

AI in biometrics security

Course Title: Research Methodology in Computer Science

Course Code: AI800

Lecturer: Dr. Mohammed Anbar

Student: Fatima Alkaff

Content List

Paper 1.....	3
Paper 2.....	4
Paper 3.....	5
Paper 4.....	6
Paper 5.....	7
Paper 6.....	8
Critical Analysis.....	9
Connections.....	11
Conflicts between the findings.....	12
Synthesis Matrix for Literature Review.....	13
References.....	17

Paper 1: Big Data And AI Innovations In Biometric Authentication For Secure Digital Transactions

This article (Galla et al., 2021) describes the manner in which big data and AI enable secure online transactions by offering biometric authentication. The study identifies improving protection against fraud, authenticating in less time, and reducing banking, e-commerce, and healthcare security vulnerabilities.

The research uses an analytical review methodology, reporting biometric authentication innovation, AI security innovation, and big data adoption. It is used to explain how AI methods such as deep learning and neural networks enhance security and authentication accuracy using multimodal biometric modalities.

Most critical findings are that biometric authentication that uses AI is more secure than the traditional mechanisms of PIN and password use. Multimodal authentication from facial recognition, fingerprint, and behavior-based biometric discourages fraud attacks. Big data analytics further enhance fraud prevention as they intercompare the pattern of customers' behaviors. All studies agree that AI and big data revolutionize biometric security but never forget that treating the issues of privacy and ethics while utilizing the biometric data matters.

Applications vary by industry. In finance and business, AI biometric identification provides convenience to consumers and safeguarding against counterfeiting. It keeps medical records out of reach in medicine. Regulation, privacy concerns would need to be ironed out so use could be safeguarded, though.

While the study well documents milestones of technology, empirical evidence and deployment issues thereof are not seen in it. The study fails to evaluate AI bias against biometric identification and its importance to the system's overall fairness. Overall, the study is useful but supplemented with other studies on cases, regulation analysis, and implications towards adoption

Paper 2: Biometric Information Recognition Using Artificial Intelligence Algorithms: A Performance Comparison

This research paper (Abdullahi et al., 2022) is the performance comparison of AI algorithms used to recognize the biometric features and demographic features. It's an attempt towards better crime detection, cyber security defense, and biometric authentication using higher order AI models.

The research aims to compare the performance of ANFIS-SC (Adaptive Neuro-Fuzzy Inference System with Subtractive Clustering) and SVM-ECOC (Support Vector Machine with Error Correction Output Code) artificial models in biometric data identification. The aim is to improve hand-based demographic attribute and biometric attribute identification like sex, height, weight, and foot size.

The study applies human-centered reasoning underpinned by machine learning. Pearson Correlation Coefficient (PCC) is applied as a feature selector and performance measures analysis grounded in Root Mean Square Error (RMSE), Mean Absolute Percentage Error (MAPE), Scatter Index (SI), and Nash-Sutcliffe Model Efficiency Index (NSE). Biometric information involves 112 subjects with equal women and men representation.

Outcome are models accurately detect biometric information but rather by ANFIS-SC than by SVM-ECOC. Best is ANFIS-SC with $RMSE \leq 3.85$, $AICc = 2.39E+02$, $MAPE = 0.18\%$, $R^2 \geq 0.99$, and $NSE \geq 99\%$. The research further confirms that AI algorithms fare better than traditional statistical tools to fare better than traditional algorithms for biometric data identification.

The research is sure that AI-oriented biometric identification is best suited to be used in internet security and crime management. The research states some of the challenges such as computational complexity and parameter tuning, though. The research advises improving AI models by including more demographic and psychological attributes in an attempt to improve accuracy.

Despite good literature and adequate technical knowledge, the research is lacking in tests of practical usefulness. Data also are lean in numbers (112 samples) with low generalizability. Tests involving large and large data sets and bias reduction in biometric AI models will make the research stronger. Finally, the research convincingly proves AI usability for biometric

identification but could be fortified by case studies in actual circumstances and real-world plans for applications.

Paper 3: An analysis of artificial intelligence in biometrics-the next level of security

The research (Iyer et al., 2020) covers the integration of AI and biometric identification for online security. The research indicates how AI improves biometric technology's security and limitations of current biometric technology.

The primary focus of the research is to observe the application of AI in increasing security in biometrics by evading human error and unauthorized entries.

That's where it explains how AI will assist in the creation of adaptive security models and minimize vulnerability to conventional methods of evidence such as passwords and PINs.

