VIETNAM NATIONAL UNIVERSITY HO CHI MINH CITY
THE UNIVERSITY OF SCIENCE
FACULTY OF INFORMATION TECHNOLOGY

FINAL REPORT
FINGERPRINT RECOGNITION
SUBJECT: PATTERN RECOGNITION

UNDER THE GUIDANCE OF

Le Hoang Thai
Truong Tan Khoa
Duong Thai Bao

MEMBERS

Name	**Student ID**
Huynh Nhat Nam	22127282
Pham Thanh Nhan	22127307
Huynh Thien Thuan	22127407

Date of submission: May 11, 2025

Appendix A: List of Abbreviations

CNN Convolutional Neural Network

FBI Federal Bureau of Investigation

GLCM Gray-Level Co-occurrence Matrices

IAFIS Integrated Automated Fingerprint Identification System

Contents

1 Introduction

1.1 Definition

1.1.1 Definition of fingerprint

Figure 1: A collection of fingerprint images showcasing various ridge patterns and unique minutiae details. Each fingerprint represents the intricate patterns of ridges and valleys found on human fingertips, highlighting the individuality and complexity of biometric traits used for personal identification and verification. The images illustrate the diversity in fingerprint patterns which contribute to their reliability in forensic and security applications.

A **fingerprint** is the pattern of ridges and valleys that naturally appears on the surface of a human fingertip. These patterns form during the first seven months of fetal development and remain unchanged throughout a person's lifetime under normal biological conditions. Every individual has a completely unique set of fingerprints, even identical twins or different fingers of the same person. Due to their uniqueness and long-term stability, fingerprints are considered one of the most reliable biometric traits for personal identification (see Figure 1). [9]

1.1.2 Definition of fingerprint biometrics

Fingerprint biometrics refers to the application of technology to capture, analyze, and match fingerprint characteristics to verify or identify an individual's identity. Biometric systems use algorithms to convert a fingerprint image into a digital template (feature representation), which is then compared with stored data to produce an authentication result. Due to their non-replicable nature and high level of automation, fingerprint biometrics are widely used in areas such as security, forensics, mobile devices, and access control systems. [10]

1.2 History

Biometric recognition, particularly fingerprint analysis, has a long and rich history that dates back thousands of years. Ancient Babylonian and Chinese civilizations used fingerprints as a form of signature in business transactions and clay seals. However, the scientific study and systematic application of fingerprints in forensic science did not begin until the late 19th century. One of the first proponents of fingerprinting was Henry Faulds, who published a letter in *Nature* in 1880 suggesting the use of fingerprints for identification purposes. Around the same time, Sir Francis Galton conducted extensive statistical studies on fingerprint patterns, concluding that fingerprints are unique and remain unchanged throughout a person's life. Galton also proposed the first fingerprint classification system, which laid the groundwork for modern fingerprint science [11].

Building on Galton's work, Sir Edward Henry developed the Henry Classification System, which was adopted by police forces in the UK and later by the Federal Bureau of Investigation (FBI) in the United States. This system enabled the efficient indexing and retrieval of fingerprint records, revolutionizing criminal investigations in the early 20th century [11].

By the late 20th century, the development of digital technology and computational methods led to the creation of large-scale fingerprint databases. One significant milestone was the launch of the Integrated Automated Fingerprint Identification System (IAFIS) by the FBI in 1999. IAFIS was capable of storing and matching tens of millions of fingerprint records, including full sets from all ten fingers, along with associated demographic data. This allowed for a faster and more accurate identification of individuals between jurisdictions [11].

Parallel to these developments in biometric identity verification, image processing methods have also advanced. One such technique is the use of Gray-Level Co-occurrence Matrices (GLCM), introduced by Haralick et al. in 1973, to analyze texture in images. GLCMs are still widely used today in fingerprint feature extraction and classification tasks. In recent years, researchers have proposed improvements to the GLCM approach to better handle challenges such as image rotation. For instance, Bianconi and Fernández (2014) suggested using circular symmetric neighborhoods instead of the conventional horizontal and vertical directions to enhance rotation invariance in texture features [6].

These historical developments demonstrate the continuous evolution of fingerprint analysis—from manual inspection to automated recognition using sophisticated algorithms—and highlight the interdisciplinary nature of the field, bridging biology, statistics, image processing, and computer science.

1.3 Why fingerprint recognition matters?

Fingerprint recognition plays a very important role in keeping people and information safe in today's world. A fingerprint is a pattern made up of ridges and valleys at the tip of each finger. These patterns are unique to each person and do not change over time, even as people get older. Even identical twins do not have the same fingerprints. Because of this, fingerprints are one of the most trusted and reliable ways to identify individuals. For more than 100 years, law enforcement agencies around the world have used fingerprints to solve crimes, find suspects, and confirm the identity of victims or missing people. Fingerprints are also widely used by immigration departments to track and confirm travelers at borders. In recent years, as technology has grown, fingerprint recognition has become more common in our daily lives. Today, many people use their fingerprints to unlock smartphones, open laptops, enter their homes or workplaces, and even authorize online payments. Some hospitals use fingerprint scanners to ensure that patient records are kept private and safe. Banks and financial services also rely on fingerprint recognition to allow access to accounts and to protect sensitive data. This shows how fingerprints changed from being only used in police work to becoming a part of modern digital life. One of the main reasons fingerprint systems are popular is that they are easy to use, fast, affordable, and do not require people to remember passwords or carry ID cards. However, like any system, fingerprint recognition is not perfect. If the system is poorly designed or not secure, attackers can fool or hack it and steal personal data from people or access private systems. For example, fake fingerprints can sometimes be used to trick scanners, and low-quality images can cause the system to make mistakes. That is why researchers and engineers are working hard to make fingerprint recognition systems smarter and safer. Using better image processing techniques, advanced pattern recognition, and artificial intelligence, we can build systems that are more accurate, harder to fool, and capable of working well even when the fingerprint is not perfectly clear. These improvements are especially important for large systems used by governments or companies where the safety of millions of people depends on strong security. In the future, as more devices and services connect to the Internet, the need for safe and reliable ways to verify identity will continue to grow. Fingerprint recognition will remain one of the main tools for protecting personal information, securing digital systems, and ensuring that only the right people can access certain places or services. For all of these reasons, fingerprint recognition is not only a helpful technology but also a key part of building a safer and more secure world [3].

