VISVESVARAYA TECHNOLOGICAL UNIVERSITY

"JNANA SANGAMA", BELAGAVI - 590 018

A PROJECT REPORT

on

"FINGERPRINT MATCHING"

Submitted by

Nitesh kamat	4SF20CI042
Pavan	4SF20CI043

In partial fulfillment of the requirements for VI Sem. B. E. (CSE-AI&ML)

DIGITAL IMAGE PROCESSING LABORATORY WITH MINI PROJECT

Under the Guidance of

Ms.Vaishnavi Rao

Assistant Professor, Department of CSE(AI&ML)

at

SAHYADRI

COLLEGE OF ENGINEERING & MANAGEMENT

An Autonomous Institution

Adyar, Mangaluru - 575 007

2022 - 23

SAHYADRI
COLLEGE OF ENGINEERING & MANAGEMENT
An Autonomous Institution
MANGALURU

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
(ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING)

CERTIFICATE

This is to certify that the Digital Image Processing Mini project work entitled **"Fingerprint Matching "** has been carried out by **Nitesh kamat(4SF20CI042), and Pavan (4SF20CI043)**, the bonafide students of Sahyadri College of Engineering & Management in partial fulfillment for the award of Bachelor of Engineering in Computer Science & Engineering (Artificial Intelligence & Machine Learning) of Visvesvaraya Technological University, Belagavi during the year 2022-23. It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the Report deposited in the departmental library. The Digital Image Processing project report has been approved as it satisfies the academic requirements in respect of project work prescribed for the said degree.

Guide	**Project Coordinator**	**HOD**
Ms.Vaishnavi Rao	Mr.Gurusiddaya Hiremath	Dr. Pushpalatha K

External Viva:

Examiner's Name	Signature with Date
1.	.....
2.	.....

SAHYADRI

COLLEGE OF ENGINEERING & MANAGEMENT

An Autonomous Institution

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
(ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING)

DECLARATION

We hereby declare that the entire work embodied in this Digital Image Processing Project Report titled **"Fingerprint Matching"** has been carried out by us at Sahyadri College of Engineering and Management, Mangaluru under the supervision of **Ms.Vaishnavi Rao** for the award of **Bachelor of Engineering** in **Computer Science & Engineering**. This report has not been submitted to this or any other University for the award of any other degree.

Nitesh kamat(4SF20CI042)

Pavan (4SF20CI043)

Dept. of CSE (AI & ML), SCEM, Mangaluru

Abstract

Fingerprint matching has gained significant attention as a reliable biometric authentication method due to its uniqueness and stability. In this mini-project, we propose a fingerprint matching system that leverages a Siamese network to achieve accurate and efficient fingerprint identification. The system consists of three main stages: image preprocessing, feature extraction, and matching. During the preprocessing stage, the captured fingerprint image undergoes various enhancement and noise reduction operations to ensure optimal quality for subsequent analysis. In the feature extraction stage, the Siamese network is trained to encode and extract discriminative features from pairs of fingerprint images. These features capture the unique patterns and characteristics of individual fingerprints. In the matching stage, the trained Siamese network computes a similarity score between two fingerprint images, indicating their degree of similarity. Experimental evaluations demonstrate the effectiveness of our approach in achieving high accuracy and robustness in fingerprint matching. This system offers a promising solution for biometric authentication, providing enhanced accuracy and efficiency in fingerprint recognition tasks.

Acknowledgement

It is with great satisfaction and euphoria that we are submitting the Project Report on **"Fingerprint Matching "**. We have completed it as a part of the curriculum of Visvesvaraya Technological University, Belagavi for the award of Bachelor of Engineering in Computer Science & Engineering.

We are profoundly indebted to our guide, **Ms.Vaishnavi Rao**, Assistant Professor,Department of Computer Science & Engineering(Artificial Intelligence & Machine Learning) for innumerable acts of timely advice, encouragement and We sincerely express our gratitude.

We also thank **Mr. Gurusiddaya Hiremath,** Project Coordinator, Department of Computer Science & Engineering(Artificial Intelligence & Machine Learning) for their constant encouragement and support extended throughout.

We express our sincere gratitude to **Dr. Pushpalatha K**, Head & Professor,Department of Computer Science & Engineering(Artificial Intelligence & Machine Learning)for his invaluable support and guidance.

We sincerely thank **Dr. Rajesha S**, Principal, Sahyadri College of Engineering & Management, who have always been a great source of inspiration.

We extend our sincere regards and respect to **Dr. Manjunath Bhandary**, Chairman, SCEM, having provided all the facilitites that helped us in the timely completion of this project report.

Finally, yet importantly, We express our heartfelt thanks to our family & friends for their wishes and encouragement throughout the work.

Nitesh kamat(4SF20CI042)

Pavan (4SF20CI043)

Table of Contents

List of Figures

Chapter 1

Introduction

Fingerprint recognition is a widely used biometric technology that has gained significant attention and adoption in various fields. With the unique and distinct patterns present on each individual's fingertips, fingerprint recognition has proven to be a reliable and efficient method for personal identification and authentication. This technology utilizes advanced algorithms and pattern matching techniques to capture, process, and analyze the distinctive features of fingerprints, enabling accurate identification and verification. The application of fingerprint recognition has seen tremendous growth in recent years, encompassing a diverse range of sectors such as law enforcement, access control systems, banking and finance, border security, and mobile device authentication. Its popularity can be attributed to its non-invasive nature, high accuracy, and the fact that fingerprints are difficult to forge, making it an ideal choice for ensuring security and identity verification. In this report, we will explore the fundamental principles behind fingerprint recognition, the various components involved in the process, and the challenges faced in implementing this technology. Additionally, we will delve into the potential applications and benefits of fingerprint recognition systems, as well as discussing some emerging trends and advancements in the field. By understanding the intricacies of fingerprint recognition, we can gain insights into its effectiveness, limitations, and its impact on enhancing security measures in our increasingly digital and interconnected world.

