Intelligent Fingerprint recognition ulising learning-based methods

Zofia Wilk

Neuro-Augumented Intelligence Laboratory, School of Computing

Korea Advanced Institute of Science & Technology

Research report

July 2023

This laboratory was performed in collaboration with Jayan Patel, Daniel Sung, Xinyu Zhang and Tanguy Dieudonne

Abstract

Fingerprint recognition is a widely utilized biometric technology in various security systems, authentication processes, and law enforcement applications. However, conventional recognition models often face limitations when handling damaged fingerprints caused by cuts, smudges, rotations, or distortions. In this research, we explore the efficacy of deep learning techniques for addressing these challenges, specifically employing Siamese and U-Net Neural Networks. Siamese Networks excel at comparing and identifying similarities between two input data points, making them ideal for fingerprint matching . U-Net Networks, on the other hand, are proficient in image segmentation and restoration tasks, thus aiding in the recovery of damaged fingerprint images. The models were evaluated using the Sokoto Coventry Fingerprint Dataset (SOCOFing), containing 6000 images from 600 African subjects with various levels of alterations. The Siamese Network achieved an impressive accuracy of 97.83% in fingerprint recognition, while the U-Net-Siamese pipeline obtained an accuracy of 96.35%. However, both models experienced fluctuations in the loss function during training, warranting further optimization efforts. This research highlights the potential of deep learning techniques for fingerprint recognition and provides valuable insights into enhancing accuracy and stability in real-world fingerprint recognition applications.

1 Introduction

Fingerprint recognition is a ubiquitous biometric technology that plays a crucial role in modern security systems, authentication processes, and law enforcement applications [1]. From passport controls to unlocking smartphones, the ability to accurately identify individuals based on their unique fingerprints has become an essential aspect of our daily lives. However, conventional fingerprint recognition models often struggle to perform effectively in scenarios where fingerprints are damaged due to cuts, smudges, rotations, or distortions.

The limitations of traditional fingerprint recognition systems have prompted the development of more sophisticated and adaptable approaches that can handle the challenges posed by damaged fingerprints. In recent years, deep learning has emerged as a powerful and versatile tool in the field of pattern recognition and computer vision. It has shown remarkable potential in solving complex problems by automatically learning hierarchical representations of data, without the need for manual feature engineering [1].

Deep Learning, a subset of machine learning, constitutes the foundation of this research. It encompasses artificial neural networks, computational models inspired by the human brain's structure and functioning. These networks are composed of interconnected nodes, or neurons, organized into layers [2]. Artificial Neural Networks (ANNs), the core of deep learning, consist of an input layer, one or more hidden layers, and an output layer. These networks excel at learning abstract representations of data by sequentially processing input signals, applying activation functions, and propagating the outputs forward through the layers [3]. By leveraging multiple hidden layers, ANNs can capture intricate patterns and relationships in complex datasets, making them highly suitable for fingerprint recognition tasks [1]. In this research the neural networks utilized are Siamese and U-Net Neural Networks.

Siamese Neural Networks represent a specific class of neural networks tailored for comparing and identifying similarities between two input data points [4]. Initially introduced for signature verification [2], Siamese networks have since found applications in various similarity-based tasks, including fingerprint recognition. The key feature of Siamese networks lies in their shared weights, enabling them to process both input data points with the same set of parameters. This characteristic empowers Siamese networks to excel at measuring fingerprint similarities, even in the presence of damaged or distorted fingerprints, and efficiently identify matching entries within a registry database.

U-Net Neural Networks, on the other hand, are specialized architectures primarily employed in image segmentation tasks. Such tasks involve dividing an image into distinct and meaningful segments or regions [5]. U-Net architectures consist of an encoder pathway, where the input image undergoes progressive downsampling to capture contextual information, and a corresponding decoder pathway that upsamples the encoded features to reconstruct the segmented image [6]. Due to its ability to capture fine details and local features, U-Net networks are ideal for fingerprint recognition tasks requiring precise localization and restoration of damaged regions.

