Integration of Cyber Security and Artificial Intelligence in Fingerprint Recognition Systems using Convolutional Neural Networks

Muhamad Zafri Wahab 1, a), Nur Erlida Ruslan1, 2, b) and Su-Cheng Haw1, 3, c)

*1Faculty of Computing and Informatics, Multimedia University, Persiaran Multimedia, Cyberjaya, 63100, Malaysia*

*2Centre of Image and Vision Computing, CoE of Artificial Intelligence, Multimedia University, Persiaran Multimedia, Cyberjaya, 63100, Malaysia*

*3Centre for Digital Innovations, CoE of Immerse Experience, Multimedia University, Persiaran Multimedia, Cyberjaya, 63100, Malaysia*

*b) Corresponding author: nurerlida@mmu.edu.my  
a) 1221301781@student.mmu.edu.my*

*c) sucheng@mmu.edu.my*

**Abstract.** This review paper examines the integration of cybersecurity and artificial intelligence (AI) in fingerprint recognition systems with a specific focus on the use of convolutional neural networks (CNNs). These technological innovations aim to tackle complicated security risks such as spoofing, adversarial attacks, and other difficulties related to present systems. The rise of mobile and IoT platforms has made personal biometric data especially fingerprints a tempting target for hackers. Such data is irreplaceable once exposed. History shows even minor security oversights can lead to months or years of damage control. Computer vision specialists often default to convolutional networks because they automatically spotlight relevant features and cope surprisingly well with noisy or rotated prints. These networks reveal intricate hierarchies of detail and catching the fine valleys and ridges that distinguish one finger from another. Unfortunately, that power comes at a price like high compute demand, enormous annotation chores, and a stubborn inability to generalize across the mixed bag of sensors now on the market. Researchers are countering by downsizing models and experimenting with privacy-hardened pipelines such as federated learning (FL) and cancellable biometrics. By training in separate divisions or quickly eliminate prints, they prevent raw templates from ever interacting. with a public network. The present manuscript reviews this emerging toolkit, compiles the insights gained, and highlights protocols for integrating rapid AI progress with the resilient cyber defenses that large-scale fingerprint systems will inevitably need.

# INTRODUCTION

Researchers started combining AI with cybersecurity in ways that focus on next-generation fingerprint scanners. The topic is both urgent and timely given that cyber attackers no longer settle for phishing emails and also they investigate biometric vaults and client databases. Experts treated fingerprint data as durable evidence of identity but yet scanners must now defend that evidence from pixel-perfect counterfeits well before machine learning (ML) arrived. CNNs shine by stripping away irrelevant background noise and recognize pore patterns almost as quickly as they are collected. Every network still needs memory that is as good as a small weather station, and smart hackers keep coming up with new ways to mess with the feature maps, even though they are strong. Recent publications warn that speed without supplementary encryption is a formula for exploitation and researchers are developing models that place robust security measures next to the CNN classifiers. This review assembles ongoing upgrades while defining areas where journals show an unmarked surface and ultimately proposes a hybrid architecture that integrates rapid identification with protections against digital tampering.

