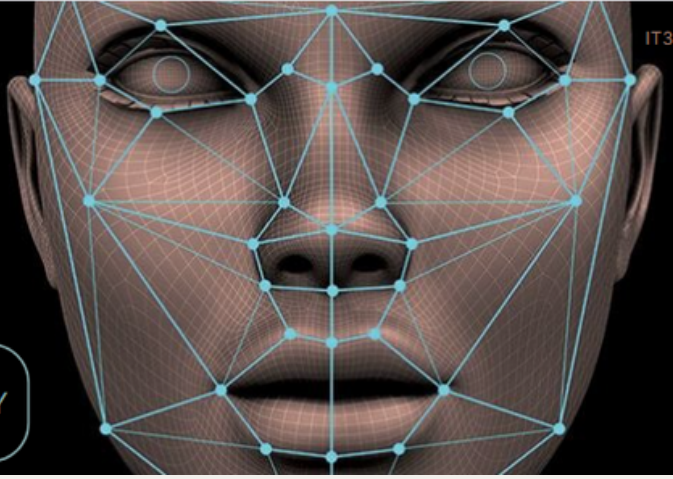
21/03/2024

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

Unveiling the Face of Security: A Deep Dive into Existing Facial Authentication Systems

In today's digital landscape, security and user convenience are paramount. Traditional password-based authentication methods are increasingly vulnerable to breaches, prompting the need for more robust and user-friendly solutions. Facial authentication systems (FAS) have emerged as a promising alternative, leveraging the power of facial recognition technology for secure and seamless user identification.

This report delves into the world of existing FAS solutions. We'll explore the core components that make up a web-based facial authentication system, examining both the client-side (user's web browser) and server-side (backend infrastructure) functionalities. We'll then shed light on the most popular existing solutions, including cloud-based services and on-premise options.

Furthermore, we'll delve into the technical aspects of FAS, analyzing the different facial recognition algorithms, security protocols, and data handling practices employed. This analysis will encompass the advantages and limitations of each approach, considering factors like accuracy, scalability, privacy concerns, and user acceptance.

Ultimately, this report aims to provide a comprehensive understanding of the existing landscape of facial authentication systems. By exploring the technical intricacies, advantages, and limitations, we can pave the way for informed discussions about the future of this evolving technology in the realm of secure and convenient online experiences.

Amazon Rekognition

Amazon Rekognition is a cloud-based facial recognition software with superpowers. It not only recognizes faces in images and videos, but also identifies objects and scenes. Rekognition offers features like:

- Custom labels for specific objects you need to identify.
- Content moderation to flag inappropriate content
- Text detection to recognize text within images.
- PPE detection to ensure worker safety.
- Face search and verification within a private database.
- Video analysis for real-time insights.

Amazon Rekognition

Advantages

- **Simple Integration:** Pre-built APIs make Rekognition easy to add to your web applications.
- **Effortless Scaling:** Amazon handles infrastructure, so Rekognition scales with your user base.
- **High Accuracy:** Continuously improved algorithms ensure reliable facial recognition.
- **Cost-Effective:** Saves development time and money by eliminating the need to build your own system.
- **Secure:** Uses HTTPS encryption and hashed data storage for robust security.
- **Versatile:** Offers object and scene detection in addition to facial recognition.

Disadvantages

- **Vendor Lock-In:** Switching to another provider can be difficult after integrating Rekognition.
- **Privacy Concerns:** Storing facial data on Amazon's servers raises privacy issues, requiring compliance with regulations and transparency.
- **Limited Customization:** Rekognition offers less customization compared to building your own system, with control limited to thresholds and filters.
- **Security Risks:** Cloud storage remains vulnerable to cyberattacks, requiring strong access controls.

