`

SAPIENZA
UNIVERSITÀ DI ROMA

Fingerprint Matching and Verification System Using Siamese Neural Networks

Course: Biometric Systems

Professor: Prof. Maria De Marsico

Authors:

Azmeera Qureshi (Matricola: 2103626)

SAAD HAMZA MUNZIR (Matricola: 2243239)

Date of submission: 20-01-2026

Abstract

This report presents the design, implementation, and evaluation of a fingerprint matching and verification system based on a Siamese Convolutional Neural Network (CNN). The system combines classical fingerprint image preprocessing and enhancement techniques with deep learning–based similarity learning. The objective is to accurately verify and identify individuals using fingerprint biometrics while maintaining low error rates. Experimental results demonstrate high verification accuracy and a low Equal Error Rate, confirming the effectiveness of the proposed approach.

1. Introduction

Biometric systems are increasingly used for secure and reliable personal identification in applications such as access control, forensic investigation, and identity management. Among the various biometric modalities, fingerprints remain one of the most widely adopted traits due to their uniqueness, permanence, and ease of acquisition. Traditional fingerprint recognition systems primarily rely on handcrafted features such as minutiae points. While effective, these approaches can suffer from performance degradation when faced with noisy images, partial fingerprints, or variations in pressure and orientation. Recent advances in deep learning have enabled the development of data-driven methods that automatically learn discriminative representations from raw data. In this project, a fingerprint matching system based on a Siamese neural network is implemented. The system learns to measure similarity between fingerprint images directly, enabling robust verification and identification.

2. System Overview

The proposed fingerprint matching system follows a modular pipeline consisting of following main stages:

1. Fingerprint image preprocessing and enhancement

2. Feature extraction using a Siamese CNN

3. Similarity-based matching and decision making

Each stage is designed to enhance fingerprint quality and improve recognition performance.

System Pipeline:

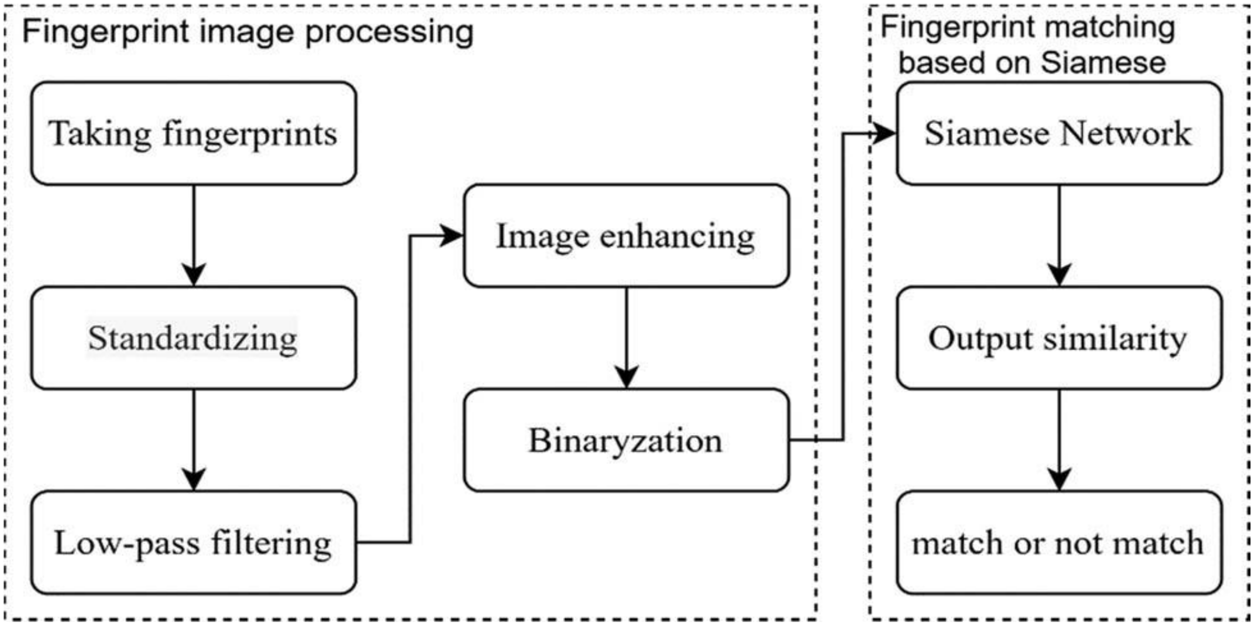

Figure 2.1: Flowchart of the Fingerprint Matching System

3. Dataset Description

This project utilizes the Sokoto Coventry Fingerprint Dataset (SOCOFing), a publicly available biometric fingerprint database designed for academic research. The dataset contains fingerprint images collected from 600 subjects, with a total of 6,000 original fingerprint images. Each fingerprint is labeled with metadata such as gender, hand, and finger name. In addition to the original samples, the dataset includes synthetically altered fingerprints generated using three types of distortions: obliteration, central rotation, and z-cut, each applied at multiple severity levels.

For this project, fingerprint images were preprocessed and converted into fixed-size grayscale inputs of 90 × 90 × 1. To train the Siamese neural network, fingerprint pairs were generated, resulting in a total of 49,270 image samples, where each sample is associated with a 4-dimensional feature label used for similarity learning.

The dataset was divided into training and testing sets as follows:

- Total dataset: 49,270 samples
- Training set: 44,343 samples (90%)
- Testing set: 4,927 samples (10%)

This split ensures that the model is trained on a diverse set of fingerprint variations while maintaining a separate testing set for unbiased performance evaluation. The use of both original and synthetically altered fingerprints increases robustness against noise, rotation, and partial fingerprint degradation, making the dataset suitable for evaluating fingerprint verification systems based on deep learning.

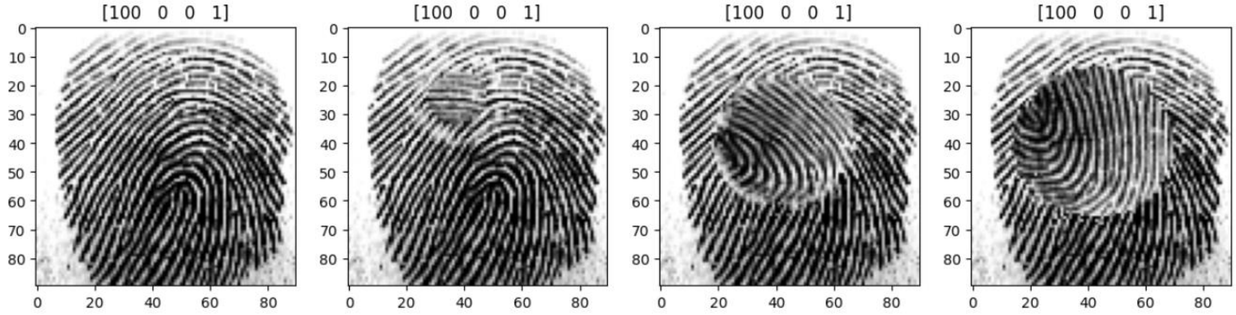

Figure 3.1: Sample images from dataset

4. Fingerprint Image Processing

4.1 Image Preprocessing

Fingerprint images are first converted to grayscale to simplify processing and focus on intensity information. Histogram equalization is then applied to enhance contrast and normalize pixel intensity distributions across images. To further suppress noise and improve ridge clarity, a low-pass filtering approach based on the Fast Fourier Transform (FFT) is employed. This step removes high-frequency noise while preserving essential ridge structures.

4.2 Fingerprint Enhancement

Additional enhancement techniques are applied to improve ridge-valley patterns. These include noise reduction using Gaussian or median filtering, ridge thinning to obtain single-pixel-wide ridges, ridge orientation estimation, and ridge frequency estimation. These steps enhance the structural consistency of fingerprint patterns.

