Journal of Engineering Science and Technology
Vol. 20, No. 4 (2025) 887 - 900

ENHANCING BIOMETRIC AUTHENTICATION IN HEALTHCARE APPLICATIONS USING CONVOLUTIONAL NEURAL NETWORK

ABDULRAHMAN W. H. AL-ASKARI*, KARAM M. Z. OTHMAN

Northern Technical University - Iraq
*Corresponding Author: abdulrahman21@ntu.edu.iq

Abstract

Personal data security is a growing concern due to daily technological advancements. As a result, there has been a significant increase in interest precise procedures to protect data and maintain confidentiality. Various techniques are available; however, their effectiveness varies. The use of biometric identification is a recent trend employed to verify authorized system users. Using the FVC2000 dataset, this research paper explores the application of convolutional neural networks (CNN) for biometric authentication, which has been proven to heighten user verification accuracy. The proposed CNN model feature specifically designed for finger print based authentication, trained end to end from scratch to capture unique characteristics of data. This research robust biometric authentication methods in health care by showing the effeteness of proposed model in distinguishing between authorized and unauthorized users When the CNN model was trained and tested using authorized user fingerprint images, it achieved 97% accuracy. With unauthorized fingerprints, the accuracy remained high at 96%. However, the accuracy of varying fingerprint images drops to 93.75%. These results provide strong evidence for the potential use of CNNs in the field of biometric authentication. Moreover, the model introduces a custom-built CNN architecture designed to be trained end-to-end, significantly improving both verification accuracy and security in a biometric authentication context. This paper further demonstrates its applicability by enhancing verification efficiency across a broader range of biometric images. The proposed model presents an effective avenue for implementing multi-factor authentication techniques, thereby strengthening data security.

Keywords: Biometric authentication, Deep learning, Fingerprint, FVC2000, Healthcare biometric systems, Verification.

1. Introduction

The development of the world today leads to search for secure, and highly accurate methods to preserve personal data and prevent unauthorized access. Conventional approaches encounter several challenges in accurately identifying authorized personnel due to the absence of advanced techniques. Biometric authentication has gained broad popularity due to its superior capabilities compared to other approaches for instance using fingerprints to identify the authorized person [1].

Technological advances have major impact in the medical field, where the diagnosis of diseases through the collection and analysis of data is possible [2]. The advances in artificial intelligence (AI) have led to the creation of applications to enhance treatment and disease management [3]. Moreover, AI has successfully helped maintain the privacy of medical data using biometric authentication [4]. Hence, deep learning models show high levels of accuracy and efficiency compared to other cryptographic-based approaches.

The implementation of deep learning techniques in the healthcare system, utilizing biometric authentication, has shown breakthrough results in verifying authorized individuals and reducing unauthorized access to sensitive patient data. One of the effective technique used is Convolutional neural networks (CNNs) which showed high accuracy in this matter [5].

Notwithstanding the aforementioned and the encouraging outcomes of using deep learning in biometric authentication, there exist several challenges, particularly those pertaining to the training model when varied images are required. In order to achieve precise identification of people, it is necessary to have a substantial collection of fingerprint picture. Clearly, mitigating the risk of unauthorized access to medical systems – specifically patient information-demands both time and resources.

The implementation of a deep learning-based authentication system in healthcare facilities enhances accuracy and security. It not only fortifies security measures but also reduces the possibility of unauthorized access. The provided study and model promise to substantially improve the healthcare sector by offering more effective methods to secure medical data.

While previous methods have explored pre-trained models and multimodal approaches to biometric authentication, the contribution of our work lies in the development of a fully customized CNN architecture tailored specifically for fingerprint recognition. Despite the various advancement in in deep learning for biometric authentication, the explored models in this paper often depend on pre-trained which may not be suited for the purposed that highlighted. whereas most of the models face challenges for instance limited adaptability to diverse fingerprint data.

In contrast the proposed CNN model feature specifically designed for finger print based authentication, trained end to end from scratch to capture unique characteristics of data This architecture, built from the ground up, offers enhanced adaptability without relying on external pre-trained models, thus improving both efficiency and accuracy in complex scenarios. Our work expands the scope of biometric authentication by addressing the limitations in traditional systems, such as the reliance on static datasets or failure under varied conditions, through a more flexible and scalable approach.

The need for a fully customized convolutional neural network (CNN) architecture specifically designed for fingerprint recognition, which addresses the limitations of traditional biometric systems that rely on static datasets and struggle under varying conditions. Additionally, there is a lack of comprehensive exploration into the adaptability and efficiency of deep learning techniques in biometric authentication within the healthcare sector, particularly when dealing with diverse and variable fingerprint images.