2 Fingerprint structure

2.1 Skin Anatomy of the Finger

The human fingertip skin is a specialized structure composed of two main histological layers: the **epithelium**, a stratified squamous keratinized epithelium derived from the ectoderm, and the underlying **dermis**, composed primarily of dense irregular connective tissue of mesodermal origin. The interface between these layers is characterized by interdigitating structures: the downward projections of the epidermis (rete ridges) and the upward dermal projections (dermal papillae), which enhance mechanical strength and surface area for metabolic exchange. One of the most distinctive features of volar skin (skin on the palms and soles, including fingertips) is the presence of **primary friction ridges**, which are epidermal ridges aligned with underlying dermal structures. These ridges are supported by **primary dermal ridges** and contain openings of **eccrine sweat glands**, which play role in thermoregulation and tactile grip. As shown in Figure 2, the sweat ducts pass through the dermis and epidermis and open at the apex of the epidermal ridges. The formation of fingerprint patterns begins during fetal development, specifically between 10^{th} and 16^{th} gestational weeks. Initially, transient swellings known as **volar pads** form at specific locations on the fingers, palms, and soles. The shape, size and regression timing of these pads, along with intrinsic genetic instructions and extrinsic mechanical forces such as amniotic pressure and fetal movement, contribute to the three main classes of ridge patterns: *arches*, *loops*, and *whorls*. By the 16^{th} week of gestation, the formation of the primary ridge stabilizes. The resulting ridge architecture becomes permanently embedded in the basal layer of the epidermis and is maintained throughout life, even with injury or epidermal turnover, due to the regenerative properties of the basal keratinocytes aligned along

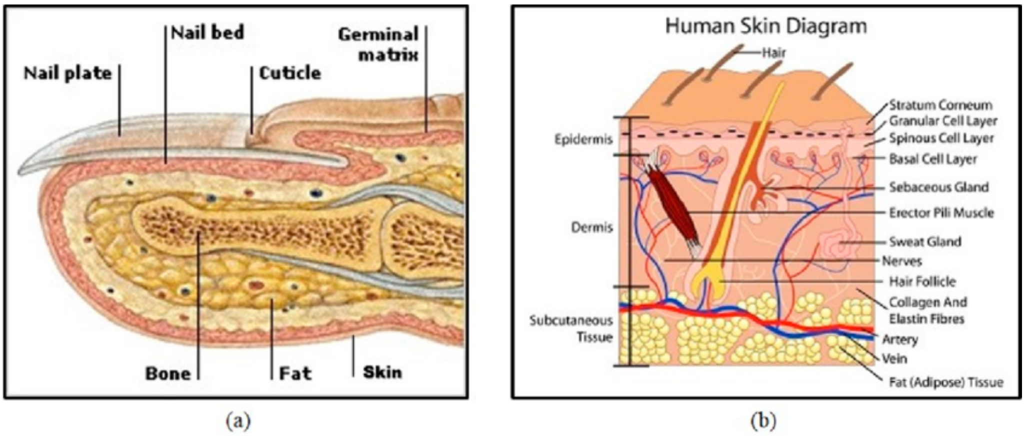

Figure 2: Cross-sectional view of the fingertip and human skin. (a) The fingertip structure includes parts like the nail, nail bed, cuticle, and layers underneath such as skin, fat, and bone. These parts help protect and heal the fingertip. (b) A diagram of human skin showing three main layers: epidermis, dermis, and subcutaneous tissue. The epidermis has smaller layers, including the one where fingerprint patterns start. The dermis contains sweat glands, oil glands, hair roots, blood vessels, nerves, and collagen. These help with touch, temperature control, and skin strength. The image shows how skin structure is connected to fingerprint patterns.

the dermal template. This unique combination of permanence, uniqueness, and accessibility makes fingerprints one of the most reliable biometric modalities for personal identification in medical and forensic applications [5, 7].

2.2 Types of fingerprint patterns

The fingerprint patterns, as illustrated in 3, are classified into three major categories based on the unique flow and arrangement of the ridge lines. These categories are determined by the overall structure of the ridges and how they interact with each other on the surface of the finger, which plays a critical role in distinguishing different types of fingerprint.

- **Loops**: Approximately 60 to 65% of fingerprint patterns are the most common type and are characterized by ridge lines that enter from one side of the finger, recur and exit from the same side. A single delta, a triangular region which ridge lines diverge, is typically present. There are two types of loops: the **ulnar loop**, which opens toward the ulna bone (the side of the little finger) and is the most common type found on all fingers except the thumbs, and the **radial loop**, which opens toward the radius bone (the side of the thumb) and is less frequent than ulnar loops, particularly rare on the little finger. Loops are often associated with a high degree of symmetry and are found in both healthy individuals and those with certain congenital syndromes. Any asymmetry or unusual development in loops may correlate with developmental disorders.

- **Whorls**: Approximately 30—-35% of the fingerprint patterns exhibit ridge formations that are typically circular, spiral, or concentric. They are distinguished by the presence of two or more deltas and a central core. Subtypes of whorls include: **Plain whorl**,

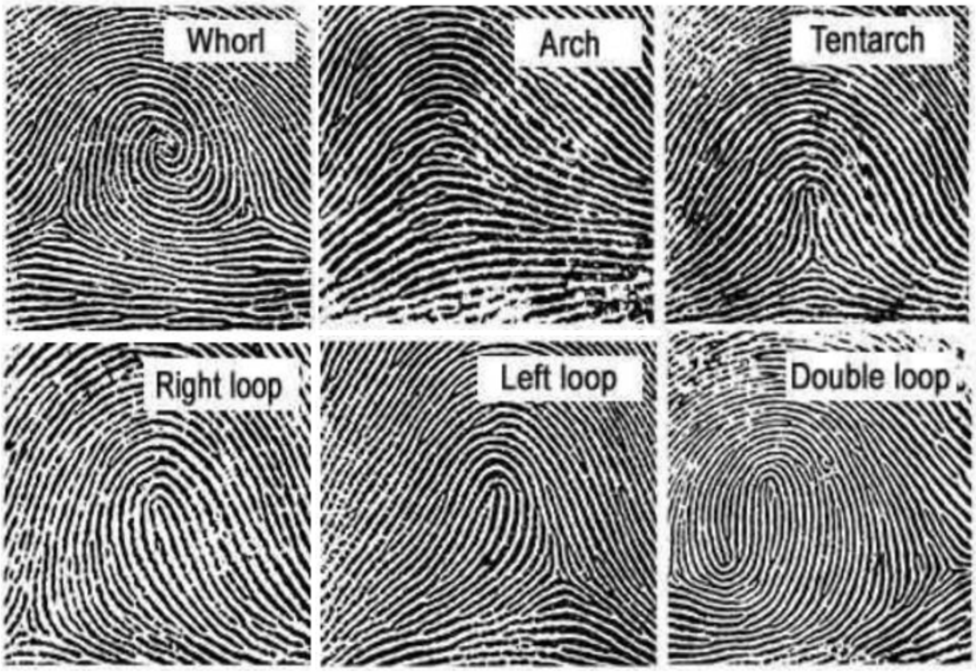

Figure 3: Fingerprint patterns classified based on the distribution and structure of ridge lines: (a) Loops, characterized by ridge lines that enter from one side and recur, exiting from the same side; (b) Whorls, with ridge lines forming circular or spiral patterns, featuring at least two delta points; (c) Arches, the rarest pattern, where ridge lines enter from one side and exit from the other without curving, typically without delta points except in the case of tented arches.

Central pocket loop whorl, **Double loop whorl**, and **Accidental whorl**. From a medical genetics standpoint, whorls may have a slightly higher prevalence in individuals with certain chromosomal abnormalities, such as trisomy 21 (Down syndrome), where atypical dermatoglyphic patterns can serve as diagnostic markers.

- **Arches**: The rarest fingerprint pattern, which account for approximately 5% of all patterns. Arches consist of ridge lines that enter from one side and exit the other without curving back. Unlike loops and whorls, arches lack deltas (except tented arches, which may have one). There are two subtypes of arches: **Plain arch**, characterized by a gentle, wave-like rise in the center, and **Tented arch**, which features a more pronounced vertical rise, sometimes with a sharp up-thrust or a loop-like formation at the core. Arches are more frequently observed in certain congenital malformation syndromes. For instance, an increased frequency of arch patterns has been reported in individuals with Turner syndrome and Klinefelter syndrome.

