International Journal of Engineering and Techniques - Volume 12 Issue 4, July - August - 2026

Implementation of a Fingerprint Recognition System for Biometric Authentication Using MATLAB

Sandeep Kumar

sandeepkumar60@live.com

Department of Computer Science, GCET, Gurdaspur

Suraj Pal

Ersurajpal8@gmail.com

Department of Computer Science, GCET, Gurdaspur

Abstract

With the rapid growth of modern technology, ensuring secure and reliable identification has become a major necessity. This thesis presents the design and implementation of a fingerprint recognition system using MATLAB for secure and reliable biometric authentication. Traditional security methods such as passwords, PINs, and ID cards are increasingly vulnerable to unauthorized access, duplication, and hacking. To address these limitations, biometric systems offer a more dependable solution by using unique human characteristics. Among various biometric techniques, fingerprint recognition is widely preferred because of its uniqueness, permanence, accuracy, and cost-effectiveness. The proposed system compares two fingerprint images to determine whether they belong to the same individual using digital image processing techniques. The process begins with image acquisition, where fingerprint images are imported into MATLAB for analysis. Since raw images may contain noise and poor contrast, several pre-processing techniques are applied to improve image quality. These include grayscale conversion, resizing, histogram equalization, and noise reduction. Segmentation is then performed to isolate the fingerprint area, followed by binarization to clearly distinguish ridges and valleys. Further processing involves thinning or skeletonization, which reduces ridge thickness to a single pixel for accurate feature extraction. Distinct fingerprint features are then identified and used in the matching process to calculate a similarity score between images. This score is compared with a predefined threshold to verify fingerprint authenticity. If the score exceeds the threshold, the system declares the fingerprint as valid; otherwise, it is marked invalid. Experimental results show that the system successfully differentiates between matching and non-matching fingerprints under normal conditions. Although performance may decline with poor image quality or incorrect finger placement, the system demonstrates the effectiveness of image processing techniques in biometric recognition. This work provides a strong foundation for future enhancements using advanced algorithms and real-time biometric applications.

I. Introduction

In the modern era of rapid technological advancement, the need for secure and reliable identification systems has become increasingly important. With the expansion of digital platforms, online transactions, cloud computing, and interconnected systems, protecting sensitive information and ensuring user authenticity have become critical challenges. Traditional authentication methods such as passwords, Personal Identification Numbers (PINs), and identity cards have been widely used for many years. However, these methods are becoming less effective due to their vulnerability to various forms of attacks, including hacking, phishing, duplication, and unauthorized access. As a result, there is a growing demand for more secure, efficient, and user-friendly authentication mechanisms. Biometric systems have emerged as a powerful solution to address these challenges. A biometric system is a technology that identifies or verifies individuals based on their unique physiological or behavioural characteristics. Unlike traditional methods that rely on what a person knows (such as a password) or what they possess (such as a card), biometric systems rely on who the person is. This fundamental difference makes biometric authentication more secure and reliable, as biometric traits are inherently linked to an individual and cannot be easily shared, lost, or stolen.

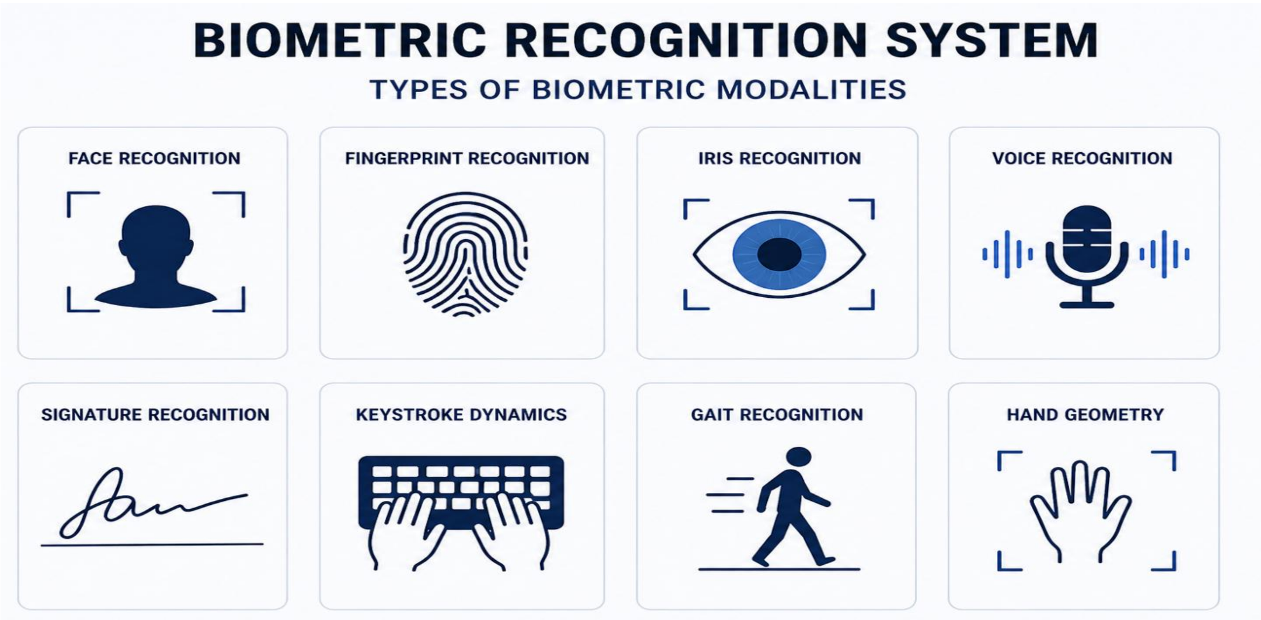

Figure 1.1: Different Types of Biometric Recognition system

During authentication, the system captures a new biometric sample and compares it with the stored template. This comparison is performed using matching algorithms that calculate the similarity between the input and stored data. The system then makes a decision based on a predefined threshold. If the similarity score exceeds the threshold, the identity is verified; otherwise, access is denied. Biometric systems can operate in two modes: verification and identification. In verification mode the system checks whether the input matches a specific stored template. In identification mode the system compares the input with all templates in the database to determine the identity of the individual. The adoption of biometric systems has increased significantly in recent years due to their numerous advantages. They offer a high level of security, as biometric traits are difficult to replicate or forge. They also provide convenience, as users do not need to remember passwords or carry physical tokens. Biometric systems are widely used in various applications, including mobile device security, banking and financial services, healthcare systems, law enforcement, and border control. The integration of biometric authentication with modern technologies such as artificial intelligence and the Internet of Things (IoT) has further enhanced their capabilities and expanded their applications.