2. Related Work

This section discusses various previous studies related to biometric systems and related topics. Balaji and Rahamathunnisa [5] achieved 94% accuracy using multimodal biometrics, but their model required separate pipelines for fingerprints and iris scans. Our unified CNN architecture simplifies deployment while maintaining accuracy (97%).

Recognition techniques can vary based on the specific biometric model used. While traditional fingerprint systems rely on minutiae-based methods [6]. Yadav and Srinivasulu [7] fused minutiae with CNN features, but their hybrid model retained dependency on sequential handcrafted extraction, limiting scalability in healthcare settings.

Praseetha et al. [8] proposed a two-stage fingerprint authentication system using a lightweight CNN for feature extraction and graph-based minutiae matching, achieving 96% accuracy. While effective, their workflow requires manual alignment, increasing complexity. In contrast, Feng and Kumar [9] introduced an end-to-end CNN with attention mechanisms to automate minutiae detection, to enhance fingerprint accuracy.

Prakash et al. [10] employed Siamese Neural Networks for ECG-based authentication (99.85% accuracy) but noted challenges in sensor variability. For fingerprint-specific robustness, Myshkovskyi and Nazarkevych [11] optimized CNNs for real-world deployment in the field of biometric security.

Heidari and Chalechale [12] proposed a biometric system that used CNN with AlexNet as a pre-trained model. They suggested using fusion techniques to combine different features extracted from hand images. Their system demonstrated high reliability, marking it as a suitable choice for various applications.

Preetha and Sheela [13] integrated preprocessing with CNN recognition to reduce false rates. Expanding on this, Badhusha et al. [14] designed a specific CNN to enhance fingerprints recognition, also helps curb fingerprint spoofing, thereby improving security. Heidari and Chalechale [12] fused hand biometric features using AlexNet but lacked fingerprint specialization. Kouamo et al. [15] addresses deep neural network which reduces false rejections rate during the authentication-using fingerprint.

Maltoni et al. [16] reiterated the limitations of classical minutiae techniques. Our model builds on these insights, eliminating preprocessing and leveraging end-to-end learning for raw data.

3. Convolutional Neural Network Architecture

The CNN provided has been specially designed to improve user verification via fingerprint enhancement. This model lies in the custom architecture of the proposed CNN model, specifically designed for fingerprint-based authentication. Unlike

conventional architectures that incorporate pre-trained components, it is fully trained from scratch, allowing it to adapt specifically to the nuances of fingerprint data. This custom design incorporates optimized convolutional layers and enhanced feature extraction techniques tailored to biometric identification, which significantly improves both verification accuracy and computational efficiency.

The proposed CNN architecture can be integrated into practical biometric systems by providing a detailed implementation guide, such as the required hardware, procedures for real-time data acquisition, and considerations for software compatibility, with current healthcare data management systems. Figure 1 shows the CNN structure, which includes several layers and interconnected nodes. This structure allows the CNN to independently gain knowledge and recognize patterns.

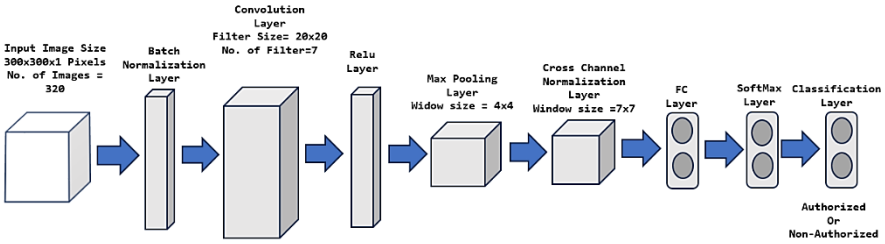

Fig. 1. The general architecture of the suggested Deep learning for Intensifying User Verification.

The suggested CNN incorporates hidden layers and parameters, which have been validated in [17]. The architecture is tailored to address fingerprint-specific challenges in healthcare, such as variable image quality and ridge pattern preservation. The layers are justified as follows.

(a) Image Input Layer: The CNN is configured to receive fingerprint images, each with a size of (300×300×1) pixels. Larger filters capture macroscopic ridge-valley structures in low-resolution fingerprints [7].