2 Method

2.1 Dataset

The dataset utilized in this research laboratory is the Sokoto Coventry Fingerprint Dataset (SOCOFing) [7]. Comprising a total of 6000 images, this dataset captures biometric fingerprints from 600 African subjects. Each fingerprint image comes with corresponding labels indicating the gender, finger name, and hand from which it was taken. Additionally, the dataset includes altered versions of the fingerprints, classified based on three difficulty levels: easy, medium, and hard. These alterations involve synthetic superimpositions of cuts, obliterations, and central rotations, simulating various real-world challenges encountered in fingerprint recognition.
To facilitate experimentation, the dataset was organized into distinct folders, namely: "real," "altered-easy," "altered-medium," and "altered-hard." Each folder encompasses numerically labeled classes, with each class containing either real fingerprint images or one of the three types of altered images derived from the same fingerprint. The data loading process involved randomly selecting two images from the "real" folder and one image from any of the "altered" folders. By comparing these images, a binary label was assigned, with "0" denoting a match between the fingerprints and "1" indicating a non-match. Figure 1 illustrates the data loading process for Siamese Network and the matching label assignment.

[0. 1. 1. 1. 0. 0. 0. 1.]

Figure 1: Dataloader for the Siamese Network.Upper row shows altered fingerprints randomly chosen from all difficulty levels. The row below plots real fingerprints. If the two fingers match, the label for the pairs is 0, if they are different it is 1.

2.2 Siamese Network

The Siamese Neural Network is a model designed for similarity-based tasks, particularly fingerprint recognition in this context. The architectural design of this model adopted for this research

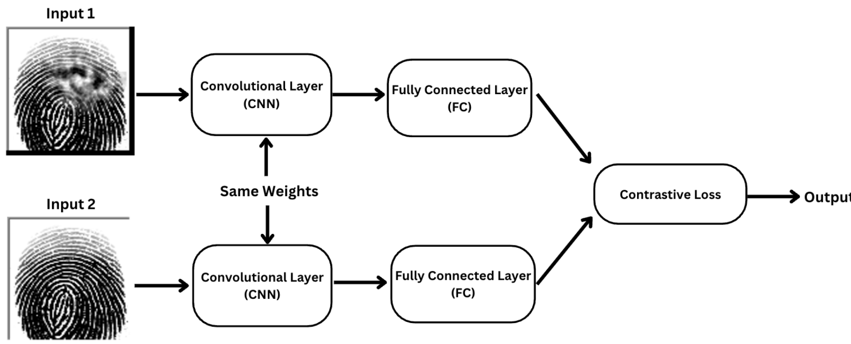


Figure 2: Siamese Neural Network model

is inspired from a similar model utilized by Strahinja Stefanovic in facial recognition [8]. It consists of two identical sub-networks that share the same architecture and weights, hence the term "Siamese". Each sub-network processes an input fingerprint image independently and produces a feature vector that represents the fingerprint's characteristics. These feature vectors are then compared to determine the similarity between two input fingerprints.

The Siamese Network is built using Convolutional Neural Network (CNN) layers and Fully Connected (FC) layers. The CNN layers serve as a feature extractor, capturing important patterns and features from the input fingerprint images [9]. The architecture includes three sets of CNN layers, each followed by a Rectified Linear Unit (ReLU) activation function and max-pooling operations to reduce the spatial dimensions of the feature maps.

The FC layers form the latter part of the Siamese Network. They take the flattened output from the last CNN layer and perform computations to learn the relationship between the feature vectors and the target similarity labels [9](0 for matching fingerprints and 1 for non-matching fingerprints). These FC layers are responsible for further extracting high-level representations from the CNN feature maps and projecting them into a lower-dimensional space.

The whole model architecture used in the final run can be seen on Figure 2.

During the research, various network architectures were evaluated, including the ResNet model. Although exhibiting promising capabilities in feature extraction, the ResNet was not ultimately utilized to obtain the final results for the fingerprint recognition task. It was found that the architecture for the Siamese Network from Figure 2 demonstrated better performance in terms of accuracy.

In summary, the Siamese Network takes two fingerprint images as inputs and processes them through the identical sub-networks. Each sub-network comprises CNN layers for feature extraction and FC layers for similarity determination. The Siamese Network's output consists of two feature vectors representing the input fingerprints, and these vectors are used to calculate the similarity between the fingerprints, enabling accurate fingerprint recognition and matching.

