IMPACT OF IMAGE COMPRESSION AND FORMAT CONVERSION ON FINGERPRINT RECOGNITION: EXPLORING SECURITY AND PERFORMANCE TRADE-OFFS

by

KARTHIK ASHOK HONGUNTIKAR

Thesis submitted to University of Plymouth in partial
fulfilment of the requirements for the degree of

MSc Advanced Engineering Design

University of Plymouth
Faculty of Science & Engineering

In collaboration with
CERC Field Research Facility, Duck, NC, USA
(where appropriate)

June 2025

Copyright statement

Abstract

Biometric systems, particularly fingerprint recognition, are essential in modern identity verification, offering high accuracy and security. However, image quality degradation from compression significantly impacts system performance. This study examines the effects of compression formats (JPEG, PNG, BMP, WebP) and levels (20%, 60%) on fingerprint recognition using high- and low-quality datasets. Key performance metrics, including False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER), were analysed to assess recognition reliability.

The results show that high-quality datasets-maintained accuracy under 20% compression, with minimal increases in FAR and FRR, while 60% compression caused performance degradation by over 30% for low-quality datasets. Lossless formats like PNG preserved minutiae integrity but required higher storage, whereas lossy formats like JPEG introduced artifacts that reduced recognition accuracy. Emerging formats like WebP demonstrated potential for balancing storage efficiency and quality, offering improved performance over JPEG at moderate compression levels.

This research provides actionable insights into designing robust fingerprint recognition systems, identifying critical compression thresholds, and proposing hybrid compression strategies. The findings have practical implications for diverse applications, including mobile authentication and large-scale biometric databases, highlighting the need for tailored solutions to balance storage efficiency, usability, and security.

Contents

List of Tables

List of Figures

Acknowledgements

I would like to express my heartfelt gratitude to my supervisor, Professor Ji-Jian Chin, whose guidance, support, and encouragement have been invaluable throughout this research journey. His expertise and insightful feedback have been instrumental in shaping the direction and development of my thesis on "Impact of Image Compression and Format Conversion on Fingerprint Recognition: Exploring Security and Performance Trade-offs." I deeply appreciate his patience and commitment, which have motivated me to reach higher levels of achievement.

I am also grateful to the School of Engineering, Computing, and Mathematics at the University of Plymouth for providing the resources and facilities necessary to conduct this research. The supportive academic environment fostered within the Faculty of Science and Engineering was essential for the successful completion of my work.

Special thanks to my colleagues and peers, whose discussions and collaboration contributed greatly to the research process. Their input has not only enhanced the depth of my research but also enriched my overall learning experience.

Lastly, I am deeply thankful to my family and friends, whose unwavering support and encouragement provided me with the strength and determination to persevere. Their belief in me has been a constant source of motivation throughout this journey.

1 Introduction

1.1 Background and Context

Biometric technology has revolutionised identity verification by leveraging unique physical and behavioural attributes such as fingerprints, facial features, iris patterns, and voice. Unlike traditional methods like passwords and physical tokens, biometrics provides greater accuracy and simplicity, making it indispensable in a digitally driven era. As digital transformation accelerates, secure and efficient authentication solutions are critical for protecting personal and institutional data.

Fingerprint recognition is one of the most widely adopted biometric technologies due to its reliability and ease of use. It powers applications ranging from personal device authentication and national identity programs to cost-effective systems like smart locks and wearable gadgets. However, challenges persist in ensuring the robustness of these systems under real-world conditions, particularly when resource constraints necessitate data compression.

1.2 Problem Statement

Fingerprint-based biometric systems rely heavily on image quality to ensure accurate recognition. To optimise storage and transmission efficiency, fingerprint images often undergo preprocessing steps such as compression. While compression is critical for practical deployment especially in resource-constrained environments like mobile and IoT systems it introduces artifacts that distort ridge structures and minutiae details. These distortions not only degrade recognition accuracy but also increase error rates, creating vulnerabilities that attackers can exploit.

While traditional image formats like JPEG and PNG have been studied extensively, emerging formats such as WebP remain underexplored in the context of biometric systems. Additionally, low-cost applications like IoT devices often store lower-quality data, exacerbating these challenges. There is a clear need to investigate how compression impacts performance metrics and to develop strategies for balancing security, storage, and usability in fingerprint recognition systems.

1.3 Objectives of the Study

This study addresses the challenges associated with image compression in fingerprint recognition systems. The key objectives are:

1. To evaluate the impact of image formats (e.g., JPEG, PNG, BMP, WebP) and compression levels (20%, 60%) on biometric performance metrics such as False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER).

2. To compare the resilience of high-quality and low-quality fingerprint datasets to compression-induced artifacts and minutiae reduction.

3. To identify optimal compression thresholds that maintain recognition reliability while improving storage efficiency.

4. To propose practical recommendations for deploying fingerprint recognition systems across diverse real-world applications, including cost-sensitive IoT and mobile environments.

1.4 Research Questions

This research is guided by the following questions:

1. How do different image formats and compression levels affect the accuracy and reliability of fingerprint recognition systems?

2. What are the critical thresholds for compression levels beyond which recognition performance deteriorates significantly?

3. How do high-quality and low-quality fingerprint datasets differ in their sensitivity to compression and minutiae reduction?

4. What practical measures can be implemented to optimise fingerprint recognition performance while minimising storage and computational costs?

1.5 Significance of the Study

This research contributes valuable insights to the design and optimisation of biometric systems:

1. For System Designers and Developers: It highlights trade-offs between compression efficiency and recognition accuracy, enabling informed decisions for developing cost-effective systems, especially in IoT and mobile applications.

2. For End-Users: It ensures reliable performance in low-cost devices, enhancing user trust and reducing risks in consumer-grade systems like smart locks and mobile authentication.

3. For Policymakers and Regulatory Bodies: It provides evidence-based recommendations for data storage and transmission policies to ensure security and usability in biometric systems.

1.6 Methodology Overview

To achieve these objectives, this study adopts an experimental approach:

1. Image Preprocessing: Fingerprint images were converted into different formats (JPEG, PNG, BMP, WebP) and compressed at varying levels (20%, 60%).

2. Performance Evaluation: Recognition accuracy was assessed using standard metrics, including FAR, FRR, and EER.

3. Threshold Analysis: Compression thresholds causing significant performance degradation were identified.

4. Trade-Off Analysis: Relationships between storage efficiency, recognition reliability, and system security were examined to develop actionable recommendations.

1.7 Challenges and Limitations

This research acknowledges several limitations:

1. Dataset Variability: Differences in fingerprint dataset quality may impact generalisability.

2. Compression Artifacts: The extent to which artifacts affect minutiae extraction may vary across algorithms.

3. Real-World Applicability: Environmental factors, such as user behaviour and noise, are difficult to replicate in experimental settings.

1.8 Conclusion

In a world increasingly reliant on digital security, fingerprint recognition systems must balance storage efficiency and recognition reliability. This study aims to address these challenges by analysing the impact of image compression on system performance. Through rigorous experimentation, the findings will provide practical insights to improve biometric system reliability, security, and usability across diverse applications.

2 Literature Review

2.1 Biometric Systems Overview

Biometric recognition represents a significant advancement in authentication technology, utilising sophisticated algorithms to analyse and authenticate individuals based on their unique physical or behavioural characteristics. These characteristics can be broadly categorised into two main groups: physiological features, which include fingerprints, facial features, iris patterns, hand geometry, and palm prints; and behavioural traits, encompassing voice patterns, typing rhythm, gait analysis, and signature dynamics. The evolution of these systems marks a paradigm shift from traditional authentication methods, offering enhanced security and user convenience across various sectors.

The implementation of biometric systems spans multiple domains, including government services, law enforcement, healthcare facilities, financial institutions, and corporate security. Their growing adoption is driven by several key advantages: they eliminate the need to remember complex passwords, reduce the risk of credential sharing or theft, and provide an audit trail of authentication attempts. In healthcare settings, biometric systems prevent medical identity theft and ensure accurate patient identification, while in financial services, they enhance transaction security and comply with Know Your Customer (KYC) requirements.

Fingerprint recognition has emerged as the predominant biometric modality due to several compelling factors. The uniqueness of fingerprints is well-established through extensive research, with studies demonstrating that even identical twins possess distinct fingerprint patterns. This inherent uniqueness, combined with the relative stability of fingerprint patterns throughout an individual's lifetime, makes them particularly suitable for long-term identification purposes. The technology's maturity, demonstrated through decades of successful implementation in various contexts, further reinforces its position as a preferred biometric solution.

The fundamentals of fingerprint recognition rely on the analysis of specific features within the ridge patterns. These features are categorised into three levels: Level 1 features include general ridge flow patterns and singular points; Level 2 features comprise minutiae points such as ridge endings and bifurcations; and Level 3 features encompass fine details like ridge contours and sweat pore locations. Modern systems primarily utilise Level 2 features for matching, as they offer an optimal balance between distinctiveness and computational efficiency.

Minutiae-based matching algorithms have become the industry standard, employing sophisticated techniques to compare the spatial relationships and orientations of minutiae points between samples. These algorithms typically follow a multi-stage process: image acquisition, preprocessing, feature extraction, and matching. Advanced systems incorporate adaptive preprocessing techniques to enhance image quality and robust matching algorithms that can accommodate various types of finger placement and pressure variations. (Sekhar Rajendran)

The challenges facing fingerprint recognition systems are multifaceted and require careful consideration in system design. Environmental factors such as temperature and humidity can affect the quality of captured images, while physical conditions like cuts, scars, or worn fingerprints can impair recognition accuracy. Sensor-related issues, including resolution limitations, noise, and distortion, further complicate the recognition process. These challenges are particularly pronounced in scenarios involving partial fingerprints, whether due to limited sensor size or forensic circumstances where only fragmentary prints are available.

India's Aadhaar system stands as a landmark case study in large-scale biometric deployment, managing the biometric data of over 1.3 billion individuals. As the world's largest biometric implementation, Aadhaar employs multiple modalities, including fingerprints, iris scans, and facial recognition, to ensure robust identification. However, its deployment has uncovered several challenges. These include the need for highquality image capture devices that can operate reliably in diverse environmental conditions, the importance of efficient data compression techniques for managing massive databases, and the difficulty of maintaining consistent performance across a demographically diverse population. Additionally, balancing system accessibility with stringent security requirements has proven to be a critical yet complex task.[1]
The experiences of the Aadhaar system have provided valuable lessons for other large-scale biometric implementations. Key takeaways include the necessity of robust quality assessment algorithms to ensure captured images meet minimum standards, efficient database management techniques to handle vast volumes of biometric data, and comprehensive testing protocols that account for diverse user populations. Furthermore, regular system audits and performance monitoring are essential for maintaining reliability, and clear policies on data privacy and security are crucial to building public trust. These insights underscore the importance of thoughtful planning and adaptive strategies in managing large-scale biometric systems. (Veena N, 2022)
Beyond fingerprint recognition, the biometric landscape continues to evolve with emerging modalities and multimodal approaches. Facial recognition has gained prominence, particularly in surveillance and mobile authentication applications, while

iris recognition offers high accuracy in controlled environments. Behavioural biometrics, such as gait analysis and keystroke dynamics, are emerging as promising supplementary authentication methods, especially in continuous authentication scenarios.

The integration of artificial intelligence and machine learning has significantly enhanced biometric system capabilities. Deep learning algorithms have improved feature extraction accuracy, while neural networks have enhanced matching performance and reduced false acceptance rates. These advances have also enabled better handling of challenging scenarios, such as aging effects, environmental variations, and partial prints.

2.2 Key Performance Metrics: FAR, FRR, and EER

The evaluation of fingerprint recognition systems relies on standardised performance metrics that balance security and usability, providing a universal framework for benchmarking systems, comparing algorithms, and determining their suitability for various applications. Among these metrics, the False Acceptance Rate (FAR) measures the likelihood of a biometric system erroneously granting access to an unauthorised individual, making it a critical indicator in security-sensitive contexts. In financial systems, even a FAR as low as 0.01% can lead to millions of dollars in unauthorised transactions, prompting institutions to adopt stringent thresholds and supplementary security measures. In military installations, where security demands are exceptionally high, FAR values below 0.001% are required, often complemented by multi-factor authentication for added protection. Commercial applications, such as retail and office environments, prioritise a balance between security and operational efficiency, with acceptable FAR values of around 0.1%. Healthcare systems typically adopt intermediate FAR values, such as 0.05%, to protect patient privacy while ensuring quick access to critical services like electronic health records. By tailoring FAR thresholds to the specific requirements of each application, organisations can achieve an optimal balance between security and usability, making FAR a cornerstone metric in biometric system evaluation. [2]

Case studies underscore the pivotal role of False Acceptance Rate (FAR) in the deployment of biometric systems. A 2022 study on biometric access control in banks revealed that systems with FAR values exceeding 0.05% were significantly more vulnerable to fraud, requiring additional manual oversight to mitigate risks. Conversely, a pilot project at a secure government facility demonstrated the potential for advanced technologies to achieve exceptional security, with FAR values as low as 0.0001%. This was accomplished through the integration of advanced matching algorithms and high-resolution sensors, setting a new benchmark for secure access in high-stakes environments. These examples highlight how tailoring FAR thresholds and employing cutting-edge technologies can significantly enhance the reliability and security of biometric systems across different applications.