(b) The Batch Normalization layer: positioned as the initial hidden layer, functions to normalize input values through rescaling and re-centering processes. This normalization step accelerates the network's training by diminishing the required number of epochs. BatchNorm mitigates internal covariate shift caused by sanitization-induced skin dryness or sensor variability, accelerating convergence for healthcare-grade accuracy [18].

$$BN_{r,c} = \frac{I_{r,c-\mu}}{\sqrt{v^2+x}} \quad (1)$$

Here, $BN_{r,c}$ represents a batch normalization value, where r and c correspond to the row and column, v^2 denotes the variance, μ represents the mean, and x is a constant [18].

(c) The Convolution Layer, positioned as the second layer, conducts the convolution process wherein input data is convolved with kernels kr, employing Two-Dimensional (2D) convolutions or filters. These filters are instrumental in extracting essential features, resulting in the creation of feature maps from normalized input images. The mathematical equation below encapsulates the formula governing the convolution layer:

$$\mathrm{CL}_{\mathrm{n}}^{\mathrm{C}} = \sum_{\mathrm{z}=1}^{\mathrm{z}^{\mathrm{L}-1}} \mathrm{kr}_{\mathrm{n,z}}^{\mathrm{L}} * \mathrm{BN}_{\mathrm{r,c}} + \mathrm{b}_{\mathrm{n}}^{\mathrm{L}} \quad (2)$$

Here, *L* signifies the current layer, *L-1* denotes the preceding layer, and *n* represents the number of nodes.

CL_n^C is a convolution value, $BN_{r,c}$ is an input to be convolved, $kr_{n,z}^L$ refers to a kernel value and b_n^C represents a bias [19].

(d) Following the convolution process, the activation function employed in this layer is Rectified Linear Unit (ReLU), a non-linear function that retains positive values unchanged and sets negative values to zero. ReLU's sparsity promotes efficient learning of non-linear ridge relationships while avoiding vanishing gradients in deep networks [20].

$$Re_n^c = \max(0, CL_n^{c-1}) \quad (3)$$

where: Re_n^C is a ReLU value and max refers to the maximum operation.

(e) The Pooling Layer functions as a reduction layer, aiming to diminish the dimensions of preceding data, thereby enhancing computational efficiency. Typically, maximum pooling is employed, where the maximum values within pixel batches (windows) are selected using a specific formula [21]. The pooling layer's operational principle can be expressed as follows:

$$P_n^C = \max(Re_M^{C-1}) \quad (4)$$

where: P_n^C is a maximum pooling value, *M* is the index of a batch of pixels (window) [21].

(f) Cross Channel Normalization Layer: It's employed to normalize the output of the preceding layer. The formula utilized for this normalization process is as follows:

$$CNL_n = \frac{P_n^{C\,ak}}{(j+p\sum_{jr=max\,(0,ak-\frac{km}{2})}^{min\,(KM-1,ak\frac{km}{2})}(P_n^{C\,jr})^z)^\beta} \quad (5)$$

Where: CNL_n is a channel normalization layer value, *KM* denotes the kernel map, *km* refers to the neighbouring kernel maps, ak is the applied kernel, and j, p and β are hyper-parameters. Normalizes adjacent feature maps to enhance ridge-valley contrast, reducing false matches from distorted or partial prints [22].

(g) The Fully Connected (FC) Layer: establishes connections between the preceding and subsequent layers. In this layer, the desired number of verification nodes can be specified. The formula governing the FC layer is as follows:

$$F_n = \sum_{h=1}^{m_1^{C-1}} \sum_{j=1}^{m_2^{C-1}} \sum_{k=1}^{m_3^{C-1}} WE_{h,j,k,n}^C \, CNL_n \qquad 1 \le n \le m^C \quad (6)$$

where: F_n is a fully connected value, m_1^{C-1} and m_2^{C-1} are respectively the height and width of the pooling layer, m_3^{C-1} is the number of channels, $WE_{h,j,k,n}^C$ signifies the weight value that establishes connections between the FC layer and the preceding layer [23].

(h) The Softmax Layer is responsible for generating probability distributions for each input image across multiple nodes. It applies the softmax formula, which can be expressed as follows:

$$SL_n = \frac{e^{Fn}}{\sum_{s=1}^{m^{c-1}} e^{Fn}} \qquad \text{n =1,2, …, } m^C \tag{7}$$

where: SL_n is a softmax layer value [23].

(i) The Classification Layer, serving as the final hidden layer in the proposed model, generates binary outputs of 1s and 0s. These outputs are determined through the implementation of the winner takes all rule, which can be articulated as follows:

$$cfl_n = \begin{cases} 1 & \text{if } SL_n = max \\ 0 & \text{otherwise} \end{cases} \text{ n =1,2, …, } m^C \tag{8}$$

where: cfl_n is a classification layer value.

