Review Article ***https://doi.org/10.5281/zenodo.18690728***

Volume 7, Issue 2, pp 76-93, December 2025

ACHIEVERS JOURNAL OF SCIENTIFIC RESEARCH

Opecn Access Publications of Achievers University, Owo

Available Online at www.achieversjournalofscience.org

Advances in Fingerprint Biometric Recognition for Modern Attendance Management: A State-of-the-Art Review

Adagbonyin T. I.[1]*, Aranuwa F. O.[2], and Oyekanmi E. O.[1]

[1]Department of Computer Science, Achievers University, Owo, Ondo State, Nigeria.
[2]Department of Computer Science, Adekunle Ajasin University, Akungba-Akoko, Ondo State, Nigeria

***Corresponding Author's Email Address:** adagbonyin.ti@achievers.edu.ng

Submitted: Jul 7, 2025; **Revised:** Aug 26, 2025; **Accepted:** Dec 12, 2025; **Published:** Dec 31, 2025

Abstract

The manual attendance system has been in use for decades; however, shortcomings such as impersonation, ineffective manual record-keeping, and unreliable token-centric methodologies limit its application for this digital age. Biometric-based fingerprint technique is one of the recently evolving approaches developed to mitigate the shortcomings of manual attendance methods. It is on these premises that this current study examines the principal methodologies employed in fingerprint recognition, focusing on attendance management. Efforts were made to review the recent progress in preprocessing techniques such as normalization, segmentation, orientation estimation, ridge frequency analysis, and Gabor filtering. Also, feature extraction techniques like minutiae-based, ridge-based, and hybrid techniques were extensively analyzed. Furthermore, matching algorithms, performance metrics, and error quantification for evaluating the performance of biometric-based fingerprint systems were examined. The strengths, weaknesses, and associated bottlenecks with the biometric-based fingerprint technique, particularly the management of low-quality prints, scalability assurance, and robustness enhancement, were looked into. The outcome of this review opens up gaps for new research directions in the development of more reliable and efficient fingerprint-based attendance mechanisms.

Keywords: Attendance management, Fingerprint recognition, Gabor filtering, Minutiae features, Ridge-based features

1. Introduction

Traditional methods such as passwords, pen-and-paper records, and identification cards are associated with several shortcomings, including theft, misplacement, and proxy attendance (Hoo & Ibrahim, 2019). The need to overcome these limitations has driven the development of modern attendance management systems, particularly biometric fingerprint-based recognition systems, which remain among the most widely studied biometric technologies (Akinduyite *et al.,* 2013). Fingerprint recognition has been adopted across various domains, including security, forensics, and identity management, due to its uniqueness, permanence, and ease of use. Over the years, advancements in sensing hardware, image processing, pattern recognition, and machine learning have significantly improved fingerprint recognition systems, making them suitable for large-scale deployment and real-time applications such as border access control, financial transaction monitoring, healthcare systems, and institutional attendance tracking. In fingerprint recognition, the extraction of distinctive characteristics from ridge patterns is a critical step in the identification process (Jain *et al.*, 2024).

Conventional fingerprint recognition techniques primarily rely on minutiae-based methods, which analyze ridge endings and bifurcations that form unique fingerprint structures. Goyal and Jindal (2017) identified minutiae as highly dependable fingerprint features, as they retain their uniqueness despite variations in finger pressure, rotation, or partial impressions. However, minutiae-based systems are highly sensitive to image quality and require extensive preprocessing to ensure accurate feature extraction. According to Yang *et al.* (2019), factors such as noise, smudging, moisture, and low sensor resolution can obscure genuine minutiae or introduce false points, thereby increasing error rates. To address these limitations, researchers have explored ridge-based recognition approaches that capture global ridge flow, frequency, curvature, and orientation patterns. While ridge-based methods provide improved robustness and stability, they are generally less distinctive than minutiae-based approaches, particularly when distinguishing individuals with similar global ridge patterns. Jain *et al.* (2000) introduced orientation maps and global texture descriptors that enhance recognition performance under poor image quality and partial fingerprint conditions.

More recent studies have shifted toward hybrid fingerprint recognition techniques that combine minutiae-based and ridge-based features. Krish *et al.* (2019) demonstrated that hybrid fusion significantly improves recognition accuracy by integrating the precision of minutiae features with the noise tolerance of global ridge descriptors. Additional improvements have also been achieved through advanced preprocessing techniques such as Gabor filtering. Görgel and Ekşi (2021) reported that Gabor filtering effectively enhances ridge–valley structures through frequency- and orientation-selective filtering, thereby improving the reliability of subsequent feature extraction, especially for low-quality or uneven fingerprint impressions. The increasing interest in biometric attendance systems has further driven research into scalable, fast, and robust fingerprint recognition solutions for real-world deployment. Studies by Akinduyite *et al.* (2013), Oyebola *et al.* (2018), and Oloruntoba and Akinode (2020) have shown that fingerprint-based attendance systems reduce administrative errors and impersonation in educational institutions. Nevertheless, challenges such as noisy images, large user databases, partial fingerprints, and security threats including spoofing remain prevalent in many implementations (Yang *et al.*, 2019; Mizinov *et al.*, 2024). These issues continue to motivate research into more robust, efficient, and secure fingerprint recognition systems.

Given the rapid growth and diversity of fingerprint recognition research, a systematic review is necessary to highlight recent developments, compare existing approaches, and identify persistent challenges and open research directions. This review synthesizes current progress, applications, limitations, and future research directions in fingerprint recognition systems. The remainder of this paper is organized as follows: Section 2 presents the conceptual background of fingerprint recognition, Section 3 reviews related works, Section 4 summarizes and analyzes the findings of the review, and Section 5 concludes the paper.

2.0 Conceptual Perspective of Fingerprint Recognition

Fingerprint recognition has evolved from traditional minutiae-based techniques to more advanced hybrid and deep learning approaches. Feature extraction plays a central role in this evolution, as it directly determines how effectively an individual can be identified. Three major categories of feature extraction techniques are prominent in the literature: minutiae-based, ridge-based, and hybrid approaches. Minutiae-based methods are widely used because of their high discriminative power, ridge-based methods offer improved robustness to noise and poor-quality images, while hybrid techniques integrate multiple feature cues to enhance reliability (Goyal & Jindal, 2017). According to Jain *et al.* (2024) and Yang *et al.* (2019), these approaches differ in their emphasis on local ridge structures, global ridge patterns, texture information, or learned representations. Reviewing these techniques highlights the progression of fingerprint recognition and illustrates how different methods complement one another in practical, real-world applications.

2.1 Fingerprint Biometric Authentication: An Overview

Biometric authentication refers to the automated process of verifying or identifying an individual based on distinctive physiological or behavioral characteristics. Because biometric traits are inherently linked to the individual, they provide strong resistance to impersonation. Abdulrahman and Alhayani (2023) reported that biometric systems offer improved security compared to traditional password-based or token-based methods, which may be forgotten, stolen, or intentionally shared. Common biometric modalities include fingerprints, facial images, iris patterns, voiceprints, hand geometry, and behavioral traits such as gait or typing rhythm. A typical biometric system consists of four main stages: sensing, preprocessing, feature extraction, and matching. During the sensing stage, a scanner or sensor captures the biometric sample, while preprocessing enhances sample quality by reducing noise and correcting distortions. Feature extraction then identifies distinguishing characteristics, such as ridge flows or minutiae points, and the matching stage establishes identity by comparing the extracted features with stored templates.

