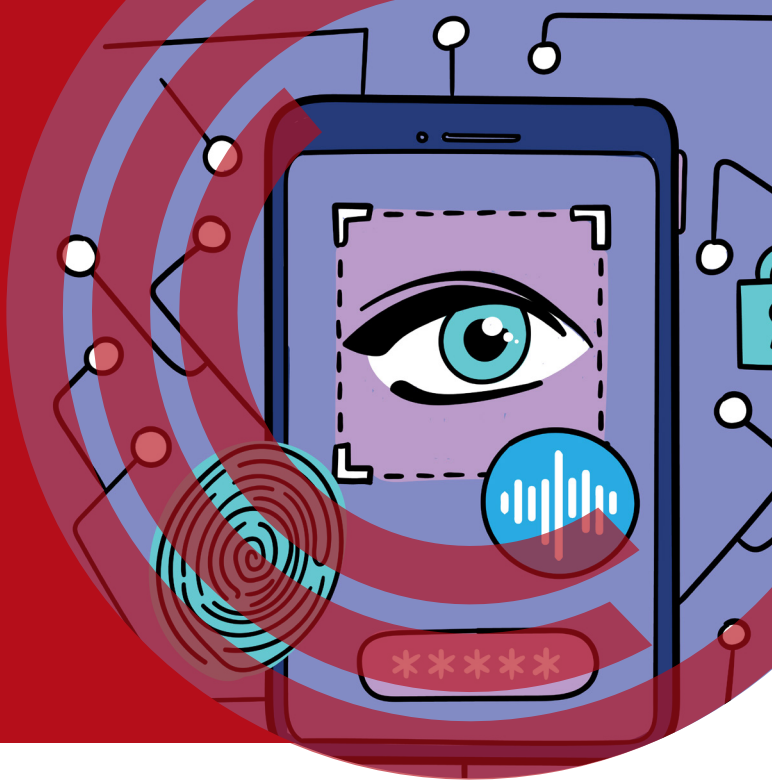
CENTRE FOR RESEARCH AND EVIDENCE ON SECURITY THREATS

5 MINUTE READ

GENERAL

MULTIMODAL BIOMETRICS: A BETTER SECURITY SYSTEM?

This guide looks at the advantages and disadvantages of unimodal and multimodal biometrics.



> **A multimodal biometric security system uses two or more different biometric identifiers**

INTRODUCTION

Biometric security systems are any system that uses a form of biometric identification for security. Some of these you already see in use today such as unlocking phones using fingerprints and face scanning.

Some emerging biometrics are less commonly used as scientific research continues to examine the uniqueness of a wide range of biological traits, e.g., the way people using these systems type, the way they speak, or even their gait while walking (Babich, 2012).

- A unimodal biometric security system is one that only uses one form of biometric to gain access.
- A multimodal biometric security system is a system that uses two or more different biometric identifiers as a form of multi-factor authentication.

Unimodal biometric systems are the most common biometric systems in place today (Sanjekar & Patil, 2013), however the systems are not without flaws or weaknesses in their security:

BIAS RECOGNITION

Unimodal biometrics can be biased or less effective at recognising any other demographics than white men, in particular being much less effective for demographic subgroups, with black women, in particular, having difficulties using the systems (Terhörst et al., 2020).

EASIER TO FAKE

A singular biometric is likely to be easier for hackers to fake or replicate, such as that a face detection system may be hoodwinked by a convincing picture of the person, especially if the person is from one of the subgroups the biometric security systems have higher false acceptance rates on (Alshareef et al., 2021).

HIGHER FALSE REJECTION RATE

Unimodal systems may also face issues with non-universality if the biometric being used can be affected by disability or illness. Dynamic device positioning to read biometrics (where you hold the device to read your face) is the key issue, as with just one angle for the face being recorded and accepted, it can lead to higher false rejections if a feature on that angle changes significantly (Brink, 2019).

> **...with just one angle for the face being recorded and accepted, it can lead to higher false rejections if a feature on that angle changes significantly.**

WHAT CAN MULTIMODAL SYSTEMS DO THAT UNIMODAL SYSTEMS CAN'T?