Fingerprint recognition technology has evolved significantly over the past several years. Older systems relied mainly on classic image-processing methods that pin-pointed key features such as ridge endings and bifurcations using minutiae- and ridge-based algorithms [1]. Classic biometric algorithms remain popular because their low computational cost and long-standing presence in the field create a reassuring sense of operational comfort. The same simplicity lays bare to a host of weaknesses, blurred input images, sudden shifts in lighting, and crafty spoofing attempts where frequently inflate the False Acceptance Rate (FAR) and ultimately compromise system security. [2][3]. Minutiae-based fingerprint analysis frequently fails when confronted with low-resolution scans and unexpected distortion. Such artifacts dilute the clarity of ridge structure and obstruct system consistency [3]. A number of recent investigations have turned to ML algorithms especially CNNs to improve liveness detection and strengthen resistance to spoofing attacks [2]. Recent studies have exposed a significant blind spot in the assessment of CNN fingerprint readers. In field trials involving deliberate spoofing and sensor tampering where even state-of-the-art models proved remarkably breakable. The incidents underline the necessity of stress-testing biometric systems under genuinely hostile conditions before deploying them. Robust countermeasures can be designed and validated only once that baseline vulnerability is clearly established [4]. The application of FL for privacy-preserving model training in biometric systems is unexplored despite its potential to protect sensitive user data as noted by Phong et al. [5]. A major problem is the scalability of fingerprint recognition solutions for edge devices including smartphones and Internet of Things (IoT) platforms which remain poorly addressed in the current literature [6]. Although advanced encryption techniques such as homomorphic encryption (HE) present significant promise for the protection of biometric templates, their application within fingerprint security systems remains limited [7]. Findings emphasize the necessity for an integrated approach that merges the advantages of traditional fingerprint recognition with modern DL, privacy-preserving methods, and strong encryption to create reliable, safe, and scalable biometric systems.

## Modern AI-Driven Methods

Modern AI-based fingerprint recognition techniques utilize deep learning (DL) to improve feature extraction and classification within the field of biometrics. DL techniques especially CNNs demonstrate enhanced proficiency in learning structures that effectively capture complicated fingerprint details going over traditional feature engineering methods [8][9]. In contrast to traditional ML models like support vector machines (SVMs) and Random Forests, CNNs autonomously extract key characteristics from raw fingerprint images. This capability reduces the reliance on manual preprocessing and enhances resilience to variations and spoofing attacks [10][11].  Recent studies demonstrate that AI-driven approaches improve classification accuracy and enhance spoof detection capabilities which address vulnerabilities related to conventional systems [12][13]. The integration of DL into fingerprint recognition systems indicates a significant advancement in biometric authentication by enhancing reliability and security as supported by extensive literature reviews [14].

## Challenges and Research Opportunities

Fingerprint recognition systems face various challenges along with opportunities for further study. Distortions such as noisy inputs, incomplete fingerprints, and sensor variability routinely undermine the reliability of biometric match scores [1][13]. The problems outlined point directly to a demand for robust image-enhancement routines and dynamically adjustable feature-extraction methods. Biometric information by its very character raises maintaining authenticity and privacy during both storage and use. Researchers insist on tightly enforced data-governance schemes paired with privacy-preserving technologies to counter the threat of abuse and unauthorized surveillance [15]. Significant gaps persist in making biometric systems truly adversarial-proof and able to process input in real time. Most studies call for new algorithms that not only dismiss spoofing and manipulation attempts but also deliver fast and reliable authentication. [1][13].  In the end, progressing on reliable fingerprint scanners comes down to tackling stubborn technical, ethical, and sharpening the research methods used [15].

# Role of Convolutional Neural Networks

CNNs have greatly improved fingerprint analysis by learning strong hierarchical representations directly from raw image data which means they don't have to rely on hand-crafted features. [9]. CNNs are much better at handling things like background noise or missing parts of a print than older algorithms. That greater resilience leads to more accurate fingerprint sorting and matching results [10]. CNN-based methods work better on standard datasets like NIST DB4 [16]. Specialised architectures like PoreNet also help get high-resolution details out of the data [8]. Systematic reviews show that CNNs are an important part of fingerprint authentication because they solve problems with spoof detection and image degradation [13]. CNNs offer a powerful and scalable way to recognise fingerprints that meet modern biometric security standards [10][13].

