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 3, September 2026
Impact Factor: 8.2

Role of Deep Learning in Improving Physical Biometric Authentication Accuracy

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 : *Physical biometric authentication has become an important technology for identity verification in smartphones, banking systems, healthcare institutions, border security, and digital access-control applications. Traditional biometric authentication methods rely on manually designed features and conventional pattern-recognition algorithms, which may experience limitations under variations in lighting, image quality, sensor characteristics, facial expressions, fingerprint conditions, and environmental factors. Deep learning provides advanced computational techniques for automatically extracting complex features from biometric data and improving the reliability of identity verification.*

Keywords: Deep Learning, Physical Biometrics, Iris Recognition, Convolutional Neural Networks, Multimodal Biometrics.

I. INTRODUCTION

Biometric authentication is a method of verifying an individual's identity using distinctive physiological characteristics, including fingerprints, facial features, iris patterns, and palmprints. Unlike passwords and personal identification numbers, biometric characteristics are directly associated with an individual's physical identity, making them valuable for convenient identity verification.

However, biometric systems must distinguish between genuine users and unauthorized individuals under diverse operational conditions. Conventional recognition approaches frequently depend on manually engineered features, predefined thresholds, and traditional classification algorithms.

Their performance may decline when biometric samples are incomplete, noisy, poorly illuminated, distorted, or captured using different sensors. Deep learning has emerged as a significant development in biometric recognition because it enables models to learn complex representations directly from large collections of training data. Minaee et al. (2023) reviewed deep learning applications across several biometric modalities, including face, fingerprint, iris, palmprint, and ear recognition, demonstrating the breadth of this research area.

CNNs are particularly useful for processing biometric images because they learn spatial patterns, edges, textures, and distinctive local features. In fingerprint authentication, these representations can help identify ridge structures and minutiae. In facial recognition, deep neural networks can learn discriminative facial representations that remain useful despite moderate changes in expression and appearance.

Similarly, deep learning techniques support iris segmentation and recognition by extracting informative patterns from iris images (Nguyen 2024). Nevertheless, higher classification accuracy does not automatically guarantee stronger security. A reliable authentication system must also control false acceptance, minimize false rejection, detect presentation attacks, and protect biometric templates against misuse. Therefore, this research examines deep learning as a means of improving both recognition accuracy and practical authentication reliability.

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 3, September 2026
Impact Factor: 8.2

II. LITERATURE REVIEW

Existing research demonstrates growing interest in applying deep learning to biometric identification and verification. Minaee et al. (2023) presented a comprehensive survey of deep learning-based biometric recognition, examining different modalities, datasets, model architectures, and research challenges. Their work indicates that deep neural networks have become important tools for learning discriminative biometric features and improving recognition performance across a range of applications. Chiroma (2021) reviewed deep learning algorithms for fingerprint authentication and discussed CNN-based feature extraction, classification, and end-to-end learning approaches. This research highlights the importance of selecting appropriate network architectures and training strategies for fingerprint recognition.

Chowdhury and Imtiaz (2022) reviewed contactless fingerprint recognition using deep learning and discussed the potential of learning-based approaches to address challenges associated with contact-based fingerprint acquisition. Contactless systems offer convenience, but variations in finger position, distance, illumination, and image quality can affect recognition outcomes. Nguyen et al. (2024) reviewed deep learning for iris recognition, covering segmentation, feature extraction, recognition, and presentation-attack-related challenges. Their study provides evidence of the expanding use of deep learning throughout the iris-recognition pipeline.

Shaheed et al. (2024) examined deep learning techniques for biometric presentation-attack detection, including methods designed to identify fraudulent attempts involving different biometric modalities. This area is important because a system may correctly recognize biometric patterns in ordinary conditions while remaining vulnerable to manipulated samples. Overall, the literature suggests that deep learning can improve feature representation and biometric matching, but comparisons between studies require careful interpretation because datasets, evaluation procedures, and performance measures differ.

III. RESEARCH METHODOLOGY

The present study adopts a descriptive and qualitative literature-review methodology to investigate the role of deep learning in improving physical biometric authentication accuracy. The research is based on secondary information obtained from peer-reviewed journal articles, systematic reviews, conference publications, and established academic research on biometric recognition. Relevant literature was identified through sources including IEEE Xplore, Springer, the Association for Computing Machinery (ACM), and other scholarly publication platforms. The review focuses primarily on research published between 2010 and 2024, with particular attention to recent developments in deep learning-based authentication.