LOWER FALSE REJECTION RATE

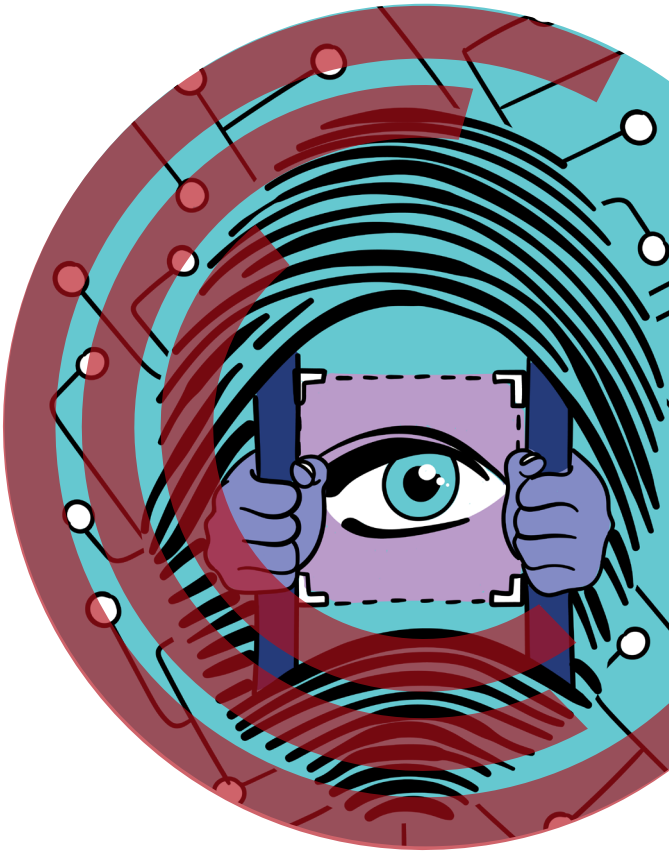
Multimodal biometric security systems mitigate a lot of the issues posed by unimodal as they have higher accuracy than looking at a singular biometric trait (Mishra, 2010). This is achieved by the two biometrics working in unison to minimise the False Acceptance Rate (FAR) (where a person is accepted/recognised within a system when they shouldn't be) and the False Rejection Rate (where a person is rejected/not recognised by the system when they should be) (FRR) (Parkavi et al., 2017).

TWO LOCKS ARE MORE SECURE THAN ONE

Multimodal systems also have higher levels of security, as two biometric traits are much more difficult for hackers to fake than just one trait ('What are Multimodal Biometrics and Why We Need Them - Imageware', 2022).

FLEXIBLE AND COMPENSATING

The system is also a lot more flexible for users than unimodal biometrics, as it's easier to combat noise in the data. If a voice is altered by an illness or a fingerprint altered by an injury, the other biometric trait measured can be used to compensate ('Multimodal Biometrics | Face and Eye Biometrics - BioID', 2022).



WHAT ARE THE DISADVANTAGES OF USING MULTIMODAL BIOMETRICS SYSTEMS FOR SECURITY?

COSTS

Multimodal systems are much more expensive than unimodal. Costs can include the system itself, the necessary computing power to run it, and the storage space for the databases to hold the biometric data (Gawande & Golhar, 2018).

VERIFICATION

- There's also a risk that users may become bogged down in verification processes. However, this is no different to other multifactor authenticators used to secure access.

- Multimodal systems may also face issues with non-universality if the biometric being used can be affected by disability or illness, just the same as unimodal systems (Shahnewaz, 2015).

- Similarly, multimodal systems may still be affected by the environment as it may affect the system's ability to identify an individual. For example, the accuracy of facial recognition is affected by illumination, pose, and facial expression creating noise in the data. Environmental noise in the data can affect whichever biometrics are being measured. However, this could also affect unimodal biometrics (Shahnewaz, 2015).

TRUST AND ETHICS

Ethics and trust of unimodal biometrics such as automatic face recognition (AFR) technology have been debated widely by the public, and recent research shows that the public trust the police using these types of technology much more than private companies, and trust the government using it less than the police but more than private companies (Ritchie et al., 2021).

There's a clear gap in academic literature looking at whether multimodal biometrics are more trusted and accepted by the public. Additionally, none of the reviewed literature discussing the police use of technology mentioned the necessary ethical considerations for doing so.

> **...none of the reviewed literature discussing the police use of technology mentioned the ethical considerations...**

In the case of council-owned CCTV footage, the police have lawful basis for holding and processing personal data. Yet, police access to other personal data, for example via social media, is less clearcut and should be in line with UK GDPR regulations.

