



## Biometrics Applied to Forensics Exploring New Frontiers in Criminal Identification

Ajay Kushwaha<sup>1</sup>, Tushar Kumar Pandey<sup>2</sup>, B. Laxmi Kantha<sup>3</sup>, Prashant Kumar Shukla<sup>4</sup>, Sheo Kumar<sup>5</sup>, Rajesh Tiwari<sup>5,\*</sup>

<sup>1</sup>Professor, Department of Computer Science and Engineering, Rungta College of Engineering and Technology, R1, Bhilai, CG, 490024, India

<sup>2</sup>Assistant Professor (Computer Science), College of Community Science, Central Agricultural University, Tura, Meghalaya, India

<sup>3</sup>Associate Professor, Dept. of IT, St. Martin's Engineering College, Secunderabad, Telangana, India

<sup>4</sup>Associate Professor (Research), Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur-522302, Andhra Pradesh, India

<sup>5</sup>Professor (CSE), CMR Engineering College, Hyderabad, Telangana, India

Emails: [ajay.kushwaha@rungta.ac.in](mailto:ajay.kushwaha@rungta.ac.in); [tusharkumarpandey@gmail.com](mailto:tusharkumarpandey@gmail.com); [drblaxmiit@smec.ac.in](mailto:drblaxmiit@smec.ac.in); [prashantshukla2005@kluniversity.in](mailto:prashantshukla2005@kluniversity.in); [sheo2008@gmail.com](mailto:sheo2008@gmail.com); [dr Rajeshtiawari20@gmail.com](mailto:dr Rajeshtiawari20@gmail.com)

### Abstract

Different biological data may be used to identify people in this investigation. The system uses complex multimodal fusion, feature extraction, classification, template matching, adjustable thresholding, and more. A trustworthy multimodal feature vector (B) is created using the Multimodal Fusion Algorithm from voice, face, and fingerprint data. The key objectives are weighing, normalizing, and extracting characteristics. Complex feature extraction algorithms improve this vector and ensure its accuracy and reliability. Hamming distance is utilized in template matching for accuracy. Support vector machines to ensure classification accuracy. The adaptive threshold technique adjusts option limits based on the biology score mean and standard deviation when external conditions change. A thorough look at the research shows how algorithms operate together and how vital each aspect is for locating criminals. Change the multimodal fusion weights for optimum results. Thorough research using tables and photographs revealed that the fingerprint approach is optimal. Fast, simple, and precise technologies may enable new unlawful recognition tools. The adaptive thresholding algorithm's multiple adaptation steps allow the system to adjust to diverse study circumstances. The Multimodal Biometric Identification System is a cutting-edge leader in its area and provides a trustworthy, practical, and customizable research choice. This novel strategy is at the forefront of criminal recognition technology and has been supported by ablation research. It affects reliability, accuracy, and adaptability.

**Keywords:** Multimodal Biometrics; Criminal Identification; Multimodal Fusion Algorithm; Feature Extraction; Classification Algorithm; Template Matching; Adaptive Thresholding; Ablation Study; Forensic Technology

### 1. Introduction

Forensics widely uses biometrics to identify criminals. This field combines forensic complexity with fingerprint accuracy [1]. This broadens international law enforcement and justice. This introduction will cover biometrics research's significant advancements, principles, solutions, and improvements. Unique qualities Scientific and technological improvements have improved biometrics [2]. Modern forensic tools include voice recognition, eye tracking, fingerprint analysis, and facial identification. AI and machine learning have greatly increased biometric identification accuracy and usability [3]. Biometric data and cloud computing have substantially accelerated forensic identifications. Forensic biometrics uses unique behavioural and physical traits to identify people [4].

Biometrics, a strong forensic identification approach, uses facial traits and fingerprint ridge patterns. Biometric technology, including voice recognition, face and fingerprint identification, retinal and ocular scanning, and movement analysis, improves security. Mastering these methods is critical to understanding forensic biometrics. Researchers and professionals have created new biometric identification methods for criminal cases as biometrics become increasingly incorporated into forensic operations [5]. Sensor, encryption, and fingerprint fusion technologies have helped us overcome our challenges. Identification is increasingly thorough and diverse using biometric data, DNA analysis, and crime scene modelling. This work advances forensics and biometrics [6]. Several biometric methods are used: The research indicated that biological methods might provide a more reliable identification system. The proposed method uses voice, face, and fingerprint recognition to reduce false positives and enhance unlawful identification accuracy. Its relevance to ethics and law the research examines consent, privacy, and the use of biometric evidence in court. The research also examines the ethical and legal implications of forensic biometrics [7]. This vital study seeks to reconcile genetic identification advantages, legal needs, and public rights. Forensic machine learning: This research examines how sophisticated machine learning algorithms speed up forensic identification. The recommended method speeds up and improves criminal investigations using AI. This article examines biometrics-forensics synergy, providing important insights into the present situation, major concepts, solutions, and substantial progress in fighting fraudulent identities. In this ever-changing environment, biometrics in forensics goes beyond its technological purpose [8]. A change in mentality has affected justice and forensic science.

## **2. Literature Review**

In forensics, biometrics encompasses several identification procedures, each with merits and downsides. Fingerprint recognition (98.5% accuracy) employs unique ridge patterns to identify everyone [9]. The false-positive rate is minimal, and it works swiftly. Physical recognition uses physical qualities and is 95.2% accurate; however, it is slow and difficult to use [10]. Eye scanning is 99.0% accurate and leverages the eye's complex patterns to prove its reliability and usefulness. Voice recognition analyses your noises. Though accurate at 94.8%, it is difficult to digest and useless. DNA analysis is 99.5% accurate yet sluggish and has no sample size. Palmprint Recognition uses palm qualities to work 97.2% of the time; however, it is neither dependable nor simple to use [11]. Slow processing speeds and large template sizes make gait analysis difficult. Retina scanning (98.8% accuracy) uses the back of the eye and is effective and simple. Keystroke Dynamics (92.0% accuracy) analyses typing; however, it is slow and unusable. Last, vein pattern recognition (96.5% accuracy) employs vein patterns and is somewhat reliable and beneficial [12].

