Extensive research has been conducted in multimodal biometrics. Studies have shown traditional security authorisation methods can increase chances of breaches in the system as it can be easily accessed via spoofing (Kumar, K., & Farik, M. 2016). Therefore, the introduction of biometrics minimised this risk and upgraded its security for users.

Multimodal biometrics have been introduced to provide a user's own biological data to access a system. Furthermore, technological development has allowed two types of biometrics to be invented – unimodal and multimodal (multimodal meaning more than one sensor to check if user is accepted by the system by verifying their biology whereas unimodal uses only one sensor for the same purpose). Unimodal has been critiqued by researchers suggesting there are many issues such as noisy data, spoofing attacks and unacceptable error rates and rejection rates (Ross, A., & Jain, A. K. 2004, September). Consequently, researchers suggest the use of multimodal system is an improvement which can also be supported by real world application since US congress has stated approximately 2% of the United State of Americas population does not have valid form of fingerprint therefore cannot be enrolled in the fingerprint system (Besbes, F., Trichili, H., & Solaiman, B. 2008, April). Further research added, multimodal will allow users freedom of choice for the biology presented this can be applied to many real-life scenarios such as border security at airports (Leghari et al 2021).

Multimodal biometrics system responds to the issue regarding non-universality and insufficient population coverage where a certain percentage of population has certain lack of characteristics in biometric that may be detected invalid for recognition (such as no fingerprint) and therefore reduces the chance of enrolment into the system (Frischholz & Dieckmann, 2000).

Multimodal biometric devices according to (Ross, A., & K. Jain, A. 2004) have stated that multimodal biometric devices have high sensitivity which can cause an increased chance of rejection to its users that should be authorised. This causes a trade-off between security and availability to bypass the security system, this should be considered profusely to designers of multimodal biometrics. The argument develops by suggesting that if a user presents an alter in the way they present their biometric feature for example a scar across the face or a burnt finger then the system may not recognise the biometric data due to an alter in the way the data is presented, increasing the likelihood of false rejection rates. This can potentially limit the possibility for the system to only recognising the user in certain forms which can be unrealistic over large periods of times.

Biometrics works based on a system which consists of 4 components and uses an algorithm based on user acceptance or rejection. User inputs biometric feature, sensor then gathers all appropriate biometric data by fusing and merging the data together from both sensors and then a decision is determined to see whether the user should be accepted or rejected. The system then creates and compares the default template on the database to spot how similar the match is for the next time it is used.

Researchers still debate whether the system for multimodal biometrics have a flawed design as its algorithm has been criticised for needing improvements for user acceptance and denial (Snelick et al 2003, November). Others counter this argument by advising for system fusion(merging of both sensory data at once) at earlier stages for more efficiency and higher performance when presenting data.

According to (Kathed, A., Azam et al 2019, January) there are multiple frameworks for multimodal biometrics. Multi-algorithmic biometric frameworks are used to take a user's biometric data and find two distinctions in their biology to recognise the individual. Multi-occurrence biometric framework does a similar job as the previous example but uses multiple sensors instead. Multi-sensorial biometric framework uses 2 unique sensors to detect similar biometric data. However, alternate research has underlined this as an issue describing how multimodal biometric devices has no standardised method of use therefore can be difficult to design and implement due to many different types being introduced(Mane, V. M., & Jadhav, D. V. 2009).

Studies have highlighted when using multimodal biometrics – the type of sensor used must be considered very closely. Studies conducted by Mishra, A. (2010) highlights voice recognition combined with other sensor devices has a higher average for false acceptance rate and false rejection rate. Whereas face recognition has a lower false acceptance rate. The same study also acknowledged biometric devices having a lack of consideration for the aging process whilst designing multimodal biometric systems. Meaning that voice, face and palm recognition can all be affected by aging therefore this must be taken into account whilst designing making it harder to create a multimodal biometric device which can be maintainable for long-term use.

In the journal published by Jain, A. K., & Ross, A. (2004) they demonstrated a graph showing the difference between genuine acceptance rate and false acceptance rate on multimodal devices compared to unimodal. The results had shown a higher genuine acceptance rate for multimodal devices in comparison to the false acceptance rate presented by the same system. Multimodal biometric devices are receiving further interest from the government, further testing and more funding from the national institute of science and technology highlighting the development of biometrics are emerging into our daily life.

Research conducted shows 1000 participants had been used in a multimodal analysis(where all their biological data was placed into a system) and had shown significant improvement compared to previous models introduced (Snelick et al 2003, November). In support of this was the study conducted by Hariprasath. S et al (2012) who discovered very specific combinations of multimodal sensors give further accuracy such as iris and palmprint and this was measured at various fusion levels on the system and had reduced the number of false rejection rates presented by the system.

Conclusion

Multimodal biometric devices give a “safety-net” for its users when initiating access to a system. But multimodal biometric devices have become evident for being a highly advanced system with a range of algorithms and design for acceptance or user rejection, which can complicate its implementation. Many types of designs may indicate greater flexibility and allow for it to meet user demands however this means that those designing the system has no standardised procedure to follow. Further funding by the government has meant that engineers can refine the flaws presented within the system and allows for further research and amendments as well as development in the field itself.

Referencing

- Ross, A., & Jain, A. K. (2004, September). Multimodal Biometrics: an overview. In *2004 12th European Signal Processing Conference* (pp. 1221-1224). IEEE.

- Ross, A., & Jain, A. (2003). Information fusion in biometrics. *Pattern recognition letters*, *24*(13), 2115-2125.

- Snelick, R., Indovina, M., Yen, J., & Mink, A. (2003, November). Multimodal biometrics: issues in design and testing. In *Proceedings of the 5th international conference on Multimodal interfaces* (pp. 68-72).

- Mishra, A. (2010). Multimodal biometrics it is: need for future systems. *International journal of computer applications*, *3*(4), 28-33.

- Sanjekar, P. S., & Patil, J. B. (2013). An overview of multimodal biometrics. *Signal & Image Processing*, *4*(1), 57.

- Besbes, F., Trichili, H., & Solaiman, B. (2008, April). Multimodal biometric system based on fingerprint identification and iris recognition. In *2008 3rd international conference on information and communication technologies: from theory to applications* (pp. 1-5). IEEE.

- Kathed, A., Azam, S., Shanmugam, B., Karim, A., Yeo, K. C., De Boer, F., & Jonkman, M. (2019, January). An enhanced 3-tier multimodal biometric authentication. In *2019 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-6). IEEE.

- Mane, V. M., & Jadhav, D. V. (2009). Review of multimodal biometrics: applications, challenges and research areas. *International Journal of Biometrics and Bioinformatics (IJBB)*, *3*(5), 90-95.

- Kumar, K., & Farik, M. (2016). A review of multimodal biometric authentication systems. *Int. J. Sci. Technol. Res*, *5*(12), 5-9.

- Jain, A. K., & Ross, A. (2004). Multibiometric systems. *Communications of the ACM*, *47*(1), 34-40.

- Hariprasath, S., & Prabakar, T. N. (2012, March). Multimodal biometric

- Gavrilova, M. L., & Monwar, M. (2013). *Multimodal biometrics and intelligent image processing for security systems*. IGI Global.

- Frischholz, R. W., & Dieckmann, U. (2000). BiolD: a multimodal biometric identification system. *Computer*, *33*(2), 64-68.

- Leghari, M., Memon, S., Dhomeja, L. D., Jalbani, A. H., & Chandio, A. A. (2021). Deep Feature Fusion of Fingerprint and Online Signature for Multimodal Biometrics. *Computers*, *10*(2), 21.