

MACHINE LEARNING

Enhanced Grey Wolf Optimization-Based Support Vector Machine for Multimodal Biometric Border Security System

Omotayo Job Ojo¹, Abigail Bola Adetunji², Oluwaseun Modupe Alade¹, Victoria Oluwaseyi Adedayo-Ajayi¹, Yetomiwa Sinat Jeremiah²

¹Cybersecurity Department, Ladoke Akintola University of Technology, Ogbomosho, Nigeria

²Computer Science Department, Faculty of Computing and Informatics, Ladoke Akintola University of Technology, Ogbomosho, Nigeria

Published October 2026

Abstract

Accurate and efficient identity verification is essential for border security. Unimodal biometric systems can be affected by sensor noise, non-universality, inter-class similarities, intra-class variations, and spoof attacks. This paper presents the Enhanced Grey Wolf Optimization-based Support Vector Machine (EGWO-SVM) developed in the study. Support Vector Machine (SVM) penalty parameter C and kernel parameter γ were optimized with the Enhanced Grey Wolf optimizer (EGWO), and the model was trained using face, iris, and fingerprint data from 300 subjects. EGWO represented candidate feature subsets as binary vectors and used a fitness function combining classification error and feature reduction, with $\alpha=0.9$ and $\beta=0.1$. An RBF-kernel SVM was then optimized using k-fold cross-validation. At the 0.51 threshold, the multimodal EGWO-SVM achieved FAR of 0.67%, FRR of 2.67%, F1-score of 98.32%, recognition accuracy of 98.33%, and computational time of 121.31 s, compared with 4.00%, 6.00%, 5.45%, 94.95%, 95.00%, and 147.68 s for SVM. The findings indicate that the Tent-map enhancement improved the optimization-based biometric classification framework.

Keywords: multimodal biometrics; border security; grey wolf optimization (GWO); tent chaotic map; support vector machine

1 Introduction

Due to increased threats and terrorism reported over the last two decades, security technologies have become increasingly important (Yu et al., 2021; Hassan et al., 2023). Despite the many advantages of biometrics, it has limitations. Integrating biometric information systems for border control increases surveillance by collecting and storing personal data, such as fingerprints, as individuals' cross borders, apply for visas, or request asylum (Abomhara et al., 2022). Border security is essential for national safety, legal immigration management, preventing smuggling, and protecting against security threats. Biometric technology establishes identity using physiological or behavioral characteristics. Face, fingerprint, and iris are among the most useful biometric traits for identification, although each has limitations under specific acquisition and operating conditions (Siham et al., 2022; Ali and Shaikh, 2024).

A biometric system typically acquires biometric data, extracts features, compares the resulting representation with stored templates, and decides. Unimodal systems rely on a single biometric trait and can be affected by noisy or poor-quality data, non-universality, and inter-class similarity.

Multimodal systems combine two or more modalities to provide complementary evidence and improve recognition reliability (Ross and Jain, 2004; Sumalatha et al., 2024).

However, using multiple modalities introduces a feature-selection problem. Differences in feature dimensionality, quality, and reliability can cause some modalities to contribute more strongly than others, leading to feature imbalance and potentially reducing generalizability (Jia et al., 2022). The study therefore focused on an enhanced optimization model that selects relevant features and optimizes SVM parameters.

GWO is a population-based metaheuristic inspired by the social hierarchy and cooperative hunting of grey wolves. Although GWO has strong convergence characteristics and few parameters, the study identifies premature convergence and entrapment in local optima as limitations in high-dimensional feature-selection problems (Mirjalili et al., 2014). The proposed EGWO uses a Tent map, which provides a more uniform chaotic distribution and improved ergodicity.

This paper's specific contribution is to formulate and integrate the Tent-chaos-enhanced GWO with SVM for multimodal biometric border security.