1.1 Fingerprint Recognition

Among the various types of biometric systems, fingerprint recognition is one of the most widely used and well-established methods. Fingerprint recognition has been used for over a century in forensic science and has become a standard method for personal identification due to its reliability and accuracy. A fingerprint is formed by the patterns of ridges and valleys present on the surface of a human finger. These patterns are unique for every individual and remain unchanged throughout a person's lifetime, except in cases of severe injury. Even identical twins, who share the same genetic makeup, have different fingerprint patterns, highlighting the uniqueness of fingerprints. Fingerprint patterns can be broadly classified into three main types: loops, whorls, and arches. Loops are the most common pattern, where ridges enter from one side and exit from the same side. Whorls form circular or spiral patterns, while arches have ridges that flow from one side to the other without looping. In addition to these global patterns, fingerprint recognition systems rely on local features known as minutiae points. Minutiae points include ridge endings, where a ridge terminates, and bifurcations, where a ridge splits into two branches. The position, orientation, and distribution of these minutiae points form a unique signature for each fingerprint. The process of fingerprint recognition involves several stages. The first stage is image acquisition, where a fingerprint scanner captures the fingerprint image. The quality of the captured image is crucial for accurate recognition. The next stage is pre-processing, which includes converting the image to grayscale, enhancing contrast, and removing noise. Image enhancement techniques are applied to improve the visibility of ridges and valleys. The enhanced image is then converted into a binary image through a process called binarization, where ridges are represented as black pixels and the background as white pixels.

In this Thesis, a fingerprint recognition system is developed using MATLAB, focusing on fundamental image processing techniques. The system demonstrates the complete process of fingerprint recognition, including image acquisition, pre-processing, enhancement, binarization, edge detection, feature extraction, and matching. By implementing these steps, the project provides a clear understanding of how biometric systems operate in practice and highlights the importance of image processing in improving recognition accuracy.

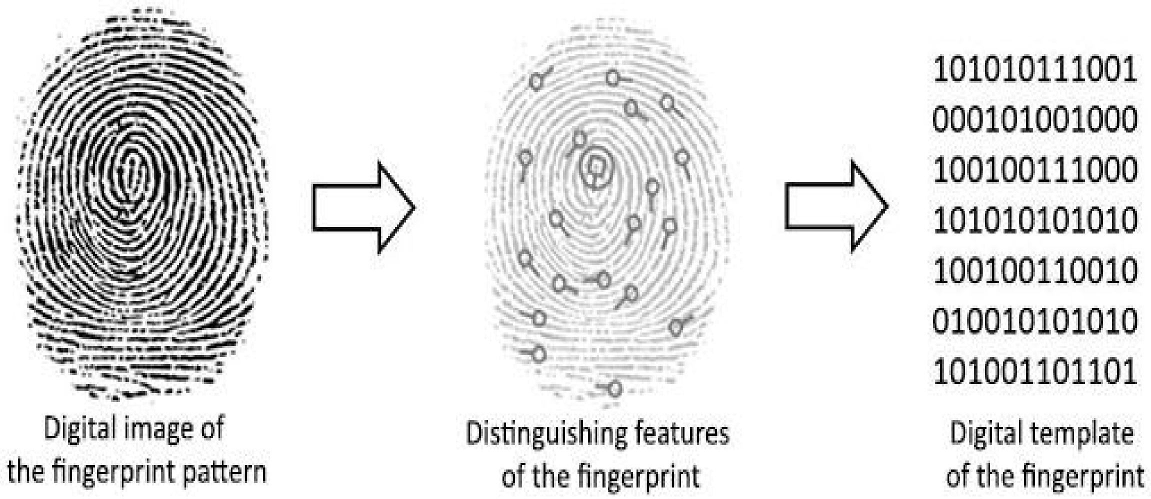

Figure 1.2: Fingerprint Recognition Process

1.2 Face Recognition

Face recognition is a widely used biometric technology that identifies or verifies an individual based on their facial features. It is considered one of the most convenient and non-intrusive biometric methods, as it does not require physical contact with any device. This technology analyses various facial characteristics such as the distance between the eyes, nose shape, jawline, cheekbone structure, and overall facial geometry to uniquely identify a person

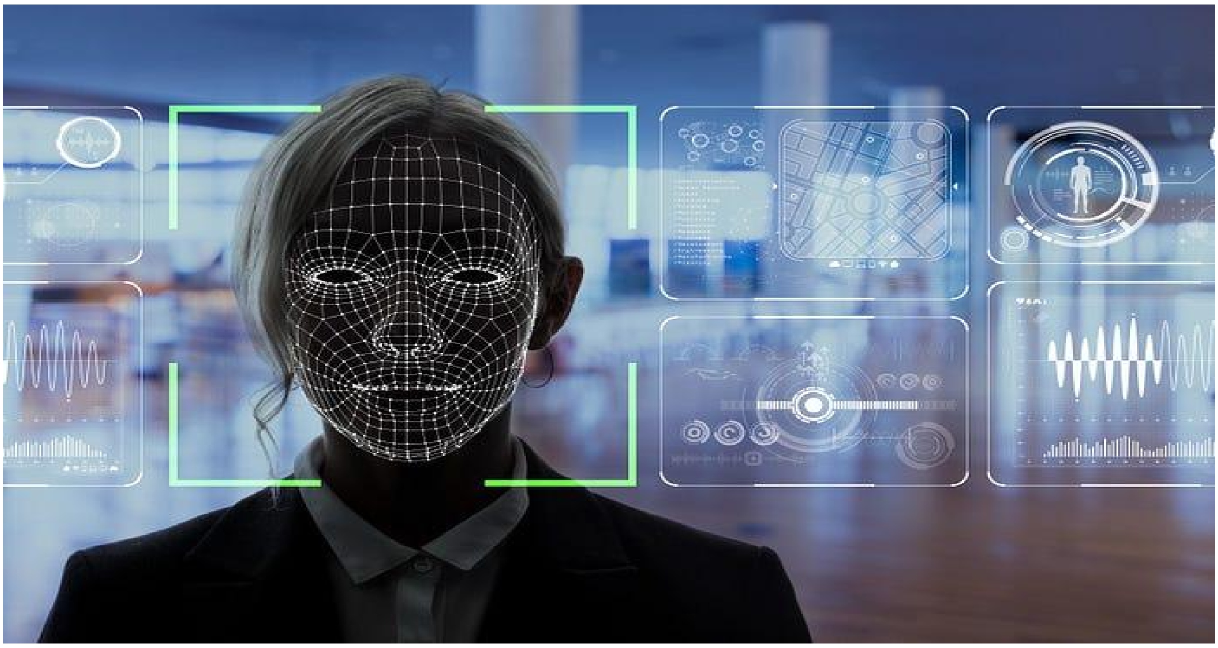

Figure 1.3: Face Recognition system

During authentication, a new facial image is captured and processed in a similar manner. The extracted features are compared with stored templates using matching algorithms. If the similarity score exceeds a predefined threshold, the identity is confirmed.

