Understanding Biometrics and their uses

Guidance for end-users

THE VOICE OF THE **PROFESSIONAL SECURITY INDUSTRY**

bsia
british security industry association

Contents

1. Evaluating Biometric Technologies

As biometric technologies become increasingly integral to our security infrastructure, the need for comprehensive guidance for end users is more pressing than ever. Such a guide demystifies the complexity of biometric systems, highlighting the necessity for universal interoperability standards and robust privacy measures to protect irreplaceable personal data. It also sheds light on technology's performance under diverse conditions, underscores the imperative of inclusivity in system design, and advocates for more robust security through multi-factor and multi-modal authentication. Additionally, a well-crafted guide can help build public trust, illuminating how biometric data is managed and safeguarding against misconceptions. This supportive approach ensures users are informed, comfortable, and confident as they interact with these advanced identification technologies.

Biometrics technologies require evaluating the current state of the technology, its applications, and potential future developments against the desired state or potential needs. Here are some preliminary observations:

1.1. Interoperability

Biometric systems from different manufacturers often lack standardisation, which leads to interoperability issues. For instance, a fingerprint recognition system from one manufacturer may not be compatible with one from another manufacturer. As biometrics are increasingly adopted, the need for global standards becomes apparent. Standards allow different systems to 'communicate', improving functionality and efficiency and enhancing security by allowing information sharing and verification across systems.

1.2. Privacy and Security

The increasing use of biometrics presents privacy and security challenges. Biometric data, by its nature, is deeply personal and cannot be changed like a password if compromised. Breaches involving biometric data can have severe long-term consequences. Therefore, there is a gap in establishing stringent security measures to safeguard this sensitive data, from the point of capture, during transmission, to storage. Techniques such as data anonymisation, encryption, and using secure channels for data transmission need to be standardised and widely adopted.

1.3. Performance in Varying Conditions

Many biometric technologies are affected by environmental conditions. For instance, face recognition systems may struggle in low-light conditions, while voice recognition may be ineffective in noisy environments. While considerable strides have been made, more research and development are required to make these systems more adaptable and resilient to varying conditions. This would involve improving the underlying algorithms and potentially incorporating supplementary technologies.

1.4. Inclusion and Accessibility

Biometric systems should be designed to be usable by the widest possible range of users. However, they can fall short. For example, people with certain skin conditions may have difficulty using fingerprint scanners, while individuals with certain disabilities may not be able to use iris scanners. To ensure fairness the industry needs to focus on developing and implementing more inclusive biometric systems that consider the wider demographic of human characteristics.

1.5. Multi-factor and Multi-modal Biometrics

Despite the inherent security of biometrics, single-factor or single-modal systems can be vulnerable. Multi-factor authentication (using biometrics along with a password or an RFID card) and multi-modal biometrics (using multiple types of biometric identification) offer higher security levels. Industry advancements are underway to expand the prevalence of high-security, user-friendly systems incorporating multi-factor and multimodal biometric authentication, signalling a commitment to making these enhanced security measures more accessible to users.

1.6. Public Perception and Trust

Despite the prevalence of biometrics, there is a general lack of understanding and trust among the public regarding these technologies. Many people are unaware of how their biometric data is used, stored, and protected, leading to hesitation and resistance to adopting such systems. This gap can be addressed through educational initiatives, increased transparency from biometric solution providers, and more stringent regulations governing the use of biometrics.

In summary, while biometrics have transformed security and identification methods, transparency is key to providing trust in the use of biometric systems to ensure their security, privacy, effectiveness, accessibility, and public acceptance.

2. Biometrics Interfaces List & Example of Multifactor Authentication

2.1. Fingerprint Recognition

This is the most common biometric interface for unlocking smartphones to access control in secure facilities. Every individual has unique fingerprint patterns, and these systems identify users based on the minutiae points on their fingerprints. This method is generally secure, affordable, and user-friendly.

2.2. Face Recognition

This technology uses the unique features of a person's face to identify them. Applications range from unlocking smartphones to surveillance systems and personalised advertising. AI algorithms measure facial features and their relative positions to create a unique facial signature. Despite occasional issues with lighting and angles, it remains widely used.

2.3. Iris Recognition

Iris recognition uses unique patterns in an individual's iris for identification. It's considered highly reliable due to the uniqueness and stability of iris patterns over time. It's used in high-security areas like airports and border control, but its high cost and required user cooperation limits its wider adoption.

2.4. Voice Recognition

This technology analyses vocal behaviour by identifying unique speech patterns and other vocal characteristics. It's used in virtual assistants like Siri, Google Assistant, and Alexa and also for authentication in customer service. The ease of use makes it popular, though background noise can sometimes pose challenges.

2.5. Retina Scan

Retinal scanning is a highly accurate biometric technology that maps the unique patterns of a person's retina blood vessels. Due to the invasive nature of the scan (a light source has to be directed into the eye); it's only used in specific high-security applications.

2.6. Palm Recognition

Involves scanning the hand's vein patterns, lines, and structures. It is becoming more widely used in secure access systems and payment applications due to its non-contact nature and high accuracy.

2.7. Behavioural Biometrics

This technology measures unique patterns in how individuals interact with systems, such as typing rhythm, mouse movements, or touchscreen gestures. It's often used in cybersecurity to detect fraudulent behaviour, providing a layer of security that's difficult to circumvent a biometric system through the use of a fake biometric sample i.e., to spoof can involve presenting a false match to the biometric sensor with the intention of masquerading as a legitimate user.