## Fundamentals of CNN in Image Processing

The strength of CNNs comes from their modular and stacked design. A bank of trained kernels scans the image in each convolutional block and revealing local features like edges, colour shifts, and grainy textures. Interconnected pooling stages then shrink the representation and keep the important parts still across small translations [10]. Activation functions like ReLU add non-linear transformations which makes it easier for the network to model complex data distributions. This architecture allows CNNs to acquire strong hierarchical features and rendering them especially effective for biometric pattern recognition.  CNNs effectively capture complex information in fingerprint images by reducing the necessity for extensive manual feature engineering and enabling precise classification despite data variations and noise [9].  Deep architectures show higher resistance to distortions and enhanced performance in biometric applications as highlighted in extensive surveys on DL for biometrics [14].

## CNN Architectures Applied in Fingerprint Recognition

CNN architecture utilized in fingerprint recognition incorporates both traditional designs and customized changes to improve feature extraction. Early architectures such as LeNet and AlexNet created essential frameworks that enable the extraction of local features critical for fingerprint analysis. ResNet improves the training of deep networks through the introduction of residual connections and enhancing the ability to capture complex fingerprint details as pointed out in the survey [10].  Inception networks utilize parallel convolutional filters to acquire multi-scale representations which are crucial for identifying fine minutiae patterns. MobileNet effectively addresses computational constraints by making it suitable for deployment in environments with limited resources. Custom CNNs designed for small-scale biometric datasets as shown in fingerprint classification experiments [9], optimize network parameters to achieve a balance between model complexity and available training data leading to robust and efficient biometric systems.

Table 1 shows the advantages of LeNet, ResNet, and MobileNet when it comes to image classification. LeNet is one of the first convolutional networks and it is still popular because it is simple and works well on hardware with low specs. ResNet solves the common problem of vanishing gradients by adding skip connections between layers. This lets it stack hundreds of blocks without losing representational power. This same feature also lets it do well on datasets with very complex visuals. MobileNet is a new way to do things for mobile and edge scenarios. It uses depth-wise separable convolutions which make the model smaller while still giving good accuracy even when latency is low. Practitioners can choose the one that fits their processing budget and error-tolerance margin by knowing what each architecture is good at. They can get the best performance possible within reasonable limits.

|  |  |  |
| --- | --- | --- |
| **TABLE 1.** Accuracy of the various models | | |
| **Pre-Trained Model** | **Accuracy** | **Loss** |
| MobileNetV2 | 87.72 | 0.4119 |
| ResNet | 96.74 | 0.2659 |
| LeNet | 96.52 | 0.2097 |

## Feature Extraction and Classification

Fingerprints can now be analysed by CNNs without the need for human experts. Networks automatically learn to identify the broad ridge flow and more difficult minutiae points by stacking successive convolutional layers. Operators are relieved of manual annotation tasks and feature extraction is improved by this layered self-learning process [8]. Traditional handcrafted systems rely on the difficult and inflexible process of carefully engineering local feature sets and fixed rules. CNNs quickly adapt to changes in ambient noise and fingerprint clarity. The ability to resolve minute details and fine pore structures qualities is necessary for accurate matching which has been demonstrated by recent architectures like PoreNet [8]. CNNs can be integrated directly into the fingerprint recognition pipeline through custom architectures and combining feature collection and decision-making into a single module. Notable improvements in processing speed and accuracy are frequently the result of such integration [9]. This comprehensive approach reduces errors from individual preprocessing steps and shows greater accuracy than traditional techniques because of the existence of distortions and partial impressions according to recent systematic reviews [13]. CNNs have become essential in the advancement of fingerprint biometric systems.

## Performance Metrics and Evaluation

Fingerprint-recognition systems use performance metrics to see how well they can tell the difference between real users and fakes and to prove identity claims. Accuracy, precision, recall, and F1-score are the most common metrics. They turn the classifier's raw output into a single number that can be accepted [13]. False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (ERR) are the three benchmark measures that give modern biometric systems the ability to evaluate. FAR measures how often an unauthorised user is let in by mistake and FRR measures the opposite which is how often a legitimate user is kept out by mistake. EER is where these two curves meet. It gives a single number that shows the overall accuracy and lets you compare different technologies directly [12]. Ongoing research into DL and CNN architectures for biometric assessment shows big improvements in accuracy. Better feature harvesting and stronger classification routines are the reasons why failure rates are lower across many modalities [13]. These metrics allow researchers to benchmark system performance against traditional methods and notify improvements in biometric security frameworks.

