International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 7s, 2025
https://www.theaspd.com/ijes.php

An Optimized Feature-Level Fusion Framework for Multimodal Biometric Authentication Using ML Classifiers

Princy Tyagi[1], Dr. Amit Kumar Bindal[2*] & Deepak Srivastava[3]
[1]Research Scholar Department of Computer Science and Engineering, Maharishi Markandeshwar (Deemed to Be University) Mullana, Ambala, India – 133207
Assistant Professor, Department of Computer Science and Engineering, School of Science & Technology, Swami Rama Himalayan University, Dehradun, India – 248001
[2]Professor, Department of Computer Science and Engineering, M. M. Engineering College, Maharishi Markandeshwar
(Deemed to Be University), Mullana, Ambala, India – 133207
[3]Department of Computer Science and Engineering, School of Science & Technology, Swami Rama Himalayan University, Dehradun, India – 248001
[*]Corresponding author: amitbindal@mmumullana.org

Abstract: Ensuring secure and accurate identity verification remains a central challenge in biometric authentication systems, particularly when relying on unimodal inputs. This paper proposes a novel hybrid multimodal biometric authentication framework that integrates facial, fingerprint, and iris modalities to enhance performance, security, and robustness. Unlike previous works that rely on isolated biometric traits, the proposed system utilizes a custom-compiled dataset combining two publicly available sources—one for face and iris data and another for fingerprint images—thereby creating a rich, multimodal input space. To optimize feature representation, advanced feature-level fusion is applied, enabling the system to learn complementary biometric patterns across modalities. Machine learning classifiers including Support Vector Machines (SVM), Random Forest, and K-Nearest Neighbors are evaluated, with Optuna-based hyperparameter tuning employed to maximize predictive performance. Experimental results demonstrate that SVM and Random Forest classifiers achieve the highest accuracy (98.28% and 97.24%, respectively), outperforming unimodal models in both recognition accuracy and robustness against environmental variations. This study establishes a scalable and resilient framework for multimodal biometric verification and offers insights into the synergy of data fusion and intelligent optimization in biometric security.

Keywords: Multimodal biometric authentication, Feature-level fusion, Machine learning classifiers, Face, iris, and fingerprint recognition, Biometric security.

1. Introduction

1.1. Background and Need for Multimodal ML-Based Biometric Authentication

Biometric identification has emerged as a foundational component of modern security systems due to its ability to leverage unique physiological and behavioral traits—such as fingerprints, facial features, iris patterns, and voice—to verify identities with high confidence [1]. These modalities are widely deployed across domains like mobile device security, banking, healthcare, and border control [2]. Unlike traditional password- or token-based systems, biometric methods offer enhanced security by utilizing traits that are difficult to replicate or steal.

However, unimodal biometric systems—those relying on a single biometric trait—face notable limitations. Environmental noise (e.g., poor lighting, sensor degradation), physiological variations (such as aging or injuries), and susceptibility to spoofing (e.g., fake fingerprints or masks) significantly affect their reliability and accuracy [3][4]. These constraints render unimodal systems less effective, especially in high-security environments.

To overcome these issues, multimodal biometric authentication systems have been developed, integrating multiple traits—such as face, fingerprint, and iris data—to enhance robustness, accuracy, and spoof-resistance [5][6] By fusing complementary biometric characteristics, these systems achieve higher recognition performance and lower error rates, making them suitable for mission-critical applications like border control, banking, and healthcare [7][8].

Moreover, machine learning (ML) significantly elevates the effectiveness of multimodal biometrics by enabling intelligent feature extraction, pattern recognition, and adaptive classification. Models such as Support Vector Machines (SVM), Random Forest, and Convolutional Neural Networks (CNNs) improve recognition accuracy and reduce false acceptance/rejection rates by handling complex feature relationships [9][10]. Advanced techniques like feature-level fusion and hyperparameter optimization (e.g., using Optuna) further optimize classifier performance across diverse biometric inputs, enabling scalable, secure, and generalizable authentication systems [11][12].

1.2. Objective of the Paper

Traditional biometric authentication systems that rely on a single modality, such as facial recognition, fingerprint analysis, or iris scanning, face significant limitations, including low accuracy, susceptibility to spoofing, and environmental variations. These challenges reduce their reliability for secure identity verification, making them less effective in high-security applications. To address these shortcomings, this research aims to develop a hybrid multi-modal biometric authentication system that integrates facial, fingerprint, and iris recognition to enhance accuracy, security, and resilience. (Younis et al., 2021) By leveraging feature fusion techniques, the system combines multiple biometric traits to improve decision-making. Additionally, Machine learning models, such as Support Vector Machine (SVM) and Random Forest, are utilized for robust biometric identification. To further refine performance, hyperparameter tuning is applied, optimizing model efficiency and accuracy. (Mohammed et al., 2025) The goal of this research is to overcome the limitations of unimodal biometric systems and establish a highly secure, efficient, and reliable multi-modal authentication framework suitable for practical applications.

2. Related Research

2.1. Overview of Existing Biometric Authentication Systems

Traditional biometric systems typically employ unimodal traits such as fingerprints, facial features, or iris scans. While effective in controlled environments, these systems are prone to errors under real-world conditions due to noise, spoofing, sensor issues, and variability in user appearance (Biggio et al., 2012; Hadid, 2014). Multimodal biometric systems have emerged as a reliable solution, integrating two or more biometric traits to enhance recognition accuracy, resilience to environmental changes, and security against spoofing attempts (Govindarajan et al., 2024; Ryu et al., 2021).