1.3 Iris Recognition

Iris recognition is a highly accurate biometric identification method that uses the unique patterns present in the coloured part of the human eye, known as the iris. These patterns are extremely complex and remain stable throughout a person's lifetime, making iris recognition one of the most reliable biometric techniques. The iris contains intricate patterns such as rings, furrows, freckles, and crypts that are unique to each individual. Even identical twins have different iris patterns, which highlights the uniqueness of this biometric trait. Additionally, the iris is protected behind the cornea, making it less susceptible to damage or environmental effects.

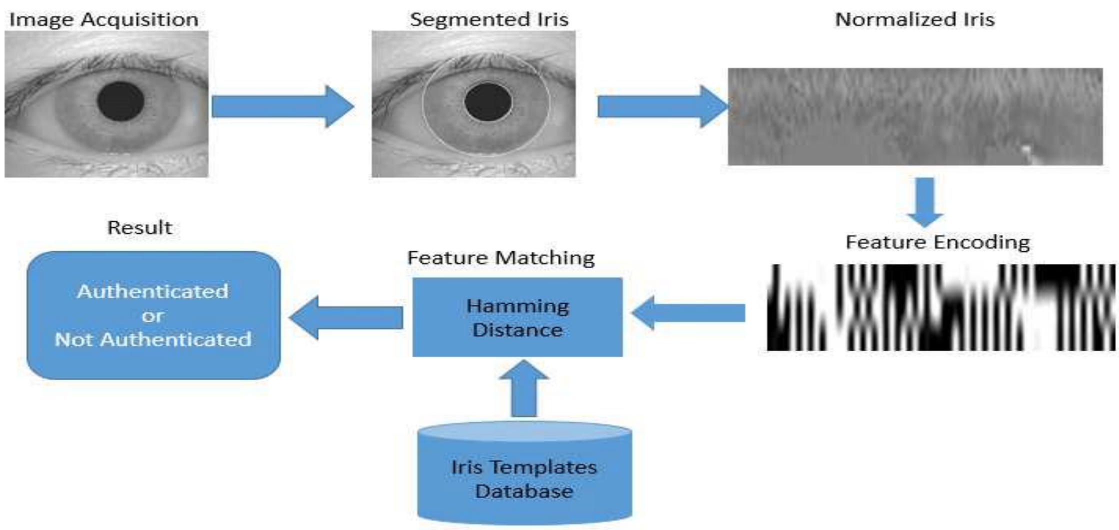

Figure 1.4: IRIS Recognition system

The process of iris recognition begins with image acquisition using a specialized camera, often equipped with infrared illumination. Infrared light helps capture clear images of the iris without causing discomfort to the user. Once the image is captured, it undergoes pre-processing to enhance quality and remove noise. These features are encoded into a digital template and stored in a database. During authentication, a new iris image is captured and compared with stored templates using matching algorithms. It is highly resistant to forgery and spoofing, as replicating iris patterns is extremely difficult. The technology is also fast and efficient, providing quick authentication results. This biometric method is widely used in high-security environments such as airports, border control systems, military facilities, and government institutions. It is also used in national identification programs in some countries.

1.4 Retina Recognition

Retina recognition is a biometric identification technique that relies on the unique pattern of blood vessels located at the back of the human eye, known as the retina. It is considered one of the most secure and accurate biometric methods due to the complexity and uniqueness of retinal patterns. These patterns are formed naturally and remain stable throughout a person's lifetime, making them highly reliable for identification purposes.

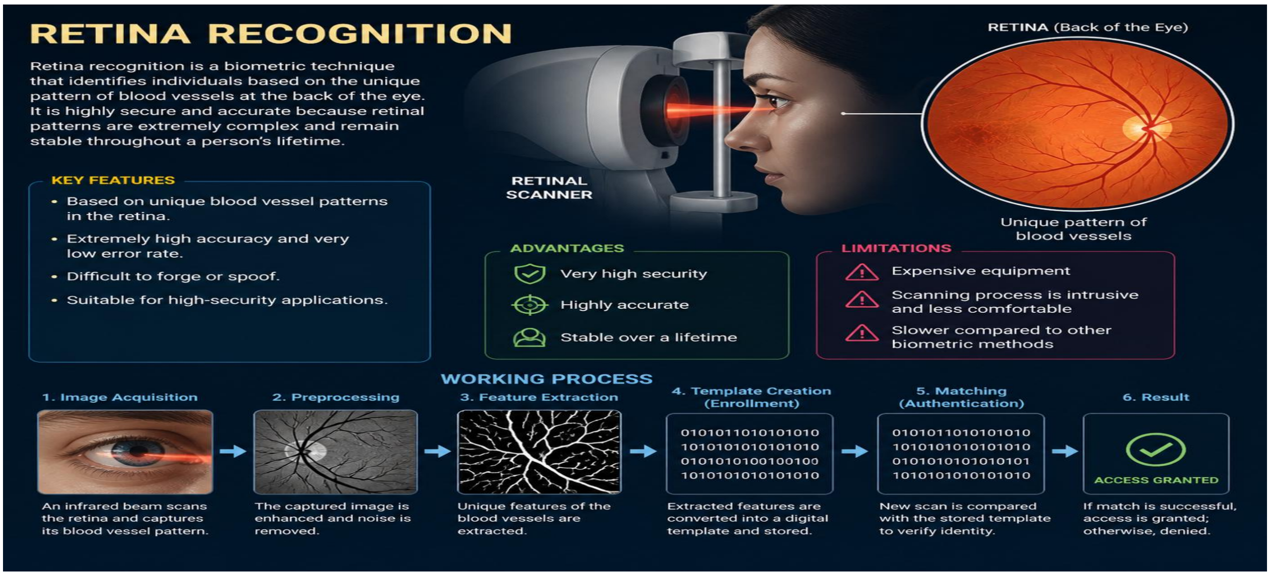

Figure 1.5: Retina Recognition system

The retina consists of a network of blood vessels that supply oxygen and nutrients to the eye. The arrangement of these blood vessels is unique to each individual, even among identical twins. Since the retina is located internally within the eye, it is well protected from external damage and environmental changes. This makes retina recognition highly resistant to forgery and spoofing attempts. The process of retina recognition begins with image acquisition using a specialized retinal scanner. The user is required to look into the device while a low-intensity infrared beam scans the eye. The infrared light is reflected by the blood vessels in the retina, allowing the system to capture a detailed image of the vascular pattern. This process requires precise alignment of the eye with the scanner, which can sometimes be challenging for users.