Softmax converts logits to probabilities for interpretable confidence scores, while the winner-takes-all rule ensures unambiguous binary decisions (authorized/unauthorized) [24].

(j) The Output Layer is responsible for determining the outcome of the user verification process. This indicates that an authorized person is assigned the logical value of "1" in the classification layer, while a non-authorized individual is assigned the logical value of "0". At the beginning of the process, an individual intending to submit fingerprint input images must assert their identity. Subsequently, each fingerprint image is passed through the proposed CNN network with specific weights assigned to them. If the resulting output corresponds to the claimed identity, the authorization is deemed successful. Conversely, if the output does not align with the claimed identity, the authorization is considered unsuccessful, leading to the rejection of the identity claim. The concept of user verification based on this principle was demonstrated in [25-28].

4. Results and Discussions

4.1. Explanation of the utilized dataset

The finger print image dataset (FVC2000-DB1) is found in the fingerprint verification competition and acquired by using a low-cost optical sensor [16]. This dataset represents the authorized persons and have the following features:

- The dimensions of the images are 300×300 pixels in TIF format.
- The fingerprint samples predominantly originate from students aged between 20 to 30 years, with an approximate gender distribution of 50% male.
- Number of participants is 10 persons and each participant contributed 8 fingerprints from both hands.
- Sequential acquisition of different fingers was interleaved, capturing samples such as the left forefinger, right forefinger, left middle, right middle, and so forth.

For non-authorized phase, the finger print image datasets (FVC2000-DB2, DB3 and DB4) are found in the fingerprint verification competition. These datasets representing the non-validate persons and collected by low-cost capacitive sensor, optical sensor, and synthetic generator respectively and have the following features:

- The dimensions of the images are 300×300 pixels in TIF format.

- The fingerprint samples originate from 73-year-olds with an approximate distribution of 33%.
- The fingerprint samples originate from 50-year-olds with an approximate distribution of 33% and 34% from 18 to 5 -year-olds.
- Number of participants is 30 persons and each participant contributed 8 fingerprints from both hands.

In this study, we analyze a total of 320 fingerprint images sourced from the FVC2000-DB1 dataset. It comprises 80 segmented images from authorized fingerprints belonging to ten individuals and 240 segmented images from non-authorized fingerprints belonging to thirty individuals. Figure 2(a) presents examples of fingerprint samples for authorized and Fig. 2(b) for non-authorized users. A CNN uses these images as follows: 60% for training, 20% for validation, and the remaining 20% for testing.

(a) Eight instances of authorized fingerprint users.

(b) Eight instances of unauthorized fingerprint users.

Fig. 2. Examples of fingerprint samples.

4.2. Description of CNN model layers

The proposed CNN is a deep learning model specifically designed for fingerprint-based individual verification [7, 29]. This model's architecture is layered: it begins with an image input layer of a 300 × 300 pixel size. Numerous hidden layers are included, such as a batch normalization layer to normalize input values.

A convolutional layer follows with a filter size of 20 × 20 pixels and seven filters. Subsequently, a Rectified Linear Unit (ReLU) layer rectifies any negative values. A max-type pooling layer with non-overlapping 4 × 4 pixel windows comes next, followed by a cross-channel normalization layer with a 7 × 7 pixel window. A fully connected (FC) layer containing two neurons is then utilized, accompanied by *softmax* and classification layers; both also contain two neurons each. The model concludes with an output layer that makes the final verification decision.

4.3. Performance during CNN training

The training parameters are set as follows initially: an Adam optimizer with a gradient decay factor of 0.9, a squared gradient decay rate of 0.99, an epsilon training of 1×10^{-8}, a mini-batch size of 32, a maximum of 50 epochs, and an initial learning rate of 0.001. These parameters were chosen based on their effectiveness in training CNN, as demonstrated in numerous studies. The Adam optimizer is particularly favored for its adaptive learning rate capabilities, which can lead to faster convergence. The learning rate of 0.001 is a common starting point that balances the speed of training and stability, while a mini-batch size of 32 is often found to provide a good trade-off between computational efficiency and model performance.

Figure 3 demonstrates the training performance of fingerprint input images. It displays the accuracy and loss errors observed during the training iterations. The training curve, as depicted in the figure, clearly indicates significant accuracy improvements and notable error reductions throughout the iterations. High levels of accuracy accompanied by very low error values were achieved by the end of the training, indicating the successful training of the fingerprint images.

