WHITE PAPER

SAFR®

from realnetworks

ACCESS CONTROL USING FACIAL AUTHENTICATION

OCTOBER 2023

White Paper: Frictionless Access Control Using Facial Authentication

ABSTRACT

Access control systems are critical for ensuring security in various environments, from corporate offices to healthcare facilities and residential complexes. Traditional methods often involve keycards, PINs, or physical keys, which can be lost, stolen, or shared. This white paper explores the concept of frictionless touchless access control using facial authentication, highlighting its security advantages over traditional methods. We will delve into the technology behind facial authentication, its implementation, privacy and security implications and the key benefits it offers to organizations.

Contents

INTRODUCTION

Access control systems play a vital role in safeguarding physical and digital assets. The emergence of facial authentication technology has introduced a new dimension to access control by providing a highly secure and convenient method for granting access. This paper examines why facial authentication is a superior solution to traditional methods and how it can enhance security while reducing operational overhead.

The Technology Behind Facial Authentication

1. Facial Recognition Algorithms

Facial authentication relies on sophisticated facial recognition algorithms. These algorithms analyze the unique characteristics of an individual's face, such as the distance between the eyes, the shape of the nose, and the contours of the cheeks. Dependable accuracy and performance are central to any viable recognition solution. Latency, false positives, and questionable results render a system unusable. The algorithms powering the SAFR platform were tested by NIST and contrasted with over one hundred other algorithms submitted by companies and institutions from around the world. SAFR achieved an enviable level of accuracy and performance that squarely established its position in a best-in-class category for live video applications.

2. Anti-spoofing Detection

To enhance security, modern facial authentication systems employ anti-spoofing detection techniques (a.k.a. presentation attack detection or PAD) to ensure that the presented face is a live and not a static image or video. The SAFR SCAN solution employs two different anti-spoofing technologies to ensure maximum security. The first method is a 3D depth sensing technology using a structured light projector while the second method uses an internally developed set of algorithms that analyze the 2D images for texture and context. When used together, these two technologies provide the best anti-spoofing technology available.

3. Deep Learning and Neural Networks

Deep learning models, especially Convolutional Neural Networks (CNNs), have significantly improved the accuracy and reliability of facial authentication. These models can identify facial features even in challenging conditions, such as low light or partial face obstructions.

How Facial Authentication Works

1. **Enrollment**: Users' facial biometric data is captured and stored securely in a database or on the user's mobile device during the initial setup. While most solutions typically involve taking multiple images from different angles, SAFR SCAN requires a simple 2D image taken from the SAFR SCAN device, from a mobile device or from an existing database of images.
2. **Authentication**: When a user attempts to gain access, the system captures their live facial image. It then compares the live image with the stored biometric data (stored onboard the device or on the users mobile device), performing anti-spoofing detection to ensure the face is real.
3. **Access Granting**: If the authentication process is successful, the access control system grants access, either by unlocking a door, turnstile, or granting digital access to systems.

Advantages Over Traditional Methods

Facial authentication offers several distinct advantages over traditional access control methods:

1. Strong Biometric Authentication

Facial recognition is based on biometric data that is unique to each individual. This reduces the risk of unauthorized access due to lost, stolen, or shared keycards or PINs.

2. User Convenience

Users appreciate the convenience of a touchless system. There is no need to carry access cards or remember PINs, making the process both efficient and user-friendly.

3. Anti-spoofing Detection

Modern facial authentication systems incorporate anti-spoofing detection, mitigating the risk of spoofing through static images. This significantly enhances security.

4. Non-Contact

Especially in the context of post-pandemic considerations, facial authentication minimizes physical contact with surfaces, reducing the spread of germs and ensuring a hygienic environment.

5. Scalability

Facial authentication is highly scalable. Adding or revoking user access is a straightforward process that doesn't require physical card management or reconfiguration.

6. Audit Trails

Facial authentication systems often include robust logging and audit trail capabilities, allowing organizations to monitor access events and respond to security incidents effectively.

7. Tailgating Detection

Many biometric solutions can address security concerns with traditional methods, however only video at the door can solve the problem of tailgating. Once a user has been granted access and opens the door, most systems cannot provide insight into what happens next. SAFR SCAN can track tailgating, sending an alert and recording the video of the event.

Data Privacy

Personal Identifiable Information (PII) are unique identifiers — any information that can be used to identify, contact, or locate a specific person. For access control systems, this typically includes facial image, name, and access credentials. For facial authentication, biometric data is also required.

SAFR has been designed with privacy in mind and gives users full control over how PII is stored and retained. Principals of data minimization should be applied to limit the distribution of sensitive information. Because images are not an essential part of biometric face matching, they are not stored on the device. Security can be improved by persisting sensitive PII data only in volatile memory to ensure data can't leave a facility. Users can be given control over their PII data by storing all PII data, including biometric signature, on their mobile device, granting access to that data only when in the user is in physical proximity. In this way PII is never out of control by the owner.

Data Security

Information Security is a mission-critical function for systems handling PII data and responsible for granting access to the organization's physical infrastructure. A facial authentication-based access control system must be designed, built, maintained, monitored, and regularly updated with security in mind to protect the sensitive data it manages and prevent unauthorized use of the system.

The SAFR platform puts the operator in charge of data and maintains it securely from end to end. The operator controls what is persisted, where it is distributed and how long it is retained. SAFR uses a multi-layer encryption architecture to protect data at rest and over the wire. Data-at-rest is protected with 256-bit AES encryption with exclusive keys per device. Data-in-transit is protected with TLSv1.2 + TLS1.3 encryption algorithms.

User Roles and Permissions control makes it possible to restrict access to data to only those personnel that are authorized.   Permissions allow independent read/write control over the data and roles enable grouping of individuals given access to the system to ensure consistency in access granted to the data.

Architecture

Access control systems must support a wide range of deployment architectures. The system must be able to operate over disparate networks without adding management overhead or duplicate system management across multiple sites. Seamless integration must be offered between different elements that make up the entire access control system.

SAFR offers the ability to easily integrate into existing access control systems and share data across wide area networks (WANs) in a simple efficient manner. Because of SAFR's unique ability to use 2D images for enrollment, persons and credentials can be seamlessly synchronized from most popular access control systems as a background automated service. And multiple SAFR subsystems can be easily connected across WANs to synchronize person records and event data.

SAFR's support of industry standards allows it to interface in a tightly coupled manner to physical access control hardware through standard Wiegand or OSDP protocols. Integration goes beyond simply sending credentials. SAFR interfaces with access control panels to determine access granted or denied disposition, support door state as well as display panel feedback to credential holders.

Use Cases and Implementation

Facial authentication using access control systems can be implemented in various environments, including:

- Corporate offices
- Healthcare facilities
- Educational institutions
- Residential complexes
- Government buildings
- Data centers
- Critical Infrastructure
- Airports and transportation hubs

Implementing facial authentication typically involves:

1. Selecting appropriate hardware (SAFR SCAN).
2. Integrating the hardware with software that manages the authentication process. SAFR SCAN currently integrates with many leading access control software solutions and continues to create more integrations.
3. Enrolling authorized users and their facial biometric data.
4. Configuring access policies and permissions.
5. Monitoring and managing access events.

Conclusion

Facial authentication is emerging as a secure and convenient alternative to traditional access control methods. Its strong biometric authentication, anti-spoofing detection, and non-contact nature make it a superior choice for organizations looking to enhance their security while streamlining access management. As technology continues to advance, facial authentication is expected to play an increasingly critical role in access control and security management.