System Security Report:
A Comparative Analysis of of Biometric Schemes for the University of Sheffield's Faculty of Engineering

Author: Yan Kong

Introduction

The University of Sheffield's Faculty of Engineering is considering the adoption of a biometric scheme for enhanced security and authentication. This report provides a thorough analysis of three biometric systems – fingerprint recognition, iris recognition, and facial recognition – based on four key performance criteria: acceptable performance, acceptability, resilience to attack, and permanence. Additionally, the report delves into continuous biometric authentication, inclusivity, privacy concerns, and the overall advisability of adopting such systems.

I. Performance Criteria for Biometric Schemes

The following four performance criteria stand out in assessing biometric schemes.

Performance: It's crucial that the system accurately manages access to facilities and resources. We need high accuracy to prevent unauthorised entries while ensuring legitimate users aren't wrongly blocked, all within our budget constraints.

Acceptability: The system must be comfortable for everyone - students, staff, and faculty. If it's seen as intrusive or raises privacy concerns, it won't work well in our diverse university setting.

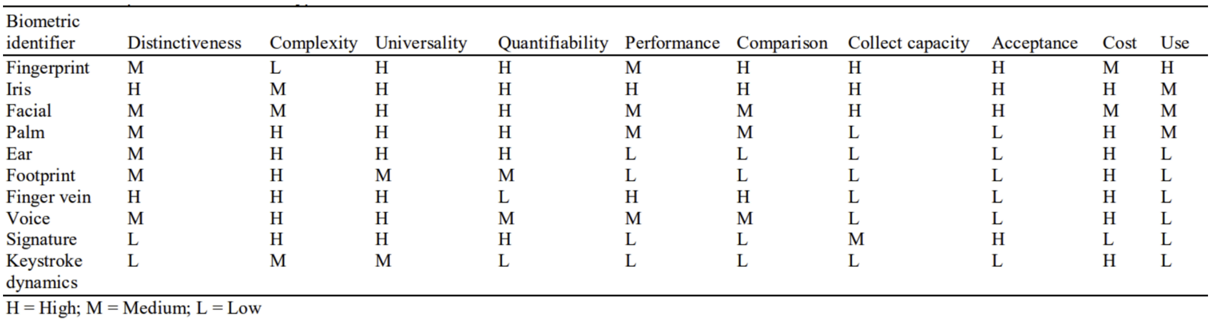
Resilience to Attack: With so much sensitive information on campus, the system must be tough against security breaches, especially to uphold the integrity of exams and research.

Permanence: We need a system that remains reliable over time. Constantly updating biometric data would be impractical, so stability is key for long-term use.

These criteria ensure a secure, efficient, and user-friendly system for our unique academic environment.

II. Assessment of Biometric Schemes

In this section, we evaluate the three proposed biometric systems – fingerprint recognition, iris recognition, and facial recognition – against the established criteria of performance, acceptability, resilience to attack, and permanence.



Biometric identifier	Distinctiveness	Complexity	Universality	Quantifiability	Performance	Comparison	Collect capacity	Acceptance	Cost	Use
Fingerprint	M	L	H	H	M	H	H	H	M	H
Iris	H	M	H	H	H	H	H	H	H	M
Facial	M	M	H	H	M	M	H	H	M	M
Palm	M	H	H	H	M	M	L	L	H	M
Ear	M	H	H	H	L	L	L	L	H	L
Footprint	M	H	M	M	L	L	L	L	H	L
Finger vein	H	H	H	L	H	H	L	L	H	L
Voice	M	H	H	M	M	M	L	L	H	L
Signature	L	H	H	H	L	L	M	H	L	L
Keystroke dynamics	L	M	M	L	L	L	L	L	H	L

H = High; M = Medium; L = Low

Table 1: A comparison of biometrics types based on the characteristics of biometric entities [1]

Fingerprint Recognition

Performance: Fingerprint recognition is known for its high accuracy. However, its effectiveness can be compromised by skin conditions or injuries. It's moderately priced, making it a cost-effective option for the university.

Acceptability: This method is generally well-received due to its widespread use. Post-pandemic, however, there are heightened concerns about hygiene which might affect its acceptance.

Resilience to Attack: While fingerprint systems are susceptible to spoofing, technological advancements have led to improved scanners capable of detecting and preventing such attempts. [2]

Permanence: Fingerprints are relatively stable, although they can be affected by aging or skin damage, which might necessitate occasional re-enrollment.

Iris Recognition

Performance: Iris recognition stands out for its exceptional accuracy, benefiting from the unique iris patterns. However, it's more expensive and complex, which could be a significant factor given our budget constraints. [1]

Acceptability: The close interaction required with the scanning device might be perceived as intrusive, potentially affecting user comfort and acceptance.

Resilience to Attack: It offers high security with a low risk of spoofing due to the intricate nature of iris patterns, making it a robust choice against unauthorised access.