2.3 Minutiae Features

The minutiae of the fingerprints refer to localized ridge characteristics that serve as the cornerstone of fingerprint comparison and identification. These microscopic features are pivotal in forensic science, biometrics, and security systems due to their uniqueness to each individual. The distinct arrangement and variability of minutiae enable highly accurate identification,

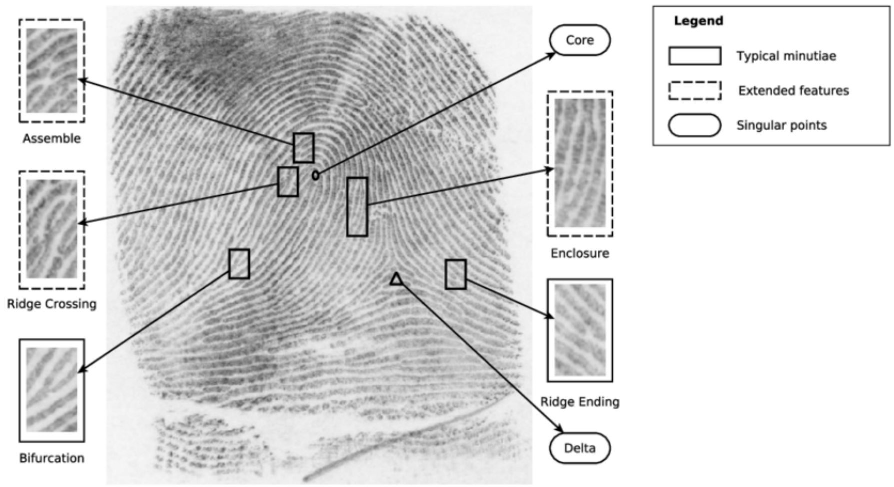

Figure 4: An illustrative depiction of the primary minutiae types critical for fingerprint recognition and identification. This figure highlights key ridge characteristics, such as ridge endings, bifurcations, islands, lakes, and bridges, which form the basis of biometric and forensic fingerprint analysis. Each minutia type is uniquely defined by its structural properties, contributing to the distinctiveness of individual fingerprints used in security, law enforcement, and identity verification systems.

making them indispensable in applications ranging from criminal investigations to secure access control. The following list details the most common types of minutiae, categorized based on their unique structural forms and variations in fingerprint ridge patterns:

- **Ridge Ending**: A ridge that abruptly terminates, forming a distinct endpoint. Ridge endings are among the most prevalent and critical minutiae in fingerprint matching, providing clear reference points for analysis. Their precise location and orientation are essential for comparing fingerprints, particularly in forensic investigations where identifying ridge terminations helps map the overall structure of the fingerprint [12].

- **Bifurcation**: A point where a single ridge diverges into two separate ridges. Bifurcations are vital for recognizing the complex branching patterns that contribute to the uniqueness of a fingerprint. Their presence in a fingerprint creates a distinctive network of ridges, which is highly unlikely to replicate between individuals, making them a key feature in comparative analysis [18].

- **Island (Dot)**: A short, isolated ridge or dot situated between two larger ridges. Despite their small size, islands are important in identifying specific fingerprint patterns, particularly in dense or intricate ridge structures. They serve as subtle yet reliable markers in the matching process, enhancing the precision of fingerprint identification [12].

- **Lake (Enclosure)**: A ridge that splits and subsequently rejoins, forming a closed loop resembling a "lake." Lakes are prominent in complex fingerprint patterns with looping or circular structures. Their unique formation, influenced by skin pressure and growth variations, makes them a strong feature to distinguish fingerprints with similar macrolevel patterns [18].

- **Bridge (Crossover)**: A short ridge connecting two parallel ridges, creating a "bridge" or crossover effect. Bridges are significant in intricate fingerprints where the ridges intersect or form connections. They provide critical reference points in identification systems that require high-accuracy ridge matching, particularly in automated biometric systems [12].

These types of minutiae form the foundation of modern fingerprint analysis, enabling forensic scientists, law enforcement, and biometric systems to identify individuals with exceptional precision. The variability, distribution, and combination of minutiae in each fingerprint ensure their reliability as a tool for identification, particularly in high-stakes applications such as criminal justice and national security. Advances in automated fingerprint identification systems (AFIS) have further enhanced the ability to detect and analyze minutiae, strengthening their role as a pillar of forensic science and biometric technology [18].

3 Problem Statement

Fingerprint recognition has become a widely adopted biometric technique due to the uniqueness, permanence, and universality of fingerprint patterns. It is commonly used in diverse applications, including identity verification, law enforcement, and access control in smartphones and secure systems. Despite considerable advancements in fingerprint recognition technology, numerous challenges remain that hinder its robustness and reliability in real-world scenarios. One of the primary issues is the low quality of fingerprint images captured during acquisition. In practical environments, images are often degraded due to improper finger placement, partial impressions, excessive or insufficient pressure, or external conditions such as dirt, moisture, dryness, or poor lighting. These factors can significantly affect the clarity of ridge patterns and minutiae points, which are essential for accurate recognition. Another critical challenge is intra-class variation, where multiple impressions of the same fingerprint may differ due to rotation, scaling, distortion, smudging, or partial capture. Such variability is especially prevalent in uncontrolled environments, such as public kiosks or mobile devices, where consistent finger positioning cannot be guaranteed. As a result, traditional fingerprint matching systems often struggle with high false rejection rates and reduced accuracy. To address these limitations, deep learning-based methods have been introduced, offering improved tolerance to image variability and distortions. These models can learn complex representations from large-scale fingerprint datasets, leading to enhanced performance in challenging scenarios. However, deep learning approaches introduce new concerns. They typically require extensive labeled data and significant computational resources for training and deployment. Furthermore, their black-box nature limits transparency and interpretability, making them less suitable for sensitive applications such as legal or forensic investigations, where explainability is essential. In addition, scalability presents another significant challenge. Matching a query fingerprint against millions of entries in a large-scale database can result in substantial computational overhead and increased latency, which is detrimental to time-sensitive applications. Moreover, maintaining a suitable balance between false acceptance rates (FAR) and false rejection rates (FRR) remains a difficult trade-off. A system optimized for security may inconvenience legitimate users, whereas a lenient system may compromise security. In summary, while fingerprint recognition remains a promising biometric modality, it continues to face practical challenges related to image quality, variability, system transparency, scalability, and performance trade-offs. Addressing these issues is essential for improving the robustness, fairness, and usability of fingerprint recognition systems in real-world deployments.

