Journal of Artificial Intelligence and Data Mining (JAIDM Vol. 12, No. 2, 2024, 241-248.

Shahrood University of Technology

Journal of Artificial Intelligence and Data Mining (JAIDM)
Journal homepage: http://jad.shahroodut.ac.ir

Research paper

A Deep Learning-based Model for Fingerprint Verification

Mobina Talebian, Kourosh Kiani* and Razieh Rastgoo

Faculty of Electrical and Computer Engineering, Semnan University, Semnan, Iran.

Article Info

Article History:
Received 09 March 2024
Revised 08 July 2024
Accepted 16 August 2024

DOI:10.22044/jadm.2024.14298.2531

Keywords:
Fingerprint; Verification; Deep learning; Pretrained; Convolutional Neural Network.

**Corresponding author: Kourosh.kiani@semnan.ac.ir (K. Kiani).*

Abstract

Fingerprint verification has emerged as a cornerstone of personal identity authentication. This research introduces a deep learning-based framework for enhancing the accuracy of this critical process. By integrating a pre-trained Inception model with a custom-designed architecture, we propose a model that effectively extracts discriminative features from fingerprint images. To this end, the input fingerprint image is aligned to a base fingerprint through minutiae vector comparison. The aligned input fingerprint is then subtracted from the base fingerprint to generate a residual image. This residual image, along with the aligned input fingerprint and the base fingerprint, constitutes the three input channels for a pre-trained Inception model. Our main contribution lies in the alignment of fingerprint minutiae, followed by the construction of a color fingerprint representation. Moreover, we collected a dataset, including 200 fingerprint images corresponding to 20 persons, for fingerprint verification. The proposed method is evaluated on two distinct datasets, demonstrating its superiority over existing state-of-the-art techniques. With a verification accuracy of 99.40% on the public Hong Kong Dataset, our approach establishes a new benchmark in fingerprint verification. This research holds the potential for applications in various domains, including law enforcement, border control, and secure access systems.

1. Introduction

In recent decades, the rapid progress in information and communication technology, combined with advancements in Artificial Intelligence and deep learning, has brought about profound changes across various aspects of human life, owing to the limitless possibilities they offer [1]. One notable domain significantly affected by these advancements is fingerprint recognition and verification, recognized as critical technologies for ensuring security and safeguarding information [2]. The main differences between fingerprint recognition and fingerprint verification lie in their purposes. Fingerprint recognition is employed for verification, whereas fingerprint verification is predominantly utilized for the authentication of individual identities [3]. To enhance accuracy and efficiency in the fingerprint recognition and verification process, the utilization of AI, particularly neural networks and deep learning, has emerged as a novel and effective approach. Fingerprint features include distinctive patterns known as minutiae, pinpointing crucial points like bifurcation and ridge endings in fingerprints [3]. These patterns are crucial for confirming an individual's identity. Despite significant progress in this field, challenges persist, such as sensitivity to changes in viewing angles, issues stemming from low fingerprint quality, responsiveness to various environmental conditions [4], and various kind of attack [5]. Solutions to address these challenges are currently in development, leveraging a combination of different models, deep learning techniques, and adaptability to diverse conditions, especially incorporation to biological domains. Figure 1 and Figure 2 show various examples of fingerprints and their details. Moreover, fingerprints find applications in a range of areas [6,7], including organizational, urban, medical, and security-related activities. Within the realm of fingerprint recognition and verification, various models are employed for feature extraction and analysis. In addition to the conventional machine learning models that are used in image-based tasks [8], one of the foremost models is Convolutional Neural Networks (CNNs) [9], utilizing convolutional layers to extract hierarchical features from fingerprints. These layers excel at identifying different patterns, ranging from lines and loops to more intricate structures. Additionally, Recurrent Neural Networks (RNNs) [10] are utilized for modeling extended sequences of fingerprints. These networks prove especially effective in cases where the temporal sequence of fingerprints conveys specific meaningful information. To make an improvement in the area of fingerprint verification, we propose a deep learning-based model by using the minutiae features and the CNN model. Moreover, we present a dataset, including 200 fingerprint images corresponding to 20 persons, for fingerprint verification. Details of the proposed model as well as the collected dataset are presented in the following sections. Our main contributions can be listed as follows:

- **Model**: We propose a model using the pre-trained Inception model and a novel identity verification model. This model involves aligning fingerprints based on their minutiae details and creating a color image by merging three processed and base binary images in three color channels of RGB, serving as the input to the network. To the best of our knowledge, this is the first time that such a model is proposed to the fingerprint identity verification. Results on two datasets show the superiority of the proposed model compared to state-of-the-art models in the field.

