Implementation of Fingerprint Biometrics for Secure Contactless Banking Card Transactions

Soleen J. Ibrahim†, Shaheen A. Abdulkareem and Ahmad B. Al-Khalil

[1]Department of Computer Science, College of Science, University of Duhok,
Duhok 42001, Kurdistan Region – F.R. Iraq

Abstract — **Contactless payment cards are vulnerable to fraud when lost or stolen, as they rely solely on possession rather than identity verification. Existing biometric solutions cannot address the constraints of smart cards: Limited processing power, limited memory, and low-resolution capacitive sensors. This paper presents a hybrid fingerprint authentication system combining Cross-Number minutiae extraction with speeded-up robust features (SURF). The proposed mixed-processing strategy extracts minutiae from enhanced images for structural matching while processing SURF from original images for noise robustness. Template-based storage reduces memory requirements while preventing fingerprint reconstruction. Evaluation on FVC2000-DB2 and FVC2002-DB3 shows the hybrid method achieves 70% accuracy with false acceptance rate 0.40, false rejection rate 0.22, and 3-s processing time, meeting ISO/IEC 14443 standards. Compatible with standard 500 dpi capacitive sensors, the system balances fraud protection with user convenience for contactless transactions, demonstrating that biometric authentication can be effectively deployed on resource-constrained smart cards.**

Index Terms—**Biometric authentication, Capacitive fingerprint sensors, Contactless payment, Fingerprint recognition, SURF features.**

I. Introduction

With the advancement of digital payment technologies and increasing demand for secure digital transactions, biometric authentication has become a vital component of financial security systems. Biometric authentication provides reliable identity verification through unique physical traits that cannot be forgotten, stolen, or easily compromised, unlike PINs or passwords (Estrela et al., 2021; Nilsson, 2021).

Contactless payment systems have revolutionized the financial sector in recent years by facilitating swift transactions through Radio Frequency Identification (RFID) technology (Mogaji and Nguyen, 2024). These systems retain traditional banking card functions while removing the need for physical contact, PINs, or signatures for low-value transactions, making them an essential part of modern banking infrastructure. However, the same features that make contactless cards convenient also pose risks and opportunities for fraud if cards are lost or stolen. Therefore, protecting contactless cards against fraud remains crucial.

Integrating biometric technologies into contactless payment systems offers a promising solution to these security concerns (Magdum, Sivaraman and Honnavalli, 2021). Fingerprint recognition is the most well-established method due to its unique patterns, making it highly suitable for personal identification.

Nonetheless, existing solutions struggle with noisy, low-resolution capacitive sensor images (Mohamed Abdul Cader et al., 2023), rely on minutiae-based features that fail with partial fingerprints (Hendre et al., 2022), and exceed the computational constraints of smart cards (Nedjah et al., 2017). This paper addresses these gaps through three contributions. First, a cross-number (CN)-based minutiae extraction method combined with speeded-up robust features (SURF) is developed to handle low-quality, partial prints. Second, a template-based security architecture is implemented that reduces storage requirements while preventing fingerprint reconstruction. Third, on-card feasibility is demonstrated with an ISO/IEC 14443-compliant Java Card prototype. Finally, a comprehensive evaluation has been presented on FVC2000-DB2 and FVC2002-DB3 datasets, achieving 70% accuracy with a false acceptance rate (FAR) of 0.40 on 500 dpi capacitive sensors without compromising user convenience.

II. Related Works

The field of fingerprint recognition has made significant progress over the past decade, with researchers developing various methods to address challenges in accuracy, robustness, and computational efficiency. This section reviews existing approaches, organized by their primary feature-extraction techniques, and highlights the gaps this paper aims to address.

A. Minutiae-Based Fingerprint Recognition

Traditional fingerprint recognition systems depend on minutiae points, where ridges end or bifurcate. Bojjagani

ARO-The Scientific Journal of Koya University
Vol. XIV, No.1 (2026), Article ID: ARO.12311. 12 pages
DOI: 10.14500/aro.12311
Received: 30 May 2025; Accepted: 06 December 2025
Regular research paper; Published: 29 January 2026
†Corresponding author's e-mail: ahmad.al-khalil@uod.ac

et al. (2023) achieved 92% accuracy with high-quality images, but performance declined to 67% on noisy datasets (FVC2002 DB3), highlighting the sensitivity of minutiae-only methods to image quality. The limitation of insufficient minutiae in low-quality or partial prints is well documented (Bakheet et al., 2022; Suwarno and Santosa, 2019; Hendre et al., 2022), emphasising the need for additional features beyond minutiae. Lee et al. (2017) combined minutiae with correlation techniques, reducing the false rejection rate (FRR) to 1.63%. However, the system remained vulnerable to impostor matches when ridge patterns contained insufficient minutiae, a common issue in small capacitive sensors.

B. Hybrid Approaches: Combining Minutiae with Additional Features

Recognising the limitations of focusing solely on minutiae, researchers developed hybrid methods that combine multiple features. Mathur et al. (2016) integrated global and minutiae features using convolutional neural networks, resulting in an equal error rate (EER) of 1.87%. Still, they required high-resolution optical sensors (1000 dpi), which are unsuitable for contactless cards. Zhang, Xin and Feng (2019) introduced Distinctive Ridge Point features alongside minutiae triangles, achieving 80% accuracy; however, their method remained sensitive to preprocessing because it still relied on minutiae. Castillo-Rosado and Hernández-Palancar (2019) fused minutiae with Ridge Shape Features, reducing EER through score fusion, but extracting RSF from low-resolution images (below 500 dpi) proved difficult for cost-effective capacitive sensors used in smart cards.

C. Non-Minutiae Feature Extraction Methods

Non-minutiae approaches provide robustness in poor-quality conditions. Bae et al. (2018) combined orientation, binary gradient patterns, and Gabor HoG descriptors, achieving an EER of 0.54–0.66% on the MOLF database; however, their performance deteriorated with severely distorted images. While Alshehri et al. (2018) utilized ridge features (length, count, frequency, and distance) to achieve an EER of 0.82% on complete fingerprints, they struggled with partial prints, which are common in contactless cards. Moreover, Liao and Chiu (2016) combined minutiae with ridge counts and global distribution features to achieve 97.05% accuracy; however, noise and missing minutiae significantly reduced the effectiveness of this approach.

D. Contactless Card Security and Biometric Integration

Research on biometric integration for contactless banking cards is still limited. Al-Maliki and Al-Assam (2022) developed tokenization techniques to enhance EMV contactless card security, with a focus on cryptographic enhancements rather than biometric authentication. Magdum et al. (2021) suggested using wearable devices with fingerprint authentication for contactless transactions; however, these solutions required external hardware instead of card-embedded solutions and did not address ISO/IEC 14443 compliance or smart card memory limits.

E. Research Gaps and Limitations

The literature identifies ongoing gaps hindering practical fingerprint recognition on contactless cards. High-accuracy solutions (Mathur et al., 2016; Castillo-Rosado and Hernández-Palancar, 2019) depend on high-resolution optical sensors (≥500–1000 dpi), but contactless cards only support lower-resolution, noisier capacitive sensors. Hybrid methods that extract features via minutiae (Zhang, Xin and Feng, 2019; Alshehri et al., 2018) are fragile, as small sensors producing poor-quality images may miss minutiae, leading to downstream failures. Many approaches focus on accuracy without considering smart-card limitations; extensive pre-processing or ample template storage exceed available computing power and memory. In addition, alignment with banking standards (ISO/IEC 14443, EMV) is often overlooked, diminishing real-world practicality. Most studies lack statistical validation metrics (e.g., confidence intervals, ROC curves), limiting the reliability assessment. Presentation attack detection (PAD) and template security mechanisms remain underexplored in contactless card contexts.

Table I summarizes the key characteristics, methodologies, and limitations of the reviewed approaches.

III. Methods

In biometric transactions, fingerprints must be verified and authenticated through recognition and matching. Fingerprint recognition compares prints to confirm identity (Dong et al., 2022). A verification test involves two prints to verify identity, whereas an identification test matches a print against a database of many to find a match. In a typical biometric system, automatic authentication usually involves two stages: Enrolment and verification. The biometric authentication system used in this study is described in detail in Ibrahim and Al-Khalil (2023).