1.5 Hand Geometry

Hand geometry is a biometric identification method that measures the physical characteristics of a person's hand, including its size, shape, length, width, and thickness. Unlike other biometric systems that rely on highly detailed features, hand geometry focuses on general structural measurements, making it a simple and efficient method for identity verification. The hand geometry recognition process begins with image acquisition using a hand geometry scanner. The user places their hand on a flat surface within the device, aligning it with predefined guides or pegs to ensure consistent positioning. A camera or sensor then captures an image of the hand from different angles. Once the image is captured, the system performs pre-processing to enhance image quality and remove any noise or distortions. The next step is feature extraction, where various measurements of the hand are calculated. These may include finger length, finger width, palm size, and the distances between joints. These measurements are then converted into a numerical template and stored in a database.

Figure 1.6: Hand Geometry Recognition system

During authentication, the user places their hand on the scanner again, and the system captures a new image. The extracted features are compared with stored templates to determine a match. If the similarity is within an acceptable range, access is granted.

1.6 Voice Recognition

Voice recognition is a behavioural biometric system that identifies individuals based on their unique speech patterns. It analyses characteristics such as tone, pitch, frequency, and speaking style to verify identity. This method is widely used due to its convenience and ability to perform authentication remotely. The process of voice recognition begins with recording a voice sample using a microphone. The system captures the user's speech and converts it into a digital signal. This signal is then processed to remove background noise and enhance clarity. Feature extraction is performed to identify unique characteristics of the voice. These features may include pitch, cadence, pronunciation patterns, and spectral features. The extracted data is converted into a digital template and stored in a database.

Figure 1.7: Voice Recognition Biometric system

During authentication, a new voice sample is recorded and compared with stored templates. Matching algorithms analyse the similarity between the input and stored voice patterns. If the similarity exceeds a predefined threshold, the identity is verified. Voice recognition systems can be text-dependent, where the user speaks a specific phrase, or text-independent, where the system analyses natural speech. This flexibility makes voice recognition suitable for various applications.

2. Limitations of Traditional Authentication Methods

Traditional authentication methods depend on either:

- **Knowledge-based factors** (passwords, PINs)
- **Possession-based factors** (cards, tokens)

These approaches have several weaknesses:

2.1 Passwords

Passwords are the most commonly used authentication method due to their simplicity and ease of implementation. However, they are highly vulnerable if not managed properly. Many users tend to create weak passwords that are easy to remember, such as simple words, numbers, or personal information. Additionally, users often reuse the same password across multiple platforms, increasing the risk of multiple accounts being compromised if one password is exposed. Attackers exploit these weaknesses using techniques such as brute force attacks, where all possible combinations are tried, dictionary attacks using common password lists, and phishing attacks that trick users into revealing their credentials. As a result, passwords alone are no longer considered a secure method of authentication.

2.2 PINs (Personal Identification Numbers)

PINs are short numerical codes typically used for secure access in systems like ATMs and mobile devices. While they offer simplicity and speed, they suffer from significant limitations. Due to their short length (usually 4–6 digits), the number of possible combinations is limited, making them easier to guess or crack. PINs are also vulnerable to **shoulder surfing**, where an attacker observes the user entering the code. In many cases, users select predictable PINs such as birth dates or repeated digits, further weakening security. Therefore, PIN-based systems provide only a basic level of protection.

2.3 ID Cards

Identification cards are widely used in offices, educational institutions, and secure facilities. They function as proof of identity but rely on possession rather than actual identity verification. ID cards can be lost, stolen, duplicated, or forged. If an unauthorized person gains access to someone else's card, they may be able to enter restricted areas without detection. Unless combined with additional authentication methods such as PINs or biometrics, ID cards alone cannot guarantee secure access.

2.4 Security Tokens

Security tokens are physical or digital devices used to generate authentication codes or provide access credentials. They are considered more secure than passwords because they add an extra layer of authentication. However, tokens also have limitations. They can be lost, stolen, or damaged, making them unavailable to the rightful user. In some cases, tokens may be targeted by hackers through malware or interception techniques. Managing and distributing tokens can also be costly and inconvenient, especially in large organizations.

3 Overall Limitation of Traditional Methods

All traditional authentication methods share a common weakness: they are **external to the user**. This means they depend on something the user knows (password/PIN) or possesses (card/token), rather than something inherent to the individual. As a result, these methods can be easily transferred, shared, stolen, or duplicated, making them less reliable in ensuring true identity verification.

II. Literature Survey

[1] Deng et al. (2026) Deep learning has significantly transformed biometric recognition systems, particularly in face recognition where accuracy and robustness are essential. This study focuses on advanced architectures that combine convolutional neural networks with transformer-based attention mechanisms to improve feature extraction. Traditional face recognition systems faced challenges such as variations in illumination, pose, and facial expressions, which affected system performance. The proposed model addresses these issues by incorporating attention mechanisms that allow the system to focus on important facial regions while ignoring irrelevant background information. Large-scale datasets were used to train the model, improving its ability to generalize across diverse conditions. Experimental results showed that the system achieved higher accuracy compared to traditional CNN-based models, especially in unconstrained environments.

[2] Kakade et al. (2026) This study presents a comprehensive analysis of modern biometric authentication systems, focusing on the importance of multimodal approaches. It explains that unimodal systems often suffer from limitations such as noise, spoofing attacks, and lack of universality, which reduce reliability. To overcome these challenges, the study proposes combining multiple biometric traits such as fingerprint, face, and iris recognition. Artificial intelligence techniques, including convolutional neural networks, are used to enhance feature extraction and matching accuracy.

[3] Rjab et al. (2026) This study explores biometric authentication systems integrated with blockchain technology to enhance security and privacy. Traditional centralized biometric systems are vulnerable to data breaches and single points of failure. The proposed framework uses decentralized storage of biometric templates, ensuring improved data protection. The system integrates multiple biometric modalities such as fingerprint, face, and iris recognition to improve accuracy. Cryptographic techniques are applied to secure sensitive data, preventing unauthorized access. Experimental results show that the system is resistant to spoofing and replay attacks.

[4] Ma et al. (2026) This study focuses on gait recognition as a biometric method for identifying individuals based on their walking patterns. The research uses deep learning techniques, particularly convolutional neural networks, to extract motion-based features from video sequences. The system analyzes parameters such as stride length, walking speed, and posture to create unique gait signatures. The study highlights that gait recognition is a non-intrusive method, as it does not require physical contact or user cooperation. Experimental results demonstrate that the system performs well under varying conditions such as low resolution and occlusion. However, the study also identifies limitations such as sensitivity to clothing variations and walking speed changes. Despite these challenges, the research concludes that gait recognition is a valuable biometric method for surveillance applications, especially when combined with other biometric techniques.

