Biometrics

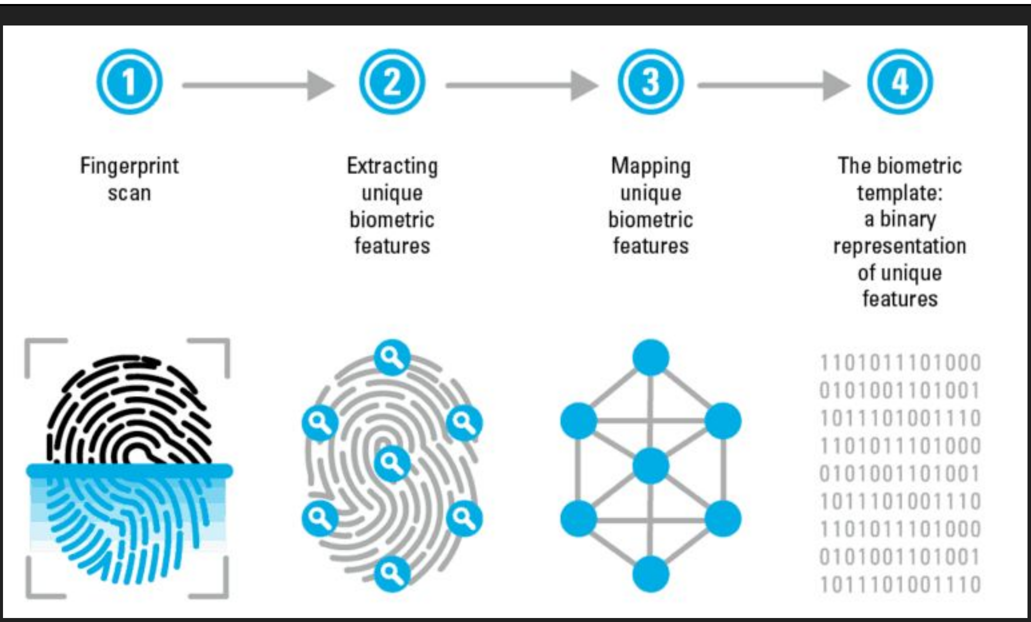
Naomi Shimizu

Overview

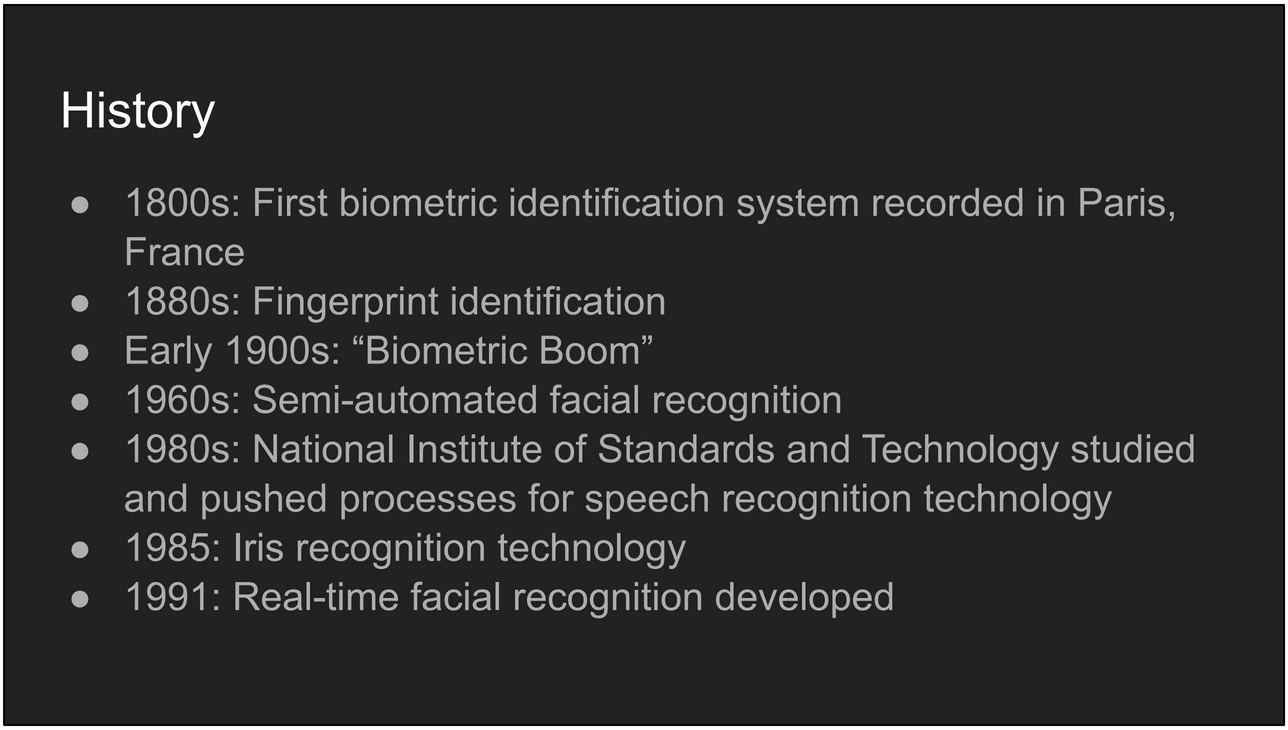
- History
- Plan and implementation
- Positives
- Negatives
- Summary
- References