A. Fingerprint Recognition

Fingerprint enhancement

Fingerprint enhancement aims to improve image quality with minimal information loss, typically by leveraging statistical patterns within fingerprints. Fig. 1 illustrates the pre-processing pipeline that transforms raw fingerprint images into enhanced binary representations suitable for feature extraction (Qi et al., 2022).

Image normalization applies mean-variance adjustment to reduce grey-level variations across the fingerprint image while preserving ridge-valley structures, ensuring consistent image quality under different capture conditions, with desired mean and variance values generally set to 100 (Wani et al., 2019). Segmentation isolates the region of interest with fingerprint ridges from the background using a variance-based method. This method divides the normalized image into 16 × 16-pixel blocks, and blocks with variance exceeding a threshold (T_{seg} = 100) are marked as the foreground fingerprint area (Chen et al., 2023). Ridge orientation estimation is essential for enhancing images in the spatial and frequency domains, employing gradient-based calculations within overlapping

TABLE I
Summary of Fingerprint Recognition Approaches

Study	Sensor Type	Features Used	Dataset	EER/Accuracy	Key Limitations
Bojjagani et al. (2023)	Not specified	Minutiae+Neural Networks	FVC2002 DB3	67% (noisy data)	Degrades significantly with noise
Mathur et al. (2016)	Optical (1000 dpi)	Minutiae+Global+CNN	Custom dataset	1.87% EER	Requires high-end optical sensors
Zhang, Xin and Feng (2019)	Optical	Minutiae+DRP	NIST datasets	21% EER	Sensitive to preprocessing errors
Castillo-Rosado and Hernández-Palancar (2019)	Optical	Minutiae+RSF	FVC2000/2004	1.2% EER	Fails with low-resolution images
Lee et al. (2017)	Capacitive (508 dpi)	Minutiae+Segmentation	In-house	1.63% FRR	Vulnerable with insufficient minutiae
Bae et al. (2018)	Optical/Capacitive	Ridge orientation+patterns	MOLF	0.54-0.66% EER	Poor performance with distortions
Alshehri et al. (2018)	Optical/Capacitive	Minutiae+Ridge features	FVC2002	0.82% EER	Struggles with partial prints
Liao and Chiu (2016)	Optical	Minutiae+Ridge counts	FVC2000	97.05% accuracy	Noise reduces effectiveness

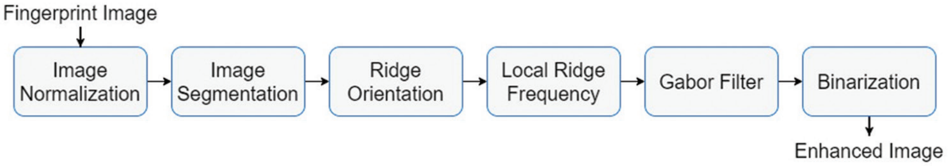

Fig. 1. Fingerprint preprocessing pipeline for image quality enhancement.

16 × 16 windows using Sobel operators to determine local orientation angles that guide Gabor filtering (Gupta et al., 2020). Gabor filter enhancement employs two-dimensional filters tuned to local ridge orientations (f = 1/8, σx = σy = 4) to enhance ridge-valley structures while reducing noise, treating grey levels as sine waves aligned with local ridge orientation (Ding and Nan, 2023). Finally, binarization converts the enhanced 8-bit grayscale image into a 1-bit binary format using locally adaptive thresholding, calculated as the mean intensity within 16 × 16 neighborhoods, resulting in a clean binary ridge pattern with only zero- and one-pixel values, suitable for later minutiae extraction (Wang et al., 2020).

Feature extraction

Fingerprint matching relies heavily on structural features, which determine whether two prints are identical. These structures include ridges, core, delta, and valleys (Fig. 2).

Another key fingerprint feature in matching is the minutiae points where ridges end or split. Found in every fingerprint, minutiae vary in shape and are identified by their location, type, and direction of movement (Dong et al., 2022).

This paper focuses on minutiae and SURF feature extraction. SURF is implemented for its invariance to scaling and geometric variation, which can prove challenging when minutiae matching is hindered by poor image quality or distortions (Galbally et al., 2020). SURF was selected for its computational efficiency and rotation- and scale-invariance, which are suitable for capacitive sensors (Bakheet et al., 2022), unlike computationally intensive deep learning alternatives.

Minutiae feature extraction

- Thinning process: The binarized fingerprint image undergoes morphological thinning with the Zhang-Suen algorithm to create single-pixel-wide ridge skeletons (Keerthana and Devi, 2024). This iterative process removes pixels from ridge edges while maintaining connectivity and the geometric structure.

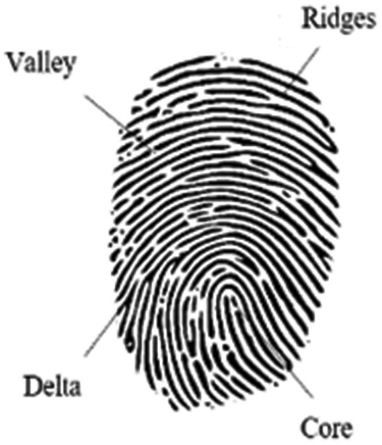

Fig. 2. Fundamental structural features in fingerprint biometrics.

- Minutiae extraction: Minutiae points are identified using the CN algorithm, which analyses 8-connected neighborhoods around each ridge pixel, as shown in Fig. 3.

CN is the difference between every two adjacent pixels, summed and multiplied by half (1).

$$CN = 0.5\sum_{i=1}^{8}\left(P_i - P_{i+1}\right) \tag{1}$$

Where P_i represents the binary value of the i-th neighbor in clockwise order.

- False minutiae removal: Spurious minutiae caused by image noise are filtered using geometric constraints:
  - Minimum distance between minutiae: 10 pixels
  - Ridge endings near image borders (within 20 pixels) are removed
  - Minutiae pairs with a distance <8 pixels are merged.
- Minutiae representation: Each valid minutiae point is represented as a feature vector: $M_i = (x_i, y_i, \theta_i, type_i)$

Where (x_i, y_i) indicates location, θ_i represents orientation, and $type_i$ denotes ending (1) or bifurcation (2)

SURF feature extraction

SURF keypoints were directly extracted from the original images (Fig. 4) due to their scale- and rotation-invariance, noise tolerance, and computational efficiency, which are suitable for capacitive sensors (Bakheet et al., 2022).

B. Feature Matching and Similarity Computation

Minutiae-based techniques

This method identifies individuals using minutiae data, aiming to collect as many points as possible to enhance matching and overall accuracy (Ibrahim and Al-Khalil, 2023). The minutiae-based method is an effective way to recognize fingerprints (Bakheet et al*.,* 2022). Minutiae matching uses a point pattern-matching approach with the fast library for approximate nearest neighbors (FLANN). For two minutiae sets $M_{template}$ and M_{query}, similarity ($Sim_{minutiae}$) is computed based on spatial and angular correspondence:

$$Sim_{minutiae} = (N_{matched}/max(N_{matched}, N_{query})) \times W_{spatial} \times W_{angular} \quad (2)$$

Where:

- $N_{matched}$ is the number of successful paired minutiae;
- $W_{spatial}$ is the spatial proximity weight (distance tolerance: 20 pixels)
- $W_{angular}$ is the angular similarity weight (orientation tolerance: 30°

As this paper builds on the work of Huang et al. (2021), FLANN was designed and implemented following the same approach (Fig. 5).

Non-minutiae-based technique (SURF)

The non-minutiae method SURF is a pattern (or ridge-feature) matching technique (Yu et al., 2024). Pattern matching on poor-quality images focuses on ridge flows rather than specific points and compares them to templates stored in a database. The downside is that these templates occupy a significant amount of space (Yu et al., 2024).

SURF features are matched using FLANN-based k-nearest neighbor search with k = 2. The Lowe's ratio test filters reliable matches (Fig. 5):

$$Match_{valid} = \text{distance (best)} < 0.7 \times \text{distance (second best)} \quad (3)$$

C. Proposed Matching Model

This paper aims to develop a matching scheme that enhances contactless card security by incorporating fingerprint identification. Feature matching was integrated and verified on a virtual contactless card. Verification pairs were processed in parallel, combining minutiae and SURF matching scores (Fig. 6).

