ISSN: 0067-2904

Fingerprint Forgery Detection and Person Identification Based on Deep Learning

Mohammed Abdul Ameer Jabbar[1], Abdulkareem Merhej Radhi[2]*, Sabreen A.Zahra Mghames [3], Suhad Faisal Behadili [4], Muneera Alsaedi[1]

[1]*Department of Intelligent Systems, College of Biomedical Informatics, University of Information Technology and Communications, Baghdad, Iraq*

[2]*Department of Computer Science, College of Science, Al-Nahrain University, Baghdad, Iraq*

[3]*Department of Scholarships and Cultural Relations / University of Information Technology and Communications, Baghdad, Iraq*

[4]*Department of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq*

Received: 27/5/2024 Accepted: 21/11/2024 Published: 30/12/2025

Abstract

Automated fingerprint recognition and authentication have been widely used in biometrics applications and as a personal identity tool due to their dependability and unique characteristics. The person's fingerprint must be authentic and not altered or forged to be used to verify that person's identity. It is more difficult to determine whether a fingerprint is real /authenticated. The presented work aims to design two models based on a convolutional neural network (CNN) with the ability to detect whether the fingerprints are authenticated or not. The proposed methodology includes two levels: the first involves forgery detection of fingerprints. Whereas the second level examines fingerprint identification. Furthermore, a reliable deep learning technique that includes Transfer Learning (TL) and building the architecture of CNN from scratch was utilized to diagnose and identify fingerprints for 100 persons using the SOCO dataset. Thus, the results recorded higher accuracy at 98.69% and 99.08% sensitivity of forgery detection. Furthermore, it achieved an optimal rate for matching fingerprints and outperformed other TL models (VGG16, VGG19, ResNet50) and related works. For this reason, it could be considered a successful model for Biometric fingerprint authentication and forgery detection.

Keywords: Automated matching fingerprint, Biometric fingerprint authentication, Fingerprint forgery detection, CNNs, Deep learning.

الكشف عن تزوير بصمات الأصابع وتحديد هوية الشخص بناءً على التعلم العميق

محمد عبد الأمير جبار عيسى[1], عبد الكريم مرهج راضي [2] *, صابرين عبد الزهرة مغامس[3], سهاد فيصل البهادلي[4] , منيرة الساعدي[1]

[1] قسم الأنظمة الطبية الذكية، كلية المعلوماتية الطبية الحيوية، جامعة تكنولوجيا المعلومات والاتصالات، بغداد، العراق

[2] قسم علوم الحاسوب، كلية العلوم، جامعة النهرين، بغداد، العراق

[3] قسم البعثات والعلاقات الثقافية، جامعة تكنولوجيا المعلومات والاتصالات، بغداد، العراق

[4] قسم علوم الحاسوب، كلية العلوم، جامعة بغداد، بغداد، العراق

*Email: abdulkareemradhi@gmail.com

الخلاصة

تم استخدام التعرف الآلي على بصمات الأصابع والمصادقة عليها على نطاق واسع في تطبيقات القياسات الحيوية وأداة التعرف على هوية الشخص نظرًا لموثوقيتها وخصائصها الفريدة. يجب أن تكون بصمة الشخص أصلية وغير معدلة أو مزورة حتى يمكن استخدامها للتحقق من هوية ذلك الشخص، ومن الصعب تحديد ما إذا كانت بصمة الإصبع حقيقية / موثوقة. يهدف العمل المقدم إلى تصميم نموذجين يعتمدان على شبكة عصبية ملتوية (CNN) مع القدرة على اكتشاف ما إذا كانت بصمات الأصابع موثوقة أم لا. تتضمن المنهجية المقترحة مستويين: المستوى الأول يتضمن الكشف عن تزوير بصمات الأصابع. في حين أن المستوى الثاني التعرف على هوية الشخص من خلال بصمات الأصابع. علاوة على ذلك، تم استخدام تقنية التعلم العميق الموثوقة التي تتضمن التعلم الانتقالي (TL) وبناء بنية CNN من الصفر من أجل تشخيص وتحديد بصمات الأصابع لـ 100 شخص باستخدام مجموعة بيانات SOCO. وبالتالي، سجلت النتائج دقة أعلى بنسبة 98.69٪ وحساسية 99.08٪ للكشف عن التزوير. علاوة على ذلك، فقد حقق معدلًا مثاليًا لمطابقة بصمات الأصابع وتفوق على نماذج TL الأخرى (VGG16 وVGG19 وResNet50) والأعمال ذات الصلة. لهذا السبب، يمكن اعتباره نموذجًا ناجحًا لمصادقة بصمات الأصابع البايومترية وكشف التزوير.

1. Introduction

Fingerprint recognition is extremely popular due to its success in a wide range of applications, including government, forensic, and civilian domains [1]. Biometric systems have developed as revolutionary security systems in pattern recognition tasks [2]. For instance, face detection [3], contactless palm-vein [4], and forgery detection [5] due to the rapid development of information technology [6]. In general, verification or identification forms the basis of the biometric information system. Based on the person's claimed individuality, the verification system seeks to confirm that they are unique. Contrarily, the identification system establishes the individual identity (among individuals registered in the expert system) without allowing the user to contest their specifications [7].

One of the most frequent threats to biometric security systems is the use of forgery biometrics. For instance, it is simple to create phony fingerprints utilizing gummy fingers made from particular components like silicone, wood glue, and gelatin [8]. Modern advanced technologies make use of widespread adoption and ubiquity to support the anti-theft system. The increased crime rate makes figuring out the answer and identifying the fingerprint a difficult process. To overcome these issues, Artificial Intelligent methods propose solutions for spoofed fingerprint detection [9].

