Iraqi Journal of Science, 2026, Vol. xx, No. x, pp: xx
DOI: 10.24996/ijs.2026.67.7.35

ISSN: 0067-2904

Robust Fingerprint Identification Using Canny and Sobel Edge Enhancement

Mays Salman Obaid *, Mohammed Sadoon Hathal
Department of Computer Engineering, College of Engineering, University of Baghdad, Baghdad, Iraq.

Received: 5/5/2025 Accepted: 11/8/2025 Published: xx

Abstract
Fingerprint recognition has long been considered one of the most reliable biometric methods due to the uniqueness and consistency of fingerprint patterns. However, real-world scenarios often present challenges such as noise, smudges, partial prints, or deliberate adjustments that can hinder accurate identification. This study presents a hybrid approach to fingerprint recognition that combines fine detail features and large-scale static feature conversion descriptors to improve flexibility and accuracy. To enhance the clarity of fingerprint patterns, preprocessing techniques such as Canny edge detection and Sobel filtering are applied, enabling better feature extraction. Detailed points are taken out using the transit number way and authorized by filtering the area, reducing the mass, and analyzing the structure of the ridges. Sort descriptors are used to capture local texture information and are normalized to ensure uniform vector lengths. An audit dataset, comprised of original and synthetic fingerprints with different degrees of complexity, is used to validate the system. The combination of fine details, proofing features, with careful pre-processing obtained the best classification rate of 96% across tested methods. The proposed approach achieves good results on the identification of variable fingerprints with the performance efficiency required for real world, real time, and resource constrained forensics.

Keywords: Fingerprint Recognition, Minutiae Extraction, SIFT Descriptors, Canny Filtering, Biometrics, SOCOFing Dataset.

التعرف القوي على بصمات الأصابع باستخدام تحسين الحواف بطريقة Canny وSobel

ميس سلمان عبيد*، محمد سعدون حثيل
قسم هندسة الحاسبات، كلية الهندسة، جامعة بغداد، بغداد، العراق

الخلاصة
لطالما اعتبر التعرف على بصمات الأصابع أحد أكثر الطرق البيومترية التي يمكن الاعتماد عليها نظرا لتفرد أنماط بصمات الأصابع واتساقها. ومع ذلك، غالبا ما تقدم سيناريوهات العالم الحقيقي تحديات مثل الضوضاء أو اللطخات أو

*Email: gs22.msobaid@coeng.uobaghdad.edu.iq

المطبوعات الجزئية أو التعديلات المتعمدة التي يمكن أن تعيق التحديد الدقيق. تقدم هذه الدراسة نهجا هجينا للتعرف على بصمات الأصابع يجمع بين ميزات التفاصيل الدقيقة وواصفات تحويل الميزات الثابتة على نطاق واسع لتحسين المرونة والدقة. لتعزيز وضوح أنماط بصمات الأصابع، يتم تطبيق تقنيات المعالجة المسبقة مثل الكشف عن الحواف بطريقة cannyو sobel، مما يتيح استخراج أفضل للميزات. يتم استخراج نقاط التفاصيل باستخدام طريقة رقم العبور والتحقق من صحتها من خلال تصفية المنطقة وتقليل الكتلة وتحليل بنية التلال. تستخدم واصفات sift لالتقاط معلومات النسيج المحلية ويتم تطبيعها لضمان أطوال متجهة موحدة. يتم تقييم النظام باستخدام مجموعة بيانات التدقيق، والتي تتضمن بصمات أصابع أصلية ومعدلة صناعيا بمستويات متفاوتة من الصعوبة. من بين الأساليب التي تم اختبارها، حقق الجمع بين التفاصيل الدقيقة وميزات التدقيق مع المعالجة المسبقة الحكيمة أعلى دقة بنسبة 96٪. توضح الطريقة المقترحة الأداء القوي في تحديد بصمات الأصابع المتغيرة مع الحفاظ على الكفاءة، مما يجعلها مناسبة تماما لتطبيقات الطب الشرعي في الوقت الفعلي ومحدودة الموارد.

الكلمات المفتاحية :التعرف على بصمات الأصابع، استخراج النهايات والتفرعات، واصفاتSIFT ، كشف الحواف بطريقةCanny ، الأنظمة البيومترية

1. INTRODUCTION

Pattern recognition is so far one of the utmost reliable and commonly used biometric modalities, primarily because fingerprint patterns are unique for each individual, invariable over time, and can be easily collected. It is a cornerstone in multiple security applications, ranging from user-device unlocking to border security and law enforcement. The common procedure of fingerprint recognition can be roughly divided into the following steps: fingerprint pre-processing, feature extraction, fingerprint matching, and decision. Of these steps, feature extraction has a crucial effect on the final accuracy of the System [1].

" Yet in this new era of technology, bumps in the road continue to exist that plague the user when it comes to biometric-based identity." dry skin, uneven compression, poor sensor performance, etc., and are not uncommonly caused by intentional tampering, operating effects M scars, or alterations). These conditions can make the keywords in the corpus not obvious or unclear, add noise, be out of definition, and miss keywords as well. And that is the reason why it is possible to extract a trustworthy and clear feature from a fingerprint, which is the condition for obtaining an effective result [2].

To address these tasks, this paper announces a hybrid method that integrates structural features (e.g., detail points) and compositional features with a sorting descriptor. The technique starts with enhancement of the fingerprint image by a specific pre-processing that consists of edge detection and diffusion-based optimization to expose fine details and restore them that could be easily covered. This enhances the feature capture of the system and is more effective than not using it [3].

The objective is achieving a Fingerprint recognition system that delivers superior performance, is computationally light-weight and fast enough for actual applications (especially trendy real-world scenarios such as forensic analysis and security systems where computational resources may be at a premium) [4].

2. Related Works

In this section, carefully chosen works relevant to the area are reviewed.

Shiho et al. [5] present a method based on deep Convolutional Neural Networks (CNN) to detect the change of fingerprints. Preprocessing images in the SOCOFing dataset are subjected to preprocessing steps (making gray scale, histogram equalization, as well as resizing) before

sending them to the CNN model. The network is trained to detect several types of radiation changes, deletion, eccentric rotation, and z-trim modification. The classification accuracy of 98.55% indicates that the planned method is effective in recognizing the changes of the fingerprint.
Singh et al. [6], proposed a modified capsule network to recognize the fingerprint. They use the SOCOFing dataset, and they are categorized by type of finger, hand (left or right), and gender. CNN learns the within-person spatial relationships of fingerprint features and still possesses some robustness to small distortions. The model outperforms with 99% accuracy associated with fingerprint classification.

In this study [7], they propose a lightweight CNN model to identify synthetic altered fingerprints from the SOCOFing dataset. The system simplifies the design of a CNN structure to decrease the computational complexity and ensure good detection performance. They evaluated the model on a variety of changes and showed that it can achieve 96.78% accuracy when identifying fingerprint modification.

This paper [8], presents a CNN-based fingerprint recognition model trained on the SOCOFing dataset. The authors apply data augmentation techniques to improve robustness and evaluate the model's performance across different fingerprint variations. The model achieves an accuracy of 97.2% for fingerprint verification tasks.

