Mesopotamian journal of Cybersecurity
Vol.5, No.2, **pp**. 899–912
DOI: https://doi.org/10.58496/MJCS/2025/051; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

Enhancing Multifactor Authentication Using Machine Learning Techniques

Rafea Mohammed Ibrahim[1,*]

[1] *Department of Hadith and its Sciences, College of Islamic Sciences, Al-Iraqia University, Baghdad, Iraq*

ARTICLE INFO

Article History
Received 6 Jun 2025
Revised 20 Jul 2025
Accepted 23 Aug 2025
Published 30 Aug 2025

Keywords
Distributed Database Security
Multifactor Authentication
Machine Learning
Facial recognition
Biometric Security

ABSTRACT

Securing access to distributed database systems presents unique challenges because of their decentralized nature and exposure to multipoint threats. Traditional single-factor authentication mechanisms, such as passwords or PINs, are insufficient in such environments, prompting the need for more resilient solutions. This study proposes a biometric-based multifactor authentication (MFA) framework that combines fingerprint and facial modalities through a unified machine learning (ML) pipeline. ML plays a crucial role in enhancing classification performance by enabling the system to learn complex patterns across biometric inputs. The framework standardizes input preprocessing (by applying grayscale conversion, histogram equalization, and normalization) and employs the histogram of oriented gradients (HOG) technique for feature extraction. To improve classification performance and generalizability, three decision-level ensemble models are used: support vector machine (SVM) integrated with random forest (RF), stochastic gradient descent (SGD), and eXtreme gradient boosting (XGBoost). These hybrid combinations exploit the complementary strengths of different classifiers, such as margin optimization, ensemble learning, and fast convergence, resulting in superior accuracy compared with standalone models. All the models were trained and evaluated via a 10-fold cross-validation scheme on the family fingerprint dataset and face recognition dataset under consistent conditions. The experimental results indicate that the SVM with the RF model achieves the highest accuracy, with scores of 0.92 for fingerprint recognition and 0.97 for facial recognition. These outcomes underscore the framework's suitability for high-security applications, particularly in distributed database environments where reliable and adaptive authentication is essential.

1. INTRODUCTION

The need for strong authentication systems has been exacerbated by the increasing use of digital applications for services that are identity sensitive [1], [2]. Conventional single-factor methods, especially those based on passwords or PINs, have long been viewed as inadequate in the context of growing threats to cybersecurity. Therefore, multifactor authentication (MFA) has been adopted as a standard defense mechanism worldwide [3] . Users are required to prove their identity through at least two independent credentials. Among several other features, fingerprints and facial characteristics are known for their uniqueness and immutability [4]. To leverage these biometric traits effectively, machine learning (ML) has emerged as a transformative approach in classification and identification tasks. Unlike traditional rule-based systems, ML models can automatically learn patterns from data, adapt to variability in biometric inputs, and generalize across diverse conditions. These capabilities are especially valuable in fingerprint and facial recognition, where input quality may be affected by lighting, pose, or partial features. ML techniques also outperform conventional algorithms in handling high-dimensional data, enabling more accurate and reliable authentication in real-world environments. However, the performance of a biometric-based MFA system largely relies on the accuracy, liveness, and resilience of computational representations [5]. In addition to improving authentication accuracy, the implementation of MFA systems in a distributed database environment would yield explicit security and operational benefits [6], [7]. These distributed systems manage sensitive data pertaining to multiple interconnected nodes or servers; hence, they exhibit good proclivity toward the attraction of the data breach, as well as insider threats [8], [9] . The integration of biometric-based MFA in such environments enhances access control at the node level and ensures that only authenticated users and those with valid biometric credentials can access or modify specific data segments to specific segments of the data [10], [11]. Furthermore, the distributed architecture of such databases makes the single points of failure even riskier; MFA mitigates these risks by requiring multiple independent credentials of the likelihood of successful intrusion when one authentication layer is compromised [12] ,[13] .

While earlier multimodal authentication systems made progress in integrating fingerprint and facial traits, many relied on single biometric modalities or implemented basic fusion strategies such as simple feature concatenation or score-level combination, which limited both accuracy and generalizability [14]. For example, Singh and Om (2019) reported gains via unimodal and basic fusion approaches but did not address heterogeneity across biometric datasets, whereas Al-Dulaimi et

*Corresponding author. Email: rafea.ibrahim@aliraqia.edu.iq

al. (2020) focused on unimodal designs without standardizing preprocessing [15]–[17]. In contrast, the present work introduces a concrete methodological advance: decision-level hybridization of a support vector machine (SVM) with random forest (RF), stochastic gradient descent (SGD), and eXtreme gradient boosting (XGBoost) under a unified preprocessing chain (grayscale conversion, histogram equalization, normalization, and histogram-of-oriented gradient feature extraction). This design ensures reproducibility, enhances cross-dataset generalization, and addresses inconsistencies in prior MFA research, establishing a more reliable basis for secure biometric authentication in distributed database environments.

The goal of this study is to propose a dual-modality multi-ML-based MFA framework that integrates fingerprint and facial biometrics via a coherent multi-ML pipeline. This study aims to identify the most reliable and accurate model configuration for secure biometric authentication, which can be conducted properly in a distributed database environment.

2. LITERATURE REVIEW

Recent advancements in biometric-based MFA have shown promising results, particularly with the integration of ML techniques. Researchers are actively exploring how these technologies can make authentication systems more secure and accurate [10], [18].

Several studies have explored unimodal and multimodal approaches. The study introduced a powerful hybrid model that blends the SVM and RF algorithms [19]. Their framework supports multiple biometric inputs, such as fingerprints, facial images, and iris scans, and uses optimization algorithms to sharpen feature selection and classification, achieving good accuracy rates. Another study [20] examined an MFA system for mobile devices via a convolutional neural network (CNNs) that combines multiple biometric and graphical elements, i.e., images of faces and visual cues selected by users. This demonstrated how in-memory deep learning can be applied to real-time mobile environments to enhance user authentication.

Hybrid frameworks that combine deep learning with traditional ML have also been explored. For example, one study [21] presented a CNN–ML hybrid model where Monte Carlo dropout is used for increasing generalizability when the environment is uncertain. This finding shows that blending deep and classical models can improve system reliability. Similarly, another work [22] developed a multimodal system that is based on multiple ML models and adaptive particle swarm optimization (APSO)-integrated face, fingerprint, and finger vein data. The results of feature extraction via histogram of oriented gradients (HOG) are above 94% accuracy.

The fusion of modalities at different levels has also been investigated. A previous study [23] designed a hybrid system that integrates facial recognition via a CNN and fingerprint authentication. Their fusion of modalities at the score level yielded a system accuracy of 96.54%, underscoring the value of combining multiple biometric traits.