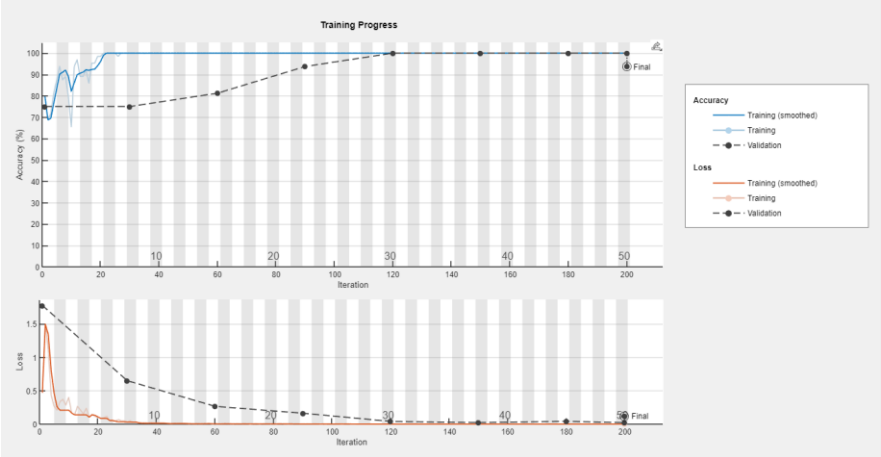

Fig. 3. Curve depicting the training progress for fingerprint input images.

4.4. Feature extraction workflow in CNN model

In the proposed CNN model, hidden layers carry out feature extraction, incorporating batch normalization, convolution, ReLU, pooling, and cross-channel normalization. The rest of the hidden layers contribute to the recognition process. Feature extractions of fingerprint images retrieved from the feature extraction layers of the CNN post-training (as shown in Fig. 4).

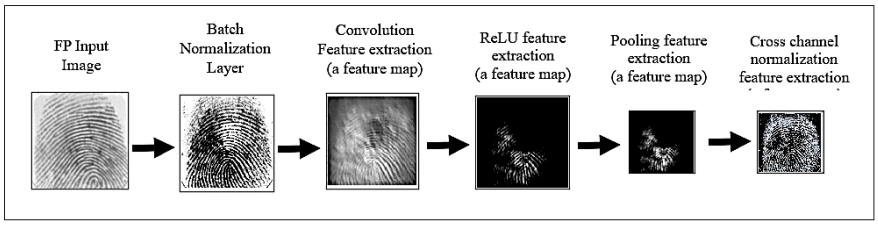

Fig. 4. Instances of feature extractions from fingerprint input images gathered from the layers dedicated to deep learning feature extraction post-training.

Figure 4 exhibits examples of fingerprint input images and their respective feature extractions via a CNN. It is clear that the batch normalization layer is vital in transforming the input images' values, thus effectively standardizing their information and boosting the overall operation of the CNN. The convolutional layer produces an array of feature maps for each 2D fingerprint image using kernel values yielded during the training phase. The ReLU layer strategically discards negative values from the convolutional feature maps while preserving the positive ones.

Afterward, the pooling layer lessens the dimensions of the ReLU feature maps bidimensionally, focusing on the maximum values within pre-set window sizes. The cross-channel normalization layer further modifies the preceding values, corresponding to the values of each 2D pooling feature map. This layer forms the final stage of feature extraction in the suggested CNN, normalizing previous values within the same spatial area and, therefore, improving the CNN computations. Ultimately, the CNN model allows for an effective and automated extraction of fingerprint features.

4.5. Performance during CNN testing

During the testing phase of the CNN model, 32 fingerprint images were used. The results showed that the model's accuracy was 93.75%, with an error rate of 6.25%. Table 1 displays the verification performance of the proposed model.

Table 1. Verification performance for fingerprint images.

Categorizing FP Image	Accuracy	Error
Authorized FP Image	97%	3%
Non-authorized FP Image	96%	4%
Diverse Fingerprints	93.7%	6.25%

Table 1 documents the verification accuracy and error rates for authorized fingerprint images as 97% and 3%, respectively. Furthermore, non-authorized fingerprint images exhibited a verification accuracy of 96% and an error rate of 4%.

Lastly, the verification rate for diverse fingerprint images was marked at 93.75%, with an error rate of 6.25%.

4.6. Comparative analysis

Our study focuses on developing a task-specific, custom-built CNN model that is trained end-to-end without deploying pre-trained networks. The proposed approach deviates from previous work by creating a task-specific CNN architecture that is trained from scratch, in contrast to many existing models that rely on pre-trained networks. While Preetha and V. [13] used an Inception CNN for fingerprint authentication and applied preprocessing techniques, our model integrates the entire training process into a single custom CNN workflow.