[5] Gopal Varma et al. (2025) This study proposes a multimodal biometric authentication system integrating fingerprint, face, and voice recognition using artificial intelligence. The system uses machine learning algorithms for feature extraction and classification, improving accuracy and reliability. Each biometric modality contributes unique information, allowing the system to compensate for errors in individual traits. The fingerprint module extracts minutiae points, the face recognition module analyses facial features, and the voice module processes speech characteristics such as tone and frequency. Experimental results show a significant reduction in error rates compared to unimodal systems.

[6] Gimba et al. (2025) This study presents a deep learning-based multimodal biometric authentication system that combines face and fingerprint recognition to enhance accuracy and reliability. Traditional biometric systems rely on manual feature extraction, which can be time-consuming and less effective in complex scenarios. To overcome this limitation, the proposed system utilizes convolutional neural networks to automatically extract features from biometric data. The fingerprint module focuses on identifying minutiae points such as ridge endings and bifurcations, while the face recognition module analyses facial structures and key landmarks

[7] Garg et al. (2025) This study introduces a multimodal biometric system that combines fingerprint, iris, and electrocardiogram signals to enhance authentication security. The research highlights that while fingerprint and iris recognition provide high accuracy, the inclusion of ECG signals adds an additional layer of security. The system uses machine learning algorithms for feature extraction and classification. Experimental results show that the system achieves accuracy close to 99%. The study concludes that multimodal systems provide superior performance and are ideal for high-security applications.

[8] Al-Refai et al. (2025) This study provides a comparative analysis of various biometric modalities including fingerprint, face, and iris recognition. The findings indicate that face recognition has improved significantly with deep learning, while fingerprint systems remain vulnerable to spoofing. Iris recognition is highly accurate but expensive. The study concludes that multimodal systems provide

III. Research Gap

In the base papers, fingerprint recognition techniques are mostly discussed as theoretical concepts or traditional matching approaches based on minutiae extraction. However, these studies often lack detailed practical implementation, especially in terms of automation, accuracy improvement, and real-time performance using modern tools like MATLAB.

While existing research highlights fingerprint recognition as a reliable biometric method, it does not fully address:

1. **Real-World Implementation:**
   Limited development of fully automated systems using MATLAB for fingerprint preprocessing, feature extraction, and matching.
2. **Image Quality Issues:**
   Insufficient focus on handling poor-quality fingerprint images caused by noise, distortion, dryness, or improper finger placement.
3. **Advanced Processing Techniques:**
   Minimal use of modern image enhancement techniques such as filtering, binarization, thinning, and edge detection to improve recognition accuracy.
4. **Performance Optimization:**
   Lack of efficient algorithms for fast and accurate fingerprint matching suitable for real-time applications.

This research addresses these gaps by developing **a** MATLAB-based fingerprint recognition system that incorporates image enhancement, binarization, feature extraction, and matching techniques. The system improves accuracy and reliability while demonstrating practical implementation.

3.1 Problem Definition

Fingerprint recognition is one of the most widely used biometric identification methods due to its uniqueness and permanence. However, developing an accurate fingerprint recognition system remains a challenge due to various factors affecting image quality and feature extraction.

Fingerprint images captured using sensors may suffer from issues such as noise, distortion, low contrast, and improper finger placement. These issues make it difficult to accurately extract important features such as minutiae points (ridge endings and bifurcations), which are essential for matching.

Traditional fingerprint recognition methods often rely on simple image processing techniques, which may not perform well under varying conditions. In addition, variations in finger pressure, rotation, and environmental conditions can lead to mismatches or reduced accuracy.

Therefore, there is a need to develop a robust fingerprint recognition system that:

- Enhances image quality
- Accurately extracts features
- Performs reliable matching
- Works efficiently in real-world conditions

This research aims to solve these challenges by implementing a MATLAB-based fingerprint **recognition system** using advanced image processing techniques.

3.2 Objectives

1. Enhance the fingerprint image to improve ridge visibility.
2. Convert grayscale image to binary image using thresholding.
3. Apply noise removal and filtering techniques.
4. Perform thinning to reduce ridge thickness.
5. Extract minutiae points (ridge endings and bifurcations).
6. Match fingerprint features using correlation or pattern matching.
7. Evaluate system performance and accuracy using MATLAB.

IV. Experimental Setup

4.1 Introduction

Simulation can be defined to show the eventual real behaviour of the selected system model. It is used for performance optimization on the basis of creating a model of the system in order to gain insight into their functioning. We can predict the estimation and assumption of the real system by using simulation results. Simulator, which is created by MathWorks, is one of the most dynamic and resourceful applications. It is basically a simulation platform that incorporates MATLAB and a model design system. It features a fantastic environment for programming, simulation, and modelling. Multi-domain dynamical systems can be analysed with this software by a variety of professions. Its principal interface consists of a graphical block diagramming tool and a collection of block libraries that may be customized. Moreover, it has amazing features such as product style control, traceability criteria, and application coverage analysis, among others. You will learn more about it in this article. Let's get this party started.

4.2 Simulator

In this thesis, MATLAB add-on product with a user-friendly, graphically appealing interface used for simulation programming and modelling. This tool allows any user to quickly and simply create virtual prototypes for exploring diversified design concepts at any degree of detail with minimum effort. You do not need any previous expertise to use this platform. Simply utilise a vast collection of preconfigured blocks to build graphical models of systems using drag-and-drop mouse operations to get started. It may represent nonlinear and linear systems in continuous-time, sampled time, or a combination of the two.

4.3 MATLAB Features

4.3.1 Introduction to MATLAB Simulator

In recent years, MATLAB has emerged as a powerful tool for image processing and enhancement due to its comprehensive set of functionalities and user-friendly environment. This section introduces the MATLAB simulator developed for the purpose of image enhancement, highlighting its key features and capabilities.

4.3.2 Purpose and Scope

The MATLAB simulator discussed herein is designed to facilitate research and experimentation in the field of detects Glaucoma. It serves as a platform to implement and evaluate various algorithms and techniques aimed at improving the visual quality and interpretability of digital images.

4.3.3 Application Areas

The fingerprint recognition system can be used in:

- Security and access control systems
- Mobile device authentication
- Attendance systems
- Banking and financial services
- Law enforcement and forensic analysis

4.4 Methodology

The Research work is carried out in several stages, starting from problem identification to implementation in MATLAB.

The system follows these steps:

1. Image acquisition of fingerprint
2. Pre-processing
3. Noise removal and filtering
4. Binarization of image
5. Thinning of ridges
6. Feature extraction (minutiae detection)
7. Matching with stored templates

Each step is implemented in MATLAB using image processing techniques. The system improves fingerprint clarity and enables accurate matching. The methodology ensures that the fingerprint recognition system is efficient, reliable, and suitable for real-world applications.