While the reviewed studies demonstrate strong performance when various combinations of ML techniques are used for biometric MFA, several gaps remain. Most notably, the majority of the systems focus on either individual or simple fusion of biometric modalities without exploring the impact of ensemble hybridization of classifiers at the decision level. Additionally, the preprocessing pipelines in prior works often lack unified optimization for multiple data types, and few studies explicitly evaluate the generalization performance across diverse user populations. Moreover, despite their high accuracy, many models remain untested under constrained or noisy real-world conditions. This study addresses these gaps by introducing a dual-modality system that combines fingerprint and facial data, applying a consistent image preprocessing pipeline, extracting features, and experimenting with ensemble-based hybrid ML models. This structured approach provides a fresh contribution by demonstrating the comparative strengths of decision-level ensembles for secure biometric MFA in distributed environments.

3. METHODOLOGY

This section outlines the methodological framework employed to design and implement a multi-ML-based MFA system utilizing biometric data. The primary objective of this methodology is to develop an efficient and secure authentication process by integrating fingerprint and facial recognition with robust ML techniques. The methodology is organized into a sequence of four interdependent phases, as illustrated in Fig. 1. Each phase contributes to the overall performance and reliability of the MFA system. These phases include dataset description and preprocessing, feature extraction, model development, and performance evaluation. Each is described in detail in the following subsections, with emphasis on the techniques and algorithms employed to ensure the best accuracy, scalability, and generalizability of the authentication framework.

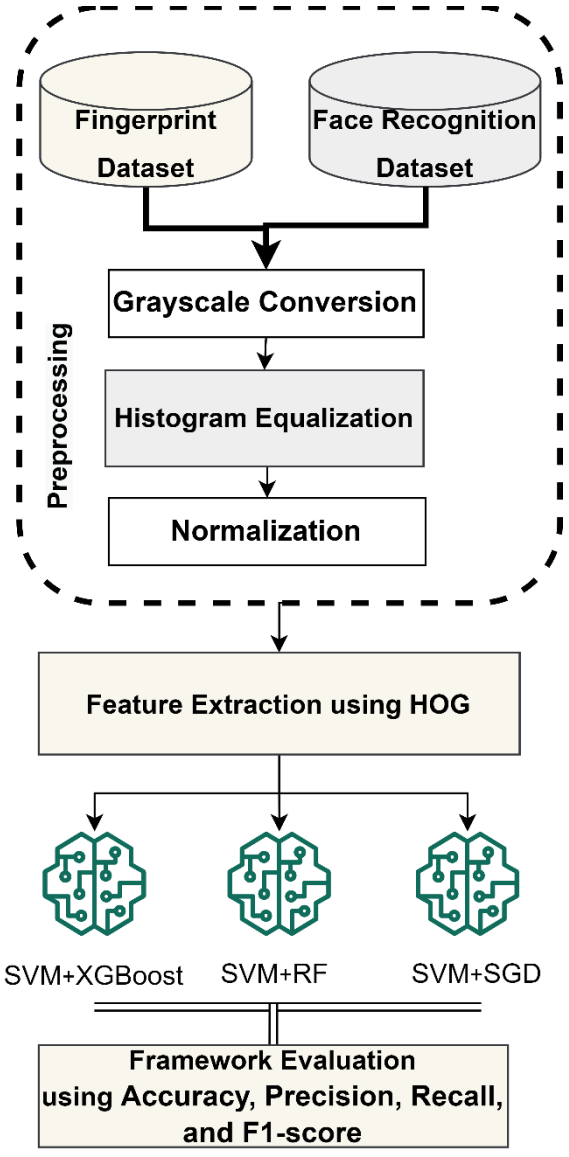

Fig. 1. The proposed methodology phases

3.1 Phase 1: Dataset Description and Preprocessing

The design of the proposed MFA system begins with the identification and preprocessing of the biometric data, which act as the backbone throughout the pipeline. This is the most important stage because the quality and consistency of input images directly impinge on the later functioning stages of feature extraction and classification. In this study, two biometric modalities, fingerprints and facial images, taken from open-source datasets, which are familiar to the research community, were considered. These were chosen not only for their wide acceptance in modern security systems but also because they provide independent and diverse factors that, when combined, improve the level of authentication. Many preprocessing steps are applied to make the data ready for ML models. The pictures are changed to grayscale, histogram equalization is used to improve the contrast, and normalization is used to make the contrast even. Together, these steps help reduce complexity and obtain data that are ready for good feature extraction.

3.1.1 Biometric dataset description

To develop and evaluate the proposed MFA system, two publicly available biometric datasets were utilized, one for fingerprint recognition and the other for facial recognition. These datasets provide a diverse collection of biometric samples necessary for training and testing the multi-ML models.

1) Dataset 1: Fingerprint Dataset

The Mendeley data were the source of the fingerprint dataset used in this study, titled the "Family Fingerprint Dataset" [24]. It consists of 2,000 grayscale images of fingerprints belonging to five main classes of typical fingerprint patterns: arch, left loop, right loop, tented arch, and whorl. There were 400 images per class to maintain a balanced representation for all the categories. These images were in JPEG format with uniform resolution and quality; thus, they are apt for image-based biometric analysis. The accompanying CSV file has metadata and ground truth class labels for each fingerprint image, aiding supervised ML applications. The dataset comprises fingerprints of numerous individuals taken under different conditions, which results in intraclass variation while maintaining interclass separability. This is a very clearly marked dataset with images and is highly applicable to the fingerprint classification task in the real world. Its standardized format and balanced class distribution provide a sound basis for feature extraction, model training, and performance evaluation within the proposed MFA framework.

2) Dataset 2: Face Recognition Dataset

The facial recognition dataset used in this study is taken from Kaggle and is titled the "Face Recognition Dataset" by Vasuki Patel [25]. It comprises facial pictures divided into 31 different classes; each most likely represents an individual class. The dataset serves the purpose of facial recognition and multiclass classification, portraying a lucid structure apt for multi-ML models. There are several high-resolution pictures for each person in each class; the images were taken in different lighting, expressions, and angles. All the pictures are RGB and have the same appearance quality, which makes it possible to work well in terms of extracting facial features and classifying them. The dataset has a folder structure with the names of individual identities. This helps with easy preprocessing and labelling during model training. This dataset was chosen because of its format, high interclass difference, and intraclass variability, all of which are very important for testing the reliability and generalizability of a facial recognition model. It is intended for real-world facial verification scenarios, thus making it a good supplement to the fingerprint dataset in this multimodal biometric authentication study.

Together, these two datasets enable the construction of a dual-modality authentication system, allowing the evaluation of multi-ML models across both fingerprint and facial biometric features.

3.1.2 Preprocessing

Preprocessing has been very important in preparing biometric data for feature extraction and multi-ML model classification. Since raw images of fingerprints or facial structures may have noise and lighting inconsistencies and redundant information, the multi-ML algorithms for MFA systems may not perform well [26]–[29]. To standardize both biometric modalities and address these challenges, a standardized preprocessing pipeline was applied to all the images, consisting of three main stages: conversion to grayscale, histogram equalization, and normalization. The same preprocessing pipeline, grayscale conversion, histogram equalization, and normalization, was uniformly applied to both the fingerprint and facial datasets. Although facial images were originally RGB, grayscale conversion was applied to reduce computational complexity and standardize feature extraction across both modalities. Prior research suggests that structural features such as contours, textures, and edge gradients are sufficient for facial recognition when robust descriptors such as HOG are used. Since HOG primarily captures gradient information rather than color distribution, converting to grayscale does not significantly degrade recognition performance and instead enhances consistency across biometric modalities.