To further highlight the contributions of our model, we conducted a comparative analysis with several state-of-the-art methods in biometric authentication. Praseetha et al. [8] achieved 94% accuracy using a two-stage Inception CNN and minutiae matching, while our approach achieved a superior accuracy of 97% for authorized fingerprints without relying on pre-trained networks.

Although their method excels in signal processing, our model offers a more general solution applicable to image-based verification, particularly fingerprint identification, demonstrating versatility in real-world biometric applications. Heidari and Chalechale [12] utilized a fusion-based CNN model with AlexNet for feature extraction, achieving high reliability, yet our custom-built CNN offers a more streamlined and efficient architecture tailored to biometric verification without relying on pre-existing architectures. Additionally, Preetha and V. [13] used preprocessing with CNN-based recognition to enhance image quality before classification, achieving high accuracy, but our model eliminates the need for such preprocessing while still maintaining comparable results.

Therefore, the demonstrates the robustness of the model in distinguishing between genuine and imposter inputs, even under varied conditions. This improvement is largely attributed to the custom-built CNN architecture, which enhances the feature extraction process and allows for more precise classification.

Table 2 presents a comparative analysis between our model and several existing state-of-the-art approaches in biometric authentication. As seen in the table, our proposed model achieves higher accuracy for authorized users (97%) compared to the 94% reported by Praseetha et al. [8] . In contrast to Heidari and Chalechale [12], who employed a fusion-based CNN model, our architecture achieves similar reliability with a more streamlined training process, as demonstrated by our 96% accuracy for unauthorized fingerprints. The outperforms Preetha and V. [13] in terms of classification efficiency, despite their use of image preprocessing. These comparisons underscore the effectiveness of our method in various biometric scenarios.

While the results of this study demonstrate promising accuracy for both authorized and unauthorized fingerprint verification, the limited size of the FVC2000 dataset used in this research imposes certain constraints. The small sample size, consisting of only 320 fingerprint images, may not fully represent the variability found in real-world biometric systems. This limited diversity in the dataset could affect the generalizability of the model when applied to larger or more heterogeneous populations. Additionally, the dataset's restricted range of age groups and environments limits the assessment of the model's robustness in more

complex, real-life scenarios. Consequently, further research is required to validate the model's effectiveness across a broader range of biometric datasets, including larger and more diverse samples.

Table 2. Comparative analysis between the Proposed model and other approaches in biometric authentication.

Ref.	Suggested approach	Accuracy of Existing approaches	Accuracy of the proposed model custom- built CNN
Praseetha et al. [8]	Two-Stage Approach Pre-Trained Inception CNN	94%	97%
Heidari and Chalechale [12]	CNN With Alexnet	94.75%	97%
Preetha and V. [13]	Integrated system with CNN-based recognition	Outperformed single-stage designs	97%

Future work should focus on expanding the dataset to include a wider range of fingerprint samples from a more diverse population in terms of age, gender, and environmental conditions. To address dataset limitations, advanced data augmentation techniques tailored to healthcare contexts-such as synthetic fingerprint generation via GANs (simulating dry/wet skin effects [30]. Additionally, transfer learning could leverage pre-trained CNNs on large-scale healthcare fingerprint datasets. Boosting feature extraction accuracy, particularly for underrepresented groups [31]. Integrating multimodal biometrics (facial recognition, voice ID) may further strengthen authentication. However, prioritizing fingerprint-specific augmentation and transfer learning would directly mitigate current scalability constraints while maintaining computational efficiency for clinical deployment.

The proposed convolutional neural network (CNN) model for biometric authentication presents significant real-world applications, particularly in enhancing multi-factor authentication (MFA) systems. Therefore, its application in mobile device security enhances user authentication for applications. Overall, the CNN-based biometric authentication model offers a promising avenue for implementing robust security measures across various industries.

5. Conclusion

The study focuses on biometric authentication, proposing a CNN to improve user verification, specifically through fingerprint recognition in healthcare systems. The model's structure includes an input image layer, a batch normalization layer, a convolutional layer, a ReLU layer, a max pooling layer, a cross-channel normalization layer, a FC layer, a softmax layer, and classification layer. These components work together to differentiate between authorized and unauthorized individuals.