False Rejection Rate (FRR) measures the percentage of legitimate users mistakenly denied access by a biometric system, significantly impacting usability, user satisfaction, and operational efficiency. High FRR values can have far-reaching consequences that vary by application. In workplaces where biometric systems are used for time tracking, elevated FRR can cause delays and disputes, reducing overall productivity. In customer-facing applications, such as retail or customer service, false rejections can frustrate users, damaging their perception of the system and potentially harming the business's reputation. Healthcare settings are particularly sensitive, as delayed access due to false rejections can jeopardise patient outcomes by hindering timely interventions. Additionally, high FRR values increase the burden on system administrators, who must manually verify identities or implement alternative access procedures, adding to operational overhead. [2]

FRR is also influenced by user demographics and environmental conditions. Elderly individuals or manual labourers often have worn or scarred fingerprints, making them more susceptible to rejection. Environmental factors like dirt, moisture, or temperature fluctuations can further degrade fingerprint quality, amplifying the risk of false rejections. A 2021 study of biometric time tracking systems in manufacturing plants demonstrated this impact; an FRR of 2% resulted in a cumulative loss of 1,500 productive hours annually due to delays and manual corrections. These findings highlight the need to optimise system parameters and employ adaptive algorithms to minimise FRR, ensuring both security and usability across diverse environments.

Equal Error Rate (EER) is a pivotal metric for evaluating biometric system performance, representing the point where the False Acceptance Rate (FAR) and False Rejection Rate (FRR) are equal. EER offers a balanced view of system performance, making it invaluable for benchmarking, setting performance baselines, and assessing improvements across software iterations. It is particularly effective in comparing different biometric technologies, such as fingerprint, facial recognition, or iris scanning, by providing an objective metric for evaluation.

EER has several practical applications. It facilitates system comparisons, allowing for an unbiased evaluation of competing biometric systems. For new biometric solutions or algorithm updates, EER serves as a performance baseline, validating improvements and ensuring alignment with required standards. Additionally, EER is instrumental in threshold optimisation, identifying the ideal operating point where the trade-off between security and usability is balanced. [2]

Research underscores the importance of EER in determining system suitability for specific applications. High-performing systems typically achieve EER values below 1%, making them suitable for critical environments. For example, a 2023 evaluation of national ID systems found that systems with EER values under 0.5% consistently outperformed those with higher EERs, excelling in both security and user satisfaction. Conversely, a study of low-cost IoT biometric access systems revealed EER values exceeding 2%, deeming them unsuitable for applications requiring stringent security.
These findings highlight EER's role as a comprehensive and practical metric for evaluating and optimizing biometric systems.

The performance metrics of biometric systems—False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER)—are significantly influenced by image quality and processing parameters. High-resolution images with sharp contrast are critical for accurate minutiae extraction, with studies showing that increasing resolution from 300 DPI to 600 DPI can improve recognition accuracy by up to 25%. Noise and artifacts, often introduced during image capture or through compression, can degrade system reliability, as compression artifacts in lossy formats like JPEG distort ridge structures and elevate EER values. Poor sensor maintenance further impacts performance, as suboptimal image capture reduces system accuracy, highlighting the importance of regular sensor cleaning and calibration. Environmental conditions such as temperature, humidity, and lighting variations during fingerprint acquisition introduce inconsistencies that affect matching accuracy, especially in uncontrolled settings. Additionally, user interaction plays a key role; incorrect finger placement, excessive pressure, or wet/dry hands can lower image quality, negatively influencing performance metrics. By addressing these factors, biometric systems can achieve greater reliability and accuracy, ensuring they meet the diverse demands of their applications. [2]

Processing parameters play a critical role in the performance of biometric systems, influencing the accuracy of False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER). Advanced feature extraction algorithms that adapt to varying image qualities enhance system performance, particularly in challenging environments. Matching thresholds must be carefully adjusted to balance FAR and FRR; for instance, higher thresholds may reduce FAR but at the cost of increased FRR. Image enhancement techniques such as noise reduction, histogram equalisation, and minutiae reconstruction help mitigate the impact of poor-quality images, improving overall reliability. Template generation plays a pivotal role in maintaining consistent and high-quality templates for reliable matching across sessions, while efficient database management systems ensure quick and accurate retrieval, minimising false matches in large-scale applications. [2]

The impact of image quality on FAR, FRR, and EER has been extensively documented. Research highlights a strong correlation between resolution and recognition accuracy, with low-resolution images (e.g., below 300 DPI) significantly increasing both FAR and FRR due to lost minutiae detail. Sensitivity to noise is another critical factor; studies reveal that adding just 5% noise to fingerprint images can raise EER by over 20%, underscoring the importance of robust noise reduction techniques. Compression effects are also notable, as lossy formats like JPEG introduce artifacts that obscure ridge structures, with compression ratios exceeding 10:1 resulting in an average EER increase of 15%. Additionally, environmental conditions such as excessive dryness or moisture can degrade fingerprint capture, amplifying FRR. Systems deployed in outdoor environments often require specialised sensors to mitigate these challenges. By addressing these factors, biometric systems can achieve greater accuracy, scalability, and reliability across diverse operational scenarios.

2.3 Image Compression and Biometric Performance

The role of image compression in biometric systems extends beyond simple storage optimization, directly influencing system performance, operational costs, user experience, and the security of biometric data. As biometric systems scale, particularly in applications involving massive databases or real-time processing—such as national ID systems or mobile authentication—efficient storage and transmission management without compromising performance becomes critical. Lossy compression techniques, widely used for reducing file sizes, discard data deemed less critical to human perception, but in biometric contexts, this often includes essential ridge structures and minutiae details required for fingerprint recognition. Among the prevalent formats, JPEG and WebP stand out for their unique features and implications in biometric systems. [3]

JPEG, a widely used lossy compression format due to its compatibility and simplicity, has significant limitations in biometric applications. At quality factors below 70, artifacts such as blurred ridge structures emerge, hampering minutiae extraction. Its blockbased encoding introduces artificial patterns at high compression levels, leading to false minutiae detection, while colour subsampling can degrade ridge contrast even in grayscale systems. Progressive encoding, though useful for faster loading in web contexts, introduces layering artifacts that interfere with biometric matching processes.

In contrast, WebP, developed by Google, addresses many of JPEG's limitations with advanced compression capabilities. It preserves edge details and ridge structure fidelity, essential for accurate minutiae detection while minimising block artifacts that often degrade recognition reliability. WebP achieves up to 30% smaller file sizes compared to JPEG without significant quality loss, making it particularly suitable for large-scale biometric systems. It also retains more information in high-frequency regions, such as ridges and minutiae, which are crucial for fingerprint analysis. A 2023 study highlighted WebP's potential, demonstrating that it maintained 95% recognition accuracy at compression ratios 20% higher than JPEG, proving its utility in storageconstrained systems. These advancements make WebP a promising alternative to traditional lossy compression formats in biometric applications. [3]

Lossless compression formats, such as PNG and BMP, play a crucial role in biometric systems by ensuring that no image data is lost during compression, thus preserving the integrity of fingerprint minutiae. These formats are essential for guaranteeing maximum accuracy in applications where minutiae details are critical, but they come with significant trade-offs in terms of storage and processing requirements.

PNG is a highly efficient lossless format widely used in biometric systems where minutiae integrity is paramount. It offers several advantages, including no quality degradation, as it preserves all ridge details to ensure that minutiae points remain unaffected. This makes PNG ideal for archival purposes, particularly in high-security systems or forensic databases. However, the file size of PNG images can be three to five times larger than lossy formats, significantly increasing storage costs for largescale deployments. [3]

BMP, a raw and uncompressed format, is used in scenarios where absolute image fidelity is required, such as forensic applications or laboratory testing. BMP ensures that every detail of the fingerprint image is retained, making it invaluable in environments demanding the highest accuracy. However, its practicality is limited in large-scale deployments due to high storage demands, necessitating extensive infrastructure to accommodate large files. Additionally, the bandwidth requirements for transmitting BMP files are substantial, hindering their use in real-time processing scenarios.

While lossless formats like PNG and BMP are indispensable for applications where recognition accuracy is critical, their scalability is often constrained by the high costs associated with storage and processing. For large-scale or real-time biometric systems, these limitations necessitate careful consideration and optimization of resources.

Emerging compression technologies are introducing advanced formats and techniques that achieve a better balance between compression efficiency and biometric performance, addressing the limitations of traditional formats. Two notable innovations in this space are AVIF and JPEG XL, both of which hold significant promise for biometric applications. [4]

AVIF, developed from the AV1 video codec, marks a substantial advancement in image compression technology. It delivers superior quality retention, achieving higher compression ratios than JPEG and WebP while preserving ridge details essential for biometric accuracy. Its enhanced support for both colour and grayscale images makes it adaptable to a wide range of biometric systems. Moreover, its efficient storage capabilities are increasingly attractive for IoT-enabled biometric devices, where resource constraints are a critical consideration.

JPEG XL, a modern evolution of the traditional JPEG format, combines flexibility with efficiency. It supports dual modes of compression, allowing systems to toggle between lossy and lossless formats depending on application needs. Improved efficiency enables it to outperform both JPEG and PNG in compression ratios, making it ideal for scenarios requiring optimized storage and performance. Additionally, backward compatibility with existing JPEG infrastructure simplifies its adoption, enabling a smooth transition for legacy systems.

These emerging formats offer promising solutions for biometric systems, providing enhanced compression efficiency while maintaining the high-quality image fidelity required for accurate recognition. As these technologies gain wider adoption, they have the potential to redefine the standards for image compression in biometric applications. [4]

Neural Network-Based Compression is a groundbreaking approach in biometric systems, leveraging AI-driven models to enhance compression strategies while preserving critical biometric features like minutiae and ridges. These models offer custom optimization, tailoring compression to specific modalities such as fingerprints or irises. Their adaptability allows dynamic adjustment of compression parameters based on environmental factors or image quality, ensuring consistent performance across diverse conditions.

Hybrid Compression Approaches combine lossy and lossless techniques to balance storage efficiency and recognition accuracy. For example, region-specific compression applies lossless compression to high-priority areas containing minutiae points while compressing peripheral regions with lossy methods to save space. Preprocessing-integrated compression employs AI algorithms to enhance image quality during compression, mitigating the drawbacks of lossy techniques and improving overall system reliability. [4]

The selection of compression formats and techniques significantly influences the performance of biometric systems. Recognition accuracy is directly affected, with lossless formats like PNG consistently outperforming lossy formats such as JPEG. A 2024 study found that lossy compression increased the Equal Error Rate (EER) by up to 25% compared to lossless methods in high-security applications. Storage efficiency is another critical factor, where emerging formats like WebP and AVIF deliver substantial savings while maintaining high accuracy, making them well-suited for large-scale deployments. Transmission speed is also improved with efficient compression, enabling faster data transfer in real-time applications such as mobile authentication and IoT-enabled devices. [5]

The integration of emerging technologies, such as neural network-based and hybrid compression strategies, represents a significant advancement in biometric system optimization. These innovations provide a nuanced balance between storage, processing, and accuracy, paving the way for scalable, efficient, and reliable biometric deployments. [5]

2.4 Emerging Trends and Security Concerns in Biometric Applications

The proliferation of biometric authentication in consumer devices and IoT applications marks a significant evolution in technology, emphasizing convenience and costeffectiveness. From smartphones to smart locks, biometric systems have become an integral part of modern security infrastructure. However, this widespread adoption introduces complex challenges, particularly when cost, usability, and security requirements are at odds. Addressing these challenges requires a nuanced understanding of emerging trends and associated vulnerabilities.

The increasing affordability of biometric devices has enabled the integration of fingerprint sensors into consumer-grade products. However, these cost-effective implementations often compromise sensor quality, precision, and robustness, leading to significant performance disparities compared to premium systems.