Advancements in deep learning, particularly Convolutional Neural Networks (CNNs), have strengthened biometric feature extraction across modalities, resulting in more robust and scalable recognition models (Walia et al., 2019; Alay et al., 2020). These systems often employ fusion techniques—at the feature, score, or decision level—to aggregate information from multiple modalities and improve overall decision-making.

2.2. Fusion and Machine Learning in Multimodal Biometric Systems

Feature-level fusion remains one of the most effective methods in multimodal systems, where raw features from multiple sources are concatenated to form a comprehensive representation. This approach leverages complementary characteristics across modalities (e.g., facial structure and fingerprint ridges), improving system discriminability (Kamlaskar & Abhyankar, 2021).

Machine learning algorithms such as Support Vector Machine (SVM), Random Forest, and K-Nearest Neighbors (KNN) have been widely used for classification tasks in biometric systems. Recent research has demonstrated the effectiveness of ensemble learning and hyperparameter tuning to boost recognition performance (Singh & Kant, 2025; Tuleski et al., 2024). Moreover, optimization techniques such as Optuna have emerged as powerful tools for fine-tuning ML models, improving generalization, and minimizing error rates.

2.3. Comparative Studies on Multimodal Biometric Authentication

Citation	Year	Techniques Used	Biometric Traits	Key Contribution
Walia et al.	2019	Score-level fusion, Machine Learning	Face, Fingerprint	Demonstrated enhanced performance using score-level fusion on benchmark datasets.
Alay & Al-Baity	2020	CNN-based deep learning	Face, Iris, Finger Vein	Integrated three modalities using CNNs for improved recognition accuracy.
Ali et al.	2018	Edge-centric system, Encrypted biometric templates	Multiple	Focused on real-time, low-latency multimodal authentication on edge devices.
Younis & Abuhammad	2021	Hybrid fusion (Feature + Decision-level)	Face, Fingerprint	Improved verification through hybrid-level fusion strategies.
Kamlaskar & Abhyankar	2021	Feature-level fusion, Optimal fusion model	Iris, Fingerprint	Achieved high accuracy using optimal feature-level fusion on heterogeneous data.
Singh & Kant	2025	SVM + Random Forest hybrid classifier, Ensemble learning	Face, Iris, Fingerprint	Validated effectiveness of ensemble ML models for robust multimodal authentication.

2.4. Research Gap

Although prior research has established the advantages of multimodal biometric systems over unimodal approaches, several limitations persist in existing studies. Most frameworks are restricted to combining only two biometric modalities, which may limit their effectiveness in complex or high-security scenarios. In contrast, the proposed system integrates three distinct biometric traits—face, iris, and fingerprint—to leverage their complementary strengths. Furthermore, while fusion techniques are widely used, few studies have implemented feature-level fusion in conjunction with automated hyperparameter optimization tools like Optuna, which significantly enhance model accuracy and adaptability. Additionally, many previous studies rely on limited or homogenous datasets, reducing generalizability across diverse populations. To address this, our approach involves the creation of a custom hybrid dataset that improves the robustness and scalability of the biometric authentication framework.

3. Proposed Methodology

Figure 1 illustrates the stepwise methodology adopted for training the machine learning model. The workflow comprises multiple stages, including data preprocessing, augmentation, and exploratory data analysis to enhance data quality. The model undergoes training and evaluation cycles, ensuring optimization through hyperparameter tuning. A decision step determines whether the model's performance metrics satisfy the predefined thresholds, leading to either model storage or further refinements.

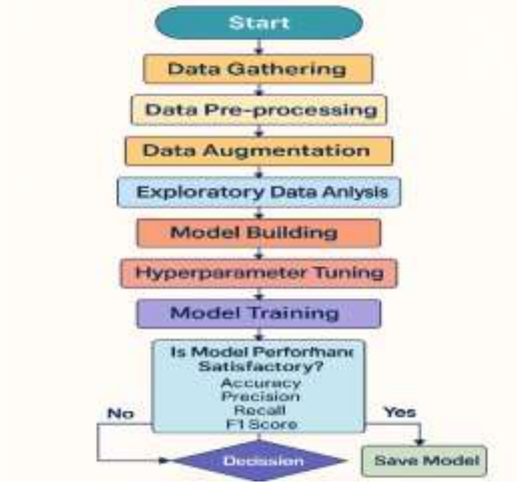

Figure 1: Machine Learning Model Development Workflow

3.1. Data Collection & Preprocessing

The dataset employed in this experiment comprises multimodal biometric inputs—facial, iris, and fingerprint data—gathered from two separate datasets:

- **Self-portraits and Identification Photographs Dataset:** Utilized for face recognition and iris extraction. (Bhatt et al., 2021)
- **Multimodal Iris and Fingerprint Dataset:** Utilized for iris and fingerprint authentication. (Mustafa et al., 2020)
- **Preprocessing Techniques-Data Preprocessing Methods**-Several preprocessing processes were implemented to prepare the data for model training:
- **Image Normalization:** Image Normalization: Standardizing pixel intensity levels to improve model training. (Pisani et al., 2017)
- **Grayscale Conversion:** Minimizing computational complexity by emphasizing essential feature structures. (Weitzner et al., 2020)
- **Gaussian Blurring:** A technique for image smoothing that diminishes noise while maintaining critical features. (Liu et al., 2020)

Data Augmentation

Augmentation strategies were employed to rectify class imbalances and enhance model generalization.