The issue of forgery detection was thoroughly researched, and falsified fingerprints have a significant negative impact on the performance of biometric-based security systems. Many algorithms have been discussed previously to address this issue. However, they struggle to improve their security performance [10]. Biometric authentication has drawn a lot of attention because of its uniqueness, non-replicability, heredity, and invariance.

Today, one-to-many, which is called identification tasks, and one-to-one tasks, known as matching or (authentication) are two common uses for fingerprint identification systems globally. For sensitive real-world applications like banking transactions, computer/cellphone security, forensics, and cross-border transactions, they are able to recognize individuals reliably [11]. Biometric verification is widely used in a variety of access control applications, such as border control, forensic science, smartphone access, attendance systems, and so on. Biometric systems can be built to use physiological (e.g.,

fingerprint, face, iris) or behavioral (e.g., stride, keystroke, voice) biometrics or a combination of the two.

Face, iris, and fingerprint have dominated the majority of applications because of their dependability and precision in performance, which can be linked to the uniqueness of these biometric characteristics. However, fingerprint biometrics is one of the traditional biometric characteristics used in a variety of applications due to the long-term reliability of finger patterns and the representation and matching of features that can achieve a billion fingerprint comparisons in a single second with high accuracy [8]. Moreover, when adapted to highly secure access control applications, the flaws of fingerprint authentication systems have created security concerns. Machine learning and other recent deep learning approaches have been studied in terms of fingerprint classification, detection, and authentication. Moreover, Fingerprint Presentation Attack Detection (FPAD) approaches are critical for providing effective fingerprint authentication [10]. In the aspect of biometric fingerprint authentication, an approach to fingerprint recognition based on sparse proximity has been proposed in [12]. The purpose was to assess the vulnerabilities of a higher resolution fingerprint sensor (operating at 1000 dpi) without applying a decision threshold but only considering the comparison scores returned by the matcher. This will allow us to better understand the processes involved in the reproduction of fake fingerprint information. figures 1, shows the altered process of fingerprint images.

Figure 1: Deposited fingermark (left), final image (middle) after processing with Adobe Photoshop1 CS2, and capture (right) taken from the final fake fingerprint built with glue from an indirect cast printed on an acetate sheet [12].

Another aspect of fake fingerprint classification depends on changing color when it contacts a hard surface. Thus, imitation fingers can be identified. Once a finger pushes a hard surface, the force used alters the blood flow, giving the area a whiter appearance than it would in a normal, uncompressed region. A technique to identify and measure this color change is suggested and utilized to distinguish the real finger from imitations [13].

Based on what was mentioned, we can conclude that verifying a fingerprint is the process of determining its reliability and whether it is fake or original. In contrast, fingerprint identification is the process of matching its features by comparing fingerprints to those stored in a database. As a result, the research problem raises an important question: **how can we ensure that the fingerprint is not forged while also being identical?** Certainly, addressing both issues together will result in more secure and accurate fingerprint authentication. Therefore, in this paper, we introduce a powerful system that can handle both issues of fingerprint authentication (forgery detection and

matching person identity) utilizing deep learning techniques based on the CNN algorithm. Moreover, this research contributes a novel approach to increase the security of biometric fingerprint verification based on two levels of security. The first level involves forgery fingerprint detection by utilizing two phases: the first phase implements transfer learning techniques (TL) which include VGG16, VGG19, and Resnet50, while the second phase includes developing the CNN model from scratch [14] in order to obtain the best detection results. The second level of security involves fingerprint person identification (matching) while the best model from the proposed first level is selected to do this issue. Ultimately, the decision is made using the verified and authenticated fingerprints following the suggested two levels.

The rest of the paper will present in Section 2 the related works that explore other studies' contributions and limitations. The description of used dataset is found in section 3. In Section 4 the proposed methodology is explored. In addition, section 5 presents the discussion of the results, and then section 6 declares the concluded issues with future perspectives.

2. Related Works

In this section, several related works based on fingerprints (classification, recognition, and detection) are presented. Each study was explained as the main contribution, and method used in addition to the obtained results.

- This study [15] refers to utilizing the CNN as TL for individual hands and gander fingerprints classification using the SOCOFing dataset. The results achieved from proposed TL models were accuracy of 75.2%, 93.5%, and 76.72%, respectively.
- The author in [16] proposed fingerprint liveness detection based on machine learning algorithms using LivDet 2019 Dataset, the features were extracted from CNN and used to train the proposed machine learning algorithms, which include, K-Nearest Neighbors, Logistic Regression, and Naïve-Bayes (NB) classifiers. The best classification results were achieved at an accuracy of 95% in NB.
- In [17] the authors introduced an approach based on a fingerprint image taken by a 1310 nm laser device and compared the long short-term memory (LSTM) network to several CNN models. The collected experimental findings show that the LSTM model outperforms the CNN models.
- The authors in [18] used a fully convolutional neural network (FCN) to assess FPAD performance under various sensing modalities. The studies are conducted using fingerprint pictures collected in the visible (VIS), near-infrared (NIR), SWIR, LSCI, and near-infrared back-illumination domains. The overall fingerprint recognition accuracy achieved 97.11%.
- In [19] the authors suggested a novel One-Class presentation attack detection (OCPAD) approach for fingerprint images that provides an internal representation of the fingertip skin rather than a basic feature. The proposed OCPAD framework comprises reference bona fide modeling based on auto-encoder networks and achieved robust classification results.
- The authors in [20] propose fingerprint classification based on deep learning state of art in order to classify the left and right-hand fingerprints. This study aimed to speed up the process of distinguishing individual identification. They used the methods CNN, vgg16, Resnet50, and Yolo-v2 and achieved the highest results of accuracy at 90.98% for the left-right hand in the Yolo-v2 model, and the highest accuracy at 91.29% for the sweat-pore classification in Resnet50 model.

