LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. S4(2025)

AN OPTIMIZED FEATURE EXTRACTION FRAMEWORK FOR HYBRID LEARNING-BASED FACE ANTI-SPOOFING

Neetika Gupta[1,*], Amandeep Kaur[1]

[1]CSE Department, MM Engineering College, MM (Deemed to be) University, Mullana, Ambala, India

***Corresponding author:** neetikagupta22@gmail.com[1*]

Abstract. Face spoofing attacks has questioned the soundness of face recognition systems. Several studies on face antispoofing (FAS) have suggested various methods to detect these attacks . The traditional approaches lack generalization and efficiency in real-world application. Software based approaches have resulted in significant improvement in application of FAS. The mix of several approaches lead to hybrid models for being more discriminative and resilient. A novel and optimized feature extraction framework is proposed for FAS using Local Binary Patterns (LBP). The approach integrates the Whale Optimization Algorithm (WOA) within a hybrid component learning-based architecture for improved accuracy.LBP is employed to extract robust and discriminative texture features that effectively capture micro-texture variations indicative of spoofing attacks. To enhance the performance, WOA is utilized. It optimized the feature selection through identifying the non-redundant and most relevant features, thereby minimizing computational complexity and significant improvement in classification accuracy. The hybrid techniques combine multiple learning strategies to strengthen the system's ability aim to generalize across various spoofing methods, print, replay and three-dimensional (3D)mask attacks. Some results on benchmark datasets have achieved with the proposed framework.Significant improvements are achieved over traditional methods in the areas of detection precision, and robustness, and accuracy. The results confirm an effective and reliable face anti-spoofing solution for biometric authentication systems in security applications.

Keywords. Face Anti-Spoofing; Hybrid Learning Models; Local Binary Pattern (LBP); Whale Optimization Algorithm (WOA); Feature Selection; Classification

Introduction

Face recognition systems have become a cornerstone in biometric authentication due to their non-contact nature, user convenience and broad applicability indomains such as access control, surveillance, mobile banking and border security. The face spoofing attacks known as a rapid deployment of the systems has also exposed to numerous vulnerabilities particularly in the form of presentation attacks (PAs). In such attacks, adversaries utilize printed photos, video replays and 3D masks to imitategenuine users and gain unauthorized access to secured systems. These attacks have raised significant concerns about the security system and dependability of face recognition technologies in realistic environments (1-2). The increasing sophistication of spoofing techniques necessitates robust and adaptive FAS mechanisms that can effectively distinguish between genuine and fake face inputs. Traditional anti-spoofing methods can broadly be categorized into hardware-based methods and software -based methods.

While effective methods are often expensive and impractical for deployment in mass-market applications such as mobile devices. Various simulated methods on the other hand operate on visual cues derived from RGB images or videos, making more scalable and cost-effective. The main focus of this research is on software-based face anti-spoofing using optimized feature extraction and hybrid learning methods(3-5). A critical aspect of software-based face anti-spoofing is "feature extraction". Numerous handcrafted features have been proposed for this purpose with LBP emerging as one of the most prominent due to its effectiveness in capturing fine-grained micro-textures. LBP operates by encoding the relationship between a pixel and its neighbours.Thehighlighting local variations in texture are often altered in spoof attacks