- **Dataset**: We collected a dataset, including 200 fingerprint images corresponding to 20 persons, for fingerprint verification.

The remainder of this paper is organized as follows: Section 2 presents a brief review of relevant research on fingerprint recognition and verification. Sections 3 and 4 describe the proposed dataset and approach in detail, respectively. In section 5, the results of experiments conducted on two datasets are presented and discussed. Finally, section 6 concludes the paper by summarizing the key contributions of our work and outlining potential future research in this area.

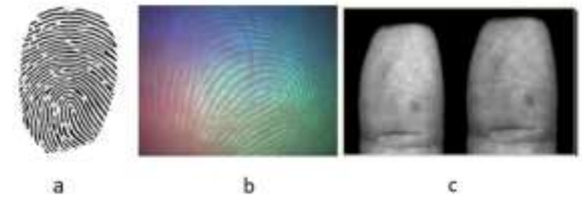

Figure 1. Fingerprint images: (a) Touching the Sensor, (b) Touchless Fingerprint, and (c) Three-dimensional(3D).

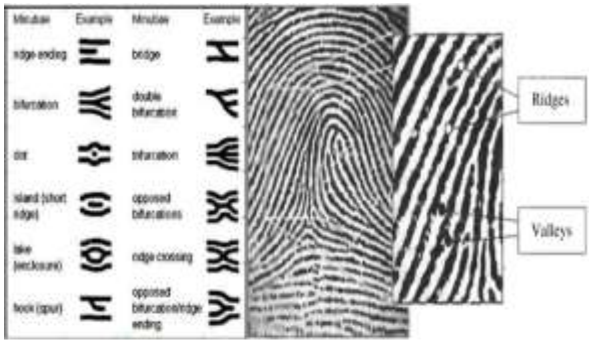

Figure 2. Different Categories of Minutiae.

2. Related Work

Previous research can be divided into two categories: identity recognition and identity verification. Here, we briefly review recent works in these categories.