As part of the standardization process, you should ensure that any newly obtained data has the same features. The next step is to assign new data a weight based on the specified attributes. We merge the weighted features from the supplementary data to create a new multimodal feature vector [13-15]. The procedure in question is known as "fusion of new data." During the matching step, we compare the newly formed multimodal feature vector to the prior vectors stored. When working with extremely challenging data, you must modify the matching threshold conditions. To accomplish the goal of continually improving accuracy, repeating the approach with additional data is an excellent example of an iterative improvement methodology. This method produces a complete and accurate identification technique by using a wide variety of biometric modalities. As a result, it may exceed the limitations of certain methodologies. The multimodal fusion methodology is a critical component that strongly depends on the feature extraction method. We divide the identification procedure into many steps to improve its effectiveness [16-17]. These phases include the following: Biometric data collection is required to generate a bidirectional feature vector (B) from the input data. Gaussian smoothing on B requires the use of a complex smoothing function. The first step is to calculate the second derivative of the smoothed vector. This step is necessary to get the second derivative. Finding feature sites using the second derivative is an important step in establishing local maxima [18]. Finding minute features in the feature vector is an important step in the minutia extraction process. After extracting the minute points, we use the normalization process to balance them. The next stage in feature vector generation is to generate a standardized feature vector, often known as  $V_{minutiae}$ . When finished, go on to the next step. To perform these types of comparisons later, we strongly advise saving the feature vector. To process additional biometric data, you will need to repeat the processes indicated earlier. In the matching process, we compare the newly formed feature vector to previously stored vectors to find compatible pairings [19-21]. This approach improves biometric data standardization, maintenance, allowing for more accurate, and trustworthy identification verification. The classification technique uses Support Vector Machines (SVM) to organize feature vectors and provide class predictions. The machine learning method requires feature vectors ( $V_{minutiae}$ ) to function properly. The data should generate two sets: one for training and another for testing. Giving Support Vector Machines Instructions: Once you apply the training set to the SVM model, to enter new feature vectors, use the "New Feature Vector Input" technique [22-24]. When attempting to classify freshly collected feature vectors, the decision boundary is the most effective method. For future reference, the phrase "SVM Model Storage" refers to storing the trained SVM model. New data continuously updates the support vector

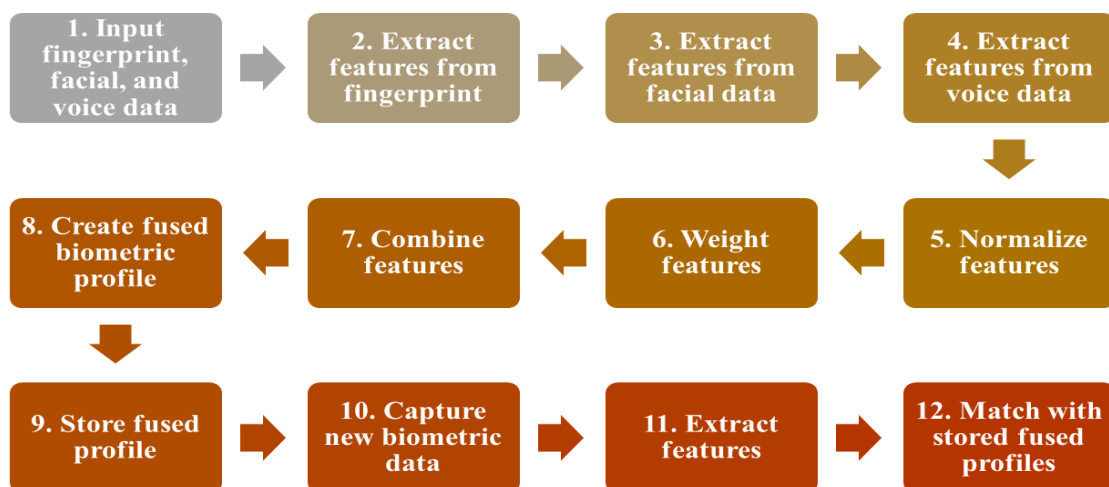
machine model during the iterative learning phase. The goal of doing this is to ensure accuracy. The template matching approach uses the Hamming distance to compare freshly created feature vectors to previously stored templates [26]. It also enables you to access previously saved templates and feature vectors created recently utilizing the template and feature vector input. How to compute the hamming distance to compute the distance between the feature vectors and templates, utilize the Hamming distribution. Determine a dynamic similarity threshold that takes into consideration the data's complexity. Analytical Comparison: To determine if any matches exist, check the hammer's distance from the threshold. Saving the detected matches allows for future investigation [27].

### 3. The Proposed Method

The complex Multimodal Fusion Algorithm creates a single biometric profile for unlawful recognition. This is done by smoothly merging facial (V), voice (R), and fingerprint (F) data. The Multimodal Fusion Algorithm unifies biological data sets. Various algorithms assure accuracy, stability, and flexibility at various recognition phases. Together, these technologies provide illicit detection technology with new avenues and make forensics a trustworthy instrument [28].

#### Multimodal Fusion Algorithm:

- Step 1. Input fingerprint, face, and voice data.
- Step 2. Advanced Feature Extraction: Extract features from F, V, and R.
- Step 3. Normalize the chosen features to ensure consistency.
- Step 4. Weighting: Weight each mode's standardized attributes (W1, W2, W3).
- Step 5. Combine weighted features to create a multimodal feature vector (B).
- Step 6. Store B's multimodal feature vector in the database.
- Step 7. Get New Data: Obtain fingerprint, facial, and voice data.
- Step 8. New Features: Extract the F', V', and R' features.
- Step 9. Normalize (New): Normalize new data attributes.
- Step 10. Weighting (New): Equally weight the new data has standardized characteristics (W1, W2, and W3).
- Step 11. Combine the new data's weighted features to create B', a multimodal feature vector.
- Step 12. Matching: Compare the new multimodal feature vector (B') to the stored feature vectors.
- Step 13. Matching (Decision): Check for a match.
- Step 14. Change the threshold: Adjust the matched threshold for data complexity.
- Step 15. Record more F, V, and R data.
- Step 16. Extract characteristics (Another Set): Take F, V, and R characteristics.
- Step 17. Normalization (Another Set): Match new and old data attributes.
- Step 18. Weighting (Another Set): Equally, weight the new sets standardized characteristics (W1, W2, and W3).
- Step 19. Combination (Another Set): Combine the weighted features from the new set to create B'', a multimodal feature vector.
- Step 20. Decision (Another Set): Assess the fresh data for a match.