Betaface

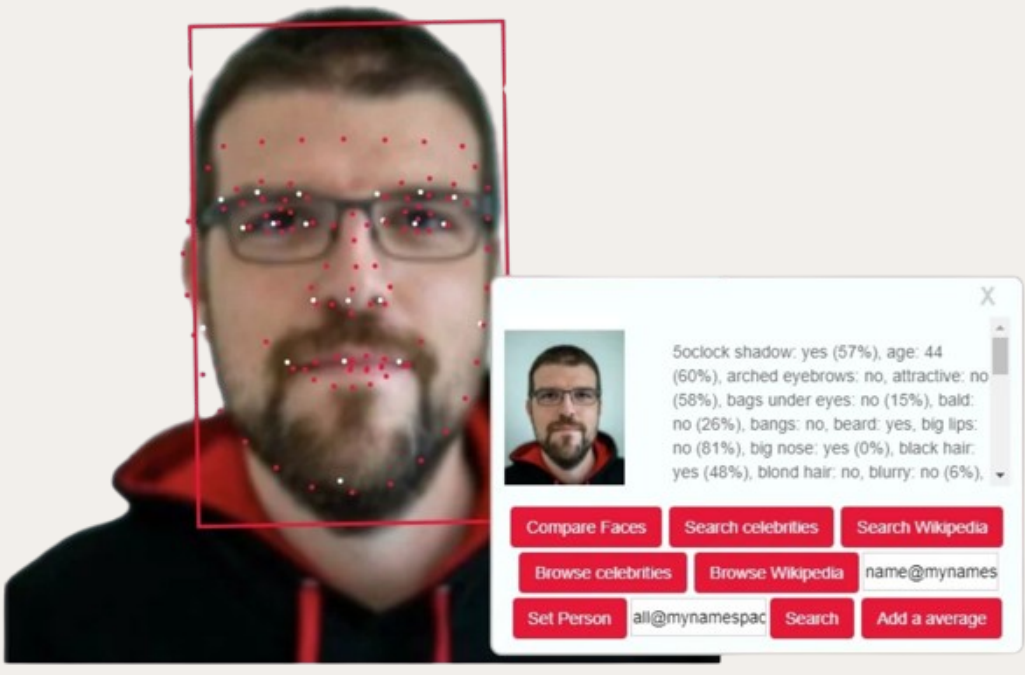
Core Concept:

Betaface mainly focuses on image and video analysis and face and objection recognition.It offers 3 kinds of services:

- Facial recognition SDKs
- Hosted web services
- Custom software development services

It's capabilities:

- Simple face detection
- Complex facial recognition (identification and verification)
- Emotion and ethnicity recognition
- Skin, hair, facial feature, and hairstyle tracking



Betaface

Advantages

- **Data Privacy:** Betaface lets you store facial data on-site, ideal for companies with strict privacy concerns or those uncomfortable with cloud storage.
- **Customization:** Betaface offers more control over the facial recognition system than cloud options. Developers can tailor the algorithms and how it works to fit specific needs.
- **Cost-Effectiveness:** For companies with many users, Betaface's on-premise solution might be cheaper in the long run compared to paying subscription fees for cloud-based services.