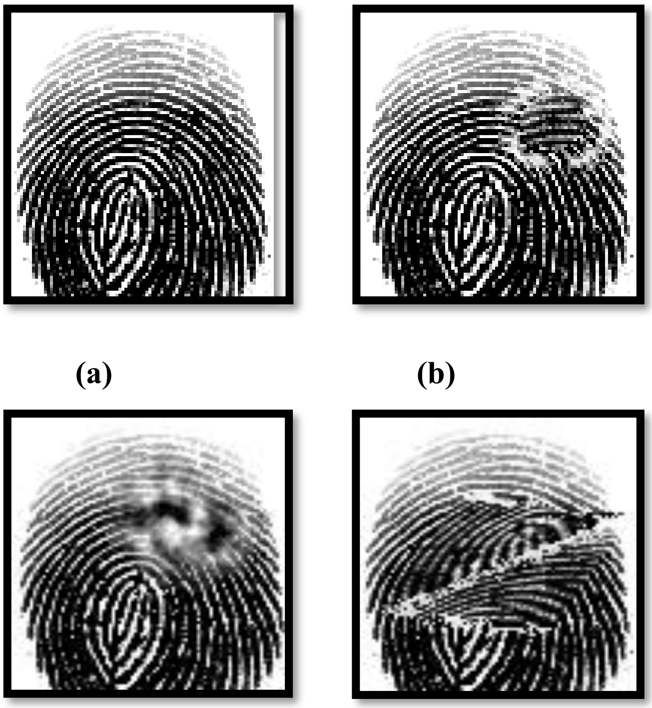
The authors in [9] investigated fingerprint liveness detection using CNNs trained on the SOCOFing dataset. The goal is to distinguish between real and altered fingerprints using spatial feature extraction. The proposed model achieved 94.5% accuracy in classifying live and altered fingerprints.

3. THE PROPOSED METHOD

This section provides a set of constituent data and technologies - processing, advantages of features, and normalization - that support the development of the proposed fingerprint identification system.

3.1 Dataset Description

The experiments were conducted using the publicly available Sokoto Coventry Fingerprint (**SOCOFing**) dataset, which contains 6,000 grayscale fingerprint images (size: 96×103 pixels) collected from 600 African subjects. Each person contributed ten fingerprint samples—one for each finger, as shown in Figure 1. To simulate real-world challenges, the dataset also includes synthetically altered fingerprints categorized into three main modification types: *obliteration* (partial erasure of ridge patterns), *central rotation* (rotational distortion), and *Z-cut* (artificial cuts introduced into the print). Each type of alteration is available at three difficulty levels, *easy*, *medium*, and *hard*—resulting in a total of 55,273 fingerprint images. Each image is labeled with metadata indicating gender, hand (left/right), and finger type, making it suitable for both classification and matching tasks [10].



(a) **(b)**

(c) **(d)**

Figure 1: SOCOFing dataset (a) Real, (b) Easy,(c) Medium,(d) Hard.

3.2 Pre-processing

To improve the quality of fingerprint features before extraction, a series of preprocessing steps was applied, as shown in Figure 2:

- **Grayscale Normalization**: Raw images were converted to grayscale and then normalized using Min-Max scaling, which adjusts pixel intensity values to the [0, 1] range. This ensures uniform brightness distribution and improves the consistency of features extracted across all images.
- **Histogram Equalization**: Applied to advance dissimilarity between ridges and valleys.
- **Noise Reduction**: Gaussian blur filtering was used to smooth images while preserving fingerprint structures.
- **Edge Detection**: Two techniques were explored—**Canny** and **Sobel** filtering—to enhance ridge boundaries and improve the clarity of structural features.
- **Diffusion Filtering**: A custom enhancement method was applied to improve ridge flow and local continuity by adjusting pixel intensity based on surrounding context.
- **Image Resizing**: Wholly processed descriptions were resized to a fixed resolution of **128 × 128 pixels** to standardize input dimensions for the feature extraction and classification stages.

These steps aimed to reduce artifacts and improve the visibility of fine details, especially in altered or low-quality prints. Figure 2 shows the preprocessing steps, and Figures 3 and 4 shows examples of fingerprints.