The results validate the proposed model's effectiveness in fingerprint classification, achieving noteworthy accuracy. The model demonstrated a verification accuracy of 97% and an error rate of 3% for authorized fingerprint images. The performance with non-authorized fingerprints was also robust, yielding a 96% verification accuracy and a 4% error rate. However, for varied fingerprints, the model's accuracy dropped to 93.75%, and the error rate rose to 6.25%.

Our comparative analysis with existing methods further confirms that the proposed CNN model offers competitive accuracy and efficiency. By comparing our results with state-of-the-art techniques, we demonstrated that our approach not only simplifies the architectural complexity but also improves performance in fingerprint-based biometric authentication, particularly in real-world, varied datasets. Although the proposed CNN model demonstrated high accuracy for fingerprint-based biometric verification, the small dataset used in this study presents a limitation. While deep learning in biometric authentication offers substantial benefits, several challenges need to be addressed for future advancements. Key limitations include the necessity for large, diverse datasets to avoid bias, privacy concerns related to biometric data collection, and the high computational costs of training deep learning models.

Future work should focus on developing robust data governance frameworks, exploring efficient algorithms, and employing adversarial techniques to enhance system security against spoofing. Additionally, fostering interdisciplinary collaboration will ensure that the deployment of these technologies is effective and ethically sound. By tackling these issues, healthcare organizations can improve security measures and protect patient records more effectively.

Nomenclatures

$BN_{r,c}$	Batch Normalization Value
cfl_n	Classification Layer
P_n^C	Pooling Value
SL_n	Softmax Layer Value

Abbreviations

AI	Artificial Intelligence
CNN	Convolutional neural network
FC	Fully Connected
FP	Finger Print
ReLU	Rectified Linear Unit

References

1. Joseph, A.A.; Ho Lian, A.N.; Kipli, K.; Lee Chin, K.; Awang Mat, D.A.; Chin Voon, C.S.; Sing Ngie, D.C.; and Sze Song, N. (2021). Person verification based on multimodal biometric recognition. *Pertanika Journal of Science and Technology*, 30(1), 161-183.
2. AL-Askari, A. (2023). Computer-aided auscultation system for cardiac monitoring. *Przegląd Elektrotechniczny*, 1(12), 173-176.

3. Othman, K.M.Z.; and Zeki, N.M. (2023). Therapeutic management of diseases based on fuzzy logic system- hypertriglyceridemia as a case study. *TELKOMNIKA* (*Telecommunication Computing Electronics and Control*), 21(2), 314-323.
4. Benlamoudi, A.; Bekhouche, S.E.; Korichi, M.; Bensid, K.; Ouahabi, A.; Hadid, A.; and Taleb-Ahmed, A. (2022). Face presentation attack detection using deep background subtraction. *Sensors*, 22(10), 3760.
5. Balaji, S.; and Rahamathunnisa, U. (2023). Multimodal biometrics authentication in healthcare using improved convolution deep learning model. *International Journal on Artificial Intelligence Tools*, 32(03), 2340013.
6. Alhamad, E.A.; Logmani, M.S.A.; Essa, A.T.A.; and Hammoudeh, M. (2024). A minutiae-based method to store and compare fingerprints. *International Journal of Biometrics*, 16(2), 176-194.
7. Yadav, K.A.; and Srinivasulu, T. (2021). Fingerprint authentication using CNN for minutiae based authentication. *International Journal of Engineering Research and Applications*, 11(2), 23-29.
8. Praseetha, V.M.; Bayezeed, S.; and Vadivel, S. (2019). Secure fingerprint authentication using deep learning and minutiae verification. *Journal of Intelligent Systems*, 29(1), 1379-1387.
9. Feng, Y.; and Kumar, A. (2023). Detecting locally, patching globally: An end-to-end framework for high speed and accurate detection of fingerprint minutiae. *IEEE Transactions on Information Forensics and Security*, 18, 1720-1733.
10. Prakash, A.J.; Patro, K.K.; Samantray, S.; Pławiak, P.; and Hammad, M. (2023). A deep learning technique for biometric authentication using ECG beat template matching. *Information*, 14(2), 65.
11. Myshkovskyi, Y.; and Nazarkevych, M.(2023). Robustness of fingerprint liveness detection based on convolutional neural networks. *Cybersecurity Providing in Information and Telecommunication Systems*, 281-288.
12. Heidari, H.; and Chalechale, A. (2022). Biometric authentication using a deep learning approach based on different level fusion of finger knuckle print and fingernail. *Expert Systems with Applications*, 191, 116278.
13. Preetha, S.; and Sheela, S.V. (2021). Analysis of fingerprint biometric authentication using CNN. *SSRN Electronic Journal*.
14. Badhusha, K.; Arif.M, M.; Faruk, M.; Elumala, S.; Devi, T.K.; and Kumanan, T.(2023). CNN based fingerprint extraction and recognition. *International Journal of Novel Research and Development* (*IJNRD*), 8(4), 370-374.
15. Kouamo, S.; Tangha, C.; and Kouamo, O. (2020). Reduction of false rejection in an authentication system by fingerprint with deep neural networks. *Journal of Software Engineering and Applications*, 13(01), 1-13.
16. Maltoni, D.; Maio, D.; Jain, A.K.; and Feng, J. (2022). *Fingerprint classification and indexing*. In Maltoni, D.; Maio, D.; Jain, A.K.; and Feng, J. (Eds.), *Handbook of Fingerprint Recognition*. Springer International Publishing, 299-338.
17. Zhu, Z.; Wang, S.-H.; and Zhang, Y.-D. (2023). A survey of convolutional neural network in breast cancer. *CMES-Computer Modeling in Engineering and Sciences*, 136(3), 2127-2172.