The project was demonstrated in a very pragmatic manner as a review using latest biometric identity technology and artificial intelligence technology. Military applications, airport security clearance, payment systems, and biometric passports were shown as demonstrable examples for application. Artificial fingerprints created because of the deployment of AI are some of the problems encountered to date. Moreover, spoofing attacks on the biometric platform have also occurred.

The research verifies that AI enhances the security of biometrics by way of enhanced recognition and lower error rates. The research postulates the possibility of AI minimizing false accept and reject rates. The research verifies the fact that biometric systems are not infallible and need regular upgrades to remain ahead of evolving threats.

The study concludes that AI biometric verification is the future of online safety. Although the way it is being used is flawless, its privacy, ethics, and vulnerability to AI-facilitated cyber attacks is gigantic. It is henceforth highly recommended by the study that unveiling of AI-facilitated biometric security should be expedited in the future so that problems are minimized.

Use cases are sector-agnostic. In finance, AI biometrics combat financial crime and provide an improved customer experience. AI enhances surveillance and identification verification for national security purposes. AI bias, ethics, and regulation issues must be solved.

As useful as it is, empirical evidence and real case studies would be applicable to this research here. Practical application analysis of AI bias in biometrics as a variable and studies would be a gem to find. Otherwise, the study is good enough to demonstrate the potential of AI as much as

biometric security is the issue but can improve with even more representative of issues of privacy, ethics, and use.

Paper 4: The Role of AI and Biometrics in Identity Security

This article (Clarke et al., 2019) illustrates how biometric technologies increase identity security. The research analyzes the performance, advantages, and disadvantages of biometric identification in securing identity verification processes.

The study will reveal how biometric authentication is more secure than the traditional use of passwords and PINs. It gives an example of how biometrics—fingerprint recognition, face recognition, iris scan, voice recognition, and behavior biometrics—improve the security aspect while offering more convenient experience.

The research approach adopted is review-based and is grounded in industry reports and existing studies. The research translates adoption rates, effectiveness, user satisfaction rates, cost, and privacy concerns of biometric authentication. There is proof that biometric authentication is usable and secure. Face and fingerprint recognition are the most prevalent, while iris scan and behavior biometrics are newer generation systems.

Though they work absolutely fine, biometric systems are plagued by privacy issues, cost, and legal requirements. The study offers the growing applications of biometric authentication across industries, particularly in finance and national security.

The study concludes that biometrics are revolutionizing identity security by offering a new alternative to traditionally used authentication. The cost, system vulnerability to attacks, and adherence to the law of implementing the technology must be overcome. The authors identify the importance of good data protection policies and AI development for improving biometric security.

The range of impact of the study is extensive and diverse. Economically, biometrics insulates against fraud and eases authentication. Biometrics driven by AI fortifies identification authentication at police stations, airports, and financial transactions. It is still necessary, however, that privacy issues, the use of ethical AI, and state surveillance are regulated firmly through legislation.

While the study is useful, it does not include empirical data and real case studies. The study would even be more useful with critique of AI bias impacts on biometric recognition and additional

details on privacy protection. Generally, the study assists in summarizing well AI and biometrics' role in protecting identity but needs additional critique of ethical issues and regulatory policies.

Paper 5: The Role of AI and Biometrics in Identity Security

The article (Jain et al., 2025) puts into perspective the manner in which AI is employed for biometric security. It sets on record capabilities of AI which increase security and efficiency of biometric identification, and security threats.

The overall objective of the current study is to discuss the interaction of AI and biometric identification, such as the contribution of deep learning, CNNs, and other uses of AI in enhancing biometric security. The study will explore AI uses in anomaly detection, pattern recognition, and feature extraction to be applied in law enforcement security systems, finance, and healthcare.

The research takes a review strategy and includes biometric technologies like fingerprinting, iris scanning, facial recognition, and behavioral biometrics. The research discusses the AI advancements in the above categories and explores the security and ethics of AI-based biometrics. Technical derivations, the process of encryption, and mathematical models are suggested by the research to improve biometric verification.

Consequences are that AI improves biometric security by improving accuracy, reducing fraud, and enabling real-time authentication. AI models, particularly CNNs and machine learning algorithms, improve accuracy and robustness of biometric identification. However, privacy concerns, AI biases, and adversarial attacks are present.

The study concludes that AI-based biometric security is the future of verification and has the potential to bring about greater precision and speed. Ethics, laws, and AI-based cyberattacks are some of the issues to be addressed. The study demands that AI be calibrated time and again in an attempt to reach perfection in biometric authentication processes.