- **Rotation:** Arbitrary picture rotation to replicate real-world variances.
- (Mekruksavanich et al., 2021)

- **Flipping:** Horizontal reflection to enhance variation in image orientation. (Ametefe et al., 2023)
- **Brightness Adjustment:** Modifying picture luminance to accommodate varying illumination conditions. (Hsu et al., 2021)
- **Noise Augmentation:** Incorporating Gaussian noise to enhance model resilience against sensor deficiencies (Mekruksavanich et al., 2021)

3.2. Feature Extraction

To guarantee rapid and precise biometric recognition, diverse feature extraction approaches were employed across distinct modalities—facial, fingerprint, and iris—to augment discriminative features and boost classification efficacy. (P. P. Jena et al., 2021) Face recognition approaches, like Local Binary Patterns (LBP) for texture pattern capture, enhance system robustness against illumination fluctuations, while Principal Component Analysis (PCA) diminishes dimensionality while retaining critical facial traits. Furthermore, Histogram of Oriented Gradients (HOG) retrieved gradient-based features, while Gabor Filters caught multi-scale and multi-orientation texture information, hence enhancing overall identification performance. (Fronitasari et al., 2017) In fingerprint recognition, Minutiae Extraction was utilized to discover essential ridge features such as bifurcations and terminations, while Gabor Filters and Wavelet Transform improved ridge and valley structures for higher identification accuracy. (Fronitasari et al., 2020) The Fourier Transform enhanced fingerprint patterns by augmenting ridge contrast and identifying global features. Gabor Filters were utilized for extracting intricate texture information in iris detection, whereas Daugman's Rubber Sheet Model standardized iris regions into a uniform size for comparative analysis. Supplementary methods, such as Discrete Cosine Transform (DCT) for feature reduction and Wavelet Transform for multi-resolution analysis, improved the system's capacity to differentiate complex iris patterns. (Fronitasari et al., 2020) The integration of sophisticated feature extraction algorithms across many biometric modalities enhances the system's accuracy, resilience, and security, hence assuring reliable and efficient biometric authentication.

3.3. Machine Learning Classifier

The machine learning classifiers used in the proposed multi-modal biometric authentication system were evaluated based on their ability to accurately classify facial, fingerprint, and iris features. Among the models tested, Support Vector Machine (SVM) and Random Forest (RF) demonstrated the most consistent performance, showcasing excellent generalization and robustness across biometric traits (Singh et al., 2025). In contrast, the Decision Tree (DT) model exhibited significant overfitting—it performed perfectly on the training set but failed to generalize to unseen data, indicating memorization rather than true learning (Yaman et al., 2021).

The K-Nearest Neighbors (KNN) algorithm delivered moderate results, balancing simplicity and performance, though it fell short of SVM and RF in overall accuracy (Kadhm et al., 2021). The Naïve Bayes (NB) classifier, while computationally efficient, struggled with capturing the complex dependencies among biometric features. Similarly, AdaBoost showed limited learning capacity, likely due to weak base learners or poor hyperparameter configurations.

To enhance performance, Optuna-based hyperparameter tuning was employed across all classifiers, which refined model parameters and significantly improved accuracy. SVM and Random Forest continued to outperform, while DT showed improvement after pruning. These findings underscore the necessity of robust classifier selection and fine-tuning to build secure and reliable biometric authentication systems (Tuleski et al., 2024).

The mathematical formulations of the key classifiers are as follows:

Support Vector Machine (SVM)The SVM classifier constructs a hyperplane that maximizes the margin between different classes. The decision function is given by:

$f(x)=sign(w^{T}x+b)$

Where x is the feature vector, w is the weight vector, b is the bias term. This formulation allows SVM to effectively separate biometric patterns in high-dimensional spaces.

Random Forest (RF) Random Forest operates by aggregating predictions from multiple decision trees:

$\hat{y}=mode(\{h_t(x)\}_{t=1}{}^{T})$

Where: - $h_t(x)$ is the output of the t-th decision tree,T is the total number of trees.

The ensemble voting mechanism improves overall prediction accuracy and reduces overfitting.

K-Nearest Neighbors (KNN) KNN assigns a class label based on the majority vote from the closest k neighbors:

$\hat{y} = argmaxc \in C\sum_{i=1}{}^{k} \delta(y_i = c)$

Where:$\delta(\cdot)$ is the indicator function (1 if true, 0 otherwise), y_i is the class label of the i-th nearest neighbor,C is the set of all possible classes.

KNN's simplicity makes it interpretable, though it may be sensitive to feature scaling and data distribution.

3.4. Model Training & Optimization

The biometric identification system underwent training using several machine learning models, subsequently enhanced through optimization strategies to augment performance and guarantee precise recognition.

Training of Distinct Models

Each biometric modality—facial recognition, fingerprint analysis, and iris recognition—was first trained independently utilizing Convolutional Neural Networks (CNNs) to acquire modality-specific characteristics. CNNs proficiently identified intricate patterns and structures inherent to each biometric characteristic, guaranteeing elevated precision in individual biometric categorization (Soleymani et al., 2018).

Strategies for Fusion and Integration

Fusion methods were implemented at multiple levels to improve the system's overall accuracy and dependability:

Feature-Level Fusion: Features extracted from facial, fingerprint, and iris modalities were amalgamated into a cohesive feature vector, enabling the model to assimilate complementary biometric characteristics (Kamlaskar et al., 2021).

Score-Level Fusion: Confidence ratings from distinct classifiers were amalgamated to enhance decision-making, hence decreasing false acceptance and rejection rates (Dwivedi et al., 2021).