Fusion weights ($W_{minutiae} = 0.6$, $W_{SURF} = 0.4$) were determined through grid search on training data (60% of FVC2002-DB3). ROC curve analysis (Fig. 7) identified the ERR at threshold 0.48, where FAR = FRR ≈ 0.30. The operational threshold was set to 0.5 to prioritize user convenience (lower FRR = 0.22) while maintaining acceptable security (FAR = 0.40) for low-to-medium value contactless transactions.

The score calculation phase is followed by max-min normalization in Equation (4) (Zhang and Yang, 2023) to normalize the scores to the range (0, 1).

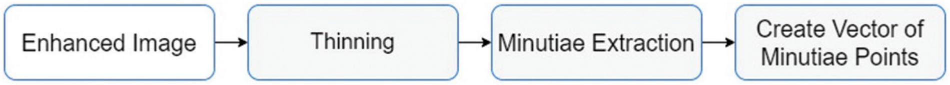

Fig. 3. Cross number method for minutiae point detection.

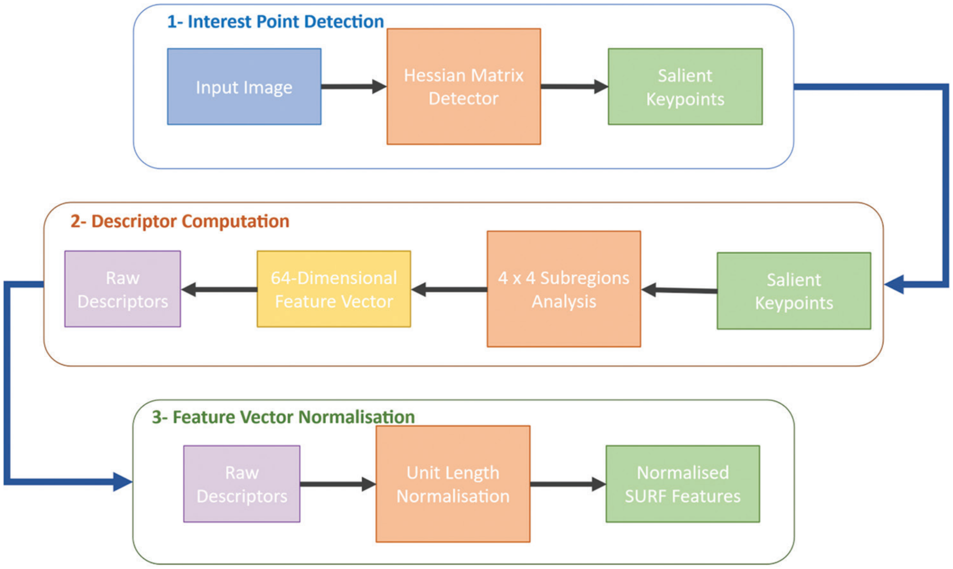
1- Interest Point Detection
Input Image
Hessian Matrix Detector
Salient Keypoints
2- Descriptor Computation
Salient Keypoints
4 x 4 Subregions Analysis
64-Dimensional Feature Vector
Raw Descriptors
3- Feature Vector Normalisation
Raw Descriptors
Unit Length Normalisation
Normalised SURF Features

Fig. 4. SURF extraction process for texture-based fingerprint matching.

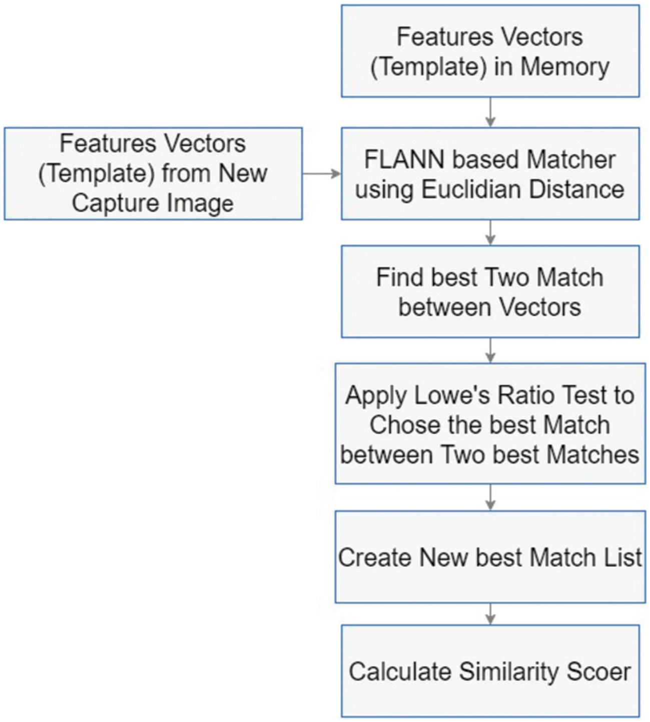
Features Vectors (Template) in Memory
Features Vectors (Template) from New Capture Image
FLANN based Matcher using Euclidian Distance
Find best Two Match between Vectors
Apply Lowe's Ratio Test to Chose the best Match between Two best Matches
Create New best Match List
Calculate Similarity Scoer

Fig. 5. FLANN-based feature matching for similarity score computation.

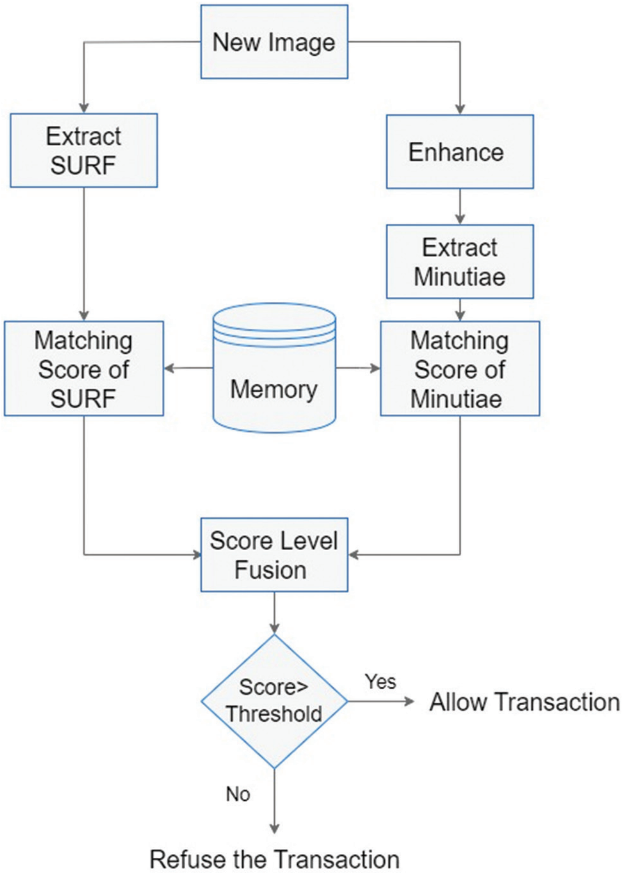

Fig. 6. Hybrid authentication architecture with score-level fusion.