4 Related Works

Method 1: CNN with Inversion and Augmented Techniques [2]

Fingerprint recognition has long been a critical area of study in biometric identification, with traditional machine learning methods forming the backbone of earlier approaches. Techniques such as Support Vector Machines (SVM) [14, 19, 25], Random Forest with Oblique Decision Trees (RF-ODT) [8, 24], Bag of Words (BoW) [13, 22], and Scale-Invariant Feature Transform (SIFT) [15, 16] have been widely adopted due to their simplicity and effectiveness, particularly when applied to small datasets. These methods are valued not only for their computational efficiency in constrained settings but also for their interpretability, which provides insights into the decision-making process—a feature often lacking in more complex models. However, their limitations become apparent when tackling intricate, real-world tasks like fingerprint recognition. Scalability poses a significant challenge; as dataset sizes grow, these methods incur substantial computational overhead, often resulting in diminished performance. Moreover, they struggle to process high-dimensional data effectively and exhibit sensitivity to noise, which can compromise accuracy in practical scenarios where fingerprint images may vary in quality. In parallel, minutiae-based techniques [20, 23] have been developed specifically for fingerprint recognition. These methods focus on identifying and matching minutiae—unique ridge characteristics such as bifurcations and terminations—within fingerprint images. By incorporating advanced techniques like fuzzy sets and sophisticated matching algorithms, minutiae-based approaches can achieve commendable recognition accuracy under controlled conditions. Nevertheless, their reliance on specific fingerprint features limits their flexibility, and the computational complexity of extracting and matching minutiae increases significantly with larger datasets. Another critical drawback is their limited generalization; variations in image quality, orientation, or acquisition methods can degrade performance. To overcome these challenges, recent research has shifted toward Convolutional Neural Network (CNN)s, which have revolutionized image recognition tasks across various domains. Unlike traditional methods, CNNs eliminate the need for manual feature engineering by automatically learning hierarchical feature representations directly from raw data. CNNs also excel at handling high-dimensional data and demonstrate greater resilience to noise. The proposed method [2] introduces two such strategies within a CNN framework: the **Inversion method** and the **Multi-Augmentation method**.

- **Inversion method:** The Inversion Method is a novel preprocessing technique designed to enrich feature representation. It operates by splitting each fingerprint image into two equal halves, inverting each segment (e.g., flipping the pixel intensities or orientations), and then processing these inverted segments in parallel through the CNN. The hypothesis is that inversion reveals complementary information not readily apparent in the original image. Feeding both the original and inverted segments into the network effectively doubles the feature space, improving classification accuracy and robustness.

- **Multi-Augmentation method:** The Multi-Augmentation method aims to mitigate overfitting by increasing the diversity of the training dataset. It generates eight distinct variants of each fingerprint image through transformations such as rotation, scaling, flipping, shearing, and brightness adjustments. The resulting dataset exposes the CNN to a broader spectrum of image variations, enhancing its generalization ability and resilience to poor-quality inputs.

Model	**Precision (%)**	**Recall (%)**	**F1-score (%)**	**Accuracy (%)**
VGG16 (Normal)	91	91	91	91
VGG16 (Inversion)	93	93	93	93
VGG16 (Augmentation)	**97**	**97**	**97**	**97**
VGG19 (Normal)	93	93	92	93
VGG19 (Inversion)	88	88	87	88
VGG19 (Augmentation)	93	93	93	93

Table 1: Comparison of the classification performance of VGG16 and VGG19 models under different preprocessing strategies, including normal input, image inversion, and data augmentation. The table reports four standard evaluation metrics: Precision, Recall, F1-score, and Accuracy, all expressed as percentages. Among all configurations, the VGG16 model with data augmentation achieved the highest performance across all metrics (97%), indicating that augmentation significantly enhances the model's generalization ability. In contrast, applying image inversion did not consistently improve results and, in the case of VGG19, slightly reduced performance. These findings suggest that model architecture and preprocessing choices both substantially affect classification outcomes.

These techniques were evaluated using two CNN architectures: VGG16 [21] and VGG19 [21], with results summarized in Table 1 under various preprocessing strategies. The VGG16 model with augmentation achieved the highest performance across all metrics, reaching 97%, significantly outperforming the baseline VGG16 and the inversion variant, while VGG19 also benefited from augmentation though its gains were less pronounced and degraded under inversion. These outcomes highlight the particular effectiveness of augmentation with VGG16, likely due to its architecture's capacity to better utilize enriched data. The method offers notable benefits, such as improved feature diversity, faster convergence, resilience to poor image quality, and strong performance on small datasets. However, it also brings limitations including higher computational demands, architecture-sensitive performance, and restricted generalizability across datasets. Potential future directions involve optimizing augmentation to reduce resource consumption, evaluating other CNNs like ResNet or MobileNet, expanding testing across diverse datasets, and exploring ensemble methods. Overall, the integration of Inversion and Multi-Augmentation into a CNN framework represents a significant advance over conventional and minutiae-based methods, particularly excelling with VGG16 by effectively addressing challenges in feature extraction and generalization, though further work is needed to mitigate computational overhead and enhance cross-dataset robustness.

Method 2: Integrating attention modules with lightweight deep learning models [1]

Lightweight deep learning models have become increasingly prominent in practical applications where computational resources are limited, such as mobile devices and embedded systems.

These models achieve efficiency primarily by reducing network depth, width, or complexity of convolutional layers, as exemplified by architectures like MobileNet and EfficientNet-B0 [4]. MobileNet leverages depth-wise separable convolutions to decompose standard convolutions into lightweight operations, drastically decreasing the number of parameters and computations required. Meanwhile, EfficientNet-B0 adopts a compound scaling method to optimally balance the network's depth, width, and resolution, resulting in a model that offers state-of-the-art accuracy with relatively low resource consumption. Despite these efficiencies, lightweight models tend to experience performance degradation compared to their deeper, more complex counterparts, mainly due to reduced representational capacity and limited feature extraction. To counteract this, recent research has focused on integrating attention mechanisms within lightweight architectures. Attention modules serve to recalibrate feature maps dynamically, allowing models to selectively emphasize informative features while suppressing less relevant ones. This capability is critical for maintaining or improving classification accuracy without compromising computational advantages. Among various attention designs, the Squeeze-and-Excitation (SE) module is widely regarded for its simplicity and effectiveness. It performs channel-wise feature recalibration by applying global average pooling followed by two fully connected layers to generate channel attention weights. However, SE exclusively focuses on channel attention and ignores spatial information, which can be a limiting factor for complex visual recognition tasks where spatial context is important. To address this limitation, self-attention mechanisms have been proposed that capture long-range dependencies in both channel and spatial dimensions. These modules typically employ parallel convolutional layers and softmax operations to model relationships between distant spatial locations, enhancing the network's contextual awareness. Building on this idea, the Convolutional Block Attention Module (CBAM) sequentially applies channel attention and spatial attention in a lightweight manner. This two-step process enables CBAM to refine feature representations more comprehensively by considering both what and where to attend in the feature maps. Further advancing this concept, Dual Attention mechanisms combine position attention (spatial) and channel attention in a unified framework. This approach simultaneously models the interdependencies across channels and spatial positions, leading to richer and more discriminative feature maps. Such dual-attention integration has shown notable improvements in various computer vision tasks, including classification, detection, and segmentation. Our experiments investigated the effects of integrating these attention modules into two representative lightweight models: MobileNet+ and EfficientNet-B0+. Both models were augmented with SE, Self-Attention, CBAM, and Dual Attention modules, and evaluated on a standard classification benchmark. The results clearly indicate that attention-enhanced lightweight models achieve superior performance across multiple metrics, including accuracy, precision, recall, and F1 score, compared to their vanilla counterparts. Specifically, the Dual Attention module consistently outperformed other attention types in both MobileNet+ and EfficientNet-B0+ models, achieving the highest accuracy and balanced precision-recall trade-offs. CBAM also demonstrated strong performance, surpassing SE and Self-Attention in most cases, which underscores the importance of combining channel and spatial attentions. Interestingly, the SE module, despite its popularity, yielded comparatively lower improvements, likely due to its exclusive focus on channel-wise recalibration and lack of spatial attention components. Moreover, the EfficientNet-B0+ model with Dual Attention achieved the best overall results, highlighting the synergy between advanced attention modules and carefully optimized lightweight architectures. This approach not only maintains the low parameter count and computational cost inherent to lightweight models but also bridges the accuracy gap relative to more computationally intensive deep learning architectures, such as those used in the study by Ametefe et al. These findings reinforce the potential of attention mechanisms as a vital enhancement technique for lightweight deep learning models, enabling practical deployment in resource-constrained environments without sacrificing classification performance. Future work may explore further refinements, such as dynamic attention gating or hybrid attention models, to push the efficiency-accuracy trade-off even further.

