



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. EXISTING SOLUTIONS	6
3. FACIAL AUTHENTICATION USE CASES	12
4. ADVANTAGES	16
5. LIMITATIONS	17
6. CONCLUSION	20
7. REFERENCES	21



INTRODUCTION

Web-based facial authentication systems utilize facial recognition technology to verify a user's identity online.


These systems work by analyzing unique facial features to grant access to digital platforms.

This report will serve as an overview of the main characteristics, advantages, and limitations of existing web-based facial authentication solutions.




INTRODUCTION

Characteristics of web-based facial authentication solutions:

- Detection: This stage involves finding a face within an image. Initially, the system extracts the facial area from the input image.
 - Analysis (Face Mapping): After detection, the system analyzes the facial features by marking specific landmarks on the face. These landmarks include characteristics like the distance between the eyes, depth of eye sockets, and nose shape, which tend to remain consistent regardless of age or size. Approximately 80 such landmarks are identified, and their measurements are used to generate a unique code known as a 'faceprint' for each individual.
- 

INTRODUCTION

- Matching: In this stage, the generated faceprint is compared with prints stored in the system's database. To ensure accuracy, the system utilizes various layers of technology. Since most databases contain 2D photos, the images undergo processing to resemble their 3D counterparts. This process may involve pulling out facial landmarks and adjusting for factors like differences in lighting, facial expressions, and angles. If the subject image is low resolution, additional encoding and decoding may be required to enhance detail. The algorithms assess similarity scores obtained from comparing features of the new face image with those of known faces.
 - Recognition (Confirming Identity): Based on the similarity scores obtained during the matching stage, the system makes a decision regarding the identity of the individual. This decision-making process may involve applying threshold values to similarity scores or employing more sophisticated techniques. Ultimately, the system confirms the identity of the person based on the comparison results.
- 


EXISTING SOLUTIONS

1. Off-the-Shelf Solutions and APIs:

- Companies can opt for ready-made solutions like Microsoft Face API, Amazon Rekognition, or utilize existing facial recognition libraries such as DeepFace, FaceNet, InsightFace, among others.
- Off-the-shelf solutions offer a faster option for general public applications, reducing the need for custom software development
- *Characteristics:* Ready-made solutions, easy integration, cost-effective, and time-saving.


EXISTING SOLUTIONS

Examples of facial recognition technologies:

1. **Amazon** previously promoted its cloud-based face recognition service named **Rekognition** to law enforcement agencies.
 2. **Apple FaceID** uses facial recognition to help users quickly unlock their phones, log in to apps, and make purchases.
 3. **British Airways** enables facial recognition for passengers boarding flights from the US. Travellers' faces can be scanned by a camera to have their identity verified to board their plane without showing their passport or boarding pass.
 4. **Cigna**, a US-based healthcare insurer, allows customers in China to file health insurance claims which are signed using a photo, rather than a written signature, in a bid to cut down on instances of fraud.
- 

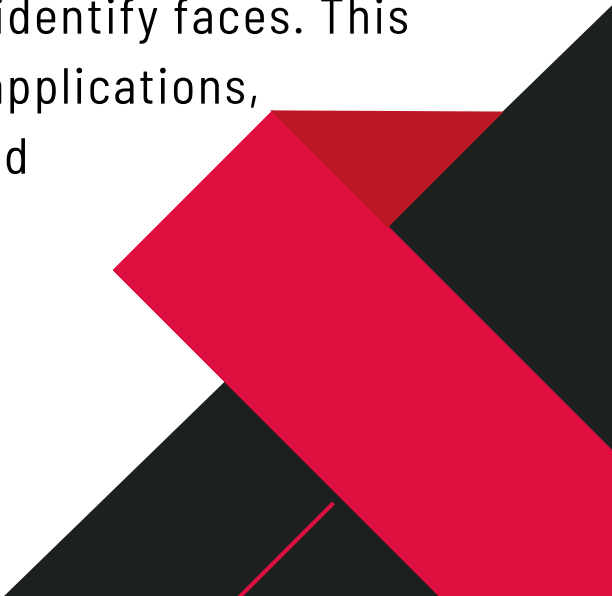
EXISTING SOLUTIONS

2. Custom Software Development:

- For specialized needs or industries, custom software development may be necessary to tailor facial recognition systems to specific requirements
 - Custom solutions allow for more control over the technology and can be fine-tuned to meet unique business needs
 - *Characteristics:* Tailored solutions, high precision, flexibility, and scalability.
 - *Example:* Developing a custom facial recognition system for a financial institution to enhance security and streamline customer authentication processes.
- 