# Integration of Cybersecurity in Biometric Systems

Biometric systems are using cybersecurity principles to keep sensitive data safe and make strong authentication systems. These systems use AI and CNN-based methods that combine strong encryption and anomaly detection methods [17]. The combined architecture makes sure that biometric samples are stored, sent, and processed in an encrypted state. This safety measure makes it much less likely that they will be stolen or tampered. Khaw's methodical reviews provide comprehensive cybersecurity blueprints that offer a tested framework for adding access controls and real-time threat monitoring [18]. Multimodal biometric systems that combine fingerprints with other identifiers improve security by using multiple layers [3]. A well-designed multimodal architecture protects the core integrity of the biometric system, even if one input source is damaged. The combination of AI, CNNs, and cybersecurity architectures creates a strong framework that makes biometric data more accurate and makes defences against new cyber threats stronger.

## Proposed Hybrid Architecture for Secure Fingerprint Recognition

This study suggests a hybrid architecture that integrates CNNs, encryption, and FL to improve security and efficiency in fingerprint recognition systems. The system starts by collecting fingerprints using optical or contactless sensors which are the main way to collect biometric data. Next, an image enhancement module reduces residual noise and divides the image into separate areas. This step is configured to give the CNN architecture clean input. The CNN-based feature extraction phase learns and extracts hierarchical patterns from the fingerprint image on its own such as ridges and minutiae. This means that less manual feature engineering is needed. The gathered features are then turned into secure biometric templates using HE and cancelable biometrics. This makes sure that the data is safe while it is being processed or stored. The encrypted templates use FL to process data which matching happens on user devices without sending raw data. Only model updates are properly shared and combined which lets the whole system get better while still protecting user privacy and following the GDPR law. This layered approach makes sure that the system is accurate and can grow while protecting privacy and keeping people safe from spoofing and other types of attacks.

## Threats in AI-Based Fingerprint Recognition

Fingerprint recognition systems that use AI are facing more complex threats. Spoofing attacks which involve the creation of counterfeit fingerprints to mislead the system continue to be a significant concern. Advanced generative adversarial network techniques can generate highly realistic counterfeit fingerprints which pose challenges to liveness detection mechanisms [12]. Replay attacks characterized by repeated use of previously intercepted authentic fingerprint data present a significant risk to system integrity. Adversarial ML attacks increase these vulnerabilities by introducing deliberately designed changes into the input data which can mislead algorithms and result in incorrect decisions [12]. Manipulated inputs even with minimal distortion can bypass security protocols and reducing the reliability of fingerprint recognition systems. These threats highlight the necessity for ongoing research into effective countermeasures including advanced training techniques, anomaly detection frameworks, and enhanced spoof resistance to protect AI-based biometric authentication systems [12].

## Biometric Template Protection Techniques

Biometric template protection techniques are essential for protecting the confidentiality and integrity of fingerprint data throughout storage, transport, and processing. Cancelable biometrics utilize noninvertible transformations on fingerprint data, enabling cancellation and replace of compromised templates without decreasing recognition efficacy. Biometric cryptosystems, shown by the fuzzy vault scheme, enhance security by connecting fingerprint characteristics with cryptographic keys, thereby blocking the extraction of raw biometric data even in the event of template theft. Furthermore, fundamental hash encryption may conceal collected features, therefore reducing the possibility of reverse engineering. These strategies are especially crucial for features obtained from CNNs which are recognized for being vulnerable to adversarial changes and inversion attacks.