2.1.1 Minutiae-Based Fingerprint Recognition

Minutiae-based recognition remains the most widely adopted fingerprint recognition approach because it relies on distinctive and stable local ridge characteristics, primarily ridge endings and bifurcations. These features offer strong individual discrimination, as their spatial locations and orientations remain largely consistent even when fingerprint images are captured under varying conditions (Goyal & Jindal, 2017). As a result, minutiae-based methods form the foundation of most classical fingerprint recognition systems.
In typical implementations, minutiae extraction is performed after preprocessing steps such as binarization and thinning, which enhance ridge clarity and reduce noise. The most commonly used extraction technique is the Crossing Number (CN) method, which identifies minutiae by examining directional transitions in the neighborhood of each ridge pixel in a thinned binary image. However, studies have shown that minutiae-based systems are sensitive to noise, partial fingerprints, and low-quality images, which may introduce spurious or missing minutiae and increase false rejection rates (Yang *et al.*, 2019; Akinduyite *et al.*, 2013).
For each ridge pixel P in the thinned binary fingerprint image, the Crossing Number (CN) is computed using its eight-connected neighborhood as shown in Eqn (1). Let $P_1, P_2, \dots, P_8$ denote the eight neighboring pixels surrounding P, ordered clockwise, and let $P_9 = P_1$ to complete the circular sequence. The Crossing Number is defined as:

$$\mathrm{CN}(P) = \frac{1}{2}\sum_{i=1}^{8} | P_i - P_{i+1} | \quad \text{where } P_9 = P_1 \qquad \text{Eqn (1)}$$

where $P_i \in \{0,1\}$ represents the binary pixel value at the i-th neighboring position. The CN value indicates the type of ridge structure at pixel P: $CN = 1$ corresponds to a ridge ending, $CN = 3$ indicates a bifurcation, and $CN = 2$ represents a normal ridge continuation.
Each detected minutia is represented as a triplet (x, y, θ), where $x$and y denote the spatial coordinates of the minutia in the fingerprint image, and θ represents the local ridge orientation at that point, estimated from the orientation field as depicted with Eqn (2). A complete minutiae template is defined as:

$$T_m = \{(x_1, y_1, \theta_1), (x_2, y_2, \theta_2), \dots, (x_n, y_n, \theta_n)\} \qquad \text{Eqn (2)}$$

where n denotes the total number of extracted minutiae points in the fingerprint. As noted by Krish *et al.* (2019), minutiae templates are compact and highly discriminative, but they remain sensitive to noise, partial fingerprints, and variations in finger placement.

Minutiae matching involves comparing two aligned minutiae templates to determine whether corresponding points represent the same fingerprint. Two minutiae are considered a match if they satisfy both a spatial proximity constraint and an orientation similarity constraint.

Let $m_i = (x_i, y_i, \theta_i)$ and $m_j = (x_j, y_j, \theta_j)$ denote minutiae points from fingerprint templates A and B, respectively as shown with Eqn (3). The spatial distance between two minutiae points is computed using the Euclidean distance as:

$$sd(m_i, m_j) = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \qquad \text{Eqn (3)}$$

where (x_i, y_i) and (x_j, y_j)represent the pixel coordinates of the two minutiae points. Two minutiae are considered spatially consistent if this distance is below a predefined threshold (typically 8–12 pixels). Orientation consistency between minutiae is evaluated using the minimum angular difference in Eqn (4):

$$od(m_i, m_j) = \min(|\theta_i - \theta_j|, 360° - |\theta_i - \theta_j|) \qquad \text{Eqn (4)}$$

where $\theta_i$and θ_j are the local ridge orientations of the two minutiae, measured in degrees. This formulation accounts for angular wrap-around by constraining the difference to the range $[0°, 180°]$. A match is accepted if the orientation difference is below a specified threshold (commonly 10–15 degrees).

After identifying all valid minutiae correspondences, a normalized matching score is given with Eqn (5):

$$\text{Score}_m = \frac{N_{\text{matched}}^2}{N_A \cdot N_B} \qquad \text{Eqn (5)}$$

where N_{matched} denotes the number of matched minutiae pairs, and N_A and N_B represent the total number of minutiae points in templates $A$and B, respectively. This normalization ensures that the score reflects the degree of similarity between the two fingerprints independent of template size.

2.1.2 Ridge-Based Recognition

Ridge-based recognition focuses on capturing global fingerprint characteristics, including overall ridge flow, ridge frequency, orientation, curvature, and texture. Unlike minutiae-based methods, which depend on precise local details, ridge-based features remain relatively stable even when fingerprint images are noisy or incomplete because they represent the global structural patterns of the fingerprint. Jain *et al.* (2000) demonstrated that ridge flow patterns provide strong complementarity to local minutiae and showed that ridge-based techniques, such as FingerCode, are more robust to noisy or low-quality images. This robustness makes ridge-based methods particularly useful in cases where only a limited number of minutiae can be reliably detected. However, although ridge-based techniques help reduce false rejection rates, they may lack the high level of uniqueness offered by minutiae-based methods, especially in large-scale databases.

Ridge-based techniques typically operate by dividing the fingerprint image into blocks and computing orientation or frequency maps that describe ridge flow patterns. Pradeep and Ravi (2022) noted that ridge-based matching often relies on vector similarity measures, such as Euclidean distance, which generally allow faster comparisons than minutiae-based approaches. As a result, ridge-based recognition is well suited for large-scale attendance systems where computational speed and robustness are critical. Orientation field estimation is commonly performed using gradient-based techniques, as proposed by Bazen and Gerez (2002). Let $\partial_x(u, v)$ and $\partial_y(u, v)$denote the horizontal and vertical intensity gradients at pixel location (u, v) within a local block centered at (x, y). Two coherence terms are computed as given with Eqn (6) and Eqn (7) respectively:

$$V_x(x, y) = \sum_{(u,v)} 2 \cdot \partial_x(u, v) \cdot \partial_y(u, v) \qquad \text{Eqn (6)}$$

$$V_y(x, y) = \sum_{(u,v)} \left[\partial_x^2(u, v) - \partial_y^2(u, v)\right] \qquad \text{Eqn (7)}$$

where the summation is performed over all pixels within the local block. These coherence values capture the dominant gradient structure of the ridge pattern based on Eqn (8). The local ridge orientation is then estimated as:

$$\theta(x, y) = \frac{1}{2} \cdot atan2(V_y, V_x) \quad \text{Eqn (8)}$$

where $\theta(x, y)$ represents the ridge orientation at location (x, y). This formulation accounts for the periodic nature of ridge orientation.