Identity recognition: A novel patch-based approach utilizing deep neural networks is proposed in [11] for latent fingerprint matching. By partitioning fingerprint images into patches and employing deep learning models to assess their similarity, the method achieves an accuracy of 81.35%. However, its performance in handling low-quality latent fingerprints and its reliance on a relatively small dataset remain areas for improvement. Enhanced accuracy and invariance to rotation are reported benefits. Minutiae information is integrated to refine the matching process. Additionally, the proposed methodology in [9] employs a multi-step approach to fingerprint recognition. Minutiae are initially extracted, followed by the creation and hashing of arrangement vectors for efficient retrieval. A CNN is then trained to classify query fingerprints based on these vectors. The system demonstrates robustness to deformations and benefits from efficient spatial indexing due to hashing. Achieving accuracy rates of 80% and 84.5% on FVC2004 and NIST SD27 datasets, respectively, highlights the method's effectiveness. The effectiveness of this method is hindered by its reliance on sufficient minutiae extraction, sensitivity to fingerprint quality, and potential for false matches due to hash-index-based approach. While the method demonstrated promising results, further research is required to address these limitations and optimize performance through exploration of alternative hashing and quantization techniques. A deep learning model incorporating fuzzy theory is utilized in [12] for fingerprint identification. The authors propose a framework that employs the One-Pass Thinning Algorithm (OPTA) to classify and reconstruct damaged fingerprint images, achieving a reported accuracy rate of 97.1%. However, the model's performance is contingent upon the quality of preprocessed fingerprint images. To address the challenge of high-dimensional feature spaces, the authors integrate fuzzy theory for feature reduction. This approach constitutes a significant contribution of the study. The proposed method's effectiveness is hindered by its reliance on image quality, limited dataset, and a relatively simple comparison framework, suggesting a need for further refinement and rigorous evaluation through the investigation of alternative deep learning architectures and feature extraction techniques. In [13], a novel fingerprint classification approach is presented that leverages a deep neural network architecture, specifically a stacked sparse autoencoder (SAE), for direct feature learning from fingerprint images. Following SAE training, a softmax regression model is employed to categorize fingerprints into four classes: arch, left loop, right loop, and whorl. To enhance classification accuracy for ambiguous fingerprint patterns, the authors introduce a complementary fuzzy classification method. This hybrid approach eliminates the need for manual feature extraction and demonstrates a substantial improvement in classification accuracy, reaching 99%. The proposed fingerprint recognition method faces challenges in achieving optimal accuracy and robustness due to factors such as threshold sensitivity, limited dataset size, and the need for more sophisticated spoof detection mechanisms. The study highlights the potential for further advancements through the exploration of hybrid methodologies, addressing class imbalance issues, and incorporating additional features. Moreover, [14] reported accuracy rate of 95% by introducing a system harnesses a CNN for contactless fingerprint recognition, showcasing proficiency in preprocessing, feature extraction, and matching stages with databases containing authentic and spoof fingerprints, employing a subset of 140 images for testing out of the original 275. This method not only demonstrates robustness through effective fingerprint spoof mitigation techniques but also excels in high accuracy, low complexity, and practical applicability. The proposed CNN-based model exhibits limitations in accuracy and robustness, primarily due to sensitivity to threshold values and a relatively small dataset. There exists the potential for further refinement through the expansion of the training set and the adoption of advanced strategies, while [15] introduces an advanced fingerprint recognition framework that utilizes CNN and transfer learning. The method involves refining a pre-trained ResNet50 model, originally trained on ImageNet, focusing on a fingerprint recognition task with a dataset containing numerous subjects but limited images per subject. Employing data augmentation techniques enhances the training set. The fine-tuned CNN model exhibits notable adaptability, achieving an impressive accuracy rate of 95.7% and surpassing previous methodologies. Additionally, the study introduces a visualization technique inspired by prior work, systematically occluding regions to identify crucial areas for fingerprint recognition. The proposed fingerprint recognition method, while demonstrating promising results, faces limitations in dataset size, potential biases from the pre-trained model, and the simplicity of the visualization technique. A more comprehensive evaluation against a wider range of methods and datasets would be beneficial to assess its overall effectiveness and generalizability.

Identity verification: Praseetha et al. [2] proposed fingerprint verification system leveraged a pre-trained Inception v3 model as a preliminary filter coupled with k-nearest neighbor algorithm for minutiae detection, achieving 94% accuracy. While demonstrating potential to mitigate noise challenges in emerging sensor technologies, the system's robustness to various fingerprint conditions and potential security vulnerabilities warrants further investigation. Expanding the dataset and conducting rigorous security analysis are essential for practical implementation. A novel dual neural network architecture for minutiae detection in fingerprint images is proposed in [16]. Combining a pixel-wise local dilated network with a patch-wise global network, the method incorporates an orientation-aware loss function and dynamic end-to-end training. Demonstrating superior accuracy and reduced computational complexity, the approach holds promise for biometric authentication applications. Evaluated on the Benchmark 2D/3D database, the method achieved a verification accuracy of 98.91%. The proposed minutiae extraction model demonstrates limitations in handling challenging fingerprint