The work was carried out through a systematic sequence of stages, starting from problem identification and progressing to implementation using MATLAB. Initially, fingerprint images were acquired from a standard dataset or sensor and used as input for the system. These images often contained noise and variations, so pre-processing techniques such as grayscale conversion and normalization were applied to enhance image quality. Following this, noise removal and filtering methods were implemented to eliminate distortions and improve ridge visibility

V. Results

The results obtained from the implemented fingerprint recognition system show that the developed system is effective in accurately identifying and matching fingerprint images. The system was tested using multiple fingerprint samples under different conditions to evaluate its performance and reliability. After pre-processing, the fingerprint images showed noticeable improvement in clarity, with enhanced ridge structures and reduced noise. The binarization process successfully separated ridges from the background, while the thinning process reduced ridge thickness to a single pixel, making the structure suitable for feature extraction.

5.1 Image Enhancement

After selecting the dataset and acquiring the fingerprint images, image enhancement techniques were applied to improve the overall quality and clarity of the fingerprint patterns. The raw fingerprint images often contain issues such as low contrast, uneven illumination, and unclear ridge structures, which can affect the accuracy of further processing steps. To address these problems, enhancement methods were used to highlight ridge and valley structures, making them more distinguishable. Techniques such as contrast adjustment, histogram equalization, and filtering were applied to enhance the visibility of important features. These operations helped in improving the sharpness and definition of ridges while suppressing background noise. As a result, the enhanced images provided a better foundation for subsequent steps such as binarization, thinning, and feature extraction. The use of MATLAB’s image processing functions made it easier to implement and visualize these enhancements. Overall, image enhancement played a crucial role in improving the reliability and accuracy of the fingerprint recognition system.

Figure 5.1: Before and After Image Enhancement

Figure 6.2 illustrates the effect of noise removal on the fingerprint images used in the system. The original image (before processing) contains various types of noise such as small speckles, uneven intensity, and background disturbances, which can interfere with accurate feature extraction. After applying a noise removal technique—such as median filtering—the image becomes smoother and cleaner while preserving important ridge patterns. This enhancement reduces unwanted variations and improves the clarity of fingerprint structures, making subsequent steps like binarization, skeletonization, and feature matching more reliable. Overall, noise removal plays a crucial role in improving the accuracy and robustness of the fingerprint recognition system.

Figure 5.2 Image Before and After Noise Removal

Figure 5.3 presents the results of the segmentation and binarization processes applied to the fingerprint images. In the segmentation stage, the region containing the actual fingerprint is separated from the background, removing unnecessary areas and focusing only on the region of interest. This helps in reducing computational complexity and avoids interference from irrelevant pixels. Following segmentation, binarization is performed, where the image is converted into a binary format consisting of only two intensity levels—foreground (ridges) and background (valleys). This transformation enhances the visibility of ridge structures and simplifies further processing steps such as skeletonization and feature extraction. Overall, segmentation and binarization are essential for improving the clarity and accuracy of fingerprint analysis.