Once orientation and frequency information are obtained, each block contributes a set of numerical descriptors, forming a ridge feature vector which can be evaluated with Eqn (9), thus:

$$\mathrm{T_r} = [\mathrm{f_1}, \mathrm{f_2}, \dots, \mathrm{f_n}] \quad \text{Eqn (9)}$$

Let T_{rA} and T_{rB} denote ridge feature vectors extracted from two fingerprint images. Matching compares two feature vectors R_A and R_B using Eqn (10) which is performed by computing the Euclidean distance between the corresponding feature vectors and converting distance to similarity through Eqn (11);

$$\mathrm{T_{rA}} = [\mathrm{a_1}, \mathrm{a_2}, \dots, \mathrm{a_n}], \mathrm{T_{rB}} = [\mathrm{b_1}, \mathrm{b_2}, \dots, \mathrm{b_n}] \quad \text{Eqn (10)}$$

$$\mathrm{D} = \sqrt{\sum_{\mathrm{i}=1}^{\mathrm{n}} (\mathrm{a_i} - \mathrm{b_i})^2} \quad \text{Eqn (11)}$$

2.1.3 Texture-Based Recognition

Texture-based recognition extends fingerprint analysis beyond ridge orientation and minutiae by examining fine-grained texture patterns, including local descriptors, spatial filters, and frequency-domain techniques. The Gabor filter-based FingerCode model, first introduced by Jain *et al.* (2000), extracts texture features using a bank of filters tuned to specific orientations and frequencies. Texture-based systems are capable of capturing subtle fingerprint details that may not be visible in ridge-orientation fields or minutiae maps. Görgel and Ekşi (2021) reported that Gabor-based features are particularly effective for handling partial or noisy fingerprints, as they enhance ridge–valley structures while capturing local texture variations. In addition to Gabor-based methods, recent studies have explored other texture descriptors, such as local binary patterns (LBP) and wavelet-based techniques, which provide compact and invariant representations of fingerprint images. By complementing the limitations of minutiae-only approaches, texture-based recognition contributes to improved robustness in fingerprint recognition systems.

2.1.4 Deep Learning-Based Recognition

Recent advances in convolutional neural networks (CNNs) have significantly transformed fingerprint recognition by enabling automatic learning of multi-level representations directly from raw fingerprint images, rather than relying on manually designed features. Studies by Görgel and Ekşi (2021) and Mulay *et al.* (2024) demonstrated that CNN-based minutiae extractors outperform traditional techniques, particularly when processing distorted or low-quality fingerprint images. In addition, Chhabra *et al.* (2023) showed that CNN-based segmentation and enhancement models can substantially improve the clarity of latent and low-contrast fingerprints. Deep learning approaches are capable of generating highly discriminative embeddings for matching, performing reliable classification, and detecting fine-grained fingerprint details with improved precision. However, their adoption in low-resource environments or real-time attendance systems is often constrained by the high computational demands and large training datasets required. Despite these challenges, deep learning has become a central focus of contemporary fingerprint research and has inspired the development of hybrid learning-based recognition frameworks.

2.1.5 Hybrid Techniques

Hybrid recognition techniques combine multiple fingerprint feature types to exploit the strengths of each approach. These systems integrate minutiae, ridge-based descriptors, and texture features to produce fingerprint templates that are both accurate and stable. Krish *et al.* (2019) demonstrated that hybrid systems achieve lower equal error rates (EERs) than single-technique approaches, particularly when handling

partial fingerprints or noisy images. By fusing global and local features, hybrid methods preserve high discriminative power while improving robustness under varying acquisition conditions.
Hybrid fingerprint recognition systems commonly employ score-level fusion strategies to combine matching results obtained from multiple feature extractors. This integration compensates for the limitations of individual techniques by leveraging complementary information from local, global, and texture-based descriptors. A representative hybrid template may take the form as described with Eqn (12);

$$H = \{M, R, T\} \quad \text{Eqn (12)}$$

where M denotes the set of extracted minutiae features, Rrepresents the ridge-based feature vector, and T corresponds to the Gabor-based texture feature vector. Each feature component produces an independent similarity score, namely S_{minutiae}, S_{ridge}, and S_{gabor}, respectively.
The overall hybrid similarity score is computed using a weighted sum fusion rule as shown in Eqn (13):

$$S_{hybrid} = w_1 S_{minutiae} + w_2 S_{ridge} + w_3 S_{gabor} \quad \text{Eqn (13)}$$

where w_1, w_2, and w_3 are weighting coefficients that control the contribution of each feature type. The weights are constrained such that the weighted sum must be equal to one represented in Eqn (14):

$$w_1 + w_2 + w_3 = 1 \quad \text{Eqn (14)}$$

ensuring proper normalization of the combined similarity score. Studies such as Krish *et al.* (2019), Yadav *et al.* (2024), and Mulay *et al.* (2024) reported that hybrid fusion strategies reduce both false acceptance and false rejection rates, improve robustness to partial or distorted fingerprints, and enhance stability in large-scale deployments.

2.2. Fingerprint Image Preprocessing Techniques

Preprocessing is a critical stage in fingerprint recognition because it provides the foundation for accurate feature extraction, matching, and classification. Raw fingerprint images often suffer from low contrast, uneven finger pressure, smudging, moisture, noise, and partial impressions. Effective preprocessing significantly improves the reliability of both minutiae-based and ridge-based recognition by enhancing image quality before feature extraction. According to Yang *et al.* (2019), inadequate preprocessing is a major contributor to high error rates, including increased false rejection rates (FRR) and distorted or missing feature points. Over time, several preprocessing techniques have been developed and refined to improve ridge–valley clarity, suppress noise, and prepare fingerprint images for reliable analysis. Commonly used methods include normalization, orientation estimation, ridge-frequency estimation, Gabor filtering, binarization, and thinning. These stages are typically applied sequentially as part of a preprocessing pipeline, and many studies combine them to address shortcomings identified in earlier fingerprint recognition systems.

2.2.1 Normalization

Normalization is one of the earliest and most important preprocessing stages in fingerprint recognition, as it reduces variations in gray-level intensity caused by uneven finger pressure, sensor limitations, or environmental conditions. A widely adopted normalization approach was introduced by Hong *et al.* (1998), which standardizes image intensities by adjusting each pixel relative to a target mean and variance. By constraining the pixel intensity distribution, normalization enhances consistency across fingerprint samples while preserving subtle ridge information. Chhabra *et al.* (2023) noted that normalization is particularly effective for faint or low-contrast fingerprints, as it improves ridge visibility prior to filtering or enhancement. Consequently, most modern fingerprint recognition systems incorporate normalization to stabilize subsequent operations such as orientation and ridge-frequency estimation.
Mathematically, let $I(x, y)$denote the original grayscale intensity at pixel location (x, y), $M$and Vrepresent the mean and variance of the image, and $M_0$and V_0denote the desired mean and variance. The normalized pixel intensity as depicted with Eqn (15):

$$N(x,y) = \begin{cases} M_0 + \sqrt{\frac{V_0(I(x,y)-M)^2}{V}} & \text{if } I(x,y) > M \\ M_0 - \sqrt{\frac{V_0(I(x,y)-M)^2}{V}} & \text{otherwise} \end{cases} \quad \text{Eqn (15)}$$

where the transformation maps pixel values above and below the mean symmetrically, ensuring that the resulting image has the specified statistical properties while preserving ridge contrast.