Results Achieved for MobileNet+ Model

Attention Module	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
Squeeze and Excitation	95.8	95.7	95.8	95.7
Self-Attention	96.2	96.1	96.2	96.1
CBAM	96.6	96.6	96.7	96.6
Dual	96.8	96.7	96.8	96.7

Table 2: Results achieved for each attention module in the MobileNet+ model

Results Achieved for EfficientNet-B0+ Model

Attention Module	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
Squeeze and Excitation	96.8	96.7	96.8	96.8
Self-Attention	96.4	96.3	96.4	96.3
CBAM	96.7	96.6	96.7	96.6
Dual	97.0	96.8	97.0	96.9

Table 3: Results achieved for each attention module in the EfficientNet-B0+ model

Despite the demonstrated improvements brought by integrating attention modules into lightweight deep learning models, several limitations remain. Not all attention mechanisms yield equal benefits; for example, the Squeeze-and-Excitation module often underperforms compared to more advanced attention designs due to its lack of spatial attention. Additionally, although these modules are designed to be lightweight, they inevitably introduce some computational overhead and may increase inference time, which could pose challenges in extremely resource-constrained environments. The effectiveness of attention-enhanced models can also vary depending on dataset characteristics and task complexity, necessitating careful selection and tuning of the attention mechanisms. Moreover, this approach primarily focuses on improving classification accuracy without explicitly addressing other important aspects such as model robustness, interpretability, or adaptability to different domains. Nonetheless, integrating attention mechanisms like CBAM and Dual Attention into architectures such as MobileNet and EfficientNet-B0 significantly enhances feature representation and classification performance. These attention-augmented lightweight models consistently outperform their baseline versions and approach the accuracy levels of more complex networks. Among the tested modules, Dual Attention provides the most substantial improvements, highlighting the benefit of jointly modeling spatial and channel dependencies. Overall, this approach presents a promising balance between efficiency and accuracy for practical applications requiring lightweight models.

5 Dataset

The fingerprint dataset employed in this research is the FVC2000 DB4 B dataset, part of the Fingerprint Verification Competition 2000 (FVC2000) benchmark suite. The FVC series, initiated by Maio et al. [17], has become a standard in the fingerprint recognition community, providing a controlled and publicly accessible set of fingerprint images for algorithm evaluation and comparison.

5.1 Description

FVC2000 DB4 B is a benchmark dataset comprising synthetic fingerprint images generated using the Synthetic Fingerprint Generator (SFinGe), a specialized software designed to simulate the appearance and variability of real fingerprint impressions with high fidelity. Unlike datasets derived from physical fingerprint acquisition involving live subjects and biometric sensors, DB4 B provides an entirely artificial yet highly controlled environment, enabling researchers and developers to systematically examine and evaluate the performance of fingerprint recognition algorithms under a wide range of conditions. The dataset is composed of 80 grayscale fingerprint images, organized into 10 unique fingerprint classes, each representing a different synthetic finger, with 8 distinct impressions per class that simulate multiple acquisition instances. Each fingerprint image is stored in TIFF format with a spatial resolution of approximately 500 dots per inch (dpi), ensuring fine-grained detail necessary for feature extraction and analysis, and standardized dimensions of 240 pixels in width and 320 pixels in height. The images capture plain fingerprint impressions, the most commonly used format in biometric authentication systems, providing consistency with practical applications. The synthetic nature of the dataset allows for the inclusion of controlled variations such as geometric distortions, noise, and positional shifts, which are critical for testing algorithm robustness under real-world conditions. As a result, DB4 B serves as a reliable and reproducible benchmark for the academic and industrial development of fingerprint recognition technologies, offering both diversity in fingerprint patterns and consistency in format and quality to facilitate fair comparison and repeatable experimentation.

5.2 Synthetic generation method

The SFinGe tool, employed in generating the FVC2000 DB4 B dataset, utilizes a sophisticated parametric model to synthesize fingerprint images that closely replicate the features of real fingerprints, including ridge structures, minutiae (like ridge endings and bifurcations), and texture. This model supports systematic variation, enabling the creation of diverse fingerprint patterns that mirror the variability found in real-world scenarios influenced by skin conditions, pressure, and scanner quality. To simulate practical challenges in fingerprint acquisition, the method incorporates controlled variations such as geometric distortions (mimicking pressure-induced warping), rotational and translational changes (reflecting inconsistencies in finger placement), partial prints (representing incomplete captures), and noise (imitating environmental or scanner-induced imperfections). These variations are systematically applied to master fingerprints—initial templates produced by the parametric model—resulting in multiple unique impressions per finger that reflect real-world variability across scans. This synthetic generation approach offers a standardized and comprehensive testing environment for fingerprint matching algorithms, providing known ground truths like minutiae positions and applied distortions to support accurate and fair performance evaluation. By replicating both the diversity of fingerprint patterns and the acquisition inconsistencies encountered in practice, the method significantly contributes to the development and benchmarking of more robust and effective fingerprint recognition systems.

5.3 Relevance and applications

The FVC2000 DB4 B dataset holds significant value in the domain of fingerprint recognition research and development due to its role as a standardized collection of synthetic fingerprint images. This dataset provides researchers, engineers, and developers with a consistent and widely accepted benchmark for designing, testing, and evaluating fingerprint matching algorithms. By using this common dataset, it becomes easier to fairly compare the performance of different fingerprint recognition techniques since all methods are tested on the same set of images under the same conditions. Such comparability is critical for advancing the field, as it helps identify the strengths and weaknesses of various approaches objectively. Moreover, the synthetic images within the DB4 B dataset are carefully crafted to replicate many of the challenges encountered in real-world fingerprint acquisition. These include common issues such as partial fingerprints, where some parts of the fingerprint are missing due to incomplete finger placement; noisy or blurred images caused by motion or sensor imperfections; and distortions resulting from skin elasticity or pressure variations. The presence of these imperfections allows the dataset to serve as a useful testing ground for assessing the robustness and resilience of fingerprint recognition systems when confronted with imperfect or degraded data. This is particularly important because real-life fingerprint images rarely appear in ideal conditions. In addition to its utility for testing, the DB4 B dataset is well-suited for training machine learning models that underpin many modern fingerprint recognition systems. Its moderate size strikes a balance between diversity and manageability, offering a range of fingerprint patterns without overwhelming computational resources. This makes DB4 B especially valuable during early development phases, where rapid prototyping and algorithm tuning are necessary without the expense or complexity of very large datasets. Consequently, both academic researchers exploring new fingerprint recognition methods and industry practitioners seeking to evaluate or refine their systems benefit from the availability of DB4 B. It serves as a stepping stone—enabling initial validation and experimentation—before committing to larger-scale data collection or deployment with more complex, real fingerprint databases.