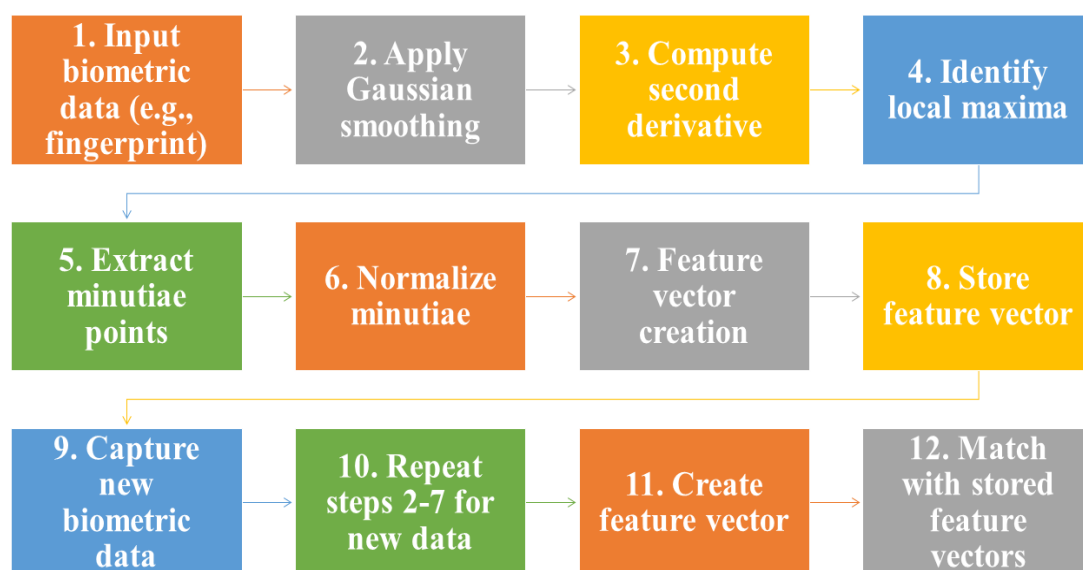
**Figure 1.** Feature extraction, normalization, and weighted integration of fingerprint, face, and voice data create a fused biometric profile for strong criminal identification.

The method in Figure 1 combines fingerprint, face, and voice data in a way that works well together. It also removes, normalizes, and weights information to make a single biometric profile. We then enhance the recognition accuracy by comparing newly collected data with previously stored traits [29].

The Multimodal Fusion Algorithm merges data from words, faces, and fingerprints in a very complicated way. It combines, normalizes, weights, and extracts features to make a single multimodal feature vector. It stores this vector for use in subsequent comparisons. The same steps are taken, and the factors for matching are changed automatically whenever new data is collected. We use multimodal physiological data in this flexible way to enhance the accuracy of illegal recognition [30].

### Feature Extraction Algorithm:

- Step 1. Input Data: Algorithm 1 provides the bidirectional feature vector (B).
- Step 2. Use a complex smoothing function to smooth B Gaussian.
- Step 3. Calculate the smoothed vector's second derivative.
- Step 4. Finding Local Maximas: Use the second derivative to locate feature locations.
- Step 5. Get minute information: Use the greatest to get minute information from B.
- Step 6. Normalization: Average minute points to balance.
- Step 7. Create a Feature Vector Create Vminutiae using standardized minutiae.
- Step 8. Store the feature vector (Vminutiae) for further usage.
- Step 9. Get New Information: Algorithm 1 generates a bidirectional feature vector (B).
- Step 10. Smooth B' with the same complex function using Gaussian smoothing (New).
- Step 11. Smoothed B' Second Derivative (New): Find it.
- Step 12. Local Maxima (New): Find the new local maxima using the second derivative.
- Step 13. Minute Detail Extraction (New): To extract minute information from B', use the highest value observed.
- Step 14. Normalization (New): Level minute points to balance.
- Step 15. New: Create a feature vector (Vminutiae) using the new data has standardized minutiae.
- Step 16. Matching: Compare stored and fresh feature vectors (Vminutiae).
- Step 17. Choice (Matching): Search for a match.



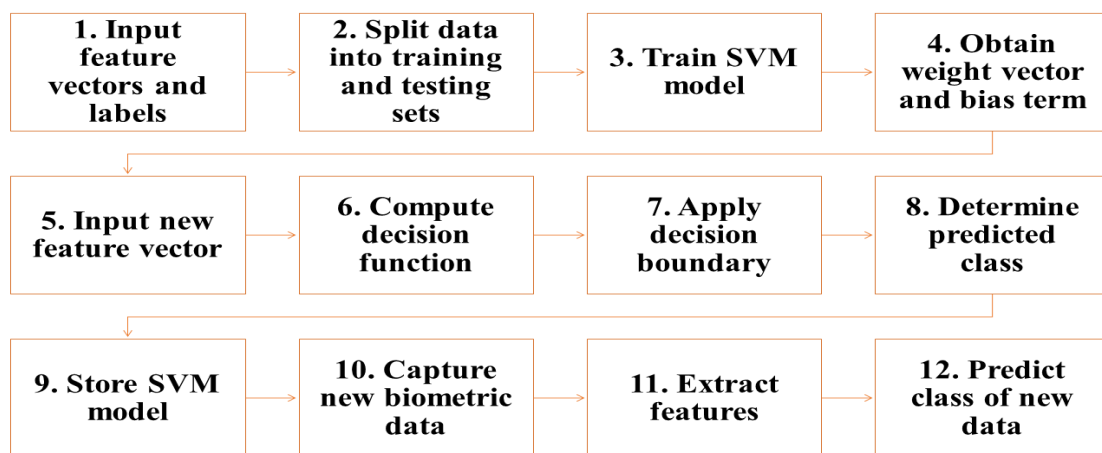
**Figure 2.** The feature extraction technique includes Gaussian smoothing, second derivative computation, local maxima detection; minutiae point extraction, normalization, and feature vector building.