2.2.2 Orientation Estimation

Orientation estimation determines the direction of ridge flow across a fingerprint image, as described by Bazen and Gerez (2002), and plays a central role in enhancement, feature extraction, and classification. Most classical approaches compute local image gradients along horizontal and vertical directions and use these values to estimate the dominant ridge orientation within predefined image blocks. Jain *et al.* (2000) noted that accurate orientation estimation improves local ridge coherence, enabling filters such as Gabor kernels to be properly aligned with ridge directions. Because noise and partial impressions can disrupt ridge continuity in low-quality fingerprints, reliable orientation fields are particularly important under such conditions. Görgel and Ekşi (2021) emphasized that refined orientation maps significantly enhance minutiae extraction, as local ridge direction directly influences the interpretation of ridge endings and bifurcations. For a block of size $W \times W$, two coherence terms are computed using Eqn (16) to Eqn (18), thus:

$$V_x(x,y) = \sum_{u,v} 2\,\partial_x(u,v)\partial_y(u,v) \quad \text{Eqn (16)}$$

$$V_y(x,y) = \sum_{u,v} \left(\partial_x^2(u,v) - \partial_y^2(u,v)\right) \quad \text{Eqn (17)}$$

$$\theta(x,y) = \frac{1}{2} atan2\left(V_y(x,y), V_x(x,y)\right) \quad \text{Eqn (18)}$$

here $\partial_x(u,v)$ and $\partial_y(u,v)$ denote the intensity gradients along the horizontal and vertical directions at pixel (u, v) within the block, $W$is the block size, and $\theta(x,y)$ represents the estimated ridge orientation at location (x, y).

2.2.3 Ridge-Frequency Estimation

Ridge frequency estimation determines how frequently ridges occur within a fingerprint image and helps identify anomalous regions such as smudges, scars, or excessively smooth areas. The process typically involves projecting pixel intensities along the ridge direction and detecting peaks corresponding to ridge-valley transitions. Ridge frequency estimation is important because it guides the tuning of Gabor filters and other enhancement kernels. Jain *et al.* (2000) demonstrated within the FingerCode framework that accurate frequency estimation allows filter parameters to be matched to the natural spacing of ridges, resulting in improved enhancement quality. Studies by Chhabra *et al.* (2023) and Yang *et al.* (2019) further noted that inaccurate frequency estimation may cause over-smoothing or distortion of ridge patterns, negatively affecting matching accuracy. The ridge-frequency estimation can be obtained with Eqn (19):

$$\text{Frequency} = \frac{1}{\text{Average Ridge Distance}} \quad \text{Eqn (19)}$$

where D denotes the average ridge-to-ridge distance measured along the ridge direction.

2.2.4 Gabor Filtering

Gabor filtering remains one of the most influential and widely adopted techniques for fingerprint image enhancement. A Gabor filter captures local orientation and frequency characteristics by combining a sinusoidal carrier with a Gaussian envelope. Görgel and Ekşi (2021) reported that Gabor filters are particularly effective for low-quality or latent fingerprints because they enhance ridge structures while suppressing noise. Since Gabor filters are directionally selective, accurate orientation and ridge-frequency estimates are required for effective filtering. When applied correctly, Gabor filtering increases ridge–valley contrast, reduces smudging effects, and restores clarity in regions affected by uneven finger pressure. Many modern fingerprint recognition systems apply a bank of Gabor filters at multiple orientations to enhance ridge structures in all directions. A two-dimensional Gabor filter is expressed as depicted in Eqn (20):

$$G(x, y; f, \theta) = \exp\left\{-\frac{1}{2}\left(\frac{x_\theta^2}{\sigma_x^2} + \frac{y_\theta^2}{\sigma_y^2}\right)\right\}\cos(2\pi f x_\theta) \qquad \text{Eqn (20)}$$

Where; $x_\theta = x\cos\theta + y\sin$, $y_\theta = -x\sin\theta + y\cos$, σ_x, σ_y = control the spread of the Gaussian envelope, f = ridge frequency with the coordinate transformation: (x', y')= rotated coordinates. θ represents the local ridge orientation and f is the local ridge frequency. Chhabra *et al.* (2023) showed that Gabor filtering significantly improves segmentation and feature extraction accuracy, particularly for partial or latent fingerprints.

2.2.5 Binarization

Binarization converts the enhanced grayscale fingerprint image into a binary representation, where ridges appear as black pixels and valleys as white pixels. This transformation simplifies the image and improves both the speed and accuracy of subsequent feature extraction. According to Jain *et al.* (2024), adaptive thresholding techniques apply different threshold values across local regions based on ridge contrast and illumination conditions, generally outperforming global thresholding in noisy or unevenly illuminated fingerprints. Milewski (2024) emphasized that effective binarization improves ridge path clarity, which is essential for the accurate detection of ridge endings and bifurcations. However, inadequate binarization may amplify noise or introduce false ridge breaks, increasing the likelihood of spurious minutiae. The thresholding operation is shown in Eqn (21):

$$B(x, y) = \begin{cases} 1 & \text{if } E(x, y) > T(x, y) \\ 0 & \text{otherwise} \end{cases} \qquad \text{Eqn (21)}$$

where $E(x, y)$represents the enhanced pixel intensity and $T(x, y)$denotes the locally adaptive threshold.

2.2.6 Thinning (Skeletonization)

Thinning reduces fingerprint ridge lines to a one-pixel-wide skeleton while preserving their overall connectivity. This step is essential for minutiae extraction, as it ensures that ridge endings and bifurcations are accurately represented at their true locations. Goyal and Jindal (2017) noted that effective thinning minimizes the generation of false minutiae caused by spurious branches or excessively thick ridges. Most thinning approaches employ iterative algorithms that remove outer ridge pixels while maintaining ridge continuity. Milewski (2024) described several cycle-based thinning techniques that are widely used in biometric systems due to their computational efficiency and stability. When thinning is performed correctly, minutiae detection algorithms such as the Crossing Number (CN) method can produce reliable and consistent feature sets.

2.2.7 Modern and Deep Learning–Based Preprocessing

Recent scholarly studies have proposed and implemented deep learning–based methods for fingerprint preprocessing tasks such as segmentation, orientation estimation, and image enhancement. Chhabra *et al.* (2023) developed a convolutional neural network (CNN) model capable of correcting distorted ridge patterns and enhancing the clarity of latent fingerprints. Similarly, Mulay *et al.* (2024) investigated learning-based minutiae extraction pipelines that integrate preprocessing into end-to-end neural network architectures. Although these approaches typically outperform conventional techniques when processing degraded or low-quality fingerprints, they require substantial computational resources and large annotated datasets. As a result, their deployment in real-time or resource-constrained environments remains limited. Nevertheless, deep learning–based preprocessing methods represent an important direction for future research in fingerprint recognition.

Preprocessing continues to play a critical role in fingerprint recognition research by improving robustness under real-world conditions, reducing error rates, and enhancing overall accuracy. Earlier systems, particularly those relying solely on minutiae-based recognition, depended heavily on normalization, binarization, and thinning, but often struggled with noisy or partially captured fingerprints (Akinduyite *et al.*, 2013; Oyebola *et al.*, 2018). More recent studies have increasingly adopted Gabor filtering, frequency-guided enhancement, and deep learning techniques to improve orientation estimation and image quality (Krish *et al.*, 2019; Görgel & Ekşi, 2021). Despite these advances, challenges such as deep skin damage, poor sensor quality, and severe image degradation remain difficult to resolve, even with advanced preprocessing techniques (Chhabra *et al.*, 2023; Mulay *et al.*, 2024). Consequently, hybrid feature strategies and learning-based approaches continue to be actively explored.