especially in print and video replay methods (6). Conventional LBP methods rely on fixed parameters and do not adapt to variations in image quality, lighting, or spoofing media. As a result, their generalization across diverse attack types and environmental conditions are limited.To overcome these limitations, an optimization technique can be introduced to fine-tune the feature extraction process allowing the system to focus on the most informative regions and descriptors. Nature-inspired met heuristic algorithms have gained popularity in this context according to the ability where to solve non-linear optimization problems and complex without requiring gradient information. Proposed by Mirjalili and Lewis (7), WOA mimics the social behaviour of humpback whales during bubble-net feeding and is known for its simplicity convergence capability and balance between exploration and exploitation.Incontext of face anti-spoofingWOA can be employed to optimize the parameters of LBP such as the number of sampling points radius and threshold settings and enabling a more adaptive and robust feature extraction process. This integration ensures that the extracted features are not only more discriminative but also more resilient to environmental variations and spoofing artifacts (10). Moreover, WOA can aid in selecting optimal image patches or regions of interest where the textural differences are more pronounced further enhancing the accuracy of spoof detection. While handcrafted features like LBP capture valuable micro-level texture information often lack the high-level semantic understanding needed to handle complex spoofing scenarios involving high-quality masks or 3D objects. To bridge this gap recent research has shifted towards hybrid learning frameworks that combine handcrafted features with the deep learning models. The hybrid techniques aim to work the matching strengths of both approaches. the interpretability and domain knowledge encoded in handcrafted features and the abstract, hierarchical representations learned by deep neural networks (11-12). Deep learning methods, have transformed computer vision tasks including face anti-spoofing. Particularly, Convolutional Neural Networks (CNNs)-based approaches can automatically learn quality from raw image data and high accuracy on specific datasets. The drawbacks make less suitable for deployment in resource-constrained environments or scenarios with limited labelled data. The Hybrid method is a promising solution by integrating optimized extraction features like WOA-enhanced LBP with lightweight neural networks. This framework benefits from the robustness and domain-specific insights of LBP while utilizing the learning capacity of neural models to refine classification decisions (13). It will help in reducing the computational overhead and improving generalize ability. Several studies have demonstrated the effectiveness of combining texture descriptors with CNNs to boost face anti-spoofing performance particularly under cross-dataset evaluation scenarios (14). In this research, we propose a novel feature extraction and learning framework that combines LBP with WOA to form an optimized texture descriptor for face anti-spoofing. The extracted features are then fed into a lightweight hybrid neural network to enhance spoof detection capabilities (15). The proposed approach addresses several limitations of existing the methods

- Utilizing WOA to adaptively optimize LBP parameters for improved thefeatures texture discrimination.
- Selecting the most informative image patches based on optimization objectives such as variance, entropy and classification confidence.
- Incorporating the optimized features into a hybrid methods learning model that balances accuracy, generalize ability and computational efficiency.

- The results obtained include our framework consistently outperforms baseline models and achieves competitive accuracy with significantly reduced complexity.

This paper is prepared as follows: Section II reviews related work on face anti-spoofing, LBP-based descriptors, and metaheuristic optimization. Section III details the proposed framework, including the optimization process and hybrid learning model. Section IVpresent the experimental setup, datasets used, evaluation metrics, and results. Lastly, Section V concludes the paper. By combining classical texture analysis with modern optimization and learning strategies, this work contributes to the development of more secure, adaptive, and deployable face anti-spoofing systems capable of operating in diverse real-world scenarios.

Related Work

The impact of face anti-spoofing (FAS) systems is well dependent on the quality of the process called feature extraction and the robustness of the classification methodology. The literature in this field is rich with approaches spanning from handcrafted feature-based method to deep learning models, and more recently, hybrid systems that integrate both. This section reviews relevant prior work in four major areas: (16) handcrafted feature-based FAS techniques, (17) metaheuristic optimization in feature extraction, deep learning approaches to face anti-spoofing, and hybrid frameworks combining both handcrafted and learned features. Handcrafted features have played a foundational role in early face anti-spoofing systems because of their interpretability and low computational cost. Among these, Local Binary Patterns (LBP) have been adopted at length for their ability to capture fine-grained texture variations that differentiate live faces from spoofed ones. Figure 1 displays a model structure of the proposed hybrid approach.