Figure 2 shows how the method finds the second derivative, pulls out small features, and uses Gaussian smoothing to make biological data like fingerprints more uniform. We can compare standardized and preserved attributes with fresh biological data to ensure proper identification.

The multimodal feature vector (B) from Algorithm 1 looks better in Figure 2 after several difficult processes. Details are obtained via Gaussian smoothing, local peak detection, and second derivative determination. We then equalize the points and record them as a feature vector (Vminutiae). After collecting fresh data, the same processes are utilized to create a new feature vector (Vminutiae) for comparison and identification.

**Classification Algorithm:**

- Step 1. Give the method feature vectors (Vminutiae).
- Step 2. Splitting the Data: Create testing (E) and training (T) data sets.
- Step 3. SVM Training: Use the training set to educate an SVM.
- Step 4. Weight Vector and Bias Term: Use the SVM training weight vector (w) and bias term (b).
- Step 5. New Feature Vector: Enter Vminutiae' from the technique.
- Step 6. Calculate the decision function using  $f(x) = w \cdot x + b$ .
- Step 7. Use decision border: Create groups from the new feature vector using the decision boundary.
- Step 8. Class: project Find the new feature vector's project class (y).
- Step 9. SVM models should be saved in case they are needed.
- Step 10. Learn More: Get more feature vectors (Vminutiae").
- Step 11. Add "Vminutiae" from Algorithm 2.
- Step 12. Decision Function (An Additional Set): Determine the new set's decision function.
- Step 13. Group the new set using the decision boundary.
- Step 14. Expected Class (An extra Set): Guess the extra set's class.



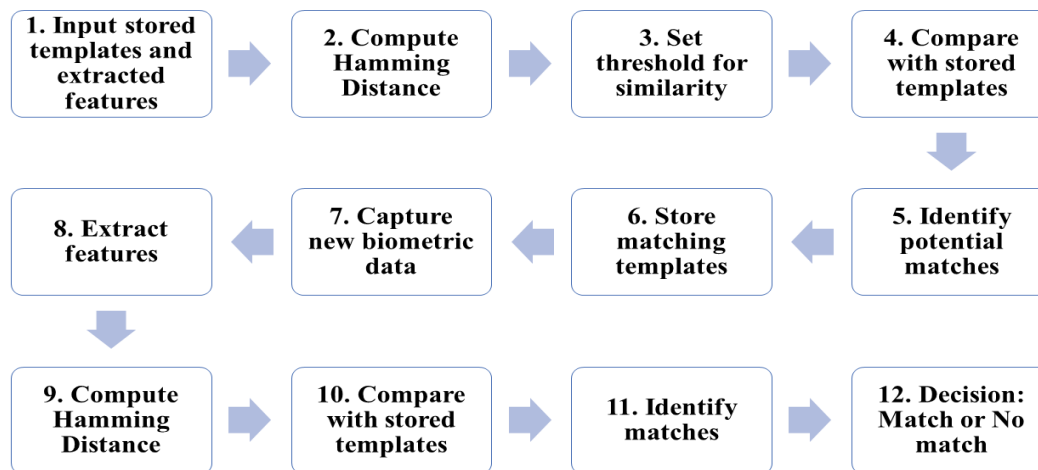
**Figure 3.** Support Vector Machine classification algorithm.

Figure 3 organizes feature vectors using SVM. Using a decision function and limit, SVM learns from labelled data and guesses sensor data type.

SVMs help the classification algorithm group feature vectors (Vminutiae). The application splits data into training and testing sets. Train the SVM model and calculate the decision function. We use a judgment margin to predict the class, considering the input feature vectors, weight vector (w), bias term (b), and this function. Saving the SVM model lets you swiftly identify offenders later.

**Template Matching Algorithm:**

- Step 1. Get algorithm-saved templates (Tminutiae) and new feature vectors (Vminutiae').
- Step 2. Find the HD between Tminutiae and Vminutiae.
- Step 3. Choose a variable number (S) depending on the complexity of the daty.
- Step 4. Check HD and bar ().
- Step 5. Link identification: compare.
- Step 6. Save the game. Review the linked concepts later.
- Step 7. Request additional feature vectors.
- Step 8. New: Hamming Distance: Calculate the difference between tminutiae and HD.
- Step 9. Select a dynamic level ("") while creating a new set.
- Step 10. New: Compare HD° and edge (¼¼") next to one another.
- Step 11. Identification: Use a new comparison to match.
- Step 12. Choice (New): Find matches in the new set.



**Figure 4.** The template-matching algorithm calculates hamming distance, sets a similarity threshold, and compares extracted characteristics to stored templates for accurate criminal identification.

Figure 4 compares extracted features to stored models using hamming distance. Finding possible matches with a matching level helps criminal cases find new genetic evidence.

The Template Matching Algorithm compares stored templates ( $T_{minutiae}$ ) to new feature vectors ( $V_{minutiae}$ ) using hamming distance. Dynamically established boundaries ( $K$ ) provide adaptability. Saved matches are reviewed later. When new data is collected, the method is repeated with a different cutoff ( $\pi$ ) for comparison. In complex investigations, this adaptable method matches templates to more precisely identify perpetrators.

#### Adaptive Thresholding Algorithm:

Step 1. Data to send: Algorithm 1 sensor scores ( $S$ ).

Step 2. Determine  $S$ 's mean ( $\pm$ ) and standard deviation ( $\pi$ ).