2.3 Performance Evaluation Metrics in Fingerprint Recognition Systems

Performance evaluation metrics are essential for assessing the effectiveness, reliability, and practical readiness of fingerprint recognition systems. These metrics determine how well a system distinguishes between genuine users and impostors and evaluate its suitability for real-world applications such as authentication, identification, and attendance management. Common evaluation criteria include statistical error rates, matching accuracy, computational efficiency, and overall system robustness. Frequently used metrics include false acceptance rate, false rejection rate, true acceptance rate, true rejection rate, and equal error rate (Mingote *et al.*, 2019). In addition, measures such as matching time, ranking accuracy, and receiver operating characteristic (ROC) curves are often considered. This subsection reviews widely used performance metrics to provide a clear reference for researchers in fingerprint recognition.

2.3.1 False Acceptance Rate (FAR)

The false acceptance rate represents how often a fingerprint recognition system incorrectly accepts an impostor as a genuine user. In biometric evaluation, FAR measures the probability that a non-matching fingerprint pair is incorrectly classified as a match. A false acceptance occurs when the similarity score between two fingerprints exceeds the system's decision threshold despite originating from different individuals. Jain *et al.* (2024) emphasized that minimizing FAR is particularly important in high-security applications, although stricter thresholds may increase false rejection rates. Krish *et al.* (2019) reported that hybrid feature fusion methods generally achieve lower FAR due to improved discriminative capability. A high FAR indicates vulnerability to security breaches. FAR is expressed using Eqn (22):

$$FAR = \frac{\text{Number of False Acceptances}}{\text{Total Number of Impostor Attempts}} \qquad \text{Eqn (22)}$$

2.3.2 False Rejection Rate (FRR)

The false rejection rate measures how often a system incorrectly rejects a genuine user and reflects its sensitivity to intra-class variations such as partial fingerprints, dry or moist skin, pressure differences, and environmental noise. A false rejection occurs when the similarity score between two genuine fingerprint samples falls below the decision threshold. Yang *et al.* (2019) observed that systems relying solely on minutiae-based features often exhibit higher FRR when processing low-quality images due to missing or spurious minutiae. Ridge-based and Gabor-based features can help reduce FRR by providing greater tolerance to image distortion. Akinduyite *et al.* (2013) emphasized that FRR, alongside FAR, remains a fundamental metric for evaluating fingerprint recognition performance. Batubara *et al.* (2021) focused primarily on FRR to assess system sensitivity to legitimate users. FRR is usually expressed with Eqn (23):

$$FRR = \frac{\text{Number of False Rejections}}{\text{Total Number of Genuine Attempts}} \qquad \text{Eqn (23)}$$

2.3.4 Equal Error Rate (EER)

Equal error rate is a standard benchmark used to evaluate and compare biometric systems. EER represents the operating point at which the false acceptance rate and false rejection rate are equal. A lower EER indicates better overall system performance, as it reflects fewer errors of both types. This metric is widely used because it provides a single, concise measure of system accuracy. Comparative studies, including Krish *et al.* (2019) and Görgel and Ekşi (2021), frequently report EER, particularly for hybrid fingerprint systems that must balance sensitivity and specificity. Graphically, EER is obtained at the intersection of the FAR and FRR curves as the decision threshold varies as described with Eqn (24) by Ogundepo *et al.* (2019):

$$EER = FAR(\tau) = FRR(\tau) \qquad \text{Eqn (24)}$$

Where; $\tau$is the threshold value.

2.3.5 Accuracy

Accuracy is one of the most commonly reported evaluation metrics in fingerprint recognition research because it indicates how often the system makes correct decisions overall. It measures the proportion of true outcomes, including correctly accepted genuine users and correctly rejected impostors, relative to all verification attempts. In biometric evaluation, accuracy is computed as the sum of true positives and true negatives divided by the total number of outcomes, including false matches and false non-matches. Although accuracy provides a general view of system performance, it does not always capture behavior under imbalanced data or strict security requirements. For this reason, accuracy is often interpreted alongside metrics such as FAR or EER. Görgel and Ekşi (2021) defined accuracy as the proportion of correct decisions made by the system and is computed using Eqn (25):

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \qquad \text{Eqn (25)}$$

Where TP is true positives, TN is true negatives, FP is false positives, and FN is false negatives. Rahman *et al.* (2023) similarly reported both accuracy and EER as key performance metrics in modern fingerprint recognition studies.

2.4. Other Metrics of Evaluation

Several additional evaluation metrics appear in the fingerprint recognition literature but are less frequently reported in experimental studies. Nevertheless, they remain valuable for assessing the performance of biometric fingerprint systems. These metrics include genuine acceptance rate (GAR), false match rate (FMR), false non-match rate (FNMR), receiver operating characteristic (ROC) curves, matching time, throughput, and template size. Genuine acceptance rate represents the proportion of legitimate users who are correctly verified by the system. False match rate and false non-match rate are alternative terminologies commonly adopted in ISO biometric standards and correspond closely to FAR and FRR, respectively. These measures are widely used in industry-grade fingerprint recognition systems.

Receiver operating characteristic (ROC) curves provide a graphical representation of the relationship between GAR and FAR across varying decision thresholds and are commonly used to visualize the trade-off between security and usability. Matching time measures the speed of the fingerprint matching process and is particularly important for large-scale one-to-many (1:N) systems, such as attendance management platforms, immigration control, or national identity databases. Throughput refers to the number of fingerprint verification operations a system can process per second and is critical for real-time applications. Template size indicates the amount of memory required to store fingerprint features, with smaller templates generally improving storage efficiency and computational performance. Although these additional metrics do not appear explicitly in all the reviewed studies, they are widely discussed in biometric system evaluations and help position the reviewed work within the broader fingerprint recognition research landscape.

3.0 Related Works

Fingerprint-based recognition systems have been extensively studied across application domains including biometric authentication, access control, financial security, and attendance management. A survey of literature published between 2012 and 2024 reveals notable advancements in preprocessing techniques, feature extraction strategies, and system architectures. However, challenges related to scalability, robustness, and security remain persistent. For example, Aranuwa and Ogunniye (2012) developed a fingerprint-based authentication system for secure electronic payment applications in Nigeria. While the system demonstrated improved security in user verification, limited details were provided regarding feature extraction algorithms or performance metrics such as FAR and FRR. Although the study established the relevance of fingerprint biometrics for secure identity management, it did not explore hybrid recognition approaches or advanced preprocessing techniques.

Akinduyite *et al.* (2013) proposed a fingerprint-based attendance management system that employed the Crossing Number (CN) method for minutiae extraction, alongside normalization, binarization, and thinning as preprocessing stages. Performance evaluation reported a false acceptance rate below 2% for small datasets; however, false rejection rates of up to 5% were observed for low-quality fingerprint images. Matching time increased with database size, highlighting early concerns regarding system scalability. While the study demonstrated the feasibility of minutiae-based recognition for attendance systems, it also revealed limitations that subsequent research sought to address through improved robustness and efficiency.