5.4 Dataset limitations

While the FVC2000 DB4 B dataset offers numerous advantages, it also has important limitations that must be carefully considered when applying its results to practical fingerprint recognition problems. One of the primary constraints stems from the fact that DB4 B contains synthetic fingerprint images, which are computer-generated simulations rather than genuine fingerprints collected from human subjects. Although these synthetic images are designed to mimic real fingerprints closely, they inevitably lack some of the subtle complexities and unpredictable variations that arise naturally in actual fingerprint data. Real fingerprint images exhibit a wide range of characteristics influenced by various physical and environmental factors. For instance, the way skin deforms under pressure can alter ridge patterns subtly but meaningfully, and differences in finger placement angle or contact force can produce variations that are challenging to replicate synthetically. Additionally, fingerprints may be affected by sweat, dirt, cuts, or scars, and sensors themselves can introduce artifacts such as smudging, partial impressions, or electronic noise. These real-world nuances increase the difficulty of fingerprint matching, as algorithms must be robust enough to handle such inconsistencies. Because synthetic images often lack these detailed imperfections or may only approximate them to a limited extent, fingerprint recognition algorithms that perform well on the DB4 B dataset might not necessarily maintain the same level of accuracy or robustness when applied to real fingerprint images. This gap highlights the importance of cautious interpretation of experimental results obtained solely with synthetic datasets. Another notable limitation is the relatively small size of DB4 B compared to more extensive fingerprint databases. The limited number of samples restricts its effectiveness for training very complex models—especially those based on deep learning architectures—which generally require large and diverse datasets to achieve optimal generalization. Therefore, while the FVC2000 DB4 B dataset is a valuable resource for early-stage research, prototyping, and benchmarking, it is essential to complement its use with larger and more representative real fingerprint datasets when developing systems intended for deployment. Testing on real-world data helps ensure that fingerprint recognition systems are not only accurate but also reliable and resilient to the wide range of practical conditions encountered during everyday use, ultimately safeguarding their effectiveness in security-critical applications.

6 Our proposed Method

In this first method, two widely recognized deep convolutional neural network (CNN) architectures—**VGG16** and **VGG19**—are implemented to address the challenging problem of fingerprint recognition and matching. These architectures were selected due to their proven effectiveness in image classification tasks and their relatively simple yet powerful layer designs that facilitate hierarchical feature extraction. The main objective is to optimize classification accuracy while enhancing the model's generalization capabilities, especially under conditions of limited available data. To this end, specialized input data processing techniques are integrated to enrich and robustify the fingerprint feature representations before feeding them into the CNN models. The first technique, referred to as the **Inversion Method**, aims to augment fingerprint features by exploiting the intrinsic local structures and symmetries present in fingerprint images. This method involves splitting each fingerprint image into two parts, either vertically or horizontally, and independently inverting each part. Subsequently, features are extracted in parallel from these two halves through the CNN, thereby encouraging the model to capture complementary multi-dimensional structural variations. The rationale behind this approach is that dissecting and transforming local regions may reveal discriminative patterns that a holistic view might miss, potentially expanding the effective input feature space. However, empirical results indicate that this inversion-based augmentation leads to a slight decrease in accuracy compared to training on the original images. We hypothesize that the inversion operation introduces unnatural distortions to the fingerprint ridge and valley patterns, which disrupt the stable morphological features essential for reliable classification. As a result, the model's ability to learn robust and discriminative features is hindered. To mitigate overfitting and further enhance robustness to realistic variations in fingerprint acquisition—such as shifts, lighting changes, and scanning orientation—the **Multi-Augmentation Method** is employed.

In this method, from each original fingerprint image, eight augmented versions are generated by applying a combination of common transformations including rotation, flipping (horizontal and vertical), contrast adjustment, zooming, and local translations. This data augmentation simulates the variability encountered in practical fingerprint scanning environments, enabling the CNN models to learn invariant features and improving their generalization to unseen samples. Experimental results demonstrate that this augmentation technique maintains, and in some cases slightly improves, classification accuracy, achieving performance levels comparable to training solely on the original dataset. This confirms the effectiveness of multi-augmentation in preventing overfitting and promoting the learning of robust fingerprint representations.

Model	**Method**	**Accuracy**
VGG16	Original	0.93
VGG16	Inversion	0.86
VGG16	Augmentation	0.92
VGG19	Original	0.93
VGG19	Inversion	0.88
VGG19	Augmentation	0.93

Table 4: Summary of the experimental results comparing the classification accuracy of VGG16 and VGG19 convolutional neural network architectures on the fingerprint recognition task. The table presents accuracy metrics for three different input processing methods: training on the original fingerprint images, the Inversion Method which involves splitting and independently inverting image halves, and the Multi-Augmentation Method that generates multiple augmented samples through realistic transformations. The results highlight that both VGG16 and VGG19 achieve the highest accuracy when trained on the original and augmented datasets, whereas the Inversion Method yields lower performance, likely due to distortions affecting fingerprint morphology. This comparison underscores the effectiveness of augmentation techniques in enhancing model generalization under varying acquisition conditions.

Based on the experimental findings summarized above, several important conclusions can be drawn. Both VGG16 and VGG19 demonstrate strong learning capabilities for fingerprint features, achieving high accuracy around 93% when trained on the original dataset. Although the Inversion Method was intended to enrich feature diversity, it proves ineffective due to the structural distortions it introduces, which impair the model's ability to capture stable morphological patterns. In contrast, the Multi-Augmentation Method emerges as a promising strategy for improving model performance by simulating realistic fingerprint variations while preserving essential structural characteristics. This method facilitates more effective feature learning and enhances generalization across diverse real-world conditions.
Besides the method discussed earlier, this report also looks into how well the MobileNet and EfficientNet-B0 models perform when used for fingerprint matching. These models are improved by adding different attention mechanisms. The report explains what these models are, how the attention methods work, and how they affect the accuracy of fingerprint recognition. All conclusions are supported by experimental results. **MobileNet** is a light and fast convolutional neural network that is useful when computing power is limited, like on mobile devices. It uses a special type of convolution called depthwise separable convolution. This method splits a normal convolution into two simpler steps—depthwise and pointwise convolutions—which lowers the number of calculations needed while still keeping good accuracy. **EfficientNet-B0**

is a stronger and more modern model. It works by carefully balancing three things in the network: depth (how many layers), width (how wide each layer is), and input resolution (image size). By adjusting these factors together, EfficientNet-B0 can give better accuracy with fewer parameters compared to older models. This makes it a good choice for more complex tasks like fingerprint recognition. To help the models focus on the most important parts of the fingerprint images, attention mechanisms are added. These mechanisms help the models pay attention to useful features during learning. The **Squeeze-and-Excitation (SE)** attention mechanism uses average pooling and two dense layers to decide which channels (features) are more important, so it can give more focus to them. **Self-Attention** looks at the relationship between all parts of an image. It allows the model to learn from areas that are far apart but still important to each other. This is done using special layers like convolution and softmax activation. **Convolutional Block Attention Module (CBAM)** combines two types of attention: one for channels and one for spatial location. This helps the model learn better feature maps in both directions. **Dual Attention** combines position attention and channel attention. It tries to give the model more power to focus on both where and what to look at in the image. We tested how well MobileNet and EfficientNet-B0 work with each of these attention mechanisms. The results show that different attention types affect performance in different ways. For MobileNet, the best performance comes from adding Self-Attention, which gives an accuracy of 0.8148. This shows that being able to look at long-range features is helpful for this light model. However, when using Dual Attention, the accuracy drops to 0.2901. This suggests that MobileNet cannot handle the extra complexity well. For EfficientNet-B0, the highest accuracy is 0.9444 when using SE attention. This shows that the model benefits from learning which channels are most useful. CBAM also works very well with EfficientNet-B0. On the other hand, Self-Attention gives lower accuracy (0.6975), which may be due to the model overfitting or not being tuned well for that type of attention.