1) Stage 1: Greyscale Conversion

The first step changes all the images from RGB to grayscale. This conversion reduces the data dimensions by deleting color channels, which usually does not matter for biometric pattern recognition [27],[30]. This is not only the case for grayscale conversion, since it also enables the models to concentrate on structural and textural information such as ridges in fingerprints or facial contour lines, which are more critical for authentication [31].

2) Stage 2: Histogram Equalization

After the images are converted to grayscale, histogram equalization is applied to enhance the visual quality and contrast of each image. The technique redistributes the values of pixel intensity across the available space, highlighting minute variations in texture that may not be well perceived in low-contrast areas [32], [33]. Fingerprint images assist in identifying ridges and valley patterns; facial images include features such as the outline of the face, shadows, and expressions, leading to better recognition [34], [35].

3) Stage 3: Normalization

This process scales all pixel intensities to a consistent range, usually 0--1 [36]. Normalization makes the input data statistically uniform, which in turn stabilizes the training process for the multi-ML models of the MFA system [37], [38]. If not normalized, the pixel values may have large disparities, which in turn may either bias the learning process or cause

convergence issues in optimization. By setting the dynamic range of the biometric images, normalization improves the quality and speed of the feature extraction and classification phases.

Together, these preprocessing techniques contribute to a cleaner, more informative representation of the biometric data. They form a crucial foundation for extracting robust features and achieving high classification performance, particularly when dealing with two different data modalities in a unified authentication system.

3.2 Phase 2: Feature Extraction via the HOG technique

Once the biometric images have been preprocessed and standardized, the next critical process in the development of an MFA system is feature extraction. This process converts image data into a structured dataset describing the most relevant patterns and textures needed for classification while ignoring redundant or noninformative content [39]. The HOG method was used for this study because it is an efficient method for preserving edge and gradient information in visual data, which is exceptionally valuable in biometrics [40]. HOG first calculates the image gradient orientations within very small spatial regions known as cells [41], [42]. The local histograms are then computed over the larger blocks for variations in illumination and contrast to normalize these gradient orientation distributions [43]. The resulting feature vector encodes the shape, structure, and directional intensity changes in an image, which are mostly characteristic and discriminative over various samples of the same individual. The extraction of an HOG feature vector of an image is performed according to the following steps [43]–[46]:

Step 1: Use a gradient filter [1; 0; 1] to compute the horizontal Ii(i, j) and vertical Ij(i, j) gradients of an image.

Step 2: Compute the magnitude I(i; j), as in (1), and angle θ(i; j), as in (2), of the gradient.

$$|I(i,j)| = \sqrt{I_i(i,j)^2 + I_j(i,j)^2} \qquad (1)$$

$$\theta(i,j) = \arctan\left(\frac{I_I(i,j)}{I_i(i,j)}\right) \qquad (2)$$

Step 3: Divide an image into cells of (8 × 8) pixels. Then, a histogram with nine orientation bins at (0° − 180°) is computed. The magnitude |I(i, j)| whose angle θ(i, j) belongs to the same bin is added up as the value of this bin.

Step 4: Four connected cells are combined into a block, and histograms of the cells can be normalized in the block via the low-style clipped L2 norm normalization method. The combination of all the histograms constitutes the HOG feature vector of the image.

By applying the HOG algorithm uniformly to both the fingerprint and facial datasets, the system ensures consistency in feature representation across modalities. The extracted features serve as the input to the multi-ML models described in the next phase, enabling robust classification on the basis of the geometric and structural characteristics of the biometric inputs.

3.3 Phase 3: Development of Hybrid Multi-ML Models

After feature extraction via HOG has been described, classification models are designed and trained to accurately differentiate individual biometric identities. In this study, we take an approach that combines several different ML algorithms to form multimodel MFA system frameworks. The reason for such an approach is that different classifiers' strengths are complementary; for example, one excels in margin optimization, whereas the other has better generalizability or computational efficiency [47]. By using these combinations, the system will attempt to attain superior classification performance with more robustness in the face of variability in biometric data [48]. Three hybrid model configurations were proposed and evaluated. The first model integrates an SVM with an RF. One is a powerful margin-based classifier, which excels at handling high-dimensional data and finding optimal hyperplanes for separation; the other is ensemble learning based on decision trees, which offers high accuracy and robustness to overfitting as well as the ability to handle nonlinear relationships [49], [50]. This model combines the best of both worlds for the MFA system framework: the clear boundary-drawing capability of one component and the ensemble strength of the other for managing noisy or diverse biometric features [51], [52]. The second setting integrates SVM with SGD, motivated by the need for scalability and fast convergence in large-scale datasets. While SVM provides structured and stable classification, the stochastic gradient method provides dynamic, iterative learning that can fairly easily manage the implementation of models on the basis of new batches of data [53]. This approach would be particularly useful for model-based adaptive and computationally efficient MFA systems. The third approach unites SVM with XGBoost, a method known for its speed and quality in tasks with structured data. A sequence of weak learners is used to reduce classification errors in a very adaptive process [54]. Integrating XGBoost with SVM results

in system learning on two layers: SVM works on maximizing the margin, whereas XGBoost improves the predictions through boosting and thereby makes the final classification more confident and more accurate.

In this study, hybridization is performed at the decision level. After feature extraction via HOG, the feature vectors are classified via a baseline SVM. The decision scores generated by the SVM are then combined with those of a secondary classifier to form an ensemble. A weighted voting mechanism is adopted, where the SVM score carries the primary weight owing to its robustness in high-dimensional spaces, while the secondary classifier refines cases near decision boundaries. This design ensures that the strengths of both models are leveraged: the SVM contributes margin-based separation, whereas the secondary classifier enhances generalization. Compared with single-model baselines, this fusion reduces misclassification in ambiguous samples and improves system stability across different biometric modalities.

Every such hybrid configuration was trained on the identical extracted feature set from images of both fingerprints and faces so that a fair comparison can be ensured. Their performance is assessed in the next phase, wherein validation metrics are used to discern the fittest model for biometric MFA that is secure and dependable.