images and requires further optimization for real-time applications. To further enhance performance, future research should focus on refining minutiae localization and evaluating the method on a broader range of fingerprint datasets, including real-world scenarios.
Aiming to enhance the accuracy of identity verification, in this paper, we propose a deep learning framework, leveraging a pre-trained Inception v3 model and incorporating minutiae features. We propose a new image fusion technique and the adaptation of a pre-trained model for fingerprint verification. While building upon established methodologies such as minutiae-based alignment and comprehensive performance evaluation, the study's overall contribution to the state-of-the-art is mitigated by the relatively small dataset and limited comparative analysis. The motivation for this research stems from the potential for enhanced accuracy, improved robustness to noise and distortion, and the exploration of a novel combination of image fusion and pre-trained model adaptation. An innovative multimodal biometric system is presented in [17] to address the challenge of presentation attacks in fingerprint authentication. The system integrates fingerprint and electrocardiogram (ECG) data, utilizing a deep learning architecture based on efficient transformers. Feature-level fusion, incorporating stacking and channel-wise combination, is employed to create a robust representation. The integration of ECG-derived "Heartprint" data significantly enhances resistance to spoofing attacks. Rigorous evaluation on a multimodal dataset demonstrates the system's effectiveness, with a ResNet50 model achieving 99% accuracy in the multimodal configuration. Future research could explore alternative fusion strategies, such as feature selection, weighting, and decision-level fusion, to further improve system robustness. The primary limitations of the presented research lie in its restricted evaluation environment, potential vulnerabilities to adversarial attacks, and the exploration of a single fusion strategy.
In [18], the authors address the challenge of low-quality fingerprint images by proposing a deep learning-based enhancement approach prior to verification. The study experimented with various deep learning models, including SRCNN, FSRCNN, VDSR, and Finger Flow for minutiae extraction, in conjunction with a Siamese neural network for fingerprint verification. Results indicated a significant improvement in verification accuracy (62%) when using VDSR-enhanced images compared to original images (61%). To further enhance the system, the authors suggest integrating the three neural networks into a unified model and exploring diverse fingerprint datasets.

3. Proposed dataset

Here, we present our collected dataset, including the fingerprint images, featuring biometric characteristics from 20 individuals aged 18 to 70. This collection ensures a representative population cross-section, mirroring the demographics of the secondary dataset. Participants contribute ten distinct fingerprint images, resulting in a comprehensive compilation of 200 samples of finger images. Despite facing challenges such as variations in image size to emulate real-world scenarios in fingerprint recognition, the images are stored in JPG format. The precision and reliability of fingerprint acquisition are maintained through the use of the FS88HS model from Futronic's fingerprint scanner [15], renowned for its accuracy. Some samples of the collected dataset are shown in Figure 3.

4. Proposed model

The proposed methodology in this current study involves two steps: fingerprint preprocessing and subsequent verification within a pre-trained CNN (See Figure 4). Details of these steps can be found in the following sub-sections.

4.1. Preprocessing

Preprocessing is executed in two primary stages. The initial stage involves generating a minutiae vector for each fingerprint image, followed by the synthesis of a composite fingerprint image from three input fingerprints. The first stage comprises six sequential steps. Noise reduction and contrast normalization are applied to each fingerprint image in the dataset. Subsequently, an adaptive thresholding technique is employed to convert the image into a binary representation. Thinning of fingerprint ridges is performed using the Zhang-Suen algorithm [10] to enhance the definition of prominent ridge boundaries
for segmentation purposes. Boundary points are extracted from the thinned ridges, resulting in a minutiae vector represented by binary coordinates. In the subsequent preprocessing stage, the input fingerprint is aligned to a base fingerprint through minutiae vector comparison. The aligned input fingerprint is then subtracted from the base fingerprint to generate a residual image. This residual image, along with the aligned input fingerprint and the base fingerprint, constitutes the three input channels for a pre-trained Inception model. To construct the training set, all remaining

fingerprints of the same individual are utilized as input fingerprints and assigned to the "same" class. Fingerprints from different individuals are classified as the "not same" class.

Figure 3. Some samples of the proposed dataset.