2 Related works

Several studies have explored multimodal biometric systems. For instance, Nadheen and Poornima (2013), in a paper titled Feature Level Fusion in Multimodal Biometric Authentication System, examined the performance of ear and iris recognition individually and in combination using score-level fusion. They extracted features using Principal Component Analysis (PCA) to reduce dimensionality while preserving information and demonstrated a 95% success rate with the multimodal approach. Similarly, Channegowda and Prakash (2021) proposed a multimodal biometric system that fuses fingerprint and signature biometric traits at multiple levels, using a deep learning model for classification. They conducted experiments on the SDUMLA-HMT and MCYT datasets. The study reported a 6-9% improvement in classification accuracy compared to unimodal systems. The results may lack generality because the datasets used are not diverse. Latha et al. (2021) also developed a feature selection algorithm based on Grey Wolf Optimization with Random Differential Grouping, aiming to improve classification efficiency in machine learning and address the challenges of big data classification. The algorithm was tested on a large, high-dimensional dataset and achieved a 12% improvement in classification efficiency over traditional selection techniques. The algorithm sometimes misinterprets features as outputs, introducing potential bias into the model. Ahmed et al. (2023) developed a hybrid Support Vector Machine with Grey Wolf Optimization model for anomaly detection in solar power plants. GWO optimized SVM hyperparameters, and the system was tested using physical, regression, and classification models. The hybrid model improved detection accuracy by 11% over conventional SVM models. GWO's effectiveness depends heavily on hyperparameter configuration, which can lead to inconsistencies.

3 Research method

The study implemented a multimodal border security system that integrates face, fingerprint, and iris biometrics, using the Enhanced Grey Wolf Optimization Support Vector Machine (EGWO-SVM) algorithm in MATLAB 2023a. The system development proceeded through five stages: data acquisition, pre-processing, feature extraction, fusion, and classification. Figure 1 illustrates the EGWO-SVM border security system framework, detailing its design and development stages.

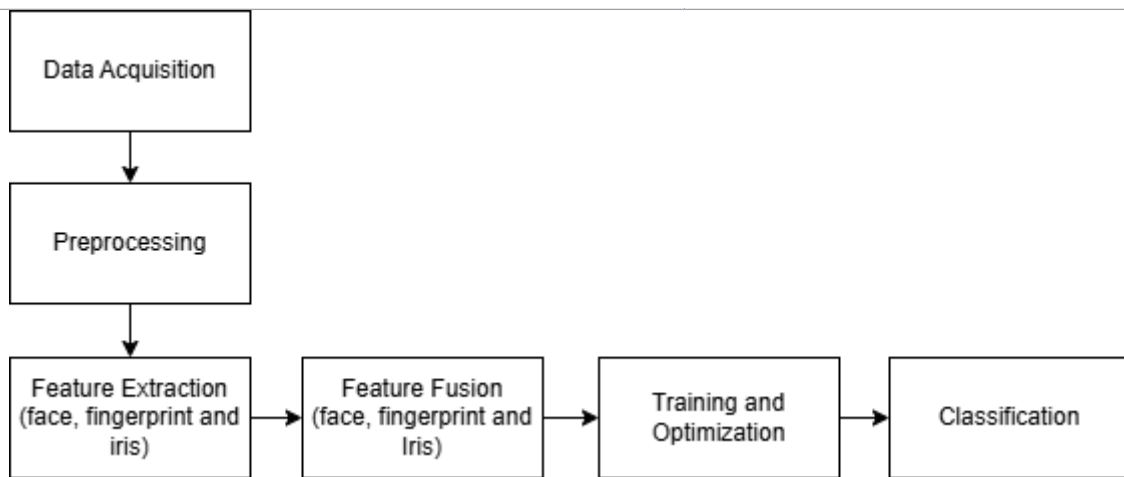


Figure 1. Framework for the EGWO-SVM biometric border security system.