Disadvantages

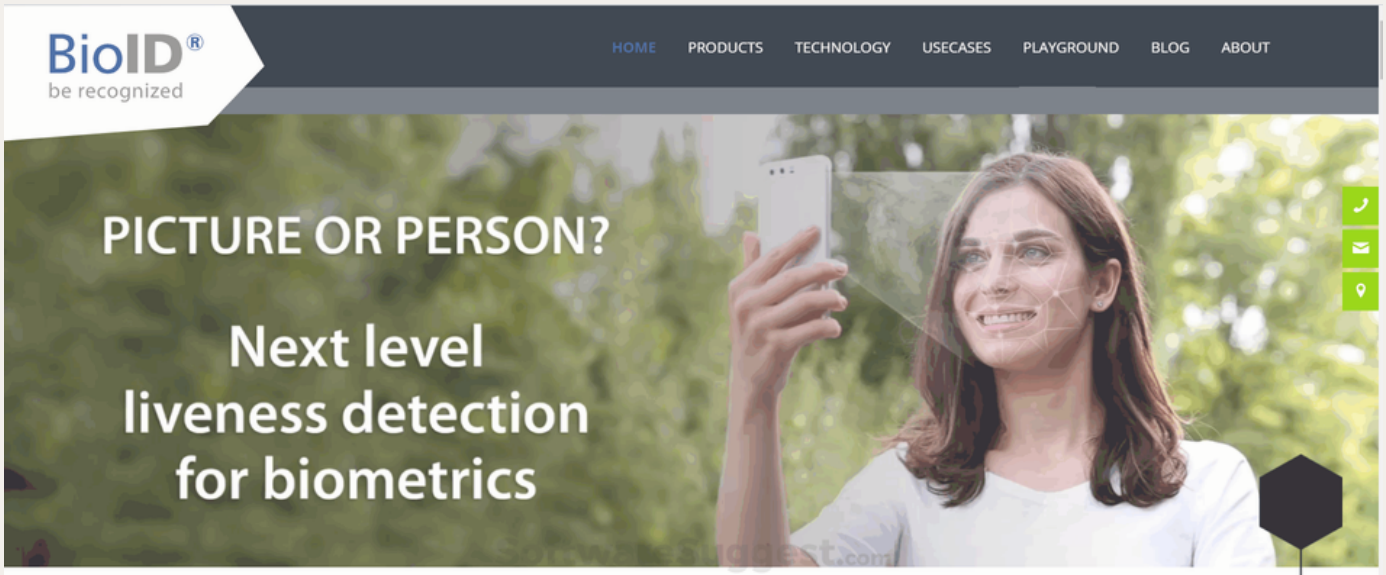
- **More Work Upfront:** Using Betaface requires more development effort than cloud solutions. You'll need to manage your own infrastructure and update the software yourself.
- **Scaling Issues:** Adding more users to Betaface can be trickier than cloud-based options. You might need to buy more hardware to handle it.
- **Security Burden:** The security of your facial data and the Betaface system is entirely your responsibility. You'll need strong cybersecurity practices to avoid breaches.
- **Tech Skills Needed:** Running Betaface might require in-house experts on facial recognition technology and system administration, which some companies might not have.

BioID

Core Concept:

BioID is a GDPR-compliant solution that provides biometrics-as-a-service. It provides cloud-based FRS services that can be accessed by your product using APIs. The software offers three products:

- **BioID web service:** This is a SaaS offering that can be deployed on-premise or on the cloud.
- **Liveness detection:** This is a recognition service to detect user presence using face, eye, and voice recognition. It is used to prevent online fraud and identity threats.
- **PhotoVerify:** This solution combines face detection technology with BioID's Liveness Detection service to verify photos used as identity proofs.



BioID

Advantages

- **Multi-Factor Authentication:** BioID offers solutions that can combine facial recognition with other biometric modalities like fingerprint scanning or iris recognition. This multi-factor approach enhances security by requiring users to present more than one credential for authentication.
- **Focus on Usability:** BioID emphasizes user experience and ease of use in their facial recognition products. Their solutions aim to be user-friendly and provide a smooth authentication experience.
- **Potential Customization:** While information about the extent of customization is limited, BioID might offer some level of customization compared to completely pre-built cloud solutions. This could involve tailoring the user interface or specific authentication workflows.

Disadvantages

- **Hard to Research:** BioID's website doesn't offer as much detail on their products as some cloud-based solutions, making it difficult to learn about their accuracy, security, and technical features.
- **Potential Lock-In:** Switching from BioID to another facial recognition company might be tricky depending on how their system is integrated.
- **Hidden Costs:** It's hard to find information about BioID's pricing, so it can be tough to compare them to other options in terms of cost.
- **Limited Use Cases:** BioID's facial recognition might be designed for specific industries or purposes, so it might not work for everything like some cloud-based solutions.