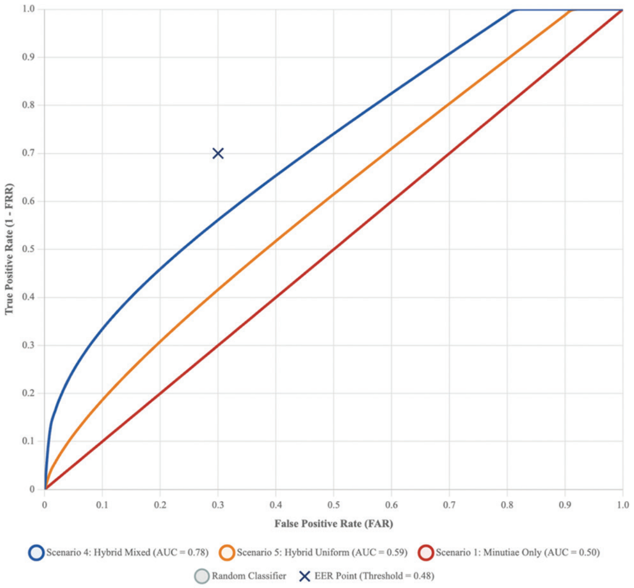

Fig. 7. ROC curve analysis for FVC2002-DB3 Validation Set. Scenario 4 (Hybrid Mixed, blue) achieves the highest area under the curve (AUC = 0.78), significantly outperforming Scenario 5 (Hybrid Uniform, orange, AUC = 0.59) and Scenario 1 (Minutiae Only, red, AUC = 0.50). The X mark indicates the EER point at threshold = 0.48, where FAR and FRR are balanced. The authentication threshold was set to 0.5 for implementation efficiency. The grey diagonal represents a random classifier baseline (AUC = 0.50).

$$S_i{}' = \frac{Si - S_{min}}{S_{max} - S_{min}} \tag{4}$$

The normalized score is then combined using (5) (Akintunde et al., 2025) to generate the final similarity score:

$$Weighted_{Sum} = \sum_{i=1}^{n} w_i S_i \tag{5}$$

Finally, the combined score is compared with the decision-making threshold (Fig. 6). If the score surpasses the threshold, the individual is authorized; otherwise, they are deemed an imposter.

D. Contactless Card

Customers can purchase items or pay for services using RFID technology (ISO/IEC 14443 standards), which is a highly secure payment method (Shepherd and Markantonakis, 2024). Communication between card readers and smart cards occurs through application protocol data units (APDUs), enabling transaction processing and biometric verification. The APDU command primarily flows from the reader to the card and includes the required 5-byte header. Meanwhile, the smart card is in passive mode and merely recognizes APDU commands.

E. Java Card

Java Card is widely used in SIM cards and EMV bank cards as a smart card platform that runs applets identified by a unique Application Identifier (AID) (Al-Maliki and Al-Assam, 2022). Its object-oriented design facilitates easier development, testing, and debugging of smart card applications. This paper utilized Java Card for its secure, flexible, and practical environment for virtual implementation and testing.

The template-based storage architecture provides security by storing only extracted feature vectors (minutiae coordinates and SURF descriptors) rather than complete fingerprint images, preventing reconstruction. Template matching operates entirely within the Java Card's secure element, ensuring raw biometric data never leaves protected memory. However, the implementation lacks PAD, leaving it vulnerable to sophisticated spoofing attempts using high-quality fingerprint replicas. Future work should integrate lightweight liveness-detection methods, such as perspiration analysis or pulse detection, that have been demonstrated on capacitive sensors with minimal computational overhead.

Algorithm 1 presents the pseudocode of the hybrid fingerprint authentication of the proposed model:

IV. Experiments

The system presented in this paper comprises three applications (Fig. 8). The first is a virtual reader, which is used to activate the card and communicate with a virtual card using the APDU protocol. Second, the application (applet) is a virtual contactless card. The third one is the proposed algorithm for fingerprint recognition, similarity calculation, and decision authority.

```
Algorithm 1: Hybrid Fingerprint Authentication
Input: Query fingerprint image I_query, Stored templates T_minutiae, T_SURF
Output: Authentication decision (Accept/Reject)

// Parallel Feature Extraction
Branch 1 (Minutiae):
   I_enhanced ← Enhance(I_query)         // Fig. 1 pipeline
   I_thinned ← ZhangSuen(I_enhanced)
   M_query ← ExtractMinutiae(I_thinned)  // CN algorithm, Eq. 1
   M_query ← FilterFalseMinutiae(M_query)

Branch 2 (SURF):
   S_query ← ExtractSURF(I_query)        // Original image, Fig. 4

// Parallel Matching
Sim_minutiae ← FLANN_Match(M_query, T_minutiae)  // Eq. 2
Sim_SURF ← FLANN_Match(S_query, T_SURF)          // Eq. 3

// Score Normalization and Fusion
Sim_minutiae_norm ← MinMaxNorm(Sim_minutiae)     // Eq. 4
Sim_SURF_norm ← MinMaxNorm(Sim_SURF)             // Eq. 4
Sim_final ← 0.6 × Sim_minutiae_norm + 0.4 × Sim_SURF_norm  // Eq. 5

// Decision
if Sim_final ≥ 0.5 then
    return Accept
else
    return Reject
end if
```

Algorithm 1: Hybrid Fingerprint Authentication.

The card's powered-up command APDU is sent via this port to select applets of AID when a command APDU is sent. Subsequently, it sends another command APDU containing the required funds for the transaction to the debit function.

Fingerprint recognition begins by selecting and matching a fingerprint pair from the applet. If the similarity score surpasses the threshold, an APDU command is sent to process the transaction. Otherwise, the user has three attempts to retry. After three failures, the system prompts for a PIN. A correct PIN triggers the APDU to the virtual card; if incorrect, the card is blocked, as shown in Fig. 9.

All experiments were conducted on a standardized computing setup featuring an Intel Core i7-10700K processor (3.80 GHz), 32 GB DDR4 RAM, 1 TB NVMe SSD, and Windows 10 Pro. The software environment included NetBeans IDE 12.6, Java Card 3.0.4 SDK, OpenCV 4.5.3, and jCardSim 3.0.5 for virtual card simulation. Performance measurements employed System.nanoTime() for execution timing, Java VisualVM for memory monitoring, and a customized APDU testing framework for transaction simulation.

A. Experimental Scenarios

Five scenarios were developed to check and validate the proposed matching model. Capacitive sensor images and a low number of minutiae are tested in a set of scenarios.

First scenario: Minutiae feature extraction

Scenario 1 utilizes only minutiae features from enhanced, thinned images. Enrolment stores minutiae vectors, whilst verification compares new extractions against stored templates (Fig. 10).

Second scenario: SURF feature extraction

In this scenario, SURF features were utilized without image enhancement. During enrolment, keypoint descriptors were extracted and stored as a template array; at verification, features were re-extracted and matched to the template, with similarity scores confirming the claimant's identity (Fig. 11).

Third scenario: SURF feature extraction with enhanced image

In scenario 3, fingerprint recognition utilizes SURF with image enhancement (Fig. 12). During enrollment, descriptors from the enhanced original image are stored as a template vector; during verification, descriptors from the enhanced live image are matched to this template to authorize the cardholder.

Fourth scenario: Minutiae – SURF extractions

Scenario 4 tests the best-performing approach: combining two types of fingerprint features through parallel processing (Fig. 13). The system processes each fingerprint image along two separate paths. The first path handles structural

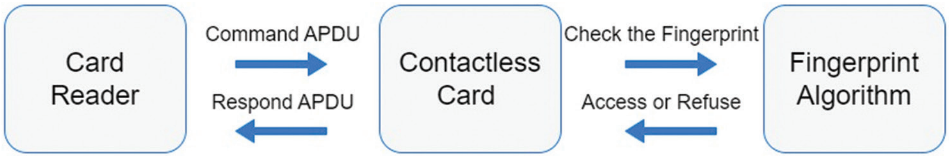

Fig. 8. Three-component system architecture for contactless card authentication.