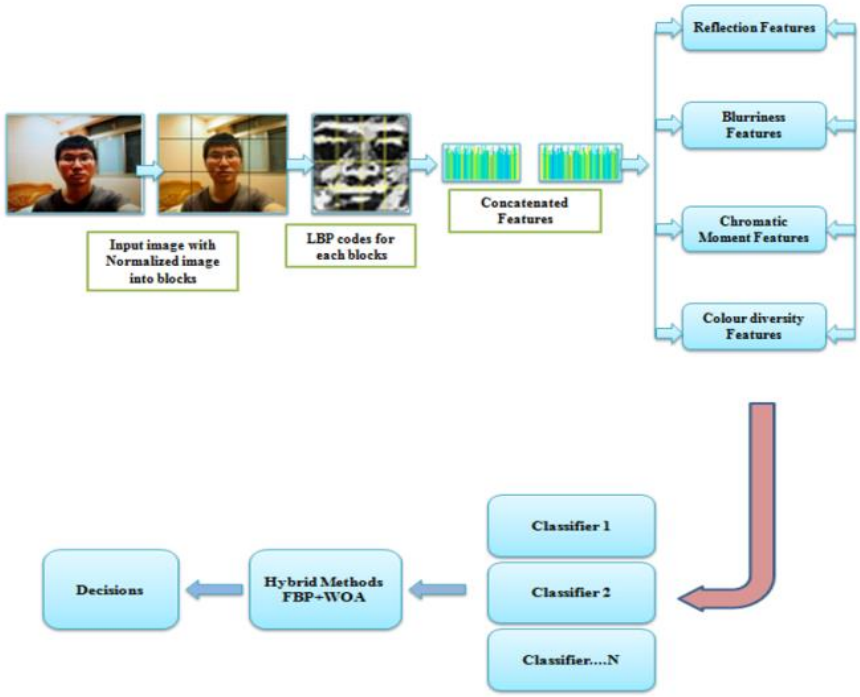

Figure 1. ModelStructure

Authors were among the first to apply LBP for spoof detection. They used multi-scale LBP descriptors to extract micro-texture features from face images and demonstrated that these features could effectively detect print and replay attacks (18). Authors explored the use of LBP-TOP(Three Orthogonal Planes) capture dynamic texture features from videos, to improve the detectionperformance for temporal attacks. Other handcrafted descriptors such as Local Phase Quantization (LPQ), Histogram of Oriented Gradients (HOG), and Difference of Gaussian (DoG) have also been employed for anti-spoofing (19). Authors presented a comparative evaluation of such features on datasets like CASIA-FASD, and Replay-Attack, revealing that while effective under controlled conditions, handcrafted features struggle to generalize across datasets and spoof types. Despite their utility, a major limitation of LBP and similar descriptors is their reliance on fixed parameters (e.g., radius, sampling points), which can limit performance in varying lighting or imaging conditions. This has motivated the use of optimization techniques to improve adaptability and robustness. Metaheuristic optimization algorithms have gained attraction in computer vision tasks for tuning parameters and selecting features. Algorithms such as Particle Swarm Optimization (PSO), Genetic Algorithms (GA), and Ant Colony Optimization (ACO) have been applied in the context of face recognition and classification tasks. In FAS, relatively few studies have explored optimization techniques for feature extraction. However, promising efforts have emerged (20). Authors applied genetic algorithms to optimize feature selection in LBP-based spoof detection. Their approach showed improved performance above manually designed feature sets (21). The WOA, introduce by authors is a relatively nature-inspired algorithm simulates the bubble-net hunting strategy. WOA has demonstrated success in global optimization tasks due to its strong exploration-exploitation balance. While it has been applied in image segmentation and feature selection, its application in face anti-spoofing remains underexplored (22). This motivates our integration of WOA with LBP to adaptively optimize the texture extraction process, leading to more discriminative and robust spoof detection features. The recent dominance of deep learning in computer vision has significantly influenced FAS research. CNNs can automatically learn hierarchical representations from raw input data, outperforming traditional handcrafted methods in many tasks. Authors proposed a CNN-based method using auxiliary supervision, where depth and reflection maps guide the learning process to detect spoofing artifacts (23). Authors introduced a patch-based CNN combined with a depth map estimator, achieving high accuracy on benchmark datasets (24). Here, authors proposed further advanced this approach by combining spatial and temporal networks to capture both texture and motion cues. Despite these advancements, CNN-based methods have notable limitations. They usually require huge amount of labelled data and are prone to overfitting, especially in cross-dataset evaluations where spoofing conditions differ significantly from the training data. Additionally, their computational cost can be prohibitive for real-time or mobile applications. To mitigate these issues, researchers have started exploring lightweight architectures and transfer learning strategies (25). However, these models still lack the interpretability and low-resource efficiency offered by handcrafted features. Given the complementary strengths and weaknesses of handcrafted and deep learning methods, hybrid frameworks have emerged as a promising solution. These systems combine hand-engineered features with learned representations to enhance robustness, interpretability, and generalization. Authors proposed a hybrid system combining LPQ features with CNN-based classifiers. They