5. Siamese Network Architecture

The core of the fingerprint matching system is a Siamese neural network composed of two identical convolutional branches that share weights. Each branch processes one fingerprint image and extracts a compact feature representation. A pre-trained VGG16 model is used as the base network, enabling transfer learning from large-scale image data. The network accepts grayscale fingerprint images resized to 90×90 pixels and outputs a four-dimensional embedding vector representing fingerprint features.

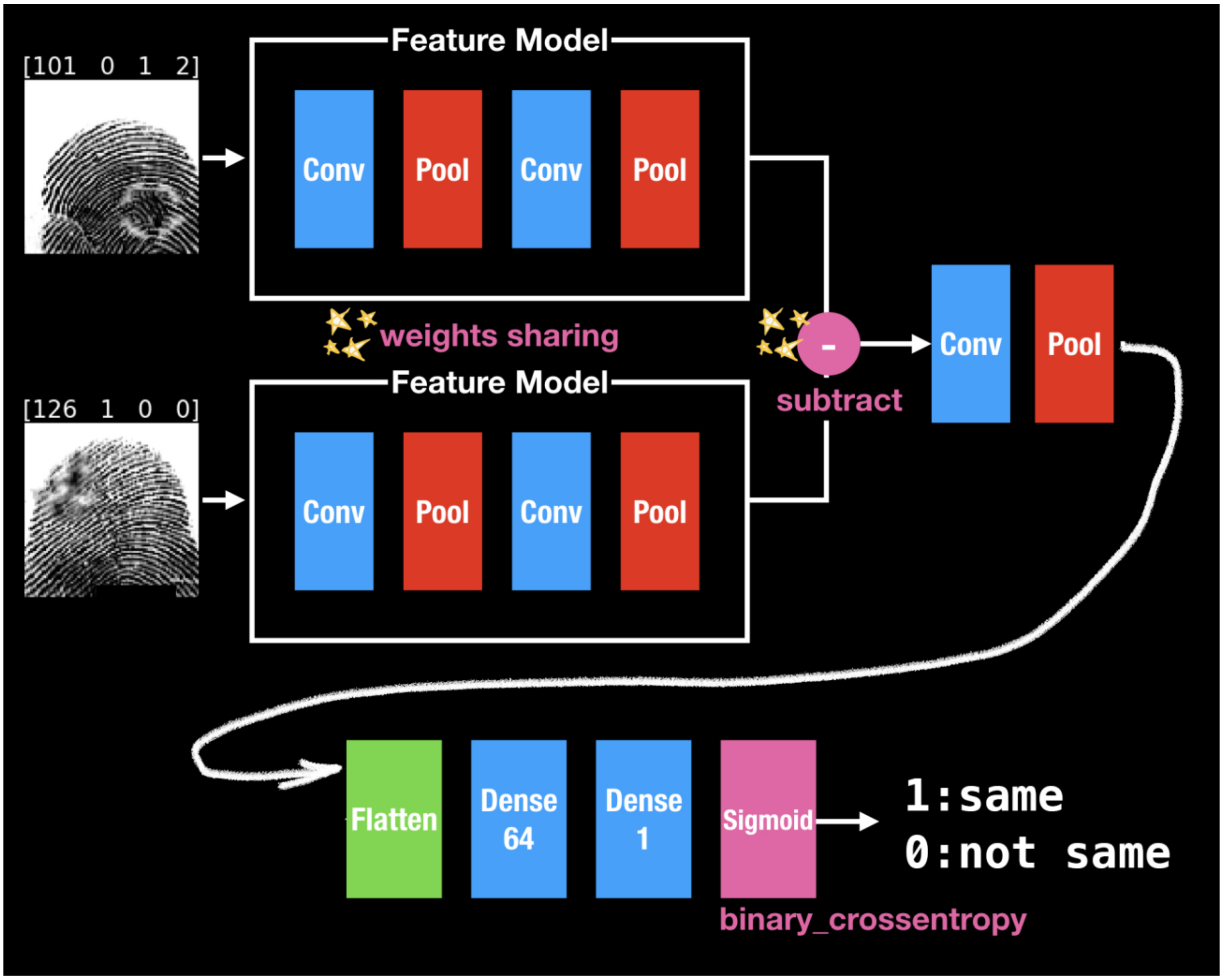

Figure 5.1: Siamese Network Architecture

6. Training Strategy

The Siamese network is trained using contrastive loss, which minimizes the distance between embeddings of genuine fingerprint pairs while maximizing the distance between impostor pairs. This loss function is well suited for similarity-based biometric verification. The network utilized VGG16 pre-trained weights as the backbone for feature extraction during training. The training dataset consisted of 66 unique fingerprint classes acquired using an AS60x fingerprint sensor, with an average of 10 images available per fingerprint. All training images were processed using the fingerprint preprocessing techniques described previously. To enhance the robustness of the training data, each fingerprint image was augmented by applying five rotational transformations, resulting