AI in biometrics security

Course Title: Research Methodology in Computer Science
Course Code: AI800
Lecturer: Dr. Mohammed Anbar
Student: Fatima Alkaff

Problem Statement

1. Problem Domain Identification

Biometric security today is integrated into our existing authentication processes and is implemented on a large scale in bank applications all the way to medicine, government security, and phone applications (Galla et al,. 2021). The systems use the unique physiological and behavioral characteristics such as fingerprints, facial outlines, iris scanning, and voice in trying to identify the users and authenticate them (Abdullahi et al,. 2022). Artificial Intelligence (AI) brought with it speed, accuracy, and efficiency to this kind of authentication into the fray (lyer et al,. 2020). Above all the advantages it brings with itself, AI-powered biometric systems of authentication have some challenges en route to privacy, security problems, bias from algorithms, and ethics too (Malik et al,. 2024).

2. Stating the Problem

As nice as AI is at improving security with less false positive and false negative error in biometric authentication, there are several rather ugly consequences of the technology that need to be dealt with before it goes into widespread use globally and to its blanket acceptance on which it will come to depend (Clarke et al,. 2019):

- Privacy Issues: Biometric information, as non-replicable and non-reversible as opposed to classical passwords, are prone to misuse, leakage, and storage, to the detriment of identity theft, compromise of surveillance, and ethical problems. AI-driven biometric technology has to be stored safely, encrypted, and anonymized to facilitate users' data protection (Jain et al,. 2025).
- AI Bias and Fairness Problems: Biometric identification and face recognition technology have proven to be discriminatory against multicultural communities, specifically. Discriminatory data, driven by AI algorithms, may mislead or discriminate against a certain ethnic group, gender category, or age category and develop discriminatory security protocols. The issue in this case is fairness, inclusiveness, and stability of AI-based biometric technology (Abdullahi et al,. 2022).
- Cyber Threats and Vulnerabilities in AI: Artificial intelligence-driven biometric authentication can be vulnerable to adversarial attacks, spoofing, and deepfakes. Adversarial attackers are able to manipulate artificial biometric information, artificial

fingerprints, or AI-generated artificial faces with a focus on trying to circumvent authentication controls and thus compromise security. AI models can be hacked, poisoned, or compromised unless suitable security is implemented (Iyer et al,. 2020).

- Lack of Standardization and Regulation: There is no single standard for the regulation, utilization, and deployment of AI-based biometric systems at an ethical level yet. Protection like GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act) provides a certain degree of protection, but varying legislation all over the world causes issues in compliance as well as safeguarding the rights of the users (Malik et al,. 2024).

3. Highlighting the Significance

With the digitization moving at a faster pace, good biometric verification is gaining in significance (Galla et al,. 2021). With AI-driven biometric solutions, it is possible to provide for the perfection of the identity check process and flawless error-free mechanism, with zero forgery and making the overall experience simple for customers. But no human work is going into them (Clarke et al,. 2019). The solutions can therefore go into private space, reinforce discrimination, and become security threats rather than a security solution. The worth of this work is in the multi-dimensional capability to improve AI-based biometric identification security and make it fair, accurate, and safe for applications across industries (Iyer et al,. 2020).

4. Deficiencies of Current Solutions

Some alternatives to enhancing AI-based biometric security, i.e.:

- Deep Learning and Neural Networks: Machine learning processes are more accurate in biometric authentication but adversary-proof, equitable, and live-time adaptive (Jain et al,. 2025).
- Multi-Factor Authentication (MFA): Use of biometrics with traditional practices like PIN and password is safe but too inconvenient to implement on the users' end (Malik et al,. 2024).
- Encryption and Anonymization Controls: Biometrically stored data is encrypted but exposed to AI-driven attack processes, model inversion attacks, or bias diffusion (Abdullahi et al,. 2022).

- Liveness Authentication and Anti-spoofing Protection Controls: AI can identify deepfakes and biometric spoofing but will be susceptible to future software patches in an attempt to be effective with the ever-evolving nature of cybersecurity threats (Iyer et al,. 2020).

These and numerous others are solving nothing, however, to address privacy invasion concerns, AI bias, security vulnerabilities, and ethics concerns whatever. All of this is all a show that research must be conducted.

5. Justifying the Demand for Research

With more deployment and utilization of AI, study needs to:

- Develop Equilibrium AI Models – Improve AI training data sets for minimum bias and attain biometric identification as detailed as possible (Abdullahi et al,. 2022).
- Scale Privacy Protection – Implement safe data storage, encryption, and anonymization processes to safeguard biometric data (Galla et al,. 2021).
- Improve Cybersecurity Capabilities – Secure AI models against adversarial attacks, deepfake interference, and synthetic forgery (Iyer et al,. 2020).
- Build Ethical and Regulatory Structures – Develop strong regulatory structures, transparency of AI-driven decisions, and ethical use of biometric data (Malik et al,. 2024).
- Scale Again and Roll Out More Sensibly – Scale out AI across sectors without compromising one's security and privacy (Jain et al,. 2025).

In addition to the above, the future will bring confidence, credibility power, and global acceptability of AI-driven biometric authentication and make it an ethical and secure digital identity platform.

Research Objectives

- To be adequately informed of different applications of AI for safe and reliable biometric identification.
- To be adequately informed of open issues, i.e., vulnerability of privacy, bias of AI, and cyber-attack.
- To be adequately informed of available solutions of biometric security: comparison of performance.
- To make AI-informed recommendations on bias suppression of AI and unbiased recognition.
- For effective design of mechanisms of protection of privacy, i.e., encryption and anonymization.
- To remain up to date with adversarial attacks and keep security protocols with inputs of AI.
- To develop legal and ethical standards for secure processing of biometrics.
- To gain knowledge on AI-based biometric authentication in sectors.

References

- Galla, E. P., Madhavaram, C. R., & Boddapati, V. N. (2021). Big Data And AI Innovations In Biometric Authentication For Secure Digital Transactions. Available at SSRN 4980653. https://dx.doi.org/10.2139/ssrn.4980653
- Abdullahi, S. B., Khunpanuk, C., Bature, Z. A., Chiroma, H., Pakkaranang, N., Abubakar, A. B., & Ibrahim, A. H. (2022). Biometric information recognition using artificial intelligence algorithms: A performance comparison. IEEE Access, 10, 49167-49183. https://ieeexplore.ieee.org/abstract/document/9766125
- Iyer, A. P., Karthikeyan, J., Khan, R. H., & Binu, P. M. (2020). An analysis of artificial intelligence in biometrics-the next level of security. J Crit Rev, 7(1), 571-576.
- Clarke, A., & Charles, J. (2019). The Role of AI and Biometrics in Identity Security.
- Jain, C., Bhawani, H., & Saxena, A. Enhancing Biometric Security with Artificial Intelligence: A Cutting-Edge Approach. https://www.ijsat.org/papers/2025/1/1771.pdf
- Malik, S. (2024). The Future of AI in Biometric Security: Enhancing Authentication and Privacy Protection.