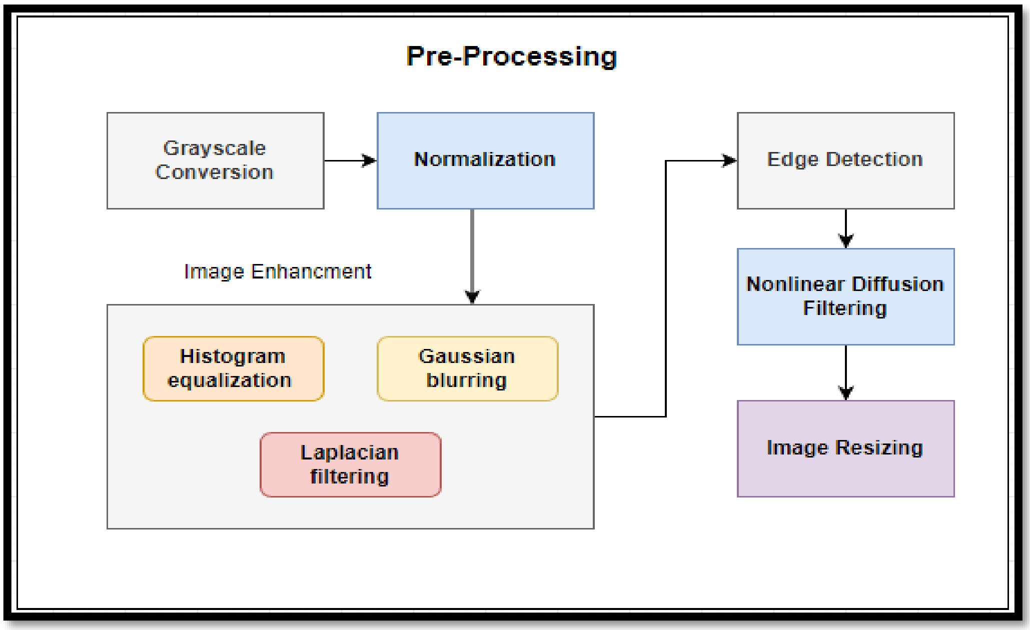


Figure 2: pre-processing steps

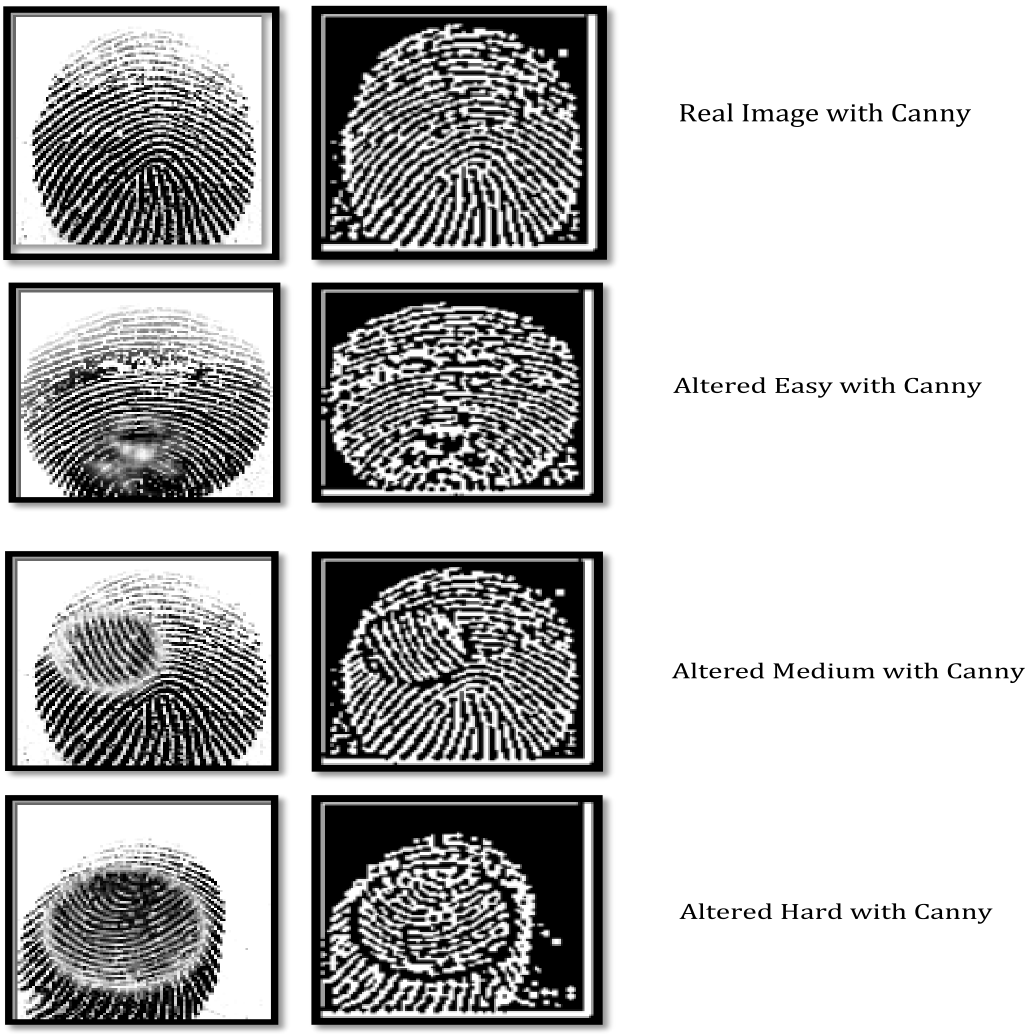


Figure 3: Image preprocessing with Canny

Real Image with Canny

Altered Easy with Canny

Altered Medium with Canny

Altered Hard with Canny

Figure 3: Image preprocessing with Canny

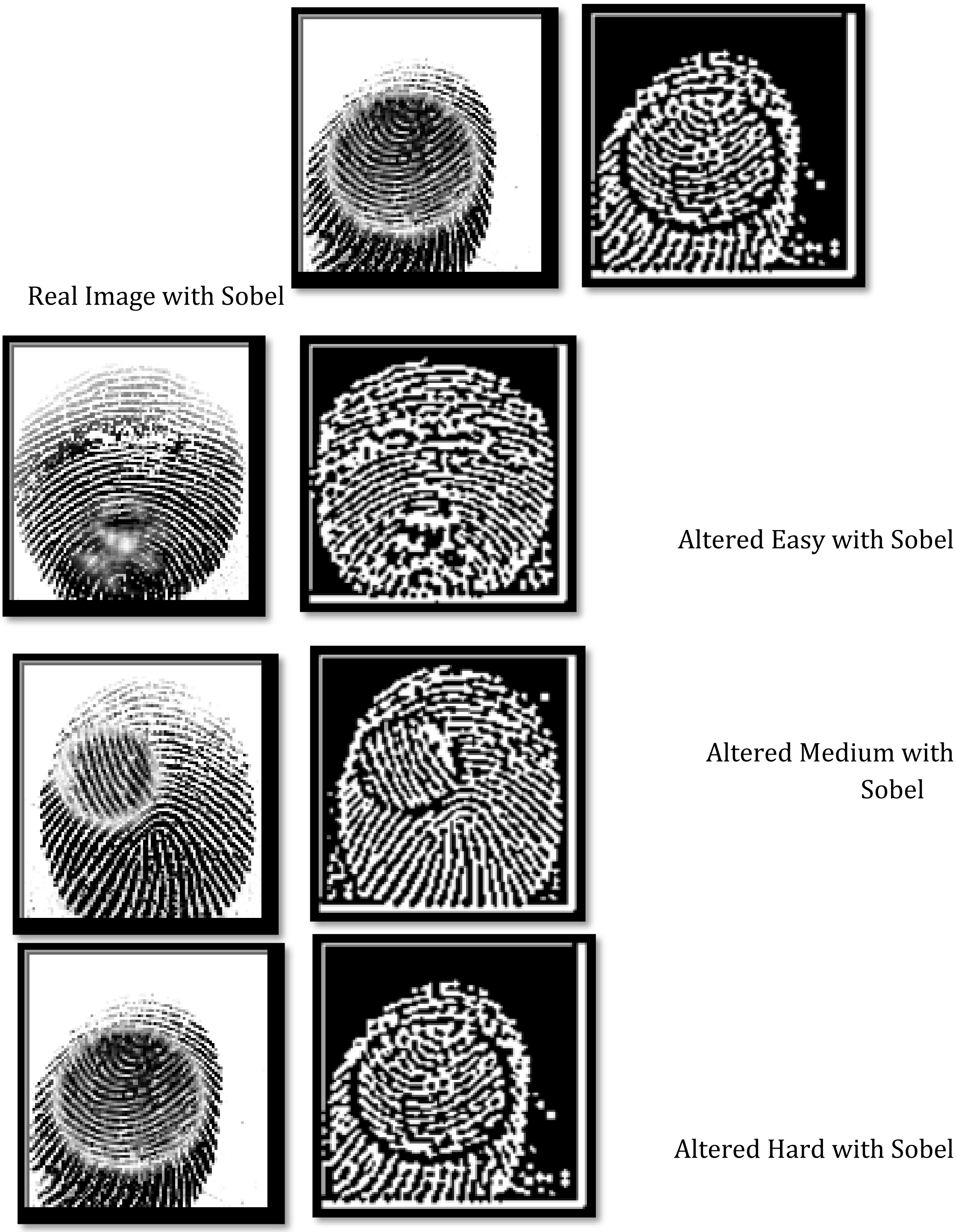


Figure 4: Image preprocessing with Sobel

3.3 Minutiae Feature Extraction

Minutiae are among the most consistent and reliable features for fingerprint recognition, comprising two main types: ridge endings and bifurcations. These are local ridge structures considered invariant and unique to each individual.

One of the most popular methods for detecting minutiae on a thinned binary fingerprint image (skeleton) is the Crossing Number (CN) approach [10]. In this method, a 3×3 pixel window is used to examine the neighborhood of each ridge pixel. This window size provides the minimal context required to assess ridge connectivity while maintaining low computational complexity. The CN value is calculated by counting the number of 0→1 transitions in the eight neighboring pixels as the window is traversed clockwise. Based on this value:

- CN = 1 shows a ridge ending.
- CN = 3 shows a bifurcation.

This localized analysis enables efficient identification of key structural points in the fingerprint. After extraction, the minutiae set undergoes post-processing to improve reliability:

- Minutiae points located outside the valid fingerprint area are removed.
- Redundant or clustered minutiae, which lie too close together, are filtered out to avoid duplications.
- Spurious minutiae introduced by image noise or poor-quality scans are discarded using ridge continuity and orientation analysis [11][12].