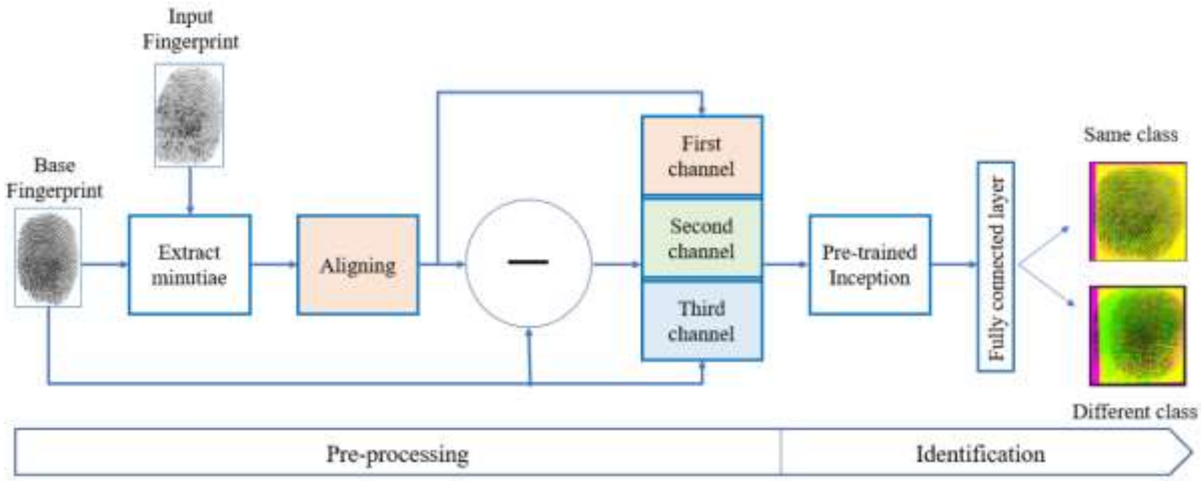

Figure 4. An overview of the proposed model, including two main steps: Pre-processing and verification.

4.2. Verification

The verification phase entails the utilization of the three-channel fingerprint output, derived from the preceding preprocessing stage, as input for a pre-trained Inception V3 model. A proposed architectural modification involves the elimination of the model's probability layer and its replacement with a flattened layer, followed by a Multi-Layer Perceptron (MLP) classifier. The resulting feature vector is subsequently subjected to classification by the aforementioned MLP. The classifier's primary function is to discriminate between "same" and "not same" classes, thereby affirming or refuting identity claims. Figure 5 shows the flowchart of the proposed model.

5. Experimental results

This section presents the details of the experimental results obtained from the proposed model, including the implementation details, datasets, ablation analysis, comparison with the state-of-the-art models and discussion on the results.

5.1. Implementation details

The Google Colab environment equipped with a GPU with approximately 7GB of available RAM and the Python programming language have been used in the implementation. The total training time for the model was approximately 20 minutes, involving 20 epochs with early stopping. The input shape of the proposed model is set to (299,299,3). The Adam optimizer with a learning rate of 0.0001 has been used in the model. To leverage the pre-trained network, we remove the final layer containing probabilities and introduce a flattened layer, along with two fully connected layers. We experiment with three different neuron numbers for the first fully connected layer: 8, 16, and 32. We do not train the pre-trained network.

5.2. Dataset details

This study leverages two distinct datasets. The first set originates from the Hong Kong Polytechnic University, featuring subsets categorized by two-dimensional touch-base and two-dimensional touch-less modalities. This comprehensive fingerprint dataset covers 336 individuals, each contributing six fingerprint impressions.

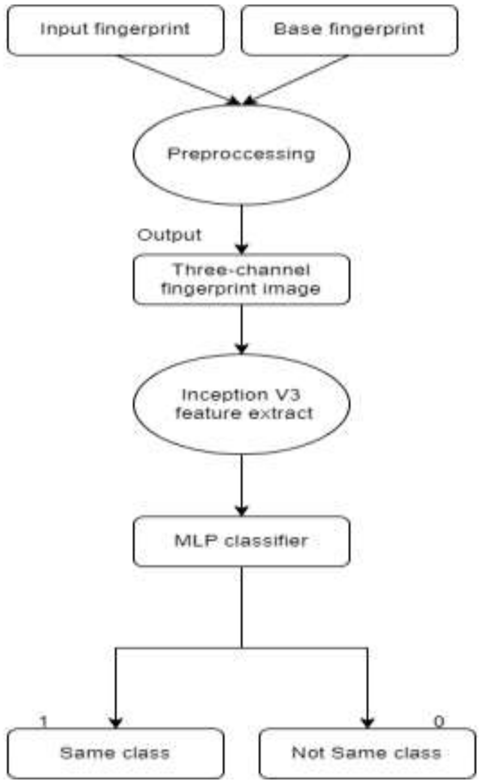

Figure 5. Flowchart of the proposed model.