Evaluation Metrics

To assess the system's efficacy, several biometric assessment indicators were employed:

Accuracy: Assesses the device's absolute efficiency in predictions.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Where: TP = True Positives, TN = True Negatives, FP = False Positives, FN = False Negatives

Precision: Measures the accuracy of positive predictions.

$$Pr\ e\ cision = \frac{TP}{TP + FP}$$

Recall: Measures the completeness of positive predictions.

$$Recall = \frac{TP}{TP + FN}$$

F1-score: Balances precision and recall, useful for unbalanced datasets.

$$F1\text{-}Score = 2 \times \frac{Pr\ e\ cision \times Recall}{Pr\ e\ cision + Recall}$$

FAR (False Acceptance Rate): Represents the likelihood of an unauthorized individual being erroneously accepted.

$$FAR = \frac{FP}{FP + TN}$$

FRR (False Rejection Rate): Indicates the probability of an authentic user being erroneously rejected.

$$FRR = \frac{FN}{TP + FN}$$

EER (Equal Error Rate): The juncture at which FAR and FRR are equal, functioning as a critical standard for biometric systems.

Loss Function In the training of the model, a cross-entropy loss function is used for classification tasks, as it quantifies the difference between the true labels and the predicted probabilities:

$$\text{Loss=-}\textstyle\sum_{i=0}^{N} 1\,(Yi\ *\ log(pi)\ +\ (1\ -\ Yi)\ *\ log(1\ -\ Pi))$$

Where: yi= true label (0 or 1), pi= predicted probability of class 1, N= number of samples

This formulation provides a comprehensive mathematical basis for evaluating the biometric recognition system's performance, ensuring that it is precise and resistant to fluctuations in biometric data, delivering strong, secure, and efficient authentication (Younis et al., 2021).

To further refine model performance, hyperparameter tuning was conducted using Optuna, a Bayesian optimization framework. Although not the central focus of this work, it helped adjust key parameters such as tree depth in Decision Trees, kernel type in SVM, and the number of estimators in ensemble models. These refinements contributed to marginal gains in testing accuracy, particularly for underperforming models like AdaBoost and KNN, without significantly altering the model hierarchy.

4. Hybrid Multi-Model Biometric Authentication System

4.1. Explanation of the Hybrid Model

The suggested system amalgamates various biometric modalities—facial recognition, fingerprint analysis, and iris scanning—to augment accuracy, resilience, and security in biometric authentication. The hybrid technique entails:

- Multi-input processing: Integrating several biometric characteristics.
- Feature fusion: Integrating features from several modalities to enhance decision-making.
- Machine learning-based classification: Employing ML models for the effective recognition of biometric IDs.
- Optimization techniques: Improving performance through hyperparameter adjustment.

Utilizing multi-modal biometric fusion, the model addresses the shortcomings of single-modality systems, which frequently encounter challenges due to environmental fluctuations and diminished accuracy. (Aleem, et al., 2020)

4.2. Selection of Biometric Modalities

The system integrates three biometric modalities:

- Face Recognition: Obtained from the Selfies, ID Images Face Dataset utilizing MTCNN for facial detection.
- Iris Recognition: Extracted from facial photos with MTCNN-based eye extraction.
- Fingerprint Recognition: Derived from the Multimodal Iris and Fingerprint Dataset, including preprocessing approaches.

Each biometric characteristic is selected for its distinctiveness, dependability, and accessibility

4.3 Fusion Techniques Used

The system utilizes fusion techniques at many levels to efficiently combine biometric data. (Prabu, et al., 2019)

- Feature-Level Fusion: Merging feature vectors from facial, iris, and fingerprint pictures into a unified input representation of size 9408 (3136 per modality).
- Score-Level Fusion: Integrating confidence ratings from several classifiers.
- Decision-Level Fusion: Employing ensemble techniques such as Random Forest to get conclusive forecasts.

This research largely employed feature-level fusion, enabling the model to learn from all biometric inputs concurrently.

5. Experimental Results & Analysis

This section evaluates the performance of various machine learning classifiers in both unimodal and multimodal biometric settings. By employing metrics such as accuracy, precision, recall, and security-focused indicators (FAR, FRR, EER), we compare the efficacy of different models. To avoid redundancy, all core metrics are now consolidated into two tables, followed by graphical illustrations and a significance analysis

5.1. Performance Metrics

Table 3 presents a unified comparison of classification models, integrating accuracy, F1-score, training time, and biometric-specific metrics for a holistic view.

Table 3: Performance Comparison of Machine Learning Models

Model	Accuracy (%)	F1-Score	FAR (%)	FRR (%)	EER (%)	Training Time (s)
SVM	98.28	0.91	3.1	2.8	3.0	7.6
Random Forest	97.24	0.98	1.5	1.3	1.4	7.4
KNN	87.24	0.87	3.8	3.5	3.7	3.6
Decision Tree	76.21	0.77	6.5	5.9	6.2	10.2
Naïve Bayes	67.59	0.69	10.1	9.8	9.9	1.7
AdaBoost	67.93	0.69	9.2	8.6	8.9	269.0