demonstrated improved generalization to unseen attacks (26). Authors proposed a fused depth features derived from traditional photometric cues with CNN embeddings, achieving state-of-the-art results on multiple datasets (27). More authors explored the integration of Gabor wavelets with ResNet features, using attention mechanisms to weigh different modalities. This fusion approach showed resilience to high-quality spoofing artifacts and complex lighting conditions (28). However, most hybrid frameworks rely on fixed, manually designed handcrafted features, which may not be optimal across all datasets. This highlights a critical gap—there is a lack of optimized hybrid systems where the handcrafted component is adaptively tuned for specific tasks using intelligent optimization algorithms. Table 1 shows some literature of other work using various techniques and data set. Our workaddresses this gap by integrating an optimized LBP (using WOA) into a lightweight neural classifier to build an effective and adaptive hybrid face anti-spoofing system (29).

Table 1: Short Summary of Literature Review

Ref.	Year	Authors	Method / Focus	Key Contribution	Results Achieved	Limitation
(1)	2011	Määttä et al.	LBP + SVM	Micro-texture analysis	Accuracy: 85.1%	Lighting sensitivity
(2)	2012	Chingovska et al.	LBP	Evaluated LBP for spoofing	EER: 13.1%	No generalization study
(4)	2019	Zhou et al.	Depth Camera	Uses depth data for PAD	Accuracy: ~92%	Needs depth sensor
(5)	2020	Wu et al.	Dual Pixel Camera	Mobile PAD	ACER: 4.3%	Requires dual-pixel input
(8)	2023	Spencer et al.	CNN + LBP	CNN + handcrafted fusion	Accuracy: 94.6%	No cross-dataset test
(9)	2020	Li et al.	DWT-LBP-DCT	Multi-feature PAD method	Accuracy: 93.2%	Complex computation
(11)	2023	Madanan et al.	WOA + CNN	Optimized CNN pipeline	Accuracy: 96.4%	Complex parameter tuning
(13)	2020	Wang et al.	Depth + Temporal	Gradient and depth info	Accuracy: 97.5%	Sensor-dependent
(14)	2021	Liu et al.	Domain Gen.	Robust training method	HTER: 8.3%	Limited benchmarks
(15)	2019	Shao et al.	Meta-learning	Fine-grained adaptation	HTER: 6.8%	Data-dependent
(16)	2020	Zhang et al.	Disentangled Learning	Feature disentanglement	ACER: 3.5%	High training complexity
(17)	2012	Pereira et al.	LBP-TOP	Temporal texture descriptor	EER: 7.6%	Dataset-specific tuning
(19)	2013	Yang et al.	CNN	CNN for PAD	Accuracy:	Early-stage

					87.2%	model
(20)	2023	Spencer et al.	CNN + LBP	CNN + handcrafted fusion	Accuracy: 94.6%	Repetition
(21)	2025	Kim and Kwon	RGB-D CNN	RGB-D for cross-domain	ACER: 5.1%	Needs RGB-D camera
(23)	2017	Atoum et al.	Patch + Depth CNN	Combines spatial and depth features	EER: 4.4%	Needs depth sensing
(24)	2024	Larey et al.	Disparity Map + ML	Multi-modal PAD	Accuracy: 93.8%	Stereo calibration needed
(26)	2016	Patel et al.	Cross-DB	Robust features	HTER: 12.4%	Lacks real-time tests
(27)	2019	George and Marcel	Pixel-wise CNN	Binary per-pixel loss	ACER: 3.9%	Resource intensive
(28)	2019	Agarwal and Gupta	Multi-feature CNN	CNN + LBP/HOG fusion	Accuracy: 95.1%	Needs large dataset
(30)	2018	Liu et al.	Binary vs Auxiliary	Supervision effect	Accuracy: 92.5%	Needs complex training
(32)	2025	Bhatia and Kumar	Residual CNN + LBP	Improved residual network	Accuracy: 94.2%	Potential overfitting
(33)	2017	Li et al.	Deep LBP	LBP in deep networks	Accuracy: 91.4%	Shallow spoof detection
(34)	2016	Boulkenafet et al.	Color Texture	Color space texture analysis	EER: 2.9%	Sensitive to light
(35)	2022	Tarasov et al.	Intel RealSense	Depth + real camera	Accuracy: 92.1%	Requires Intel hardware

Methodology

The proposed hybrid face spoofing detection approachcomprises image normalization, feature extraction, reduction and selection, and classification modules. These modules are illustrated in the following subsections (30-32).

