IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, August 2026
Impact Factor: 8.2

A Review of Artificial Intelligence-Based Physical Biometric Authentication Systems

Sandhya Chaudhary[1] and Dr. Sankalp Mehandiratta[2]
[1]Research Scholar, Department of Computer Application
[2]Assistant Professor, Department of Computer Application
Sunrise University, Alwar, Rajasthan

Abstract : *Artificial Intelligence-based physical biometric authentication systems have emerged as important technologies for secure identity verification, access control, and digital security. These systems use unique physiological characteristics, such as fingerprints, facial features, iris patterns, palm prints, and hand geometry, to identify and authenticate individuals. Traditional biometric systems often depend on predefined feature extraction and matching techniques, whereas AI-based approaches employ machine learning, deep learning, and neural networks to improve recognition accuracy, processing speed, and adaptability. This review examines the major physical biometric authentication techniques, the role of AI in biometric feature extraction and classification, and the effectiveness of integrated multimodal authentication systems.*

Keywords: Artificial Intelligence, Deep Learning, Fingerprint Recognition, Facial Recognition, Iris Recognition, Multimodal Biometrics, Information Security.

I. INTRODUCTION

Biometric authentication is a security mechanism that verifies an individual's identity through distinctive biological characteristics. Unlike passwords, personal identification numbers, and access cards, physical biometrics are based on measurable characteristics of the human body. Fingerprints, facial features, iris patterns, and palm characteristics are among the most widely studied biometric identifiers. The increasing use of digital services and automated identity verification has encouraged the development of more accurate and intelligent biometric authentication systems.

Artificial intelligence has become particularly important because it enables computers to learn complex patterns from biometric data and distinguish genuine users from unauthorized individuals. Deep learning models, including convolutional neural networks, can automatically extract discriminative features from fingerprint images, facial images, and iris patterns, reducing dependence on manually designed features (Jain 2016; Minaee 2021). AI-based biometric authentication is increasingly relevant to mobile devices, financial transactions, border management, healthcare records, and institutional access control. However, authentication reliability depends not only on algorithmic accuracy but also on data quality, sensor characteristics, presentation attack resistance, and secure storage of biometric templates. Consequently, an effective biometric system must balance recognition performance, privacy, usability, fairness, and computational efficiency.

II. AI-BASED PHYSICAL BIOMETRIC AUTHENTICATION TECHNIQUES

Physical biometric authentication systems differ according to the human characteristics captured and analysed. Fingerprint recognition examines ridge patterns and minutiae, facial recognition identifies distinguishing facial features, and iris recognition analyses the complex texture of the iris. Palmprint recognition uses lines, creases, and texture patterns, whereas hand-geometry recognition measures characteristics such as finger length and hand dimensions.

AI algorithms can learn relevant patterns from these biometric samples and compare them with enrolled templates. Convolutional neural networks are widely used for image-based biometric recognition because they learn spatial

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, August 2026
Impact Factor: 8.2

features directly from images. Deep metric-learning approaches can also produce feature representations that improve similarity comparisons between samples of the same individual (Minaee 2023). Fingerprint systems can benefit from automated ridge and minutiae analysis, while facial systems can use deep feature embeddings to support identity verification under different lighting and pose conditions. Iris systems require careful image acquisition and segmentation because image quality directly affects the features available for classification. Nevertheless, no modality is universally superior: suitability depends on the application, sensor quality, environmental conditions, accessibility, and the consequences of false acceptance or rejection.

Biometric technique	AI application	Major advantage	Key limitation
Fingerprint recognition	CNN-based feature extraction and minutiae classification	Compact sensors and established applications	Poor-quality, worn, or damaged fingerprints
Facial recognition	Deep neural networks and feature embeddings	Contactless and convenient authentication	Lighting, pose, demographic differences, and spoofing
Iris recognition	Deep feature extraction and pattern matching	Highly discriminative iris patterns	Sensitive to capture quality and sensor alignment
Palmprint recognition	Texture analysis and deep feature learning	Uses distinctive palm lines and patterns	Requires suitable image acquisition
Hand geometry	Feature classification and dimensional analysis	Straightforward physical measurements	Less discriminative than some fine-grained traits
Multimodal biometrics	Feature, score, or decision-level fusion	Can improve robustness by combining traits	Higher cost, complexity, and privacy requirements

The literature indicates that deep learning has substantially expanded the range of methods available for biometric feature extraction and recognition. However, results from different studies should not be compared directly unless they use comparable datasets, evaluation protocols, and error definitions (Minaee 2023).

III. ROLE OF ARTIFICIAL INTELLIGENCE AND PERFORMANCE EVALUATION

Artificial intelligence supports biometric authentication through automated feature extraction, classification, matching, anomaly detection, and presentation-attack detection. Conventional machine-learning approaches, such as support vector machines and random forests, can classify engineered biometric features, while deep neural networks can learn representations from large collections of training samples. AI models may improve performance when biometric samples vary in orientation, illumination, quality, or acquisition conditions. However, performance must be evaluated through clearly defined metrics rather than accuracy alone.

1. **Accuracy:** The proportion of all authentication decisions that are correct.
2. **False Acceptance Rate (FAR):** The proportion of unauthorized attempts incorrectly accepted.
3. **False Rejection Rate (FRR):** The proportion of genuine attempts incorrectly rejected.
4. **Equal Error Rate (EER):** The operating point at which FAR and FRR are equal, based on the evaluated score distributions and threshold.
5. **Processing time:** The time required to capture, process, and verify a biometric sample.