3.1 Data acquisition

The research used face, fingerprint, and iris images collected from students at Ladoke Akintola University of Technology, Ogbomoso. The experimental dataset contained images from 300 subjects and used a predefined training/testing split. The images were acquired under controlled conditions representative of biometric research. Face images were JPEGs with variable original resolution, normalized to 128×128 pixels in RGB before grayscale conversion, with frontal pose, neutral expression, and controlled indoor illumination. Fingerprint images were JPEG grayscale images normalized to 128×128 pixels, acquired with an optical fingerprint scanner from the left index finger. Iris images were JPEG grayscale images acquired under near-infrared illumination, with frontal gaze and normalized iris regions.

3.2 Pre-processing and feature representation

Face preprocessing comprised grayscale conversion, cropping, and histogram equalization. Iris preprocessing involved image enhancement, Hough-transform-based segmentation, and normalization using Daugman's rubber sheet model. Fingerprint preprocessing involved segmentation and orientation-field estimation. The extracted modality features were normalized and fused at the feature level using a serial rule. Feature-level fusion was selected because the source document indicates that feature vectors contain more information than matching scores or decisions.

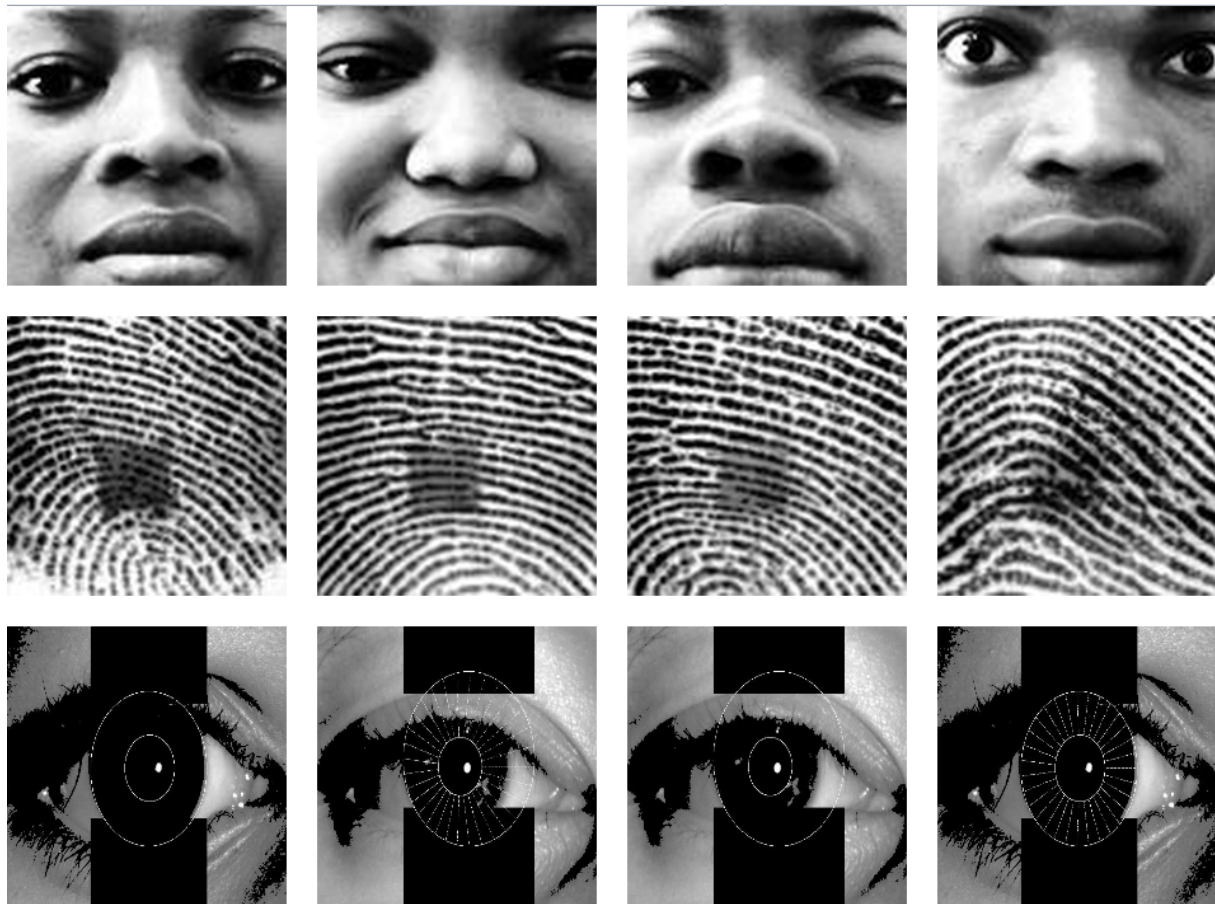


Figure 2. Samples of pre-processed images using histogram equalization: face (top row), fingerprint (middle row) and iris (bottom row).

3.3 Feature extraction

The Local Binary Patterns (LBP) technique was used to extract significant features from the preprocessed images. The LBP operation depends on the eight neighbors of the current pixel, with the center pixel serving as a threshold for its neighbors. The final code for the center pixel was then generated by combining the binary codes of its eight neighbors. The gray values of the neighbors were computed using bilinear interpolation, and the neighbors' values were then compared with the center.

3.4 Feature fusion

Merging features from face, fingerprint, and iris images to create a single feature set. The weighted average fused the features extracted from the face, ear, and iris images, as shown in Equation (1).