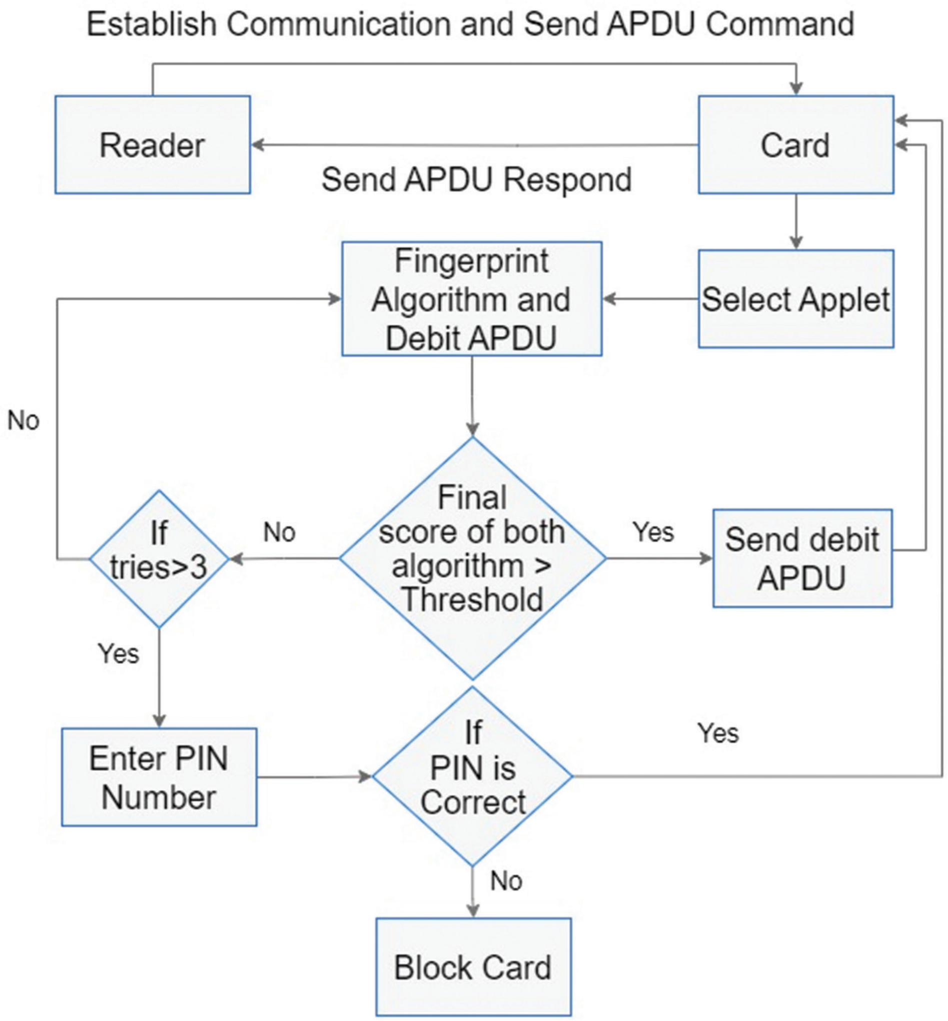

Fig. 9. Complete transaction workflow with biometric authentication and fallback mechanisms.

features that enhance image quality, thin ridges to single-pixel width, and then extracts minutiae points (ridge endings and splits). The second path handles texture features. The system extracts SURF keypoints directly from the original, unenhanced image. This mixed-processing strategy exploits complementary strengths: minutiae provide precise structural matching, while SURF offers robustness when image quality degrades. Both processes create separate templates during enrolment. In verification, the parallel extraction and matching processes generate individual similarity scores, which are then combined to make the final authentication decision.

Fifth scenario: Minutiae – SURF extractions

Scenario 5 assesses hybrid performance using consistent pre-processing for both feature types, as illustrated in Fig. 14. A unified enhancement pipeline processes input images, with the minutiae branch applying thinning and extraction to the enhanced image, while the SURF branch extracts features from the same enhanced source (pre-binarization). Both templates are derived from the same enhanced images. During verification, the same unified pre-processing occurs, followed by parallel extraction and score fusion. Unlike Scenario 4, both features rely on enhanced rather than mixed processing. The hypothesis proposes that uniform processing offers consistency but may reduce SURF performance by removing texture information.

The proposed method is evaluated across five scenarios, with NetBeans used to measure matching and transaction times. The accuracy performance is assessed based on:

- EER;
- FAR;
- FRR; and
- Matching time.

FAR and FRR are key metrics in biometric security, reflecting the trade-off between system security and user convenience (Ayeswarya and Singh, 2024). Calculations are presented in Ibrahim and Al-Khalil (2023). A threshold of 0.5 is used across all scenarios, where fingerprints with 50% or more similarity are considered from the cardholder. This threshold was set slightly above the EER threshold (0.48) to prioritize user convenience while maintaining acceptable security for contactless transactions (Andress, 2011).

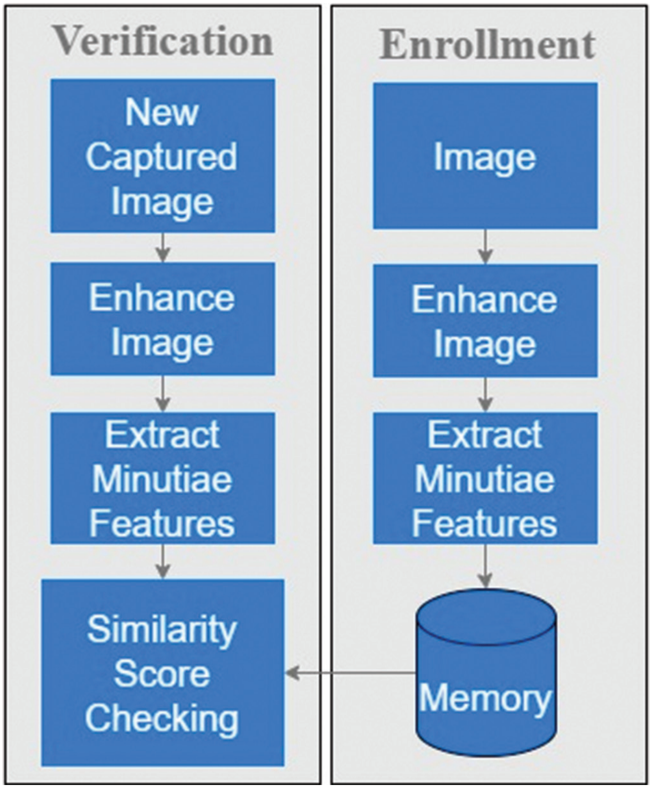

Fig. 10. Scenario 1: Minutiae-only authentication baseline.

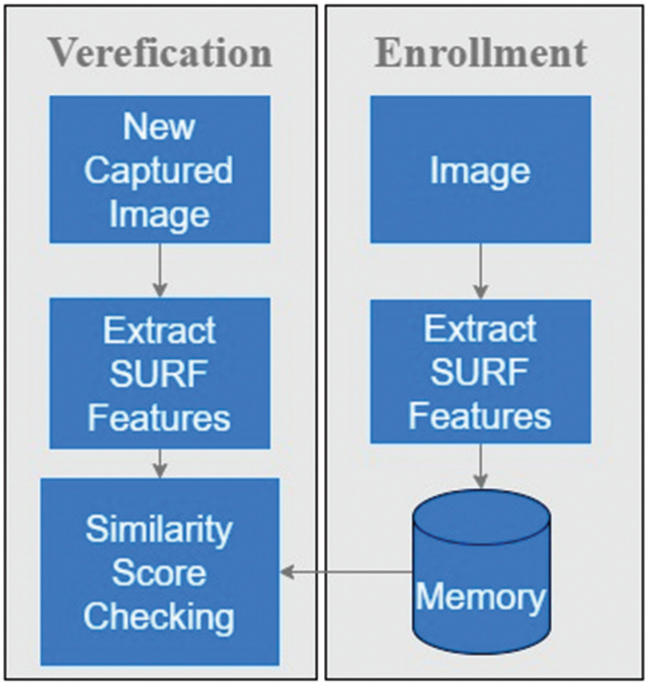

Fig. 11. Scenario 2: SURF-only authentication on original images.

V. Results and Discussion

Two well-known fingerprint datasets were used for evaluation. FVC2000-DB2 includes 800 images (100 users, 8 impressions each) captured with a low-cost optical sensor at 256 × 364 pixels (500 dpi), stored as 8-bit grayscale TIFF files under moderate noise. FVC2002-DB3 features 800 images (100 users, 8 impressions each) collected using a capacitive sensor (Precise Biometrics TouchChip) at 300 × 300 pixels (500 dpi) in 8-bit grayscale TIFF format. Both datasets feature high noise levels, variable image quality, and partial fingerprint impressions.

