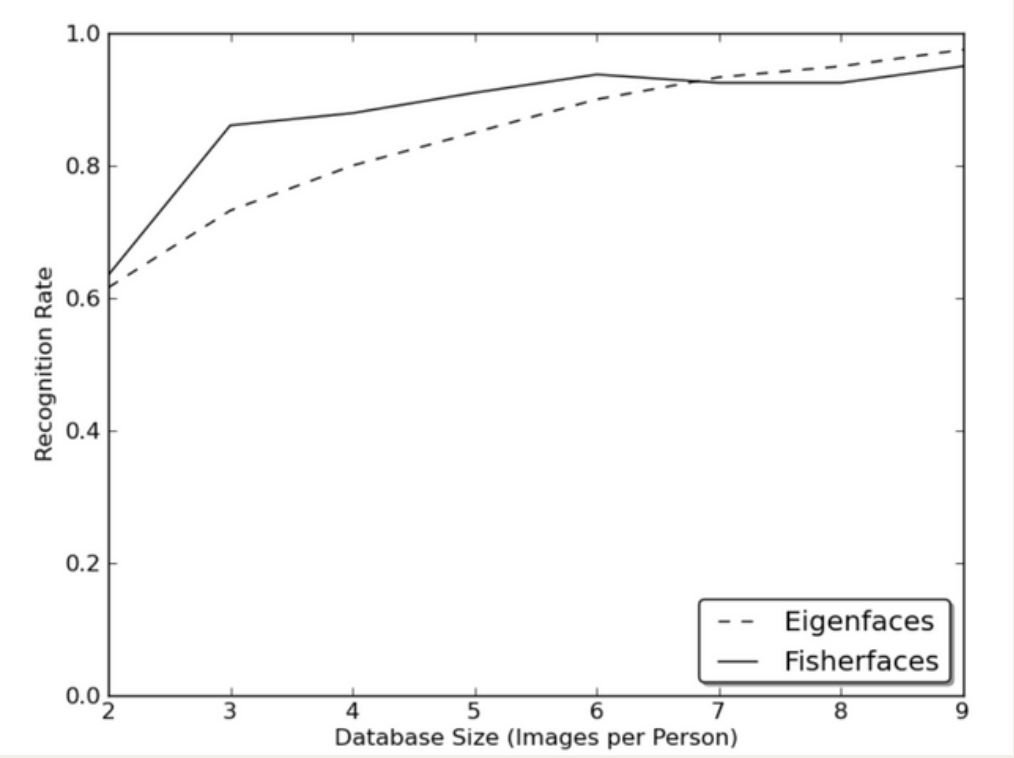
Deep Dive into Technical Aspects of a Web-Based Facial Authentication System

Facial detection and recognition are the core functionalities of a web-based facial authentication system.

❷ Face Recognition

Recognizes and identifies an individual based on their facial characteristics.

Fisherfaces method vs Eigenfaces method



Deep Dive into Technical Aspects of a Web-Based Facial Authentication System

Facial detection and recognition are the core functionalities of a web-based facial authentication system.

❷ Face Recognition

Recognizes and identifies an individual based on their facial characteristics.

3.**Local Binary Patterns (LBP)**: This approach analyzes small regions of the face and creates a binary code based on the intensity patterns of neighboring pixels. These LBP codes capture textural information about the face, which can be robust to lighting variations.