in six images per original sample. This augmentation strategy increased the average number of images per fingerprint to almost 60. During Siamese network training, pairs of images belonging to the same fingerprint class were labeled with an output value of 1, while pairs composed of images from different fingerprint classes were labeled with an output value of 0. This pairing process was repeated across the dataset using different image combinations. As a result, the network learned to produce higher similarity scores for matching fingerprint pairs and lower scores for non-matching pairs. The training process uses the Adam optimizer with a batch size of 32 and is conducted for two epochs with validation monitoring.

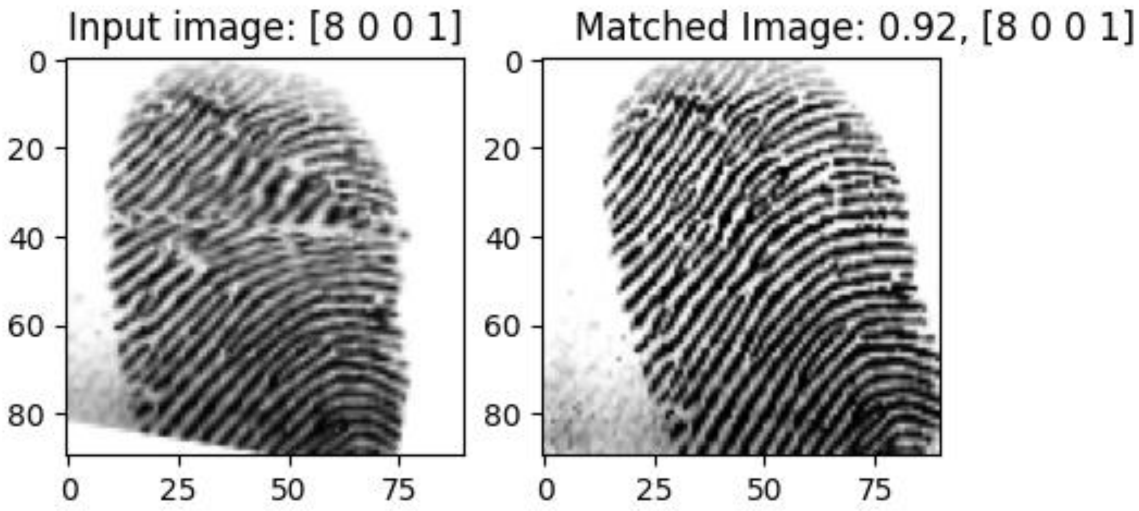

Figure 6.1: Fingerprint matching 92%

7. Performance Evaluation Metrics

System performance is evaluated using standard biometric metrics, including False Acceptance Rate (FAR), False Rejection Rate (FRR), Receiver Operating Characteristic (ROC) curves, and Equal Error Rate (EER). FAR measures incorrect acceptance of impostors, while FRR measures rejection of legitimate users. ROC curves illustrate the trade-off between these errors across different thresholds, and EER provides a single value of overall accuracy. Together, these metrics give a clear assessment of the system's verification reliability and error balance.