Low-cost fingerprint sensors face several limitations that impact their performance and reliability. The reduced sensor size in budget devices captures a smaller fingerprint area, increasing the likelihood of partial or incomplete matches. Their lower resolution, often below 300 DPI, compromises minutiae detection and recognition accuracy. Environmental factors such as moisture, dirt, or lighting variations further degrade performance, while inconsistent manufacturing quality results in fluctuating device performance. Additionally, limited on-device processing capabilities restrict the complexity of matching algorithms, affecting both speed and accuracy. Comparative studies highlight these disparities, showing that premium sensors achieve Equal Error Rates (EER) as low as 0.5%, while budget sensors typically range between 2.5% and 4.0%. High-end systems also process matches up to three times faster and produce sharper, more detailed fingerprint images for robust minutiae extraction. Advanced sensors integrate features like adaptive algorithms and protective coatings to tolerate environmental factors, which are often absent in budget devices. Practical implications are evident in case studies, such as a 2022 analysis of smart lock systems that revealed failure rates up to 30% higher for devices with low-cost sensors under conditions like wet or dirty fingers. In mobile authentication, premium ultrasonic fingerprint sensors demonstrated a 40% improvement in recognition accuracy compared to budget optical sensors, underscoring the critical advantages of high-quality technology. (Sunil Kumar Singla)

The integration of biometric systems into consumer devices and IoT applications presents various security vulnerabilities, particularly in the compression, transmission, and storage of biometric data. Compression, commonly used to optimise storage and transmission in resource-constrained environments, introduces several risks. Lossy compression formats like JPEG create predictable patterns that attackers can exploit to reconstruct ridge structures, compromising the integrity of the data. Compression artifacts further generate irregularities in fingerprint images, which can be manipulated in spoofing attempts. Additionally, compressed templates exhibit reduced data entropy, making them more susceptible to reconstruction attacks where attackers approximate original biometric features from compressed data. This process undermines system security and the reliability of biometric authentication. Furthermore, compression may weaken encryption mechanisms, as the noise introduced by compression can interfere with template matching algorithms and compromise template protection schemes. These vulnerabilities underscore the importance of developing robust strategies to balance compression efficiency with security in biometric systems. [6]

Biometric data transmission over networks, especially in IoT ecosystems, poses significant security challenges, exposing the systems to various types of attacks. Manin-the-Middle (MITM) attacks are a critical concern, where attackers intercept biometric data during transmission, potentially modifying or duplicating it for malicious use. Replay attacks, another common vulnerability, involve the reuse of previously captured data to bypass authentication, which is frequently observed in unsecured IoT devices. Additionally, the interception of unencrypted or poorly encrypted biometric templates increases the risk of large-scale data breaches. Weak or outdated communication protocols further exacerbate these risks by providing opportunities for attackers to compromise system integrity. Moreover, attackers can deploy Denial of Service (DoS) attacks, overwhelming systems with fraudulent biometric data, disrupting normal operations, and causing downtime. These vulnerabilities highlight the need for robust encryption, secure communication protocols, and advanced threat detection mechanisms in biometric systems. [5]

Documented security breaches involving biometric systems emphasize the real-world consequences of their vulnerabilities. In the 2017 August Smart Lock incident, attackers exploited weaknesses in compressed template storage, bypassing authentication and illustrating the dangers of using lossy compression without adequate safeguards. Similarly, replay attacks on mobile devices have highlighted the inadequacy of secure transmission protocols in many consumer products. Spoofing attempts further underscore these risks; a 2021 study revealed that 80% of low-cost fingerprint systems were successfully spoofed using reconstructed prints derived from compressed images. Large-scale database compromises, such as a 2019 breach affecting millions of biometric templates, demonstrate the critical need for robust encryption and secure storage practices. Additionally, IoT devices like smart locks have proven vulnerable, with weak authentication mechanisms exploited to gain unauthorized access by leveraging network vulnerabilities. These incidents underscore the importance of implementing comprehensive security measures across biometric systems.

The adoption of biometric systems in consumer and IoT applications is increasingly regulated by stringent frameworks and industry standards to ensure the secure and ethical handling of biometric data while safeguarding user privacy. The General Data Protection Regulation (GDPR) in the European Union provides a robust legal foundation for the management of biometric data, outlining specific requirements for compliance. Organizations must obtain explicit and informed consent from users before collecting biometric data, adhering to the principle of transparency. Data minimization is a key mandate, ensuring that systems collect only the data necessary for their intended purpose. Additionally, storage limitations require organizations to securely delete biometric data once it is no longer needed, minimizing the risk of misuse. Robust security measures are mandatory to protect biometric data during storage, processing, and transmission. Cross-border transfers of biometric data outside the EU are heavily regulated, with strict conditions in place to prevent unauthorized access or misuse, further reinforcing data protection. These regulations emphasize the importance of secure practices and ethical considerations in the deployment of biometric technologies. [5]

Industry standards play a critical role in guiding the design and implementation of biometric systems, ensuring security, compatibility, and reliability across applications. The ISO/IEC 19794-4 standard defines requirements for fingerprint image data formats, facilitating interoperability and consistency in biometric systems worldwide. FIPS 201, a standard for personal identity verification in government systems, emphasizes secure template management and encryption to safeguard sensitive data. Similarly, NIST SP 800-63-3 provides comprehensive digital identity guidelines, including best practices for biometric authentication systems to enhance security and usability. The Common Criteria framework offers a structured methodology for evaluating the security of biometric systems against predefined benchmarks, enabling organizations to assess and certify their solutions. Additionally, the NIST Minutiae Interoperability Exchange (MINEX) program evaluates the performance and reliability of fingerprint-matching algorithms, promoting standardization and advancing the efficacy of biometric technologies. Together, these standards ensure the secure and effective deployment of biometric systems across various industries.

Addressing the challenges posed by low-cost implementations and security vulnerabilities in biometric systems requires a comprehensive and collaborative approach from manufacturers and regulators. Improving sensor quality is paramount, with an emphasis on adopting higher-resolution sensors capable of advanced environmental tolerance to enhance accuracy and reliability. Robust data protection mechanisms, such as end-to-end encryption, secure multiparty computation, and homomorphic encryption, are essential to safeguard biometric templates against unauthorized access and attacks. AI-driven preprocessing can play a transformative role by leveraging machine learning algorithms to enhance low-quality images, reduce noise, and mitigate compression artifacts, thereby improving system performance. Standardized communication protocols should be implemented to secure data transmission, preventing interception and replay attacks. Furthermore, regulatory oversight needs to be strengthened, with comprehensive compliance frameworks ensuring that consumer devices adhere to minimum security and privacy standards. These strategies collectively aim to bolster the resilience and reliability of biometric systems in an increasingly interconnected world. [7]

2.5 Minutiae Reduction and Recognition Reliability

Minutiae points—such as ridge endings, bifurcations, and deltas—form the backbone of fingerprint recognition systems. Their extraction and analysis are critical for accurate matching and authentication. Minutiae reduction, which refers to the loss or degradation of these points, can severely impact system performance, reliability, and security. A detailed understanding of the factors contributing to minutiae reduction, its effects on system accuracy, and the strategies to mitigate these issues is essential for designing robust biometric systems. (Kamlesh Tiwari)

Minutiae reduction significantly impacts fingerprint recognition performance, with a non-linear and exponential relationship observed between the extent of reduction and system degradation. The Equal Error Rate (EER) rises sharply as minutiae decrease, with a 10% reduction causing a 15% increase in EER and a 20% reduction leading to a 35% increase, substantially impairing reliability. At 30% reduction, the EER surges by 70%, rendering the system nearly unusable for high-security applications. A 40% reduction makes the system unreliable due to excessive false matches and rejections, and at 50%, authentication effectively fails as insufficient minutiae compromise genuine and impostor fingerprint differentiation. Real-world examples demonstrate these effects; forensic investigations often rely on partial or smudged fingerprints with reduced minutiae, leading to EER increases exceeding 60% and requiring extensive manual intervention. Similarly, budget smartphones with low-resolution sensors frequently capture fewer minutiae points, resulting in higher False Rejection Rates (FRR) and user dissatisfaction. (Kamlesh Tiwari)

Minutiae reduction arises from various factors, including image compression artifacts, where lossy formats like JPEG obscure ridge structures and high compression ratios exceeding 20:1 cause up to 30% minutiae loss. Low-resolution sensors capture fewer details, while sensor defects introduce noise that degrades image quality. Environmental factors like dirt, moisture, and temperature variations blur ridges and cause distortions, with poor lighting, exacerbating these issues in optical sensors. User interaction issues, such as incorrect finger placement, excessive pressure, or dry and worn-out fingertips—common among elderly users or manual labourers—further reduce identifiable minutiae. Processing algorithm limitations also contribute; basic extraction algorithms struggle with low-quality images, leading to missed or false minutiae detection, while simplified matching algorithms in budget devices fail to handle partial or degraded prints effectively. These challenges underscore the need for advanced sensors, robust preprocessing algorithms, and user education to maintain system reliability, particularly in applications requiring high security or precision.

To mitigate the challenges posed by minutiae reduction, modern fingerprint recognition systems incorporate advanced strategies to enhance image quality, improve minutiae extraction, and optimize matching processes. Image enhancement techniques play a crucial role in restoring degraded prints and maximizing the detection of minutiae points. Adaptive histogram equalization enhances local contrast, making ridge patterns more distinguishable, while Gabor filtering improves ridge clarity by emphasizing frequency and orientation information in the image. Ridge orientation mapping identifies and reinforces ridge flow patterns, effectively mitigating distortions caused by compression or noise. Frequency domain enhancement, using Fourier analysis, isolates and amplifies ridge structures while suppressing noise. Additionally, neural network-based restoration methods, particularly those using AI-driven models like generative adversarial networks (GANs), have demonstrated success in reconstructing minutiae details in degraded or low-resolution images, such as smudged or partial prints. (Kamlesh Tiwari)

Case studies underscore the effectiveness of these techniques. A 2021 study showed that applying Gabor filtering to compressed fingerprint images reduced the Equal Error Rate (EER) by 25%. Similarly, neural network-based enhancement techniques restored up to 90% of minutiae points lost in low-resolution images, significantly improving recognition accuracy. These findings highlight the transformative potential of advanced image processing and AI-driven approaches in addressing the challenges associated with minutiae reduction, enhancing the reliability and precision of fingerprint recognition systems.

Modern fingerprint recognition systems address the challenges of minutiae reduction through advanced processing algorithms that enhance detection and matching accuracy. Multi-scale feature extraction captures minutiae at different resolutions, significantly improving detection in low-quality or partial prints. Robust minutiae detection algorithms are designed to identify and validate minutiae points even in noisy or distorted images, ensuring reliability. Quality-aware matching evaluates the quality of both probe and template images during the matching process, assigning greater weight to higher-quality minutiae to enhance precision. Partial print matching algorithms specialize in handling incomplete prints, which are common in forensic and mobile applications. Fusion-based approaches** combine minutiae-based matching with other fingerprint features, such as ridge patterns or texture analysis, to increase overall reliability. Testing these algorithms has demonstrated their efficacy; multi-scale feature extraction has improved minutiae detection rates by 30% in low-quality images captured under adverse conditions, while partial print matching has reduced the False Rejection Rate (FRR) by 40% in forensic databases with fragmented fingerprints. (Kamlesh Tiwari)

Advancements in AI and sensor technology promise to further mitigate the challenges of minutiae reduction. AI-driven matching systems using machine learning models can dynamically adjust matching thresholds based on minutiae quality, enhancing performance across diverse conditions. Edge computing enables real-time fingerprint image processing directly on devices, reducing reliance on external resources and minimizing latency, thus improving speed and efficiency. Additionally, improved sensor materials and designs, such as ultrasonic sensors, provide better minutiae capture, even in challenging environmental conditions like wet or dirty surfaces. These innovations hold the potential to significantly enhance the accuracy and robustness of fingerprint recognition systems in the future.

Minutiae reduction poses a significant threat to the reliability and accuracy of fingerprint recognition systems. Its effects are especially pronounced in low-cost devices, lossy compression scenarios, and adverse environmental conditions. By adopting advanced image enhancement techniques, robust processing algorithms, and cutting-edge AI technologies, biometric systems can mitigate the adverse impacts of minutiae reduction and deliver consistent performance. This focus on innovation and optimization is crucial as biometric applications continue to expand into consumer devices, IoT ecosystems, and high-security domains.

2.6 Emerging Technologies in Biometric Systems

The integration of advanced technologies is revolutionizing biometric systems, offering solutions to longstanding challenges in accuracy, security, and usability. Emerging technologies such as artificial intelligence (AI), machine learning (ML), edge computing, and adaptive algorithms are reshaping the biometric landscape, enhancing both system capabilities and user experience.

AI and ML technologies are driving innovation in biometric systems, particularly in feature extraction, image processing, and decision-making processes. These advancements are transforming how biometric systems handle noisy or incomplete data, making them more robust and scalable.

Deep learning, particularly through Convolutional Neural Networks (CNNs), has revolutionized biometric systems, offering significant advancements in feature extraction, pattern recognition, and adaptability. Enhanced feature extraction capabilities of CNNs allow for the identification and extraction of intricate biometric features, such as fingerprint minutiae and iris patterns, even in challenging conditions.

These networks are also highly resistant to noise, effectively distinguishing genuine biometric features from distortions caused by environmental factors or compression artifacts. With **superior pattern recognition, CNNs achieve unmatched accuracy in detecting complex biometric patterns, making them ideal for applications like facial recognition and multi-modal systems. Furthermore, their adaptive learning capability ensures continuous improvement as more data is processed, enhancing long-term reliability and scalability. Real-time processing is another critical advantage, with optimized CNN architectures enabling rapid authentication for applications such as mobile unlocking and border control. [2], [8]

Generative Adversarial Networks (GANs) are also transforming biometric systems, particularly in data enhancement and synthetic generation. GANs excel at high-quality image reconstruction, restoring incomplete or degraded biometric images like smudged fingerprints for accurate matching. They facilitate the creation of synthetic training data, producing realistic biometric datasets that address privacy concerns by reducing reliance on real data. Additionally, GANs improve the resolution of low-quality images, making them suitable for resource-constrained devices, and effectively remove artifacts caused by lossy compression, enhancing the integrity of biometric data. These advancements highlight the transformative potential of deep learning in overcoming traditional limitations and advancing the capabilities of biometric systems.