The effect is extensive in industries. AI biometrics propel economic security in anti-fraud, police protection, and patient information protection in the healthcare sector. Regulation has to be stringent on privacy, regulatory needs, and ethical uses of AI.

While the research is useful in making technical claims, it is neither tested nor confirmed in practical environments. The research can be enriched with case studies of AI bias in biometric authentication and privacy protection augmentation. In general, the research fully explains the

function of AI in biometric security but needs more explanations on ethical concerns and issues of practical implementation.

Paper 6: The Role of AI and Biometrics in Identity Security

The article (Malik et al., 2024) explains how AI is transforming biometric security in the context of more accurate authentication and privacy protection. The article describes the application of AI to protect biometric authentication technology and avoid security vulnerabilities.

The research aims at examining how AI supports biometric security by facilitating recognition accuracy, fraud prevention, and privacy. It clarifies that AI-driven authentication technologies like face recognition, fingerprint scanning, iris scanning, and voice analysis are unshakable for secure verification of identity.

The study adopts a review strategy to analyze existing biometric authentication methods and the role of AI. The article discusses how the deep learning architectures enhance the recognition rates and AI combines different biometric modalities for authentication at different levels. Encryption mechanisms and anonymization techniques for the security of biometric data are discussed in the article.

The results confirm that AI enhances the security of biometrics by error minimization and fraud detection optimization. AI-based systems are able to identify fraud in real-time and improve verification even in adverse environments, such as dim light or partial occlusions. AI also enables the anonymization and encryption of the biometric data even more feasible, rendering it even more secure.

The study repeats that AI-powered biometric security is the future of authentication. Short of that, privacy concerns, ethics concerns, and compliance are genuine issues. It calls for ethical application of AI, enhanced encryption techniques, and ongoing innovation in biometric authentication.

The research has worldwide application to numerous disparate industries. Smart bank fraud detection, safer law enforcement ID checks, and greater patient protection become a healthcare plus thanks to AI-driven biometrics. Yet ethical concerns, the potential for AI bias, and privacy threats call for stringent regulatory oversight.

While the study is informative, it is based on no empirical evidence and field testing. The study can be better enhanced with consideration of AI bias analysis in biometric recognition, reference

to issues of practical application challenges, and examination of possible regulation. On the whole, the study does a good job of capturing the role of AI in biometric security but calls for further elaboration on ethics, privacy vulnerability, and application challenges in the field.

Critical Analysis of AI-Driven Biometric Security Research

The AI-powered biometric security research has significant strengths and limitations within the six researched studies. Worth mentioning is a major strength where detailed examination is made of enhancing authentication accuracy, anti-fraud techniques, and multi-modal fusion of biometrics. The various studies apply alternative AI models varying from deep learning, CNN, to machine learning models like ANFIS-SC and SVM-ECOC. Performance tests show that AI-based biometric authentication significantly enhances recognition performance, reduces false acceptance and rejection rates, and enhances overall security strength. More studies, such as "Biometric Information Recognition Using AI Algorithms," contribute further by undertaking comparative assessments of AI models wherein the best-performing ones are optimized learning techniques versus traditional biometric methods.

In spite of all these developments, there are some limitations of the research. The majority of the research is based on theoretical models, simulations, or secondary data and lacks much real-world relevance as well as empirical validation. The absence of practical case studies as well as large-scale trials undermines the argument that AI is omnipresent useful in biometric security systems. Apart from it, where a couple of studies mention issues of privacy, e.g., "The Future of AI in Biometric Security," they fail to point out in clear words what must be done to avoid the following dangers of AI-based biometric fraud, unauthorized monitoring, or data leakage. It is not easy:

in the absence of standard encryption techniques or anonymization steps.

Another serious concern is that very little argument on AI fairness and bias in biometric authentication exists. Biometric systems based on AI have been accused of biased errors in the identification of people from various demographic categories. Most of the papers address accuracy measures with no mention of bias adjustment or fairness metrics. Cost and scalability considerations are utterly overlooked, and hence one is unable to judge how realistic it is to deploy AI-based biometric systems at large scales. AI-based security systems are

infrastructurally intensive and computation-requiring but none of the articles make any cost-benefit evaluation or mention any economic limitations to their implementation.