1.1 Purpose

The purpose of fingerprint recognition is to accurately and reliably identify individuals based on the unique patterns and characteristics present in their fingerprints. This biometric authentication method serves several key objectives. Firstly, it aims to provide

identification by comparing a person's fingerprint with a database of known fingerprints, enabling the determination of their identity based on the distinctiveness of their fingerprint patterns. Secondly, fingerprint recognition is used for authentication purposes, verifying the claimed identity of an individual by comparing a presented fingerprint with a stored reference template.

1.2 Scope

The scope of fingerprint recognition is broad, encompassing a wide range of domains and applications. It is a versatile technology that finds application in various fields, including security systems, forensic investigations, identity verification, financial transactions, employee management, mobile devices, healthcare, and more.

In the realm of security systems, fingerprint recognition is extensively used for access control, ensuring that only authorized individuals can gain entry to secure areas or electronic devices. It provides a high level of security and convenience compared to traditional methods like passwords or access cards.In forensic investigations, fingerprint recognition plays a crucial role in linking suspects to crime scenes. It aids in the identification and matching of fingerprints, helping law enforcement agencies solve crimes and provide evidence in court.

1.3 Overview

Fingerprint recognition is a widely used biometric technology that aims to identify and authenticate individuals based on their unique fingerprint patterns. It has gained significant attention and adoption across various industries and applications due to its reliability, security, and convenience.Fingerprint recognition has a broad scope and finds application in numerous domains. It is extensively used in access control systems to secure physical spaces, electronic devices, and confidential information. By relying on the uniqueness of fingerprints, it provides a highly secure method for granting authorized access.In forensic investigations, fingerprint recognition plays a crucial role in criminal identification. It enables the comparison of fingerprints found at crime scenes with those in a database, aiding law enforcement agencies in linking suspects to criminal activities and providing valuable evidence in court.

Chapter 2

Literature Survey

The tremendous success of fingerprint based recognition technology in law enforcement applications, decreasing cost of fingerprint sensing devices, increasing availability of inexpensive computing power, and growing identity fraud/theft have all ushered in an era of fingerprint based person recognition applications in commercial, civilian, and financial domains. In 1893 the Home Ministry Office, UK accepted that no two individuals have the same fingerprints [1]. Soon after this discovery many major law enforcement departments embraced the idea of first booking the fingerprints of criminals, so that there records are readily available and later using leftover fingerprint smudges, they could determine the identity of criminals. These agencies sponsored a rigorous study of fingerprints, developed scientific method for visual matching of fingerprints and applied the art of fingerprint recognition for nailing down the perpetrators.

In the early stages of Automatic Fingerprint Identification System (AFIS) the algorithms more or less tried to follow the manual approach of fingerprint identification. Expensive hardware was required for the computational requirements and to match the response time requirements. T. R. Gowrishankar [2] presented a feature-based scheme for fingerprint identification on a massively parallel system (architectures with 1000 or more processors). The author presented an algorithm for orientation independent identification. This automatic fingerprint identification system considers five features namely isolated points, terminating points, merge/branch points, segments and loops as primary elements of a feature vector that uniquely identify a given fingerprint pattern. These minutiae and their relative locations are found sufficient to identify a given pattern.

M Mori [3] describes the structure, function, and operation of this Automatic Switching System for high resolution Photo-telegraphic Equipment. C. A. Gunawardena and V. K. Sagar [4] described a high speed and low cost system for scanning, identifying and coding

fingerprints. In their approach the raw fingerprint image is cleaned by median filter, which makes edge extraction from the fingerprint easier. After edge extraction line thinning is performed. The image is processed by a new single pass noise removal and linethinning algorithm, which is based on contour generation. This algorithm was faster and more efficient than conventional contour tracing and parallel algorithms and was the bases for the high-speed feature extraction. For better extraction of features fingerprint enhancement is required. B. G. Sherlock; D. M. Monro and K. Millard [5] described a method of enhancing fingerprint images, based upon directional Fourier domain filtering. Fingerprints are first smoothed using a directional filter whose orientation is everywhere matched to the local ridge orientation. The proposed technique took the advantage of Fourier domain filtering which helped to convolve the fingerprint images with filters of full image size. A criminal case may require a very high degree match but an access control system may use a more relaxed matching system, simply because its database is much smaller. Sometimes it is not possible to capture the whole of fingerprint image easily

In such circumstances, how to tolerate minor distortions becomes a critical subject. M. B. Akhan, I. Emiroglu and E. G. Bahari [6] proposed a method to overcome some of these difficulties by allowing the user to set the accuracy and the degree of match. Most of the approaches to fingerprint recognition used to break down the process of ridge detection into smoothing or early pre-processing, edge detection, thresholding, binarization and subsequently thinning. This whole procedure was computationally expensive and hence required more expensive hardware to meet the response- time requirements. V. K. Sagar; D. B. L. Ngo and K. C. K. Foo [7]presented an approach based on fuzzy logic technique. This technique had the advantage of being simple and less expensive. Major advantage of using fuzzy logic is that it requires less expensive hardware for similar performance. M. H. Ghassemian [8] addressed the problem of the extraction of relevant macroscopic properties of the image, in particular the location of key features (core and delta). Author explored the transformation of the image into a reconstructed skeletal form, followed by the conversion of the image into a series of tracks. These tracks latter permits the straightforward extraction of' essential pattern characteristics. The track curvature can also be used to identify locations in the image that are in some sense pivotal to the ridge flow and can be used as substitutes for the more obvious cores. This is of significance in Arch-like patterns, which have no discernible core.