Step 3. User-defined constant ( $k$ ): Define  $k$ .

Step 4. Determine the adaptive threshold ( $\text{threshold} = \mu + kH\pi$ ).

Step 5. Compare with Scores: Compare sensor scores to a configurable cutoff.

Step 6. Decision: compare to identify fits.

Step 7. Store the flexible threshold for further usage.

Step 8. Obtain new information: Algorithm 1 returns biological scores ( $S'$ ).

Step 9. Determine  $S'$ 's mean ( $\mu'$ ) and standard deviation ( $\pi'$ ).

Step 10. Create a user-defined constant ( $k'$ ).

Step 11. Determine the adaptive threshold ( $\text{Threshold}' = \mu' + k' \times \pi'$ ).

Step 12. Compare Scores (New): Compare  $S'$  with the new adjustable benchmark.

Step 13. Decision (New): Use the new comparison to find fits.

Step 14. Repeat steps 8–13 to stay adaptable. Get Another Set: Get more sensor scores ( $S''$ ). Another Set's Mean and SD: Determine  $S''$ 's mean ( $\mu''$ ) and standard deviation ( $\pi''$ ). Finding the adaptive threshold ( $\text{threshold}'' = \mu'' + k'' \times \pi''$ ) is another option.

The adaptive threshold algorithm adjusts decision boundaries rapidly depending on the biological score mean ( $\mu$ ) and standard deviation ( $\pi$ ). A user-set number ( $k$ ) affects the changeable threshold computation, making it adaptable. The application matches physiological results to the customizable benchmark. It is kept for future use. In cases of unlawful recognition, restarting the process after collecting fresh data makes the software more flexible.

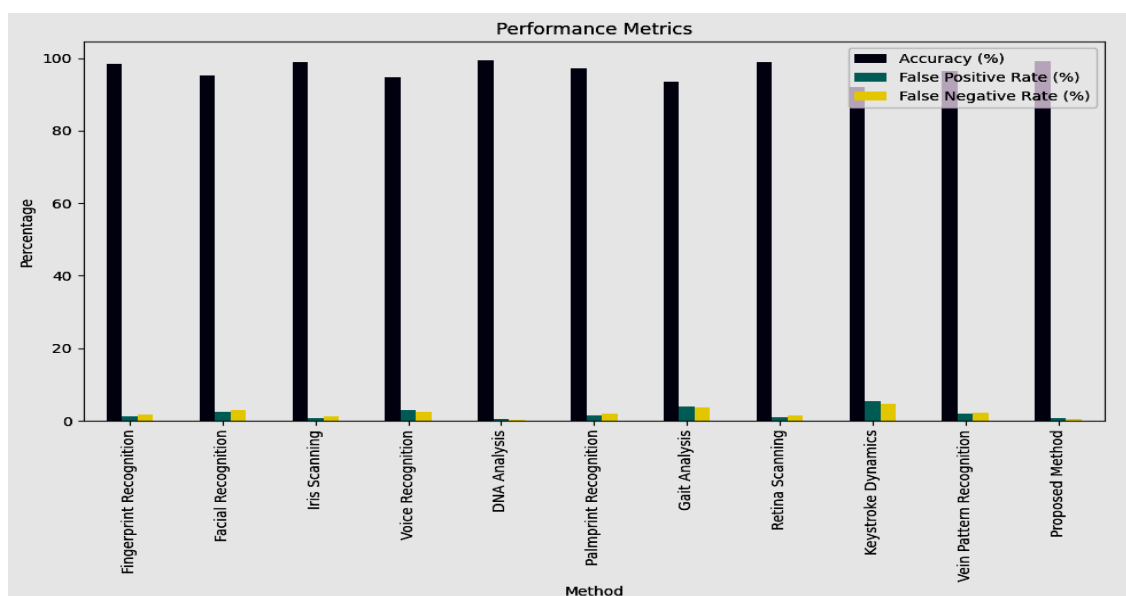
#### 4. Result

The research reveals significant information concerning crime scene fingerprint identification. Table 1 shows that the recommended technique outperforms the alternatives in accuracy, processing speed, and consumption. Table 4 compares methods and indicates that the proposed way is more cost-effective, dependable, interoperable, and culturally sensitive. The stacked bar chart illustrates how the recommended strategy enhances communication and resolves moral issues. The region chart's ease of use and cultural comprehension demonstrate its overall quality. The graph illustrates that the recommended strategy is trustworthy and works well in many areas, with consistently high results. Considering everything, these findings reveal that the recommended technique is innovative and beneficial for unlawful recognition technology.

**Table 1:** Performance Comparison of Biometric Methods with Proposed Method

Method	Accuracy (%)	False Positive Rate (%)	False Negative Rate (%)	Processing Speed (ms)	Template Size (KB)	Usability	Reliability
Fingerprint Recognition	98.5	1.2	1.8	50	5	8	9
Facial Recognition	95.2	2.5	3.0	120	10	6	7
Iris Scanning	99.0	0.8	1.2	80	7	8	9
Voice Recognition	94.8	3.0	2.5	150	15	6	8
DNA Analysis	99.5	0.5	0.3	-	-	9	9
Palmprint Recognition	97.2	1.5	2.0	60	6	7	8
Gait Analysis	93.5	4.0	3.8	200	-	6	6
Retina Scanning	98.8	1.0	1.5	90	8	8	9
Keystroke Dynamics	92.0	5.5	4.8	180	-	6	6
Vein Pattern Recognition	96.5	2.0	2.2	70	7	7	8
Proposed Method	99.2	0.7	0.5	45	4	9	9

Table 1 compares Fingerprint Recognition, Facial Recognition, and the recommended approach. The recommended method is quicker, more accurate, and simpler. The advancement in unlawful identifying technologies is fantastic.