Cognitec

Core Concept:

Cognitec provides scalable and customizable FRS to customers through its open system architecture through 'FaceVacs.' Cognitec offers five solutions:

- **FaceVACS-VideoScan ES Live:** Recognizes faces in real-time video streams. BioID expands on this by offering additional features like people counting, demographic analysis, and flow tracking.
- **FaceVACS-VideoScan ES:** A subscription service for enterprises. Cognitec handles installation, management, hardware selection (cameras and computers), and deployment (on-premise or cloud) through a partner.
- **FaceVACS-DBScan ID:** Designed for biometric verification and identification. Likely compares faces in images/videos against a known individual database.
- **FaceVACS-DBScan LE:** Caters to law enforcement, likely for criminal identification purposes through biometric verification.
- **FaceVACS-Entry:** Integrates FRS software with high-end hardware to create electronic gates for access control at border checkpoints or security areas.

Cognitec

Advantages

- **Strong Accuracy:** Cognitec is known for its high-performing facial recognition technology, leading to reliable user authentication.
- **Flexible Deployment:** Choose between cloud-based solutions (easy to use and scale) or on-premise options (for stricter data privacy control).
- **Scales with You:** Regardless of deployment, Cognitec's solutions can handle growing numbers of users without a hitch.
- **More Customization:** Compared to some cloud offerings, Cognitec allows for more customization to fit your application's needs.

Disadvantages

- **Potentially Higher Costs:** On-premise Cognitec solutions might require a larger upfront investment compared to cloud subscriptions. Cloud options might also offer pay-as-you-go plans, which can be cheaper for smaller user bases.
- **More Development Work (On-Premise):** Setting up an on-premise Cognitec system requires more development effort than using a cloud-based API. You'll need to manage your own infrastructure and update the software yourself.
- **Security Burden (On-Premise):** If you choose an on-premise solution, your company is entirely responsible for securing the facial data and the Cognitec system. This means having strong cybersecurity practices to avoid breaches.

Face++

Core Concept:

Face++ provides four types of technology solutions:

- Facial recognition for face detection, face comparison, and face search.
- Human body recognition for body detection, skeleton detection, and body outline.
- Image beautify for merging faces in multiple photographs.
- Image detection – for tagging faces on photographs.

Face++

Advantages

- **Lots of Features:** Face++ offers more than just face recognition. It can guess age and gender, find key points on faces, and even tell if it's a real person!
- **Can be Customized:** You can adjust how strict Face++ is at recognizing faces and even add other features to fit your app.
- **Easy for Developers:** Face++ offers tools (APIs and SDKs) to make it simple to add facial recognition to your app.
- **Might be Cost-Effective:** Depending on your needs, Face++ could be a good value because it offers so many features.

Disadvantages

- **Hard to Research:** Face++ might not provide as much detail on how their facial recognition works compared to bigger companies. This makes it difficult to know how accurate and reliable it is.
- **Switching Can Be Tough:** Once you start using Face++, it might be difficult to switch to another facial recognition company later on.
- **Limited Outside Asia:** Face++ might be focused on Asian markets, so customer support or information might be harder to find if you're not in Asia.
- **Check Security Measures:** Make sure you understand how Face++ protects user data, such as how they encrypt and store information.

Sense Time

Core Concept:

SenseTime provides face and body analyzing technology, besides its stand-alone FRS services. Its solutions boast high accuracy. It provides services like:

- **Face detection.**
- **Facial feature point positioning:** Feature positioning is marked irrespective of wide-angles, changing expressions, or movement.
- **Facial attributes:** The solution can accurately recognize more than ten facial attributes.
- **Liveness detection**: User verification solution to prevent spoofing attacks.

Sense Time

Advantages

- **Cutting-Edge Tech:** SenseTime uses advanced deep learning algorithms for high-accuracy facial recognition, leading to secure user authentication.
- **Flexible Options:** Choose between on-premise or cloud-based solutions from SenseTime to fit your security, privacy, and customization needs.
- **Global Reach:** SenseTime operates worldwide, providing support and expertise no matter your location.
- **Integrations Possible:** SenseTime's facial recognition can integrate with other security systems for a more well-rounded security approach.

Disadvantages

- **Privacy Concerns:** SenseTime has been criticized for potential privacy issues. Make sure they handle data carefully and follow data privacy laws before using them.
- **Hard to Understand:** There might not be enough information available about how SenseTime's technology works, how secure it is, or how users control their data. This makes it difficult to know what you're getting.
- **Potential Restrictions:** Depending on your location and political situation, using SenseTime might be restricted or require extra checks. Consider this before you choose them.
- **Limited Reviews:** There might not be many independent reviews of SenseTime's technology, making it hard to know how well it actually works.