$$\frac{\sum_{i=1}^n w_i - x_i}{\sum_{i=1}^n w_i} \quad (1)$$

Where:

n = the number of biometric modalities.

w_i = the weight assigned to the i -th modality.

x_i = is the score or output of the i-th modality.

$\sum_{i=1}^n w_i$ = weight sum, normalized to 1.

The weighted average was computed in the following steps:

3.5 Formulation of the enhanced grey wolf optimization

GWO is inspired by the social structure and hunting behavior of grey wolves (Mirjalili et al., 2014) and is an effective optimization technique widely used to solve complex problems because of its efficiency and balance between exploration and exploitation. Its structure enables rapid convergence to high-quality solutions with lower computational time. However, GWO has limitations, such as slow convergence and getting trapped in local optima (Shaikh et al., 2021). To address these issues, this study introduces EGWO, which focuses on balancing exploration and exploitation, key components of optimization. GWO mimics a social hierarchy and the hunting behavior of grey wolves. α , β , and δ denote the optimal solutions and guide the other members of the group to circle the prey (the optimal solution). For example, the wolves' movements around the leaders help them locate food. EGWO enhances GWO by using tent chaotic maps to modify exploration and convergence.

3.6 Formulation of the enhanced grey wolf optimization–support vector machine

In this research, the SVM classification algorithm, which can handle high-dimensional datasets, was optimized using the formulated EGWO. Radial Basis Function (RBF) kernel will be used as the appropriate kernel function for the following reasons: it has fewer controllable parameters than the polynomial kernel, maps samples into a higher dimension, and has fewer numerical difficulties. For the SVM with an RBF kernel, there are two parameters to optimize (C and gamma). The goal is to identify the best (C and γ), where C is a regularization parameter that controls the flexibility of the hyperplane, while γ is the kernel parameter that controls the correlation among support vectors. Selecting an improper value of γ may cause overfitting.