- In [21], the authors implemented deep learning based on fingerprint identification. They proposed a combination of pre-processing techniques and TL, and the result of this experiment achieved an accuracy of 89% using the inception-Resnet model.
- In paper [22], the author also used CNN based on image processing techniques, including (histogram equalization and Gabor filter) to enhance the input fingerprint images. The original fingerprint images were taken from a scanner finger device with a size (480,320). The enhanced images were used to train the CNN model, and the results show classification accuracy for both the training and testing model at 98.21 with 0.9 loss in 10 epochs.
- In [23], the authors proposed a fingerprint classification based on TL Vgg-16 and machine learning algorithms including random forest, SVM) and Deep Neural Network (DNN). The dataset was integrated and classified according to dry, doted, damaged, wet, and blurred fingerprint classes. This experiment achieved classification results of 93% for dry fingers as the highest performance using vgg16 based on DNN, and 84% for the lowest performance for blurred fingerprints.
- In [24], this study points to the knuckle print recognition method using a robust features algorithm that has been accelerated. The test results also demonstrate a very low computation time required to match the fingerprint for identification, with an excellent accuracy rate of 96.91%.
- [25] proposed fingerprint image identification based on frequency domain and deep learning methods. The method includes CNN, LSTM, and multi-layer perceptron (MLP), the spectrum CNN model obtained the best classification accuracy of 96.4%.
- In [26] the authors focused on the use of radio frequency fingerprints of the signals sent from the controller to the micro aerial vehicle (micro-UAV) for detection and classification of fingerprint using machine learning, and the results achieved an accuracy of 96.3 using the k-Nearest Neighbors.
- The authors in [27] proposed real/altered fingerprint classification based on texture features (HOG and SFTA) and two classifiers DCA, and GDA. This experiment was trained/tested using the SOCOFing dataset. The dataset was divided into 70% training and 30% testing with K-fold (k=10) cross-validation technique. The experimental results show outperforming in accuracy for classifier GDA over DCA for both features. For the easy-altered images, the GDA classifier achieved accuracy of 95% with HOG and 99% with SFTA features. while in hard-altered images, the GDA achieved accuracy of 93% and 97% for HOG and SFTA, respectively.

These recent studies refer to fingerprints in terms of (classification, detection, and recognition). However, the accurate and robust fingerprint authentication system relies on handling both issues (forgery/altered, and matching). Therefore, this study aims to handle both issues by introducing an accurate fingerprint authentication system that can be more generalized.

3. Description of Used Dataset

The SOCOFing (Sokoto Coventry Fingerprint Dataset) is a biometric fingerprint database created for academic study. SOCOFing is composed of 6,000 fingerprint photos from 600 African participants. It includes unique properties such as labels for gender, hand and finger names, and synthetically altered versions with three levels of alteration for obliteration, central rotation, and z-cut [28]. The samples of the dataset can be seen in Figure 2.

(a) (b) (c) (d)

Figure 2: Images samples of fingerprint datasets: a: easy altered level, b: medium altered level, c: hard altered level, d: Real sample

4. Proposed Methodology

The proposed methodology of the fingerprint authentication system consists of two levels. The first level involves selecting the best detection model with a higher detection rate. This level can be partitioned into three phases. The first phase is concerned with data integration and preprocessing techniques. This phase includes converting images into appropriate color models (gray level or RGB), image resizing at a fixed size (96*96), and data normalization.

The second phase is related to applying the TL techniques presented by CNN architecture history of VGG16, VGG19, and ResNet50 to solve the detection forgery of biometric fingerprints dataset and then select the best one according to the higher detection rate of testing results. According to previous studies, the TL techniques achieved efficient performance in classification and detection tasks. The third phase is concerned with building the CNN from scratch to increase the power of detection of fingerprint forgery by comparing it with the best-proposed models from the second phase. After we solve the problem of forgery detection from the proposed first level of methodology, the second level comes to handle fingerprint matching and identification issues. Figure 3 illustrates the block diagram of the proposed system.