2.8. Hand Geometry Recognition

A more traditional biometric system, it analyses and measures the shape of the user's hand. While it's less accurate than other biometrics like iris or fingerprint, it's robust and easy to use, making it popular in industrial settings.

2.9. Vein Pattern Recognition

This technology uses unique vein patterns in a person's finger or palm for identification. It's a secure method as the veins are internal to the body, and the pattern is difficult to replicate.

2.10. DNA Matching

DNA testing is the most accurate biometric technique in forensics and genealogy research. It involves comparing DNA sequences to determine genetic relationships or to identify individuals uniquely.

3. Existing Biometric Interfaces

3.1. Video Surveillance and Security Systems

3.1.1. Face Recognition

Utilized in surveillance systems for identifying individuals in real time. Also used in security cameras for homes and businesses to alert owners about unrecognised faces.

3.1.2. Behavioural Biometrics

Used in surveillance to identify suspicious behaviours. This can include unusual walking patterns or abnormal interactions with computer systems.

3.2. Physical Access Control

3.2.1. Fingerprint Recognition

Often used in secure access systems for buildings and rooms. Its advantage lies in its ease of use and difficulty in faking a fingerprint.

3.2.2. Iris Recognition

Used in high-security areas due to its high accuracy and difficulty in faking. It can be used in everything from data centres to government buildings.

3.2.3. Retina Scan

Utilized in very high-security scenarios due to its accuracy. Its use is limited due to the invasive nature of the scan.

3.2.4. Palm Recognition

Used in certain secure access systems due to their non-contact nature, which can benefit clean environments or during pandemics.

3.2.5. Hand Geometry Recognition

Used for access control in industrial settings due to its simplicity and robustness.

3.2.6. Vein Pattern Recognition

Employed in specialised secure access control systems. The pattern of veins is difficult to replicate, adding a layer of security.

3.3. Digital Access Control and Cybersecurity

3.3.1. Voice Recognition

Used in some online systems for user verification. It can be a good secondary verification method to improve the security of online accounts.

3.3.2. DNA Matching

While not typically used for access control, it can be a future-proof method for high-security applications.

3.4. Upcoming and Speculative Biometric Interfaces

3.4.1. Ear Recognition

Still largely in research, it can be used in surveillance systems due to its passive and non-contact nature.

3.4.2. Gait Recognition with AI

Being developed for surveillance and security, individuals can be identified from a distance based on their walk.

3.5. Physical Access Control

3.5.1. Heartbeat Recognition

While in early development, the unique nature of each individual's heartbeat could offer a new method for secure access control.

3.5.2. Infrared Vein Recognition

An advancement of vein recognition that could improve the accuracy and reliability of this method for physical access control.

3.5.3. Facial recognition

Is utilised for contactless access control in physical spaces, enhancing security by comparing real-time facial features with stored data.

3.6. Digital Access Control and Cybersecurity

3.6.1. 3D Face Recognition

This could improve the robustness and accuracy of face recognition systems for online platforms, adding a layer of security for user accounts.

3.6.2. Continuous Authentication

Systems that continuously verify a user's identity based on various behavioural biometrics can significantly enhance cybersecurity.

3.6.3. Biometric Blockchain Systems

These systems could provide a secure method of storing and managing biometric data for access control and identity verification in digital platforms.

3.7. Multifactor Authentication example

3.7.1. Multi-Factor Authentication using card entry and biometrics together

RFID cards, while not biometric, are often used alongside biometrics for enhanced security in multi-factor authentication systems, requiring both a user-held component (RFID card) and a unique biological identifier (biometric data).

4. Data Protection and Biometrics

Biometric technologies in compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 is paramount. Biometric data is considered a special category under these regulations, requiring enhanced safeguards due to its highly personal nature. To align with these legal frameworks, organizations must secure explicit consent from individuals before processing biometric data, employ data minimization strategies, and establish robust security protocols to prevent data breaches.

The Data Protection Act complements the EU General Data Protection Regulation (GDPR) within the UK, adding specific provisions and clarifications, especially in areas of national security and law enforcement. Organisations must perform thorough impact assessments to identify and mitigate risks associated with biometric data processing. Data subjects are afforded substantial rights, including access to their data, the ability to correct inaccuracies, and the right to erasure.

Crucially, transparency is essential. Entities must communicate their biometric data processing activities, purpose, and the protective measures employed. They are also required to illustrate their compliance with the GDPR and the Data Protection Act, justifying the use of biometric technologies while safeguarding individual privacy. In essence, as biometric identification becomes more commonplace, the imperative for strict adherence to data protection laws intensifies, demanding that organisations balance technological innovation with the legal and ethical considerations of data privacy.

This document was created by the FRT/AI Special Interest group of the British Security Industry Association (BSIA).

The British Security Industry Association is the trade association for the private security industry in the UK. Our members provide over 70% of UK security products and services and adhere to strict quality standards.

BSIA membership will raise your company profile and ensure that your business is at the heart of influencing the future of the security industry. You will become part of a unique group of high quality and professional companies which are well-respected and well-represented to government, end users, specifiers, standards, and legislative bodies. For more information contact the BSIA.

About **the BSIA**

The British Security Industry Association (BSIA) is the trade association representing over 70% of the UK's private security industry. Its membership includes companies specialising in all sectors of security. For security buyers, BSIA membership is an assurance of quality, with all member companies required to adhere to strict quality standards.