EXISTING SOLUTIONS

3. Facial Recognition Based on Machine Learning:

- Facial recognition based on machine learning involves training algorithms to recognize faces by extracting features from images and learning patterns from labeled data. These algorithms typically use techniques like principal component analysis (PCA), linear discriminant analysis (LDA), or support vector machines (SVM).
 - Characteristics: Machine learning-based facial recognition systems require a set of labeled training data to learn patterns and features. They are effective in identifying faces in images with varying lighting conditions, angles, and facial expressions.
 - Example: An example of facial recognition based on machine learning is the Eigenfaces algorithm, which uses PCA to extract principal components from facial images and then compares them to identify faces. This approach has been used in various applications, including access control systems and surveillance.
- 


EXISTING SOLUTIONS

4. Facial Recognition Based on Deep Learning:

- Facial recognition based on deep learning utilizes deep neural networks, such as convolutional neural networks (CNNs), to automatically learn hierarchical representations of facial features from raw image data. These networks are trained on large datasets of labeled facial images to learn discriminative features for face recognition.
 - Characteristics: Deep learning-based facial recognition systems can achieve high accuracy levels and robustness to variations in lighting, pose, and facial expression. They can learn complex patterns and features directly from raw image data without the need for explicit feature extraction.
 - Example: An example of facial recognition based on deep learning is FaceNet, a deep neural network architecture that learns embeddings of facial images in a high-dimensional feature space. This approach has been widely adopted in commercial facial recognition systems, social media platforms, and law enforcement applications.
- 

EXISTING SOLUTIONS

5. Facial Recognition Without AI:

- Facial recognition without AI refers to traditional methods of face recognition that rely on handcrafted features and rule-based algorithms rather than machine learning or deep learning techniques. These methods often use techniques like geometric feature extraction, template matching, or correlation-based matching.
 - Characteristics: Facial recognition without AI may be less flexible and adaptive compared to machine learning or deep learning approaches. These methods may struggle with variations in lighting, pose, and facial expression and may require manual tuning of parameters for optimal performance.
 - Example: An example of facial recognition without AI is the Viola-Jones algorithm, which uses Haar-like features and a cascaded classifier to detect faces in images. This approach has been used in early facial recognition systems and applications where computational resources are limited or where real-time performance is critical.
- 


FACIAL AUTHENTICATION USE CASES

- **Healthcare**

Facial authentication is increasingly utilized in hospitals to enhance patient care. Healthcare providers are exploring its application for accessing patient records, simplifying registration processes, and identifying genetic diseases. AiCure has developed an app leveraging facial recognition to confirm medication adherence, ensuring patients take their prescribed medication accurately.

- **Car Industry**

Car companies are experimenting with facial recognition to replace car keys. The technology would replace the key to access and start the car and remember drivers' preferences for seat and mirror positions and radio station presets.




FACIAL AUTHENTICATION USE CASES

- **Unlocking phones**

Various phones use face authentication to unlock the device. The technology offers a powerful way to protect personal data even if the phone is stolen. Apple claims that the chance of a random face unlocking your phone is about one in 1 million.

- **Airports and border control**

Facial recognition has become a familiar sight at many airports around the world. Increasing numbers of travelers holding biometric passports, which allow them to skip the ordinarily long lines and instead walk through an automated ePassport control to reach the gate faster. Facial recognition not only reduces waiting times but also allows airports to improve security.




FACIAL AUTHENTICATION USE CASES

- **Banking and Payment**

Biometric online banking is another benefit of face authentication. Instead of using one-time passwords, customers can authorize transactions by looking at their smartphone or computer. With facial authentication, there are no passwords for hackers to compromise. If hackers steal your photo database, 'liveless' detection – a technique used to determine whether the source of a biometric sample is a live human being or a fake representation – should (in theory) prevent them from using it for impersonation purposes. Face recognition could make debit cards and signatures a thing of the past.

“Face pay” technology could allow shoppers to skip long checkout lines with slower payment methods.



FACIAL AUTHENTICATION USE CASES


- **Tracking students**

Some educational institutions in China use face recognition to ensure students are not skipping class. Tablets are used to scan students' faces and match them to photos in a database to validate their identities.

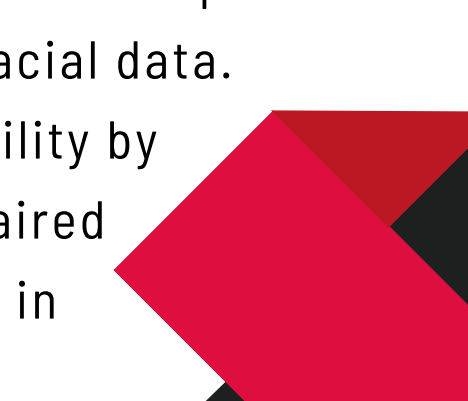
- **Employees Attendance**

The technology can be used for workers to sign in and out of their workplaces, so that employers can track attendance.