What is Biometrics?

Biometrics are measurements and calculations related to the unique characteristics of a person. Biometrics are used in computer science for identification and can be referred to as biometric authentication.



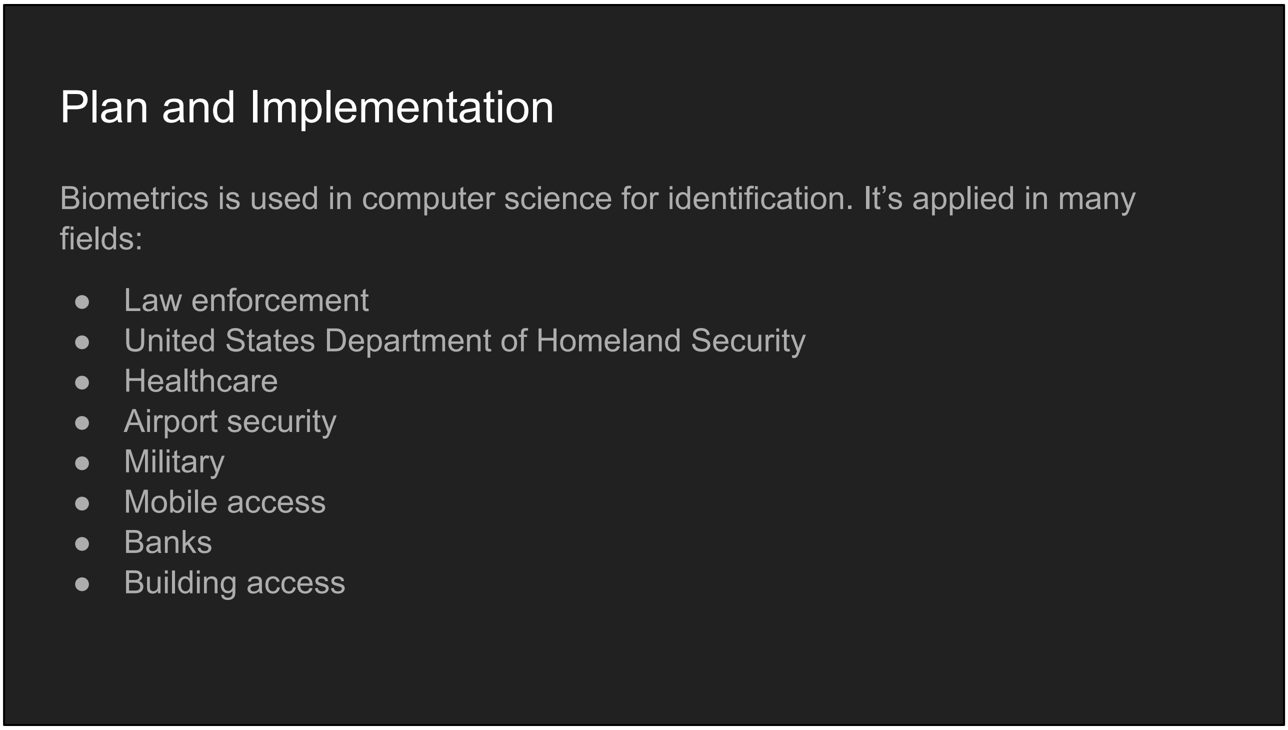
Via Loss Prevention Magazine



History

- 1800s: First biometric identification system recorded in Paris, France
- 1880s: Fingerprint identification
- Early 1900s: “Biometric Boom”
- 1960s: Semi-automated facial recognition
- 1980s: National Institute of Standards and Technology studied and pushed processes for speech recognition technology
- 1985: Iris recognition technology
- 1991: Real-time facial recognition developed

- Though the first recorded biometric identification system was from the 1800s, accounts of biometrics go back to 500B.C.
- Fingerprinting in the 1880s were used to identify criminals and as a form of signature.
- Research in biometrics grew in the early 1900s and saw many advancements.
- In the 1960s, facial recognition systems used an image to analyze facial features.
- Now, biometric technology is everywhere– hundreds of systems are patented and used in many areas of life.