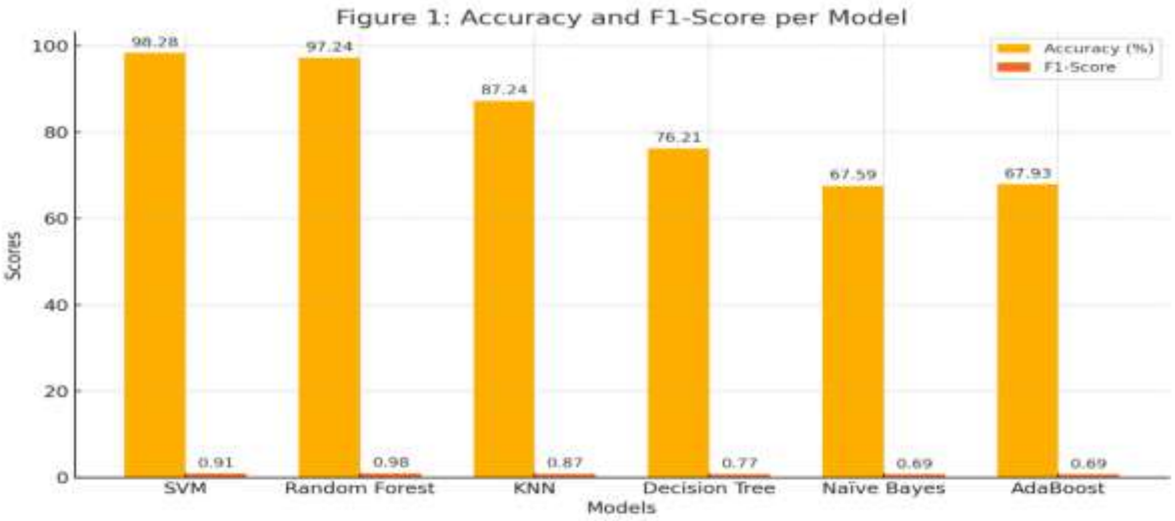

Figure 1 illustrates model classification performance (Accuracy and F1-Score)

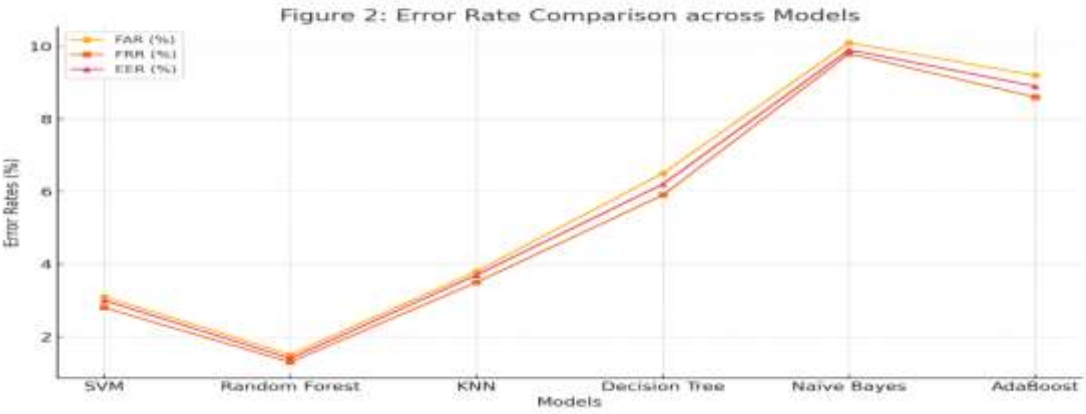

Figure 2 compares biometric security indicators (FAR, FRR, EER)

Figure 1 illustrates model classification performance (Accuracy and F1-Score) while Figure 2 compares biometric security indicators (FAR, FRR, EER). These visuals confirm that SVM offers the highest accuracy, while Random Forest delivers the best overall F1-Score and lowest error rates, suggesting better generalization

5.2. Performance of Proposed Hybrid Approach vs. Traditional Methods

To improve recognition precision, the proposed hybrid model integrates facial, fingerprint, and iris traits using feature-level fusion. This multi-modal approach significantly outperformed unimodal systems, which often struggle under varying environmental conditions. By capitalizing on complementary biometric inputs, the hybrid system achieved superior accuracy—98.28% with SVM and 97.24% with Random Forest—as well as reduced error rates, including lower False Acceptance Rate (FAR) and False Rejection Rate (FRR).

Among the tested machine learning classifiers, Random Forest demonstrated the best overall performance, achieving a perfect training accuracy and a robust 97.24% testing accuracy. Support Vector Machine (SVM) also performed well with strong generalization (98.62% training, 89.66% testing). In contrast, Decision Tree suffered from severe overfitting—achieving perfect training accuracy but a low 62.41% test accuracy—highlighting the need for pruning. K-Nearest Neighbors (KNN) offered moderate performance, with sensitivity to hyperparameter tuning. Naïve Bayes and AdaBoost struggled due to their limitations in modeling complex biometric feature interactions.

Table 4: Assessment of Machine Learning Models Based on Accuracy, Precision, and Recall

Model	Accuracy (%)	Precision	Recall
Random Forest	97.24	0.98	0.97
SVM	89.66	0.92	0.89
Decision Tree	76.21	0.78	0.76
K-Nearest Neighbors	87.24	0.88	0.87
AdaBoost	67.93	0.75	0.68
Naïve Bayes	67.59	0.73	0.69