3.4 Phase 4: Model Validation and Evaluation

The final phase of the proposed methodology focuses on validating the performance of the developed hybrid multi-ML models. Model validation is a critical step to ensure that the system not only performs well on training data but also generalizes effectively to unseen biometric samples [55], [56]. To achieve a comprehensive evaluation, the models were tested using both fingerprint and facial data under consistent conditions, with performance assessed through four standard evaluation metrics: accuracy, precision, recall, and F1 score. Table 1 provides detailed formulations for these metrics:

TABLE I. THE EMPLOYED PERFORMANCE METRICS

Evaluation metrics	Mathematical Equation	Explanation
Accuracy	$\boldsymbol{Accuracy} = \frac{\boldsymbol{TP + TN}}{\boldsymbol{TP + FP + FN + TN}}$	Accuracy measures the ratio of correctly classified biometric authentication instances (both fingerprint and face) to the total number of instances in the dataset. It offers an overall assessment of the model's ability to correctly recognize or reject user identities.
Precision	$\text{Precision} = \frac{\boldsymbol{TP}}{\boldsymbol{TP + FP}}$	Precision quantifies the proportion of biometric inputs that were correctly identified as genuine users (true positives) among all those predicted to be genuine. In MFA systems, this metric helps evaluate the system's ability to avoid false acceptances, which is critical for security.
Recall (Sensitivity)	$\text{Recall} = \frac{\boldsymbol{TP}}{\boldsymbol{TP + FN}}$	Recall reflects the model's ability to correctly identify all actual genuine user inputs in the dataset. High recall is essential in authentication scenarios to ensure that valid users are not wrongly denied access.
F1-score	$\boldsymbol{F1}\text{-score} = \frac{\boldsymbol{2 * TP}}{\boldsymbol{2 * TP + FP + FN}}$	The F1-score provides a balanced evaluation of both precision and recall, capturing the model's effectiveness in minimizing both false acceptances and false rejections. This makes it particularly useful in applications like biometric MFA, where both types of errors are significant.
TP: True Positive, TN: True Negative, FP: False Positive, TN: True Negative, FN: False Negative		

To ensure consistency in evaluation, each hybrid model (SVM with RF, SVM with SGD, and SVM with XGBoost) was trained and tested via the same training-validation split across identical datasets. This setup enables direct performance comparison and highlights the strengths and weaknesses of each approach under the same feature representation derived from HOG. Through this metric validation strategy, the most suitable hybrid model can be selected on the basis of not only overall accuracy but also reliability, robustness, and practical utility in real-world authentication environments. The evaluation results serve as the foundation for further analysis and interpretation in the next section of the study.

4. RESULTS AND DISCUSSION

The results of the developed framework are presented in the following sections. Each subsection summarizes the performance of the proposed multi-ML models for the MFA system across different biometric modalities via standard evaluation metrics. The outcomes are interpreted in light of their relevance to secure and reliable MFA systems.

4.1 Framework Results for the Fingerprint Dataset

To evaluate the effectiveness of the proposed fingerprint-based biometric authentication framework, three hybrid ML models were implemented and tested via preprocessed features extracted via the HOG technique. The models include the SVM combined with the RF, SGD, and XGBoost classifiers.

The first combination (SVM with RF) model yielded the best performance across all the evaluation metrics, with an accuracy of 0.92, precision of 0.95, recall of 0.95, and F1 score of 0.95, as presented in Fig. 2. These values indicate that the model was highly effective at distinguishing between genuine users and imposters with minimal misclassifications. The classification report confirmed consistent results across most fingerprint classes, with only minor decreases in recall observed in classes with limited samples. The combination of SVM margin-based learning with the ensemble power of the RF enables the model to generalize well, even under varying biometric input conditions.

The second combination (SVM with SGD) model also demonstrated promising results, with an accuracy of 0.82, precision of 0.90, recall of 0.91, and F1 score of 0.86, as shown in Fig. 3. While slightly lower than the SVM with the RF configuration, this model showed strong sensitivity and precision, indicating a good balance between correct positive identifications and the minimization of false acceptances. However, it exhibited more performance variation across classes, particularly where sample sizes were limited. Nonetheless, owing to its lightweight computational footprint, this model remains suitable for real-time or resource-constrained environments.

In contrast, the third combination (SVM with XGBoost) model produced significantly weaker performance, with an accuracy of 0.65, precision of 0.59, recall of 0.56, and F1 score of 0.55, as illustrated in Fig. 4. Several fingerprint classes were either poorly classified or entirely missed, as reflected by the undefined precision and F1-score warnings in the classification report. This performance drop suggests that the XGBoost component may not have been compatible with the data structure or feature representation, leading to instability and poor generalizability.

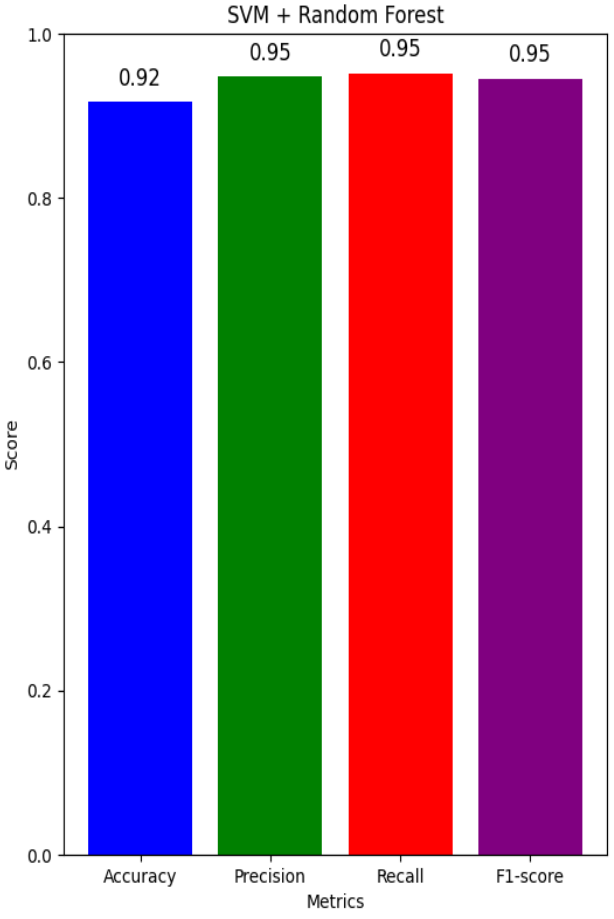

Fig. 2. Performance Metrics of SVM with the RF Model on the Fingerprint Dataset.