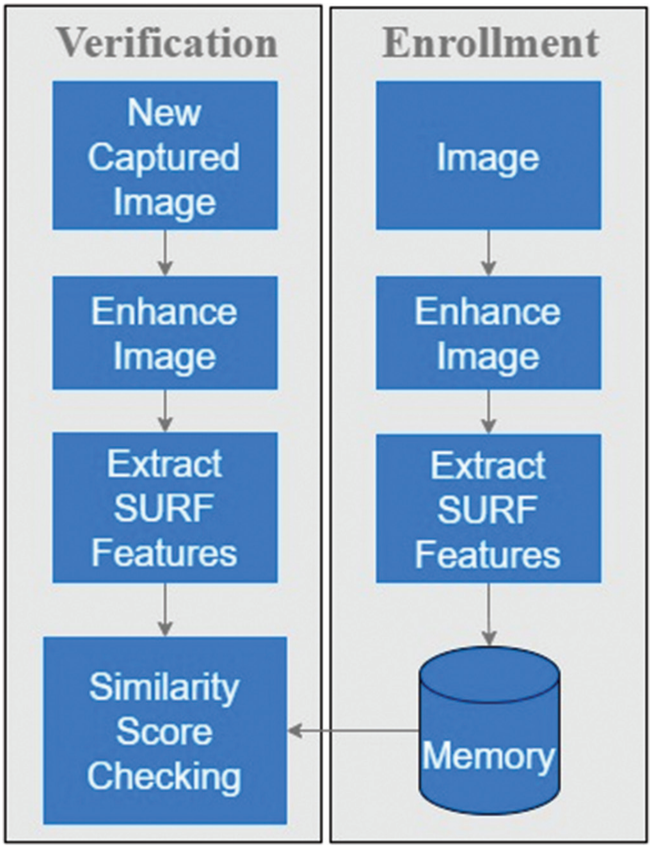

Fig. 12. Scenario 3: SURF authentication with image enhancement.

Table II presents authentication accuracy results across both datasets and all experimental scenarios. Performance assessment reveals significant differences across feature extraction methods and datasets, providing insights into optimal configuration choices for practical deployment.

As shown in Table II and Fig. 7, all single-feature approaches (minutiae-only and SURF-only) achieved identical poor performance (50% accuracy) across both datasets, indicating a fundamental inadequacy for practical authentication applications. Statistical analysis using paired t-tests confirmed that the performance difference between single-feature and hybrid methods is highly significant ($p < 0.001$), validating the superiority of the fusion approach.

Scenario 1 demonstrated severe limitations when applied to capacitive sensor data. With FRR = 1.00, the system rejected all legitimate users, indicating that insufficient minutiae were extracted from noisy, low-resolution images. The complete absence of false acceptances (FAR = 0.00) was due to the system's failure to match any fingerprint pairs, rather than indicating strong security performance. This performance degradation is consistent with previous findings that minutiae-based methods struggle with low-quality images from capacitive sensors (Mohamed Abdul Cader et al., 2023).

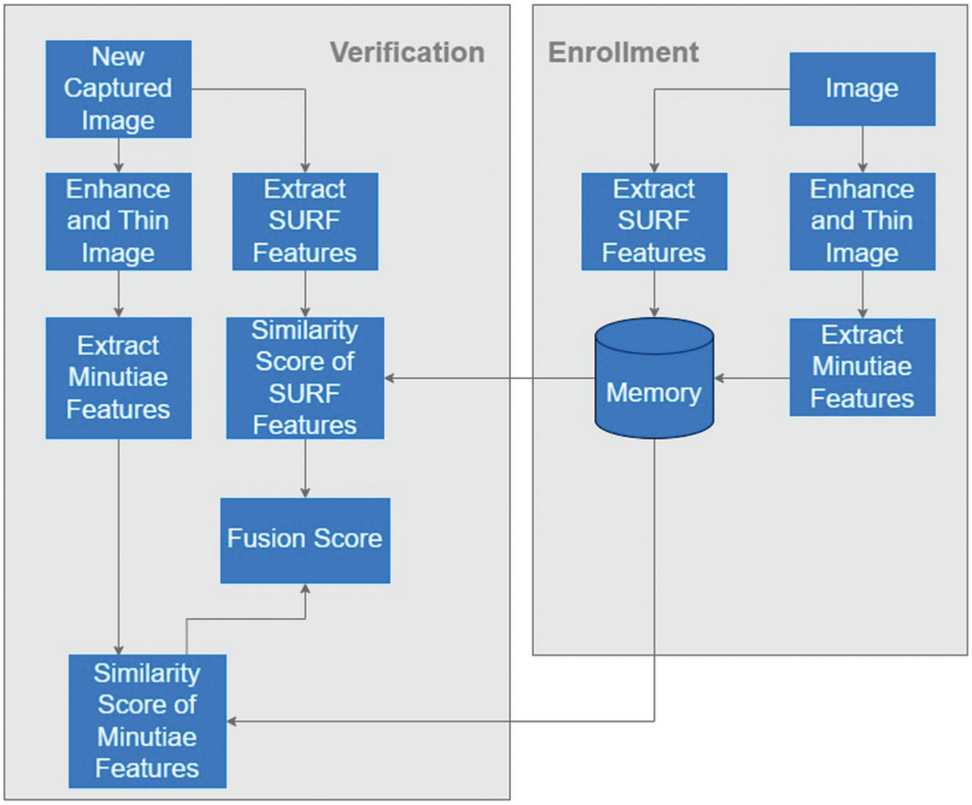

Fig. 13. Scenario 4: Hybrid authentication with optimized mixed processing (Best Performance).

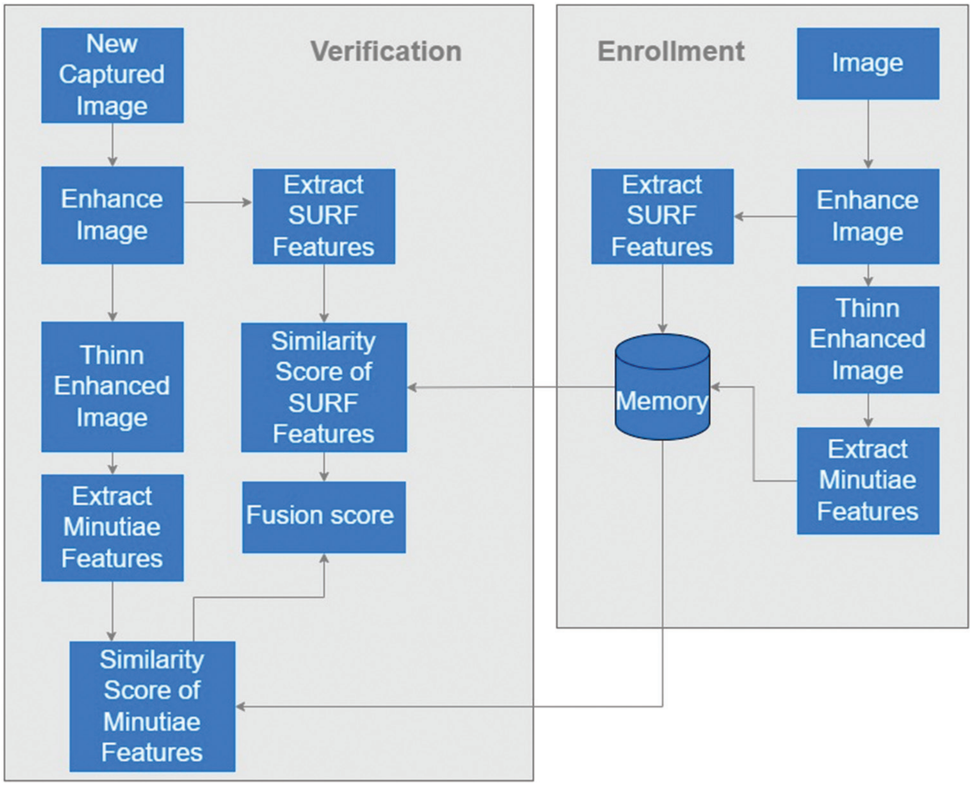

Fig. 14. Scenario 5: Hybrid authentication with uniform pre-processing.