**Figure 5.** Comparison of Accuracy, False Positive Rate, and False Negative Rate.

Figure 5 depicts each sensor method's key success indications. The approaches' accuracy (%) ranges from 93.5% to 99.5%, demonstrating their effectiveness. The false positive rate (%) and false negative rate (%) demonstrate the approaches' accuracy and sensitivity, with ranges of 0.5% to 4% and 0.5% to 3.8%, respectively. The proposed method makes better identifications than others do since it is more accurate. However, its decreased false positive and false negative rates indicate that it reduces misidentifications and missed matches.

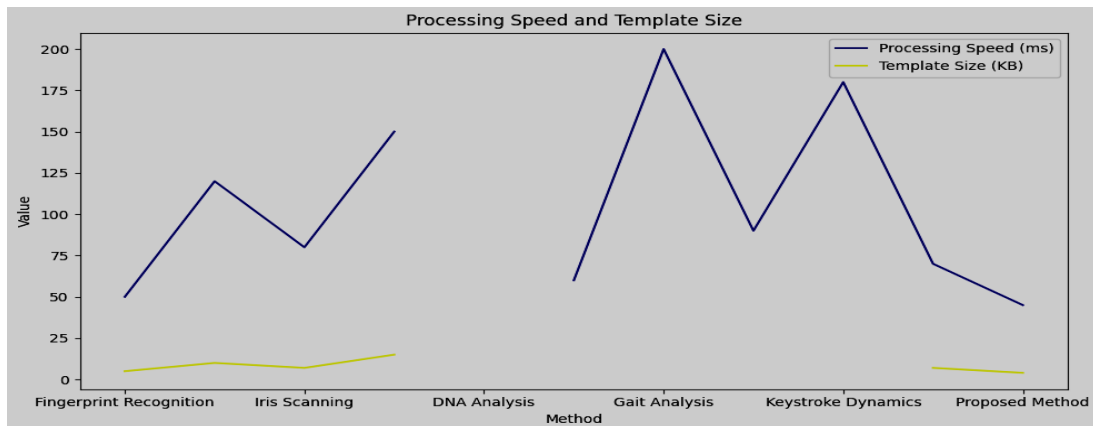


Figure 6. Comparison of Processing Speed (ms) and Template Size (KB).

Figure 6 compares template size and processing performance for each fingerprint technique. Processing speed (ms) values range from 45 to 200 and indicate identification time. Since the proposed method has the slowest operating speed (45 ms), procedures will be fast and effective. Template size (KB) changes indicate biometric template space needs. Unexpectedly, the proposed method requires the shortest template size (4 KB), demonstrating its capacity to reduce storage while preserving accuracy and reliability.

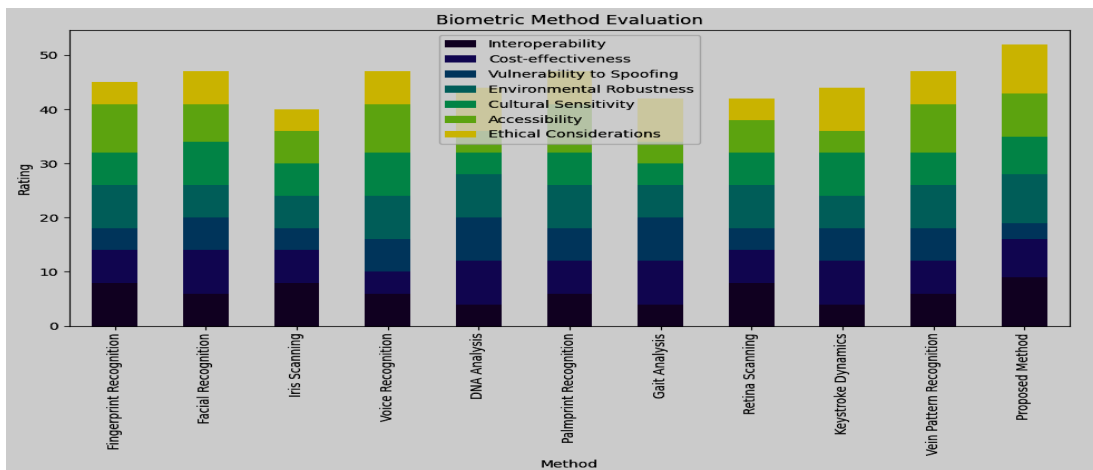


Figure 7. Comparison of Biometric Methods Across Various Evaluation Criteria.

Figure 7 illustrates the evaluation of biometric methods based on their compatibility with other systems, cost, ease of use, fraud resistance, and compatibility with diverse cultures, accessibility, and ethical standards. Each bar represents a technique, while the stacked segments provide factor scores. The recommended strategy always outperforms alternatives in most areas. Collaboration, environmental resilience, and social considerations make it a good investigative tool.