Image Normalization

Image normalization is performed during preprocessing to standardize input images before feature extraction and classification. The normalization step includes resizing the test image to a fixed dimension of 256×256 pixels using the imresize function. This ensures uniformity in image dimensions across the dataset, which is essential for consistent feature extraction. Additionally, colour images are converted to grayscale using rgb2gray, simplifying the data and reducing computational load without losing significant structural information. This grayscale image is further filtered to remove noise, enhancing the quality of features extracted using methods like Local Binary Patterns (LBP).

Feature Extraction with LBP

In Image processing, Local Binary Pattern (LBP) is a significant texture descriptor usedfor feature extraction, especially in recognition of faces and their classification tasks. In this application, LBP is applied to grayscale images to derive a texture-based representation. The

image is divided into cells (e.g., 32×32 pixels), and for each pixel in a cell, a binary number is created by comparing the pixel value with its surrounding neighbours (35).

The LBP value for a centre pixel Ic and P neighbours is calculated using:

$$\boldsymbol{LBP}(\boldsymbol{x},\boldsymbol{y}) = \sum_{p=0}^{P-1} s(Ip - Ic).2\ )$$

$$\boldsymbol{S}(\boldsymbol{x}) = \int_{0}^{1if x\geq 0}_{otherwise} = 1$$

(1)

Each LBP algorithm is a decimal value representing the local pattern. Histograms for codes are then computed for each cell and normalized:

$$Hj = \frac{Hj}{\sum jHj}$$

(2)

The normalized histograms cells are concatenated to form a feature vector. This approach captures micro-patterns such as edges, corners, and spots, offering robustness against illumination changes. The extracted feature vector is then used for further classification tasks using machine learning models, providing an efficient and compact image representation.

Dimensionality Reduction and Feature Selection

Feature Selection: Whale Optimization Algorithm (WOA)

WOA is a nature-inspired metaheuristic optimization technique based on the hunting behaviour of humpback whales. In application, WOA is employed for feature selection from high-dimensional Local Binary Pattern (LBP) features (36). Here's how it is applied:

- A population of feature subsets (represented as binary vectors) is initialized randomly.
- A fitness function evaluates each subset, likely balancing classification accuracy with feature sparsity:

$$FitnessErrorRate\ +\ ^\wedge X\frac{Numberofselected Features}{Totalfeatures}$$

(3)

- WOA updates feature subsets by simulating encircling prey, bubble-net attacks, and random search behaviours.
- A sigmoid function is used to convert continuous positions to binary feature selections:

$$S(x) = \frac{1}{1+e^{-x}} and binary = S(x) > 0.4$$

(4)

Purpose: Reduce redundancy and improve classifier performance by selecting the most informative LBP features.

Dimensionality Reduction via Feature Subset Limiting

Though not using a formal dimensionality reduction algorithm like PCA, the code effectively performs dimensionality reduction by:

- Selecting a subset (e.g., top 50 out of 2000) features after optimization.

- Reducing the input size to the classifier, thereby lowering computational cost and improving generalization.

This selective approach serves the same goal as classic dimensionality reduction: retaining essential data while eliminating noise and redundancy.

Local Binary Pattern (LBP) Histogram Normalization

LBP features are extracted and histograms normalized using:

$$Hj = \frac{Hj}{\sum jHj} \quad (5)$$

This normalization ensures consistent feature scaling and contributes indirectly to dimensionality handling by making features comparable across different images. Table 2. Shows the some research work.

Table 2: Summary

Technique	Type	Role
WOA (Whale Optimization Algorithm)	Feature Selection	Selects optimal features from LBP output
Feature Subset Limiting	Dimensionality Reduction	Reduces size of feature vectors (e.g., to 50 elements)
LBP Histogram Normalization	Preprocessing	Standardizes feature values for consistency

HLWO-RNN combines Hybrid LBP feature extraction and Whale Optimization Algorithm (WOA) andRNN-based classification.