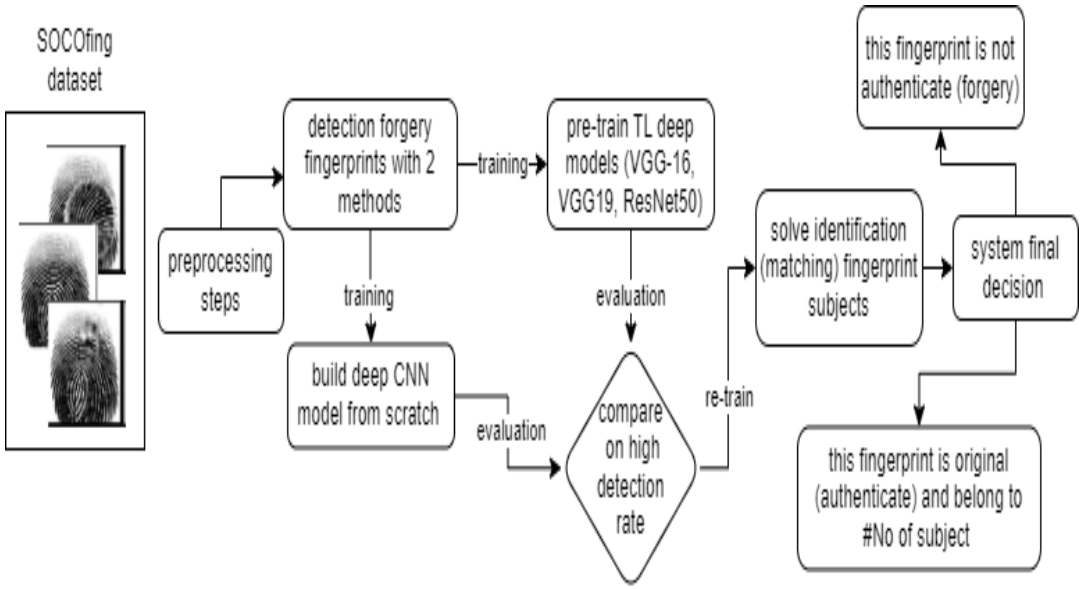


Figure 3: The block diagram of the proposed forgery detection and matching system

4.1 Preprocessing and Preparing the Dataset

In this paper, the examined images of gray level and four classes presented as (Easy, Medium, Hard, and Real) fingerprints. In order to prepare the dataset to start the proposed methodology of forgery detection and fingerprint identification , the original images are resized from the original size at (96*103) into (96*96) with one channel (gray-scale). This speeds up the training process to make the image dimensions equal because there is no need to use the zero-padding technique in the input convolution layer. The input images are normalized at 1/255 as pixel rescaling. In addition, the splitting procedure is one for all experiments at (80%,10%, and 10%) as training, validation, and final prediction tests.

4.2 Proposed forgery detection utilizing pre-trained TL

This section presents the details of the TL detection forgery models. The proposed TL models (vgg16, vgg19, and ResNet50) are fine-tuned to be suitable for this task. The last Fully Connected (FC) layers are removed and replaced as follows: two FC were fine-tuned in two hidden layers (H1, H2) with activation function rectified linear unit (relu) and Softmax output layer with 4 classes according to dataset class labels. The H1 layer contains 100 units and relu followed by the Dropout layer with a dropping rate at (0.5) to avoid the overfitting problem, while the second H2 contains 20 units also with a relu activation function. The training process was done on 80% of all samples in the dataset which includes 7379 images belonging to 4 classes, while 20% of all samples utilized for the evaluation process included 1844 images. In addition, the proposed TL models are compiled using the Adam optimizer with various learning rates from (0.001 to 0.00001) and cross-entropy as a loss function.

4.3 Proposed forgery detection model utilizing CNN from scratch

This experiment has been proposed to solve the detection and matching issues in the same architecture. Thus, the performance of TL models doesn't achieve the optimal detection results in the fingerprint dataset. The CNNs from scratch have been built to handle this problem to optimize the detection rate. Figure 4 shows in detail the proposed model architecture of this experiment.

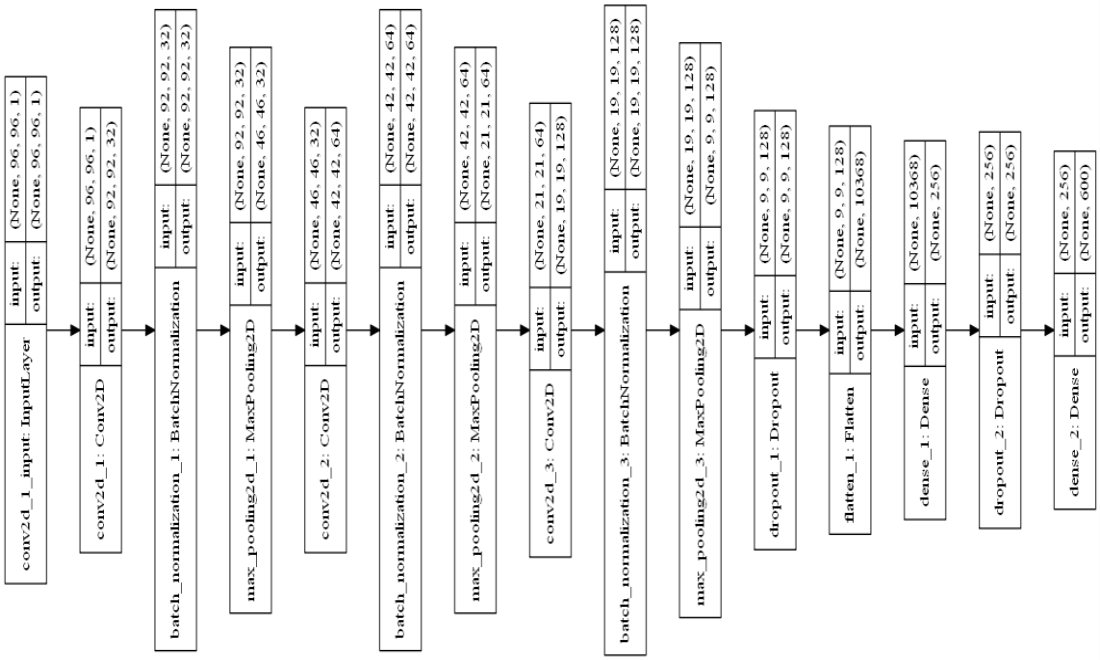


Figure 4: The proposed CNN model architecture of detection and machining fingerprint

This model is also optimized utilizing (Adam) with a learning rate at 0.0001 and cross-entropy loss function. Furthermore, two layers of the dropout regularization technique with a dropping rate (0.4) are utilized to avoid the overfitting problem. The input size of the fingerprint image is 96*96 with 1 channel (grayscale) image.