Edge computing is transforming biometric systems by enabling local data processing, reducing reliance on centralized cloud infrastructure, and improving speed, privacy, and reliability. Reduced latency is a key advantage, as local processing allows for near-instantaneous authentication, which is critical for time-sensitive applications like access control. Enhanced privacy is achieved by processing sensitive biometric data locally, minimising its exposure during transmission and reducing the risk of breaches. Additionally, edge computing lowers bandwidth requirements by eliminating the need to transmit raw biometric data to remote servers, optimising network usage. Improved system resilience ensures that localised systems remain operational even without continuous internet connectivity, making them robust in offline scenarios. Furthermore, real-time processing on edge devices enables quick decision-making, enhancing user experience and system responsiveness. [8]

However, implementing edge computing in biometric systems involves addressing several challenges. Hardware optimisation is essential, as devices must balance processing power and energy efficiency to maintain consistent performance without overheating. Power consumption management is equally important, with efficient algorithms designed to minimize energy usage and extend the operational life of battery-powered devices. Security integration is critical to protect local data from unauthorised access, requiring advanced encryption and secure boot mechanisms. Performance scaling is necessary to ensure that systems can handle varying data loads without compromising speed. Additionally, redundancy requirements must be considered, with fail-safe mechanisms implemented to guarantee uninterrupted operation in case of hardware failures. By addressing these considerations, edge computing can significantly enhance the functionality and reliability of biometric systems.

Modern biometric systems leverage adaptive algorithms to dynamically respond to input quality and environmental conditions, ensuring consistent and reliable performance. Quality-based adaptation optimizes system processes according to the quality of the biometric input. Dynamic threshold adjustment allows matching thresholds to adapt in low-quality scenarios, reducing error rates. Feature extraction optimization prioritizes high-confidence features, enhancing system reliability. Pipeline modification ensures processing pipelines dynamically adjust to varying data quality, enabling seamless operation. Additionally, resource allocation adjustment redistributes computational resources based on input complexity, optimizing performance, while performance scaling ensures efficiency across diverse operational scales, from personal devices to extensive databases. [8]

Environmental adaptation is another critical aspect of these systems, as factors like lighting, temperature, and surface conditions can impact biometric performance. Adaptive algorithms mitigate these challenges through techniques such as temperature compensation, which adjusts for heat-induced sensor variations, and humidity adjustment, which ensures reliable operation in different moisture levels. Lighting optimization dynamically enhances optical sensor performance under varying lighting conditions, while pressure variation handling compensates for differences in finger pressure during fingerprint capture. Furthermore, surface condition adaptation enables systems to account for dry, oily, or dirty surfaces, significantly improving recognition accuracy. These adaptive capabilities ensure robust performance in diverse and challenging operational environments.

2.7 Privacy and Ethical Implications

The deployment of biometric systems presents significant privacy challenges and ethical considerations that must be addressed through thoughtful design, stringent regulation, and comprehensive validation. Privacy challenges arise because biometric data is inherently sensitive and irrevocably linked to an individual’s identity, making unauthorised access or misuse potentially devastating, leading to identity theft or discrimination.

Data protection is a cornerstone of safeguarding biometric systems, requiring robust measures such as secure storage protocols to encrypt biometric templates and prevent unauthorized access. Encryption during storage and transmission ensures end-to-end data protection, while access control mechanisms restrict system access to authorized personnel. Audit trail implementation enhances accountability by recording data access and modifications, and data lifecycle management minimizes exposure risks through clear policies for data retention and deletion. [3]

Regulatory compliance is critical in governing biometric systems. Frameworks such as the GDPR mandate explicit consent for data collection, enforce data minimization, and uphold strict processing security standards. The CCPA grants users control over their biometric data, including the right to access, delete, or restrict usage, while BIPA imposes stringent informed consent and secure storage requirements for biometric systems in Illinois, USA. International standards like ISO/IEC 24745 provide global guidelines for securely managing biometric data.

Ethical considerations focus on fairness, inclusivity, and transparency in biometric systems. Demographic fairness is essential to ensure consistent performance across diverse populations, with algorithms designed for equal accuracy across genders, ethnicities, and age groups. Accessibility considerations include accommodating individuals with disabilities or less distinct biometric features, aligning solutions with cultural sensitivity, and addressing age-related changes or disabilities through adaptive technologies and alternative modalities.

Rigorous testing and validation are integral to ethical deployment. This includes selecting representative samples to ensure diverse user populations are adequately represented in training datasets and conducting bias detection to identify and mitigate algorithmic biases that could disproportionately impact specific demographics. Standardized performance metrics ensure fairness and comparability, while validation criteria establish benchmarks for inclusivity and robustness. Addressing these privacy and ethical challenges is essential for fostering trust and ensuring equitable and secure deployment of biometric systems. [3]

2.8 Real-World Applications and Trade-Offs

Biometric systems are increasingly deployed across diverse sectors, each with unique demands that require careful balancing of performance, security, and costeffectiveness. In mobile authentication, these systems prioritize usability and efficiency, emphasizing features like storage optimization to minimize on-device storage demands and lightweight algorithms to conserve battery life. A seamless, fast, and accurate user experience is crucial for adoption, alongside robust security levels to protect user data from breaches. Additionally, systems must meet high-performance expectations, operating reliably under varying environmental conditions to maintain trust and usability. [4]

The deployment of biometric systems involves innovative implementation strategies to address application-specific constraints. Hybrid approaches are increasingly common, combining on-device and cloud storage to balance efficiency with security. Multi-modal authentication enhances reliability and security by integrating multiple biometric modalities, such as fingerprint and facial recognition, while tiered security levels tailor access controls to user roles and authentication contexts.

Performance optimization is critical for ensuring smooth and reliable operation. Strategies include dynamic resource allocation, where systems adjust resource usage based on input complexity, and pipeline optimization to streamline processing workflows and minimize latency. Automated quality control mechanisms ensure consistent performance across devices, enabling biometric systems to meet the rigorous demands of modern applications. These strategies underscore the importance of adaptability and innovation in deploying biometric systems effectively.

Table 1 - Key Literature on Fingerprint Recognition and Compression Techniques

Author(s)	**Year**	**Paper Name**	**Algorithm/Method Used**
Bansal, R., Sehgal, P., & Bedi, P.	2015	Minutiae Extraction from Fingerprint Images - A Review	Minutiae-based matching

Elias, S. P., & Mythili, P.	2016	An Improved Algorithm for Fingerprint Compression Based on Sparse Representation	Sparse representation-based compression
Dhanalakshmi et al.	2017	Aadhaar-Based Biometric Attendance	Wireless fingerprint system
Karimian, N., et al.	2018	Secure and Reliable Biometric Access Control for Resource Constrained Systems and IoT	Biometric access control for IoT

Funk, W., & Arnold, M.	2018	Evaluation of Image Compression Algorithms for Fingerprint and Face Recognition Systems	Image compression evaluation
Gamassi, M., et al.	2018	Fingerprint Local Analysis for High Performance Minutiae Extraction	High-performance minutiae extraction
Liu et al.	2021	Class-Incremental Learning for IoT Fingerprints	Incremental neural classifier
Minocha, S., et al.	2023	A Fingerprint Recognition Using CNN Model	Convolutional Neural Networks (CNN)
Mari et al.	2024	Effectiveness of Learning-Based Codecs for Fingerprints	AVIF, JPEG XL, neural compression codecs
Mascher-Kampfer et al.	2024	Impact of Compression on Face and Fingerprint Recognition	SPIHT, JPEG2000, standard codecs

3 Methodology/Procedure

3.1 Experimental Design

This study was designed to assess the effects of image formats, compression levels, and minutiae reduction on fingerprint recognition performance. By systematically varying these parameters, the experiment aimed to uncover the trade-offs between recognition accuracy, system reliability, and storage efficiency.

3.1.1 Software Setup

The software setup was critical to enabling accurate fingerprint analysis:

1. Neurotechnology VeriFinger SDK:
   - Selected for its advanced fingerprint recognition and analysis capabilities.
   - Used to calculate critical performance metrics such as False Acceptance Rate (FAR) and False Rejection Rate (FRR).
   - The SDK allowed customization, including adjustments to recognition thresholds and matching parameters, ensuring precise alignment with experimental requirements.

2. Microsoft Visual Studio:
   - Integrated with the VeriFinger SDK for compiling, debugging, and executing fingerprint analysis tasks.
   - Supported preprocessing tasks, such as format conversion and compression.

Justification: The combination of VeriFinger SDK and Visual Studio ensured a seamless workflow for minutiae extraction, matching, and data analysis, making them ideal for biometric research.

3.1.2 Hardware Setup

The experiments were conducted using a high-performance computer to avoid computational bottlenecks and maintain consistency across all conditions. The system configuration included:

- Processor: Multi-core processor to manage computational demands.
- RAM: 16 GB for smooth handling of large datasets and high-resolution images.
- Storage: Ample capacity to accommodate multiple versions of datasets across formats and compression levels.
- GPU: Available for accelerating certain image preprocessing tasks, though not essential for fingerprint recognition.

Justification: The hardware setup ensured reproducibility and eliminated variables related to computational limitations.

3.1.3 Image Formats and Compression Rates

Fingerprint images were evaluated across four common image formats:

1. PNG: A lossless format that preserves image details, ensuring no loss of minutiae information.

2. JPEG: A lossy format commonly used for its storage efficiency but prone to introducing compression artifacts.

3. BMP: An uncompressed format used as the baseline for comparison.

4. WebP: A modern format offering both lossy and lossless options, less studied in the biometric context.

Compression Rates:

To simulate storage constraints and evaluate performance, two compression levels were applied:

• 20% Compression: Representing mild data reduction.

• 60% Compression: Representing moderate data reduction and more significant trade-offs between storage and recognition reliability.

3.2 Data Collection

3.2.1 High-Quality Dataset

• Source: Data was obtained from the Hong Kong Polytechnic University, a widely recognized source for biometric research.

• Characteristics:

  - High resolution with clear ridge structures and well-defined minutiae.
  - Minimal noise and distortion, ensuring optimal conditions for assessing baseline performance.

3.2.2 Low-Quality Dataset

Characteristics:

- Captured under suboptimal conditions, resulting in lower resolution and visible distortions.
- Simulated real-world challenges, such as environmental noise or poor sensor quality, to evaluate system performance under realistic constraints.
- Justification: The inclusion of both high- and low-quality datasets allowed for a comprehensive evaluation of recognition performance under varied conditions.

Figure 1 - Sample fingerprint

3.2.3 Preprocessing Steps

1. Format Conversion:

- High-quality images: Converted from JPEG to BMP and PNG using lossless methods to avoid introducing additional noise.
- Low-quality images: Converted from BMP to JPEG and PNG.

2. Compression:

- Applied compression levels of 20% and 60% using industry-standard tools to ensure consistency and reproducibility.

3. Minutiae Reduction:

    - Certain details were manually eliminated from selected images to simulate scenarios where environmental variables or quality degradation caused loss of minutiae information.

3.3 Metrics for Analysis

To evaluate recognition performance, the study used standard biometric metrics:

False Acceptance Rate (FAR)

• Measures the likelihood of unauthorized fingerprints being falsely accepted as legitimate.

False Rejection Rate (FRR)

• Measures the likelihood of genuine fingerprints being falsely rejected by the system.

Threshold Analysis

• Recognition thresholds were systematically varied to determine sensitivity to compression and minutiae reduction. For example, at 90% compression, recognition performance was severely impacted, indicating the limits of reliable operation.

Storage Efficiency

• Analysed the trade-offs between storage savings and recognition reliability, with higher compression levels expected to reduce storage space but compromise accuracy.

3.4 Experimental Steps

1. Compression Analysis:

• Objective: To evaluate how different formats and compression levels affect recognition accuracy.

• Steps:

1. Baseline matching scores were calculated for images in their original formats. 2. Images were converted to alternate formats (JPEG, PNG, BMP, WebP).

3. Compression levels of 20% and 60% were applied incrementally.

4. Matching scores were recalculated, and thresholds for performance failure were documented.

2. Minutiae Reduction:

• Objective: To assess the impact of reduced minutiae points on recognition performance.

• Steps:

1. Selected images were manually edited to remove specific minutiae points. 2. Matching scores were recalculated for modified images.

3. Results were compared with unmodified images.

3. Correlation Analysis:

• Objective: To link changes in FAR and FRR with image quality, compression levels, and minutiae reduction.

• Steps:

1. FAR and FRR values were plotted for each experimental condition.
2. Trends were analysed to identify critical thresholds.
3. Correlations were visualised using charts to illustrate relationships between variables.

4 Results

This chapter presents the experimental results for two distinct fingerprint datasets—high-quality, high-resolution images and low-quality, low-resolution images. The results evaluate the effects of file format conversion, compression, and minutiae reduction on biometric performance metrics such as False Acceptance Rate (FAR) and False Rejection Rate (FRR).

4.1 Dataset Overview

1. High-Quality, High-Resolution Dataset:

• Format: Initially in JPEG (JPG) format.

• Characteristics: Clear ridge structures and minimal noise, providing an ideal baseline for performance evaluation.

2. Low-Quality, Low-Resolution Dataset:

• Format: Initially in BMP format.

• Characteristics: Distorted and noisy images simulating real-world challenges in fingerprint acquisition.

Both datasets underwent identical preprocessing and experimental conditions to maintain consistency.

4.2 Impact of Format Conversion

High-Quality Dataset

• Process: Converted from JPEG to BMP, PNG, and WebP.

• Results: No observable changes in matching scores or FAR across formats.

• Observation: The robustness of the high-quality dataset ensured minutiae details remained unaffected by format conversion.

Low-Quality Dataset

• Process: Converted from BMP to JPEG, PNG, and WebP.

• Results:

• JPEG: Significant artifacts were introduced, resulting in increased FAR and reduced matching scores.

• PNG: Maintained scores and FAR due to its lossless compression properties.

• Observation: Low-quality datasets were highly sensitive to lossy formats like JPEG,

which distorted minutiae structures.