Algorithm 1. Pseudocode of the formulated enhanced grey wolf optimization–support vector machine (EGWO-SVM)

```

Input: training set  $D_{train}$ , validation set  $D_{val}$ , bounds  $[C_{min}, C_{max}]$ ,  $[Y_{min}, Y_{max}]$ , tent
map control parameter  $\mu$ 
Initialize Generation counter  $t=0$ ; randomly initialize population  $X_i$  ( $i=1 \dots, n$ ),
where  $X_i = (C_i, \gamma_i)$  is a candidate SVM hyperparameter pairs
Initialize the value of the chaotic map  $x_0$  randomly
Initialize parameters  $a^+$ ,  $A^+$ , and  $C^+$ 
for each wolf  $X_i$ 
    Train an SVM using hyperparameters  $X_i$  on  $D_{train}$ 
    Evaluate on  $D_{val}$ , compute fitness  $f(X_i)$ 
end for
Set  $X_\alpha, X_\beta, X_\delta$  = best, second-best, third-best wolves
while ( $t < \text{Max\_iterations}$ )
    Sort The population of the grey wolves by fitness  $f(X_i)$ 
    Update the chaotic number using the chaotic map equation
    for each search agent  $i$ 
        Coefficients  $A=2a \cdot C_{t+1}-a$ ,  $C=2 \cdot C_{t+1}$ 
         $D_\alpha, D_\beta, D_\delta$  using  $A, C$  relative to  $X_\alpha, X_\beta, X_\delta$ 
        Update Position of  $X_i(t+1)$ 
         $X_i(t+1)$  within  $[[C_{min}, C_{max}] [Y_{min}, Y_{max}],]$ 
    end for

```

```

Update  $\alpha$  (linearly decreasing  $2 \rightarrow 0$  over iterations)
for Each wolf  $X_i$ 
    Train SVM with updated  $X_i(t+1)$  on  $D_{train}$ 
    Evaluate Fitness  $f(X_i)$  on  $D_{val}$ 
end for
Update  $X_\alpha, X_\beta, X_\delta$  from new fitness values
Replace worst-fit wolf with best-fit wolf
 $t=t+1$ 
end while
Return  $X_\alpha$  (optimal =  $C, \gamma$ )

```

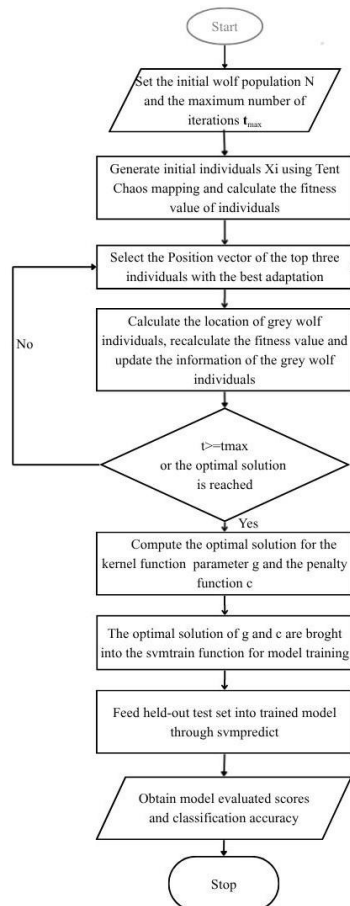


Figure 3. Flowchart of the EGWO-SVM algorithm.

3.7 Implementation

All experiments in this study were conducted in the MATLAB 2023a environment and run on a Dell 7250 with an Intel Core i5 vPro, a Windows 11 Professional 64-bit operating system, a Central Processing Unit (CPU) running at 2.4 GHz, 2.4 GHz, 16GB of Random Access Memory (RAM), and a 1 TB hard disk drive.

3.8 Evaluation measures

The performance of the developed model was evaluated by calculating its FAR, FRR, ERR, F1-score, recognition accuracy, and computational time. The evaluation was based on performance metrics derived from confusion metrics. It contains True Positive (TP), False Positive FP, False Negative (FN), and True Negative (TN). The performance of the system was measured as follows:

$$FAR = \frac{FP}{FP + TN} \times 100 \quad (2)$$

$$FRR = \frac{FN}{FN + TP} \times 100 \quad (3)$$

$$ERR = \frac{FAR(\eta) + FRR(\eta)}{2} \quad (4)$$

$$F1 = 2 \times \frac{(\text{Precision} \times \text{Recall})}{(\text{Precision} + \text{Recall})} \quad (5)$$

$$RA = \frac{TP + TN}{TP + TN + FN + FP} \times 100 \quad (6)$$

Computational time (CT): The wall-clock time required for optimization. This measures the algorithm's practical efficiency.