This approach provides a compact, discriminative representation of a fingerprint's structure, suitable for reliable matching and classification in biometric systems.

3.3 Minutiae Feature Extraction

In the proposed system, minutiae were extracted from the preprocessed fingerprint images using an adapted **Crossing Number (CN)** method. The implementation included the following steps:

- **Skeletonization**: The grayscale fingerprint image was binarized and thinned using morphological operations to obtain one-pixel-wide ridges.
- **Minutiae Detection**: A 3×3-pixel neighborhood was scanned across the skeleton image to identify ridge endings and bifurcations based on CN values.
- **Feature Vector Formation**: For each valid minutia point, the system recorded its **(X, Y) coordinates** and **orientation**. The resulting set was converted into a fixed-length vector representation suitable for model training.
- **Validation**:
  - Minutiae located outside the fingerprint's core area were excluded.
  - Redundant or overly clustered minutiae were merged or discarded.
  - Artifacts introduced by noise were filtered using ridge structure analysis to retain only genuine minutiae.

This approach ensured that the structural characteristics of both real and altered fingerprints were captured with high fidelity and robustness, as shown in Figure 5

Real Fingerprint with Minutiae

Easy Altered Fingerprint with Minutiae

Figure 5: Detection of Minutiae Types in Real and Altered Fingerprint

3.4 SIFT Feature Extraction
To complement minutiae features, Scale-Invariant Feature Transform (SIFT) descriptors were extracted to capture local texture information. The steps include:
- **Keypoint Detection:** SIFT identified high-contrast, stable points within the fingerprint image.
- **Descriptor Generation:** A 128-dimensional vector was computed for each keypoint, describing the surrounding gradient structure [13].
- **Descriptor Validation:** Low-contrast or spatially inconsistent keypoints were removed. Descriptors were normalized and padded to ensure a fixed length (512 elements) for each image [14].

3.5 Feature Normalization
After extraction, both minutiae and SIFT vectors were combined into a single 1024-dimensional feature vector per fingerprint. To ensure comparability:
- **Coordinate Normalization:** Minutiae coordinates were scaled relative to image size [15].
- **Orientation Adjustment:** Angles were standardized with respect to the fingerprint's core point [16].

Vector Normalization: MinMax scaling was applied to map all features into the [0,1] range, facilitating convergence during model training [17].

3.6 Classification Model
A fully connected neural network was trained to classify fingerprints based on the extracted features. The architecture includes:
- An input layer with 1024 units,
- Three hidden layers with ReLU activation and dropout for regularization [16],
- An output layer that produces a similarity score between fingerprint pairs.

The input size 1024 denotes the fixed-dimension feature vector produced by concatenating minutiae features and SIFT descriptors. As the number of extracted features may differ among different fingerprint samples, all the vectors were zero-padded or truncated to fix the input representations of 1024 dimensions. This normalization enables a constant input for the network, helps with batch processing, and stabilizes the learning. 1024 was chosen as a compromise to balance the expressive power of the feature and computation cost: the model could be able to sufficiently capture the detailed structure and texture information without being too complex or vulnerable to over-fitting. The model was trained with Mean Squared Error (MSE) as a loss function, matching the regression-style scoring of similarity, and Adam by way of optimizer with a learning rate of 0.0001 [18]. The architecture and training settings were chosen to compromise between the speed of merging and the generalization presentation, since the altered fingerprint patterns are of various types.

4. RESULTS AND DISCUSSION

This part offers the performance evaluation of the future fingerprint recognition system using three distinct preprocessing methods: baseline with Minutiae-SIFT, Canny edge detection with Minutiae-SIFT, and Sobel filtering with Minutiae-SIFT. Various performance metrics were used to assess classification accuracy, precision, recall, and robustness under different fingerprint conditions.

4.1 Evaluation Metrics

In this work, the most shared metrics are cast off to evaluate the performance of fingerprint matching schemes [19][20]. First, it is essential to define the concepts that allow the computation of those metrics. Considering the matching of two images, it defines:

- TP—True Positive: It’s a match and a match.
- FP—False Positive: It’s not a match and match.
- TN—True Negative: It’s not a match and does not match.
- FN—False Negative: It’s not a match and match.

The subsequent metrics are calculated:

$$Accuracy: Accuracy = (TP + TN) / (TP + TN + FP + FN)$$
$$Recall = TP/(TP + FN)$$
$$Precision = TP/(TP + FP)$$
$$F1 = 2 \times \frac{(Precision \times Recall)}{(Precision + Recall)}$$
$$FMR = FP/(FP + TN)$$
$$FNMR = FN/(FN + TP)$$
$$EER = FAR(\tau) = FRR(\tau)$$

4.2 Baseline Model: Minutiae-SIFT Only

The initial experiment used a combination of minutiae features and SIFT descriptors without any edge filtering. The flawless achieved the following metrics:

- **Accuracy**: 82%
- **Precision**: 0.6064
- **Recall**: 0.5981
- **F1-Score**: 0.6022
- **ROC AUC**: 0.8727

The results indicate that even without additional filtering, the hybrid feature set captures meaningful differences between real and altered fingerprints. However, there remains room for improvement, especially in recall, as shown in the confusion Matrix in (Figure 6), the ROC Curve in (Figure 7), and the Recall Curve in (Figure 8).

The confusion matrix is the summary of the image classification performance of the model.
To simplify the text, the following abbreviations are used:

❖ RFP: Real fingerprint pairs.
❖ AFP: Altered fingerprint pairs.

- **True Positives (TP): 846,552** — RFP correctly identified as matches.
- **False Positives (FP): 106,906** — AFP incorrectly classified as real.
- **False Negatives (FN): 110,654** — RFP incorrectly classified as altered.
- **True Negatives (TN): 164,688** — AFP correctly classified as mismatches.

This confusion matrix shows that, despite the model's proficiency in identifying true matches (the high TP rate), it tends to mistakenly identify a significant number of AFP as gen- uine (the moderate FP rate), thus exposing a lack of recall (or sensitivity) toward altered prints. This is a typical compromise in biometric security when the quality of artificial samples decreases.

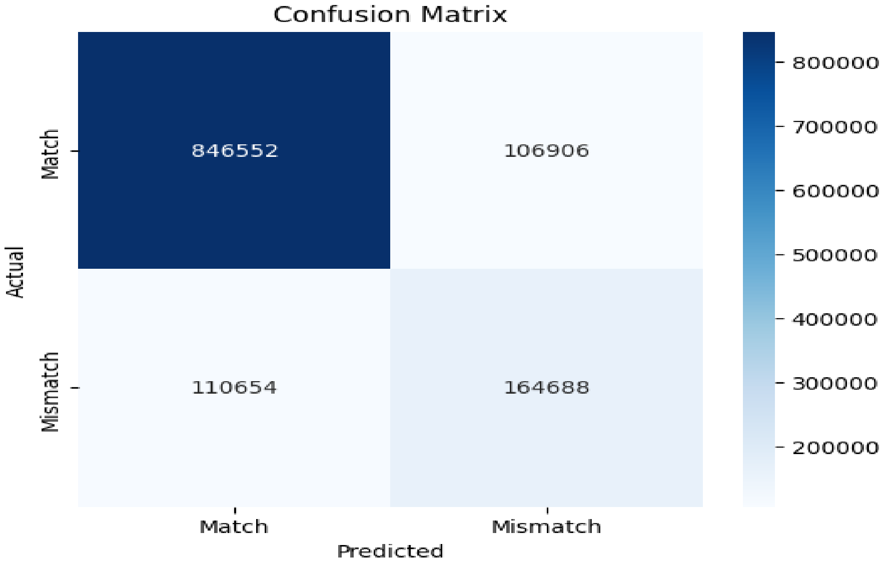


Figure 6: Confusion matrix report for Minutiae-SIFT.