Smudged furrows and cut ridges in the image of a fingerprint are the major problem in the fingerprint identification or verification systems. M. H. Ghassemian,[9] presented a new

on-line unsupervised ridge detection method that reduced the complexity and costs associated with the fingerprint identification procedure. The author describes the algorithm for restoration of the ridges of fingerprint. This algorithm was based on fuzzy classification technique. D. P. Mital and Eam Khwang Teoh,[10] presented the structural matching approach which is able to perform effective rotational invariant fingerprint identification. In this approach, each of the extracted feature is correlated with five of its nearest neighboring features to form a local feature group for a first-stage matching. After that, the feature with the highest match is used as a central feature whereby all the other features are correlated to form a global feature group for a second-stage matching. Distance and relative angle is used for finding the correlation between the features. Lin Hong and Jain A.[11] introduced a new fingerprint enhancement algorithm, which decomposes the input fingerprint image into a set of filtered images. From the filtered images, the orientation field is estimated and a quality mask, which distinguishes the recoverable and unrecoverable corrupted regions in the input image, is generated. The input fingerprint image is adaptively enhanced in the recoverable regions. Hong Lin; A. Jian and R. Bolle [12] described the design and implementation of an on-line fingerprint verification system, which operates in two stages: minutia extraction and minutia matching. An improved version of the minutia extraction algorithm proposed by Ratha et al., which was much faster and more reliable, was implemented for extracting features. For minutia matching, an alignment-based elastic matching algorithm was developed. This algorithm has the capability of finding the correspondences between minutiae in the input image and the stored template without resorting to exhaustive search and has the ability of adaptively compensating for the nonlinear deformations. Lin Hong; Yifei Wan and Jain A [13] presented a fast fingerprint enhancement algorithm, which can adaptively improve the clarity of ridge and valley structures of input fingerprint images based on the estimated local ridge orientation and frequency.

There were two major shortcomings of the traditional approaches to fingerprint representation. Firstly for a significant fraction of population, the representations based on explicit detection of complete ridge structure in the fingerprints were difficult to extract automatically. . A. K. Jain; S. Prabhakar; L. Hong and S. Pankanti[14] proposed filter-based algorithm that uses a bank of even symmetric Gabor filters to capture both the local and the global details in a fingerprint as a compact 640- byte fixed length Finger Code. The fingerprint matching is done on the bases of Euclidean distance between the two corresponding Finger codes and hence is extremely fast. The accuracy of the method was found comparable to best results of minutiae based algorithms. Lee Chih-Jen and Wang

Sheng-De [15] explained usefulness of Gabor filter based method for fingerprint recognition on small database. The method made use of Gabor filtering technology and eliminated computationally complex steps like smoothing, binarization, thinning and minutiae detection. Gabor filter based features played a central role in the processes of fingerprint recognition, including local ridge orientation detection, core point detection, and feature extraction.

In the improvement to their previous method,A. K. Jain; S. Prabhakar; L Hong and S. Pankanti proposed filter-based algorithm that uses a bank of Gabor filters to capture both local and global details in a fingerprint as a compact fixed length Finger Code. The verification accuracy, which was only marginally inferior to the best results of minutiae-based algorithms, was achieved. M. Horton; P. Meene; R. Adhami and P. Cox,[16] in their work investigated the utility of complex, 2-D Gabor filter for a fingerprint matching system. Previous approaches had used an even symmetric 2-D Gabor filter to perform fingerprint feature extraction processing. Several processing methods using a complex filter were explored and compared to the even-symmetric case. The use of the complex filter provided only marginal improvement over the real filter though the computational cost for using the complex filter was significant. L. Sha; F. Zhao and X. Tang,[17] proposed a new rotation invariant reference point location method, and then combine the direction features with the AAD features to form an oriented Finger Code. To approximate the rotation invariance features, the image was rotated cyclically to generate ten templates. Experimental results showed that the addition of direction features led to a substantial improvement in the overall matching performance. A. Jain; A. Ross and S. Prabhakar, [18] presented a hybrid matching algorithm that used both minutiae (point) information and texture (region) information for matching the fingerprints. A bank of Gabor filters was used to extract features from the tessellated cells of the template and input images. Sen Wang and Yangsheng Wang,[19]presented a new method and designed a new frequency domain filter to enhance fingerprint in the singular point area. First the singular point was detected and then filter was designed for the enhancement in this area.

Classification of fingerprint is to group similar type of fingerprints together. This helps reducing the matching time. F. You, Y.Q. Shi and P Engler[20] described a method to automatically classify fingerprints into three groups: whorl, loop and arch. Their work was motivated with the idea to help medical scientists to study the relationship between fingerprint patterns and medical disorders. They used frequency domain approach in which features of Fourier spectrum were used.

Chapter 3

Problem Definition

The problem of fingerprint matching refers to the task of accurately identifying and verifying the identity of an individual based on their fingerprint patterns. Fingerprint matching plays a crucial role in various applications, including law enforcement, access control systems, and personal authentication. The main challenge in fingerprint matching lies in the uniqueness and complexity of fingerprint patterns. Each person's fingerprint consists of ridges, valleys, and minutiae points, such as ridge endings and bifurcations, which form a distinct pattern. The goal is to compare a captured fingerprint image with a database of known fingerprints to determine if a match exists.

The problem involves several subtasks, including image preprocessing, feature extraction, and matching algorithms. Image preprocessing aims to enhance the quality of the captured fingerprint image by reducing noise, improving contrast, and removing artifacts. Feature extraction involves identifying and extracting key characteristics, such as minutiae points, from the preprocessed image. Matching algorithms then compare the extracted features of the query fingerprint with those in the database to determine the degree of similarity or dissimilarity.