Permanence: The iris pattern remains remarkably stable throughout a person's life, making it a reliable long-term option with minimal need for re-enrollment.

Facial Recognition

Performance: Facial recognition provides good accuracy but can be influenced by changes in facial hair, makeup, or lighting conditions. It requires moderate resources and can be integrated with existing camera systems, which is a plus for scalability.

Acceptability: Generally viewed as less intrusive, it requires minimal physical interaction. However, privacy concerns and the notion of constant surveillance can impact its acceptance.

Resilience to Attack: Vulnerable to deception in less advanced systems, but more sophisticated systems with 3D modelling and liveness detection offer enhanced security. [1]

Permanence: Facial features change over time due to ageing, weight fluctuations, or cosmetic procedures, which can affect long-term reliability.

Each biometric system has its strengths and weaknesses when assessed against our criteria. Fingerprint recognition scores well on performance and acceptability but falls short in resilience and permanence. Iris recognition excels in performance and resilience but is costly and less accepted. Facial recognition, while moderate in performance and acceptability, faces challenges in resilience and permanence.

The ideal system would balance these criteria within our budgetary constraints. This assessment helps us move closer to a decision that aligns with the unique needs and dynamics of our academic environment.

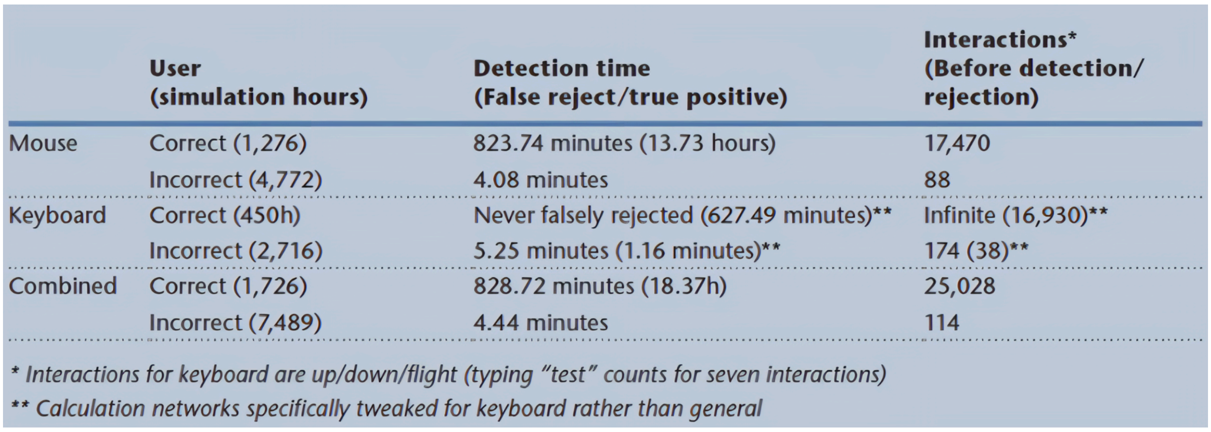
III. Continuous Biometric Authentication Features

In addressing continuous biometric authentication for standard University-provided desktop PCs, a focus on behavioural biometrics is proposed. Behavioural biometrics pertains to the unique, measurable patterns inherent in human activities. The following features are recommended for monitoring to ensure robust and continuous authentication:

Keystroke Dynamics: This involves the analysis of typing patterns. Keystroke dynamics can be seamlessly integrated into the University's existing IT infrastructure, offering a cost-effective solution for continuous verification. The uniqueness of typing rhythm, speed, and duration provides a subtle yet effective means of verifying a user's identity.

Mouse Dynamics: Monitoring mouse movement behaviour presents an additional layer of security. By analysing patterns in mouse movements, clicks, and scrolling behaviour, the system can continuously authenticate users. This method is unobtrusive and operates in real-time, enhancing security without hindering the user experience.

Application Usage Patterns: Tracking the usage patterns of commonly accessed applications provides valuable insights into user behaviour. This feature involves analysing which applications are used, along with the duration and frequency of usage. Such behavioural analysis aids in creating a user profile against which any unusual activity can be compared, thereby identifying potential security risks.



	User (simulation hours)	**Detection time (False reject/true positive)**	**Interactions* (Before detection/ rejection)**
Mouse	Correct (1,276)	823.74 minutes (13.73 hours)	17,470
	Incorrect (4,772)	4.08 minutes	88
Keyboard	Correct (450h)	Never falsely rejected (627.49 minutes)**	Infinite (16,930)**
	Incorrect (2,716)	5.25 minutes (1.16 minutes)**	174 (38)**
Combined	Correct (1,726)	828.72 minutes (18.37h)	25,028
	Incorrect (7,489)	4.44 minutes	114

** Interactions for keyboard are up/down/flight (typing ”test” counts for seven interactions)*

*** Calculation networks specifically tweaked for keyboard rather than general*

Table 2: Mouse and keyboard detection, the detection times don't include inactivity periods of more than 10 seconds [3]

These proposed features for continuous biometric authentication leverage behavioural biometrics to provide a secure, efficient, and user-friendly system. They are particularly suited for the University environment, where the need for security must be balanced with ease of access and minimal disruption to academic activities.