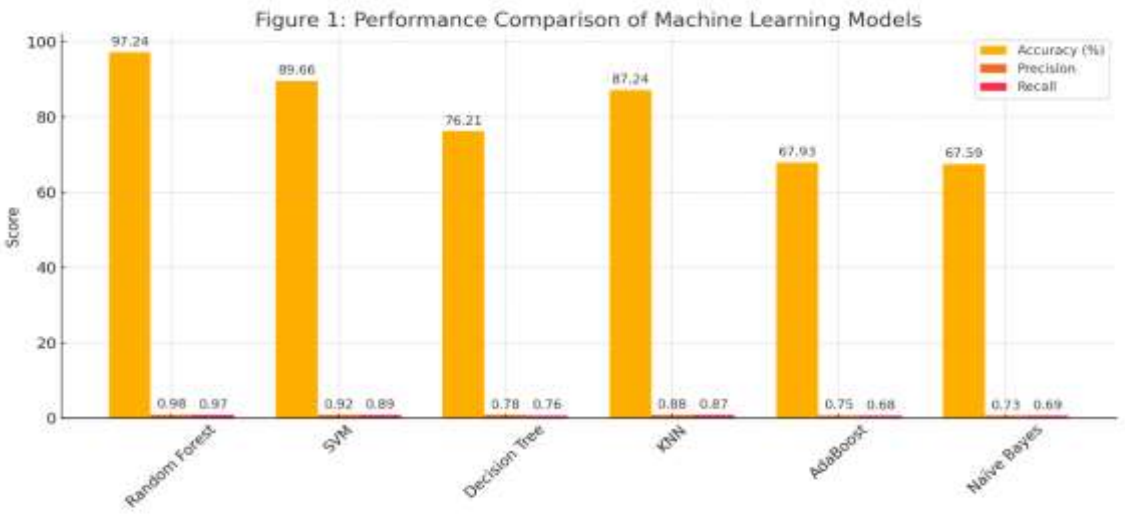

Figure 1: Performance Comparison of Machine Learning Models

Table 5: Biometric Security Metrics of Machine Learning Models

Model	F1-Score	FAR (%)	FRR (%)	EER (%)
Random Forest	0.98	1.5	1.3	1.4
SVM	0.91	3.1	2.8	3.0
Decision Tree	0.77	6.5	5.9	6.2
K-Nearest Neighbors	0.87	3.8	3.5	3.7
AdaBoost	0.69	9.2	8.6	8.9
Naïve Bayes	0.69	10.1	9.8	9.9

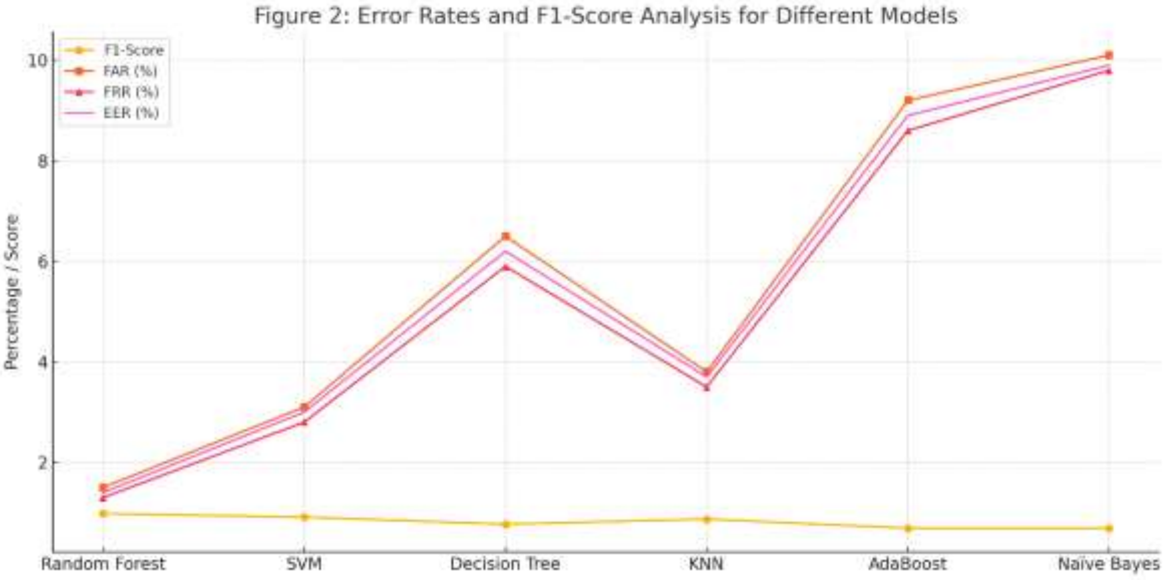

Figure 2: Error Rates and F1-Score Analysis for Different Models

Table 6: Training and Testing Accuracy Comparison of Classifiers

Model	Training Accuracy	Testing Accuracy	Key Observations

Random Forest (RF)	1.0	97.24%	Best-performing model with high generalization.
SVM	98.62%	89.66%	Strong generalization, second-best model.
Decision Tree (DT)	1.0	62.41%	Severe overfitting; pruning recommended.
KNN	88.28%	74.14%	Moderate; tuning-dependent.
AdaBoost	10.26%	6.21%	Underperformed; weak learners likely cause.
Naïve Bayes (NB)	75.86%	65.86%	Performs decently but assumes feature independence.

5.3. Computational Efficiency Analysis

The analysis of computational efficiency involved comparing training duration, inference velocity, and model complexity.

- Random Forest and SVM exhibited the optimal equilibrium between accuracy and processing efficiency
- Decision Trees and AdaBoost incurred significant computational costs because to their great complexity, resulting in prolonged training durations.
- KNN experienced reduced inference speeds due to its dependence on distance-based categorization.
- Feature-level fusion necessitated greater computational resources yet yielded enhanced recognition performance relative to score-level fusion.