5. Results and Discussion

The experimental results of the proposed methodology of fingerprint authentication based on two levels are presented in this section. The obtained results are presented as tables, figures, and images. In addition, this experiment was implemented using Python 3.9 and Keras. All proposed models are trained on GPU 6GB 4060 Nvidia, 32 RAM, and core-i7 at 12^{th} generation.

5.1 Fine-tuned TL Results

This section will explore the results obtained from the evaluation process of the proposed fine-tuned models. The classification results have been illustrated in Table 1, including the metrics on the testing phase at accuracy, Mean Square Error (MSE), and Area Under Curve (AUC).

Table 1: The Fine-tuned TL classification results

Proposed TL pre-trained models	Testing Accuracy %	MSE	AUC %
VGG-16	76.68	0. 1725	78.75
VGG-19	77.91	0.1546	79.45
ResNet50	62.55	0.3384	51.41

According to the classification results illustrated in Table (1); this experiment shows the proposed VGG-19 altered model achieved higher classification accuracy at 77.91 than others. The area under cover AUC metrics reached 0.79, and the Mean square error (MSE) was also high. In general, the model performance according to the classification results was not optimal because of the similarity between features in the dataset classes. In order to analyze this case study, the histogram was applied to understand this issue by taking 4 images with information (person number 1, Male, left fingerprint: all images belong to the same person and same fingerprint). Each image presented the type of dataset class labels for one subject (one-person fingerprint). Figure 5 shows the original images, whereas Figure 6 illustrates the histogram of these fingerprint images.

Figure 5: The dataset classes from left to right (easy, medium, hard, real) respectively

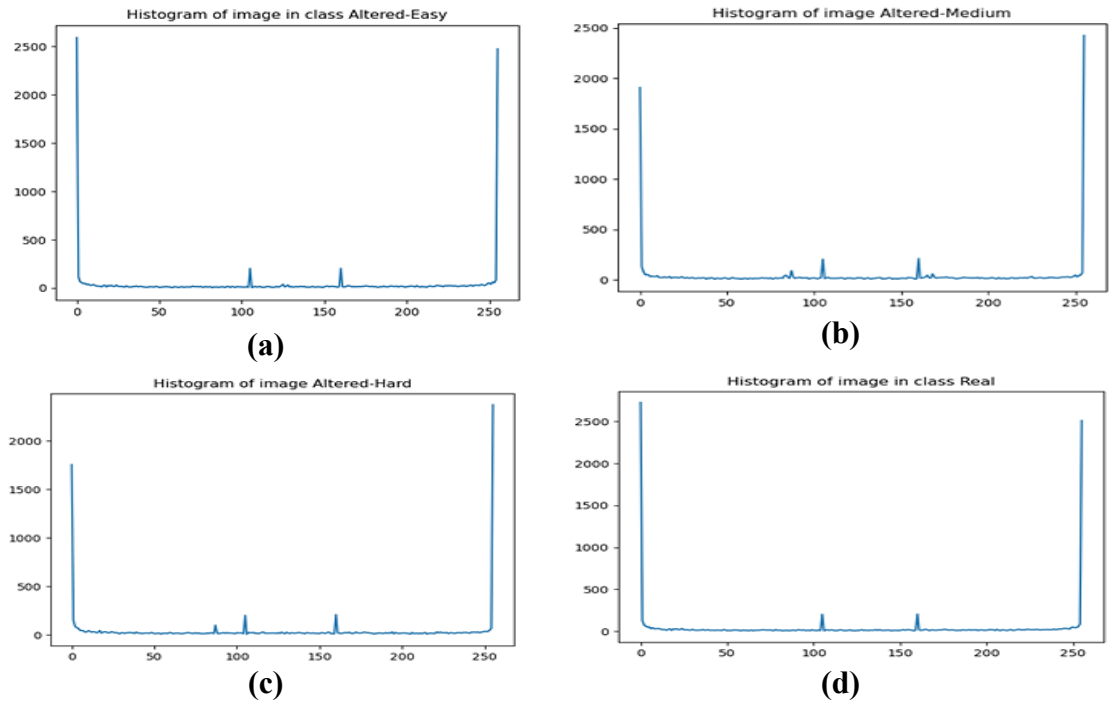


Figure 6: The Histogram of fingerprint images based on each class as in (a). Easy, (b). Medium, (c). Hard, (d). Real

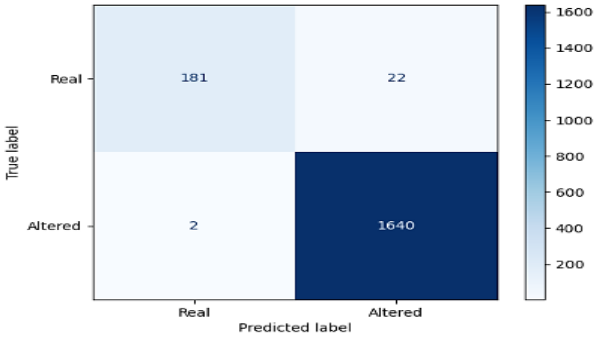
The similarity of fingerprint histograms refers to the difficulty of the model to recognize and distinguish between all fingerprint classes according to grey-level color distribution. Furthermore, shape features are almost the same. Therefore, the second phase of this paper was proposed to handle these issues by designing feature maps that were built from scratch. The design of the features map for convolutional layers must focus on edge detection features more than shape and color distribution. Furthermore, the altered level classes also must be combined as one class named (forgery) due to the similarity between features.