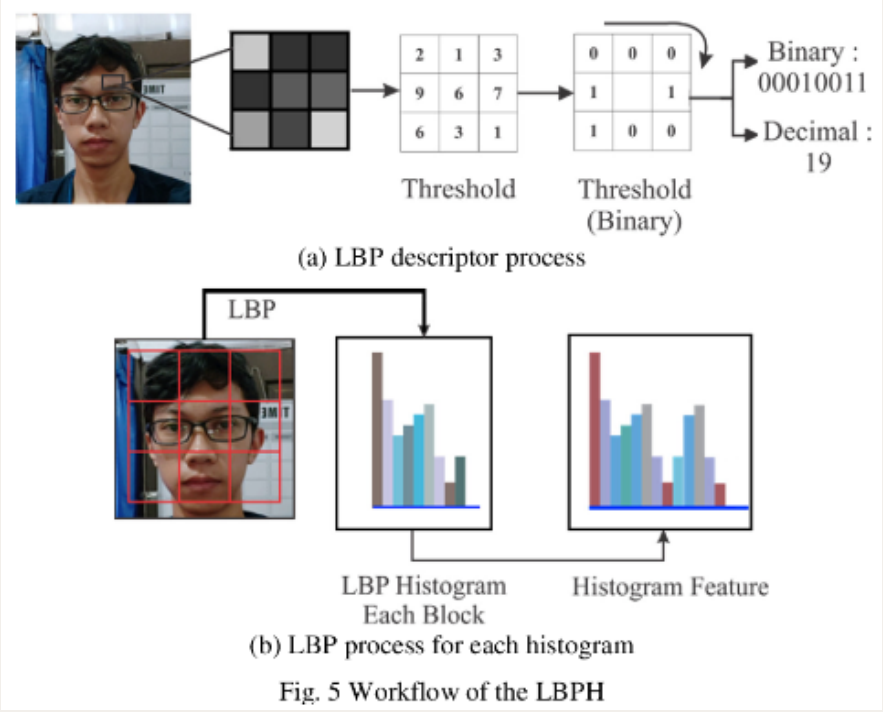


Fig. 5 Workflow of the LBPH

Deep Dive into Technical Aspects of a Web-Based Facial Authentication System

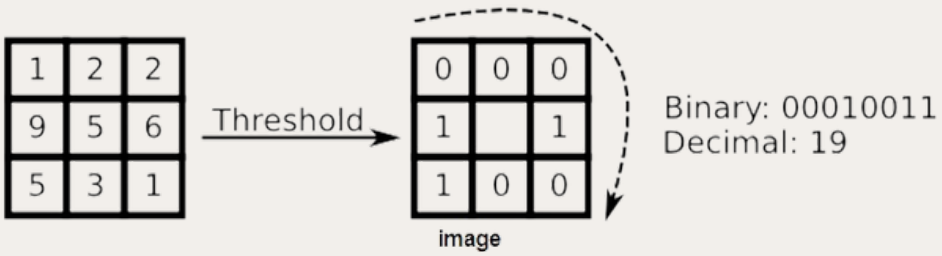
Facial detection and recognition are the core functionalities of a web-based facial authentication system.

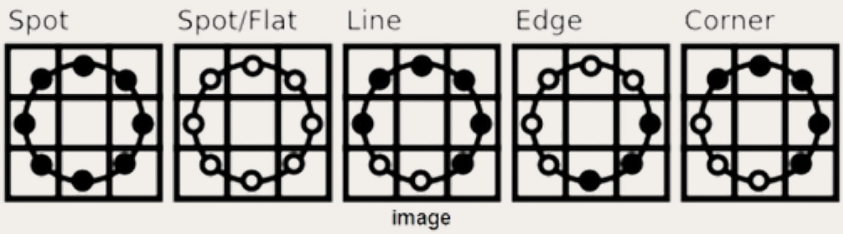
❷ Face Recognition

Recognizes and identifies an individual based on their facial characteristics.

3.Local Binary Patterns (LBP):

The basic idea of Local Binary Patterns is to summarize the local structure in an image by comparing each pixel with its neighborhood. Take a pixel as center and threshold its neighbors against. If the intensity of the center pixel is greater-equal its neighbor, then denote it with 1 and 0 if not.





For a given Point (x_c, y_c) the position of the neighbor (x_p, y_p), $p \in P$ can be calculated by:

$$x_p = x_c + R\cos(\frac{2\pi p}{P})$$
$$y_p = y_c - R\sin(\frac{2\pi p}{P})$$

Where R is the radius of the circle and P is the number of sample points.

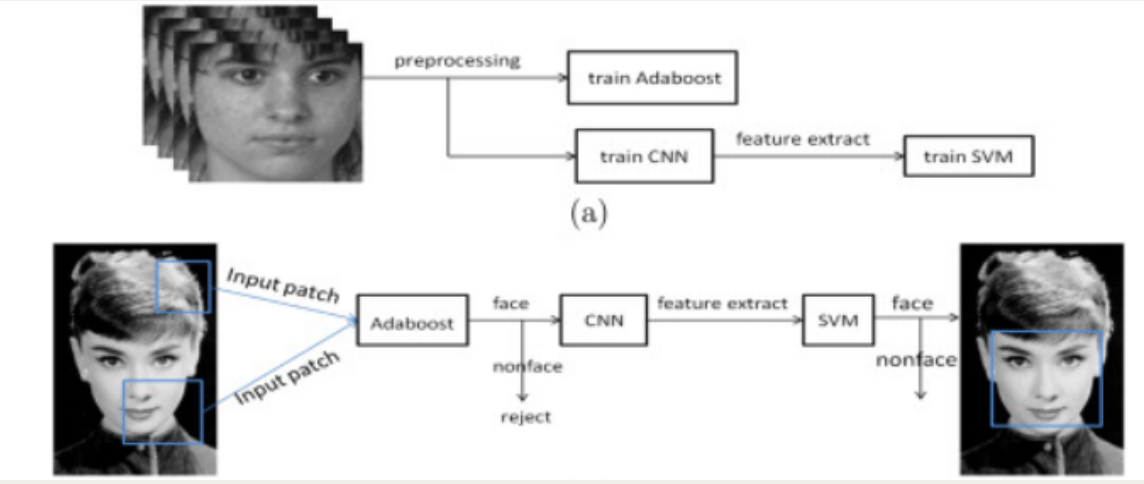
Deep Dive into Technical Aspects of a Web-Based Facial Authentication System

Facial detection and recognition are the core functionalities of a web-based facial authentication system.

❷ Face Recognition

Recognizes and identifies an individual based on their facial characteristics.