Chapter 4

Methodology

4.1 Fingerprint Image Processing

The conventional fingerprint recognition system relied on the comparison of minutiae. In this study, however, the step of minutia point extraction was omitted, and two binary fingerprint images were input into the Siamese neural network to obtain the similarity between two fingerprints and get the fingerprint recognition result. The whole system needed to complete such steps as the standardization of fingerprint image, image enhancement,binarization, input into the Siamese network, and output of the matching result. It can be divided into two parts: "fingerprint image preprocessing" and "fingerprint image matching. based on Siamese network," as shown in flowchart. The method proposed

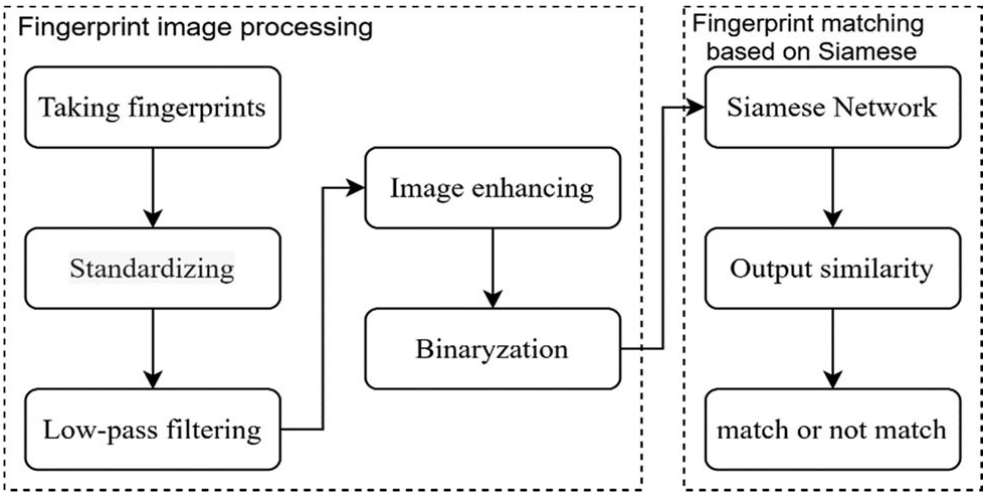

Figure 4.1: Flowchart of the Fingerprint Matching System

in this study can compare fingerprint images in a direct way, so it was more flexible in practical applications. The application method is shown in Figure 4.2, that is, to store the

enhanced image into the database and compare it with the input fingerprint, in order to control the subsequent programs.

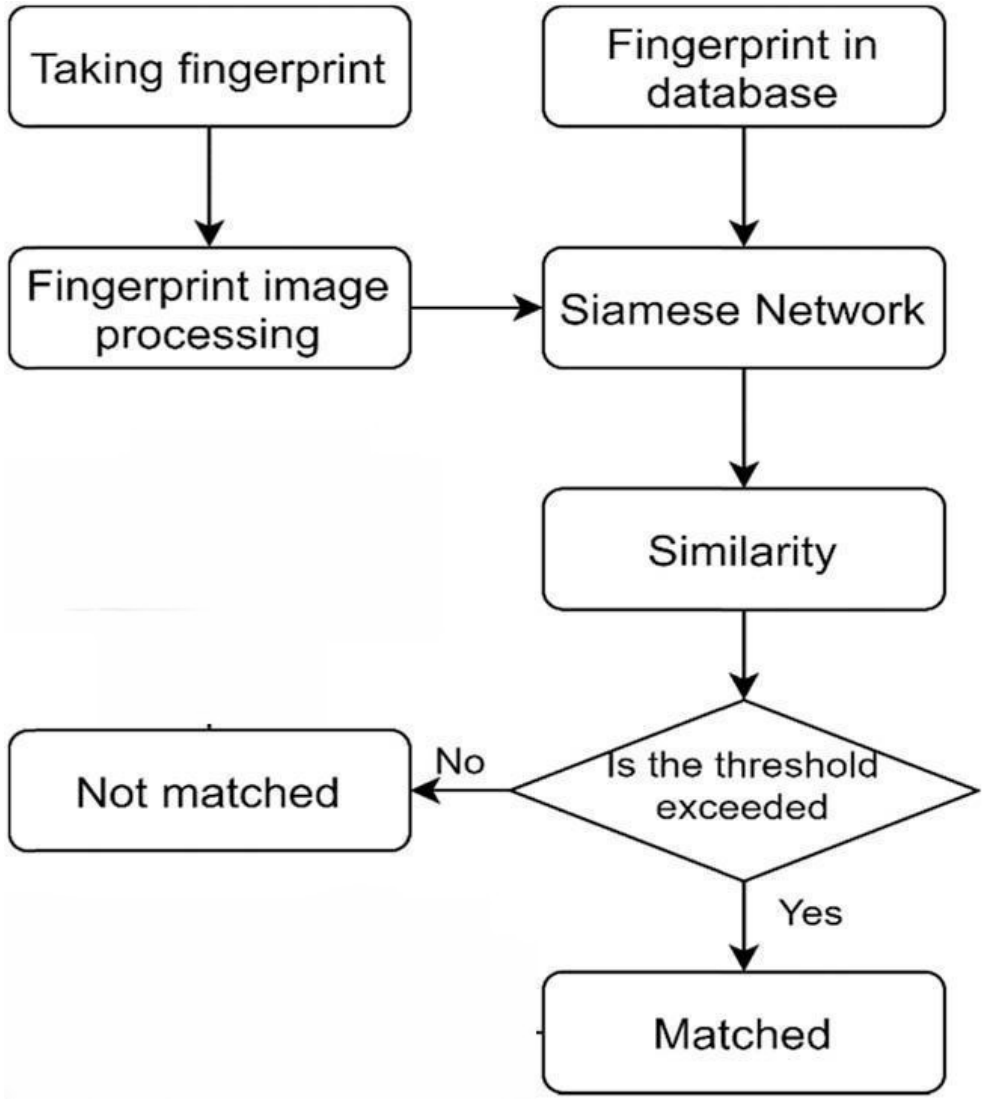

Figure 4.2: Workflow of Fingerprint Matching

4.2 Standardization of images:

Fingerprint images were standardized to eliminate the problems of inconsistent clarity, grayscale, and the number of channels between different fingerprint images. The steps were as follows: Fingerprint images were standardized to eliminate the problems of inconsistent clarity, grayscale, and the number of channels between different fingerprint images. The steps were as follows:

1. Gray Scaling: Fingerprint images were converted from color to grayscale. This conversion simplifies the image representation and reduces computational complexity, as it

focuses solely on the intensity values of pixels, which contain important fingerprint ridge information.

2. Histogram Equalization: Histogram equalization was performed to enhance the contrast and normalize the grayscale values of the fingerprint images. This step addressed the issue of inconsistent clarity and variations in grayscale due to different imaging conditions or finger pressure during image acquisition.

To perform histogram equalization, the following steps were followed:

- Compute the histogram of the grayscale image, which represents the distribution of pixel intensities.
- Calculate the cumulative distribution function (CDF) of the histogram.
- Normalize the CDF to the range of pixel intensities (usually 0 to 255) to obtain the mapping function.
- Apply the mapping function to each pixel in the grayscale image to obtain the equalized image.

3.Low-pass filtering smoothing: The image noise generated during fingerprint collection was removed and the fingerprint images were smoothed. Fast Fourier transform (FFT) was applied to the images. After the high-frequency part was eliminated, low-pass filtered images were acquired through inverse Fourier transform.

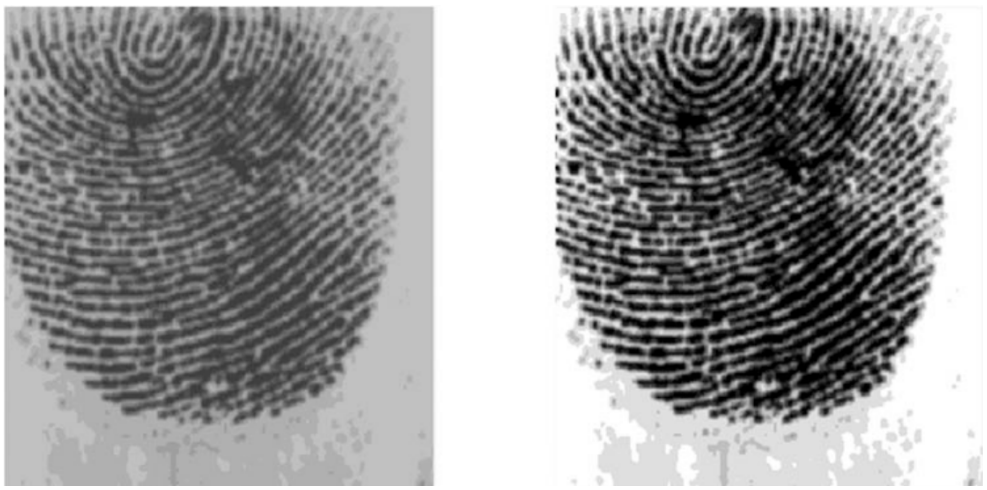

Figure 4.3: Left: original image. Right: equalized image

4. Image Enhancement Techniques: Additional image enhancement techniques can be applied to further improve the quality of fingerprint images. These techniques may

include noise reduction, ridge thinning, ridge orientation estimation, and ridge frequency estimation. Noise reduction techniques, such as Gaussian filtering or median filtering, help remove unwanted noise while preserving important ridge information. Ridge thinning algorithms aim to reduce the width of ridges to enhance their clarity and distinguishability. Ridge orientation estimation techniques help determine the local ridge direction, which is essential for subsequent feature extraction and matching processes. Ridge frequency estimation techniques estimate the frequency of ridges, allowing for adaptive filtering and analysis.

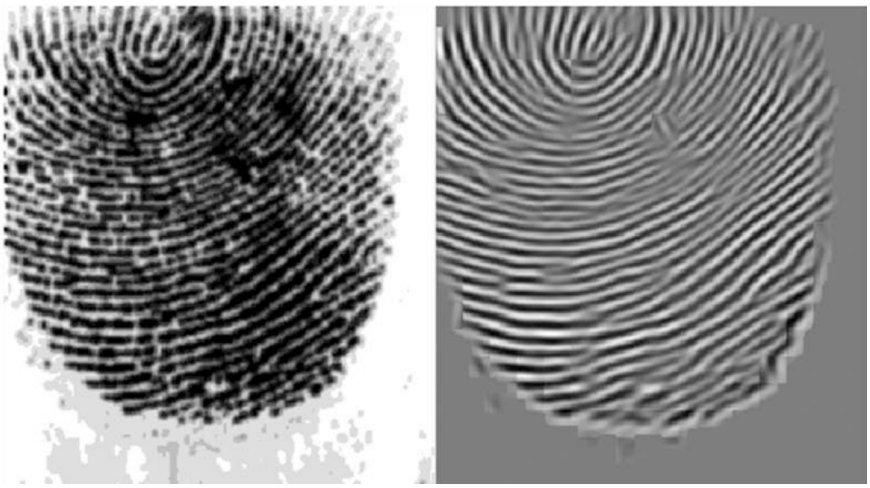

Figure 4.4: Left: filtered image Right: enhanced Fingerprint image

performing these preprocessing steps, fingerprint images are standardized and prepared for subsequent feature extraction and matching algorithms. These steps help to improve the accuracy and reliability of fingerprint matching systems by enhancing the quality and consistency of the input fingerprint images.