2.3 Loss function and measuring similarity

In this research, Contrastive Loss was employed as the primary loss function to train the Siamese Network for fingerprint recognition. Contrastive Loss is a well-established loss function commonly used in similarity-based learning tasks, aiming to encourage similar samples to be closer together in the feature space, while pushing dissimilar samples further apart [10].
Contrastive Loss is particularly suitable for fingerprint recognition task, where the objective is to determine whether two fingerprint images belong to the same individual or not. By minimizing the Euclidean distance between feature vectors of similar fingerprints and maximizing the distance between feature vectors of different fingerprints, the Siamese Network can effectively learn to distinguish between matching and non-matching fingerprint pairs. The Contrastive Loss can be mathematically represented as follows:

$$L = (1 - Y)\frac{1}{2}(D_w)^2 + (Y)\frac{1}{2}\{max(0, m - D_w)\}^2 \tag{1}$$

Where Y is a term that specifies whether two inputs are similar (Y=0) or different(Y=1) [11], m is the margin,T and the D_w is the distance measure between 2 transformed data points, given by Le Cunn like so:

$$D_w(\vec{X_1}, \vec{X_1}) = ||G_w(\vec{X_1}) - G_w(\vec{X_2})||_2 \tag{2}$$

where G_w is a mapping function i.e Neural Network used [11]. The margin used in this model is 2.0.

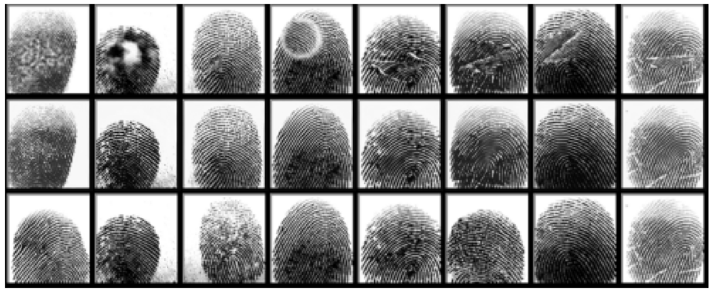
It was also observed that the Adam optimizer outperformed other optimization techniques such as Adadelta, AdamW, and Adagra hence it was used in training of the model.

2.4 U-Net-Siamese Pipeline

To improve the precision and effectiveness of the fingerprint recognition model, an U-Net Neural Network was integrated into the existing Siamese architecture. The U-Net component, build by Xinyu Zhang, aims to restore the input images during the training phase. Subsequently, the restored images are then forwarded into the Siamese Network for further processing, as depicted in Figure 3.
The incorporation of the U-Net into the pipeline aims to mitigate the impact of distortions and damages present in the input fingerprint images. By restoring the images prior to their utilization in the Siamese Network, the model can leverage more accurate and refined representations of the fingerprints, consequently enhancing the recognition performance.

3 Results

The Siamese network was trained for 10 epochs with batch size of 16, employing an 80:20 split ratio for the train and test datasets, respectively. During the testing phase, the Euclidean

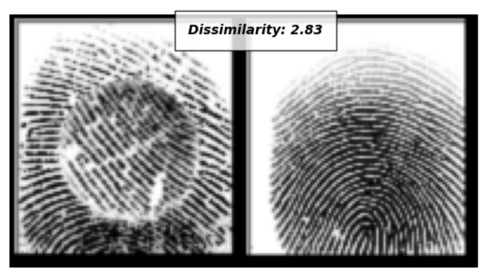


[1. 0. 1. 0. 0. 1. 0. 0.]

Figure 3: Data for Siamese and U-Net Network Pipeline. Top row displays the altered fingerprint images fed into the U-Net. The middle row shows Outputted, restored images for Siamese Network comparison. The real images for similarity evaluation are in the bottom row.

distance was computed, and a threshold of 0.62 was carefully selected based on the model's performance. This threshold served as a boundary, enabling the classification of image pairs into "match" (label 0) or "no match" (label 1) categories, depending on their similarity scores. Remarkably, the Siamese network achieved an impressive accuracy of 97.83%, signifying its good performance in fingerprint recognition. Figure 4 illustrates a sample of outputs with their corresponding Dissimilarity scores, showing the model's ability to effectively differentiate between matching and non-matching fingerprint pairs.