CONCLUSION

Overall, the main drawbacks of multimodal biometric systems such as the expense and the need for high-power computing and storage, which make it unattainable for some.

Yet the advantages of multimodal biometrics systems include ease of use; for example, no key-cards or passwords to forget, and quicker user verification systems than one-time passwords.

READ MORE

Advantages also include lower FARs and FRRs than unimodal biometrics as they can account for noise in the data caused by things such as illness affecting voice but not face, making the systems more secure than a singular biometric.

Multimodal biometric systems are also more difficult to hack due to the need to fake two biometrics rather than one. Advantages such as these make multimodal biometric systems far more effective than unimodal biometrics. In general, there is always a risk that hackers could steal the data from biometric databases, and with two (or more) databases for multimodal biometrics there's more data at risk of being stolen (Ikeda, 2019).

The biometrics commissioner should work towards putting together legislation to further protect databases of biometric data, and legislation surrounding the retention of the data which in the case of security should be stored no longer than it needs to be ('About us', n.d.).

About the authors

- Kat Gibbs, Lancaster University
- Dr Sophie Nightingale, Lancaster University

About the project

This CREST guide was produced from the Digital Emerging Biometrics project. You can find all the outputs from this project at: crestresearch.ac.uk/projects/digital-emerging-biometrics/

READ MORE

About us. GOV.UK. Retrieved 12 September 2022, from https://www.gov.uk/government/organisations/biometrics-commissioner/about

Alshareef, N., Yuan, X., Roy, K., & Atay, M. (2021). A Study of Gender Bias in Face Presentation Attack and Its Mitigation. *Future Internet*, *13*(9), 234. https://doi.org/10.3390/fi13090234

Babich, A. (2012). *Biometric Authentication. Types of biometric identifiers* [PDF]. Retrieved 17 June 2022: https://bit.ly/3qESFZm

Brink, R. (2019). *Usability of Biometric Authentication Methods for Citizens with Disabilities* [PDF]. MITRE. Retrieved 23 May 2022: bit.ly/3RL68uP

Gawande, U., & Golhar, Y. (2018). Biometric security system: a rigorous review of unimodal and multimodal biometrics techniques. *International Journal Of Biometrics*, *10*(2), 142. https://doi.org/10.1504/ijbm.2018.091629

Ikeda, S. (2019). *CPO Magazine*. CPO. Retrieved 12 September 2022: bit.ly/3UbhrOw

Mishra, A. (2010). Multimodal Biometrics it is: Need for Future Systems. *International Journal Of Computer Applications*, *3*(4), 28-33. https://doi.org/10.5120/720-1012

Multimodal Biometrics | Face and Eye Biometrics - BioID. BioID. (2022). Retrieved 24 May 2022, from https://www.bioid.com/multimodal-biometrics/

Parkavi, R., Chandeesh Babu, K., & Kumar, J. (2017). Multimodal Biometrics for user authentication. *2017 11Th International Conference On Intelligent Systems And Control (ISCO)*. https://doi.org/10.1109/isco.2017.7856044

Ritchie, K., Cartledge, C., Growns, B., Yan, A., Wang, Y., & Guo, K. et al. (2021). Public attitudes towards the use of automatic facial recognition technology in criminal justice systems around the world. *PLOS ONE*, *16*(10), e0258241. https://doi.org/10.1371/journal.pone.0258241

Sanjekar, P., & Patil, J. (2013). An Overview of Multimodal Biometrics. *Signal &Amp; Image Processing : An International Journal*, *4*(1), 57-64. https://doi.org/10.5121/sipij.2013.4105

Shahnewaz, S. (2015). *Multimodal biometric System for human identification*. M2SYS Blog On Biometric Technology. Retrieved 24 May 2022: bit.ly/3RZ2blS

Terhörst, P., Kolf, J., Damer, N., Kirchbuchner, F., & Kuijper, A. (2020). Post-comparison mitigation of demographic bias in face recognition using fair score normalisation. *Pattern Recognition Letters*, *140*, 332-338. https://doi.org/10.1016/j.patrec.2020.11.007

What are Multimodal Biometrics and Why We Need Them - Imageware. Imageware. (2022). Retrieved 24 May 2022, from https://imageware.io/why-we-need-multimodal-biometrics/