Subsequent studies focused on more scalable and digitally integrated architectures. Oyebola *et al.* (2018) developed a web-based fingerprint attendance system using standard minutiae extraction and template matching techniques. The system achieved an accuracy of 95% under controlled conditions, but matching times increased to approximately 4–5 seconds for a database of 500 users, indicating scalability constraints. The authors also reported increased false rejection rates when fingerprints were dry, smudged, or partially captured.

Ogundepo *et al.* (2019) implemented a real-time fingerprint authentication system for managing student records, incorporating normalization and thinning during preprocessing and employing minutiae-based identification. The system reported an equal error rate of approximately 3%; however, higher false rejection rates were observed when processing noisy fingerprint images. This study highlighted the difficulty of maintaining reliability under real-world imaging conditions without advanced enhancement techniques.

In order to address the limitations of single-feature approaches, hybrid recognition techniques were introduced. Krish *et al.* (2019) presented a hybrid fingerprint recognition system that combined minutiae and extended ridge features using a weighted fusion strategy. The system achieved an EER of about 2.5%, outperforming minutiae-only and ridge-only methods. However, this improvement came at the cost of increased computational complexity, with matching times exceeding 5 seconds for large datasets. The authors strengthened preprocessing through Gabor filtering, which improved robustness against noise and partial fingerprints.

Yang *et al.* (2019) provided a comprehensive review of fingerprint recognition challenges and emphasized the importance of hybrid feature integration for improved system reliability. Their analysis showed that minutiae-only systems typically exhibited EER values between 3 and 5%, while hybrid approaches achieved better accuracy at the expense of higher computational demands. Oloruntoba and Akinode (2020) proposed a web-based fingerprint attendance system that relied on minutiae features and relational database storage. Although the system achieved an accuracy of 94% for small university cohorts and reduced impersonation, it remained vulnerable to poor-quality fingerprint images and suffered from scalability limitations.

Görgel and Ekşi (2021) combined Gabor filtering with CNN-based minutiae recognition and achieved an accuracy of 97%. Despite its high accuracy, the system required substantial processing time due to the computational cost of convolutional layers, limiting its suitability for large-scale or real-time deployments. Rahman *et al.* (2023) developed a cloud-backed fingerprint attendance platform integrated with a mobile application. The system employed conventional preprocessing and minutiae matching techniques and achieved an accuracy of 93%. However, performance degraded when fingerprint quality was poor, resulting in an EER of approximately 4%. While cloud storage improved scalability, the absence of ridge-based or hybrid features limited system robustness.

Chhabra *et al.* (2023) advanced fingerprint segmentation and minutiae extraction by integrating deep convolutional neural networks, achieving an EER of approximately 2.8% and demonstrating strong robustness for latent fingerprints. However, the absence of ridge-based features limited the system's ability to exploit global fingerprint structure. Imran and Sarosh Umar (2023) combined Gabor filtering with minutiae-based recognition and reported an accuracy of 96%, although false rejection rates increased to about 5% for low-quality fingerprint images. These findings reinforced the persistent limitations of minutiae-only systems under challenging acquisition conditions.

Yadav *et al.* (2024) conducted an extensive review of hybrid fingerprint recognition approaches and reported that systems combining minutiae and ridge-flow features achieved EER values ranging from 2 to 4%. While hybrid systems demonstrated improved accuracy and robustness, the authors noted ongoing scalability challenges for large fingerprint databases. Mulay *et al.* (2024) proposed a deep learning ensemble framework for minutiae extraction and achieved an EER of 2.3%. Despite its strong resilience to fingerprint distortions, the model remained computationally intensive and did not incorporate ridge-based features, indicating opportunities for further hybrid integration.

Adedoyin *et al.* (2024) extended fingerprint recognition systems through IoT-based real-time attendance monitoring. Although the system achieved an accuracy of 95%, performance remained sensitive to noise due to reliance on minutiae-based extraction alone. The authors also reported performance degradation as the number of registered users increased. As cloud-enhanced biometric architectures gained prominence in the early 2020s, these studies collectively highlighted the trade-offs between accuracy, robustness, and scalability. A comparative summary of the reviewed works, including their strengths and limitations, is presented in Table 1.

Table 1: Summary of strengths and weaknesses fingerprint-based recognition systems

Author(s)	**Approach Proposed**	**Dataset / Environment**	**Strengths**	**Limitations**
Akinduyite *et al.* (2013)	Minutiae (CN method)	Small academic dataset (students)	Simple, accurate for clean images Low FAR (<2%)	1. High FRR for noisy/partial prints; 2. Poor scalability; 3. No ridge features
Aranuwa & Ogunniye (2012)	Fingerprint verification (algorithm unspecified)	E-payment environment in Nigeria	Improved identity security Useful for authentication	1. No detailed method; 2. No FAR/FRR report. 3. No ridge /minutiae distinction

Oyebola *et al.* (2018)	Minutiae (CN method), Web	University attendance system	95% accuracy; improved admin tasks	1. Matching time increases with DB size; 2. High FRR for dry/smudged prints
Ogundepo *et al.* (2019)	Minutiae (CN method)	Real-time student dataset	EER 3%; real-time operation	1. High FRR (6%) for noisy images; 2. No ridge features; limited scalability
Oloruntoba & Akinode (2020)	Minutiae (CN method), Web	University students	94% accuracy; reduces impersonation	1. Dependent on minutiae only; 2. Scalability challenges
Batubara *et al.* (2021)	Minutiae (CN method)	Small cohort	96% accuracy; emphasizes preprocessing	1. >3 sec matching time for 200 users; 2. No ridge features
Rahman *et al.* (2023)	Minutiae, Cloud + Mobile	Cloud attendance app	High accessibility; scalable cloud	1. EER 4%; struggles with noisy images; 2. No ridge features
Adedoyin *et al.* (2024)	Minutiae, IoT	IoT-based attendance	95% accuracy; real-time logging	1. Poor robustness to noisy images; 2. No ridge features
Krish *et al.* (2019)	Hybrid (Minutiae + Ridge)	Latent fingerprint dataset	EER 2.5%; strong robustness	1. High computation (>5 sec matching)
Yang *et al.* (2019)	Review of fingerprint methods	Multiple datasets	Detailed challenges; influential review	1. No specific system; 2. General analysis
Görgel & Ekşi (2021)	Gabor + CNN (Minutiae)	Experimental dataset	97% accuracy; strong enhancement	1. Very high computational cost
Chhabra *et al.* (2021)	CNN segmentation + minutiae	Latent fingerprints	EER 2.8%; improved segmentation	1. No ridge features; 2. Heavy computation
Imran & Sarosh Umar (2023)	Minutiae + Gabor filtering	Experimental dataset	96% accuracy; enhanced preprocessing	1. FRR up to 5% for noisy images; 2. No ridge-based features
| Mulay *et al.* (2024)	Deep learning (ensemble)	Multiple fingerprint datasets	EER 2.3%; robust minutiae detection	1. No ridge features; 2. Computationally heavy

4.0 Synthesis of Findings

Beyond summarizing individual studies, a comparative synthesis reveals clear distinctions between classical, hybrid, and deep learning–based fingerprint recognition approaches when evaluated for real-world attendance deployment. Classical minutiae-based systems remain attractive due to their simplicity, low computational cost, and ease of implementation, making them suitable for small-scale or resource-constrained environments. However, as consistently reported in the literature (Akinduyite *et al.*, 2013;

Oyebola *et al.*, 2018), their sensitivity to image quality often results in higher false rejection rates in uncontrolled classroom settings.