18. Ioffe, S.; and Szegedy, C. (2015). Batch normalization: Accelerating deep network training by reducing internal covariate shift. *arXiv*.
19. Ardakani, A.; Condo, C.; Ahmadi, M.; and Gross, W.J. (2018). An architecture to accelerate convolution in deep neural networks. *IEEE Transactions on Circuits and Systems I*: *Regular Papers*, 65(4), 1349-1362.
20. Krizhevsky, A.; Sutskever, I.; and Hinton, G.E. (2017). ImageNet classification with deep convolutional neural networks. *Communications of the ACM*, 60(6), 84-90.
21. Al-Aima, R.R.O.; Al-Askari, A.W.H.; Othman, K.M.Z.; and EESEE, A.K. (2023). Enhancing finger outer knuckles recognition using deep recurrent neural network. *Journal of Engineering Science and Technology*, 18(6), 2915-2927.
22. Yang, W.; Wang, M.; Zou, S.; Peng, J.; and Xu, G. (2021). An implicit identity authentication method based on deep connected attention CNN for wild environment. *Proceedings of the* 2021 9th *International Conference on Communications and Broadband Networking*, Shanghai China, 94-100.
23. Najeeb, S.M.M.; Al-Nima, R.R.O.; and Al-Dabag, M.L.A. (2021). Reinforced deep learning for verifying finger veins. *International Journal of Online and Biomedical Engineering* (*iJOE*), 17(07), 19-27.
24. Bishop, C.M. (2007). *Pattern recognition and machine learning*. Springer.
25. Prajapati, P.R.; Poudel, S.; Baduwal, M.; Burlakoti, S.; and Panday, S.P. (2021). Signature verification using convolutional neural network and autoencoder. *Journal of the Institute of Engineering*, 16(1), 33-40.
26. Wang, C.; Xiao, Y.; Gao, X.; Li, L.; and Wang, J. (2023). A framework for behavioral biometric authentication using deep metric learning on mobile devices. *IEEE Transactions on Mobile Computing*, 22(1), 19-36.
27. Alghamdi, M.; Angelov, P.; and Alvaro, L.P. (2022). Person identification from fingernails and knuckles images using deep learning features and the Bray-Curtis similarity measure. *Neurocomputing*, 513, 83-93.
28. Sinha, H.; Manekar, R.; Sinha, Y.; and Ajmera, P.K. (2019). *Convolutional neural network-based human identification using outer ear images*. In Bansal, J.C.; Das, K.N.; Nagar, A.; Deep, K.; and Ojha, A.K. (Eds.), *Soft computing for problem solving*. Springer Singapore, 707-719.
29. Sachin, M.; C, K.K.; Gupta Chancellor, S.; Alatba, S.R.; Pund, S.S.; and Alfurhood, B.S. (2023). A finger print recognition using CNN Model. *Proceedings of the* 2023 3rd *International Conference on Advance Computing and Innovative Technologies in Engineering* (*ICACITE*), Greater Noida, India.
30. Bamoriya, P.; Siddhad, G.; Kaur, H.; Khanna, P.; and Ojha, A. (2022). DSB-GAN: Generation of deep learning based synthetic biometric data. *Displays*, 74, 102267.
31. Samma, H.; and Azmin Suandi, S. (2021). *Transfer learning of pre-trained CNN models for fingerprint liveness detection*. In Sarfraz, M. (Ed.), *Biometric Systems. IntechOpen*.