4.3 Architecture for Fingerprint Matching

Siamese network typically consists of twin subnetworks that share weights. The following is an example of the architecture of a Siamese network for fingerprint matching:

1. **Input Layer**: Two fingerprint images are fed into the Siamese network as inputs.
2. **Convolutional Layers**: Each subnetwork begins with a series of convolutional layers. These layers apply filters to the input images, capturing local patterns and features.

3. **Pooling Layers**: Pooling layers follow the convolutional layers to reduce the dimensionality of the feature maps. Common pooling techniques include max pooling or average pooling.

4. **Fully Connected Layers**: Flattened features from the pooling layers are passed through fully connected layers. These layers learn high-level representations by combining the local features.

5. **Contrastive Loss Layer**: The outputs of the fully connected layers from both subnetworks are concatenated. This concatenated representation is passed through a contrastive loss layer, which measures the similarity between the feature representations of the two input fingerprint images.

6. **Output Layer**: The output layer produces a similarity score or distance metric that quantifies the similarity or dissimilarity between the input fingerprint images.

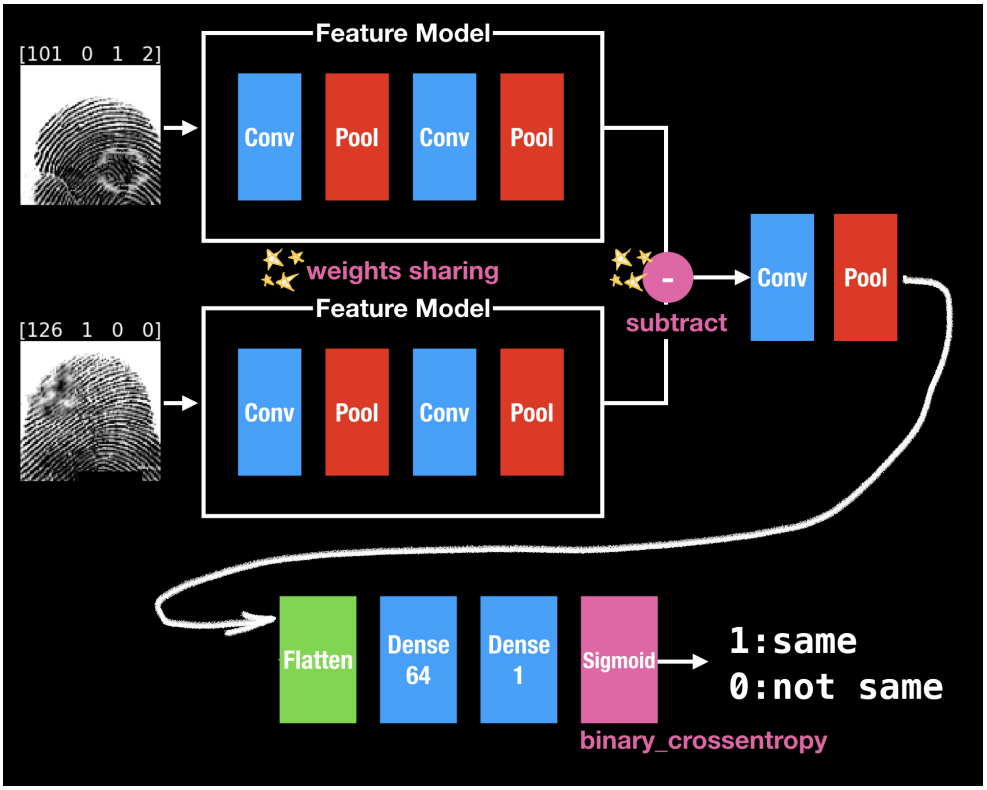

Figure 4.5: Siamese Network Architecture

4.4 Training Process

In this study, we trained the Siamese network with 63 different fingerprints using fingerprint images of size 98 × 98. The fingerprint images of the same finger in the training set were stored in the same folder. For the main network, VGG16 pre-trained weights were used for subsequent network training. The training set comprised 66 different kinds of fingerprint images belonging to different fingers, collected using an AS60x fingerprint collector. On average, 10 images were sampled for each fingerprint in the training set. All images in the training set underwent the fingerprint preprocessing steps described earlier. To increase the adaptability of the training set, each fingerprint image was rotated five times, resulting in a total of six images. Through this data augmentation technique, the number of images for each fingerprint increased to an average of 60. Regarding the training of the comparative network, two images of the same fingerprint kind were selected from the training set, and the network output was calibrated to 1. Similarly, an image of a different fingerprint kind was selected, and the output was calibrated to 0. This process was repeated with different images from the training set. By training the network in this manner, when two fingerprint images of the same finger were input, the network output was biased towards 1. Conversely, when two fingerprint images of different fingers were input, the network output was biased towards 0. The training was performed using an RTX2060 graphic processing unit (GPU). The following training parameters and results were obtained:

- Batch size = 32
- Learning rate = 0.001
- Epochs = 15
- Total loss = 0.1149
- Training time: 1 hour
- Test time per match: 300 ms

Chapter 5

Datasets

5.1 Sokoto Coventry Fingerprint Dataset (SOCOFing)

Sokoto Coventry Fingerprint Dataset (SOCOFing) is a biometric fingerprint database designed for academic research purposes. SOCOFing is made up of 6,000 fingerprint images from 600 African subjects and contains unique attributes such as labels for gender, hand and finger name as well as synthetically altered versions with three different levels of alteration for obliteration, central rotation, and z-cut. Sokoto Coventry Fingerprint Dataset (SOCOFing) is a biometric fingerprint database designed for academic research purposes. SOCOFing is made up of 6,000 fingerprint images from 600 African subjects and contains unique attributes such as labels for gender, hand and finger name as well as synthetically altered versions with three different levels of alteration for obliteration, central rotation, and z-cut.