Hybrid approaches address many of these limitations by combining minutiae with ridge-based or texture-based descriptors. Studies such as Krish *et al.* (2019) and Yadav *et al.* (2024) demonstrated that hybrid systems achieve lower equal error rates and improved robustness to partial or noisy fingerprints, which are common in real attendance scenarios. The trade-off, however, lies in increased computational complexity, which can affect scalability when databases grow large.

Deep learning-based methods further improve robustness by learning discriminative representations directly from fingerprint images, showing strong performance under severe distortion or low-quality acquisition (Chhabra *et al.*, 2023; Mulay *et al.*, 2024). Despite their accuracy, these methods require substantial training data, high processing power, and specialized hardware, limiting their practicality for real-time attendance systems in many institutions. Overall, the literature suggests that hybrid fingerprint recognition currently offers the most balanced solution for real-world attendance deployment, providing improved accuracy and robustness while remaining more feasible than purely deep learning–based approaches.

4.1 Challenges in Fingerprint Recognition

Despite significant progress in fingerprint recognition research, several technical and practical challenges continue to limit system reliability, particularly in real-world attendance deployments. These challenges stem from variability in fingerprint quality, sensitivity of feature extraction techniques, computational constraints, security vulnerabilities, and cross-sensor inconsistencies. Fingerprint recognition is widely adopted due to its uniqueness, permanence, and relatively low acquisition cost. However, fingerprints captured under uncontrolled conditions frequently suffer from noise, smudging, uneven pressure, dry skin, perspiration, scars, and partial impressions. Yang *et al.* (2019) reported that low-quality fingerprints degrade ridge–valley clarity, thereby reducing the effectiveness of feature extraction. Reduced contrast and uneven illumination further increase false rejection rates. Although preprocessing techniques such as adaptive normalization and Gabor filtering improve ridge visibility, they cannot fully correct severe distortions in degraded samples.

Minutiae-based methods remain dominant due to their high discriminative capability. However, they are highly sensitive to minor variations in ridge structure. Jain *et al.* (2024) observed that errors introduced during binarization, thinning, or ridge discontinuities may produce spurious or missing minutiae, which subsequently reduce matching reliability. Under poor acquisition conditions, this sensitivity contributes to increased false rejection rates (Akinduyite *et al.,* 2013; Oyebola *et al.,* 2018). Systems that rely solely on minutiae struggle with partial fingerprints, damaged ridges, or extreme finger placement angles. Physical deformation presents another significant challenge. Variations in finger pressure and placement angle introduce nonlinear distortions that stretch or compress ridge structures. Bazen and Gerez (2002) demonstrated that such deformation can misalign ridge orientation fields and disrupt block-based feature estimation. Compensating for nonlinear distortion remains technically complex and computationally demanding.

Enhancement techniques such as Gabor filtering improve ridge visibility but may amplify noise when ridge frequency or orientation is inaccurately estimated. Görgel and Ekşi (2021) noted that improper parameter selection can introduce artifacts that blur ridge structures rather than clarify them. This issue is particularly pronounced in low-quality fingerprints with irregular ridge spacing. Hybrid systems that combine minutiae, ridge-based, and texture descriptors generally improve recognition performance. However, the integration of multiple feature types increases computational complexity. Krish *et al.* (2019) reported that hybrid systems require substantial processing time for orientation estimation, filtering, feature extraction, and multi-stage matching. The resulting computational burden may limit scalability in large biometric databases and real-time verification environments.

Security vulnerabilities also remain a concern. Fingerprint recognition systems are susceptible to presentation attacks using artificial replicas fabricated from materials such as silicone or gelatin. Without effective liveness detection mechanisms, even high-resolution sensors may fail to distinguish authentic fingerprints from spoofed samples. Milewski (2024) emphasized the growing importance of incorporating physiological or dynamic cues to strengthen system resilience. Finally, lack of standardization across sensors presents interoperability challenges. Differences in resolution, sensing technology, and output format complicate feature consistency across optical, capacitive, and ultrasonic devices. Jain *et al.* (2000) highlighted that cross-sensor variability can significantly degrade recognition accuracy when systems operate in multi-device environments. Collectively, these challenges highlight the persistent technical and operational limitations that continue to influence fingerprint recognition performance in real-world attendance systems.

4.2 Future Research Directions

Although fingerprint recognition technology has advanced considerably, several research priorities remain essential for improving reliability in real-world attendance systems. Future investigations should focus on bridging the persistent gap between laboratory performance metrics and operational deployment outcomes. Many existing models achieve high accuracy under controlled experimental conditions but demonstrate performance degradation when exposed to variable acquisition environments. Enhancing robustness to partial and low-quality fingerprints represents a critical direction for further study. In practical attendance settings, fingerprints are often captured quickly, under time constraints, and with varying levels of user cooperation. Research should therefore prioritize adaptive feature extraction models capable of maintaining stability when only limited ridge information is available. The development of more diverse and representative datasets will also support improved generalization.

Improving cross-sensor interoperability is another important area. Algorithms that perform well on a specific sensor type may exhibit reduced accuracy when applied to fingerprints captured using different sensing technologies. Future research should emphasize domain adaptation strategies and sensor-invariant feature representations to ensure consistent recognition performance across heterogeneous devices. Security and privacy protection remain central to the evolution of biometric attendance systems. Further work is required to develop lightweight template protection schemes, secure biometric transformations, and efficient encryption mechanisms that preserve matching accuracy while preventing template compromise. Solutions must balance strong security guarantees with real-time processing requirements.

Advances in machine learning continue to create opportunities for enhanced fingerprint recognition. Transformer-based architectures, improved convolutional neural networks, and hybrid learning frameworks may further strengthen representation learning under complex distortion conditions. Additionally, multi-modal biometric integration combining fingerprint data with complementary traits such as palmprints, vein patterns, or behavioral characteristics offers potential for improving resilience against spoofing and environmental variability. Finally, computational optimization remains essential for scalable deployment. Future systems must achieve high recognition accuracy while minimizing processing time and hardware requirements. Efficient model compression, algorithmic optimization, and resource-aware implementation strategies will be crucial for supporting large-scale attendance management systems in diverse institutional environments.

5.0. Conclusion

This review critically examined recent advances in fingerprint biometric recognition for modern attendance management systems. The analyzed literature demonstrates substantial progress in preprocessing, feature extraction, and matching strategies, particularly through refinement of minutiae-based methods, incorporation of ridge-based descriptors, and integration of hybrid recognition frameworks. These developments have significantly improved recognition accuracy and robustness under varying acquisition conditions.