The Facial authentication system has achieved impressive success with a 99.5% accuracy in recognizing employees' faces and processing records for over 500 employees daily, ensuring exceptional precision and reliability.



ADVANTAGES

- **Enhanced Security:** Provides a secure and user-friendly alternative to traditional password authentication, reducing the risk of data breaches.
 - **Reduced number of touchpoints:** Facial recognition enables identification with less action required from the user. Users do not have to enter multiple forms of personally identifiable information -- or passwords -- to be authenticated, they can just show their face.
 - **Convenience:** Simplifies user experience by eliminating the need to remember multiple passwords.
 - **Efficiency:** Speeds up security checks and authentication processes, improving user experience.
 - **Personalization:** Enables personalized experiences and targeted services based on facial data.
 - **Accessibility:** Supports accessibility by describing photos to visually impaired users and streamlining processes in various industries.
- 

LIMITATIONS

- **Accuracy Concerns and Bias:** Facial recognition systems, like many artificial intelligence systems, have a history of bias. They can make mistakes and exhibit biases. Facial recognition systems with a lack of diversity in algorithm training are more likely to misidentify members of minority groups, i.e., groups that were not equally represented in the training data.
 - **Biometric Variability:** Variations in facial appearance due to aging, changes in hairstyle, or facial hair may pose challenges for accurate authentication, requiring continuous refinement of algorithms.
 - **Imperfections:** Technology can be fooled by factors like lighting, angles, or alterations, impacting its reliability.
- 

LIMITATIONS

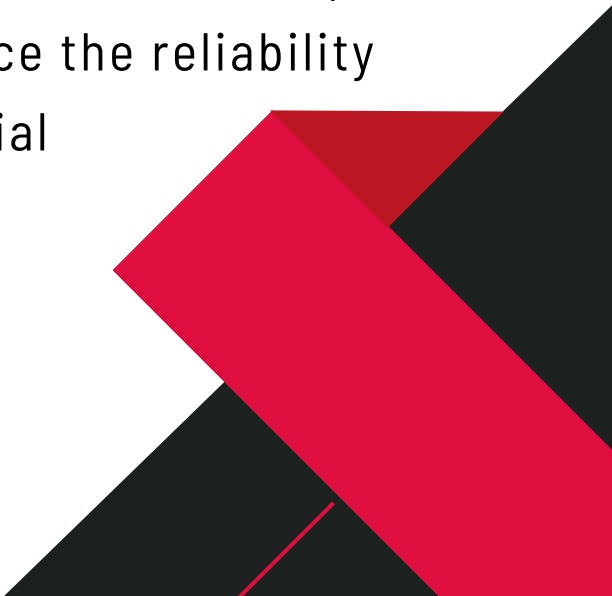
- **Ethical Considerations:** Deployment of facial recognition technology in web-based systems raises ethical dilemmas regarding consent, surveillance, and potential biases, necessitating ethical frameworks and regulatory oversight.
 - **Privacy Issues:** Raises concerns about privacy, surveillance, and unauthorized tracking or monitoring of individuals.
 - **Ownership Challenges:** Questions arise regarding the ownership of facial data when third-party tools are used.
 - **Legal and Regulatory Hurdles:** Compliance with data protection and privacy laws poses challenges, leading to potential legal and financial penalties.
- 

LIMITATIONS

- **Resource Intensiveness:** High computational requirements for facial detection and recognition algorithms may impose resource constraints, particularly in resource-constrained environments or on low-powered devices.
- **Vulnerability to Attacks:** Facial authentication systems are susceptible to adversarial attacks, such as spoofing or impersonation, highlighting the need for robust countermeasures, including liveness detection and anti-spoofing techniques.



CONCLUSION

- In conclusion, while web-based facial authentication systems offer significant advantages in terms of security, convenience, and efficiency, but they also face challenges related to accuracy, privacy, ownership, legal compliance, and technological imperfections.
 - Organizations implementing these systems need to address these limitations to ensure the responsible and effective use of facial recognition technology.
 - They should ensure informed consent mechanisms for data collection, implement explainable AI solutions, and consider backup verification methods to enhance the reliability and security of web-based facial authentication systems.
- 

REFERENCES

<https://www.techtarget.com/whatis/feature/Pros-and-cons-of-facial-recognition>

<https://visagetechnologies.com/benefits-of-face-recognition/>

<https://www.itpro.com/security/privacy/356882/the-pros-and-cons-of-facial-recognition-technology>

<https://itrexgroup.com/blog/facial-recognition-benefits-applications-challenges/>

<https://www.oloid.ai/blog/facial-authentication-technology-benefits-and-challenges/>

<https://www.spiceworks.com/it-security/identity-access-management/articles/facial-recognition-software/>

Thank You