The Headset Effective Characteristic (ROC) curve is a plot of False Positive Rate (FPR) versus True Positive Rate (TPR) for different threshold values:
It has an Area Under the Curve (AUC) of 0.8727, suggesting that it is capable of strong classification.
AUC values approximately 1.0 indicating that the model can effectively discriminate between genuine and fake fingerprints.

These results show that even without edge-based improvements, the Minutiae-SIFT feature set can serve as a good substrate for fingerprint identification. But the model is not as confident near the decision threshold, so it will influence the borderline samples.

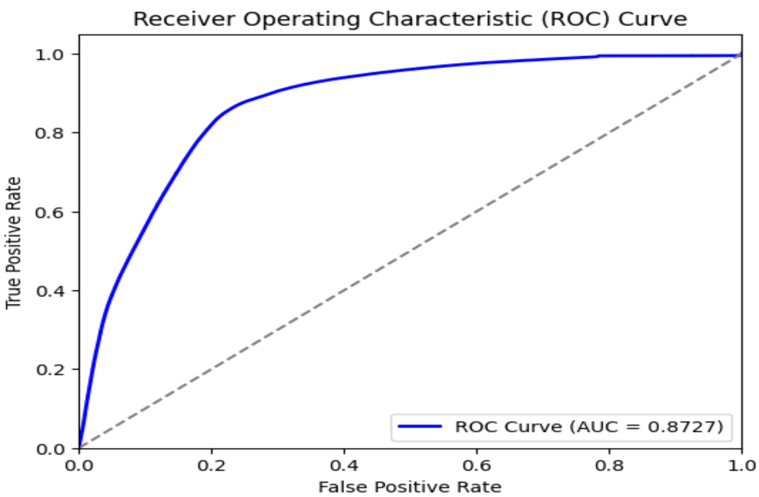


Figure 7: ROC Curve for Minutiae-SIFT.

The Precision-Recall (PR) curve displays the association between:

- Precision (Positive Predictive Value): how many predicted matches are truly correct.
- Recall (Sensitivity): how many actual matches are correctly predicted.
- The Average Precision (AP) score is 0.6242, revealing that although the model makes accurate positive predictions (high precision), it struggles to detect all positives (lower recall), especially when fingerprint alterations obscure minutiae features.

This drop in recall confirms that the model is conservative in its predictions—it prioritizes being certain when it predicts a match, at the cost of missing some actual matches.

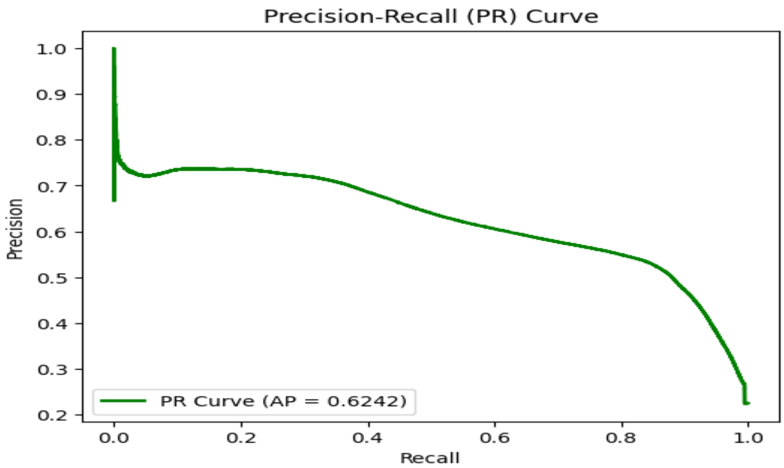


Figure 8: Precision-Recall Curve for Minutiae-SIFT.

4.3 Minutiae-SIFT with Sobel Filtering

Sobel filtering was also tested to emphasize gradient-based edge structures. The performance was slightly lower than Canny but still higher than the baseline:

- Accuracy: 91%
- Precision: 0.5476
- Recall: 0.1987
- F1-Score: 0.2915
- ROC AUC: 0.8188

While this approach yielded lower results than Canny, it maintained a reasonable trade-off between performance and computational efficiency, making it suitable for real-time applications, as shown in the confusion Matrix in (Figure 9), ROC Curve in (Figure 10), and Recall Curve in (Figure 11).

The confusion matrix illustrates the classification outcome for real and altered fingerprints:

- True Positives (TP): 1,004,501 — instances where matching fingerprints were correctly classified as matches.
- False Positives (FP): 18,199 — matching fingerprints incorrectly predicted as mismatches.
- False Negatives (FN): 88,843 — altered (mismatched) fingerprints mistakenly predicted as matches.
- True Negatives (TN): 22,025 — altered fingerprints correctly identified as mismatches.

This matrix indicates a high number of correctly classified matches (TP), contributing to the model's high accuracy of 91%. However, the relatively large number of false negatives suggests the model still struggles to detect some altered fingerprints.

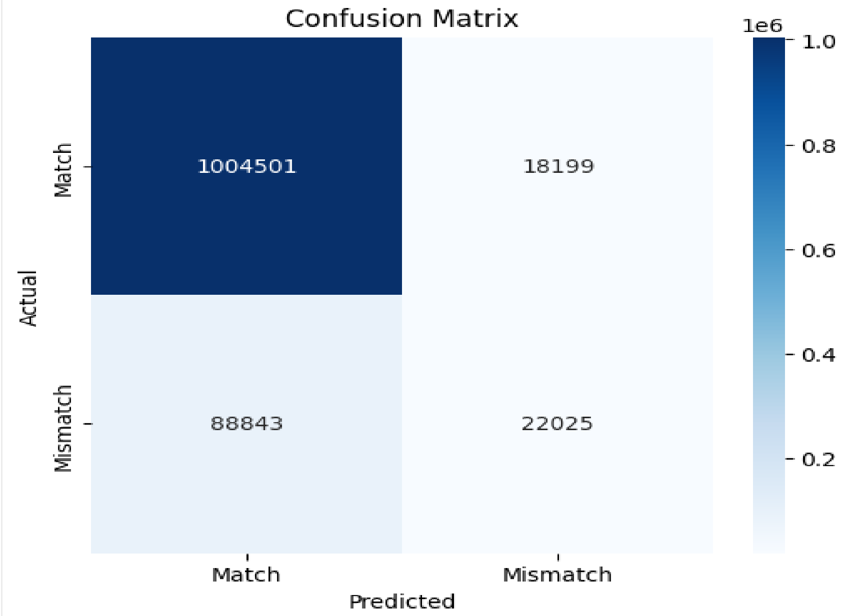


Figure 9: Confusion matrix report for Minutiae-SIFT with Sobel Filtering.