Despite these advancements, persistent limitations remain. Image quality variability, nonlinear distortion, cross-sensor inconsistencies, computational constraints, and security vulnerabilities continue to influence system performance in real-world deployments. No single recognition strategy fully addresses all operational challenges. Minutiae-based approaches offer strong distinctiveness but remain sensitive to noise and deformation. Ridge-based methods enhance robustness but may lack fine discrimination. Hybrid techniques provide improved balance between accuracy and stability, though at increased computational cost. Deep learning models demonstrate promising resilience to distortion but require substantial data and processing resources, which may limit feasibility in large-scale or resource-constrained attendance systems.

Overall, the reviewed evidence indicates that hybrid fingerprint recognition currently provides the most practical compromise between accuracy, robustness, and computational feasibility for attendance management applications. Continued research focused on cross-sensor generalization, secure template protection, computational optimization, and adaptive learning frameworks will be essential for developing scalable and deployment-ready biometric attendance systems capable of operating reliably across diverse institutional environments.

References

1. Abdulrahman, S. A., & Alhayani, B. (2023). A comprehensive survey on the biometric systems based on physiological and behavioural characteristics. *Materials Today: Proceedings*, *80*, 2642-2646.
2. Adedoyin, M. A., Shoewu, O. O., Yussuff, A. I., Adenowo, A. A., Shitta, A., & Okedokun, O. (2024). Development of an IoT-Based Biometric Attendance Management System. *FUOYE Journal of Engineering and Technology*, *9*(3), 397-405.
3. Akinduyite, C. O., Adetunmbi, A. O., Olabode, O. O., & Ibidunmoye, E. O. (2013). Fingerprint-based attendance management system. *Journal of Computer Sciences and Applications*, *1*(5), 100-105.
4. Aranuwa, F. O., & Ogunniye, G. B. (2012). Enhanced biometric authentication system for efficient and reliable e-payment system in Nigeria. *International Journal of Applied Information Systems*, *4*(2), 56-61.
5. Batubara, T. P., Efendi, S., & Nababan, E. B. (2021, March). Analysis performance BCRYPT algorithm to improve password security from brute force. In *Journal of Physics: Conference Series* (Vol. 1811, No. 1, p. 012129). IOP Publishing.
6. Bazen, A. M., & Gerez, S. H. (2002). Systematic methods for the computation of the directional fields and singular points of fingerprints. *IEEE transactions on pattern analysis and machine intelligence*, *24*(7), 905-919.
7. Chhabra, M., Ravulakollu, K. K., Kumar, M., Sharma, A., & Nayyar, A. (2023). Improving automated latent fingerprint detection and segmentation using deep convolutional neural network. *Neural Computing and Applications*, *35*(9), 6471-6497.

8. Goyal, V., & Jindal, H. (2017). A REVIEW ON IMPROVED FINGER PRINT MATCHING USING MINUTIAE SINGULAR POINTS NETWORK. *International Journal of Research Science and Management*, *4*(2), 19-22.
9. Görgel, P., and Ekşi, A. (2021). Minutiae-Based Fingerprint Identification Using Gabor Wavelets and CNN Architecture. Electrica, 21(3).
10. Hong, L., Wan, Y., & Jain, A. (1998). Fingerprint image enhancement: algorithm and performance evaluation. *IEEE transactions on pattern analysis and machine intelligence*, *20*(8), 777-789.
11. Hoo, S. C., & Ibrahim, H. (2019). Biometric-Based Attendance Tracking System for Education Sectors: A Literature Survey on Hardware Requirements. *Journal of Sensors*, *2019*(1), 7410478.
12. Imran, M., & Sarosh Umar, M. (2023, December). A Novel Authentication Approach Based on Level 2 Minutiae-based Feature Extraction Using Gabor Filter. In *Proceedings of International Conference on Recent Advancements in Artificial Intelligence* (pp. 185-194). Singapore: Springer Nature Singapore.
13. Jain, A. K., Prabhakar, S., Hong, L., & Pankanti, S. (2000). Filterbank-based fingerprint matching. *IEEE transactions on Image Processing*, *9*(5), 846-859.
14. Jain, A. K., Ross, A. A., Nandakumar, K., & Swearingen, T. (2024). Fingerprint recognition. In *Introduction to Biometrics* (pp. 75-117). Cham: Springer International Publishing.
15. Krish, R. P., Fierrez, J., Ramos, D., Alonso-Fernandez, F., & Bigun, J. (2019). Improving automated latent fingerprint identification using extended minutia types. *Information Fusion*, *50*, 9-19.
16. Milewski, P. (2024). A Review of Image Thinning Algorithms. In *International Conference on Computer Information Systems and Industrial Management* (pp. 3-16). Springer, Cham.

Mingote, V., Miguel, A., Ribas, D., Giménez, A. O., & Lleida, E. (2019). Optimization of False Acceptance/Rejection Rates and Decision Threshold for End-to-End Text-Dependent Speaker Verification Systems. In *INTERSPEECH* (pp. 2903-2907).

17. Mizinov, P. V., Konnova, N. S., Basarab, M. A., & Pleshakova, E. S. (2024). Parametric study of hand dorsal vein biometric recognition vulnerability to spoofing attacks. *Journal of Computer Virology and Hacking Techniques*, *20*(3), 383-396.
18. Mulay, A. A., Grosz, S. A., & Jain, A. K. (2024, September). Learning a Robust Minutiae Extractor via an Ensemble of Expert Models. In *2024 IEEE International Joint Conference on Biometrics (IJCB)* (pp. 1-9). IEEE.
19. Ogundepo, O. Y., Omeiza, I. O. A., & Akpojaro, M. A. (2019). Development of a real time fingerprint authentication/identification system for students' record. *Nigerian Journal of Technology*, *38*(1), 212-222.
20. Oloruntoba, S. A., & Akinode, J. L. (2020). Students' Class Attendance Monitoring System Using Fingerprint. *Journal of Women in Technical Education and Employment*, *1*(2), 29-37.
21. Oyebola, B. O., Olabisi, K. O., & Adewale, O. S. (2018). Fingerprint for personal identification: a developed system for students attendance information management. *American Journal of Embedded Systems and Applications*, *6*(1), 1-10.
22. Pradeep, N. R., and Ravi, J. (2022). An revolutionary fingerprint authentication approach using Gabor filters for feature extraction and deep learning classification using convolutional neural networks. In Innovations in Electronics and Communication Engineering: Proceedings of the 9th ICIECE 2021 (pp. 349-360). Singapore: Springer Singapore.
23. Rahman, M. S., Rumman, K. M., Ahmmed, R., Rahman, A., & Sarker, M. A. (2023). Fingerprint based biometric attendance system. *European Chemical Bulletin*, *12*, 184-190.

24. Yadav, R., Awasthi, S., Yadav, S. P., and Upadhyay, P. (2024). Fingerprint Recognition System Study. In A Practitioner's Approach to Problem-Solving using AI (pp. 57-71). Bentham Science Publishers.
25. Yang, W., Wang, S., Hu, J., Zheng, G., & Valli, C. (2019). Security and accuracy of fingerprint-based biometrics: A review. *Symmetry*, *11*(2), 141.