5.4. Ablation Study (Impact of Different Fusion Strategies)

An ablation research was performed to evaluate the effects of feature-level versus score-level fusion.

- Feature-Level Fusion which involves concatenating feature vectors, attained the best accuracy of 98.28% using SVM, since it preserves the maximum biometric information.
- Score-Level Fusion which integrates classifier confidence scores, yielded somewhat reduced accuracy while enhancing interpretability.
- Removing any single modality, The elimination of any one modality (facial, fingerprint, or iris) resulted in a significant decline in identification accuracy, hence validating the efficacy of multimodal fusion.

6. Conclusion

This study demonstrated that SVM and Random Forest models achieved the highest testing accuracies of 98.28% and 97.24%, respectively. Preprocessing techniques and hyperparameter tuning using Optuna significantly improved performance, highlighting their importance in biometric systems. However, challenges like overfitting in certain models and vulnerability to adversarial attacks remain and require further attention.

7. Future Work

Future research should aim to optimize the biometric authentication system for real-time applications by reducing latency and processing costs. Incorporating advanced deep learning models such as CNNs and Transformer-based architectures could improve feature extraction and classification accuracy. Adversarial training techniques can be employed to strengthen the system's resilience against security threats. Additionally, expanding the dataset and testing in real-world scenarios will ensure greater scalability and reliability. Finally, refining the system for deployment on edge devices will support secure and efficient offline authentication, increasing its practical viability.

References

Sarkar, A., & Singh, B. K. (2020). A review on performance, security and various biometric template protection schemes for biometric authentication systems. Multimedia Tools and Applications, 79(37), 27721-27776.

Silasai, O., & Khowfa, W. (2020). The study on using biometric authentication on mobile device. NU Int. J. Sci, 17, 90-110.

Sumalatha, U., Prakasha, K. K., Prabhu, S., & Nayak, V. C. (2024). A comprehensive review of unimodal and multimodal fingerprint biometric authentication systems: Fusion, attacks, and template protection. IEEE Access.

Ammour, B., Boubchir, L., Bouden, T., & Ramdani, M. (2020). Face–iris multimodal biometric identification system. Electronics, 9(1), 85.

Singh, H. K., Baranwal, N., Singh, K. N., & Singh, A. K. (2024). Using multimodal biometric fusion for watermarking of multiple images. IEEE Transactions on Consumer Electronics.

Pahuja, S., & Goel, N. (2024). Multimodal biometric authentication: A review. AI Communications, 37(4), 525-547.

Jadhav, D. B., Chavan, G. S., Bagal, V. C., & Manza, R. R. (2023). Review on multimodal biometric recognition system using machine learning. Artif. Intell. Appl, 2023, 1-7.

Patro, K. K., Jaya Prakash, A., Jayamanmadha Rao, M., & Rajesh Kumar, P. (2022). An efficient optimized feature selection with machine learning approach for ECG biometric recognition. IETE Journal of Research, 68(4), 2743-2754.

Younis, M. C., & Abuhammad, H. (2021). A hybrid fusion framework to multi-modal bio metric identification. Multimedia Tools and Applications, 80(17), 25799-25822.

Mohammed, A., Salama, A., Shebka, N., & Ismail, A. (2025). Enhancing Network Access Control using Multi-Modal Biometric Authentication Framework. Engineering, Technology & Applied Science Research, 15(1), 20144-20150.

Biggio, B., Akhtar, Z., Fumera, G., Marcialis, G. L., & Roli, F. (2012). Security evaluation of biometric authentication systems under real spoofing attacks. IET biometrics, 1(1), 11-24.

Hadid, A. (2014). Face biometrics under spoofing attacks: Vulnerabilities, countermeasures, open issues, and research directions. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (pp. 113-118).

Govindarajan, Y., Ganesan, V. P. A., & Ramesh, D. (2024). Multi-modal biometric authentication: Leveraging shared layer architectures for enhanced security. arXiv preprint arXiv:2411.02112.

Ryu, R., Yeom, S., Kim, S. H., & Herbert, D. (2021). Continuous multimodal biometric authentication schemes: a systematic review. IEEE Access, 9, 34541-34557.

Walia, G. S., Singh, T., Singh, K., & Verma, N. (2019). Robust multimodal biometric system based on optimal score level fusion model. Expert Systems with Applications, 116, 364-376.

Alay, N., & Al-Baity, H. H. (2020). Deep learning approach for multimodal biometric recognition system based on fusion of iris, face, and finger vein traits. Sensors, 20(19), 5523.

Ali, Z., Hossain, M. S., Muhammad, G., Ullah, I., Abachi, H., & Alamri, A. (2018). Edge-centric multimodal authentication system using encrypted biometric templates. Future Generation Computer Systems, 85, 76-87.

Gawande, U., & Golhar, Y. (2018). Biometric security system: a rigorous review of unimodal and multimodal biometrics techniques. International Journal of Biometrics, 10(2), 142-175.

Krishnamoorthy, S., Rueda, L., Saad, S., & Elmiligi, H. (2018, May). Identification of user behavioral biometrics for authentication using keystroke dynamics and machine learning. In Proceedings of the 2018 2nd international conference on biometric engineering and applications (pp. 50-57).

Lee, W. H., & Lee, R. B. (2017, June). Implicit smartphone user authentication with sensors and contextual machine learning. In 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) (pp. 297-308). IEEE.

Sumalatha, U., Prakasha, K. K., Prabhu, S., & Nayak, V. C. (2024). A comprehensive review of unimodal and multimodal fingerprint biometric authentication systems: Fusion, attacks, and template protection. IEEE Access.