Core Concept:

Trueface.ai provides FRS solutions in three modes — with an SDK, a deployable container, and a plug-and-play (beta) software solution. The software offers four primary services:

- Facial recognition
- Weapon detection
- Space analytics
- Live verification to prevent spoofing attempts

trueface | PANGIAM

Advantages

- **Security Focus:** Trueface.ai prioritizes robust security features, potentially offering strong data protection and access control measures for user data and the facial recognition system itself.
- **Customization Potential:** Similar to BioID, Trueface.ai might allow some level of customization for developers. This could involve tailoring the way users authenticate themselves (authentication workflows) or how the facial recognition system appears to users (user interfaces).
- **Easy Integration :** Trueface.ai likely provides APIs and SDKs, making it easier for developers to add facial recognition features to their web applications.

Disadvantages

- **limited Transparency:** Limited information on algorithms, accuracy, security, and data privacy compliance makes it hard to assess their solution.
- **Potential Vendor Lock-In:** Using Trueface.ai's APIs or SDKs could make switching to another provider difficult.
- **Hidden Costs:** Unclear pricing structure makes it difficult to compare costs with other options.
- **Uncertain Scalability:** Unclear how Trueface.ai scales to handle more users.

Microsoft Azure FaceAPI

Core Concept:

Microsoft Azure Face API is a cloud-based facial recognition tool that offers core functionalities like:

- **Face Detection:** Locates human faces within images or video streams. This forms the foundation for further facial analysis.
- **Face Recognition:** Identifies and verifies individuals based on their facial features. It can be used for tasks like user authentication or security purposes.
- **Facial Attribute Analysis:** Analyzes various facial attributes beyond just identity. This can include age estimation, gender recognition, emotion detection, and even hair and facial hair analysis.

Detection result:
JSON:
[
  {
    "faceId": "d4202a3d-cc61-4856-b897-6c7fe3568aa9",
    "faceRectangle": {
      "top": 128,
      "left": 459,
      "width": 224,
      "height": 224
    },
    "faceAttributes": {
      "hair": {
        "bald": 0.1,
        "invisible": false,
        "hairColor": [
          {
            "color": "brown",
            "confidence": 0.99
          },
          {
            "color": "black",
            "confidence": 0.57
          },
          {
            "color": "red",
            "confidence": 0.36

Microsoft Azure FaceAPI

Advantages

- **Cloud-Based Scalability and Reliability:** Azure's infrastructure ensures your facial recognition solution can handle a large user base and data volume efficiently.
- **Easy Integration:** Pre-built APIs (RESTful) and SDKs streamline integration into your applications, saving development time and speeding up your time-to-market.
- **Advanced Features:** Azure Face API goes beyond basic face detection and recognition. It offers functionalities like emotion recognition and facial landmark detection, enabling richer user experiences.

Disadvantages

- **Cost for Large Deployments:** For large-scale deployments, the cost of using Azure Face API might be a significant factor to consider.
- **Cloud Dependence:** The solution relies on Microsoft Azure's cloud infrastructure for processing facial data. This introduces some dependence on network connectivity and Microsoft's service availability.
- **Limited Control:** As a cloud-based solution, you have limited control over the underlying algorithms and models used for facial recognition.

KAIROS

Core Concept:

Kairos is a facial recognition platform offering APIs and SDKs for developers to integrate facial authentication into web and mobile applications.

- **Age Verification:** Kairos uses facial recognition to estimate a user's age. This can be useful for age-restricted applications or websites.
- **Emotion Recognition:** Kairos can analyze facial features to infer a person's emotions in images or videos.
- **Facial Feature Tracking:** It can track specific facial features like eye distance, nose shape, and hairstyle, potentially useful for identification or analysis.
- **Focus on Biometrics:** Kairos emphasizes using biometric measurements from facial features for various recognition and analysis tasks.