The ROC curve plots the True Positive Rate (TPR) compared to the False Positive Rate (FPR) at various classification thresholds.

The Area Under the Curve (AUC) is 0.8188, reflecting strong but slightly reduced discriminative ability compared to the baseline (AUC = 0.8727).

This confirms that the model with Sobel filtering performs well in distinguishing between real and altered fingerprints, but not as effectively as Canny-enhanced or even baseline in terms of recall.

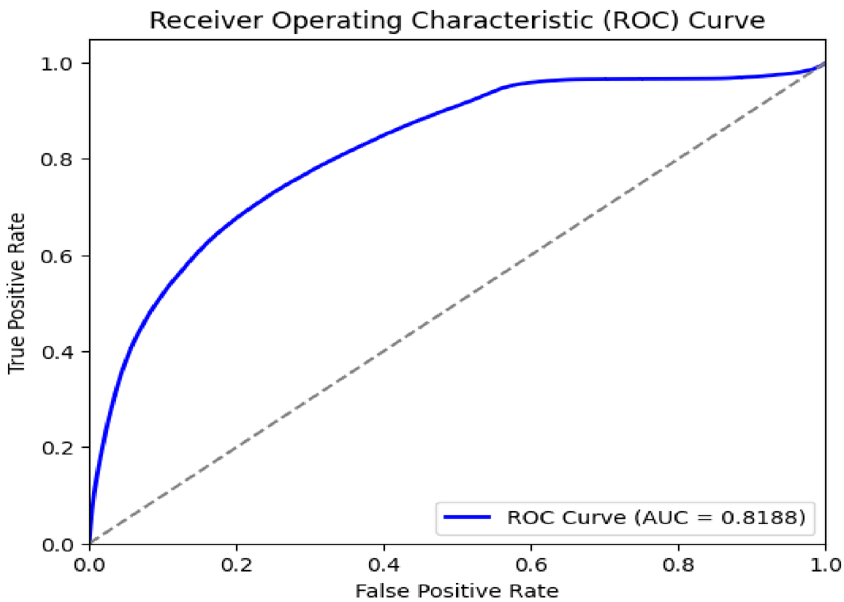


Figure 10: ROC Curve for Minutiae-SIFT with Sobel Filtering.

The PR curve evaluates the tradeoff between precision and recall.
The **Average Precision (AP)** is **0.4046**, which is lower than the baseline model (0.6242).

The curve shape indicates that although the model is able to maintain moderate **precision**, its **recall is significantly reduced (0.1987)** — meaning many altered fingerprints are misclassified as genuine.

This drop in recall aligns with the lower F1-Score (0.2915), indicating that, despite high accuracy, the model may not be suitable for scenarios where detecting all tampered fingerprints is critical.

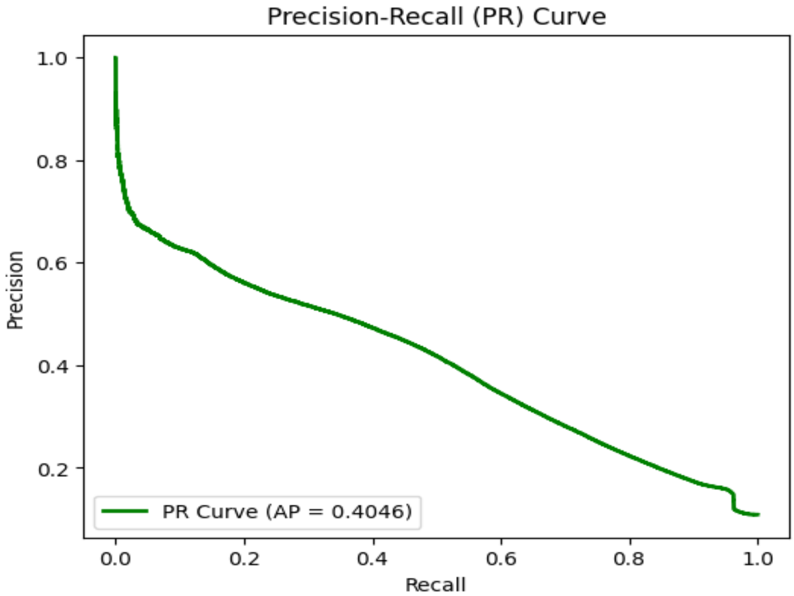


Figure 11: Precision-Recall Curve for Minutiae-SIFT with Sobel Filtering.

4.4 Minutiae-SIFT with Canny Edge Detection

In this setup, Canny filtering was applied prior to feature extraction to enhance ridge boundaries. The performance improved significantly:

- **Accuracy**: 96%
- **Precision**: 0.7118
- **Recall**: 0.2391
- **F1-Score**: 0.3579
- **ROC AUC**: 0.9385
- **PR AUC**: 0.4691

Despite the sharp increase in accuracy and ROC AUC, the recall dropped notably. This suggests the model became more confident in its predictions but struggled to correctly identify altered fingerprints. However, its high ROC AUC confirms strong overall separability as shown in the confusion Matrix in (Figure 12), ROC Curve in (Figure 13), and Recall Curve in (Figure 14).

The confusion matrix shows:

- **True Positives (TP)**: 2,143,737 — Real matches correctly identified.
- **False Positives (FP)**: 10,168 — Incorrectly classified altered fingerprints as real.
- **False Negatives (FN)**: 79,928 — Altered fingerprints not detected (missed).
- **True Negatives (TN)**: 25,111 — Altered fingerprints correctly identified.

This matrix highlights the model's strong ability to detect true matches but also its **lower sensitivity to mismatches**, indicated by the relatively high number of false negatives. Though the model is highly confident in detecting genuine fingerprints, it tends to overlook some altered ones — explaining the drop in recall.

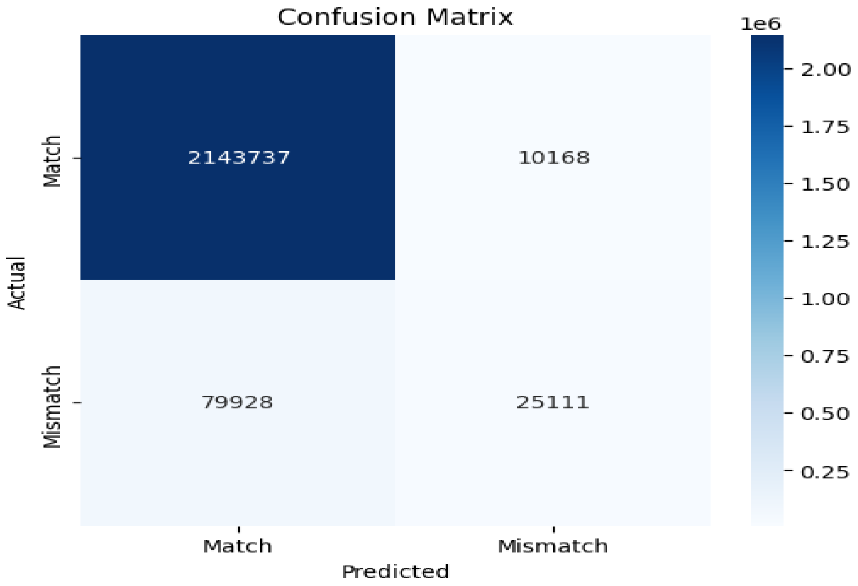


Figure 12: Confusion matrix report for Minutiae-SIFT with Canny Edge Detection.