5.2 The Proposed Forgery Detection Results

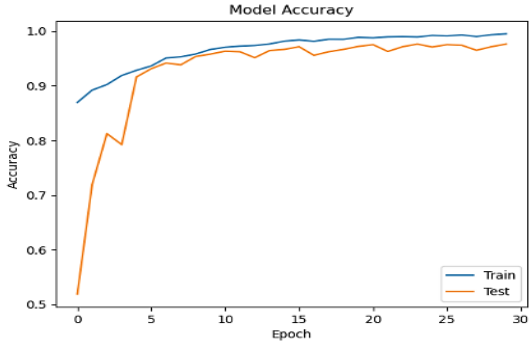
This experiment involved combining the altered versions into one class and designing the CNN model to be more suitable to improve the detection rate. Figure 7 shows the confusion matrix and the curve of training/testing process accuracy and loss across 30 epochs, which show how this proposed method improved the performance of detecting forgery in the fingerprint. The results show an improvement in the detection performance of biometrics fingerprint images. The comparison between the first and second experiments, including the classification metrics of the proposed detection method, is shown in Table 2, which refers to the model accuracy, MSE, precision, recall, and F1-score. The comparison between the first and second experiments, including the classification metrics of the proposed detection method, is shown in Table 3, which refers to the model accuracy, MSE, precision, recall, and F1-score.

Table 2: The comparison and classification results of the detection model

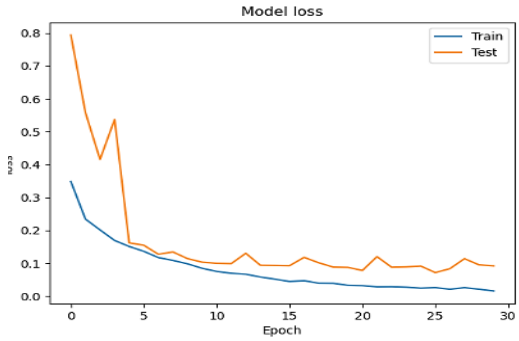
The proposed detection model	Accuracy %	MSE	Precision	Recall	F1-score	AUC %
Pretraind-VGG19	77.91	0.1546	0.5892	0.3850	0.4871	79.45
Proposed detecting model	98.69	0.0130	0.9868	0.9988	0.9927	96.88



(a) The confusion matrix of the proposed model



(b) Training/testing model accuracy on 30 epochs



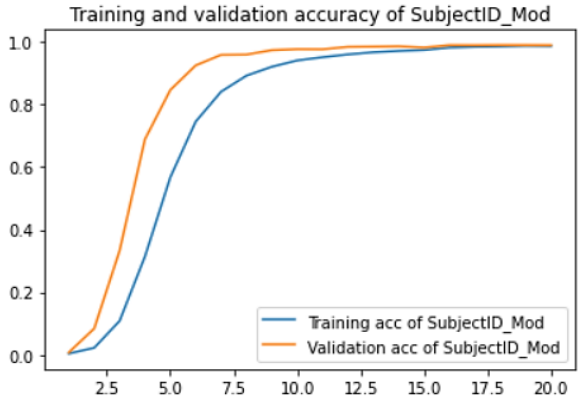
(c) Training/testing model loss on 30 epochs

Figure 7: Confusion matrix and training/testing results as in subfigure: (a). on 30 epochs, while (b). Model accuracy, (c). Model loss

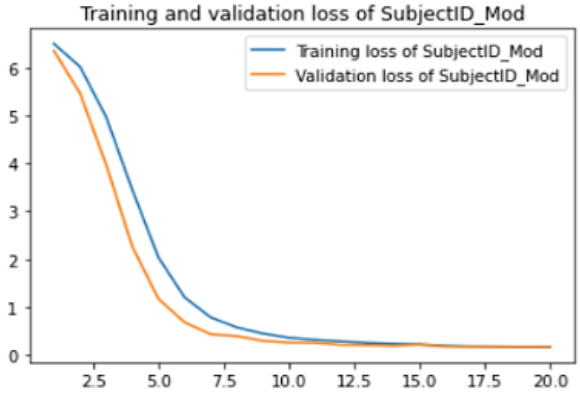
According to the classification performance, which appears in Table 3, the proposed fingerprint detection forgery model achieved the best detection rate at accuracy that reached 98%. Furthermore, the AUC of the ROC curve also improved at 96% compared with pre-training TL models.

5.3 The Proposed Model Identification / Matching Results

This section is related to utilizing the best model performance to solve the problem of identification in order to improve the authentication of subject fingerprints. Therefore, the same architecture of the proposed detection model was used to handle subject identity and matching tasks. Figure 8 shows the training/testing accuracy/loss of identification subjects, while Figure 9 shows the prediction results of the proposed model performance on random samples of subject fingerprints.