Table 2 - Score of fingerprint data of high resolution and quality database

JPEG FORMAT		**PNG FORMAT**		**BMP FORMAT**	
SCORE	ID 1	SCORE	ID	SCORE	ID
669	1_1	669	1_1	669	1_1
381	1_2	381	1_2	381	1_2
316	1_6	316	1_6	316	1_6

306	1_5	306	1_5	306	1_5
284	1_3	284	1_3	284	1_3
251	1 _4	251	1 _4	251	1 _4
SCORE	ID 2	SCORE	ID	SCORE	ID
697	2_1	697	2_1	697	2_1
434	2_3	434	2_3	434	2_3
429	2_5	429	2_5	429	2_5
429	2_4	429	2_4	429	2_4
425	2_2	425	2_2	425	2_2
412	2 _6	412	2 _6	412	2 _6
SCORE	ID 3	SCORE	ID	SCORE	ID
640	3_1	640	3_1	640	3_1
402	3_3	402	3_3	402	3_3
365	3_5	365	3_5	365	3_5
351	3_2	351	3_2	351	3_2
336	3_4	336	3_4	336	3_4
280	3_6	280	3_6	280	3_6

Table 3 - Score of fingerprint data of low resolution and quality database

BMP FORMAT		**JPEG FORMAT**		**PNG FORMAT**	
SCORE	**ID 1**	**SCORE**	**ID 1**	**SCORE**	**ID 1**
729	1	243	1	729	1

386	3	249	3	386	3
373	2	221	2	373	2
261	4	705	4	261	4
SCORE	**ID 2**	**SCORE**	**ID 2**	**SCORE**	**ID 2**
696	1	667	1	696	1
444	2	445	2	444	2
339	3	374	3	339	3
151	4	143	4	151	4
SCORE	**ID 3**	**SCORE**	**ID 3**	**SCORE**	**ID 3**
570	1	577	1	570	1
334	2	339	2	334	2
308	3	305	3	308	3
274	4	266	4	274	4

4.3 Impact of Compression Levels

Compression impacts all datasets, regardless of format or type, altering key metrics such as FAR and FRR. High-quality datasets are relatively resilient, with minimal performance degradation at 20% compression and only slight increases in FAR and FRR at 60% due to minor distortions in minutiae details. In contrast, low-quality datasets are more sensitive, showing noticeable changes in FAR and FRR at 20% compression and substantial degradation at 60%, including a higher likelihood of false matches and difficulty recognizing genuine fingerprints. While high-quality datasets can tolerate moderate compression, low-quality datasets experience significant declines in accuracy and reliability under similar conditions.

Table 4 - Score of the fingerprint database after compression

COMPRESSION 20%			**COMPRESSION 60%**	
SCORE	**ID**		**SCORE**	**ID**

519	1_1		478	1_1
383	1_2		370	1_2
316	1_5		284	1_6
306	1_6		276	1_5
290	1_3		260	1_3
254	1 _4		234	1 _4
566	2_1		518	2_1
446	2_5		445	2_5
438	2_3		423	2_3
422	2_2		405	2_2
416	2_4		395	2_4
404	2 _6		370	2 _6
474	3_1		483	3_1
348	3_3		396	3_3
345	3_5		369	3_5
334	3_2		339	3_2
298	3_4		331	3_4
269	3_6		273	3_6

4.4 Impact of Minutiae Reduction

Process: Minutiae points were manually reduced by 10%-30% to analyze the impact on recognition performance.

Results:

Up to a 20% reduction in minutiae points showed minimal effects on False Acceptance Rate (FAR) and False Rejection Rate (FRR) due to sufficient minutiae details.

Beyond 20%-30% reduction, FAR and FRR increased significantly, indicating reduced system reliability.

Observation: Systems with sufficient minutiae details were more resilient to minor reductions, but performance degraded notably with substantial minutiae loss. Systems with fewer minutiae details showed sharp increases in FAR and FRR even with a 10% reduction, becoming unreliable as minutiae loss exceeded 20%. This highlights the critical need to preserve minutiae details for reliable performance.

Table 5 - Scores of databases before and after minutiae reduction

MINUTIAE REDUCTION		
BEFORE	**AFTER**	
ID 1		
669	490	
ID 2		
697	554	
ID 3		
640	510	

4.5 Key Observations

1. Impact of Format Conversion:

• High-quality datasets remained unaffected by format changes.

• Low-quality datasets suffered significant performance degradation when converted to lossy formats like JPEG.

2. Impact of Compression:

• High-quality datasets tolerated up to 60% compression with minor performance degradation.

• Low-quality datasets experienced severe performance losses even at 20% compression.

3. Impact of Minutiae Reduction:

• High-quality datasets-maintained performance up to 20% minutiae reduction but degraded significantly beyond that.

• Low-quality datasets were sensitive even to minimal minutiae loss, underlining the importance of detail preservation.

4. Threshold Observations:

• Extreme conditions (e.g., 90% compression or substantial minutiae reduction) rendered both datasets unreliable, with FAR and FRR exceeding practical limits.

4.6 Summary

This chapter highlights the critical role of image quality, compression, and minutiae density in determining the robustness of biometric systems:

• High-quality datasets: Demonstrated resilience to moderate compression and minutiae reduction but degraded under extreme conditions.

- Low-quality datasets: These were highly sensitive to lossy compression and minutiae reduction, making them less suitable for resource-constrained or suboptimal acquisition environments.

The findings emphasise the need to select appropriate image formats, compression levels, and preprocessing techniques to optimise biometric performance while maintaining security and reliability.

5 Discussion

This research provides critical insights into the impact of image compression and minutiae reduction on fingerprint recognition performance. The discussion contextualises these findings within biometric security, system design, and practical applications, focusing on optimising trade-offs between storage efficiency, recognition accuracy, and system robustness.

5.1 The Role of Image Quality in Biometric Systems

Image quality emerged as a pivotal determinant of biometric system reliability. Highquality datasets maintained consistent performance under moderate compression and minutiae reduction due to their richness in ridge structures and minutiae points. In contrast, low-quality datasets showed significant sensitivity to even minimal compression, with sharp increases in False Acceptance Rate (FAR) and False Rejection Rate (FRR).

Implications:

1. Enrolment Quality: High-quality image acquisition during enrolment is critical to ensuring reliable long-term performance.

2. Mitigation for Low-Quality Scenarios: Applications like mobile authentication or fieldbased biometric collection should employ preprocessing techniques such as noise reduction and resolution enhancement to compensate for quality loss.

5.2 Compression Formats: Trade-Offs and Thresholds

The comparative analysis of compression formats reinforced distinct trade-offs between storage efficiency and recognition reliability:

1. Lossless Formats (PNG, BMP): These formats preserved minutiae integrity and recognition accuracy, making them ideal for high-security applications. However, their high storage demands limit practicality in large-scale or resource-constrained systems.

2. Lossy Formats (JPEG, WebP): While efficient in storage, these formats introduced artifacts that compromised minutiae extraction at higher compression levels. WebP showed potential as a balanced option for consumer-grade systems, but its suitability for critical applications requires further investigation.

Significance: This study contributes to the literature by expanding on prior work (e.g., Bansal et al.) with an in-depth evaluation of WebP, revealing its potential for noncritical applications. Future exploration of emerging formats like AVIF can further refine these trade-offs.

Practical Recommendations:

- Use lossless formats for high-stakes systems, such as border control or forensic databases.

- Employ lossy formats like WebP for applications prioritising storage efficiency and usability, such as IoT devices and mobile platforms.

5.3 Impact of Compression Levels on Recognition Metrics

Compression levels significantly affected recognition reliability, with high-quality datasets tolerating compression up to 60%, while low-quality datasets degraded noticeably at 20%. These findings align with Karimian et al. (2018), emphasising the vulnerability of low-resolution datasets.

Thresholds for Practical Use:

- High-quality datasets: Compression up to 60% is acceptable without a major impact on FAR and FRR.

- Low-quality datasets: Aggressive compression should be avoided entirely, as even moderate levels compromise reliability.

Implications for Design: System designers must consider context-specific compression thresholds. For example:

- High-Security Applications: Limit compression to below 20% and prioritise lossless formats.

- Consumer-Grade Systems: Balance usability and storage savings with moderate compression levels, supplemented by preprocessing enhancements.

5.4 Minutiae Reduction and System Reliability

The study quantified the effects of minutiae reduction, filling a gap in prior research (e.g., Mari et al., 2024). High-quality datasets tolerated up to 20% minutiae reduction with minimal impact, while low-quality datasets experienced significant degradation even at 10%.

Implications:

- Preservation of minutiae points is critical for low-quality datasets. Adaptive minutiae extraction techniques, which dynamically adjust based on image quality, can enhance reliability.

- In environments prone to quality loss (e.g., field-based collection), preprocessing methods such as resolution enhancement and noise reduction are essential

5.5 Applications and Real-World Implications

Mobile Authentication:

- Challenges: Storage and processing constraints necessitate efficient compression techniques.
- Recommendations: Use hybrid approaches combining lossy compression with advanced preprocessing to balance usability and reliability.

Large-Scale Biometric Databases:

- Challenges: National ID programs prioritise accuracy over storage efficiency.
- Recommendations: Use lossless or minimally compressed formats to ensure reliability in long-term storage.

Access Control Systems:

- Challenges: Balancing security, usability, and computational efficiency.
- Recommendations: Implement moderate compression levels and robust preprocessing to achieve this balance.

5.6 Ethical and Security Considerations

Compression artifacts and minutiae reduction may introduce vulnerabilities, such as patterns exploitable for reverse-engineering attacks. Furthermore, quality degradation may disproportionately affect certain demographics, highlighting the need for inclusive testing and fairness.

Recommendations:

- Inclusive Testing: Evaluate biometric systems across diverse user groups to ensure equitable performance.

- Robust Safeguards: Implement safeguards to mitigate security risks associated with compression artifacts.

5.7 Bridging Research Gaps and Future Directions

1. Exploration of Emerging Formats:
    - Evaluate the performance of modern formats like WebP and AVIF in biometric systems to refine trade-offs between quality and storage efficiency.
2. Development of Adaptive Algorithms:
    - Create dynamic algorithms for minutiae extraction and matching that adjust based on image quality and compression characteristics.
3. Integration of AI-Driven Enhancements:
    - Use deep learning techniques, such as convolutional neural networks (CNNs), to restore degraded fingerprint images and mitigate compression effects.
4. Real-World Testing:

- Simulate conditions such as environmental noise and user behaviour during acquisition to validate findings in practical scenarios.

5.8 Practical Recommendations

1. Adopt Lossless Compression for High-Security Applications:

- Use PNG or BMP to preserve minutiae integrity in critical systems.

2. Optimize Compression Levels:

- Limit compression to 60% for high-quality datasets and avoid aggressive compression for low-quality datasets.

3. Enhance Preprocessing Techniques:

- Apply noise reduction and resolution enhancement for low-quality datasets to improve system reliability.

4. Leverage Emerging Technologies:

- Integrate AI-driven tools and edge computing capabilities to enhance performance and mitigate security risks.

5.9 Summary of Findings and Implications

This discussion has contextualised the findings to address the research questions:

1. Lossless formats preserve accuracy but require significant storage, while lossy formats like WebP offer a balance for consumer applications.

2. High-quality datasets tolerate up to 60% compression, while low-quality datasets degrade at just 20%.

3. High-quality datasets are resilient to up to 20% minutiae reduction, but low-quality datasets are highly sensitive even to minimal reductions.

4. Practical recommendations include using lossless formats for critical systems, optimizing compression for usability, and employing advanced preprocessing techniques to mitigate quality loss.

By addressing these objectives, this research provides actionable insights for optimizing fingerprint recognition systems in diverse applications, from high-security environments to resource-constrained systems.

Table 6 - Comparison of Prior Research and This Study on Fingerprint Image Compression and Recognition Performance

Aspect	Prior Research	This Study
Focus	Impact of common compression formats (e.g., JPEG, PNG) on fingerprint recognition systems.	Comparative analysis of multiple formats (JPEG, PNG, BMP, WebP) and varying compression levels (20%, 60%).

Compression Levels	Focused on moderate compression levels, typically around 20%-40%.	Analysed both mild (20%) and moderate (60%) compression levels, emphasizing the thresholds of performance degradation.
Performance Metrics	Studied metrics like False Acceptance Rate (FAR) and False Rejection Rate (FRR).	Evaluated FAR, FRR, and Equal Error Rate (EER) to provide a comprehensive performance analysis.
Emerging Formats	Limited exploration of emerging formats like WebP and AVIF.	Highlighted the potential of WebP for balancing quality and storage efficiency, with recommendations for further investigation of modern formats.

Minutiae Reduction	Discussed impact but lacked quantitative thresholds for reduction effects.	Quantified the effect of minutiae reduction, establishing critical thresholds for high and low-quality datasets.
Security Considerations	Mentioned potential vulnerabilities in passing.	Addressed security implications of compression artifacts and vulnerabilities, providing actionable
		recommendations for risk mitigation.
Insights on Trade-offs	Highlighted general tradeoffs between storage efficiency and recognition accuracy	Provided detailed tradeoffs analysis, including critical compression thresholds and the role of emerging formats in optimizing performance and efficiency.