8. Experimental Results

The proposed fingerprint matching system achieved strong performance on the evaluation dataset. Training accuracy improved from 88.86% to 94.14%, while validation accuracy increased from 96.85% to 98.73%. The Equal Error Rate (EER) was measured at 0.0060 with a decision threshold of 0.8181. At this operating point, the False Acceptance Rate (FAR) was 0.0050 and the False Rejection Rate (FRR) was 0.0070, indicating balanced and reliable verification performance.

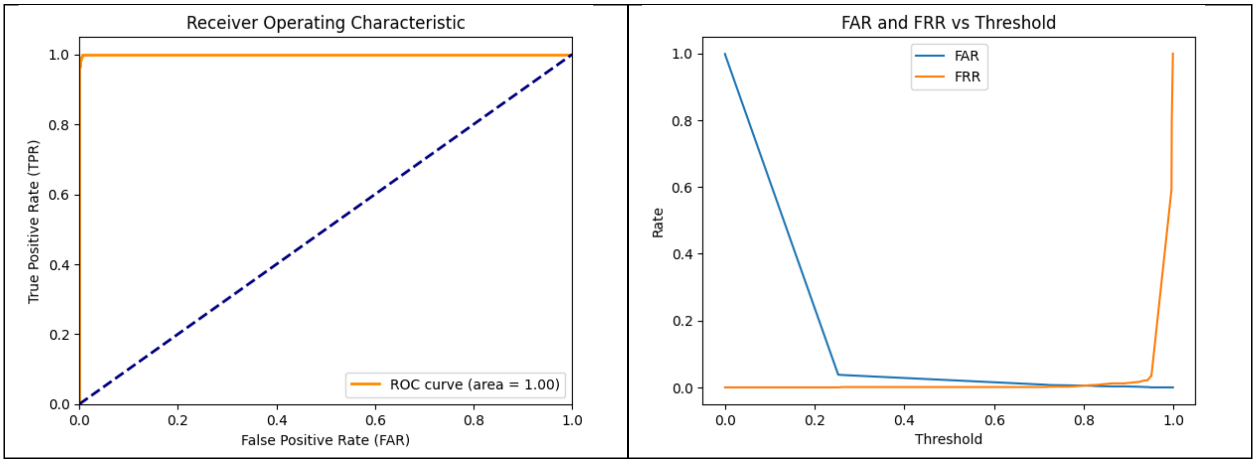

Figure 8.1: Final results graphs

9. Discussion

The low EER demonstrates the effectiveness of the Siamese CNN in learning discriminative fingerprint representations. The combination of classical fingerprint enhancement techniques and deep learning contributes to robustness against noise, rotation, and intra-class variability.

10. Conclusion and Future Work

This project demonstrates that Siamese neural networks are highly effective for fingerprint matching and verification. The system achieves high accuracy and low error rates, making it suitable for biometric applications. Future work may include extending the system to larger datasets, integrating fingerprint liveness detection, and deploying the model in real-time biometric systems.

11. References

1. S. Wang and Y. Wang, “Fingerprint enhancement in the singular point area,” *IEEE Signal Processing Letters*, vol. 11, no. 1, pp. 16–19, 2004.
2. L. Sha, F. Zhao, and X. Tang, “Improved fingercode for filterbank-based fingerprint matching,” in *Proceedings 2003 International Conference on Image Processing (Cat. No. 03CH37429)*, vol. 2, pp. II–895, IEEE, 2003.
3. A. Jain, A. Ross, and S. Prabhakar, “Fingerprint matching using minutiae and texture features,” in *Proceedings 2001 International Conference on Image Processing (Cat. No. 01CH37205)*, vol. 3, pp. 282–285, IEEE, 2001.
4. D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, et al., *Handbook of fingerprint recognition*, vol. 2. Springer, 2009.
5. M. Horton, P. Meenen, R. Adhami, and P. Cox, “The costs and benefits of using complex 2-d gabor filters in a filter-based fingerprint-matching system,” in *Proceedings of the*

Thirty-Fourth Southeastern Symposium on System Theory (Cat. No. 02EX540), pp. 171–175, IEEE, 2002.