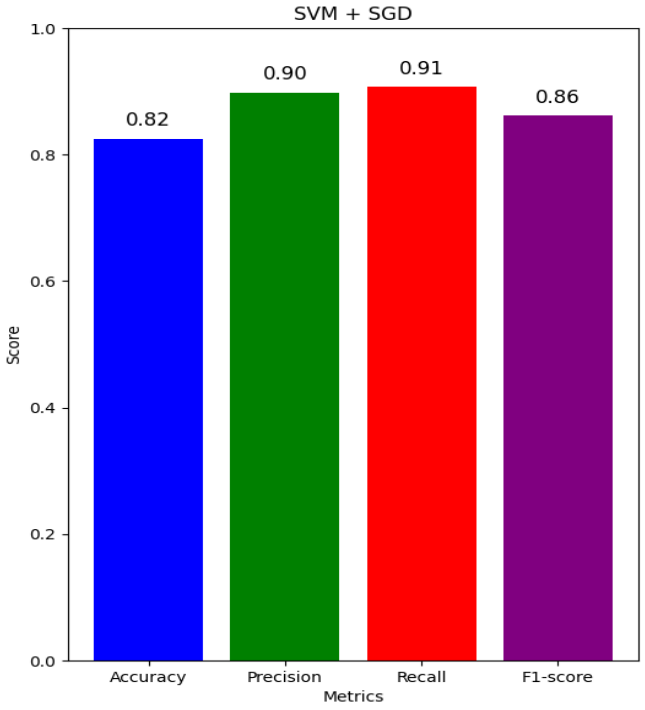

Fig. 3. Performance Metrics of SVM with the SGD Model on the Fingerprint Dataset

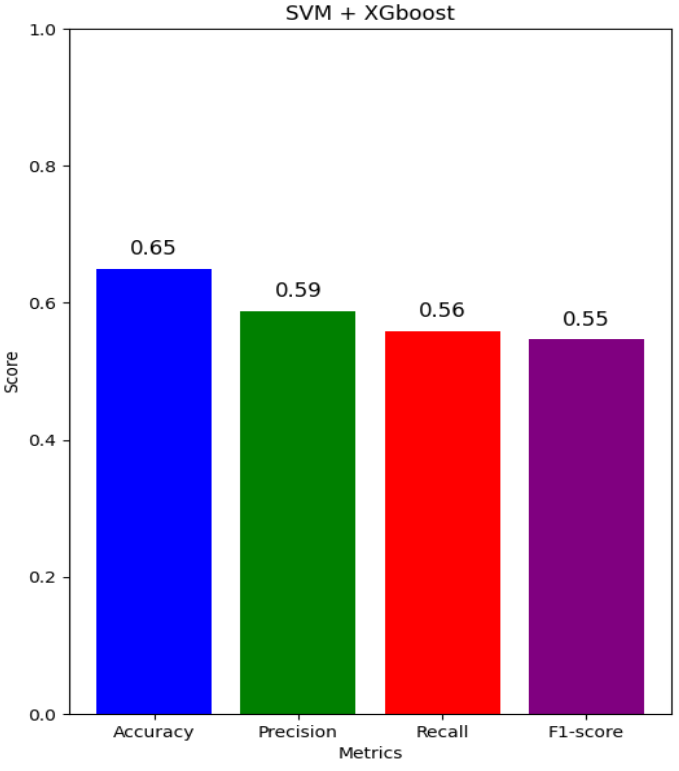

Fig. 4. Performance Metrics of SVM with XGBoost Model on Fingerprint Dataset

Table 2 summarizes the evaluation metrics for three hybrid ML models applied to the fingerprint dataset. Overall, the results confirm that the integration of SVM with RF is the most reliable configuration for fingerprint-based biometric verification within the proposed framework. The consistent scores across multiple evaluation metrics highlight its potential for use in high-stakes, real-world MFA applications.

TABLE II. PERFORMANCE COMPARISON OF HYBRID MULTI-ML MODELS ON THE FINGERPRINT DATASET

Model	Accuracy	Precision	Recall	F1-score
SVM with RF	0.92	0.95	0.95	0.95
SVM with SGD	0.82	0.90	0.91	0.86
SVM with XGBoost	0.65	0.59	0.56	0.55

While prior studies have reported fingerprint recognition accuracies ranging from 94% to 96%, it is important to consider differences in experimental settings, feature extraction methods, and datasets. Many of those studies employed deep learning models such as CNN which benefit from large-scale training data and higher computational complexity. In contrast, this approach focuses on hybrid classical ML models (SVMs with RFs) combined with handcrafted HOG features, which are significantly more lightweight and interpretable. Despite this, our framework achieved a competitive accuracy of 92% on a diverse fingerprint dataset. This demonstrates the viability of our model for secure and resource-constrained biometric authentication systems, especially in distributed database environments where real-time response and interpretability are critical.

4.2 Framework Results for the Face Recognition Dataset

Three hybrid ML models (SVM with RF, SVM with SGD, and SVM with XGBoost) were used for the evaluation of the facial recognition dataset. This confirms the robustness of the proposed MFA framework among biometric modalities. All the models were trained on HOG-extracted features, and their performances were assessed on the basis of accuracy, precision, recall, and F1 score. In the evaluation, the best performing model was found to be the SVM, with the RF having all the metrics 0.97, as shown in Fig. 5. The classification report showed excellent per-class stability with little cross-validation, indicating good generalization performance over a broad range of identities. The results further indicate that there is strong synergy between the discriminative ability of the SVM and the robustness of the RF when faced with complex facial features.

Fig. 6 shows that the SVM with the SGD model closely followed, yielding an accuracy of 0.93, precision of 0.94, recall of 0.92, and F1 score of 0.92. While its performance was slightly lower than that of the RF, it still exhibited high consistency across classes. Its stochastic optimization mechanism makes it well suited for scalable applications where computational efficiency is prioritized.

In contrast, the SVM with XGBoost model results presented in Fig. 7 recorded lower scores across all the metrics, with an accuracy of 0.87 and an F1 score of 0.86. While still acceptable, the model displayed greater class-level variation and sensitivity to sample imbalance. Nevertheless, its overall performance surpassed its counterpart on the fingerprint dataset, indicating better adaptation to the facial recognition task.

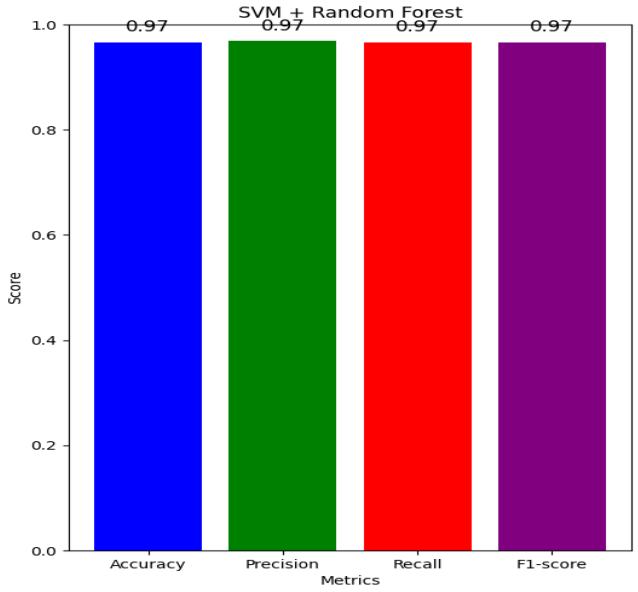

Fig. 5. Performance metrics of the SVM with the RF model on the facial recognition dataset.