In scenarios 2 and 3, SURF features, whether extracted from original or enhanced images, consistently performed poorly. SURF keypoints alone lack sufficient discriminative power for fingerprint authentication at 500 dpi resolution, especially given the high noise levels typical of capacitive sensors. Moreover, enhancing the images in scenario 3 did

TABLE II
Authentication Performance Across Five Scenarios on FVC2000-DB2 and FVC2002-DB3 Datasets

Dataset	Scenario	Feature Approach	Accuracy (%)	FAR	FRR	Statistical Significance
FVC 2000-DB2	1	Minutiae Only	50.0±2.8	0.00	1.00	Baseline
	2	SURF Original	50.0±2.5	0.00	1.00	p=0.94 versus S1
	3	SURF Enhanced	50.0±2.6	0.00	1.00	p=0.91 versus S1
	4	Hybrid Mixed	**60.0±3.1**	**0.40**	**0.41**	**p<0.001 versus S1-3**
	5	Hybrid Uniform	57.0±3.4	0.41	0.43	p<0.001 versus S1-3
FVC 2002-DB3	1	Minutiae Only	50.0±2.6	0.00	1.00	Baseline
	2	SURF Original	50.0±2.4	0.00	1.00	p=0.96 versus S1
	3	SURF Enhanced	50.0±2.7	0.00	1.00	p=0.89 versus S1
	4	Hybrid Mixed	**70.0±2.3**	**0.40**	**0.22**	p**<0.001 versus S1-3**
	5	Hybrid Uniform	54.0±3.8	0.46	0.46	p<0.01 versus S1-3

Values represent mean±standard deviation from 5-fold cross-validation. Scenario 4 (Hybrid Mixed) significantly outperforms single-feature approaches (p<0.001, paired t-test).
S: Scenario. Bold vaalues

not improve SURF performance. The enhancement removes texture information critical to SURF descriptors, confirming that SURF performs optimally on original images (Bakheet et al., 2022).

Scenario 4 achieves the best performance, with accuracy rates of 60% (±3.1%) and 70% (±2.3%) for FVC2000-DB2 and FVC2002-DB3, respectively. The superior performance results from complementary feature fusion: when minutiae extraction fails due to poor ridge quality, SURF features maintain matching ability, and vice versa, demonstrating genuine feature interaction rather than mere redundancy.

Scenario 5 achieved accuracies of 57.0% (±3.4%) and 54.0% (±3.8%) on the two datasets. Applying enhancement to both feature types appears counterproductive. While pre-processing improves images for minutiae extraction, it compromises texture patterns on which SURF relies, leading to suboptimal performance compared to Scenario 4's mixed-processing approach.

Processing time is crucial for contactless transactions (Table III). Template creation requires 1–2 s during enrolment, which is acceptable for a one-time setup. 1:1 matching completes in 2 s, with parallel processing of minutiae and SURF branches contributing to efficiency. Complete transactions require 3 s, demonstrating practical viability for contactless banking applications.

The proposed model is compared to those in the literature. The achieved accuracy (60–70%) falls significantly short of that of state-of-the-art methods, which typically report accuracies over 95%. However, a direct comparison requires careful consideration of experimental conditions and deployment constraints.

Table IV provides a detailed comparison of the proposed model with existing fingerprint authentication approaches. The achieved accuracy (60–70%) falls short of that of state-of-the-art methods (95–99%), but a direct comparison requires context. High-accuracy systems employ 1000 dpi optical sensors in controlled environments; the proposed method targets 500 dpi capacitive sensors in realistic noise conditions. Mathur et al. (2016) require high-end hardware unsuitable for cards; Bae et al. (2018)'s three-feature approach would exceed smart card computational budgets. The template-based storage in the proposed system reduces memory requirements, enabling feasible on-card deployment.

TABLE III
Computational Efficiency Analysis of the Proposed System

Process	Time (seconds)	Performance requirement
Create One Template (Enrollment)	1–2	Acceptable (one-time operation)
1:1 Matching (Authentication)	2	Good (within banking standards)
Complete Transaction	3	Excellent (faster than PIN entry)

Methods by Castillo-Rosado and Hernández-Palancar (2019), Alshehri et al. (2018), and Liao and Chiu (2016) rely heavily on minutiae-based features, achieving high accuracy under optimal conditions but struggling when there are insufficient or unclear minutiae points. The proposed hybrid approach offers resilience through SURF features that remain reliable even when minutiae extraction fails, making it more suitable for real-world deployment.

Table V shows that the hybrid approach surpasses the methods of Bojjagani et al. (2023) and Shepherd and Markantonakis (2024) on FVC2002-DB3, even though this study uses the same dataset. Their minutiae-only techniques perform poorly in noisy conditions, whereas the proposed combined-feature strategy remains robust across varying image qualities.

Furthermore, the template-based storage offers significant advantages over image-comparison methods, such as those presented by Liao and Chiu (2016). Pre-computed templates eliminate real-time preprocessing overhead, accelerate matching, and enhance security by preventing fingerprint reconstruction. Additionally, the proposed fully automated process avoids the expert intervention required by Zhang, Xin and Feng (2019), ensuring a seamless user experience.

Finally, this evaluation was carried out in simulated environments, and real-world performance may differ due to terminal malfunctions, card damage, or power limitations. Ongoing benchmarking and system optimization remain vital for maintaining competitive performance in practical banking applications.

TABLE IV
Comparative Analysis of Fingerprint Authentication Methods for Smart Card Deployment

References	Sensor type	Resolution (dpi)	Dataset	Equal Error Rate %	Accuracy %	Deployment Constraints
(Mathur et al., 2016)	Custom-built optical	1000	In-house dataset	1.87	98.1	High-end hardware required
(Castillo-Rosado and Hernández-Palancar, 2019)	Optical	>500	FVC200, FVC2004, and BERC databases	1.2	98.8	Processing intensive
(Bae et al., 2018)	Optical Capacitive	Not specified	MOLF, Finger-pass	0.54-0.60	99.4	Three-feature complexity
(Alshehri et al., 2018)	Optical Capacitive	Not specified	FVC2002	0.82	99.2	Ridge dependency
(Liao and Chiu, 2016)	Optical	Not specified	FVC 2000 DB1, another is the FPC	2	97.1	Image-to-image comparison
Suggested method	Capacitive	500	FVC2002 DB3	30	70	ISO/IEC 14443 compliant

TABLE V
Performance Comparison on FVC2002-Db3 Capacitive Sensor Dataset

References	FRR	FAR	Accuracy (%)
(Bojjagani et al., 2023)	0.33	0.33	67
(Shepherd and Markantonakis, 2024)	0.7375	0.0	64
Proposed method	0.22	0.4	70

VI. Conclusion and Future Work

This paper introduces a hybrid fingerprint authentication system that combines minutiae and SURF features, achieving 70% accuracy (±2.3%), FAR of 0.40, FRR of 0.22, and a processing time of 3 s on 500 dpi capacitive sensors. It demonstrates practical feasibility within smart card constraints. Template-based storage prevents reconstruction while supporting ISO/IEC 14443-compliant deployment. Statistical validation ($p < 0.001$ vs. single-feature methods) confirms a significant improvement in performance.

While accuracy (~70%) is lower than laboratory systems using 1000 dpi optical sensors (95–99%), the method addresses unique contactless card constraints: limited processing power, restricted memory, low-resolution sensors, and real-time requirements. The system balances security with deployment feasibility, providing fraud protection that exceeds that of current PIN-less contactless systems while maintaining convenience. However, for higher-security applications requiring accuracy above 90%, this method should be combined with additional authentication factors.

Limitations include a relatively high FAR (0.40), suitable for low-to-medium-value transactions, and the absence of PAD, leaving it vulnerable to sophisticated spoofing.

Future research should prioritize: (1) Lightweight deep learning integration; (2) multimodal biometric integration combining fingerprint with finger vein or behavioral biometrics; (3) comprehensive field testing; (4) advanced template protection through homomorphic encryption; and (5) integrating PAD.

This work demonstrates that hybrid fingerprint authentication can be effectively integrated into contactless cards within practical constraints, establishing a foundation for next-generation secure payment technologies.

References

Akintunde, O.A., Adetunji, A.B., Fenwa, O.D., Oguntoye, J.P., Olayiwola, D.S., and Adeleke, A.J., 2025. Comparative analysis of score level fusion techniques in multi-biometric system. *Journal of Engineering and Technology*, 19(1), pp.128-141.

