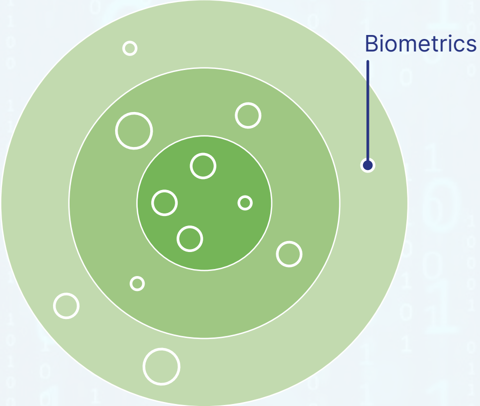
Biometrics

Digital-Technology-Radar.net

	low	medium	high
Impact	🟩	▭	▭
Complexity	●	○	○

1 INTRODUCTION



Purpose

Biometrics refers to the technology and methods used to identify individuals based on unique physiological or behavioural characteristics. This includes fingerprint recognition, facial recognition, iris scanning and voice recognition. Biometrics enhance security and convenience in authentication.

Key benefits

Biometrics provide a high level of security by leveraging unique individual traits, reducing the need for passwords or PINs. They offer convenience through seamless authentication and improve accuracy in identity verification. At the same time, biometrics can provide personalised experiences and faster/easier access to infrastructure/ICT.

2 KEY CONCEPTS

Fundamental principles

Fingerprint recognition involves identifying individuals by examining the distinct patterns of ridges and valleys in their fingerprints. Similarly, facial recognition uses the unique features and patterns of a person's face to verify their identity. Iris recognition is analysing the intricate patterns found in the iris of the eye to establish a person's identity. Additionally, voice recognition identifies individuals based on the unique characteristics of their voice, including pitch, tone and speech patterns.

Terminology

A biometric template is a digital representation of an individual's biometric data, which is used for comparison and identification within biometric systems. The False Acceptance Rate (FAR) refers to the likelihood that a biometric system will mistakenly match an individual with someone else. Conversely, the False Rejection Rate (FRR) is the probability that the system will fail to recognise a person. To enhance security, Multi-Factor Authentication (MFA) combines multiple authentication methods, including biometrics, to provide a more robust verification process.

3 POPULAR TECHNOLOGIES AND FRAMEWORKS

Regulatory principles of biometrics

1 **Data Privacy Laws:** biometric data is considered highly sensitive. Privacy regulations, such as the GDPR in Europe or the CCPA in California, govern how such data should be collected, stored and used to protect individual privacy.

2 Biometric Legislation: some countries have specific laws regulating the use of biometric technologies. These laws aim to prevent misuse and protect the rights of individuals.

Security principles

1 Biometric Data Security: biometric systems must ensure that the data stored is not manipulated or altered.

2 Data Confidentiality: biometric data must be protected to ensure it is only accessible by authorised individuals or systems.

3 System Availability: the systems must be reliable to ensure that authorised users can always access their data without being hindered by technical issues.

Ethical considerations

1 Informed Consent: the collection and use of biometric data must be based on informed consent. Individuals should be clearly informed about how their data will be used.

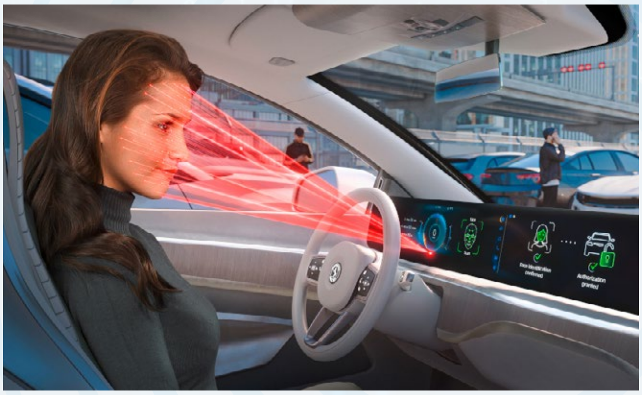
2 Transparency in Data Handling: organisations must disclose how biometric data is collected, stored and used to build trust and avoid misunderstandings.

3 Avoidance of Discrimination: biometric systems should be designed to avoid discriminatory outcomes and ensure fairness to all users.