IV. Inclusivity Concerns

The implementation of biometric technologies in a university with a diverse population can present challenges related to cultural sensitivity, and accessibility.

Firstly, cultural and religious beliefs may clash with the use of biometrics. Certain cultures or faiths may have reservations about the scanning or capturing of biometric features, considering it intrusive or against their beliefs.

Secondly, accessibility issues may emerge for individuals with disabilities or medical conditions that affect their biometric features. These technologies may not be suitable for everyone, potentially excluding some members of the university community.

To address these concerns, the university should prioritise informed consent, ensuring that individuals have the choice to opt-in or opt-out of biometric authentication. **Alternative authentication methods**, such as PINs or passwords, should be made available to accommodate those uncomfortable with biometrics.[4] The university should also respect cultural and religious sensitivities by offering exemptions when necessary. Overall, a flexible and inclusive approach is crucial to maintaining an environment where all staff and students feel comfortable and respected.

V. Privacy Issues

In the context of single-use biometric systems, privacy concerns primarily revolve around the potential for data breaches. Unlike passwords, biometric data is immutable; once compromised, it cannot be reset or altered, posing a significant risk. Additionally, there's the fear of surveillance, especially with facial recognition, where individuals might feel their privacy is invaded by constant monitoring.

For continuous biometric authentication, such as keystroke and mouse dynamics, the concerns shift towards the intrusiveness of constant monitoring of user behaviour. This raises questions about the extent of personal data being collected and how it might be used beyond authentication purposes. The idea of being continuously watched and analysed can be unsettling, leading to discomfort among users.

Both scenarios also share common concerns about consent. In an academic setting, students and staff might feel obligated to participate, raising ethical questions about voluntary participation and the potential misuse of biometric data.

VI. Feasibility and Recommendation of Biometric Systems

Upon thorough evaluation, my recommendation for our biometric scheme is: implementing iris recognition for exam authentication and facial recognition for access to the Faculty's buildings and rooms.

Why Iris Recognition for Exam Authentication?

In the high-stakes environment of formal examinations, where unequivocal identification is essential, iris recognition offers a solution of exceptional accuracy and low false acceptance rates. Its resistance to spoofing and minimal contact nature, while necessitating proximity, are considered acceptable compromises in the context of exam security, ensuring a secure yet relatively non-invasive process for students.

Why Facial Recognition for Building and Room Access?

Facial recognition, known for its non-intrusive approach and increased accuracy thanks to advancements in computer vision, is perfectly suited for controlling access to buildings and rooms. Its long-term viability is further bolstered by the potential for continual enhancements in accuracy, made possible through evolving machine learning algorithms. This positions facial recognition as a sustainable and forward-looking option for campus security.

Balancing Technology and Concerns

While we've discussed the advantages and challenges of various biometric systems, it's worth reiterating that facial recognition strikes a balance between security and user experience. Yes, there are privacy concerns and the need for robust security against potential breaches, but these are not insurmountable. With responsible data management and continuous updates to the system, we can mitigate these risks. [2]

The Bigger Picture

Adopting this technology also puts us at the forefront of digital innovation in academia. It's not just about security; it's about embracing change and preparing for a future where digital identification will likely become more prevalent.

Conclusion

In conclusion, the university's decision to go forward with biometric schemes is a step in the right direction. It reflects a thoughtful consideration of current technology, user experience, and the unique environment of our campus. With proper implementation and ongoing management, this system can provide a secure, efficient, and forward-looking solution to our authentication and security needs.

Reference

[1] Al Rousan, M. & Intrigila, B. (2020). **A Comparative Analysis of Biometrics Types: Literature Review.** Journal of Computer Science, 16(12), 1778-1788. DOI: 10.3844/jcssp.2020.1778.1788

[2] Shefali Arora & M.P.S Bhatia (2022) **Challenges and opportunities in biometric security: A survey**, Information Security Journal: A Global Perspective, 31:1, 28-48, DOI: 10.1080/19393555.2021.1873464

[3] I. Deutschmann, P. Nordström and L. Nilsson, "**Continuous Authentication Using Behavioural Biometrics,**" in IT Professional, vol. 15, no. 4, pp. 12-15, July-Aug. 2013, DOI: 10.1109/MITP.2013.50

[4] Boluma Mangata, B. et al. (2022) '**Implementation of an access control system based on bimodal biometrics with fusion of global decisions: Application to facial recognition and fingerprints**', Journal of Computing Research and Innovation, 7(2), pp. 43–53. DOI: 10.24191/jcrinn.v7i2.289