Where FP denotes the number of unauthorized individuals incorrectly accepted by the system. TN denotes the number of unauthorized individuals correctly rejected by the system. FN indicates the number of legitimate travelers who are valid but are incorrectly rejected by the system. TP indicates the number of legitimate travelers who are correctly accepted by the system.

4 Results and discussion

This research developed a face-fingerprint-iris-based border security system using the Enhanced Grey Wolf Optimization Support Vector Machine (EGWO-SVM) algorithm as a classifier. The system performance was validated using False Acceptance Rate (FAR), False Rejection Rate (FRR), Accuracy, F1-Score (all in percentages), and Recognition Time (Time) in seconds across all thresholds. The metrics were based on confusion matrices, which provide the True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) values the system achieved against the actual outcomes.

The trained model was evaluated using the face, fingerprint, and iris traits. The results were evaluated using a threshold value, a decision-boundary parameter that determines classifier behavior and ranges between 0 and 1. Thresholds between 0 and 1 were tested. Experimental results showed that the classifier produced consistent results in the ranges 0-0.3, 0.31-0.4, 0.41-0.5, and 0.51-0.99. Therefore, thresholds of 0.10, 0.31, 0.41, and 0.51 were selected.

The classification model's performance metrics across four threshold levels (0.1, 0.31, 0.41 and 0.51) show a consistent trade-off between FAR and FRR, with the highest accuracy of 95.00% achieved at a threshold of 0.51, where the model correctly identified 141 true positives and 144 true negatives, while minimizing false positives to 6 and false negatives to 9, all computed in 147.68 seconds.

From Table 1, the SVM technique correctly classified 141 multimodal face, fingerprint, and iris datasets as genuine, while it incorrectly identified 9 as impostors. Additionally, SVM correctly identified 144 imposter multimodal face, fingerprint, and iris datasets as impostors, but incorrectly classified 6 as genuine. Moreover, EGWO-SVM correctly identified 146 genuine multimodal face, fingerprint, and iris datasets, but incorrectly identified 4 as impostors. Additionally, the technique correctly identified 149 imposter multimodal face, fingerprint, and iris datasets as impostors, while it incorrectly classified 1 as genuine. Table 1 shows that at a threshold of 0.80, the SVM technique achieved a FAR of 4.00%, an FRR of 6.00%, an F1-Score of 94.95%, and an accuracy of 95.00%, with a computational time of 147.68 seconds. From Table 2, EGWO-SVM achieved an FAR of 0.67%, an FRR of 2.67%, an F1-Score of 93.32%, and an accuracy of 98.33%, with a computational time of 121.31

seconds. The results show that EGWO-SVM outperforms standard SVM for multimodal face, fingerprint, and iris biometrics. The EGWO-SVM technique reduced false negatives and false positives compared with GWO-SVM and standard SVM for multimodal face, fingerprint, and iris biometrics.

The EGWO-SVM (Enhanced Grey Wolf Optimization with Support Vector Machine) technique achieved the highest accuracy of 98.33% for multimodal face, fingerprint, and iris recognition among the three techniques evaluated. This implies that EGWO-SVM performs best at correctly identifying genuine multimodal face, fingerprint, and iris samples and rejecting impostor multimodal face, fingerprint, and iris samples. The EGWO-SVM technique exhibited the lowest FAR (0.67%) and FRR (2.67%). A lower FAR indicates that the technique better rejects impostor multimodal face, fingerprint, and iris samples, while a lower FRR implies that the technique better accepts genuine multimodal face, fingerprint, and iris samples. The low FAR and FRR values suggest that the EGWO-SVM technique is highly effective at minimizing both error types across the three techniques. This implies that EGWO-SVM is more computationally efficient and can perform multimodal face, fingerprint, and iris recognition faster than the other two techniques. This suggests that the multimodal system is more effective at minimizing both error types (false acceptance and false rejection) than unimodal and bimodal systems.