Comparison

- **Fingerprint Recognition vs Facial Recognition:** fingerprint recognition is highly accurate and reliable but requires physical contact. Facial recognition is contactless and convenient but may be affected by changes in appearance or lighting conditions.
- **Iris Recognition vs Voice Recognition:** iris recognition offers high accuracy and resistance to spoofing but requires specialized equipment. Voice recognition is less intrusive but less secure.

Driver Identification Display



Source: www.continental.com

4 APPLICATIONS

Industry use cases

- **Healthcare:** Patient Identity Verification ensures accurate patient records.
  > Best Practice: Imprivata PatientSecure.
- **Law Enforcement:** Criminal Identification with biometric data.
  > Best Practice: FBI's NGI System.
- **Retail:** enhance customer experience for automated checkouts.
  > Best Practice: Amazon Go.

Practical examples:

- CLEAR: a service that uses biometric technology to expedite airport security screening in the USA.
- Banking and Payments: Mastercard Identity Check uses fingerprint and facial recognition for secure online payments.
- Smart Home Security: Google Nest Hello doorbell uses facial recognition to identify and notify homeowners of familiar faces approaching their door.

5 IMPLEMENTATION INSIGHTS

Best practices and tips

- **Integration:** ensure that biometric systems are compatible with existing security infrastructure.
- **Privacy:** implement robust data protection measures to safeguard biometric data from unauthorised access.
- **Ethical use:** use biometric data responsibly and transparently, with clear policies on how it is used.

Common challenges

- **Accuracy:** addressing issues related to false acceptance and false rejection rates to improve system reliability.
- **User acceptance:** overcoming resistance to biometric systems due to privacy concerns or perceived intrusiveness.
- **Inclusivity:** addressing issues where biometric systems may not work equally well for all individuals, such as those with certain physical characteristics.

6 KEY TRENDS AND PREDICTIONS

Top milestones in Biometrics

- **1999:** introduction of the first commercial fingerprint recognition systems.
- **2003:** deployment of facial recognition technology in public security and surveillance.
- **2013:** Apple's introduction of Touch ID, bringing fingerprint recognition to consumer smartphones.

Current trends

- Biometric Payments: growing adoption of biometric authentication for secure and convenient financial transactions.
- Multi-Modal Biometric Systems: integration of multiple biometric methods to enhance accuracy and security.
- Contactless Biometrics: utilising technologies that do not require physical contact due to health concerns.

Future predictions

- **Advanced Biometric Fusion:** combining multiple biometric modalities for increased security.
- **Biometrics in IoT:** expanding use of biometric authentication in Internet of Things (IoT) devices.
- **Widespread Adoption:** in everyday devices, such as smartphones, banking and public safety.

7 KEY RESOURCES AND MOST HELPFUL LINKS

Websites and blogs

- Biometric Update: news and analysis on biometric technology developments.
- IBIA.ORG: International Biometrics Association is representing the identification technology industry.

Online courses

- Coursera: provides access to biometric courses from University of Toronto.
- Biometrics Institute: free introduction course.
- Scholars International Institute Of Technology: offers biometrics knowledge.

Communities and forums

- FindBiomectrics: provides news on developments in the biometrics field.
- Reddit: r/Biometrics: community for sharing news and discussing biometric technology advancements.
- GitHub: repositories for biometric technology projects and research.

8 GLOSSARY

Common terms and definitions

- Biometric Encryption: the process of converting biometric data into an encrypted code.
- Liveness Detection: a technique used to ensure that the biometric sample is from a live person, not a fake representation.
- Enrollment: the process of capturing an individual's biometric data and storing it in a database.

Authors

Dr Torsten Wingenter
Torsten established Digital Innovations at Lufthansa, founded the FlyingLab, and was responsible for the digital strategies of Austrian, Lufthansa and Swiss airlines. Today, as the "Inno Doc", he is digital advisor, coach and catalyst, interim manager and fire fighter for many organisations in their pursuit for digital innovations.
www.inno-doc.com

Prof Marc K Peter
Marc was an executive at eBay, E*TRADE (ANZ) and LexisNexis. Today, he is the "Digital Prof" at Rochester-Bern Executive Programs, the University of Rochester, at FHNW and at CSU in Australia. His research and teaching covers digital transformation, digital technology, digital leadership, cybersecurity and digital marketing.
www.digitalprof.com

n|w Business

Rochester-Bern Executive Programs
University of Rochester
Universität Bern

SIMON BUSINESS SCHOOL
UNIVERSITY of ROCHESTER

Charles Sturt University