The literature was examined according to five principal dimensions: biometric modality, deep learning architecture, feature extraction strategy, authentication performance, and security limitations. Fingerprint, facial, iris, and palmprint recognition were selected because they represent important forms of physical biometric authentication. CNNs, deep metric learning, and transformer-based architectures were considered in relation to their ability to learn discriminative representations and improve matching performance.

The principal evaluation measures considered in the study include accuracy, FAR, FRR, and EER. Accuracy measures the proportion of correctly classified samples, whereas FAR measures the proportion of unauthorized attempts incorrectly accepted and FRR measures the proportion of genuine attempts incorrectly rejected. EER represents the operating point at which FAR and FRR are equal. The study also considers robustness to image degradation, presentation attacks, variations in demographic characteristics, and differences between training and deployment environments.

As this paper is a literature-based review rather than a newly conducted experiment, it does not claim original laboratory measurements, a newly collected dataset, or experimentally verified accuracy improvements. Its findings are based on a qualitative synthesis of published research. Differences in datasets and evaluation protocols are considered when interpreting the reported benefits of deep learning.

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 3, September 2026
Impact Factor: 8.2

IV. DEEP LEARNING TECHNIQUES AND THEIR IMPACT ON AUTHENTICATION ACCURACY

Deep learning improves biometric authentication by learning informative representations from biometric samples and using these representations to distinguish genuine users from impostors. Different architectures provide different advantages depending on the modality, quality of the input data, and authentication requirements.

Table 1. Deep learning techniques used in physical biometric authentication

Deep learning technique	Application	Contribution to accuracy
Convolutional Neural Networks (CNNs)	Fingerprint, face, iris, palmprint	Learn spatial patterns and distinctive image features.
Deep metric learning	Face and fingerprint verification	Learns embedding spaces that separate genuine and impostor samples.
Transformer-based models	Facial and iris recognition	Capture relationships among features across different image regions.
Autoencoders	Biometric feature representation and quality assessment	Learn compact representations and may support detection of unusual samples.
Multimodal deep learning	Face, fingerprint, iris combinations	Combines complementary biometric information to improve reliability.
Deep learning-based presentation-attack detection	Face, fingerprint, iris	Helps identify spoofed samples and strengthens authentication security.

Source: Prepared by the author from the literature reviewed, including Chiroma (2021), Minaee et al. (2023), Chowdhury and Imtiaz (2022), and Shaheed et al. (2024). The table summarizes potential functions, not a controlled numerical comparison.

CNNs are widely applied to biometric images because their layered structure can learn increasingly complex visual features. In fingerprint recognition, early layers may identify local ridge patterns, while deeper layers can represent more complex structures. These learned features can improve the differentiation of fingerprint samples, especially when supported by adequate training data and suitable preprocessing. Chiroma (2021) discusses CNNs in fingerprint authentication as feature extractors, classifiers, and components of end-to-end learning systems.

Facial recognition systems use deep neural networks to produce numerical representations of facial images. Deep metric learning can make representations of the same person more similar while separating representations belonging to different people. This approach can support verification across changes in facial expression, pose, and image quality, although performance depends on the model, training data, and deployment conditions. Transformer-based architectures provide another approach by modelling relationships between different image regions. Their usefulness depends on appropriate training, computational resources, and the characteristics of the target dataset.

Iris recognition presents different technical challenges because accurate segmentation and feature extraction are essential for identifying distinctive iris patterns. Deep learning can support both segmentation and recognition, reducing dependence on manually designed image-processing pipelines. Nguyen et al. (2024) discuss these tasks and the continuing challenges of iris recognition. Similarly, multimodal biometric systems combine two or more physical traits to compensate for weaknesses associated with individual modalities. When the selected traits provide complementary information, fusion may improve authentication reliability. However, multimodal processing can increase computational costs, data-storage requirements, and privacy risks.

IV. PERFORMANCE EVALUATION, CHALLENGES, AND DISCUSSION

The effectiveness of deep learning-based biometric authentication should be assessed through multiple performance indicators rather than overall accuracy alone. A system that correctly classifies most samples may still be unsuitable for high-security applications if it accepts unauthorized users too frequently. FAR and FRR therefore provide important complementary measures. EER allows researchers to compare verification systems at a common error operating point, although application-specific operating thresholds remain important. Evaluation should also distinguish between

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 3, September 2026
Impact Factor: 8.2

verification, which compares a claimed identity against a stored template, and identification, which searches across multiple identities.