Methodologically, the research relies on the combination of machine learning performance analysis and discourse review to establish a general understanding of AI effects on biometric security. Higher methodological discipline would also make them reproducible. More careful attention to test specifications, deployment circumstances, and data utilized, for instance, would make conclusions valid. Some of the articles, for example, "Big Data and AI Innovations in Biometric Authentication," provide examples of fraud detection by AI without even comparing AI techniques with traditional security.

In total, while the work is useful to AI-based biometric security, it is empirically untested, economically viable, and unethical. Overcoming these constraints by conducting real-world experiments, debiasing, regulatory adherence, and economic analysis would make AI-based biometric verification systems more practical. Future research would focus on striking a balance between security enhancement and privacy maintenance and ethical utilization of AI as a tool to enhance greater fairness, scalability, and long-term effectiveness in biometric security systems.

Connections Between the Studies on AI-Driven Biometric Security

- **AI-Augmented Accuracy of Biometrics** – All the papers are concerned with the application of AI to improve recognition accuracy, decrease false acceptance/rejection rates, and pattern recognition based on models such as CNNs, SVM, and ANFIS-SC.
- **Multi-Modal Verification** – The unifying factor in all is that one biometric characteristic (e.g., fingerprints, face recognition, voice verification) is not utilized, but two or more are utilized for enhanced security, and AI is rendering their combination more powerful.
- **Privacy and Ethical Concerns** – Research identifies privacy risks, but none suggest encryption and anonymization techniques. Synthetic biometrics AI capability is security risk and strength.
- **Cybersecurity and Detection of Fraud** – AI is intensely embedded to detect fraud by behavior profiling (gait, facial recognition, keystroke dynamics), but other research warns against attacks using AI circumventing security.
- **Deployment in Real Life** – Health Care, Financial Services, Digital Identity Verification, and Law Enforcement are at the forefront as biometric authentication under AI, affordable, scalable, and regulatory friendly but yet to be researched extensively.
- **Bias and Fairness Issues** – Despite having the advantages of AI, no study does not test the bias adjustment for biometric AI models to any significant degree, an extremely important factor towards reducing fairness in security deployment.
- **Increased Research Requirement** – Studies set AI-based biometrics as the future of verification but that loopholes in field tests, cost-effectiveness, legality, and impartiality require more research.

Conflict Between the Studies on AI-Driven Biometric Security

AI Helps or Compromises Security – AI helps biometric security with better fraud prevention and reduced authentication errors (e.g., "Big Data and AI Innovations in Biometric Authentication"), whereas others advise AI against creating artificial biometrics for its use in avoiding fraud (e.g., "An Analysis of Artificial Intelligence in Biometrics").

Privacy Protection from Privacy Threats – Some of them focus on anonymization and encryption as methods of safeguarding biometric data by AI (e.g., "The Future of AI in Biometric Security"), and some mention vulnerability to storage of information and abuse of surveillance by AI (e.g., "The Role of AI and Biometrics in Identity Security").

Top AI Model for Biometric Authentication – "Biometric Information Recognition Using AI Algorithms" also ranks ANFIS-SC as the top model of biometric recognition but without juxtaposing it with other models.

Scalability and Cost Issues – Some assume biometrics based on AI to be scalable without an issue (e.g., "Enhancing Biometric Security with Artificial Intelligence"), while others cite high implementation costs, computation cost, and regulation as scalability concerns.

Ethical Challenges of AI versus Technical Impacts – Some studies reveal bias in AI-driven biometric systems but fail to provide solutions to fairness in face and fingerprint recognition. Others record technical progress only, without ethics and bias issues.

Regulatory Compliance over Lack of Regulatory Frameworks – While there are research works calling for AI-based biometric authentication to be the security future, others recommend the enforcement of stricter regulations to prevent misuse, data breach, and surveillance concerns.

Fraud Prevention vs AI-Inspired Security Threats – AI is enormously controversial as a fraud prevention solution, but there are some research papers proving that advanced AI algorithms can be utilized to bypass biometric security, and that makes AI both an enabler of security and a threat.