4.**Deep Learning Techniques**: Deep learning methods like **DeepFace** and **FaceNet** are currently state-of-the-art for face recognition. These algorithms learn complex representations of faces using large convolutional neural networks. They can achieve high accuracy even with challenging variations in pose, lighting, and expression. FaceNet, in particular, excels at generating facial embeddings - unique mathematical representations of faces - that enable efficient matching for recognition.



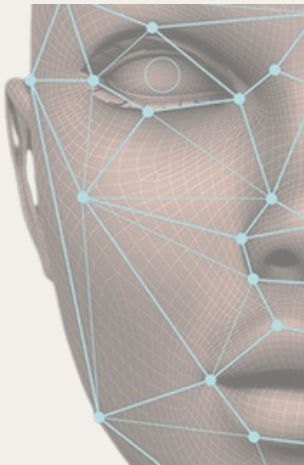
Security Protocols

- **HTTPS**: Ensures secure communication between the client-side and server-side by encrypting data transmission. This protects facial data (features or images) from eavesdropping.
- **Secure Hashing**: Facial templates stored on the server are often hashed using cryptographic techniques. Hashing transforms the data into a fixed-length value that cannot be easily reversed to obtain the original image.

Standard Requirements and Rules

Formal standards for web-based facial authentication systems are still evolving. However, some general considerations include:

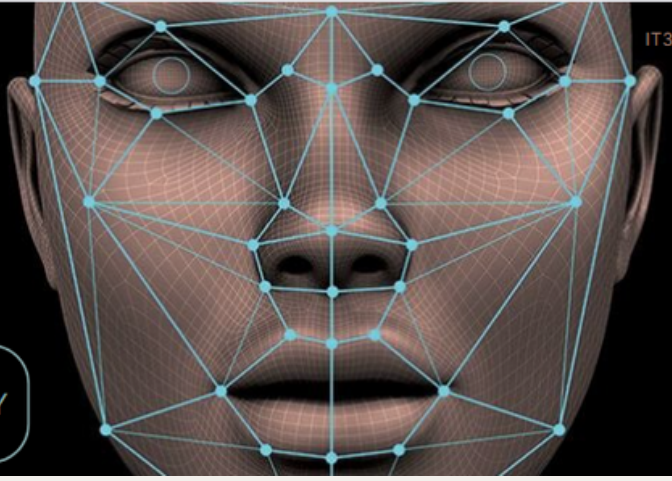
- **Data Privacy Regulations**: Compliance with regulations like GDPR (Europe) or CCPA (California) is crucial. These regulations govern data collection, storage, and user consent for facial recognition systems.
- **Accuracy and Liveness Detection**: The system should maintain a high degree of accuracy in recognizing authorized users and incorporate liveness detection measures to prevent spoofing attempts.
- **Transparency and User Control**: Users should be informed about how their facial data is collected, used, and stored. They should have the right to access, modify, or delete their data.
- **Security Auditing and Logging:** Comprehensive logging mechanisms should be in place to record all authentication attempts, system events, and administrative actions. Logs should be regularly reviewed and analysed to detect anomalies or security breaches.



Resources

OpenCV: OpenCV modules
OpenCV: Face Recognition with OpenCV
face-recognition · PyPI
Face Recognition as a Method of Authentication in a Web-Based System- Ben Wycliff Mugalu, Rodrick Calvin Wamala, Jonathan Serugunda, Andrew Katumba →explores integrating face recognition for user authentication in web systems.
Efficient Web-based Facial Recognition System Employing 2DHOG- S. Singh et al. (2016) → discusses a web-based facial recognition system using Gabor filters and a deep learning method.
Face recognition system - Shivam Singh,Prof. S. Graceline Jasmine → discusses a web-based facial recognition system using KLT Algorithm, Viola-Jones Algorithm face detection which detect human face using Haar cascade classifier.
Eigenfaces
Local Binary Patterns Histograms (LBPH)
Fisherfaces
Deep Learning
A Comprehensive Guide to Facial Recognition Algorithms
A gentle introduction to PCA
In-depth explanation of Eigenfaces
A Convolutional Neural Network Tutorial
Convolutional Neural Networks (CNNs)
Viola-Jones Algorithm
DeepFace
FaceNet
Deep Learning Techniques

Journey



To The Future

FOR VERIFIED USERS ONLY

Conclusion

Web-based facial authentication systems offer a promising alternative to traditional password-based methods. This technology leverages facial recognition algorithms to identify and authenticate users based on their unique facial characteristics. By capturing a user's face through a webcam, the system can grant access to web applications or online accounts, streamlining the login process and potentially enhancing security.

However, careful consideration of the technical challenges, privacy concerns, and user acceptance is crucial for successful implementation. Advancements in facial recognition accuracy, robust security protocols, and transparent user control over facial data are essential for wider adoption.

Overall, web-based facial authentication holds promise for the future of online security and user experience. As the technology matures and user concerns are addressed, it has the potential to revolutionize the way we interact with the digital world.

Thank You.

3 E Y E S