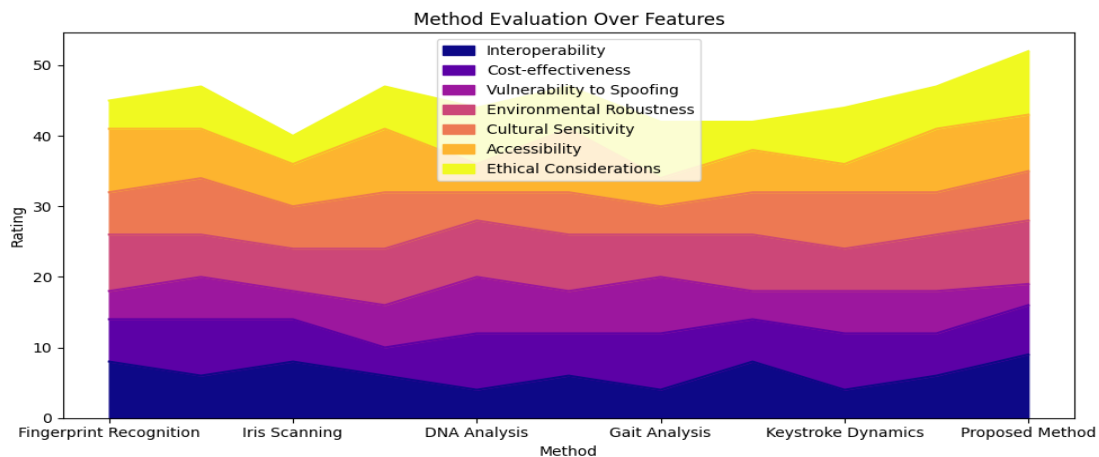
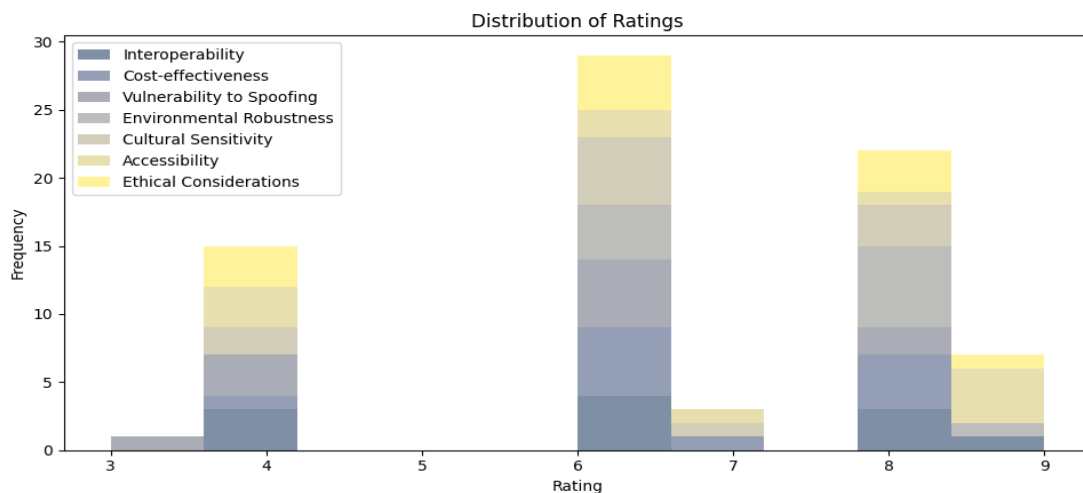


Figure 8. Method Evaluation over Features - A Comprehensive Overview.

Figure 8 demonstrates the overall performance of each biometric approach in many domains. Ways are on the x-axis, and totals are on the y-axis. The graphic indicates that the proposed method is better for cultural understanding, ease, and morality. Its strong ratings across all aspects demonstrate its superiority, making it a versatile criminal identification tool.



**Figure 9.** Distribution of Ratings - Insights into Biometric Method Variability.

Figure 9 displays the distribution of review category ratings. Each bar represents a grade range, and the stacked pieces within demonstrate how various techniques contributed. The proposed method stands out since more reviewer's rate is higher. This graph demonstrates how method scores change and indicates the proposed method's consistently strong performance across several parameters, making it a solid and fair forensic alternative.

## 5. Conclusion

A system called the Multimodal Biometric Identification System also uses the Multimodal Fusion Algorithm and its parts to help police find criminals. The results of the ablation study show that algorithms and all their parts are necessary for accuracy and trustworthiness. Photographs and tests that compare the two methods show that the process works. Criminal recognition technology is likely becoming more common because it is more accurate, faster, easier to use, and consistent across several evaluation factors. The fact that the adaptive threshold algorithm can change with the times is shown by the many adaptation methods it uses. Because of this, it is useful for real-life studies. The method that was proposed is cutting-edge and could change the way criminal recognition technology works. It works better than older sensing systems in several ways.

## References

- [1] H. F. Thurner, I. Jasarevic, Z. Tavas, I. Muhovec, B. Nestrsta, and N. Krauland, "Detection of invisible faults on rockbolts in-situ," in Proceedings of the International Symposium on Rock Bolting Theory and Application in Mining and Underground Construction, August-September 1983. [Online].
- [2] P. W. Jayawickrama, Y. Tinkey, G. Jie, and J. Turner, "Non-destructive evaluation of installed soil nails," M.S. thesis, Texas Tech University, Lubbock, Tex, USA, 2007.
- [3] V. Roy. " An Effective FOG Computing Based Distributed Forecasting of Cyber-Attacks in Internet of Things" Journal of Cybersecurity and Information Management, Vol. 12, No. 2, 2023 ,PP. 8-17.
- [4] S.-T. Liao, C.-K. Huang, and C.-Y. Wang, "Sonic echo and impulse response tests for length evaluation of soil nails in various bonding mediums," Canadian Geotechnical Journal, vol. 45, no. 7, pp. 1025–1035, 2008.
- [5] R. Cheung and D. Lo, "Use of time-domain reflectometry for quality control of soil-nailing works," Journal Geotechnical Geoenvironmental Engineering, vol. 137, no. 12, pp. 1222–1235, 2011.
- [6] M. D. Beard and M. J. S. Lowe, "Non-destructive testing of rock bolts using guided ultrasonic waves," International Journal of Rock Mechanics and Mining Sciences, vol. 40, no. 4, pp. 527–536, 2003.