Synthesis Matrix for Literature Review

Study	Authors	Year	Research Design	Key Findings/Results	Methodology	Limitations
Big Data and AI Innovations in Biometric Authentication for Secure Digital Transactions	Eswar Prasad Galla, Chandrakanth Rao Madhavaram, Venkata Nagesh Boddapati	2021	Analytical Review	- AI and big data improve the security of biometric authentication. - Multi-modal biometric authentication (i.e., fingerprint + face) provides fraud prevention. - Behavioral biometrics through AI-based techniques (e.g., gait pattern and keystroke dynamics) provide an	- Review-based research on AI integration in biometric security. - Considers the application of AI and big data in fraud detection, authentication, and privacy.	- Lacks real-world case studies or empirical tests. - Does not cover economic analysis of AI-powered biometric systems. - No meaningful discussion of AI biases and ethical concerns.

					added level of security. AI models improve digital transaction fraud detection in real time.			
The Role of AI and Biometrics in Identity Security	Andrew Clarke, John Charles	2019	Conceptual & Literature Review	Biometric authentication by artificial intelligence enhances identity protection more accurately and autonomously of passwords. Fingerprint and facial recognition remain the leading most prevalent biometric identification modalities. Privacy remains the number one concern in storage and control of biometric data.	Literature review of the use and trends of biometric authentication. Industry data from reports (e.g., Gartner, Forrester) on adoption and performance in biometrics.	No empirical facts or case studies are offered. Ethics and bias in AI are referenced but not discussed. Legal and regulatory aspects of biometric security are not referenced.		
An Analysis of Artificial Intelligence in Biometrics –	Abhishek P. Iyer, Dr. J. Karthikeyan, Md. Rakibul	2020	Theoretical & Analytical	AI biometrics improve security during authentication	Survey of available AI-based biometric authentication technology.	Does not involve real-world field testing or case		

The Next Level of Security	Hasan Khan, Dr. P. M. Binu			and reduce human error. AI is at the same time a security enhancement and vulnerability (e.g., synthetic fingerprint attack). Biometric and AI-based multi-factor authentication improves security.	Examination of AI application in war, financial processing, and aviation security.	studies on current implementation. It does not have a comparison of biometric security AI models side by side. There is less emphasis on AI policy regulation and data protection.
Biometric Information Recognition Using Artificial Intelligence Algorithms: A Performance Comparison	Sunusi Bala Abdullahi, Chainarong Khunpanuk, Zakariyya Abdullahi Bature, et al.	2022	Experimental & Comparative Analysis	ANFIS-SC is better than SVM-ECOC in biometric recognition. They are capable of supporting demographic biometrics like sex, height, and foot length and enhancing recognition rate. PCC feature selection enhances the effectiveness of the AI model.	Experimental comparison of two AI models (ANFIS-SC & SVM-ECOC) with biometric recognition. The measures of efficiency are RMSE, MAPE, AICc, R ² , and NSE.	Small dataset size (112 participants), whose generalizability is compromised. Inability to incorporate actual environment factors that have an impact on biometric performance. Disable to take into account the cost aspect involved in adopting AI biometric models.

Enhancing Biometric Security with Artificial Intelligence: A Cutting-Edge Approach	Chaitanya Jain, Hardik Bhawani, Aryan Saxena	2025	Theoretical & Review-Based	AI biometric authentication enhances user convenience and access control. Deep learning and CNN greatly enhance the accuracy of biometric recognition. Ethical issues (i.e., AI bias and surveillance risks) must be addressed in biometric AI systems.	Review-based research discussing AI on various biometric modalities. Finance, healthcare, and law enforcement real-world applications discussions. Limitations:	No performance comparisons or empirical testing of AI models. No in-depth discussion of ethical issues. Does not address regulatory compliance matters with AI-powered biometrics.
The Future of AI in Biometric Security: Enhancing Authentication and Privacy Protection	Shoaib Malik	2024	Analytical & Privacy-Centric Review	AI improves biometric accuracy and fraud detection at real-time authentication. Privacy-enabling technologies (e.g., anonymization, encryption) are capable of combating AI biometric security risks. AI-driven multi-modal biometrics are the safe authentication future.	Examination of AI techniques used in biometric authentication for protection of privacy. Discussion of how AI can help in biometric encryption and secure data handling.	Lack of empirical support and real-world case studies on AI biometric security. Legal and regulatory aspects of biometric AI are not examined thoroughly. Fails to cover AI bias and fairness in biometric identification.

Reference

- 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://doi.org/10.1109/ACCESS.2022.3171850>
- Iyer, A. P., Karthikeyan, J., Khan, R. H., & Binu, P. M. (2020). An analysis of artificial intelligence in biometrics-the next level of security. In *Journal of Critical Reviews* (Vol. 7, Issue 1, pp. 571–576). Innovare Academics Sciences Pvt. Ltd. <https://doi.org/10.31838/jcr.07.01.110>
- 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.ijstat.org/papers/2025/1/1771.pdf>
- Malik, S. (2024). The Future of AI in Biometric Security: Enhancing Authentication and Privacy Protection.