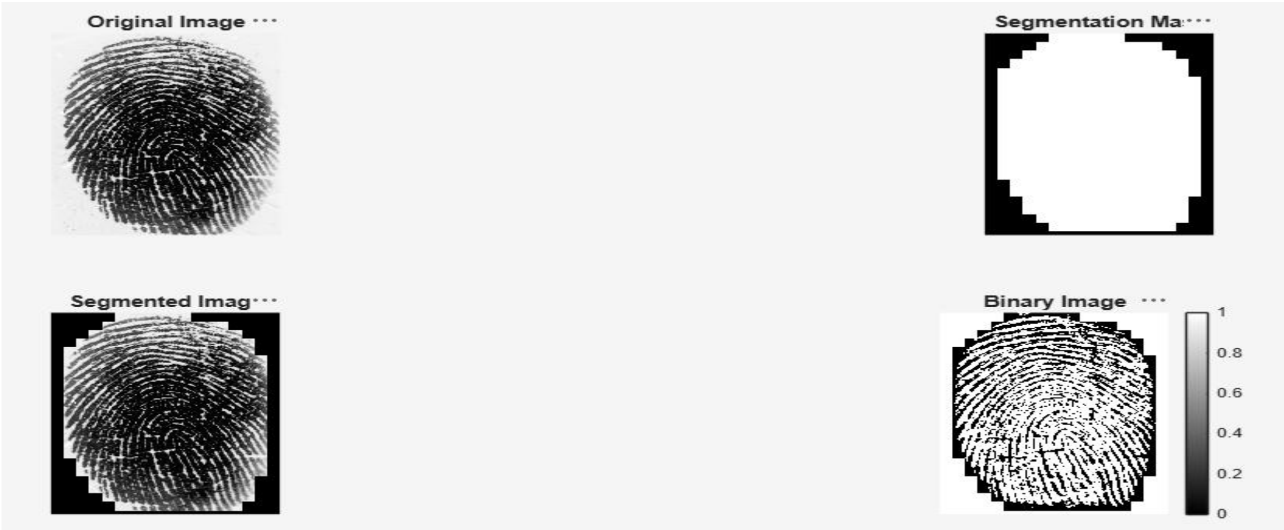

Figure 5.3: Image Segmented and Binarization

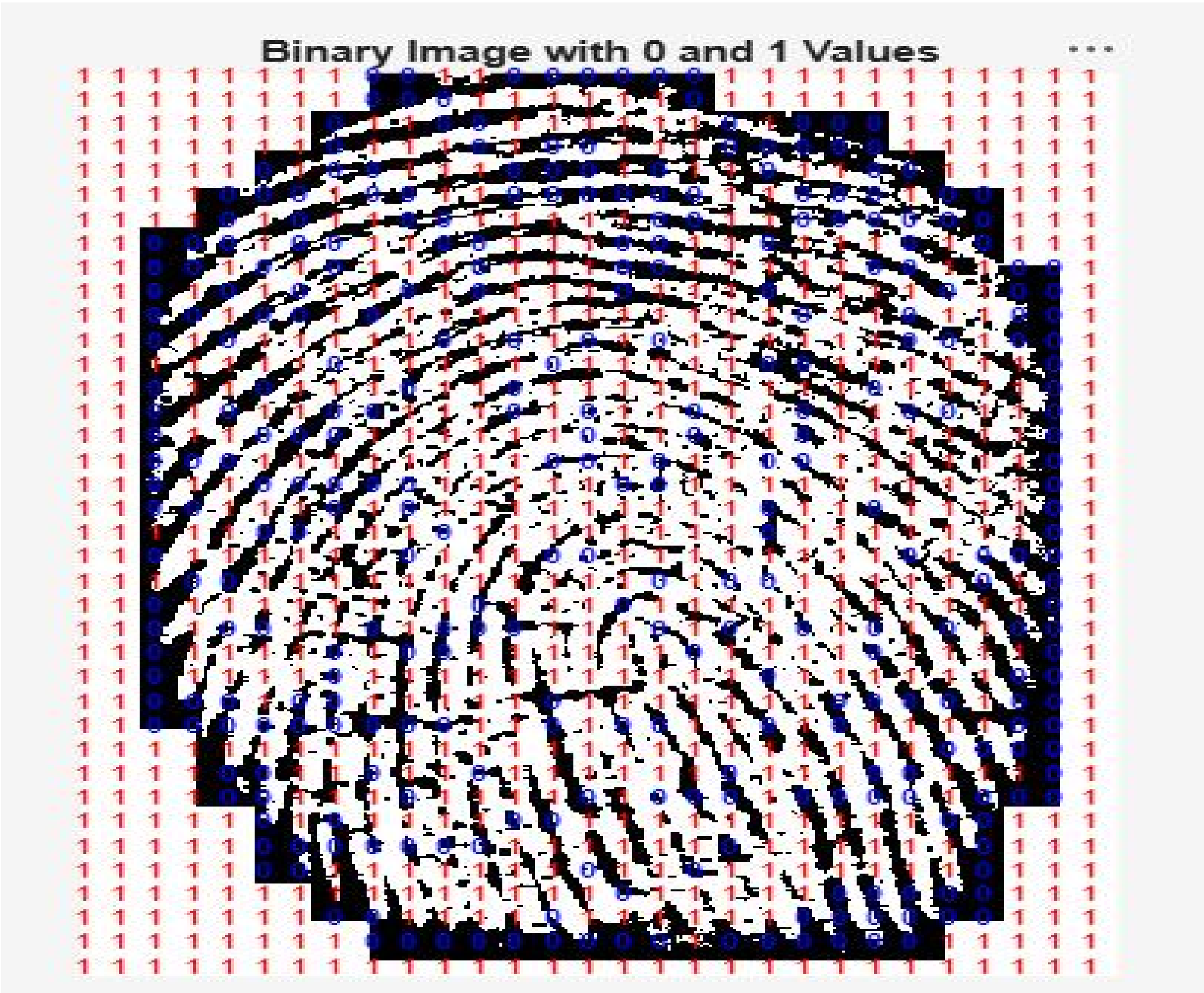

Figure 5.4: Image Binarization

The figure illustrates the complete fingerprint matching process when two different fingerprint images are compared. Initially, Fingerprint 1 and Fingerprint 2 are provided as inputs and undergo pre-processing steps such as segmentation, enhancement, and noise removal to improve image quality. The images are then converted into binary form to clearly distinguish ridge patterns, followed by skeletonization, which reduces the ridges to thin structures for better feature extraction.

After pre-processing, feature matching is performed between the two fingerprints. In this case, the computed matching score is low and does not meet the defined threshold. As a result, the system determines that the fingerprints do not match. The final output message displayed is **"**Fingerprint is NOT VALID**."** This indicates that the two input fingerprint images belong to different individuals, demonstrating the system's ability to correctly identify non-matching fingerprints.

5.2 Final Output Description

The below figure shows the complete fingerprint matching process along with the final result. Initially, two fingerprint images (Fingerprint 1 and Fingerprint 2) are provided as inputs. These images are then processed through several stages, including segmentation, where the fingerprint region is isolated from the background, and enhancement, which improves the clarity of ridge patterns. After that, binarization is applied to convert the images into black and white, making the ridge structures more distinct. The skeletonization step further refines the fingerprint by reducing the ridges to thin lines, which helps in accurate feature extraction.

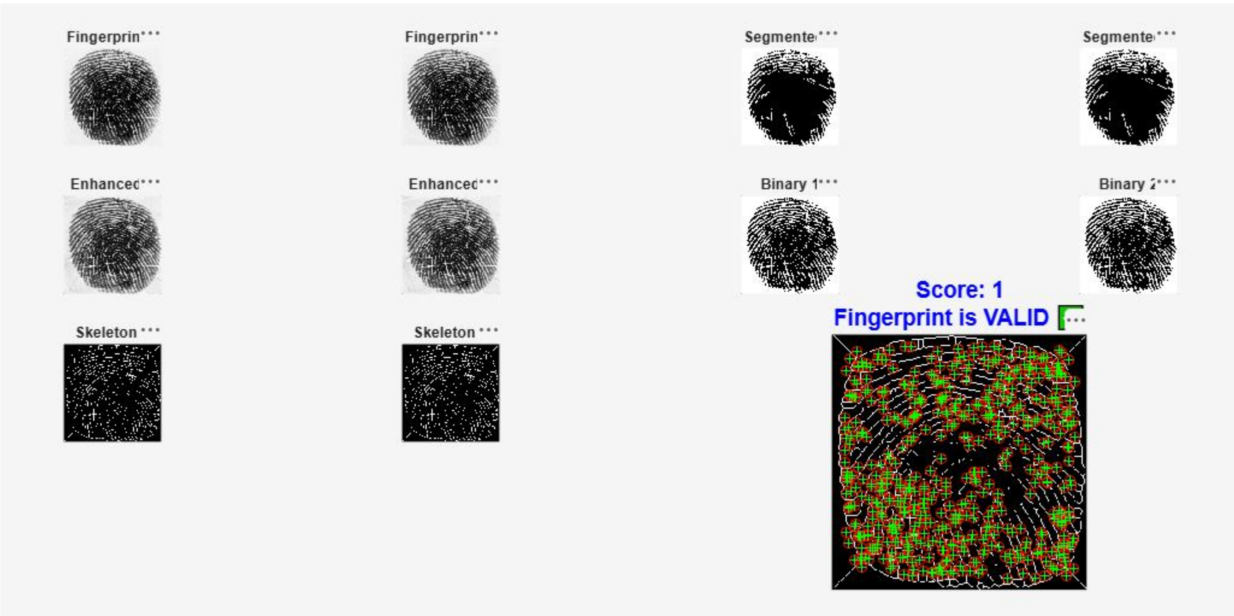

Figure 5.5: Fingerprint Matched

The figure illustrates the complete fingerprint matching process when two different fingerprint images are compared. Initially, Fingerprint 1 and Fingerprint 2 are provided as inputs and undergo pre-processing steps such as segmentation, enhancement, and noise removal to improve image quality. The images are then converted into binary form to clearly distinguish ridge patterns, followed by skeletonization, which reduces the ridges to thin structures for better feature extraction. After pre-processing, feature matching is performed between the two fingerprints. In this case, the computed matching score is low and does not meet the defined threshold. As a result, the system determines that the fingerprints do not match. The final output message displayed is "Fingerprint is NOT VALID." This indicates that the two input fingerprint images belong to different individuals, demonstrating the system's ability to correctly identify non-matching fingerprints.