Al-Maliki, O., and Al-Assam, H., 2021. Challenge-response mutual authentication protocol for EMV contactless cards. *Computers and Security*, 103, p.102186.

Al-Maliki, O., and Al-Assam, H., 2022. A tokenization technique for improving the security of EMV contactless cards. *Information Security Journal a Global Perspective*, 31(5), pp.511-526.

Alshehri, H., Hussain, M., Aboalsamh, H.A., and Al Zuair, M.A., 2018. Cross-sensor fingerprint matching method based on orientation, gradient, and gabor-hog descriptors with score level fusion. *IEEE Access*, 6, pp.28951-28968.

Andress, J., (2011). Identification and authentication. In: Andress, J., Eds. *The Basics of Information Security*. Syngress, London, pp. 17-31.

Ayeswarya, S., and Singh, K.J., 2024. A comprehensive review on secure biometric-based continuous authentication and user profiling. *IEEE Access*, 12, pp.82996-83021.

Bae, G., Lee, H., Son, S., Hwang, D., and Kim, J., 2018. Secure and Robust user Authentication using Partial Fingerprint Matching. In: *2018 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, pp. 1-6.

Bakheet, S., Alsubai, S., Alqahtani, A., and Binbusayyis, A., 2022. Robust fingerprint minutiae extraction and matching based on improved SIFT features. *Applied Sciences*, 12(12), p.6122.

Bojjagani, S., Seelam, N.R., Sharma, N.K., Uyyala, R., Akuri, S.R.C.M., and Maurya, A.K., 2023. The use of IoT-based wearable devices to ensure secure lightweight payments in FinTech applications. *Journal of King Saud University-Computer and Information Sciences*, 35(9), p.101785.

Castillo-Rosado, K., and Hernández-Palancar, J., 2019. Latent fingerprint matching using distinctive ridge points. *Informatica*, 30(3), pp.431-454.

Chen, C.L., Aymanns, F., Minegishi, R., Matsuda, V.D., Talabot, N., Günel, S., Dickson, B.J., and Ramdya, P., 2023. Ascending neurons convey behavioral state to integrative sensory and action selection brain regions. *Nature Neuroscience*, 26(4), pp.682-695.

Daas, S., Yahi, A., Bakir, T., Sedhane, M., Boughazi, M., and Bourennane, E.B., 2020. Multimodal biometric recognition systems using deep learning based on the finger vein and finger knuckle print fusion. *IET Image Processing*, 14(15), pp.3859-3868.

Ding, Y., and Nan, X., 2023. On edge detection algorithms for water-repellent images of insulators taking into account efficient approaches. *Symmetry*, 15(7), p.1418.

Dong, X., Cho, S., Kim, Y., Kim, S., and Teoh, A.B.J., 2022. Deep rank hashing network for cancellable face identification. *Pattern Recognition*, 131, p.108886.

Estrela, P.M.A.B., Albuquerque, R.D.O., Amaral, D.M., Giozza, W.F., and Júnior, R.T.D.S., 2021. A framework for continuous authentication based on touch dynamics biometrics for mobile banking applications. *Sensors (Basel)*, 21(12), p.4212.

Galbally, J., Beslay, L., and Böstrom, G., 2020. 3D-FLARE: A touchless full-3D fingerprint recognition system based on laser sensing. *IEEE Access*, 8, pp.145513-145534.

Gupta, R., Khari, M., Gupta, D., and Crespo, R.G., 2020. Fingerprint image enhancement and reconstruction using the orientation and phase reconstruction. *Information Sciences*, 530, pp.201-218.

Hendre, M., Patil, S., and Abhyankar, A., 2022. Biometric recognition robust to partial and poor quality fingerprints using distinctive region adaptive SIFT keypoint fusion. *Multimedia Tools and Applications*, 81(12), pp.17483-17507.

Huang, S., Sun, G., and Li, M., 2021. FAST and FLANN for Feature Matching Based on SURF. In: *2021 33rd Chinese Control and Decision Conference (CCDC)*, IEEE, pp. 1584-1589.

Ibrahim, S.J., and Al-Khalil, A.B., 2023. Fingerprints to authenticate transactions in contactless cards. *Science Journal of University of Zakho*, 11(4), pp.481-491.

Keerthana, N.V., and Devi, M.P., 2024. A Comprehensive Analysis of Minutiae Point Extraction in Biometric FingerPrint. In: *2024 13th International Conference on System Modeling and Advancement in Research Trends (SMART)*, IEEE, pp. 319-322.

Lee, W., Cho, S., Choi, H., and Kim, J., 2017. Partial fingerprint matching using minutiae and ridge shape features for small fingerprint scanners. *Expert Systems with Applications*, 87, pp.183-198.

Liao, C.C., and Chiu, C.T., 2016. Fingerprint Recognition with Ridge Features and Minutiae on Distortion. In: *2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, pp. 2109-2113.

Magdum, A., Sivaraman, E., and Honnavalli, P.B., 2021. Contactless transaction using wearable ring with biometric fingerprint security feature. In: *Computer Networks and Inventive Communication Technologies: Proceedings of Third ICCNCT 2020*. Springer Nature, Singapore, pp. 653-666.

Mathur, S., Vjay, A., Shah, J., Das, S., and Malla, A., 2016. Methodology for Partial Fingerprint Enrollment and Authentication on Mobile Devices. In: *2016 International Conference on Biometrics (ICB)*. IEEE, pp. 1-8.

Mogaji, E., and Nguyen, N.P., 2024. Evaluating the emergence of contactless digital payment technology for transportation. *Technological Forecasting and Social Change*, 203, p.123378.

Mohamed Abdul Cader, A.J., Banks, J., and Chandran, V., (2023). Fingerprint Systems: Sensors, image acquisition, interoperability and challenges. *Sensors (Basel)*, 23(14), p.6591.

Nedjah, N., Wyant, R.S., Mourelle, L.M., and Gupta, B.B., (2017). Efficient yet robust biometric iris matching on smart cards for data high security and privacy. *Future Generation Computer Systems*, 76, pp.18-32.

Nilsson, H., 2021. Trust issues? The need to secure contactless biometric payment cards. *Biometric Technology Today*, 2021(1), pp.5-8.

Qi, Y., Yang, Z., Sun, W., Lou, M., Lian, J., Zhao, W., Deng, X., and Ma, Y., 2022. A comprehensive overview of image enhancement techniques. *Archives of Computational Methods in Engineering*, 29(1), pp.583-607.

Routray, S., Ray, A.K., and Mishra, C., 2017. Analysis of Various Image Feature Extraction Methods Against Noisy Image: SIFT, SURF and HOG. In: *2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT)*. IEEE, pp. 1-5.

Shepherd, C., and Markantonakis, K., 2024. Isolated hardware execution platforms. In: *Trusted Execution Environments*. Cham: Springer International Publishing, pp.55-78.

Suwarno, S., and Santosa, P.I., 2019. Simple verification of low-resolution fingerprint using non-minutiae feature. *Journal of Physics Conference Series*, 1196(1), p. 012062.

Wang, J., Zhou, Y., and Yang, Y., 2020. A novel and fast three-dimensional measurement technology for the objects surface with non-uniform reflection. *Results in Physics,* 16, p.102878.

Wani, M.A., Bhat, F.A., Afzal, S., and Khan, A.I., 2019. Supervised deep learning in fingerprint recognition. In: *Advances in Deep Learning*. Springer Singapore, Singapore, pp. 111-132.

Yu, J., Niu, L., Gao, C., Cao, Z., and Zhao, H., 2024. Partial Fingerprint Matching Via Feature Similarity and Pre-Training. In: *2024 IEEE International Joint Conference on Biometrics (IJCB)*. IEEE, pp. 1-9.

Zhang, F., Xin, S., and Feng, J., 2019. Combining global and minutia deep features for partial high-resolution fingerprint matching. *Pattern Recognition Letters*, 119, pp.139-147.

Zhang, H., and Yang, Z., 2023. Biometric authentication and correlation analysis based on CNN-SRU hybrid neural network model. *Computational Intelligence and Neuroscience*, 2023(1), p.8389193.