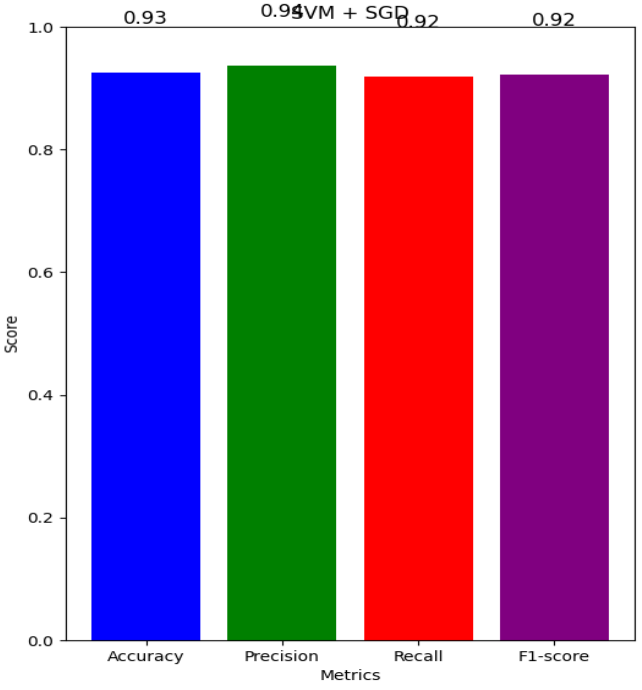

Fig. 6. Performance metrics of the SVM with the SGD model on the facial recognition dataset.

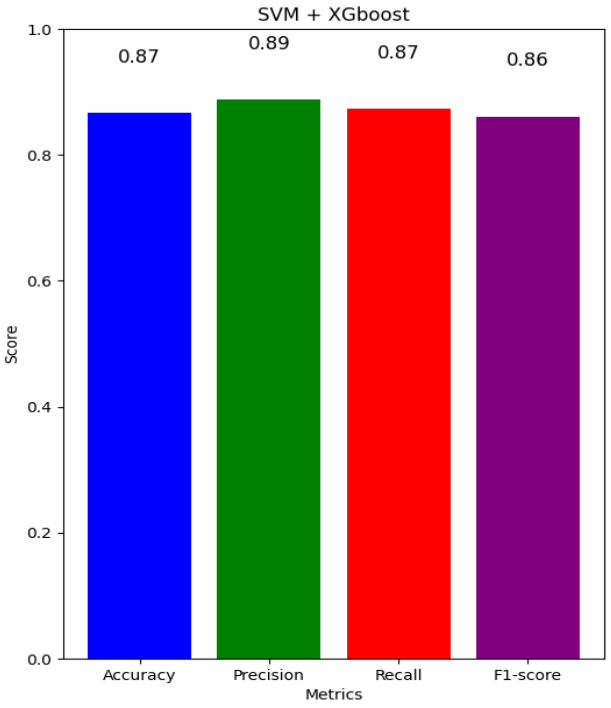

Fig. 7. Performance metrics of the SVM with the XGBoost model on the facial recognition dataset.

Furthermore, Table 3 summarizes the evaluation results for three multi-ML models applied to the facial recognition dataset. While all three hybrid models performed reasonably well, the SVM with the RF clearly stands out as the most effective configuration for facial biometric recognition within the proposed MFA framework. The other models, especially SVM with SGD, may offer valuable trade-offs in scenarios requiring faster computation or lower resource consumption.

TABLE III. PERFORMANCE COMPARISON OF HYBRID MULTI-ML MODELS ON THE FACIAL RECOGNITION DATASET

Model	Accuracy	Precision	Recall	F1-score
SVM with RF	0.97	0.97	0.97	0.97
SVM with SGD	0.93	0.94	0.92	0.92
SVM with XGBoost	0.87	0.89	0.87	0.86

5. CONCLUSION

This study proposed a robust MFA framework that leverages biometric modalities, specifically fingerprints and facial images, combined with multi-ML models to address the growing need for secure identity verification in distributed digital environments. Motivated by the limitations of traditional single-factor systems and the fragmented methodologies of prior biometric studies, this research aimed to unify the authentication pipeline through consistent preprocessing, reliable feature extraction, and comparative evaluation of multiple classifier configurations. A structured four-phase methodology was implemented: biometric datasets were acquired and preprocessed via grayscale conversion, histogram equalization, and normalization; discriminative features were extracted via the HOG; and multi-ML model combinations (SVM with RF, SVM with SGD, and SVM with XGBoost) were developed and evaluated via the same fingerprint and face datasets to ensure consistency and fairness in the comparative analysis. The experimental results demonstrated that the SVM with the RF model outperformed the other configurations across both modalities. It achieved an accuracy of 0.92 on the fingerprint dataset and 0.97 on the facial recognition dataset, with corresponding high precision, recall, and F1-scores. The findings validate the effectiveness of using a unified, multi-ML-based pipeline for biometric MFA systems. The dual-modality approach has potential for enhancing system robustness and accuracy, and it conceptually aligns with the demands of distributed database environments, where layered security and consistent user verification are critical. Future research will extend this work by integrating deep learning architectures, testing real-time authentication in distributed settings, and systematically evaluating resilience under adversarial or noisy conditions.

Conflicts of interest

The author declare that he have no conflicts of interest.

Funding

Not Applicable.

Acknowledgement

None

References

[1] S. Zou, "A robust and effective 3-factor authentication protocol for smart factory in IIoT," *Comput. Commun*, vol. 220, pp. 81–93,, doi: 10.1016/j.comcom.2024.04.011.

[2] G. . Ali , Trans., "Integration of Artificial Intelligence, Blockchain, and Quantum Cryptography for Securing the Industrial Internet of Things (IIoT): Recent Advancements and Future Trends", *Applied Data Science and Analysis*, vol. 2025, pp. 19–82, Mar. 2025, doi: 10.58496/ADSA/2025/004.

[3] D. Wang, J. Zhou, M. Masdari, S. N. Qasem, and B. T. Sayed, "Security in wireless body area networks via anonymous authentication: Comprehensive literature review, scheme classification, and future challenges," *Ad Hoc Networks*, vol. 153, p. 103332, doi: 10.1016/j.adhoc.2023.103332.

[4] J. Al-Saraireh and M. R. AlJa'afreh, "Keystroke and swipe biometrics fusion to enhance smartphones authentication," *Comput. Secur*, vol. 125, p. 103022, doi: 10.1016/j.cose.2022.103022.

[5] M. Saqib, B. Jasra, and A. H. Moon, "A lightweight three factor authentication framework for IoT based critical applications," *J. King Saud Univ. - Comput. Inf. Sci*, vol. 34, no. 9, pp. 6925–6937,, doi: 10.1016/j.jksuci.2021.07.023.

[6] S. Tanwar, D. Ribadiya, P. Bhattacharya, A. R. Nair, N. Kumar, and M. Jo, "Fusion of blockchain and IoT in scientific publishing: Taxonomy, tools, and future directions," *Futur. Gener. Comput. Syst*, vol. 142, pp. 248–275,, doi: 10.1016/j.future.2022.12.036.