Model	**Accuracy**
MobileNet + CBAM	0.3580
MobileNet + Dual Attention	0.2901
MobileNet + Self-Attention	0.8148
MobileNet + Squeeze-and-Excitation	0.4383
EfficientNet-B0 + CBAM	0.9383
EfficientNet-B0 + Dual Attention	0.8704
EfficientNet-B0 + Self-Attention	0.6975
EfficientNet-B0 + Squeeze-and-Excitation	0.9444

Table 5: Accuracy of MobileNet and EfficientNet-B0 models with various attention mechanisms on fingerprint matching. EfficientNet-B0 shows superior performance, especially with SE and CBAM, while MobileNet performs best with Self-Attention.

The results show that EfficientNet-B0 works better than MobileNet in almost all cases. When using SE or CBAM, EfficientNet-B0 gives very high accuracy. This means it can learn useful fingerprint features very well. MobileNet is faster and uses less memory, and works best with Self-Attention. But it does not perform well with more complex attention types like Dual Attention. These results suggest that for tasks where high accuracy is important, EfficientNet-B0 with SE or CBAM is a good choice. But if you need a light model for mobile or small devices, MobileNet with Self-Attention is a good option. Future studies can look at combining attention types or improving tuning to make the results even better.

7 UI/UX and Demo

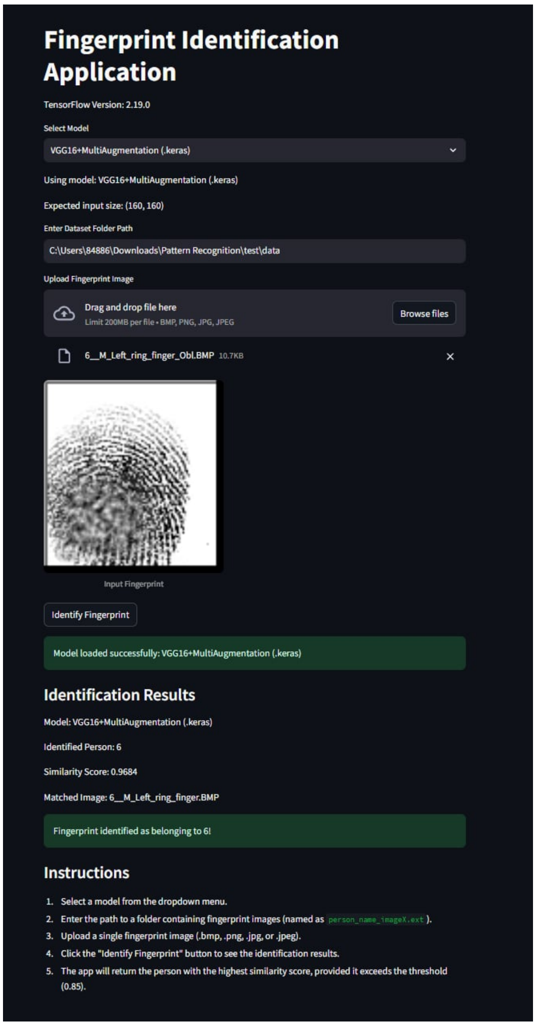

Figure 5: Interface of the Fingerprint Identification Application

Figure 5 shows the interface of the Fingerprint Identification Application, which is designed for ease of use, allowing users to perform fingerprint recognition tasks intuitively and accurately. The application is powered by TensorFlow version 2.19.0 and provides a user-friendly interface where users can select a training model in .keras format through a dropdown menu. Available models include VGG16 combined with data augmentation techniques (VGG16+MultiAugmentation). After selecting a model, the system displays key information about the selected model, including the required input image size (160×160). Users can then specify the path to the folder containing the original image dataset for comparison. The fingerprint image to be recognized can be uploaded either by dragging and dropping or by browsing for the file. The system supports common image formats such as BMP, PNG, JPG, and JPEG. Once an image is uploaded, the system shows a preview of the image and enables the ”Identify Fingerprint” button to initiate the recognition process. The recognition result includes the following details: the selected model, the ID number of the identified person, the similarity score between the input image and images in the dataset, and the file name of the closest matching image. If the similarity score exceeds the threshold of 0.85, the system will confirm the identity with a clear notification. Additionally, the interface provides step-by-step instructions to ensure that even users with limited technical knowledge can use the system effectively and accurately.

8 Conclusion and Future work

8.1 Conclusion

In this project, we developed and presented an end-to-end fingerprint recognition system that integrates both classical methodologies and cutting-edge deep learning techniques, aiming to advance the state of biometric identification. The system leverages the representational power of convolutional neural networks (CNNs), including prominent architectures such as VGG16 and VGG19, which we employed as deep feature extractors to capture intricate fingerprint patterns. To address the common challenge of limited dataset size in biometric applications, we introduced a novel inversion-based data augmentation strategy. This preprocessing step not only increased the diversity of training samples but also enhanced the robustness of the models by exposing them to a wider range of input variations. Our findings revealed that even relatively simple preprocessing techniques, when carefully designed and systematically applied, can substantially improve the discriminative capacity of deep neural networks, particularly in tasks involving high intra-class variability like fingerprint recognition. To further optimize model performance without incurring significant computational overhead, we incorporated lightweight CNN architectures integrated with various attention mechanisms. Specifically, we explored the use of Squeeze-and-Excitation Networks (SENet), Convolutional Block Attention Module (CBAM), Self-Attention, and Dual Attention mechanisms. These attention modules allowed the models to dynamically recalibrate feature maps by focusing on the most informative spatial regions and feature channels, thereby enhancing both efficiency and accuracy. Through extensive experimentation and rigorous performance evaluation, we demonstrated that combining lightweight models with attention strategies yields compelling results. Notably, our experiments indicated that the pairing of EfficientNet-B0 with the Dual Attention mechanism delivered the highest fingerprint matching accuracy across all tested configurations. This result underscores the effectiveness of jointly modeling spatial and channel-wise dependencies, which is particularly beneficial in complex pattern recognition scenarios like biometrics. Moreover, the superior performance of this combination highlights its suitability for deployment in real-time applications and on resource-constrained devices, such as mobile platforms or embedded systems, where computational efficiency is paramount. Beyond the algorithmic and architectural contributions, we also placed significant emphasis on designing an intuitive and user-friendly graphical user interface (GUI). The interface supports seamless interaction and facilitates easy fingerprint enrollment, matching, and result interpretation, making the system accessible even to non-expert users. This UI/UX design aligns with the goal of creating practical, deployable biometric systems that can be readily adopted in real-world settings, such as border control, secure authentication, and forensic investigations. In conclusion, the integration of advanced data augmentation methods, attention-enhanced lightweight neural networks, and a thoughtfully designed user interface culminated in a robust and scalable fingerprint recognition system.

The work not only illustrates the practical benefits of combining traditional biometric approaches with modern deep learning innovations but also provides a promising blueprint for future research and development in efficient, real-time biometric identification systems.