Table 1. Results for standard SVM.

Threshold	TP	FN	FP	TN	FAR(%)	FRR(%)	F1- Score (%)	ACC(%)	Time(sec)
0.10	144	6	13	137	8.67	4.00	93.81	93.67	147.80
0.31	143	7	11	139	7.33	4.67	94.08	94.00	146.63
0.41	142	8	9	141	6.00	5.33	94.35	94.33	145.45
0.51	141	9	6	144	4.00	6.00	94.95	95.00	147.68

Table 2. Results for EGWO-SVM.

Threshold	TP	FN	FP	TN	FAR(%)	FRR(%)	F1- Score (%)	ACC(%)	Time(sec)
0.10	149	1	9	141	6.00	0.67	96.75	96.67	122.30
0.31	148	2	6	144	4.00	1.33	97.37	97.33	121.22
0.41	147	3	3	147	2.00	2.00	98.00	98.00	122.41
0.51	146	4	1	149	0.67	2.67	98.32	98.33	121.31

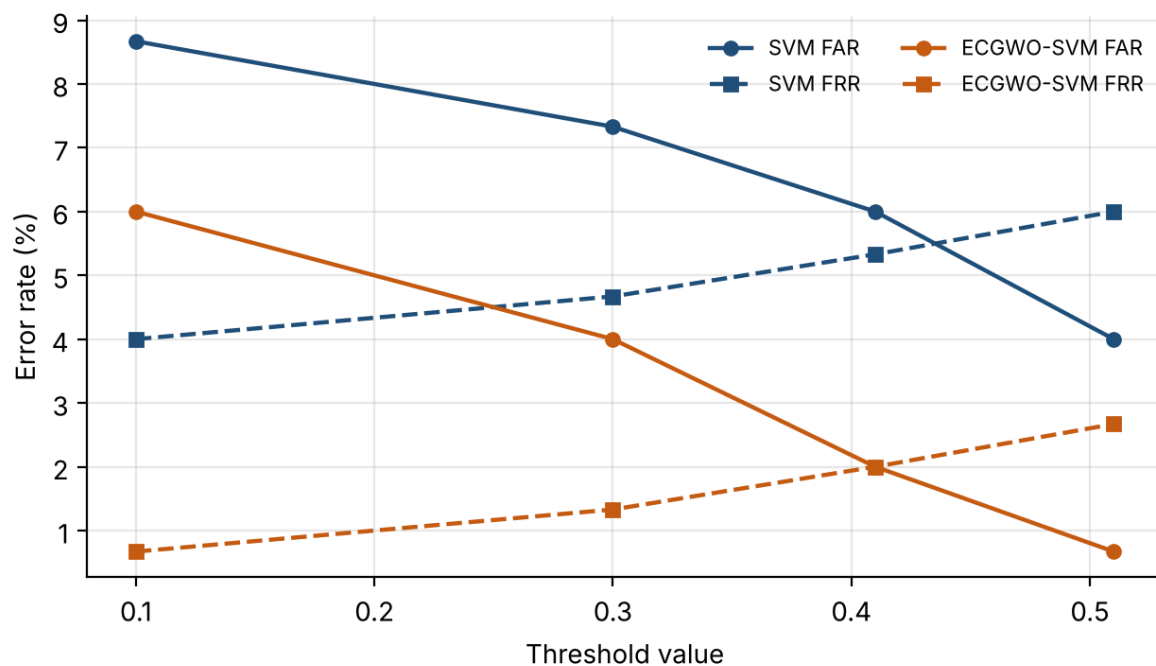


Figure 4. Equal error rate (EER) for multimodal face, fingerprint and iris biometrics.