(a) 0: Same



(b) 1: Not Same

Figure 4: Output of the test part of the Siamese Network model with similarity scores displayed above.

Despite the network's commendable accuracy, it was observed that the loss function exhibited considerable fluctuations during training, as evident in Figure 5. These fluctuations indicate the presence of potential challenges in the model's convergence and optimization process. Even with the incorporation of a scheduler during the training process, the issue persisted. Further efforts are needed to refine the loss function and optimize the training process for smoother convergence. Addressing this aspect holds the key to enhancing the model's overall stability and ensuring consistent and reliable performance.

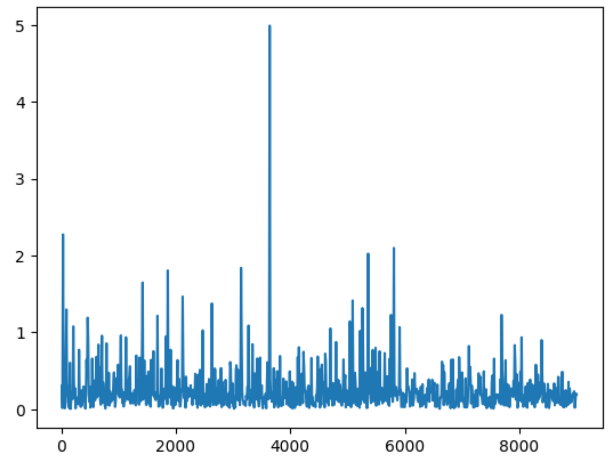
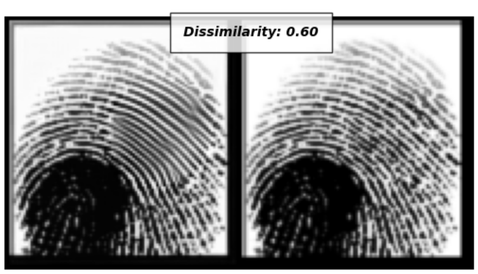


Figure 5: Contrastive Loss function for the Siamese Network

To further enhance the model's accuracy, an U-Net was integrated into the Siamese Network, constituting a U-Net-Siamese pipeline. During the training and testing phases, the U-Net was employed to reconstruct the fingerprint images before feeding them into the Siamese Network for comparison. The combined model utilized the same loss function and optimizer as the Siamese Network.

The U-Net-Siamese pipeline underwent training for 10 epochs with a batch size of 4 due to high memory usage of the connected model. As a result, the pipeline achieved a final accuracy of 96.35% based on a threshold of 0.85. Although the pipeline exhibited promising performance, it did not surpass the accuracy attained by the Siamese Network alone, as anticipated.
Sample outputs of the U-Net-Siamese pipeline can be observed in Figure 6.



(a) 0: Same

(b) 1: Not Same

Figure 6: Output of the test part of the U-Net-Siamese pipeline with similarity scores displayed above.he left hand side of the images shows the restored by U-Net fingerprints while the right-hand side shows real input.

Despite the promising results, similar to the Siamese Network, the addition of the U-Net introduced fluctuations in the loss function during training. Figure 7 illustrates the loss graph, highlighting the variability encountered during the optimization process.

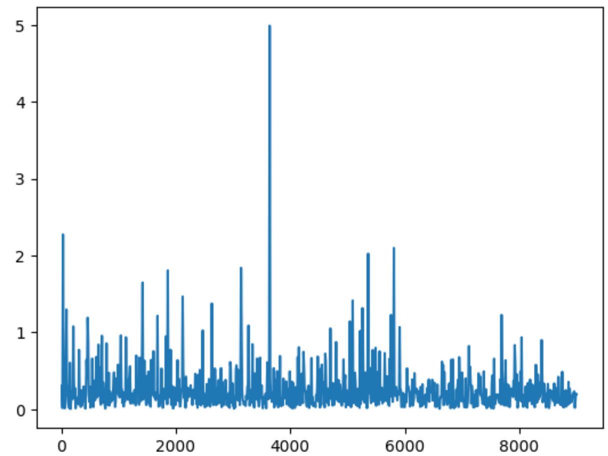


Figure 7: Contrastive Loss function for the Siamese - U-Net pipeline

These findings underscore the importance of further investigating and refining the training process of the U-Net-Siamese pipeline. Ensuring a more stable and consistent loss convergence is important for optimizing the model's performance and realizing its full potential in fingerprint recognition applications.