[7] G. Ali, "Enhancing Cybersecurity in Smart Education with Deep Learning and Computer Vision: A Survey"," *Mesopotamian J. Comput. Sci.*, vol. 2025, pp. 115–158,, doi: 10.58496/MJCSC/2025/008.

[8] Z. Ali, S. A. Chaudhry, K. Mahmood, S. Garg, Z. Lv, and Y. B. Zikria, "A clogging resistant secure authentication scheme for fog computing services," *Comput. Networks*, vol. 185, p. 107731, doi: 10.1016/j.comnet.2020.107731.

[9] "Big Data Predictive Analytics for Personalized Medicine: Perspectives and Challenges," *Applied Data Science and Analysis*, vol. 2024 SE-Articles. pp. 32–38. doi: 10.58496/ADSA/2024/004.

[10] H. A. Alameen and F. Rabee, "Blockchain-Based Metadata Management in Distributed File Systems"," *Mesopotamian J. CyberSecurity*, vol. 5, no. 2, pp. 349–360,, doi: 10.58496/MJCS/2025/022.

[11] S. M. Darwish and A. A. Ismail, "An Evolutionary Biometric Authentication Model for Finger Vein Patterns BT," in *Proceedings of the International Conference on Advanced Intelligent Systems and Informatics 2020,"*, pp. 271–281.

[12] S. A. Hussein, "Integrating Law, Cybersecurity, and AI: Deep Learning for Securing Iris-Based Biometric Systems"," *Mesopotamian J. CyberSecurity*, vol. 5, no. 2, pp. 319–336,, doi: 10.58496/MJCS/2025/020.

[13] J. J. Hathaliya, S. Tanwar, and R. Evans, "Securing electronic healthcare records: A mobile-based biometric authentication approach," *J. Inf. Secur. Appl*, vol. 53, p. 102528, doi: 10.1016/j.jisa.2020.102528.

[14] R. Srivastva, Y. N. Singh, and A. Singh, "Statistical independence of ECG for biometric authentication," *Pattern Recognit*, vol. 127, p. 108640, doi: 10.1016/j.patcog.2022.108640.

[15] R. A. Aljanabi, Z. Al-Qaysi, and M. S. Suzani, "Deep Transfer Learning Model for EEG Biometric Decoding"," *Appl. Data Sci. Anal.*, vol. 2024, pp. 4–16,, doi: 10.58496/ADSA/024/002.

[16] G. Choi, G. Ziyang, J. Wu, C. Esposito, and C. Choi, "Multi-modal Biometrics Based Implicit Driver Identification System Using Multi-TF Images of ECG and EMG," *Comput. Biol. Med*, vol. 159, p. 106851, doi: 10.1016/j.compbiomed.2023.106851.

[17] M. Singh, N. Baranwal, K. N. Singh, A. K. Singh, and H. Zhou, "Deep learning-based biometric image feature extraction for securing medical images through data hiding and joint encryption–compression," *J. Inf. Secur. Appl*, vol. 79, p. 103628, doi: 10.1016/j.jisa.2023.103628.

[18] E. A. Alkeem, "Robust Deep Identification using ECG and Multimodal Biometrics for Industrial Internet of Things," *Ad Hoc Networks*, vol. 121, p. 102581, doi: 10.1016/j.adhoc.2021.102581.

[19] A. S. Sonal and C. Kant, "Optimized hybrid SVM-RF multibiometric framework for enhanced authentication using fingerprint, iris, and face recognition," *PeerJ Comput. Sci*, vol. 11, doi: 10.7717/PEERJ-CS.2699.

[20] J. Han, "CNN-Based Multi-Factor Authentication System for Mobile Devices Using Faces and Passwords," *Appl. Sci*, vol. 14, no. 12, doi: 10.3390/app14125019.

[21] Z. Wen, S. Han, Y. Yu, X. Xiang, S. Lin, and X. Xu, "Empowering robust biometric authentication: The fusion of deep learning and security image analysis," *Appl. Soft Comput*, vol. 154, p. 111286, doi: 10.1016/j.asoc.2024.111286.

[22] C. Vensila and A. B. Wesley, "Multimodal biometrics authentication using extreme learning machine with feature reduction by adaptive particle swarm optimization," *Vis. Comput*, vol. 40, no. 3, pp. 1383–1394,, doi: 10.1007/s00371-023-02856-4.

[23] S. Bharadwaj, P. Amin, D. J. Ramya, and S. Parikh, "Reliable human authentication using AI-based multibiometric image sensor fusion: Assessment of performance in information security," *Meas. Sensors*, vol. 33, no. March, p. 101140, doi: 10.1016/j.measen.2024.101140.

[24] D. Maiti and D. Das, "FAMILY FINGERPRINT DATASET," 2023.

[25] V. Patel, "Face Recognition Dataset."

[26] T. J. Mohammed *et al.*, "Convalescent-plasma-transfusion intelligent framework for rescuing COVID-19 patients across centralised/decentralised telemedicine hospitals based on AHP-group TOPSIS and matching component," *Appl. Intell.*, no. Icci, 2021, doi: 10.1007/s10489-020-02169-2.

[27] A. R. J. Mitchell, D. Ahlert, C. Brown, M. Birge, and A. Gibbs, "Electrocardiogram-based biometrics for user identification – Using your heartbeat as a digital key.," *J. Electrocardiol.*, vol. 80, pp. 1–6, 2023, doi: https://doi.org/10.1016/j.jelectrocard.2023.04.001.

[28] A Comparative study of Chest Radiographs and Detection of The Covid 19 Virus Using Machine Learning Algorithm," *Mesopotamian J. Comput. Sci.*, vol. 2024, pp. 34–43, 2024, doi: 10.58496/MJCSC/2024/004.

[29] "Advanced Image Processing Techniques for Automated Detection of Healthy and Infected Leaves in Agricultural Systems," *Mesopotamian J. Comput. Sci.*, vol. 2024, pp. 44–52, 2024, doi: 10.58496/MJCSC/2024/006.

[30] L. Wan, K. Liu, H. A. Mengash, N. Alruwais, M. Al Duhayyim, and K. Venkatachalam, "Deep learning-based photoplethysmography biometric authentication for continuous user verification," *Appl. Soft Comput.*, vol. 156, p. 111461, 2024, doi: https://doi.org/10.1016/j.asoc.2024.111461.

[31] S. S. Thenuwara, C. Premachandra, and H. Kawanaka, "A multi-agent based enhancement for multimodal biometric system at border control," *Array*, vol. 14, p. 100171, 2022, doi: https://doi.org/10.1016/j.array.2022.100171.

[32] I. Boucherit, M. O. Zmirli, H. Hentabli, and B. A. Rosdi, "Finger vein identification using deeply-fused Convolutional Neural Network," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 3, pp. 646–656, 2022, doi: https://doi.org/10.1016/j.jksuci.2020.04.002.

[33] Y.-J. Kang, J.-I. Yoo, Y.-H. Cha, C. H. Park, and J.-T. Kim, "Machine learning–based identification of hip arthroplasty designs," *J. Orthop. Transl.*, vol. 21, pp. 13–17, 2020, doi: https://doi.org/10.1016/j.jot.2019.11.004.