8.2 Future work

Despite the promising results achieved in this project, there are several critical avenues for further exploration and improvement that could enhance the overall effectiveness and applicability of the fingerprint recognition system. One of the primary limitations of our current approach is the dataset used for model training and evaluation. Although it is sufficient for the purpose of prototyping, the dataset's size and diversity remain constrained, which impacts the generalizability of the model across various real-world conditions. To overcome this, future work could involve expanding the dataset to include a broader range of subjects, varying image qualities, and diverse environmental conditions such as lighting and background noise. This expansion would not only improve the model's robustness but also allow it to perform more reliably in diverse, uncontrolled settings. In addition to dataset expansion, advanced data augmentation techniques offer significant potential to further improve model performance. Methods such as elastic distortions, which simulate variations in finger positioning and skin elasticity, partial occlusions to mimic real-world scenarios where fingerprints may be partially obstructed, and synthetic fingerprint generation using generative models, could all play a crucial role in enhancing the model's resilience. By training the system to handle these variations, we can build a model that is more adaptable and less prone to overfitting, thus improving its real-world applicability. Another promising direction lies in the exploration of multi-modal biometrics. While fingerprint recognition is a widely used and effective method, combining it with other biometric modalities, such as facial recognition or iris scanning, could significantly enhance the security and accuracy of the system. This multi-modal approach would provide complementary sources of verification, making the system more robust against spoofing attacks and reducing the likelihood of false negatives, which is especially important in high-stakes applications like secure access or criminal investigations. On the algorithmic front, several improvements can be made to optimize the performance and efficiency of the system. One avenue worth exploring is the use of hashing-based indexing for faster and more scalable fingerprint matching. This could greatly reduce the computational cost of searching large fingerprint databases, making the system more efficient. Additionally, real-time inference acceleration is a crucial consideration for deploying the system in real-world scenarios, and techniques such as model quantization, which reduces the model size and computational requirements, could be employed to achieve faster inference times. Deploying the model on edge devices through frameworks like TensorFlow Lite would further enable on-device processing, reducing dependency on cloud-based systems and enhancing privacy by ensuring that sensitive biometric data does not need to leave the device. Furthermore, the growing interest in explainable AI (XAI) presents a valuable opportunity to enhance the interpretability and transparency of our model. By employing techniques like saliency maps or attention visualization, we can gain deeper insights into the decision-making process of the network. This would not only increase user trust in the system but also provide valuable feedback for refining model behavior, particularly in security-critical applications where understanding why a decision was made is as important as the decision itself. Finally, adapting the fingerprint recognition system for mobile platforms and embedded devices is a key objective moving forward. This would allow for the development of privacy-preserving, offline fingerprint recognition solutions, which are especially relevant given the increasing concerns about data privacy and security in the digital age. By ensuring that the system can operate on devices with limited computational resources, while still adhering to ethical and security standards, we aim to create a flexible and scalable solution suitable for a wide range of real-world applications. In conclusion, while the results of this project provide a strong foundation, the areas identified for future work offer exciting opportunities to enhance the system's robustness, efficiency, and applicability, paving the way for more secure, scalable, and user-friendly biometric recognition systems in the future.

References

[1] Enhanced fingerprint pattern classification: Integrating attention modules with lightweight deep learning models. Retrieved April 11, 2025.

[2] Fingerprint recognition using convolution neural network with inversion and augmented techniques. Retrieved April 11, 2025.

[3] Amjad Ali, X. Jiang, and Nasir Saleem. Glcm-based fingerprint recognition algorithm. *Beijing University of Posts and Telecommunications*, pages 1–5, 2011.

[4] A. Alzu'bi, Z. Alqadi, and E. Alshdaifat. A novel deep lenet-5 convolutional neural network model for image recognition. *International Journal of Electrical and Computer Engineering (IJECE)*, 12(5):5175–5183, 2022.

[5] David R. Ashbaugh. *Quantitative-Qualitative Friction Ridge Analysis: An Introduction to Basic and Advanced Ridgeology*. CRC Press, Boca Raton, 1999.

[6] Francesco Bianconi and A. Fernández. Rotation invariant co-occurrence features based on digital circles and discrete fourier transform. *Pattern Recognition Letters*, pages 1–9, 2014.

[7] Harold Cummins and Charles Midlo. *Finger Prints, Palms and Soles: An Introduction to Dermatoglyphics*. Dover Publications, New York, 1961.

[8] T.N. Do, P. Lenca, S. Lallich, and N.K. Pham. Classifying very-high-dimensional data with random forests of oblique decision trees. In *Advances in Knowledge Discovery and Management*, pages 39–55. Springer, Berlin, Heidelberg, 2010.

[9] Encyclopaedia Britannica. Fingerprint, n.d. Accessed: 2025-05-11.

[10] Federal Bureau of Investigation. Fingerprint recognition. Technical report, Biometric Center of Excellence, 2010. Accessed: 2025-05-11.

[11] Anil K. Jain, Jianjiang Feng, and Karthik Nandakumar. Fingerprint matching. *IEEE Computer*, pages 1–9, 2010.

[12] Anil K. Jain, Patrick Flynn, and Arun A. Ross. *Handbook of Biometrics*. Springer, New York, NY, 2007.

[13] F. Li and P. Perona. A bayesian hierarchical model for learning natural scene categories. In *IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR 2005)*, pages 524–531, 2005.

[14] L. Liu, T. Tan, and Y. Zhan. Based on svm automatic measures of fingerprint image quality. In *Proceedings of the 2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, pages 575–578, Wuhan, China, 2008.

[15] D. Lowe. Object recognition from local scale invariant features. In *Proceedings of the 7th International Conference on Computer Vision*, pages 1150–1157, 1999.

[16] D. Lowe. Distinctive image features from scale invariant keypoints. *Int. J. Comput. Vis.*, 60:91–110, 2004.

[17] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain. Fvc2000: Fingerprint verification competition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24(3):402–412, March 2002.

[18] Davide Maltoni, Dario Maio, Anil K. Jain, and Salil Prabhakar. *Handbook of Fingerprint Recognition*. Springer, London, 2 edition, 2009.

[19] H.M. N. N. Ain Alias. Fingerprint classification using support vector machine. In *Fifth ICT International Student Project Conference (ICT-ISPC)*, 2016.

[20] D.-L. Nguyen, K. Cao, and A. K. Jain. Robust minutiae extractor: Integrating deep networks and fingerprint domain knowledge. In *Proceedings of the 2018 International Conference on Biometrics (ICB)*, pages 9–16, Gold Coast, QLD, Australia, 2018.

[21] Karen Simonyan and Andrew Zisserman. Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556*, 2014.

[22] J. Sivic and A. Zisserman. Video google: a text retrieval approach to object matching in videos. In *9th IEEE International Conference on Computer Vision (ICCV 2003)*, pages 1470–1477, 2003.

[23] Y. Tang, F. Gao, J. Feng, and Y. Liu. Fingernet: An unified deep network for fingerprint minutiae extraction. In *2017 IEEE International Joint Conference on Biometrics (IJCB)*, pages 108–116, Denver, CO, USA, 2017. IEEE.

[24] Vladimir N. Vapnik. *The nature of statistical learning theory*. SpringerVerlag, 1995.

[25] S. Zhao, X. Hao, and X. Li. Segmentation of fingerprint images using support vector machines. In *Proceedings of the 2008 Second International Symposium on Intelligent Information Technology Application*, pages 423–427, Shanghai, China, 2008.