Figure 6: Some samples of the fingerprint images from the Hong Kong Polytechnic University dataset.

Here, a subset of 120 fingerprint impressions from a diverse group of 20 individuals, spanning ages 18 to 70 and representing both genders, is employed. The images, provided in JPG format, consist of six fingerprint images per person. Despite potential influences on identity verification accuracy, such as image quality, viewing angle, and lighting conditions, this dataset ensures uniformity under consistent conditions for all mentioned factors. Each image is sized at 356*328. Some samples of the fingerprint images from the Hong Kong Polytechnic University dataset have been shown in Figure 6. The second dataset is a personally collected dataset that details of this dataset have been presented in section 3.

5.3. Model results

Here, we present the ablation analysis of the proposed model on two datasets (See Table 1).
To this end, different neuron numbers in the first fully connected layer of two pre-trained models, Inception [2] and Visual Geometry Group (VGG) [2], have been used. As Table 1 shows, using the 32 and 16 neurons in the Hong Kong Polytechnic University and our collected datasets with the Inception model have led to the highest verification accuracies of 99.40% and 99.16%, respectively. Furthermore, the model behavior during the train and test phases have been plotted in Figure 7. As this figure shows, the model gets to a stable behavior after training.

5.4. Comparison with state-of-the-art

In this sub-section, we compare the proposed model with the state-of-the-art models in the field. While there are a lot of works in the identity recognition, only few works have been presented in fingerprint verification. Here, we compare the results of the proposed model with the state-of-the-art model in fingerprint verification on the Hong Kong Polytechnique dataset. As this table shows, the proposed model outperforms the state-of-the-art model, obtaining the verification accuracy of 99.40 % on the Hong Kong Polytechnique dataset.

Table 1. Results of different neuron numbers in the first fully connected layer of the Inception model embedded in the proposed model on two datasets. Best results on each dataset, has been shown in bold.

Dataset	Hong Kong Polytechnic University dataset			Collected dataset		
Neuron number	8	16	32	8	16	32
Proposed model (Inception)	99.10	99.19	**99.40**	98.78	**99.15**	99.03
Proposed model (VGG19)	98.54	**98.75**	97.71	97.75	**98.12**	96.75

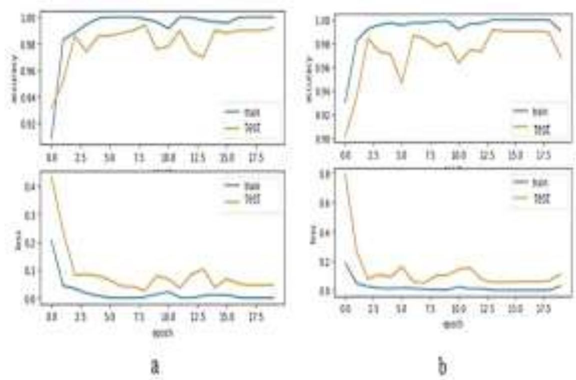

Figure 7. Accuracy and loss charts for the proposed model with the pre-trained Inception model on two datasets: (a) Hong Kong Polytechnic University dataset, (b) Collected dataset.

Table 2. Comparison results of the proposed model with the state-of-the-art model on the Hong Kong Polytechnique dataset. The best result has been shown in bold.

Model	Verification accuracy
[16]	98.91
Proposed model	**99.40**

5.5. Discussion

The proposed model demonstrated promising performance for fingerprint verification. A new image fusion technique integrated the original preprocessed image, a base image, and a residual image derived from the difference between the input and base fingerprint images into a unified RGB channel input, thereby enhancing feature representation. Image preprocessing optimized for both quality preservation and detail enhancement. Moreover, hyperparameter tuning, specifically the number of neurons in the first fully connected layer, was conducted across two datasets to empirically validate the model's robustness. A custom dataset comprising fingerprint images from 20 individuals was constructed to evaluate performance. Given the verification-centric application, a deeper focus on intra-class variability was prioritized over inter-class diversity. Consequently, the model was subjected to multiple test iterations using different subsets of 20 individuals and the results were discussed. Finally, we separately performed one-sample t-test analysis at a 5% alpha level to compare the average accuracies of two runs (first run includes 30 times of run and the second one contains 10 times of run). As Table 3 shows, it is highly likely that the mean verification accuracies of two runs are the same.