Figure 4 depicts the EER values for the multimodal face, fingerprint, and iris biometrics: 5.45% for the SVM technique and 2.07% for the EGWO-SVM technique. The results indicated that the optimization technique (EGWO-SVM) outperformed the baseline SVM across all biometric modalities (face, fingerprint, iris, bimodal face-fingerprint, bimodal face-iris, bimodal fingerprint-iris, and multimodal face-fingerprint-iris). These results suggest that optimizing the SVM model's hyperparameters using EGWO algorithms can significantly improve the biometric border recognition system's performance.

5 Conclusion and recommendations

This paper presents the EGWO-SVM framework developed for multimodal biometric border security. The method integrates a Tent chaotic map with GWO used to optimize the SVM parameters C and γ . The method fused face, fingerprint, and iris features at the feature level and classified them with an RBF-kernel SVM. Based strictly on the reported experimental results, the multimodal EGWO-SVM configuration achieved 98.33% recognition accuracy, 0.67% FAR, 2.67% FRR, 2.07% EER, 98.32% F1-score, and 121.31 s computational time at the 0.51 threshold.

The study develops a machine-learning-based multimodal biometric border security system that combines face, fingerprint, and iris features. Future recommendations include integrating deep learning for feature extraction and applying the developed techniques to high-dimensional problems such as tracking and detecting moving objects in video datasets.

References

- [1] Abomhara M, Yayilgan SY, Shalaginova M (2022). Border control and use of biometrics: reasons why the right to privacy cannot be absolute. *1-11*.
- [2] Ahmed QI, Attar H, Amer A, Deif MA, Solyman AAA (2023). Development of a hybrid support vector machine with grey wolf optimization algorithm for detection of the solar power plants anomalies. *Systems*, 1-20. <https://doi.org/10.3390/systems11050237>

-
- [3] Ali H, Shaikh S (2024). Comprehensive review on different types of biometrics and the impact of pandemic on biometric security. *International Journal of Information Systems and Computer Technologies*, 3(2), 70–79. <https://doi.org/10.58325/ijisct.003.02.0074>
 - [4] Channegowda AB, Prakash HN (2021). Multimodal biometrics of fingerprint and signature recognition using multi-level feature fusion and deep learning techniques. *Indonesian Journal of Electrical Engineering and Computer Science*, 22(1), 187–195. <https://doi.org/10.11591/ijeecs.v22.i1.pp187-195>
 - [5] Hassan B, Sherazi HHR, Ali M, Bashir AK (2023). A multi-channel soft biometrics framework for seamless border crossings. <https://doi.org/10.1186/s13634-023-01026-x>
 - [6] Jia W, Sun M, Lian J, Hou S (2022). Feature dimensionality reduction: a review. *Complex & Intelligent Systems*, 2663–2693.
 - [7] Latha RS, Balaji BS, Bacanin N, Strumberger I, Zivkovic M, Kabiljo M (2021). Feature selection using grey wolf optimization with random differential grouping. *Computer Systems Science & Engineering*. <https://doi.org/10.32604/csse.2022.020487>
 - [8] Mirjalili S, Mirjalili SM, Lewis A (2014). Grey wolf optimizer. *Advances in Engineering Software*, 46–61.
 - [9] Nadheen MF, Poornima S (2013). Feature level fusion in multimodal biometric authentication system. *International Journal of Computer Applications*, 69(18), 36–40.
 - [10] Ross A (2010). Iris recognition: the path forward. 30–35.
 - [11] Shaikh MS, Hua C, Jatoi MA, Ansari MM, Qader AA (2021). Application of grey wolf optimisation algorithm in parameter calculation of overhead transmission line system. *IET Science, Measurement & Technology*, 15(2), 218–231.
 - [12] Sumalatha U, Krishna Prakasha K, Srikanth (2024). A comprehensive review of unimodal and multimodal fingerprint biometric authentication systems: fusion, attacks, and template protection. *IEEE Access*, 1–40. <https://doi.org/10.1109/ACCESS.2024.3395417>
 - [13] Yu JY, Kim Y, Kim YG (2021). Intelligent video data security: a survey and open challenges. *IEEE Access*, 26948–26967.