Advanced encryption techniques are essential for modern biometric security systems. HE attracts attention as an innovative method that enables calculations on encrypted data without decryption and thereby protecting user privacy while ensuring operational efficacy [7]. FL protects data privacy by spreading the model-training task across many devices instead of putting all the data in one place. Users’ biometric records are still locked on the phone they came from but their contributions still help make a global model better [18]. AI has made authentication more reliable and flexible by giving users a lot of protection against new cyber threats [19]. The integration of AI, advanced encryption, and FL is a big step forward in making biometric systems safer in many fields.

## Enhancing Security with AI Techniques

Recent improvements in CNN-based biometric technology seem promising for making systems safer from spoofing and new cyber threats. The models automatically find features that set real fingerprint images apart from fake ones by training these networks on large datasets. Specialised setups like the Deep Convolutional Generative Adversarial Network (DCGAN) have shown that they can pick up on even the smallest differences in texture and structure between real and fake samples which greatly improves the overall accuracy of classification [12]. Transfer learning techniques increase resilience to different spoofing techniques and shorten training times by employing pre-trained CNN models on fingerprint datasets to improve liveness detection [20]. New anomaly detection algorithms are currently being added to biometric infrastructures by researchers. These methods flag changes from normal fingerprint paths which can help prevent network breaches before they happen [17]. Combining CNNs with a broad-spectrum intrusion detection system creates a multi-tiered security architecture. In that design, unexpected biometric readings set off extra countermeasures that make fingerprint authentication pipelines stronger when they are attacked by advanced enemies.

# Conclusion

The combination of DL techniques and cybersecurity measures has greatly improved fingerprint recognition systems. This is shown by the use of CNNs which it let feature extraction from raw fingerprint images happen automatically and reliably. This improvement has greatly decreased the system's need for handcrafted features while also making it better at accurately classifying ridge patterns and minutiae points. Fundamental challenges such as diminished image quality, the influence of noisy inputs, and sensor variability consistently affect matching accuracy and reliability. The growing risk of spoofing attacks and hostile manipulations underscores the necessity for complex algorithms that protect biometric systems and enhance comprehensive cybersecurity frameworks [21].

Both performance and security must be taken into account when developing biometric authentication for cybersecurity. This involves in improving fingerprint recognition through DL and integrating adaptive security measures capable of mitigating emerging threats [22],[23]. These approaches need to be combined for identity management systems to be strong enough to deal with cybersecurity risks [2]. Future research should be focused on developing innovative DL strategies to tackle current challenges in biometric authentication while simultaneously enhancing cybersecurity measures that ensure both quicker and accurate authentication processes [13].