Table 3. Results of the t-test for the proposed model.

H_0	$\mu = 99.40\%$
H_1	$\mu \neq 99.40\%$
t-test	H_0 is accepted

6. Conclusion and future work

This paper presents an innovative methodology for fingerprint identity verification, integrating a pre-trained Inception v3 neural network model within a distinctive identity verification framework. The proposed approach entails meticulous data preprocessing, minutiae-based fingerprint alignment, and the generation of a color-enhanced network input, resulting in a notable level of accuracy in experiments conducted on two disparate datasets. The numerical outcomes underscore the model's excellence, attaining a noteworthy accuracy rate of 99.40% on the Hong Kong Polytechnic University dataset, thereby surpassing prevailing benchmarks. Furthermore, the model demonstrates a superior performance on the collected dataset, achieving an accuracy rate of 99.15%. This substantiates the proposed model as a fundamental advancement in fingerprint-based identity verification systems. The model's success can be ascribed to its comprehensive analysis of fingerprint details, surpassing specific features, and its innovative integration of preprocessed binary images in the RGB color space. Principal contributors to its performance encompass effective noise elimination, contrast adjustment, and meticulous alignment of fingerprint images. The utilization of neural networks, notably the Inception v3 model, underscores the transformative potential of deep learning methodologies in advancing fingerprint recognition capabilities. Beyond addressing intrinsic challenges in fingerprint recognition, this research makes a substantive contribution to the broader domain of biometric identity verification. The model's demonstrated performance positions it as a promising solution with applications spanning organizational, urban, medical, and security-related domains. Looking ahead, future research endeavors should explore the integration of fractal theory and fingerprint verification, offering an avenue for further investigation into the intricacies of biometric patterns. Moreover, expanding the dataset to encompass a larger subject pool (A greater number of individuals in the dataset) and a more extensive collection of fingerprint images will be considered.

References

[1] S.P. Kodgire and A. Mohan, “Automatic fingerprint recognition systems: A review”, *International Journal of Electronics, Communication and Soft Computing Science & Engineering (IJECSCSE)*, 2014.

[2] V. M. Praseetha, S. Bayezeed, and S. Vadivel, “Secure fingerprint authentication using deep learning and minutiae verification”, *Journal of Intelligent Systems*, 2019.

[3] C. Chinnappan and R. Porkodi, “Fingerprint recognition technology using deep learning: a review”, *SSRN Electronic Journal*, 2021.

[4] Garn, Bernhard, et al. "A Two-Step TLS-Based Browser fingerprinting approach using combinatorial sequences." *Computers & Security*, (2022)

[5] Xue, Mingfu, et al. "LOPA: a linear offset based poisoning attack method against adaptive fingerprint authentication system." *Computers & Security*, (2020)

[6] Azarnoush, Arash and Kourosh Kiani. " Improving the performance of an HMM-based fingerprint recognition system." *World Symposium on Computer Applications & Research (WSCAR)*, Sousse, Tunisia, (2014).

[7] Karbab, ElMouatez Billah, et al. "Scalable and robust unsupervised android malware fingerprinting using community-based network partitioning." *computers & security*, (2020)

[8] Yang, Wencheng, et al. "A linear convolution-based cancelable fingerprint biometric authentication system." *Computers & Security*, (2022)

[9] Deshpande, Uttam U., et al. "CNNAI: a convolution neural network-based latent fingerprint matching using the combination of nearest neighbor arrangement indexing." *Frontiers in Robotics and AI* (2020).

[10] Minaee, Shervin, et al. "Biometrics recognition using deep learning: A survey." *Artificial Intelligence Review* (2023).