[34] R. G. Babu, P. Karthika, and G. Manikandan, "Polynomial Equation Based Localization and Recognition Intelligent Vehicles Axis using Wireless Sensor in MANET," *Procedia Comput. Sci.*, vol. 167, pp. 1281–1290,

2020, doi: https://doi.org/10.1016/j.procs.2020.03.444.

[35] N. Aghnia Farda, J.-Y. Lai, J.-C. Wang, P.-Y. Lee, J.-W. Liu, and I.-H. Hsieh, "Sanders classification of calcaneal fractures in CT images with deep learning and differential data augmentation techniques.," *Injury*, vol. 52, no. 3, pp. 616–624, Mar. 2021, doi: 10.1016/j.injury.2020.09.010.

[36] A. A. Al-Hillali and S. S. Omran, "Half Iris Matching Based on RED Algorithm," *Int. J. Informatics Commun. Technol.*, vol. 5, no. 1, p. 21, 2016, doi: 10.11591/ijict.v5i1.pp21-27.

[37] N. Dominic, Daniel, T. W. Cenggoro, A. Budiarto, and B. Pardamean, "Transfer learning using inception-resnet-v2 model to the augmented neuroimages data for autism spectrum disorder classification," *Commun. Math. Biol. Neurosci.*, vol. 2021, pp. 1–21, 2021, doi: 10.28919/cmbn/5565.

[38] Y. Wang, H. Lu, X. Qin, and J. Guo, "Residual Gabor convolutional network and FV-Mix exponential level data augmentation strategy for finger vein recognition," *Expert Syst. Appl.*, vol. 223, p. 119874, 2023, doi: https://doi.org/10.1016/j.eswa.2023.119874.

[39] Z. Ding *et al.*, "Multi-resolution 3D-HOG feature learning method for Alzheimer's Disease diagnosis," *Comput. Methods Programs Biomed.*, vol. 214, p. 106574, 2022, doi: https://doi.org/10.1016/j.cmpb.2021.106574.

[40] K. Fatema *et al.*, "Heliyon Development of an automated optimal distance feature-based decision system for diagnosing knee osteoarthritis using segmented X-ray images," *Heliyon*, vol. 9, no. 11, p. e21703, 2023, doi: 10.1016/j.heliyon.2023.e21703.

[41] A. K. Sharma *et al.*, "HOG transformation based feature extraction framework in modified Resnet50 model for brain tumor detection," *Biomed. Signal Process. Control*, vol. 84, p. 104737, 2023, doi: https://doi.org/10.1016/j.bspc.2023.104737.

[42] A. Sharma, D. P. Yadav, H. Garg, M. Kumar, B. Sharma, and D. Koundal, "Bone Cancer Detection Using Feature Extraction Based Machine Learning Model," *Comput. Math. Methods Med.*, vol. 2021, 2021, doi: 10.1155/2021/7433186.

[43] M. Mebarkia, A. Meraoumia, L. Houam, and S. Khemaissia, "X-ray image analysis for osteoporosis diagnosis: From shallow to deep analysis," *Displays*, vol. 76, p. 102343, 2023, doi: https://doi.org/10.1016/j.displa.2022.102343.

[44] S. Ramachandra and S. Ramachandran, "Region specific and subimage based neighbour gradient feature extraction for robust periocular recognition," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 10, Part A, pp. 7961–7973, 2022, doi: https://doi.org/10.1016/j.jksuci.2022.07.013.

[45] S. Demir, S. Key, T. Tuncer, and S. Dogan, "An exemplar pyramid feature extraction based humerus fracture classification method," *Med. Hypotheses*, vol. 140, p. 109663, 2020, doi: https://doi.org/10.1016/j.mehy.2020.109663.

[46] H. Abubakar, F. Al-Turjman, Z. S. Ameen, A. S. Mubarak, and C. Altrjman, "A hybridized feature extraction for COVID-19 multi-class classification on computed tomography images," *Heliyon*, vol. 10, no. 5, p. e26939, 2024, doi: https://doi.org/10.1016/j.heliyon.2024.e26939.

[47] T. J. Mohammed, *A Systematic Review of Artificial Intelligence in Orthopaedic Disease Detection: A Taxonomy for Analysis and Trustworthiness Evaluation*, vol. 17, no. 1. Springer Netherlands.

[48] F. Han, X. Li, J. Zhao, and F. Shen, "A unified perspective of classification-based loss and distance-based loss for cross-view gait recognition," *Pattern Recognit*, vol. 125, p. 108519, doi: 10.1016/j.patcog.2021.108519.

[49] M. K. Benkaddour and A. Bounoua, "Feature extraction and classification using deep convolutional neural networks, PCA and SVC for face recognition," *Trait. du Signal*, vol. 34, no. 1–2, pp. 77–91,, doi: 10.3166/TS.34.77-91.

[50] S. D. Mehta and R. Sebro, "Random forest classifiers aid in the detection of incidental osteoblastic osseous metastases in DEXA studies," *Int. J. Comput. Assist. Radiol. Surg*, vol. 14, no. 5, pp. 903–909,, doi: 10.1007/s11548-019-01933-1.

[51] S. K. Singh and A. Chaturvedi, "Leveraging deep feature learning for wearable sensors based handwritten character recognition," *Biomed. Signal Process. Control*, vol. 80, p. 104198, doi: 10.1016/j.bspc.2022.104198.

[52] R. C. H. Chang, C. Y. Wang, Y. H. Li, and C. Chiu, "Design of Low-Complexity Convolutional Neural Network Accelerator for Finger Vein Identification System," *Sensors*, vol. 23, no. 4, doi: 10.3390/s23042184.

[53] A. Ahmed, A. S. Imran, A. Manaf, Z. Kastrati, and S. M. Daudpota, "Enhancing wrist abnormality detection with YOLO: Analysis of state-of-the-art single-stage detection models," *Biomed. Signal Process. Control*, vol. 93, no. January, p. 106144, doi: 10.1016/j.bspc.2024.106144.

[54] V. A. Ardeti, "Development of real time ECG monitoring and unsupervised learning classification framework for cardiovascular diagnosis," *Biomed. Signal Process. Control*, vol. 88, p. 105553, doi: 10.1016/j.bspc.2023.105553.

[55] A. S. Albahri *et al.*, "A trustworthy and explainable framework for benchmarking hybrid deep learning models based on chest X-ray analysis in CAD systems," *Int. J. Inf. Technol. Decis. Mak.*, pp. 1–54, 2024.

[56] S. Guinebert, E. Petit, V. Bousson, S. Bodard, N. Amoretti, and B. Kastler, "Automatic semantic segmentation and detection of vertebras and intervertebral discs by neural networks," *Comput. Methods Programs Biomed. Updat.*, vol. 2, p. 100055, 2022, doi: https://doi.org/10.1016/j.cmpbup.2022.100055.