4 Conclusions

This research explored the application of deep learning techniques, specifically Siamese and U-Net Neural Networks, for fingerprint recognition.
The Siamese Network demonstrated exceptional accuracy of 97.83%, effectively distinguishing between matching and non-matching fingerprint pairs. Despite this remarkable performance, further investigation is required to address the fluctuations observed in the loss function during training and the possible causes for the missing 2.17% accuracy.
To enhance the recognition model's precision, an U-Net was integrated into the pipeline to restore damaged fingerprint images. However, the addition of U-Net did not surpass the performance achieved by the Siamese Network alone, resulting in an accuracy of 96.35%. Similar to the Siamese Network, the loss exhibited fluctuations during the U-Net-Siamese training, necessitating additional optimization strategies. Using different optimizers, loss functions or different connecting methods should also be tested to improve the already promising performance of the Siamese plus U-Net model.
In conclusion, the Siamese and U-Net Neural Networks present viable approaches for fingerprint recognition tasks. The Siamese Network excels at accurately comparing fingerprints, while the U-Net enhances image restoration. Future research should focus on refining the loss function and optimization process to further elevate the recognition model's stability and accuracy. The integration of more sophisticated techniques and larger datasets may further improve the system's performance in challenging fingerprint recognition scenarios. Ultimately, the application

of deep learning in fingerprint recognition holds significant promise for advancing security and identification technologies in diverse real-world applications.

References

[1] L. Zihao, W. Yizhi, Y. Zhong, T. Xiaomin, Z. Lixin, W. Xiao, Y. Jianpeng, G. Shanshan, H. Lingyi, and Z. Yang, *A novel fingerprint recognition method based on a Siamese neural network*, vol. 31. 2022. Available at https://doi.org/10.1515/jisys-2022-0055.

[2] D. Chicco, “Siamese neural networks: An overview,” *Artificial Neural Networks. Methods in Molecular Biology*, vol. 2190, pp. 73—-94, 2021. Available at https://doi.org/10.1007/978-1-0716-0826-5_3.

[3] AWS, “What is a neural network?,” 2023. Available at https://aws.amazon.com/what-is/neural-network/.

[4] F.-M. Geovanni and E. Mata-Montero, *Convolutional Siamese Network for Image-Based Plant Species Identification with Small Datasets.* 2020. Available at doi:10.3390/biomimetics5010008.

[5] C. O’Sullivan, “U-net explained: Understanding its image segmentation architecture,” *Towards Data Science*, 2023. Available at https://towardsdatascience.com/u-net-explained-understanding-its-image-segmentation-architecture-56e4842e313a.

[6] A. Arora, “U-net convolutional networks for biomedical image segmentation,” 2020. Available at https://amaarora.github.io/posts/2020-09-13-unet.html.

[7] Y. I. Shehu, A. Ruiz-Garcia, V. Palade, and A. James, “Sokoto coventry fingerprint dataset,” *Cornell Univeristy*, 2018. Available at https://arxiv.org/abs/1807.10609.

[8] S. Stefanovic, “#019 siamese network in pytorch with application to face similarity,” *Data Hacker*, 2021. Available at https://datahacker.rs/019-siamese-network-in-pytorch-with-application-to-face-similarity.

[9] D. Unzueta, “Fully connected layer vs. convolutional layer: Explained,” *Built In*, 2022. Available at https://builtin.com/machine-learning/fully-connected-layer.

[10] S. Stefanovic, “An introduction to contrastive learning,” *Baeldung*, 2023. Available at https://www.baeldung.com/cs/contrastive-learning.

[11] M. Bekuzarov, “Losses explained: Contrastive loss,” *Medium*, 2020. Available at https://medium.com/@maksym.bekuzarov/losses-explained-contrastive-loss-f8f57fe32246.