KAIROS

Advantages

- **Flexible Deployment:** Choose cloud-based for ease of use or on-premise for stricter data control.
- **Feature-Packed:** Goes beyond recognition with features like gauging emotions and age.
- **Customizable:** Tailor Kairos to your needs, like adjusting accuracy requirements or integrating with other systems.

Disadvantages

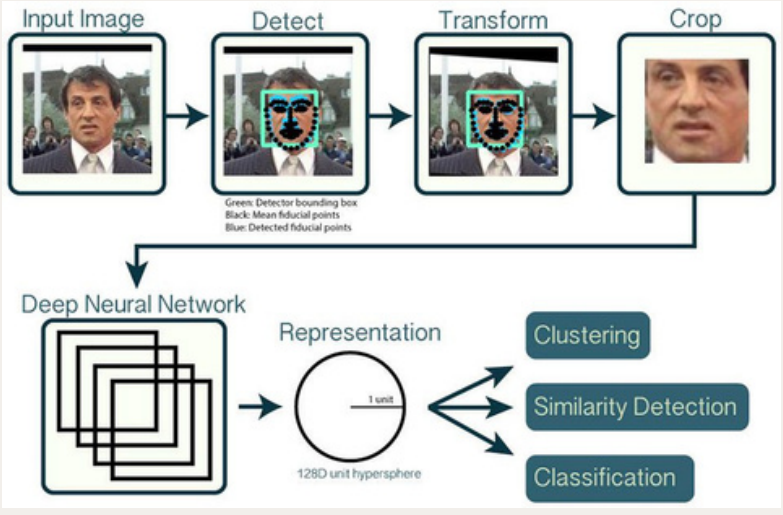
- **Potentially Higher Cost:** Compared to other facial recognition solutions, Kairos might have a higher price tag. It's important to weigh the cost against the features and flexibility it offers.
- **Less Transparency:** Limited info on data privacy, security, and user controls. Makes it hard to know how secure your data is.
- **Locked In:** Using Kairos might make it difficult to switch to another company later.
- **Fairness:** Facial recognition can be biased, meaning it might not work equally well for everyone. Be sure to check how accurate Kairos is for different demographics.
- **Privacy & Ethics:** Facial recognition raises privacy concerns and ethical questions. Consider if the benefits outweigh the risks before using it.

OpenCV

Core Concept:

OpenCV (Open Source Computer Vision Library) stands out as a powerful and free library brimming with computer vision functionalities. Within this extensive toolkit lies the potential for facial recognition, empowering developers to build custom FAS solutions. OpenCV provides a range of algorithms and tools specifically designed for this purpose.

One of OpenCV's key strengths is its platform independence. Unlike some solutions locked to specific operating systems, OpenCV seamlessly functions across Windows, Linux, macOS, iOS, and Android. This versatility empowers developers to create facial authentication systems that can be deployed on a wide array of devices and platforms.



Advantages

- **Cost-Effectiveness:** Being free to use and modify eliminates licensing fees, making it a budget-friendly option for developers.
- **Customization Prowess:** OpenCV offers a high degree of customization. Developers can tailor facial recognition algorithms and models to their specific needs and application requirements. This level of control allows for fine-tuning authentication processes and achieving optimal results.
- **Transparency and Control:** Open-source code fosters transparency. Developers have full access to the underlying algorithms, enabling them to understand how facial recognition occurs within their system. This control empowers them to implement additional security measures and address privacy concerns.

Disadvantages

- **Complexity for Beginners:** The extensive feature set and vast documentation can be daunting for new users or those unfamiliar with computer vision concepts. A significant learning curve exists before effectively utilizing OpenCV for facial recognition.
- **Development Intensive:** Building a full-fledged FAS with OpenCV requires considerable development effort. Integration with existing systems, customization of algorithms, and user interface design all contribute to the development time needed.
- **Missing Out-of-the-Box Features:** Unlike cloud-based solutions offering pre-built functionalities, OpenCV necessitates development from scratch. Features like user management, secure storage of facial templates, and real-time processing might need to be implemented by developers.