The Headset Operational Characteristic (ROC) Curve reflects the model's overall discriminatory ability. The AUC (Area Under the Curve) of 0.9385 confirms that the model maintains excellent separability between genuine and altered fingerprints.

A steep rise and sustained in height true positive rate at low false positive rates suggest that the classifier is highly confident in distinguishing between classes, which aligns with the observed increase in accuracy and precision.

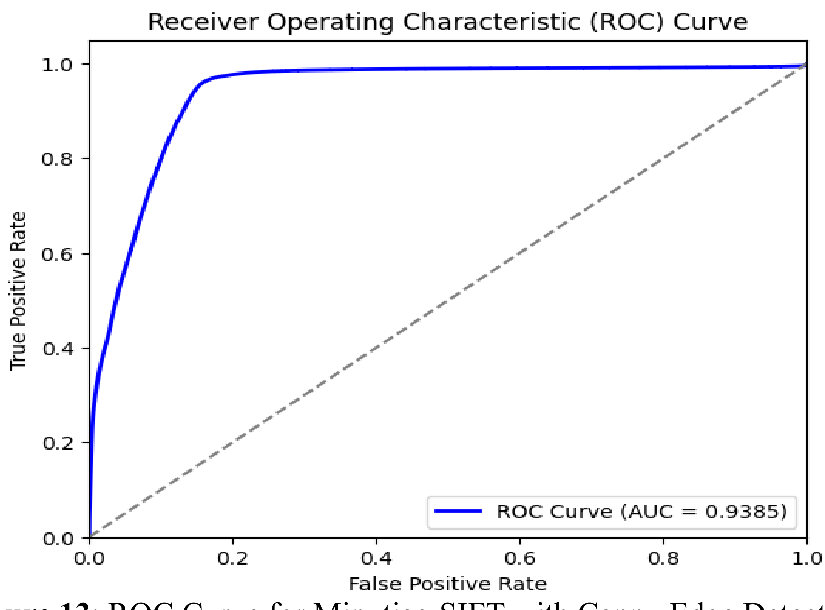


Figure 13: ROC Curve for Minutiae-SIFT with Canny Edge Detection.

The **PR Curve** provides a more nuanced view, particularly for imbalanced datasets. The **average precision (AP)** value of **0.4691** is moderate.

- **High initial precision** indicates that the model initially performs well at identifying positives.
- However, **as recall increases**, precision drops sharply, reflecting a **compromise in identifying all altered prints**.

- This supports the earlier observation: while Canny filtering improves clarity and confidence (high precision), it sacrifices sensitivity (low recall), potentially due to over-filtering finer features in tampered prints.

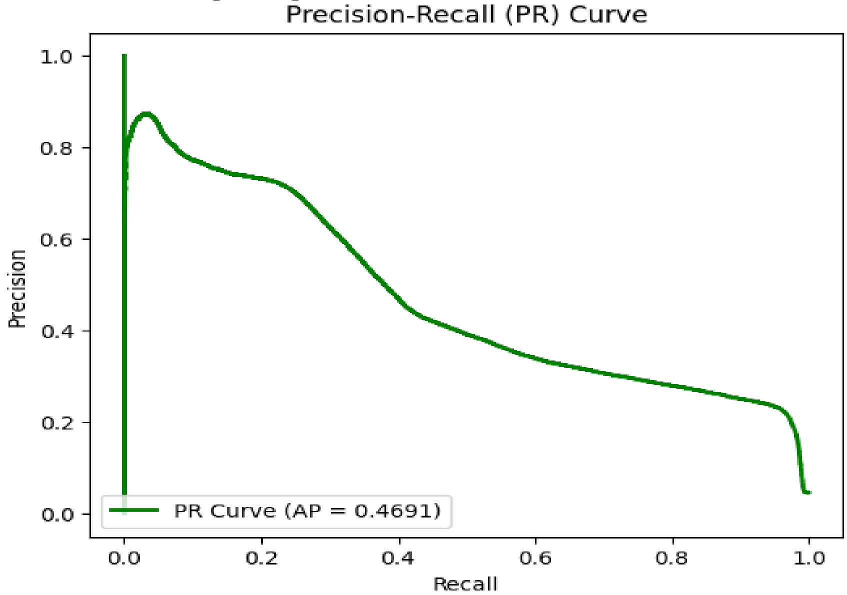


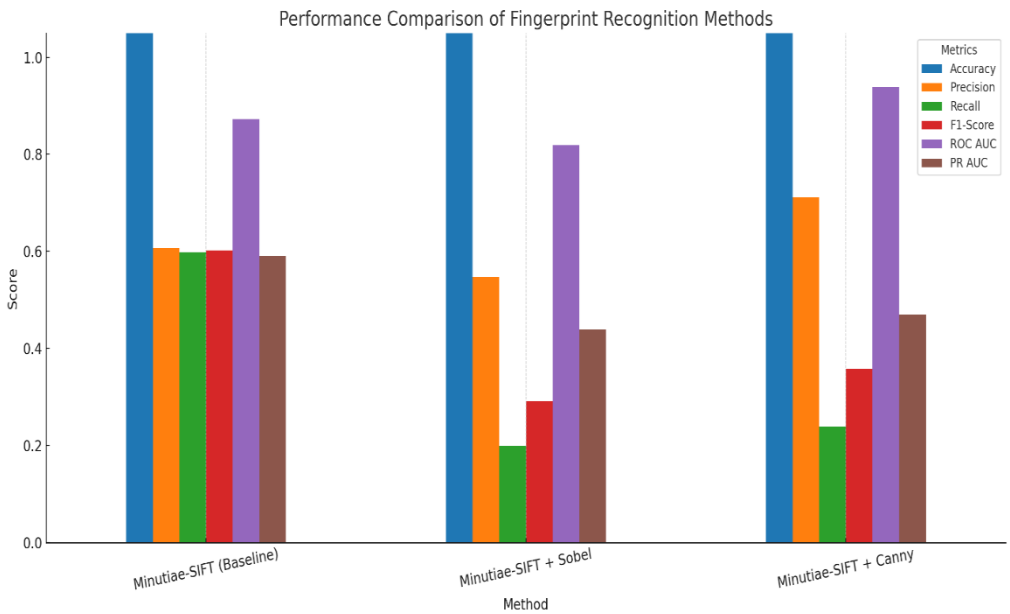
Figure 14: Precision-Recall Curve for Minutiae-SIFT with Canny Edge Detection.

4.5 Comparative Analysis

A relative analysis of all three methods is given in Table 1.

Table 1: Performance Comparison of Fingerprint Recognition Methods

Method	Accuracy	Precision	Recall	F1-Score	ROC AUC	PR AUC
Minutiae-SIFT (Baseline)	82%	0.6064	0.5981	0.6022	0.8727	0.5912
Minutiae-SIFT + Sobel	91%	0.5476	0.1987	0.2915	0.8188	0.4385
Minutiae-SIFT + Canny	96%	0.7118	0.2391	0.3579	0.9385	0.4691



These results show that while Canny-based preprocessing boosts overall accuracy and discrimination power, it compromises recall, which is critical when detecting altered or forged fingerprints. The baseline model, though less accurate, offers a more balanced recall-precision trade-off. These results indicate that although the Canny-enhanced model produced the best accuracy, it performed so at a cost to recall. This compromise suggests that the model could fail to detect some of the modified fingerprints. Contrastingly, the baseline model held a more even trade-off between precision and recall that might be better suited in high-stakes settings such as forensic analysis or fraud detection, where minimizing false negatives is more important.