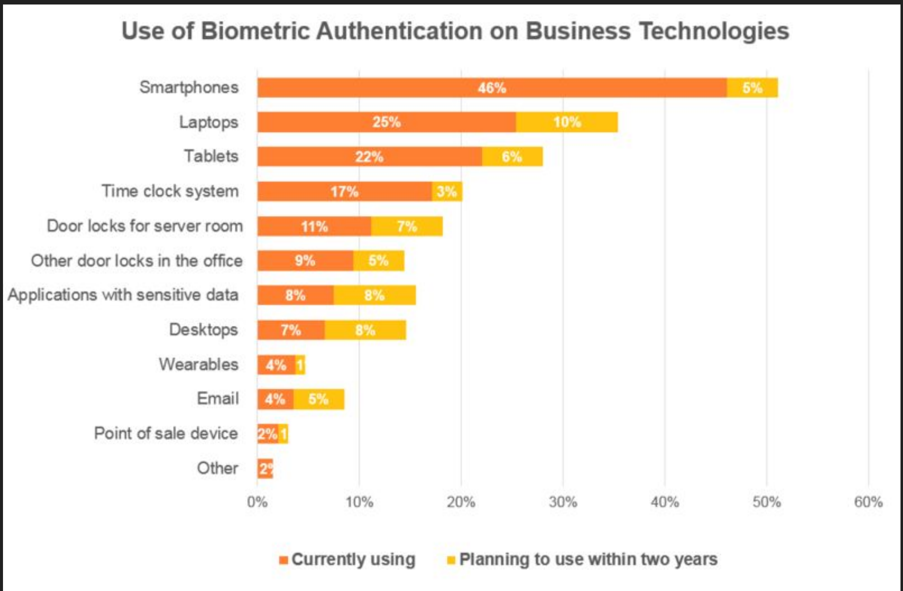


Plan and Implementation

Biometrics is used in computer science for identification. It’s applied in many fields:

- Law enforcement
- United States Department of Homeland Security
- Healthcare
- Airport security
- Military
- Mobile access
- Banks
- Building access

- Law enforcement: criminal identification
- United States Department of Homeland Security: border patrol, credential process
- Healthcare: identification for insurance
- Mobile access: smartphone security- touch id, facial recognition
- Banks: improving security and combating fraud
- Building access: fingerprints used to gain entry into a building or area



Via Spiceworks

Positives

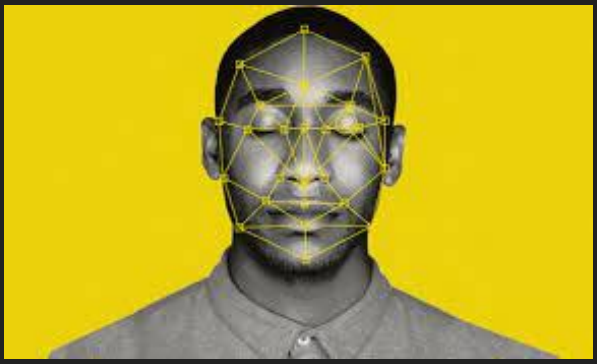
- Hard to fake or steal identity
- Convenient to use
- Efficient
- Easy to integrate

Via IFSEC Global

- It’s impossible to imitate someone’s fingerprint or other features, making biometric authentication very secure
- Very easy and straightforward to use compared to passwords
- Takes up less storage and space
- Easy to integrate because most biometric systems are used across several platforms

Negatives

- Privacy
- Cost
- Possible failure
- User injury



Via Guardian Design

- Unlike passwords, users are known
- Installation costs thousands of dollars and upkeep makes companies continually spend more
- Biometric systems are generally accurate, but errors may still occur
- If a user gets injured a biometric system may not work for to identify them

Summary

I am FOR the advancement of biometric technology. It has already been implemented in many areas of everyday life and has made identification much more secure and accurate.

References

- https://bioconnect.com/2021/12/08/a-brief-history-of-biometrics/
- https://www.techtarget.com/searchsecurity/definition/biometrics
- https://www.nec.co.nz/market-leadership/publications-media/the-top-9-common-uses-of-biometrics-in-everyday-life/
- https://ceoworld.biz/2022/05/09/the-pros-and-cons-of-biometrics/
- https://losspreventionmedia.com/the-best-kept-secret/