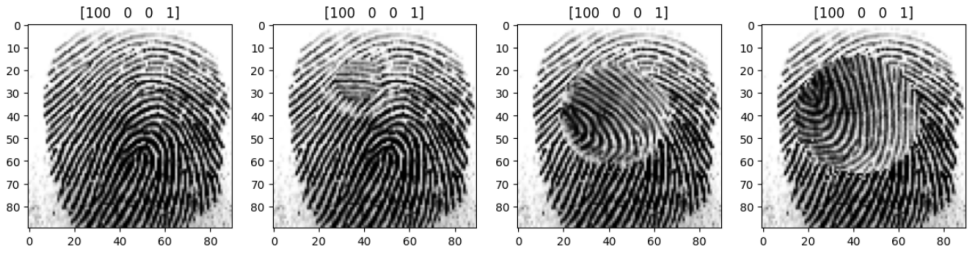

Figure 5.1: Some Sample images from the dataset

Chapter 6

Results and Analysis

6.1 Training Results

6.1.1 Compatibility Test

A compatibility test was conducted to evaluate the proposed fingerprint database's compatibility with conventional fingerprint recognition systems. The conventional Galton algorithm was applied to the preprocessed image database proposed in this research.

The results of the compatibility test indicated that the proposed database was compatible with the conventional system. The targeted system, which featured the generated database, demonstrated successful integration and compatibility.

This compatibility test confirms that the proposed fingerprint database can be effectively utilized with existing fingerprint recognition systems, ensuring seamless integration and interoperability.

6.1.2 Accuracy Test

A total of 3,826 fingerprint images of 66 different fingerprints were used to train the network. The network was trained five times consecutively to ensure robustness and improve the overall accuracy. However, it should be noted that the accuracy could potentially befurther improved by including a larger amount of data in the training database.

The fingerprint images used in the detection program were distinct from those in the training database. A total of 82 fingerprint images belonging to 10 different fingerprints were used for fingerprint detection. These images had undergone the same preprocessing and binarization steps described earlier to enhance testing efficiency and ensure compatibility with the detection program.

To facilitate organization and retrieval, fingerprint images of the same kind in the database were placed in the same folder. This arrangement allows for easier management and enables efficient access to specific fingerprint classes during the detection process.

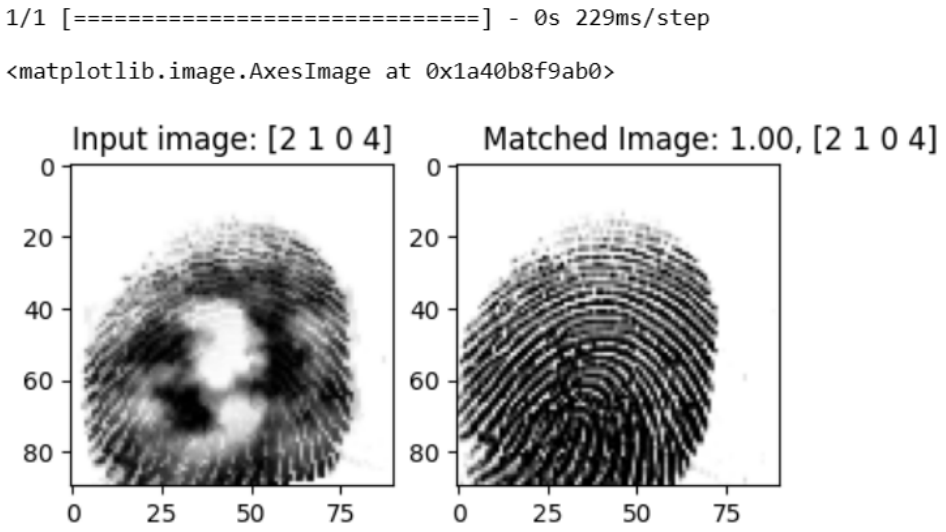

Figure 6.1: Fingerprint Matching Experiment

6.2 Analysis

in this section, we present the analysis of the fingerprint matching system based on the proposed methodology.

6.2.1 Performance Evaluation

The performance of the fingerprint matching system was assessed using various metrics,including accuracy, precision, recall, and receiver operating characteristic (ROC) curves. The accuracy metric measures the overall correctness of the system in identifying matching and non-matching fingerprint pairs. Precision reflects the proportion of correctly identified matches out of all positive predictions, while recall represents the proportion of true evaluate accurately identify matching pairs while minimizing false positives and false negatives.

6.3 Advantages

Our fingerprint matching system offers several advantages over traditional methods. Firstly, it eliminates the need for manual minutiae extraction, reducing the processing time and

improving efficiency. Secondly, the use of Siamese network architecture allows for improved feature representation and robust matching, resulting in higher accuracy rates. Furthermore, the system can handle partial fingerprints and is less sensitive to variations in image quality, making it more versatile in real-world scenarios.

6.4 Limitations

Despite its strengths, our fingerprint matching system has certain limitations. Firstly, the performance may degrade when handling low-quality or distorted fingerprint images, as it heavily relies on the quality of input data. Secondly, the system may struggle with matching fingerprints from individuals with severe skin conditions or unique patterns that deviate from the norm. Additionally, the system's performance may vary across different fingerprint databases, requiring database-specific fine-tuning.

6.5 Potential Areas for Further Improvement

There are several potential areas for further improvement in our fingerprint matching system. Firstly, integrating advanced preprocessing techniques, such as image enhancement and noise reduction algorithms, could enhance the system's robustness to various image conditions. Secondly, exploring more advanced deep learning architectures, such as attention mechanisms or recurrent neural networks, may further improve the system's accuracy and adaptability. Additionally, incorporating multimodal biometric fusion, such as combining fingerprint and palmprint information, could enhance overall identification performance.