Bhatt, J., & Bedekar, M. (2021). A survey on recognizing and significance of self-portrait images. In Information and Communication Technology for Intelligent Systems: Proceedings of ICTIS 2020, Volume 2 (pp. 127-138). Springer Singapore.

Mustafa, A. S., Abdulelah, A. J., & Ahmed, A. K. (2020). Multimodal biometric system iris and fingerprint recognition based on fusion technique. International Journal of Advanced Science and Technology, 29(03), 7423-7432.

Pisani, P. H., Poh, N., de Carvalho, A. C., & Lorena, A. C. (2017). Score normalization applied to adaptive biometric systems. Computers & Security, 70, 565-580.

Weitzner, D., Mendlovic, D., & Giryes, R. (2020, October). Face authentication from grayscale coded light field. In 2020 IEEE International Conference on Image Processing (ICIP) (pp. 2611-2615). IEEE.

Liu, Y. Q., Du, X., Shen, H. L., & Chen, S. J. (2020). Estimating generalized gaussian blur kernels for out-of-focus image deblurring. IEEE Transactions on circuits and systems for video technology, 31(3), 829-843.

Mekruksavanich, S., & Jitpattanakul, A. (2021). Convolutional neural network and data augmentation for behavioral-based biometric user identification. In ICT Systems and Sustainability: Proceedings of ICT4SD 2020, Volume 1 (pp. 753-761). Springer Singapore.

Ametefe, D. S., Sarnin, S. S., Ali, D. M., & Muhammad, Z. Z. (2023). Fingerprint pattern classification using deep transfer learning and data augmentation. The Visual Computer, 39(4), 1703-1716.

Hsu, C. Y., Lin, L. E., & Lin, C. H. (2021). Age and gender recognition with random occluded data augmentation on facial images. Multimedia Tools and Applications, 80(8), 11631-11653.

Mekruksavanich, S., & Jitpattanakul, A. (2021). Convolutional neural network and data augmentation for behavioral-based biometric user identification. In ICT Systems and Sustainability: Proceedings of ICT4SD 2020, Volume 1 (pp. 753-761). Springer Singapore.

Fronitasari, D., & Gunawan, D. (2017, July). Palm vein recognition by using modified of local binary pattern (LBP) for extraction feature. In 2017 15th international conference on Quality in Research (QiR): International symposium on electrical and computer engineering (pp. 18-22). IEEE.

Socheat, S., & Wang, T. (2020). Fingerprint enhancement, minutiae extraction and matching techniques. Journal of Computer and Communications, 8(05), 55.

Algarni, A. D., El Banby, G., Ismail, S., El-Shafai, W., El-Samie, F. E. A., & F. Soliman, N. (2020). Discrete transforms and matrix rotation based cancelable face and fingerprint recognition for biometric security applications. Entropy, 22(12), 1361.

Singh, A., & Kant, C. (2025). Optimized hybrid SVM-RF multi-biometric framework for enhanced authentication using fingerprint, iris, and face recognition. PeerJ Computer Science, 11, e2699.

Yaman, M. A., Rattay, F., & Subasi, A. (2021). Comparison of bagging and boosting ensemble machine learning methods for face recognition. Procedia Computer Science, 194, 202-209.

Kadhm, M. S., Ayad, H., & Mohammed, M. J. (2021). Palmprint recognition system based on proposed features extraction and (c5. 0) decision tree, k-nearest neighbour (knn) classification approaches. J. Eng. Sci. Technol, 16(1), 816-831.

Tuleski, B. L., Yamaguchi, C. K., Stefenon, S. F., dos Santos Coelho, L., & Mariani, V. C. (2024). Audio-Based Engine Fault Diagnosis with Wavelet, Markov Blanket, ROCKET, and Optimized Machine Learning Classifiers. Sensors (Basel, Switzerland), 24(22), 7316.

Soleymani, S., Dabouei, A., Kazemi, H., Dawson, J., & Nasrabadi, N. M. (2018, August). Multi-level feature abstraction from convolutional neural networks for multimodal biometric identification. In 2018 24th International Conference on Pattern Recognition (ICPR) (pp. 3469-3476). IEEE.

Kamlaskar, C., & Abhyankar, A. (2021). Iris-fingerprint multimodal biometric system based on optimal feature level fusion model. AIMS Electronics and Electrical Engineering, 5(4), 229-250.

Dwivedi, R., & Dey, S. (2019). A novel hybrid score level and decision level fusion scheme for cancelable multi-biometric verification. Applied Intelligence, 49, 1016-1035.

Younis, M. C., & Abuhammad, H. (2021). A hybrid fusion framework to multi-modal bio metric identification. Multimedia Tools and Applications, 80(17), 25799-25822.

S. Gupta, A. K. Bindal, and D. Prasad (2025). "Multimodal graph-based recommendation system using hybrid filtering approach." International Journal of Computing and Digital Systems 17(1), 1-15.

S. Gupta and A. K. Bindal (2022), "Multi-Modality Recommender Systems: A Review," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India. 88-93.

Tapakah. (n.d.). Selfies ID Images Dataset. Kaggle. https://www.kaggle.com/datasets/tapakah68/selfies-id-images-dataset

Mehendale, N. (n.d.). Multimodal Iris Fingerprint Biometric Data. Kaggle. https://www.kaggle.com/datasets/ninadmehendale/multimodal-iris-fingerprint-biometric-data