(a) Training/testing model accuracy



(b) Training/testing model loss

Figure 8: The training/testing of the proposed fingerprint identification model, as in subfigures (a). Model accuracy, (b). Model loss

(a) Matched person ID 31 **(b)** Matched person ID 75 **(c)** Matched person ID 97

Figure -9 The proposed model prediction matching on random subjects (a). Matched PERSON ID 31, (b). Matched PERSON ID 75, (c). Matched PERSON ID 97

As a result, figure 8 (a, b) refers to the training and testing process of the proposed model when achieving the optimal testing accuracy and loss of personal identity. In addition, the best matching fingerprint in model prediction results, as shown in Figure 9 (a, b, and c), refers to completely identifying which images belong to which person from (1 to 100).

5.4 Comparing with other related works

For the comparison with other related works, table 3 shows the proposed model performance with similar tasks of fingerprint classification and forgery detection and other related problems.

Table 3: The comparison of the proposed model and other related works

Authors	Methodology	Obtained results of Accuracy %
In **[15]**	Three CNNs based on the TL model	75.2%, 93.5%, and 76.72%
In **[29]**	Presentation attack fingerprint recognition	Above 90%
In **[16]**	Forgery fingerprint detection	95%
Pretraind-Vgg19	**Proposed Fine-tuned TL, the best model Vgg19**	**77.91**
Proposed detection model	**Proposed forgery detection and matching model architecture**	**98.69**

6. Conclusions

In this study, we introduced a new powerful method for fingerprint authentication based on two levels of security, including forgery detection and matching fingerprints. The proposed model achieved the best detection accuracy at 98.69 and 99.8% of sensitivity when tested on the SOCO-fig dataset. However, unlike the recent study, which utilizes only one task, for instance (detection or recognition), our proposed model considers all altered classes (easy, medium, hard). Furthermore, this model was used for detection and achieved 100% matching fingerprint when tested on 100 persons in the same dataset. Even though the success of transfer learning in large areas of image classification tasks, it still had some issues with performance when the datasets seemed to be similar in classes, as shown in the first phase of this study. As a result, the proposed model was carefully developed from scratch, addressing all issues of transfer learning and obtaining an impressive detection rate. For the future directions, we can generate more than three forgery classes using generative AI. In

order to ensure a strong defense system and increase the model's ability to detect and prevent advanced threats.

References

[1] P. M. A. Hambalık, "Fingerprint recognition system using artificial neural network as feature extractor: design and performance evaluation," *Tatra Mt. Math. Publ,* vol. 67, pp. 117-134, 2016, doi: 10.1515/tmmp-2016-0035.

[2] S. Kouamo and C. Tangha, "Fingerprint recognition with artificial neural networks: application to e-learning," *Journal of Intelligent Learning Systems and Applications,* vol. 8, no. 02, p. 39, 2016, doi: 10.4236/jilsa.2016.82004.

[3] M. Rostami, A. Farajollahi, and H. Parvin, "Deep learning-based face detection and recognition on drones," *Journal of Ambient Intelligence and Humanized Computing,* vol. 15, no. 1, pp. 373-387, 2024/01/01 2024, doi: 10.1007/s12652-022-03897-8.

[4] D. Luo, J. Huang, W. Yang, M. S. Shakeel, and W. Kang, "RSNet: Region-Specific Network for Contactless Palm Vein Authentication," *IEEE Transactions on Information Forensics and Security,* vol. 20, pp. 2734-2747, 2025, doi: 10.1109/TIFS.2025.3544029.

[5] L. Ma, P. Yang, Y. Xu, Z. Yang, P. Li, and H. Huang, "Deep learning technology for face forgery detection: A survey," *Neurocomputing,* vol. 618, p. 129055, 2025/02/14/ 2025, doi: https://doi.org/10.1016/j.neucom.2024.129055.

[6] K. N. Win, K. Li, J. Chen, P. F. Viger, and K. Li, "Fingerprint classification and identification algorithms for criminal investigation: A survey," *Future Generation Computer Systems,* vol. 110, pp. 758-771, 2020, doi: 10.1016/j.future.2019.10.019.

[7] R. F. Nogueira, R. de Alencar Lotufo, and R. C. Machado, "Fingerprint liveness detection using convolutional neural networks," *IEEE transactions on information forensics and security,* vol. 11, no. 6, pp. 1206-1213, 2016, doi: 10.1109/TIFS.2016.2520880.

[8] H. Li and R. Ramachandra, "Deep learning based fingerprint presentation attack detection: A comprehensive Survey," *arXiv preprint arXiv:2305.17522,* 2023, doi: 10.48550/arXiv.2305.17522.

[9] R. Tolosana, M. Gomez-Barrero, J. Kolberg, A. Morales, C. Busch, and J. Ortega-Garcia, "Towards fingerprint presentation attack detection based on convolutional neural networks and short wave infrared imaging," in *2018 international conference of the biometrics special interest group (BIOSIG)*, 2018: IEEE, pp. 1-5, doi: 10.23919/BIOSIG.2018.8553413.

[10] J. Galbally, J. Fierrez, and R. Cappelli, "An Introduction to Fingerprint Presentation Attack Detection," in *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection*, S. Marcel, M. S. Nixon, J. Fierrez, and N. Evans Eds. Cham: Springer International Publishing, 2019, ch. 1, pp. 3-31.

[11] S. Hemalatha, "A systematic review on Fingerprint based Biometric Authentication System," in *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)*, 2020: IEEE, pp. 1-4, doi: 10.1109/ic-ETITE47903.2020.342.

[12] M. Espinoza, C. Champod, and P. Margot, "Vulnerabilities of fingerprint reader to fake fingerprints attacks," *Forensic science international,* vol. 204, no. 1-3, pp. 41-49, 2011, doi: 10.1016/j.forsciint.2010.05.002.