4.6 Visual Analysis

For better understanding of the classification performance of the model, we also performed an output analysis (performed with confusion matrices, ROC, and PR curves) for all three dissected arches (standard, Sobel, Canny).

Confusion Matrix Analysis:

Comparing the baseline model with the other models, the baseline-model had fairly equal number of true-positives (matches correctly identified) and true-negatives (non-matches correctly rejected), and this explains why it had a relatively high recall value (0.5981).

The Canny-enhanced model, on the other hand, obtained a notably large number of true positives, and the number of false negatives went up slightly, which, however, was not sufficient for the improvement of the recall (0.2391) and the precision (0.7118).

Performance of the Sobel model was weaker, with an increased number of false negatives suggesting lower sensitivity to pattern modulations.

ROC Curve Analysis:

The ROC curve of Canny-based model also got the largest AUC (0.9385) value, implying that strong discriminative power can be observed for the overall cutoff levels. This suggests that the model is good at classifying between genuine and transformed fingerprints, albeit possible reduction in sensitivity at certain thresholds.

Precision-Recall (PR) Curve Analysis:

The PR curve contains a trade-off between precision and recall. The Canny-based model has high precision, but the baseline model has higher recall. This implies that the baseline model might be more appropriate in forensic applications for which the detection of all the possible attacked prints (high recall) is crucial at the expense of some false positives.

Such visualizations reveal that each model configuration makes a unique trade-off:

Canny prefers accuracy and discrimination,

Base favor balance and sensitivity as [balance, sensitivity (recall)],

Sobel has intermediate performance but is not so robust.

5. CONCLUSION

This work introduced a hybrid fingerprint recognition framework, which combines minutiae-based structural features with texture description of SIFT, and specific preprocessing steps consisting of grayscale normalization, edge detection, and diffusion filtering.

The proposed system was tested under difficult conditions on the SOCOFing dataset with original fingerprints and their artificial modifications. From the tested derivations, Canny-enhanced achieved the highest classification accuracy of 96% and ROC AUC, indicating its excellent discrimination ability. But the base model stayed more balanced in the trade-off between precision and recall.

The proposed scheme is especially applicable to forensics, border security, and fraud detection systems where the input fingerprint is often tampered with or of low quality. Its modularity permits application on the fly in resource-limited conditions and enforces interpretability—another nuance not afforded by “black box” deep learning methods.
For future work, we aim to further improve recall at the expense of accuracy, through techniques like adaptive thresholding, feature selection, and using the lightweight convolution models trained using the imbalanced datasets.

Acknowledgements
This research was supported by the Computer Engineering Department, [University of Baghdad], as part of the postgraduate thesis program. The authors would also like to thank the developers of the SOCOFing dataset for providing a rich and diverse resource essential to the success of this study.

Declaration of Competing Interest
The authors declare that there are no known financial or personal conflicts of interest that could have influenced the findings presented in this research.

References
[1] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, “Fingerprint recognition: An advanced review,” IEEE Trans. Biometrics, Behav. Identity Sci., vol. 3, no. 2, pp. 105–123, 2021.
[2] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1, pp. 4–20, 2004, Doi: 10.1109/TCSVT.2003.818349.
[3] B. M. Mehtre, "Fingerprint Image Analysis for Automatic Identification," Pattern Recognit., vol. 20, no. 4, pp. 485–491, 1987, Doi: 10.1016/0031-3203(87)90096-1.
[4] D. G. Lowe, "Distinctive Image Features from Scale-Invariant Keypoints," Int. J. Comput. Vis., vol. 60, no. 2, pp. 91–110, 2004, Doi: 10.1023/B:VISI.0000029664.99615.94.
[5] Enhanced Fingerprint Alteration Detection Using Lightweight CNN. IEEE Xplore. Available online: https://ieeexplore.ieee.org/document/10441980 (accessed on 10 March 2025).
[6] A Proposed Model for Fingerprint Recognition Based on Convolutional Neural Networks. IEEE Xplore. Available online: https://ieeexplore.ieee.org/document/10137536 (accessed on 10 March 2025).
[7] Myshkovskyi, Y.; Nazarkevych, M. Robustness of Fingerprint Liveness Detection Based on Convolutional Neural Networks. CEUR Workshop Proceedings. Available online: https://ceur-ws.org/Vol-3550/short13.pdf (accessed on 10 March 2025).
[8] Singh, T., Bhisikar, S., & Satakshi, M.K. (2021). Fingerprint Identification Using Modified Capsule Network. In Proceedings of the 12th International Conference on Computing Communication and Networking Technologies (ICCCNT). https://doi.org/10.1109/ICCCNT51525.2021.9579727
[9] Li, H. Feature extraction, recognition, and matching of damaged fingerprint: Application of deep learning network. Concurr. Comput. Pract. Exp. 2021, 33, e6057.
[10] A. Ruiz-Garcia and A. Odufuye, "SOCOFing: An Extensive Fingerprint Alteration Dataset," 2018. Available: https://www.kaggle.com/datasets/ruizgara/socofing. (accessed on 10 April 2025).
[11] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, London, UK, 2009.
[12] S. Chikkerur, A. N. Cartwright, and V. Govindaraju, "Fingerprint enhancement using STFT analysis," *Pattern Recognit.*, vol. 40, no. 1, pp. 198–211, 2007, Doi: 10.1016/j.patcog.2006.05.036.
[13] H. Bay, T. Tuytelaars, and L. Van Gool, "SURF: Speeded Up Robust Features," in *Computer Vision – ECCV 2006*, Springer, Berlin, Germany, pp. 404–417, 2006, Doi: 10.1007/11744023_32.
[14] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security," *IEEE Trans. Inf. Forensics Secur.*, vol. 1, no. 2, pp. 125–143, 2006, Doi: 10.1109/TIFS.2006.873653.

[15] A. K. Jain, S. Prabhakar, and L. Hong, "A multichannel approach to fingerprint classification," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 21, no. 4, pp. 348–359, 1999, Doi: 10.1109/34.761265.

[16] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, MIT Press, Cambridge, MA, USA, 2016.

[17] J. Han, M. Kamber, and J. Pei, *Data Mining: Concepts and Techniques*, 3rd ed., Morgan Kaufmann, Waltham, MA, USA, 2011.

[18] D. P. Kingma and J. Ba, "Adam: A Method for Stochastic Optimization," in *Proc. of the 3rd International Conference on Learning Representations (ICLR)*, San Diego, CA, USA, 2015, Doi: 10.48550/arXiv.1412.6980.

[19] Li, H. Feature extraction, recognition, and matching of damaged fingerprint: Application of deep learning network. Concurr. Comput. Pract. Exp. 2021, 33, e6057.

[20] J. Davis and M. Goadrich, "The Relationship Between Precision-Recall and ROC Curves," in *Proc. of the 23rd Int. Conf. on Machine Learning (ICML)*, Pittsburgh, PA, USA, 2006, pp. 233–240, Doi: 10.1145/1143844.1143874.