For a binary classification evaluation, accuracy can be expressed as:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \times 100$$

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, August 2026
Impact Factor: 8.2

Here, (TP) represents true positives, (TN) true negatives, (FP) false positives, and (FN) false negatives. In biometric verification, FAR and FRR are generally calculated using genuine and impostor comparison attempts, so the precise definitions and denominators should be stated in the experimental methodology. A system may achieve high overall accuracy while still having an unacceptable false acceptance rate. Therefore, researchers should report multiple metrics, test under realistic conditions, and evaluate the consequences of different decision thresholds. Standardized evaluations, such as those conducted by the National Institute of Standards and Technology (NIST), also demonstrate the importance of examining differences in facial-recognition performance across demographic groups and image-quality conditions (Grother 2019).

IV. SECURITY CHALLENGES, PRIVACY, AND RESEARCH GAPS

Despite improvements in recognition performance, AI-based physical biometric authentication systems face significant security, ethical, and operational challenges. One major concern is presentation attacks, in which an attacker presents a photograph, artificial fingerprint, replayed image, or other imitation to deceive the authentication system. Liveness detection and presentation-attack detection mechanisms can help identify such attempts, but their effectiveness varies according to the modality, attack type, sensor, and testing conditions. Another important concern is biometric template security. Unlike passwords, biological characteristics cannot easily be replaced when compromised, making secure storage, encryption, access control, and revocable biometric representations especially important.

Deep learning systems may also exhibit demographic performance differences because of training-data imbalance, image-quality variation, and differences in the representation of population groups. NIST evaluations have documented substantial variation in facial-recognition performance across algorithms and demographic groups, reinforcing the need for independent testing rather than assuming that all AI systems perform equally (Grother 2019).

Privacy is another central issue because biometric information is highly personal and can enable identity tracking when used without appropriate safeguards. Researchers should consider informed consent, purpose limitation, data minimization, secure transmission, controlled retention, and compliance with applicable data-protection requirements. Further research is needed to develop lightweight AI models for resource-constrained devices, improve cross-sensor generalization, strengthen resistance to deepfake and spoofing attacks, and evaluate systems under realistic operating conditions.

Explainable AI may help investigators understand model decisions, while privacy-preserving approaches may reduce the exposure of raw biometric information. However, these methods require rigorous validation to ensure that privacy improvements do not undermine authentication reliability. Arora and Bhatia (2022) discuss the broader security and privacy challenges associated with biometric systems, including the need for robust algorithms and improved resistance to spoofing.

V. MULTIMODAL AUTHENTICATION AND FUTURE RESEARCH DIRECTIONS

Multimodal biometric authentication combines two or more biometric characteristics, such as fingerprints and facial features, to strengthen identity verification. Information from multiple modalities may be combined at the feature, score, or decision level. Feature-level fusion integrates extracted representations, score-level fusion combines matching scores, and decision-level fusion combines the final outputs of individual classifiers. The main advantage is that a weakness in one modality may be partly compensated for by another, depending on the quality and independence of the signals.

For example, a fingerprint system affected by a damaged finger may use facial verification as an additional authentication factor. However, multimodal systems also introduce higher computational costs, more complex integration, additional sensors, and greater privacy-management requirements. A systematic review of continuous multimodal biometric authentication found that evaluation often emphasizes recognition accuracy while giving less attention to usability, scalability, and security in practical deployment (Tolosana 2021).

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, August 2026
Impact Factor: 8.2

Future research should prioritize robust multimodal fusion, reliable liveness detection, fairness evaluation, secure template protection, and energy-efficient AI architectures. Researchers should test models across diverse demographic groups, devices, lighting conditions, and attack scenarios. Standardized datasets and independent benchmarking are essential for meaningful comparison between competing approaches. Further opportunities include federated learning, privacy-preserving model training, and edge-based authentication, provided that these techniques are assessed for both security and performance. The ultimate objective should not be to maximize accuracy alone but to develop systems that offer reliable identity verification while protecting users' rights, personal information, and accessibility.

VI. CONCLUSION

Artificial intelligence has significantly expanded the capabilities of physical biometric authentication by enabling automated feature extraction, improved pattern recognition, and more flexible identity verification. Fingerprint, facial, iris, palmprint, and hand-geometry recognition each provide useful authentication options, but their effectiveness depends on the application, data quality, sensor performance, and security requirements. Deep learning models can improve recognition capabilities, while multimodal approaches offer opportunities to strengthen verification by combining complementary biometric characteristics.

Nevertheless, spoofing attacks, template theft, demographic bias, privacy risks, and computational complexity remain important limitations. A reliable biometric authentication framework must therefore integrate AI algorithms with secure data management, liveness detection, transparent performance evaluation, and appropriate privacy safeguards. Future research should emphasize real-world testing, fairness, explain ability, lightweight computation, and standardized evaluation procedures. In conclusion, AI-based physical biometric authentication systems have considerable potential to improve digital and physical security, but their long-term effectiveness depends on balancing recognition performance with security, fairness, privacy, and responsible implementation.

REFERENCES

1. Arora, S., & Bhatia, M. P. S. (2022). Challenges and opportunities in biometric security: A survey. Information Security Journal: A Global Perspective, 31(1), 28–48.
2. Grother, P., Ngan, M., & Hanaoka, K. (2019). Face recognition vendor test (FRVT) part 3: Demographic effects (NIST Interagency/Internal Report 8280). National Institute of Standards and Technology.
3. Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4–20.
4. Minaee, S., Abdolrashidi, A., Su, H., Bennamoun, M., & Zhang, D. (2023). Biometrics recognition using deep learning: A survey. Artificial Intelligence Review, 56(8), 8647–8695.
5. Chiroma, H. (2021). Deep learning algorithms based fingerprint authentication: Systematic literature review. Journal of Artificial Intelligence and Systems, 3, 157–197.
6. Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Morales, A., & Ortega-Garcia, J. (2021). Continuous multimodal biometric authentication schemes: A systematic review. IEEE Access, 9, 34541–34557.