5.10 Automation and Advanced Methods in Biometric Research

Automation and advanced methods play a critical role in enhancing biometric research by improving efficiency, accuracy, and scalability. These techniques complement the original study by enabling the analysis of larger datasets and addressing challenges in low-quality fingerprint recognition. Machine learning models, such as Generative Adversarial Networks (GANs), enhance minutiae reconstruction in degraded images, dynamically adapting to varying image qualities to reduce False Acceptance Rates (FAR) and False Rejection Rates (FRR). Hybrid compression approaches, like regionspecific compression, balance storage efficiency and recognition reliability by preserving critical areas with lossless methods and applying lossy compression to less significant regions. Additionally, automated preprocessing pipelines using tools like Python or MATLAB streamline tasks such as image enhancement and format conversion, ensuring consistent and reproducible results across datasets.

Emerging technologies further expand the scope of biometric applications. Modern image formats, including AVIF and JPEG XL, demonstrate advanced compression capabilities while maintaining ridge structure integrity, outperforming traditional formats like JPEG. Edge computing offers a transformative solution for real-time processing, allowing biometric data to be handled locally on devices, enhancing privacy and reducing latency for applications such as mobile authentication and IoT devices. Synthetic datasets, created using GANs, address limitations in dataset size and diversity, mimicking real-world conditions to enable comprehensive testing without compromising user privacy. These innovations ensure that biometric systems remain robust and scalable even in resource-constrained environments.

The integration of these advanced methods enhances the practical utility of biometric systems, enabling them to scale effectively while maintaining high reliability. Automation tools for visualisation and reporting provide actionable insights into trends in FAR, FRR, and Equal Error Rate (EER), allowing researchers to identify critical thresholds efficiently. These advancements pave the way for real-world applications, including large-scale biometric databases, IoT-enabled security systems, and realtime mobile authentication, emphasising the value of automation in addressing emerging challenges in biometric research.

6 Conclusion

6.1 Overview of the Research

This study investigated the trade-offs between storage efficiency and recognition accuracy in fingerprint-based biometric systems. By analyzing various image compression formats, levels, and minutiae reduction techniques, the research highlighted key factors influencing system performance across different scenarios. The findings provide actionable insights for optimizing biometric systems in diverse applications, ranging from resource-constrained mobile devices to high-security national ID databases.

Biometric systems are integral to modern digital security, with fingerprint-based recognition being a cornerstone of identity verification. While efficient storage and processing are crucial in real-world deployments, challenges such as image degradation and resource limitations threaten system reliability. This research bridges critical gaps by exploring these issues and offering a roadmap for enhancing system performance to meet evolving operational needs.

6.2 Key Findings and Their Significance

Compression Formats

- Findings: Lossless formats (PNG, BMP) preserved minutiae integrity, making them ideal for high-security applications. In contrast, lossy formats like JPEG introduced artifacts that degraded matching accuracy at higher compression levels. Emerging formats like WebP balanced storage efficiency and quality retention, offering potential for consumer-grade applications.

- Significance: This comparative analysis provides a framework for selecting appropriate formats based on application requirements.

Compression Levels

- Findings: High-quality datasets tolerated compression up to 60% with minimal performance degradation, while low-quality datasets experienced significant degradation at just 20%.

- Significance: Identifying these thresholds equips practitioners with guidelines for optimising compression algorithms in varying contexts.

Minutiae Reduction

- Findings: High-quality datasets-maintained reliability with up to 20% minutiae reduction, but low-quality datasets were significantly affected by even a 10% reduction.

- Significance: These results underscore the need for advanced preprocessing strategies to preserve minutiae integrity, especially in low-quality acquisition environments.

6.3 Answering the Research Questions

RQ1: How do different image formats and compression levels affect fingerprint recognition?

- Answer: Lossless formats (e.g., PNG, BMP) preserved recognition accuracy but required significant storage. Lossy formats (e.g., JPEG, WebP) reduced storage demands but introduced artifacts that compromised minutiae extraction, especially at higher compression levels. WebP showed promise as a balanced option for non-critical applications.

RQ2: What are the critical compression thresholds beyond which recognition performance deteriorates?

- Answer: High-quality datasets tolerated compression levels up to 60%, while lowquality datasets exhibited noticeable degradation at just 20%. Beyond these thresholds, recognition reliability decreased significantly, with sharp increases in FAR and FRR.

RQ3: How do high-quality and low-quality datasets differ in their sensitivity to compression?

- Answer: High-quality datasets were resilient to moderate compression and minutiae reduction, maintaining performance reliability. Low-quality datasets were highly sensitive, with significant performance degradation even under minimal compression or minutiae loss.

RQ4: What practical measures can optimise fingerprint recognition performance while minimising storage costs?

- Answer: Use lossless formats for critical applications and employ lossy formats like WebP for resource-constrained systems. Limit compression to 60% for high-quality datasets and avoid aggressive compression for low-quality datasets. Preprocessing techniques, such as noise reduction and resolution enhancement, can mitigate compression effects.

6.4 Practical Implications for Biometric System Design

Enhancing System Robustness

- Recommendations: For high-security applications, prioritize lossless compression formats (e.g., PNG) and high-quality datasets to ensure reliability. Advanced preprocessing techniques, such as adaptive minutiae extraction, can further improve robustness.

Optimising Storage Efficiency

- Recommendations: Employ hybrid compression techniques, combining lossy storage formats with lossless preprocessing. WebP's variable compression options offer a promising balance for mobile and IoT devices.

Improving User Experience

- Recommendations: Inclusive testing and tailored compression criteria across demographic groups ensure equitable and reliable system performance. Minimizing false matches and rejections enhances user trust and satisfaction.

6.5 Contributions to the Field

This research advances the understanding of compression's impact on fingerprint recognition systems and offers several key contributions:

1. Comprehensive Analysis of Compression Formats: Detailed evaluation of traditional (JPEG, PNG) and emerging formats (WebP), providing insights into their applicability.

2. Identification of Compression Thresholds: Defined actionable thresholds for maintaining system reliability under varying compression levels.

3. Focus on Minutiae Reduction: Quantified the effects of minutiae reduction on recognition accuracy, highlighting its critical role in system design.

4. Integration of Ethical Considerations: Addressed fairness and inclusivity concerns arising from compression-induced degradation.

5. Practical Recommendations: Provided actionable strategies for optimizing biometric systems across diverse applications.

6.6 Limitations of the Study

1. Dataset Variability: The study included high- and low-quality datasets but may not generalize to all acquisition conditions. Expanding the dataset to include diverse sources would strengthen the findings.

2. Scope of Analysis: Focused solely on fingerprint-based systems; extending the analysis to multimodal systems (e.g., facial recognition) would offer broader insights.

3. Controlled Conditions: Experiments were conducted in controlled settings, which may not fully reflect real-world scenarios.

4. Emerging Formats: While WebP was explored, formats like AVIF and JPEG XL warrant further investigation.

6.7 Future Research Directions

1. Multimodal Biometric Systems: Investigate the effects of compression on systems combining multiple biometric traits.

2. AI-Driven Enhancements: Leverage AI techniques, such as GANs, to reconstruct degraded fingerprint images and enhance recognition accuracy.

3. Real-World Validation: Conduct field-based experiments to assess system behaviour under practical conditions, such as environmental noise or user variability.

4. Adaptive Algorithms: Develop dynamic algorithms that adjust compression and minutiae extraction processes based on image quality.

5. Privacy-Preserving Techniques: Incorporate secure methods (e.g., homomorphic encryption) for processing compressed biometric data without exposing raw
fingerprints.

6. Demographic Bias Analysis: Explore how compression artifacts affect different demographic groups to ensure fairness and inclusivity.

6.8 Final Reflections

This research addresses critical challenges in fingerprint-based biometric systems, offering a comprehensive understanding of compression's impact on recognition performance. The findings provide a foundation for optimising systems to balance security, usability, and efficiency in diverse applications.

Looking ahead, integrating emerging technologies, ethical considerations, and user-centric design principles will drive the continued advancement of biometric systems. By aligning innovation with inclusivity and reliability, the future of biometric security promises to meet the demands of an interconnected digital world.

6.9 Supplementary Materials

Although the source code for the experiments described in this dissertation is not included as part of the formal submission, additional materials have been provided to support transparency, verification of research methods, and broader understanding of the topic.

A GitHub repository has been created to showcase demonstration scripts, sample data transformations, and relevant tools that reflect the fingerprint recognition concepts and image compression analysis techniques discussed throughout this research. While not representing the exact experimental code used in the study, the repository serves as a conceptual extension to aid readers in understanding the processes involved.

GitHub Repository (Demonstration/Reference):

Furthermore, a YouTube video presentation has been recorded to walk viewers through the objectives, methodology, key findings, and implications of the dissertation. This presentation is intended to provide a clear and accessible explanation of the research for academic, professional, and general audiences interested in biometric systems and the impact of image compression on fingerprint recognition.[9]

YouTube Presentation:

These supplementary materials are intended to enhance the educational value of the research and provide a practical complement to the written thesis. They also reflect a commitment to open sharing of knowledge and scientific communication beyond traditional academic formats.[10]

List of References

[1] N. Dhanalakshmi, S. Goutham Kumar, and Y. P. Sai, “Aadhaar Based Biometric Attendance System Using Wireless Fingerprint Terminals,” 2017, doi: 10.1109/IACC.2017.128.

[2] N. B. Shaik Riyaz and V. Parthipan, “A Novel Prediction Analysing the False Acceptance Rate and False Rejection Rate using CNN Model to Improve the Accuracy for Iris Recognition System for Biometric Security in Clouds Comparing with Traditional Inception Model,” in *Proceedings - 2022 4th International Conference on Advances in Computing, Communication Control and Networking, ICAC3N 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 690–694. doi: 10.1109/ICAC3N56670.2022.10074026.

[3] W. Funk and M. Arnold, “Evaluation of Image Compression Algorithms for Fingerprint and Face Recognition Systems.”

[4] W. Yang, S. Wang, G. Zheng, J. Yang, and C. Valli, “A Privacy-Preserving Lightweight Biometric System for Internet of Things Security,” *IEEE Communications Magazine*, vol. 57, no. 3, pp. 84–89, 2019, doi: 10.1109/MCOM.2019.1800378.

[5] X. Yin, S. Wang, M. Shahzad, and J. Hu, “An IoT-Oriented Privacy-Preserving Fingerprint Authentication System,” *IEEE Internet Things J*, vol. 9, no. 14, pp. 11760–11771, Jul. 2022, doi: 10.1109/JIOT.2021.3131956.

[6] S. Singh, S. Sharma, M. Awasthi, S. Rawat, and Y. Chanti, “Advancements of Emerging Technologies in Biometrics Authentication,” in *2024 IEEE 1st Karachi Section Humanitarian Technology Conference, Khi-HTC 2024*, Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/KHI-HTC60760.2024.10482030.

[7] D. Osorio-Roig, T. Schlett, C. Rathgeb, J. Tapia, and C. Busch, “Exploring Quality Scores for Workload Reduction in Biometric Identification,” in *2022 International Workshop on Biometrics and Forensics, IWBF 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/IWBF55382.2022.9794533.

[8] Y. Zhang *et al.*, “Robust Partial Fingerprint Recognition,” in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, IEEE Computer Society, 2023, pp. 1011–1020. doi: 10.1109/CVPRW59228.2023.00108.

[9] Karthik A H, “Fingerprint Recognition Dissertation,” https://github.com/karthikah0112/fingerprint-recognition-dissertation.

[10] Karthik, “IMPACT OF IMAGE COMPRESSION AND FORMAT CONVERSION ON FINGERPRINT RECOGNITION: EXPLORING SECURITY AND PERFORMANCE TRADE-OFFS ,” https://youtu.be/M3e6xR3-ai4.

[11] C. Watson and C. Wilson, “Effect of image size and compression on one-to-one fingerprint matching,” Gaithersburg, MD, 2005. doi: 10.6028/NIST.IR.7201.

[12] D. Valsesia, G. Coluccia, T. Bianchi, and E. Magli, “Compressed Fingerprint Matching and Camera Identification via Random Projections,” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 7, pp. 1472–1485, Jul. 2015, doi: 10.1109/TIFS.2015.2415461.

[13] R. Raghavendra Kiran, B. Raja, J. Surbiryala, and C. Busch, “A low-cost multimodal Biometric Sensor to capture Finger Vein and Fingerprint.”

[14] N. Karimian, Z. Guo, F. Tehranipoor, D. Woodard, M. Tehranipoor, and D. Forte, “Secure and Reliable Biometric Access Control for Resource-Constrained Systems and IoT,” Mar. 2018, [Online]. Available: http://arxiv.org/abs/1803.09710

[15] *Computer and Computational Sciences (ICCCS), 2015 International Conference on*. IEEE, 2015.

[16] Y. Liu *et al.*, “Class-Incremental Learning for Wireless Device Identification in IoT,” *IEEE Internet Things J*, vol. 8, no. 23, 2021, doi: 10.21227/1bxc-ke87.

[17] A. Mascher-Kampfer, H. Stögner, and A. Uhl, “Comparison of Compression Algorithms’ Impact on Fingerprint and Face Recognition Accuracy.” [Online]. Available: http://www.cipr.rpi.edu/research/SPIHT/

[18] *Information and Communication Technology for Embedded Systems (IC-ICTES), 2015 6th International Conference of*. 2015.

[19] D. Mari, S. Cavasin, S. Milani, and M. Conti, “Effectiveness of learning-based image codecs on fingerprint storage,” Sep. 2024, [Online]. Available: http://arxiv.org/abs/2409.18730

[20] M. Gamassi, V. Piuri, and F. Scotti, “Fingerprint local analysis for high-performance Minutiae extraction.”