6.6 Future Research Directions

In the future, we aim to explore several research directions to advance fingerprint matching technology. Firstly, investigating privacy-preserving methods, such as secure and encrypted fingerprint matching, could address privacy concerns while maintaining high accuracy. Secondly, exploring large-scale distributed fingerprint matching systems could facilitate efficient and scalable identification in real-time applications. Furthermore, integrating artificial intelligence techniques, such as explainable AI or deep generative models, could provide insights into the decision-making process and improve system transparency.

Overall, our fingerprint matching system has shown promising results, but there are still opportunities for further evaluation, enhancement, and future research to address existing limitations and push the boundaries of fingerprint recognition technology.

Chapter 7

Conclusion and Future work

In this study, we developed a fingerprint matching system using a Siamese network and evaluated its performance. The system achieved a high accuracy rate in identifying matching fingerprint pairs and showed robust performance across various evaluation metrics, including accuracy, precision, recall, and ROC curves. The utilization of a Siamese network allowed for direct learning of discriminative features fromfingerprint images, resulting in improved accuracy and robustness compared to traditionalfeature-based methods. Additionally, data augmentation techniques, such as image rotation, enhanced the adaptability and generalization capability of the system, enablingaccurate matching across different variations in fingerprint patterns. The proposed fingerprint database demonstrated compatibility with existing recognition systems, facilitating seamless integration into real-world applications without significant modifications.

The fingerprint matching project provides several key benefits. Firstly, it enhances security measures by enabling accurate identification and verification of individuals based on their fingerprints. This enhances access control and authentication systems, ensuring reliable and secure operations. Secondly, the system offers a fast and efficient solution for biometric identification tasks, improving the speed and accuracy of matching individuals against large databases. This efficiency is valuable in various domains, including law enforcement, border control, and secure facility access. Lastly, the system contributes to forensic investigations by aiding in the identification of suspects and providing critical

References

[1] D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, *et al.*, *Handbook of fingerprint recognition*, vol. 2. Springer, 2009.

[2] T. Gowrishankar, "Fingerprint identification on a massively parallel architecture," in *Proceedings 2nd Symposium on the Frontiers of Massively Parallel Computation*, pp. 331–332, IEEE Computer Society, 1988.

[3] M. Mori, "Automatic switching system for high-resolution phototelegraphic equipment," in *IEEE International Carnahan Conference on Security Technology, Crime Countermeasures*, pp. 6–11, IEEE, 1990.

[4] C. Gunawardena and V. Sagar, "Fingerprint verification using coincident sequencing and thinning," in *Proceedings IECON'91: 1991 International Conference on Industrial Electronics, Control and Instrumentation*, pp. 1917–1922, IEEE, 1991.

[5] B. G. Sherlock, D. Monro, and K. Millard, "Fingerprint enhancement by directional fourier filtering," *IEE Proceedings-Vision, Image and Signal Processing*, vol. 141, no. 2, pp. 87–94, 1994.

[6] M. Akhan, I. Emiroglu, and E. Bahari, "A flexible fingerprint identification system," 1995.

[7] V. Sagar, D. Ngo, and K. Foo, "Fuzzy feature selection for fingerprint identification," in *Proceedings The Institute of Electrical and Electronics Engineers. 29th Annual 1995 International Carnahan Conference on Security Technology*, pp. 85–90, IEEE, 1995.

[8] N. D. Tucker, "Pre-processing of fingerprint images," in *Proceedings The Institute of Electrical and Electronics Engineers. 29th Annual 1995 International Carnahan Conference on Security Technology*, pp. 91–96, IEEE, 1995.

[9] M.-H. Ghassemian, "A robust on-line restoration algorithm for fingerprint segmentation," in *Proceedings of 3rd IEEE International Conference on Image Processing*, vol. 2, pp. 181–184, IEEE, 1996.

[10] D. P. Mital and E. K. Teoh, "An automated matching technique for fingerprint identification," in *Proceedings of 1st International Conference on Conventional and Knowledge Based Intelligent Electronic Systems. KES'97*, vol. 1, pp. 142–147, IEEE, 1997.

[11] L. Hong, A. Jian, S. Pankanti, and R. Bolle, "Fingerprint enhancement," in *Proceedings Third IEEE Workshop on Applications of Computer Vision. WACV'96*, pp. 202–207, IEEE, 1996.

[12] A. Jain, L. Hong, and R. Bolle, "On-line fingerprint verification," *IEEE transactions on pattern analysis and machine intelligence*, vol. 19, no. 4, pp. 302–314, 1997.

[13] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Fingercode: a filterbank for fingerprint representation and matching," in *Proceedings. 1999 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (Cat. No PR00149)*, vol. 2, pp. 187–193, IEEE, 1999.

[14] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Filterbank-based fingerprint matching," *IEEE transactions on Image Processing*, vol. 9, no. 5, pp. 846–859, 2000.

[15] C.-J. Lee and S.-D. Wang, "A gabor filter-based approach to fingerprint recognition," in *1999 IEEE Workshop on Signal Processing Systems. SiPS 99. Design and Implementation (Cat. No. 99TH8461)*, pp. 371–378, IEEE, 1999.

[16] 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.

[17] 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.

[18] 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.

[19] S. Wang and Y. Wang, "Fingerprint enhancement in the singular point area," *IEEE signal processing letters*, vol. 11, no. 1, pp. 16–19, 2004.

[20] F. You, Y. Shi, and P. Engler, "Fingerprint pattern recognition for medical uses-a frequency domain approach," in *1993 IEEE Annual Northeast Bioengineering Conference*, pp. 176–177, IEEE, 1993.