Table 2. Major factors affecting biometric authentication performance

Factor	Potential effect	Recommended approach
Training dataset size	Insufficient samples may limit feature learning.	Use adequate, representative training data.
Image and sensor quality	Noise and distortion can reduce matching reliability.	Apply quality assessment and appropriate preprocessing.
Demographic variation	Performance may differ across population groups.	Conduct subgroup-based evaluation.
Environmental conditions	Lighting, pose, and acquisition differences can affect recognition.	Test under realistic operating conditions.
Presentation attacks	Fraudulent samples may be incorrectly accepted.	Integrate presentation-attack detection.
Computational requirements	Complex models may increase latency and energy use.	Optimize inference and model size.
Biometric privacy	Templates may expose sensitive identifying information.	Use encryption, access controls, and privacy-preserving methods.

Source: Author's synthesis of the reviewed literature, including Minaee (2023) and Shaheed (2024).

A major advantage of deep learning is its capacity to learn complex patterns that traditional handcrafted approaches may not capture effectively. Nevertheless, its performance depends on the representativeness of the training data and the similarity between training and deployment conditions. For example, a facial-recognition model trained primarily on well-lit images may experience degraded performance under poor illumination. Likewise, fingerprint recognition may become less reliable when the acquired sample is incomplete or distorted. These issues demonstrate why reported benchmark results should not be treated as universal indicators of real-world performance.

Security is another essential consideration. Deep learning-based presentation-attack detection can help identify fraudulent biometric samples, but attackers may adapt their methods to exploit weaknesses in recognition pipelines. Therefore, authentication and anti-spoofing components should be evaluated together. The use of multimodal biometrics can provide additional evidence during verification, but it does not automatically eliminate spoofing or guarantee a lower error rate.

Privacy and fairness also influence practical effectiveness. Biometric information is difficult to replace if compromised, making secure template storage and restricted access particularly important. Furthermore, performance should be examined across demographic groups and different acquisition conditions to identify systematic errors. Future research should emphasize independent testing, cross-dataset validation, transparent reporting, computational efficiency, and privacy-preserving learning. These measures can help establish whether improvements observed in laboratory settings translate into dependable authentication systems in real-world applications.

V. CONCLUSION

Deep learning has made an important contribution to the development of physical biometric authentication by enabling systems to learn complex features and distinguish individuals more effectively. CNNs, deep metric learning, transformer-based models, and multimodal learning approaches offer promising solutions for fingerprint, facial, iris, and palmprint recognition. The reviewed literature indicates that these techniques can improve feature extraction, matching reliability, and the ability to process variations in biometric samples (Nguyen 2024). Deep learning-based presentation-attack detection also contributes to security by helping identify fraudulent biometric samples (Shaheed 2024).

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 3, September 2026
Impact Factor: 8.2

However, improvements in authentication accuracy depend on dataset quality, model architecture, evaluation procedures, and operational conditions. High benchmark accuracy alone does not establish that a system is secure, fair, or reliable in every real-world environment. Therefore, biometric authentication should be evaluated using multiple indicators, including accuracy, FAR, FRR, EER, computational efficiency, and resistance to presentation attacks. Future research should focus on representative datasets, demographic fairness, privacy-preserving learning, lightweight architectures, and standardized testing. The integration of complementary biometric modalities may further improve reliability when implemented with appropriate security safeguards. In conclusion, deep learning offers substantial potential for improving physical biometric authentication, but its practical success requires a balanced approach that combines recognition accuracy, security, privacy, fairness, and operational efficiency.

REFERENCES

1. Chiroma, H. (2021). Deep learning algorithms-based fingerprint authentication: Systematic literature review. Journal of Artificial Intelligence and Systems, 3, 157–197.
2. Chowdhury, A. M. M., & Imtiaz, M. H. (2022). Contactless fingerprint recognition using deep learning A systematic review. Journal of Cybersecurity and Privacy, 2(3), 714–730.
3. 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.
4. Nguyen, K., Proença, H., & Alonso-Fernandez, F. (2024). Deep learning for iris recognition: A survey. ACM Computing Surveys, 56(9), Article 223, 1–35.
5. Shaheed, K., Szczuko, P., Kumar, M., Qureshi, I., Abbas, Q., & Ullah, I. (2024). Deep learning techniques for biometric security: A systematic review of presentation attack detection systems. Engineering Applications of Artificial Intelligence, 129, Article 107569.