[13] W.-Y. Yau, H.-T. Tran, E.-K. Teoh, and J.-G. Wang, "Fake finger detection by finger color change analysis," in *Advances in Biometrics: International Conference, ICB 2007, Seoul, Korea, August 27-29, 2007. Proceedings*, 2007: Springer, pp. 888-896, doi: 10.1007/978-3-540-74549-5_93. [Online].

[14] M. A. J. Al-Mohana, S. F. Behadili, A. A. Khalaf, and A. M. Radhi, "Model performance evaluation for color and grayscale images in malaria classification using deep CNN," in *AIP Conference Proceedings*, 2024, vol. 3219, no. 1: AIP Publishing LLC, p. 030008, doi: 10.1063/5.0237322.

[15] Y. I. Shehu, A. Ruiz-Garcia, V. Palade, and A. James, "Detailed identification of fingerprints using convolutional neural networks," in *2018 17th IEEE international conference on machine learning and applications (ICMLA)*, 2018: IEEE, pp. 1161-1165, doi: 10.1109/ICMLA.2018.00187.

[16] A. K. TK, R. Vinayakumar, S. V. VV, V. Sowmya, and K. Soman, "Convolutional neural networks for fingerprint liveness detection system," in *2019 International Conference on Intelligent Computing and Control Systems (ICCS)*, 2019: IEEE, pp. 243-246, doi: 10.1109/ICCS45141.2019.9065713.

[17] J. Kolberg, A.-C. Vasile, M. Gomez-Barrero, and C. Busch, "Analysing the performance of LSTMs and CNNs on 1310 nm laser data for fingerprint presentation attack detection," in *2020 IEEE International Joint Conference on Biometrics (IJCB)*, 2020: IEEE, pp. 1-7, doi: 10.1109/IJCB48548.2020.9304888.

[18] L. Spinoulas, H. Mirzaalian, M. E. Hussein, and W. AbdAlmageed, "Multi-modal fingerprint presentation attack detection: Evaluation on a new dataset," *IEEE Transactions on Biometrics, Behavior, and Identity Science,* vol. 3, no. 3, pp. 347-364, 2021, doi: 10.1109/TBIOM.2021.3072325.

[19] F. Liu, H. Liu, W. Zhang, G. Liu, and L. Shen, "One-class fingerprint presentation attack detection using auto-encoder network," *IEEE Transactions on Image Processing,* vol. 30, pp. 2394-2407, 2021, doi: 10.1109/TIP.2021.3052341.

[20] B. Rim, J. Kim, and M. Hong, "Fingerprint classification using deep learning approach," *Multimedia Tools and Applications,* vol. 80, no. 28, pp. 35809-35825, 2021, doi: 10.1007/s11042-020-09314-6.

[21] M. M. Khaled, A. A. Sayadi, M. Alsmirat, and M. Al-Ayyoub, "Fingerprint Identification from Digital Images Using Deep Learning," in *2023 3rd Intelligent Cybersecurity Conference (ICSC)*, 2023: IEEE, pp. 26-31, doi: 10.1109/ICSC60084.2023.10349980.

[22] B. Pandya, G. Cosma, A. A. Alani, A. Taherkhani, V. Bharadi, and T. McGinnity, "Fingerprint classification using a deep convolutional neural network," in *2018 4th international conference on information management (ICIM)*, 2018: IEEE, pp. 86-91, doi: 10.1109/INFOMAN.2018.8392815. [Online].

[23] P. Tertychnyi, C. Ozcinar, and G. Anbarjafari, "Low-quality fingerprint classification using deep neural network," *IET Biometrics,* vol. 7, no. 6, pp. 550-556, 2018, doi: 10.1049/iet-bmt.2018.5074.

[24] L.-q. Zhu, "Finger knuckle print recognition based on SURF algorithm," in *2011 Eighth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, 2011, vol. 3: IEEE, pp. 1879-1883, doi: 10.1109/FSKD.2011.6019781.

[25] G. Shen, J. Zhang, A. Marshall, L. Peng, and X. Wang, "Radio frequency fingerprint identification for LoRa using deep learning," *IEEE Journal on Selected Areas in Communications,* vol. 39, no. 8, pp. 2604-2616, 2021, doi: 10.1109/JSAC.2021.3087250.

[26] M. Ezuma, F. Erden, C. K. Anjinappa, O. Ozdemir, and I. Guvenc, "Micro-UAV detection and classification from RF fingerprints using machine learning techniques," in *2019 IEEE Aerospace Conference*, 2019: IEEE, pp. 1-13, doi: 10.1109/AERO.2019.8741970.

[27] S. S. Hameed, I. T. Ahmed, and O. M. Al Okashi, "Real and Altered Fingerprint Classification Based on Various Features and Classifiers," *Computers, Materials & Continua,* vol. 74, no. 1, 2023, doi: doi.org/10.32604/cmc.2023.031622.

[28] Y. I. Shehu, A. Ruiz-Garcia, V. Palade, and A. James, "Sokoto coventry fingerprint dataset," *arXiv preprint arXiv:1807.10609,* 2018, doi: 10.48550/arXiv.1807.10609.

[29] J. Kolberg, M. Gomez-Barrero, S. Venkatesh, R. Ramachandra, and C. Busch, "Presentation attack detection for finger recognition," in *Handbook of Vascular Biometrics*. Cham: Springer Nature, 2020, ch. 14, pp. 435-463.