[21] F. Tehranipoor, “Towards Implementation of Robust and Low-Cost Security Primitives for Resource-Constrained IoT Devices,” Jun. 2018, [Online]. Available: http://arxiv.org/abs/1806.05332

[22] S. Orandi, “{ { The 2010 NIST Fingerprint The 2010 NIST Fingerprint Compression Study Compression Study,” 2010.

[23] *Proceedings of the 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom) : 17th-19th March 2021, Bharati Vidyapeeth, New Delhi*. IEEE, 2021.

[24] N. Merhav, “False-Accept/False-Reject Trade-Offs for Ensembles of Biometric Authentication Systems,” *IEEE Trans Inf Theory*, vol. 65, no. 8, pp. 4997–5006, Aug. 2019, doi: 10.1109/TIT.2019.2897065.

[25] S. Minocha, K. C. Krishnachalitha, S. Gupta Chancellor, S. R. Alatba, S. S. Pund, and B. S. Alfurhood, “A finger print recognition using CNN Model,” in *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering, ICACITE 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 1490–1494. doi: 10.1109/ICACITE57410.2023.10182507.

[26] S. P. Elias and P. Mythili, “An Improved Algorithm for Fingerprint Compression Based on Sparse Representation,” in *Proceedings - 2015 5th International Conference on Advances in Computing and Communications, ICACC 2015*, Institute of Electrical and Electronics Engineers Inc., Mar. 2016, pp. 417–420. doi: 10.1109/ICACC.2015.84.

[27] R. Bansal, P. Sehgal, and P. Bedi, “Minutiae Extraction from Fingerprint Images-a Review.” [Online]. Available: www.IJCSI.org

[28] N. Veena and S. Thejaswini, “Aadhaar Secure: An Authentication System for Aadhaar Base Citizen Services using Blockchain,” in *2022 4th International Conference on Cognitive Computing and Information Processing, CCIP 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/CCIP57447.2022.10058669.

Appendices:

This section includes screenshots from the experiments conducted using the Neurotechnology VeriFinger SDK tool, showcasing the setup, minutiae analysis, and performance metrics calculations for fingerprint recognition under varying conditions.

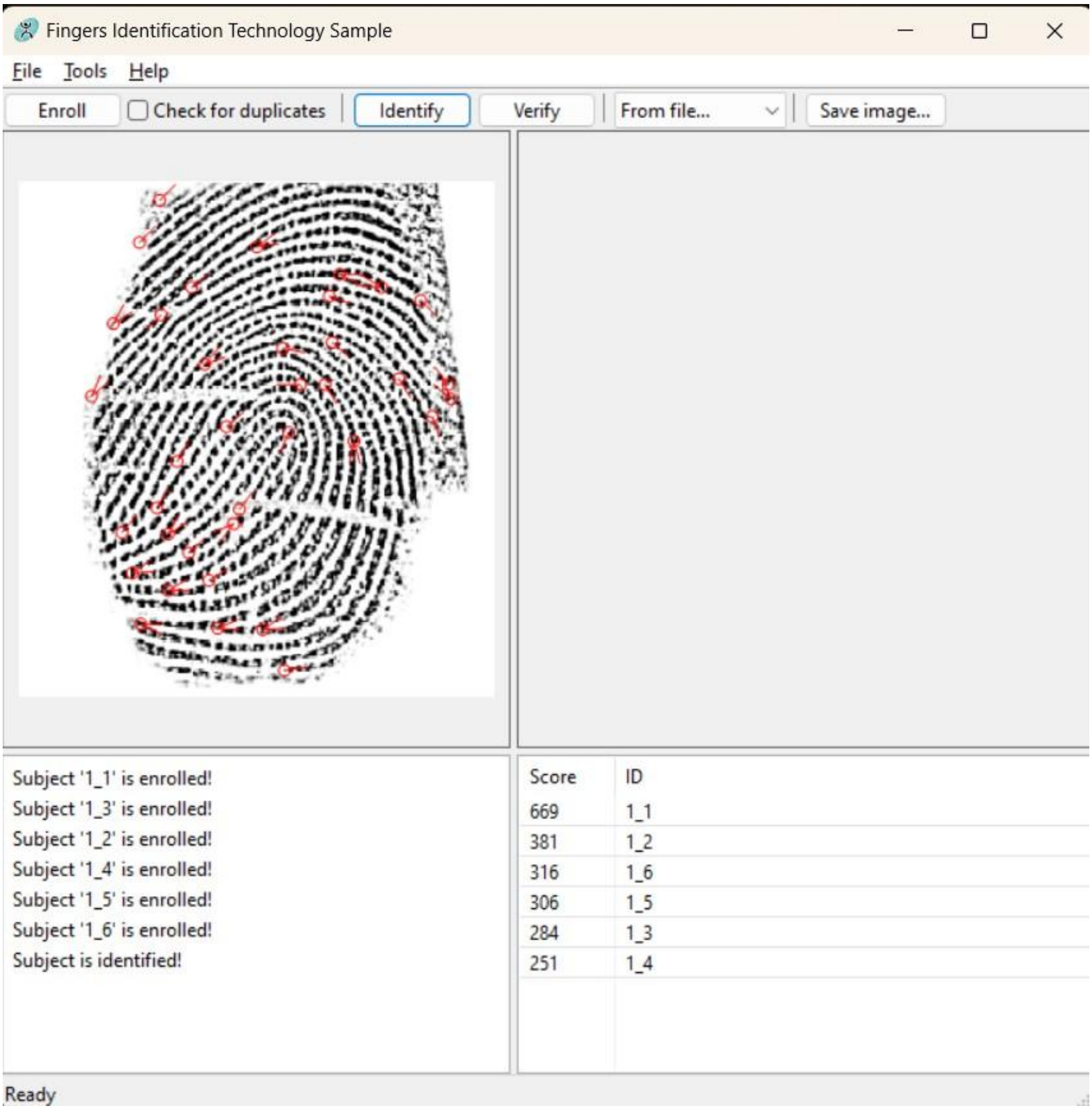

Figure 2 - Fingerprint Matching Scores for a Single Subject's Six Fingers Database

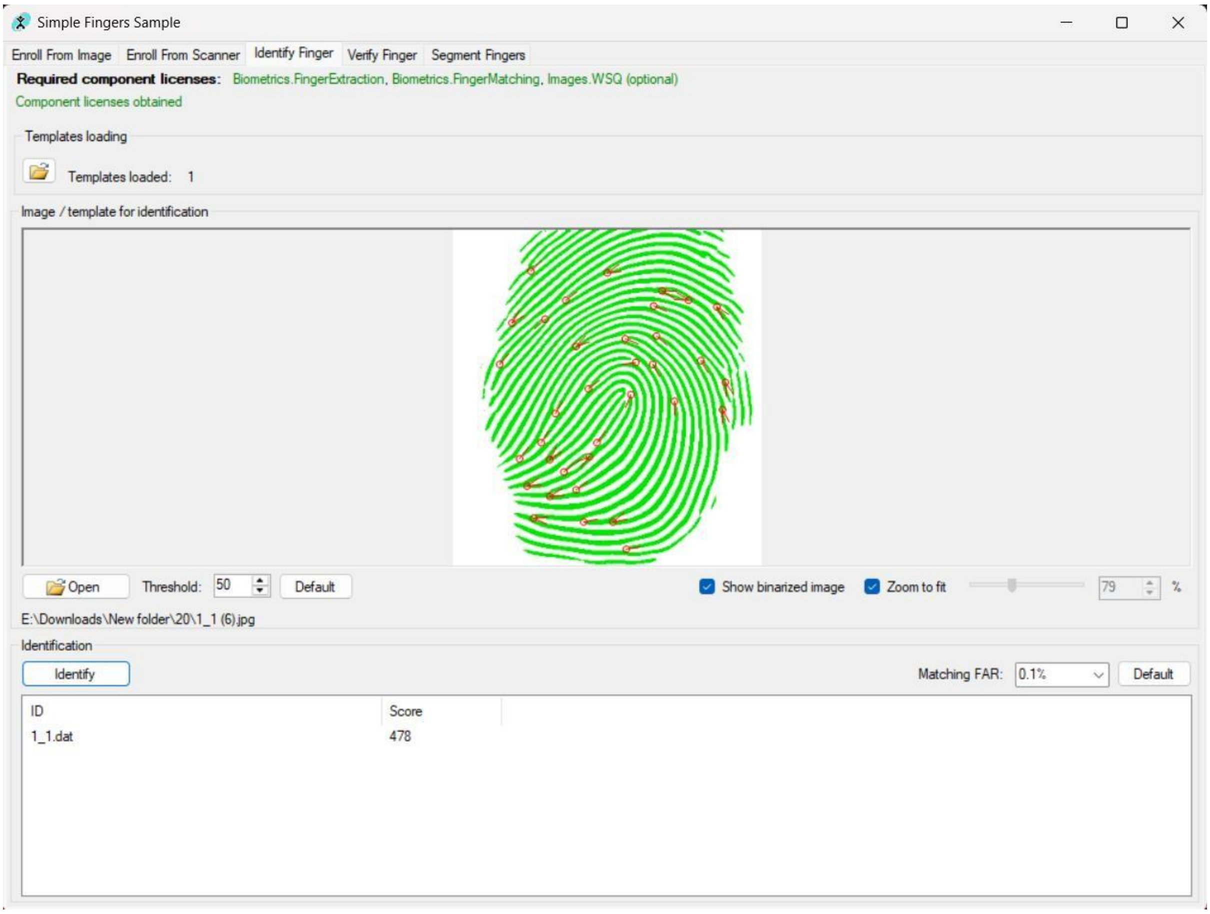

Figure 3 - Fingerprint Matching and Identification with a 50% Threshold Setting

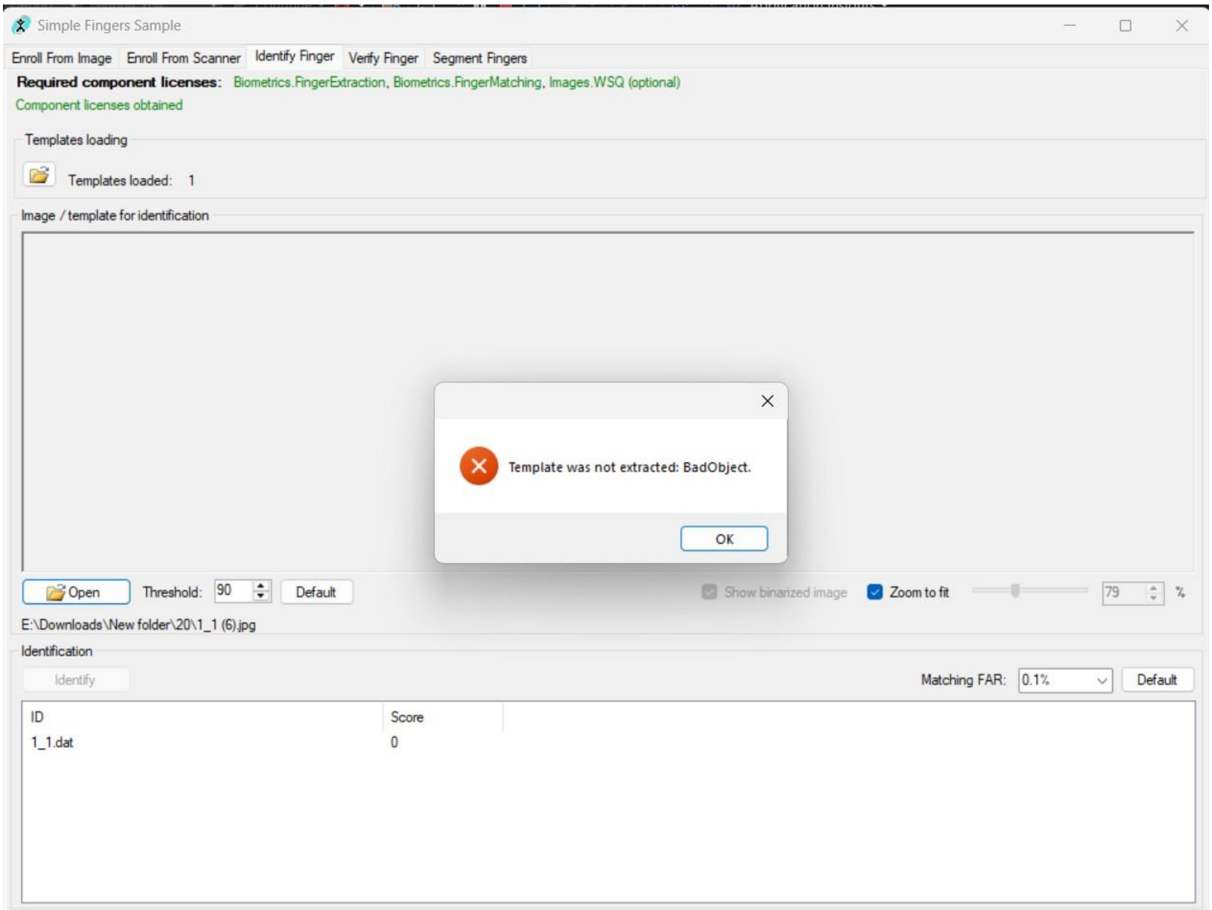

Figure 4 - Fingerprint Template Extraction Failure at 90% Threshold: Error 'BadObject