[11] Ammour, Nassim, Yakoub Bazi, and Naif Alajlan. "Multimodal Approach for Enhancing Biometric Authentication." *Journal of Imaging* (2023).

[12] Dalvi, Nikita, and Van Vung Pham. "Deep Learning Approaches for Fingerprint Verification.", Institute for Homeland Security (2023).

[13] Feng, Yulin, and Ajay Kumar. "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* (2023).

[14] Ezebiejesi, Jude, and Bir Bhanu. "Patch based latent figerprint matching using deep learning." *25th IEEE International Conference on Image Processing (ICIP), Athens* ,IEEE, (2018).

[15] Yag, Xinfeng, Qiping Hu, and Shuaihao Li. "Recogntion and classification of damaged fingerprint based on deep learning fuzzy theory." *Journal of Intelligent & Fuzzy Systems* (2020).

[16] Wag, Ruxin, Congying Han, and Tiande Guo. "A novel figerprint classification method based on deep learning." *23rd International Conference on Pattern Recognition (ICPR) Cancun,* IEEE, (2016).

[17] Nimal, Sunil B., and Kishor S. Kinage. "Contactless fingerprint recognition and fingerprint spoof mitigation using CNN." *IJRTE*, (2019).

[18] Mnaee, Shervin, Elham Azimi, and Amirali Abdolrasidi. "Fingernet: Pushing the limits of fingerprint recognition using convolutional neural network." *arXiv preprint arXiv*, (2019).

مدل مبتنی بر یادگیری عمیق برای تأیید اعتبار اثر انگشت

مبینا طالبیان، کوروش کیانی* و راضیه راستگو

دانشکده برق و کامپیوتر، دانشگاه سمنان، سمنان.

ارسال ۲۰۲۴/۰۳/۰۹؛ بازنگری ۲۰۲۴/۰۷/۰۸؛ پذیرش ۲۰۲۴/۰۸/۱۶

چکیده:

احراز هویت با استفاده از اثر انگشت به عنوان یکی از پایه‌های اصلی تأیید هویت شخصی می‌باشد. در این مقاله، چارچوبی مبتنی بر یادگیری عمیق برای بهبود دقت این فرایند حیاتی معرفی می‌گردد. با ادغام مدل از پیش آموزش دیده Inception با یک معماری سفارشی، مدلی ارائه می‌دهیم که به طور مؤثر ویژگی‌های تمایزدهنده را از تصاویر اثر انگشت استخراج می‌کند. در این راستا، تصویر اثر انگشت ورودی از طریق مقایسه بردار نقاط شاخص با اثر انگشت پایه هم‌تراز می شود. سپس اثر انگشت ورودی هم‌تراز شده از اثر انگشت پایه کسر می شود تا یک تصویر باقی‌مانده ایجاد شود. این تصویر باقی‌مانده، همراه با اثر انگشت ورودی هم‌تراز شده و اثر انگشت پایه، سه کانال ورودی را برای یک مدل از پیش آموزش دیده Inception تشکیل می‌دهند. نوآوری اصلی ما در هم‌ترازی نقاط شاخص اثر انگشت و سپس ساخت یک نمایش رنگی از اثر انگشت می‌باشد. علاوه بر این، ما یک مجموعه داده جمع‌آوری کردیم که شامل ۲۰۰ تصویر اثر انگشت مربوط به ۲۰ نفر برای تأیید هویت است. روش پیشنهادی ما بر روی دو مجموعه داده‌های مختلف ارزیابی شده و برتری آن نسبت به مدل‌های موجود فعلی نشان داده شده است. با دقت تأیید ۹۹,۴۰٪ بر روی مجموعه داده عمومی هنگ کنگ، رویکرد ما معیار جدیدی در احراز هویت اثر انگشت ایجاد می‌کند. این پژوهش پتانسیل کاربرد در حوزه‌های مختلفی از جمله اجرای قانون، کنترل مرزی و سیستم‌های دسترسی امن را دارد.

کلمات کلیدی: اثر انگشت، تأیید هویت، یادگیری عمیق، از پیش آموزش‌دیده شده، شبکه عصبی پیچشی.