# References

1. S. F. Ali, M. A. Khan, and A. S. Aslam, “Fingerprint matching, spoof and liveness detection: classification and literature review,” Front. Comput. Sci. **15**(1), 151310 (2021).
2. A. A. Talabi, O. B. Longe, A.A. Muhammad, and K. Olusanya, “Cybersecurity Risk Management in Identity Systems using Biometric-based Multimodal Authentication.,” in *Proceedings of the 28th iSTEAMS Multidisciplinary & Inter-Tertiary Research Conference*, (Society for Multidisciplinary and Advanced Research Techniques - Creative Research Publishers, 2021), pp. 61–88.
3. D. R. Tripathi, and D. K. Nishad, “Biometric Authentication Systems: A Survey,” TURCOMAT **11**(3), 2878–2884 (2020).
4. A. Galli, M. Gravina, S. Marrone, D. Mattiello, and C. Sansone, “Adversarial liveness detector: Leveraging adversarial perturbations in fingerprint liveness detection,” IET Biometrics **12**(2), 102–111 (2023).
5. L. T. Phong, T. T. Phuong, L. Wang, and S. Ozawa, “Frameworks for Privacy-Preserving Federated Learning,” IEICE Trans. Inf. & Syst. **E107.D**(1), 2–12 (2024).
6. Z. Yang, M. Chen, W. Saad, M. Shikh-Bahaei, H.V. Poor, and S. Cui, “Federated Learning in 6G Mobile Wireless Networks,” in *6G Mobile Wireless Networks*, edited by Y. Wu, S. Singh, T. Taleb, A. Roy, H.S. Dhillon, M.R. Kanagarathinam, and A. De, (Springer International Publishing, Cham, 2021), pp. 359–378.
7. W. Yang, S. Wang, H. Cui, Z. Tang, and Y. Li, “A Review of Homomorphic Encryption for Privacy-Preserving Biometrics,” Sensors **23**(7), 3566 (2023).
8. V. Anand, and V. Kanhangad, “PoreNet: CNN-based Pore Descriptor for High-resolution Fingerprint Recognition,” IEEE Sensors J., 1–1 (2020).
9. M. Hirsi Mohamed, “Fingerprint Classification Using Deep Convolutional Neural Network,” JEEE **9**(5), 147 (2021).
10. M. Krichen, “Convolutional Neural Networks: A Survey,” Computers **12**(8), 151 (2023).
11. E. Y. Boateng, J. Otoo, and D. A. Abaye, “Basic Tenets of Classification Algorithms K-Nearest-Neighbor, Support Vector Machine, Random Forest and Neural Network: A Review,” JDAIP **08**(04), 341–357 (2020).
12. J. Jenkins, and K. Roy, “Exploring deep convolutional generative adversarial networks (DCGAN) in biometric systems: a survey study,” Discov Artif Intell **4**(1), 42 (2024).
13. H. Chiroma, “Deep Learning Algorithms based Fingerprint Authentication: Systematic Literature Review,” AIS **3**(1), 157–197 (2021).
14. S. Minaee, A. Abdolrashidi, H. Su, M. Bennamoun, and D. Zhang, “Biometrics recognition using deep learning: a survey,” Artif Intell Rev **56**(8), 8647–8695 (2023).
15. E. Al. Muhammad Saad Zahoor, “Biometric Encryption: Integrating Artificial Intelligence for Robust Authentication,” Dxjb **35**(3), 25–33 (2023).
16. R. Lakshmi Mallela, S. Kamepalli, S. Naga Sandhya Guttula, S. Mendu, B. Raj Pechetti, and M. Parvathi Mendu, “Comparative Analysis of Lenet, Resnet, and InceptionV3 Models for Pest Detection in Agriculture,” in *2025 1st International Conference on AIML-Applications for Engineering &amp; Technology (ICAET)*, (IEEE, Pune, India, 2025), pp. 1–6.
17. T. Y. Khaw, A. Amran, and A. P. Teoh, “Building a thematic framework of cybersecurity: a systematic literature review approach,” JSIT **26**(2), 234–256 (2024).
18. J. Guo, H. Mu, X. Liu, H. Ren, and C. Han, “Federated learning for biometric recognition: a survey,” Artif Intell Rev **57**(8), 208 (2024).
19. I.H. Sarker, M.H. Furhad, and R. Nowrozy, “AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions,” SN COMPUT. SCI. **2**(3), 173 (2021).
20. H. Samma, and S. Azmin Suandi, “Transfer Learning of Pre-Trained CNN Models for Fingerprint Liveness Detection,” in *Biometric Systems*, edited by M. Sarfraz, (IntechOpen, 2021).
21. M. Usman, “From Detection to Defense: How Neural Networks and AI are Transforming Cybersecurity Protocols,” (2024).
22. S. G. Tetteh, “A Systematic Performance Review of Security Methods for the Cyberworld,” AJRCoS **17**(5), 10–18 (2024).
23. A. K. A. Razack and M. F. M. Saad, "Enhancing cybersecurity awareness through gamification: Design of an interactive cybersecurity learning platform for Multimedia University students," Journal of Informatics and Web Engineering 3(3), 21–40 (2024). https://doi.org/10.33093/jiwe.2024.3.3.2