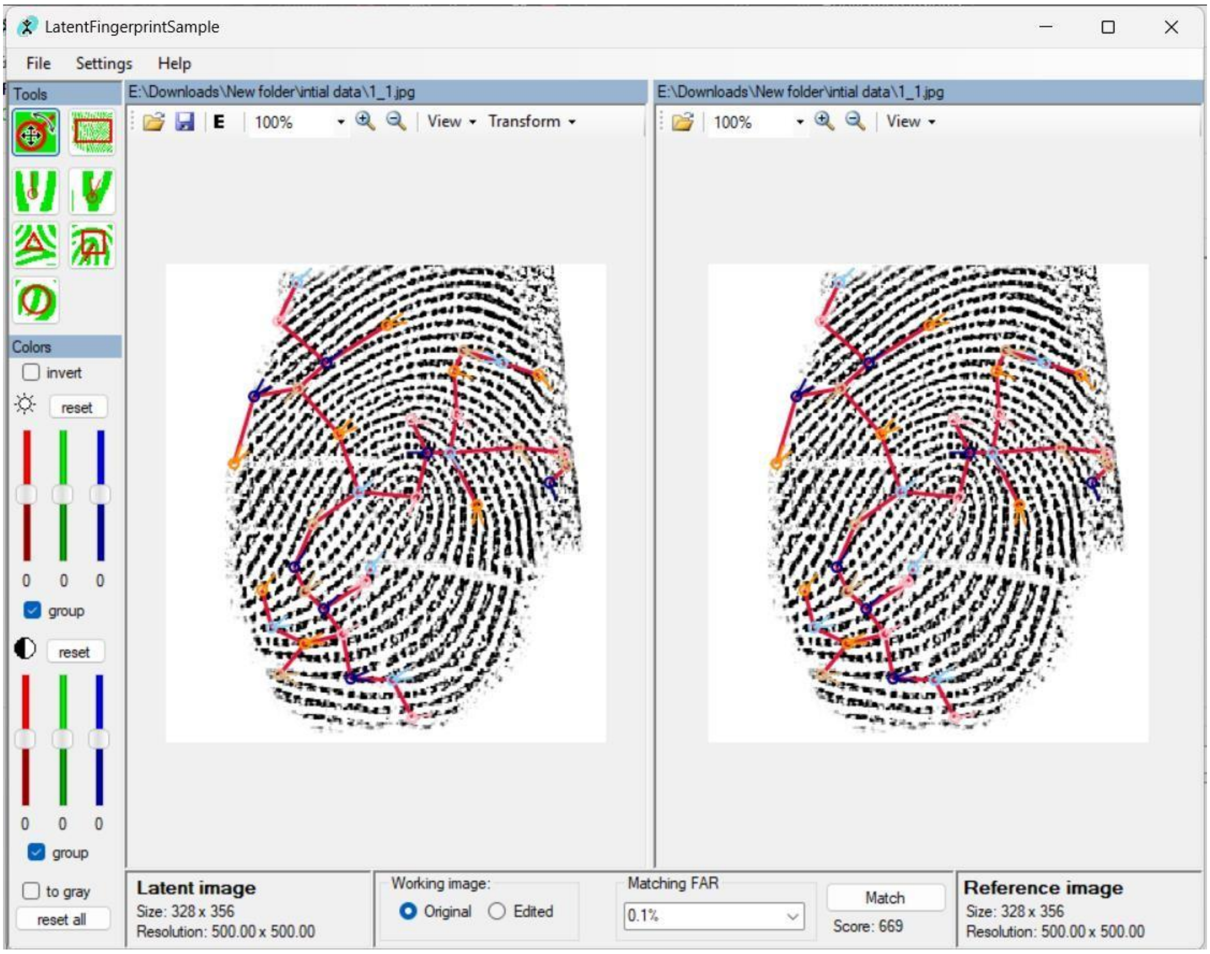

Figure 5 - Fingerprint Matching Results Before Minutiae Reduction with a Score of 669

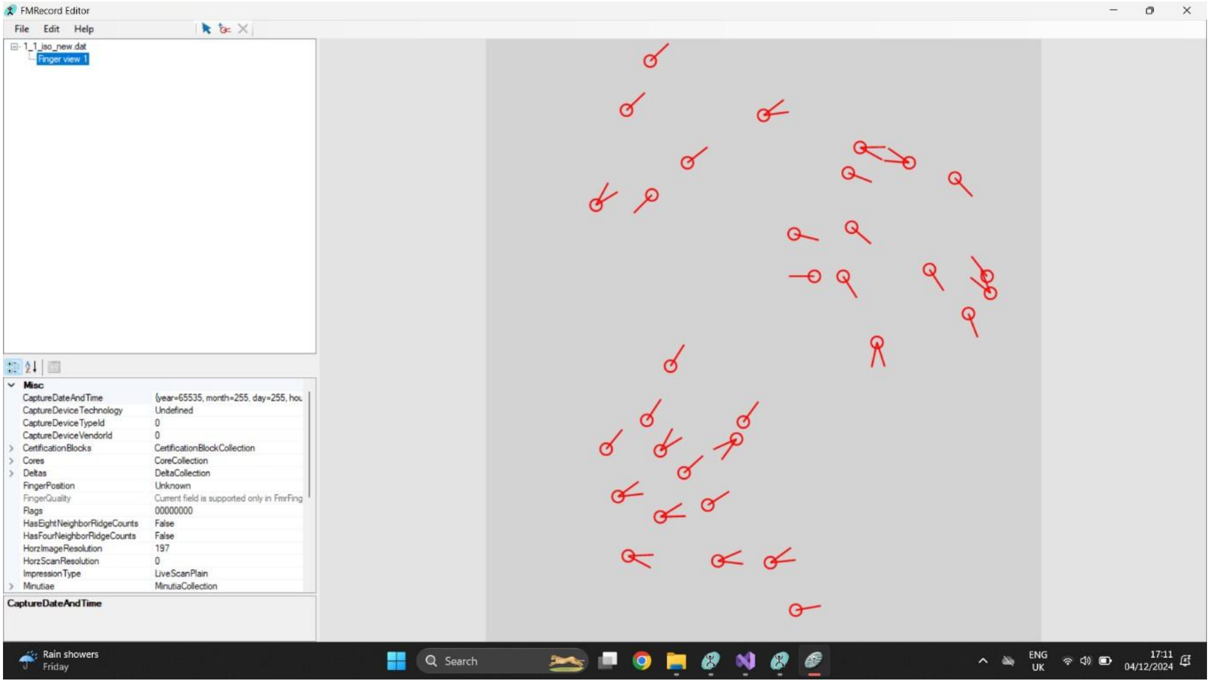

Figure 6 - Minutiae Details Before Reduction in Fingerprint Analysis

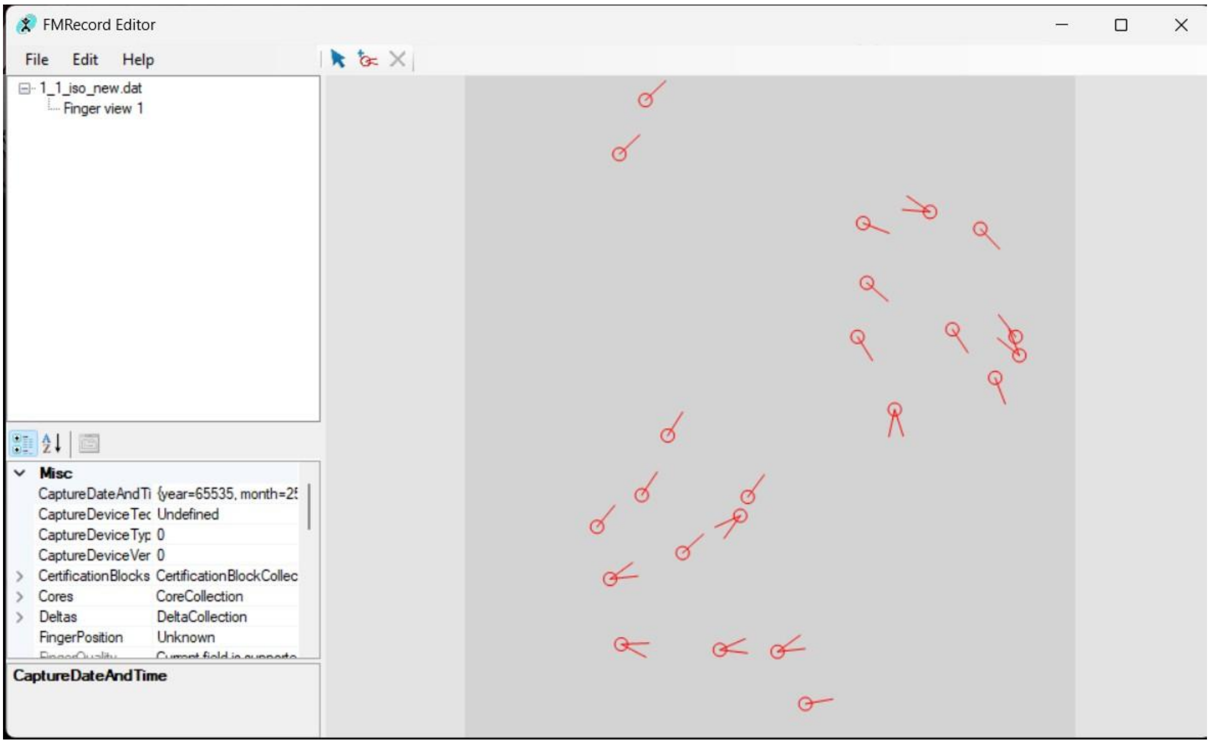

Figure 7 - Minutiae Details After Reduction in Fingerprint Analysis

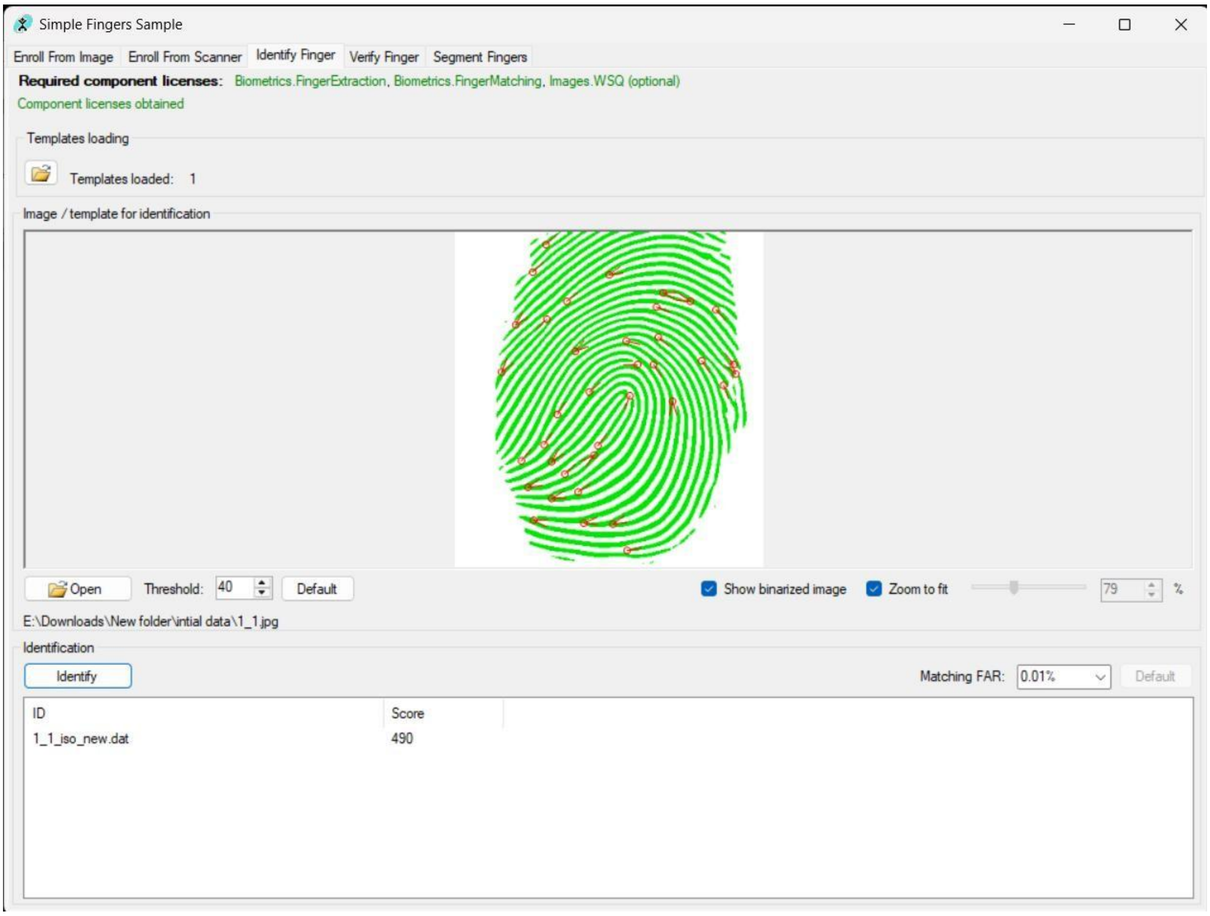

Figure 8 - Fingerprint Matching Results After Minutiae Reduction with a Score of 490