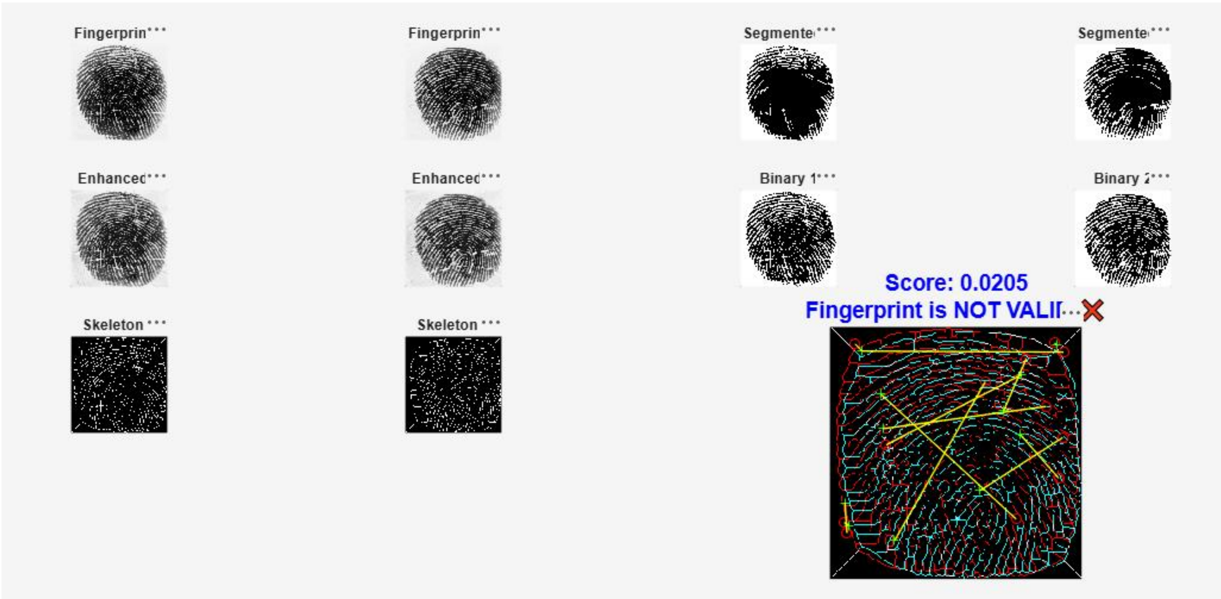

Figure 5.6: Fingerprint Mismatch.

VI. Conclusion

This work presented the design and implementation of a fingerprint recognition system using MATLAB, focusing on image processing techniques and biometric authentication. The main objective of the project was to compare two fingerprint images and determine whether they belong to the same person. To achieve this, several processing stages were implemented, including grayscale conversion, resizing, image enhancement, noise removal, segmentation, binarization, and thinning. These steps improved image quality and enabled accurate extraction of fingerprint features such as ridge patterns and structural details. The extracted features were used in the matching stage to calculate similarity between fingerprint images. Based on a predefined threshold, the system classified fingerprints as either VALID or NOT VALID. Experimental results demonstrated that the system successfully identified matching and non-matching fingerprints with satisfactory accuracy under normal conditions. Matching fingerprints produced high similarity scores, while different fingerprints generated low scores, confirming the reliability of the system. The study also highlighted the importance of image enhancement and preprocessing in improving recognition performance. MATLAB proved to be an effective platform for implementing and visualizing the fingerprint recognition process. However, the system may face limitations when dealing with poor-quality images, distortion, noise, or improper finger placement, which can affect matching accuracy. Overall, this dissertation successfully developed a functional fingerprint recognition system and demonstrated the significance of image processing in biometric authentication. The system can serve as a useful prototype for applications such as security systems, attendance monitoring, and access control, with future scope for further improvements and real-time implementation.

References

[1] Deng et al., "Deep Learning-Based Face Recognition Using Transformer Architectures," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 2026.

[2] Kakade et al., "A Comprehensive Study on Multimodal Biometric Authentication Systems," *International Journal of Advanced Computer Science*, 2026.

[3] Rjab et al., "Blockchain-Based Biometric Authentication in Decentralized Systems," *Computers & Security Journal*, 2026.

[4] Ma et al., "Gait Recognition Using Deep Learning for Human Identification at a Distance," *Pattern Recognition Letters*, 2026.

[5] Gopal Varma et al., "Multimodal Biometric Authentication Using AI: Fingerprint, Face, and Voice Integration," *Journal of Artificial Intelligence Research*, 2025.

[6] Gimba et al., "CNN-Based Multimodal Biometric System for Face and Fingerprint Recognition," *Expert Systems with Applications*, 2025.

[7] Garg et al., "Multimodal Biometric System Using Fingerprint, Iris, and ECG Signals," *Biomedical Signal Processing and Control*, 2025.

[8] Al-Refai et al., "Evaluation of Biometric Modalities: Security and Performance Analysis," *Journal of Information Security*, 2025.

[9] Kumar and Zhou, "Deep Learning Approaches for Fingerprint Recognition," *IEEE Access*, 2024.

[10] Krivokuca Hahn et al., "iCarB: A Multimodal Biometric Dataset for Real-World Applications," *arXiv preprint arXiv:2411.xxxx*, 2024.

[11] Meiramkhanov et al., "Hybrid Fingerprint Recognition Using CNN and Gabor Filters," *Applied Sciences*, 2024.

[12] Al-Dabbas et al., "Face Recognition Using Machine Learning and Deep Learning Techniques," *Engineering, Technology & Applied Science Research*, 2024.

[13] Zhang et al., "Deep Learning-Based Iris Recognition System," *Pattern Recognition Journal*, 2024.

[14] Singh et al., "Fingerprint Recognition Using MATLAB-Based Image Processing Techniques," *International Journal of Image Processing*, 2023.

[15] Sharma et al., "Face Recognition System Using MATLAB and PCA-LDA Techniques," *International Journal of Computer Applications*, 2023.

[16] Patel et al., “Multimodal Biometric System Using MATLAB: Face and Fingerprint Recognition,” *Procedia Computer Science*, 2022.

[17] Ahmed et al., “Voice Recognition Using Machine Learning for Biometric Authentication,” *IEEE Access*, 2022.

[18] Roy et al., “Iris Recognition Using Image Processing Techniques,” *International Journal of Biometrics*, 2021.