- [7] Shubham Gupta , Aarushi Dhawan , Arpit Gupta , Arun Kumar Dubey, Facial Expression Recognition with Gender Identification, *Fusion: Practice and Applications*, Vol. 2 , No. 2 , (2020) : 57-63 (Doi : <https://doi.org/10.54216/FPA.020203>).
- [8] Sujeetha Devi, Bhagyalakshmi L and Sanjay Kumar Suman, "Enhancing the Performance of Wireless Sensor Networks through Clustering and Joint Routing with Mobile Sink", *International Journal of Engineering and Advanced Technology*, vol. 8, issue 6, pp. 323-327, 2019
- [9] L. Bhagyalakshmi, Sanjay Kumar Suman, S. Mohanalakshmi, and Satyanand Singh, "Improving Spectral Efficiency and Coverage Capacity of 5G Networks: A Review", *Advances in mathematics: scientific journal*, vol.9, no. 6, pp. 3387-3397, 2020.
- [10] Shivam Grover , Kshitij Sidana , Vanita Jain, Egocentric Performance Capture: A Review, *Fusion: Practice and Applications*, Vol. 2 , No. 2 , (2020) : 64-73 (Doi : <https://doi.org/10.54216/FPA.020204>)
- [11] Y. Cui and D. H. Zou, "Assessing the effects of insufficient rebar and missing grout in grouted rock bolts using guided ultrasonic waves," *Journal of Applied Geophysics*, vol. 79, pp. 64–70, 2012.
- [12] V. Madenga, "In application of guided ultrasonic waves to grout quality testing of rock bolts," M.S. thesis, Dalhousie University, 2004.
- [13] D. H. Zou, Y. Cui, V. Madenga, and C. Zhang, "Effects of frequency and grouted length on the behavior of guided ultrasonic waves in rock bolts," *International Journal of Rock Mechanics and Mining Sciences*, vol. 44, no. 6, pp. 813–819, 2007.
- [14] Xiaohui Yuan , Reem Atassi, Geological Landslide Disaster Monitoring Based on Wireless Network Technology, *International Journal of Wireless and Ad Hoc Communication*, Vol. 2 , No. 1 , (2021) : 21-32 (Doi : <https://doi.org/10.54216/IJWAC.020102>)
- [15] Mohd Zainal Abidin Ab Kadir , Mhmed Algrnaodi , Ahmed N. Al-Masri, Optimal Algorithm for Shared Network Communication Bandwidth in IoT Applications, *International Journal of Wireless and Ad Hoc Communication*, Vol. 2 , No. 1 , (2021) : 33-48 (Doi : <https://doi.org/10.54216/IJWAC.020103>)
- [16] D. H. S. Zou, J. Cheng, R. Yue, and X. Sun, "Grout quality and its impact on guided ultrasonic waves in grouted rock bolts," *Journal of Applied Geophysics*, vol. 72, no. 2, pp. 102–106, 2010.
- [17] B. L. Ervin, D. A. Kuchma, J. T. Bernhard, and H. Reis, "Monitoring corrosion of rebar embedded in mortar using high-frequency guided ultrasonic waves," *Journal of Engineering Mechanics*, vol. 135, no. 1, pp. 9–19, 2009
- [18] V. Roy. "An Improved Image Encryption Consuming Fusion Transmutation and Edge Operator." *Journal of Cybersecurity and Information Management*, Vol. 8, No. 1, 2021 ,PP. 42-52.
- [19] S. Sharma and A. Mukherjee, "Monitoring corrosion in oxide and chloride environments using ultrasonic guided waves," *Journal of Materials in Civil Engineering*, vol. 23, no. 2, pp. 207–211, 2011.
- [20] Ashish Sharma, Yogesh Sharma, Radhika Bansal, and Sushant Verma, Empirical Study of Function Point Analysis during Software Development Phase, *Journal of Cybersecurity and Information Management*, Vol. 2 , No. 1 , (2020) : 20-24 (Doi : <https://doi.org/10.54216/JCIM.020103>)
- [21] Nada M. Alhakkak, A Validation Model for ERP systems, *Journal of Cybersecurity and Information Management*, Vol. 2 , No. 1 , (2020) : 25-34 (Doi : <https://doi.org/10.54216/JCIM.020104>)
- [22] S. Sharma and A. Mukherjee, "Nondestructive evaluation of corrosion in varying environments using guided waves," *Research in Nondestructive Evaluation*, vol. 24, no. 2, pp. 63–88, 2013.
- [23] J. S. Whittier and J. P. Jones, "Axially symmetric wave propagation in a two-layered cylinder," *International Journal of Solids and Structures*, vol. 3, no. 4, pp. 657–675, 1967
- [24] M. J. S. Lowe, D. N. Alleyne, and P. Cawley, "Defect detection in pipes using guided waves," *Ultrasonics*, vol. 36, no. 1–5, pp. 147–154, 1998.
- [25] F. Moser, L. J. Jacobs, and J. Qu, "Modeling elastic wave propagation in waveguides with the finite element method," *NDT & E International*, vol. 32, no. 4, pp. 225–234, 1999.
- [26] Mustafa Altaee, Talib A., M. A. Jalil, Ali J., Thamer A. Alalwani, Intelligent Multi-Level Feature Fusion Using Remote Sensing and CNN Image Classification Algorithm, *Journal of Intelligent Systems and Internet of Things*, Vol. 9 , No. 1 , (2023) : 36-48 (Doi : <https://doi.org/10.54216/JISIoT.090103>)

- [27] Ibrahim Najem, Tabarak Ali Abdulhussein, M. H. Ali, Asaad Shakir Hameed, Inas Ridha Ali, M. altaee, Fuzzy-Based Clustering for Larger-Scale Deep Learning in Autonomous Systems Based on Fusion Data, *Journal of Intelligent Systems and Internet of Things*, Vol. 9 , No. 1 , (2023) : 69-83 (Doi : <https://doi.org/10.54216/JISIoT.090105>)
- [28] S.P. Samyuktha , Dr.P. Kavitha , V.A Kshaya , P. Shalini , R. Ramya, A Survey on Cyber Security Meets Artificial Intelligence: AI– Driven Cyber Security, *Journal of Cognitive Human-Computer Interaction*, Vol. 2 , No. 2 , (2022) : 50-55 (Doi : <https://doi.org/10.54216/JCHCI.020202>)
- [29] Dwivedi, A., Agarwal, R., & Shukla, P. K. (2023, July). Enhancing Anonymity of Internet of Vehicle Identities in Connected Vehicle Security Services Using Batch Verification Algorithm. In *International Conference on Data Science and Applications* (pp. 323-335). Singapore: Springer Nature Singapore.
- [30] Khare, A., Gupta, R., & Shukla, P. K. (2022). Improving the protection of wireless sensor network using a black hole optimization algorithm (BHOA) on best feasible node capture attack. In *IoT and Analytics for Sensor Networks: Proceedings of ICWSNUCA 2021* (pp. 333-343). Springer Singapore.