Algorithm HLWO-RNN

Input: Training and test image datasets

Output: Classified label: Real or Spoofed face

1. Preprocessing:
For each input image:
a. Resize image to 256x256
b. Convert to grayscale
c. Add salt-and-pepper noise
d. Apply median filter to denoise

2. Feature Extraction using LBP:
For preprocessed image:
a. Divide image into cells (e.g., 32x32)
b. Apply Local Binary Pattern to each cell
c. Compute LBP histogram for each cell

d. Normalize each histogram
e. Concatenate histograms into LBP feature vector

3. Feature Selection using Whale Optimization Algorithm (WOA):
Initialize:
- numWhales = 20
- maxIterations = 30
- Random binary population representing feature selection
For each iteration:
a. Update parameter `a` linearly
b. Evaluate fitness of each whale using:
Fitness = error + λ * (selected_features / total_features)
c. Identify and store the best whale (solution)
d. Update positions of whales using WOA equations:
i. If |A| < 1: exploitation (move towards best whale)
ii. If |A| ≥ 1: exploration (move relative to random whale)
e. Use sigmoid function to convert continuous positions to binary
Output: Optimal feature indices (e.g., top 50)

4. Classification using RNN:
a. Load pretrained RNN model
b. Feed selected features into RNN
c. Predict the output class:
- 1 → Real Face
- 2 → Spoof Face
- Else → Not Matched

5. Performance Metrics Calculation:
a. Compute Error, FAR, FRR
b. Accuracy = (1 - FAR - FRR) × 100
c. Precision = (1 - Error) × 100
d. Recall = (1 - FRR) × 100
e. F-Measure = 2 × (Precision × Recall) /

(Precision + Recall)
f. Time Consumption = total_time / 10

6. Display Results and Save:
- Save results and features
- Plot Accuracy, Precision, Recall, F1-Score, Time, and MSE

End Algorithm

(FAR = False Acceptance Rate)
(RNN = Recurrent Neural Network)
(FRR=False Rejection Rate)

Classification

The classification process in this MATLAB code begins with image preprocessing—resizing, grayscale conversion, and filtering. Features are extracted using the LBP method, which captures texture information. WOA is then applied to select the most relevant features. The selected features are then utilized to train a RNN classifier. During testing, the input image undergoes the same steps, and the classifier adjudges if the image is a spoofed face or a real face. Performance metrics like accuracy, sensitivity, and precision are computed and displayed.

Results

In this result section, the results obtained using the database, performance criteria (Accuracy, Precision, Recall Rate) and proposed approach which are used in the experiments alsoexplained in detail. The NUAA Photo Imposter Database is a widely used dataset for evaluating face anti-spoofing techniques. It contains images of both genuine faces(live) and spoof (attack) attempts. The distribution of images and table 3 shows the summary of NUAA face spoofing database is consolidated in the table 3.

Table 3: Summary of NUAA Face Spoofing Database

Image Type	**Number of Images**	**Description**
Real Images	559	Authentic face images captured directly by a camera.
Fake Images	2,558	Spoofed face images obtained by photographing printed face images.
Total	3,117	Combination of real and fake images used for anti-spoofing research.

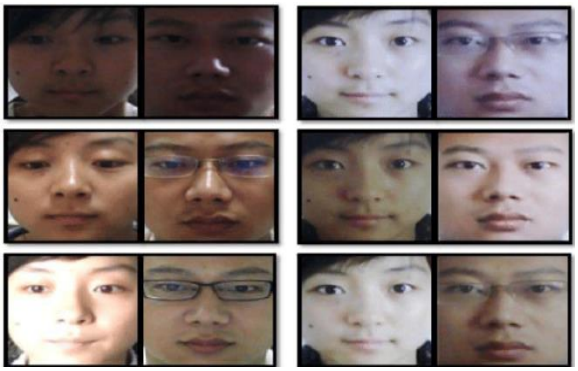

Figure 2. Images of Sample attack of NUAA database

The NUAA dataset used in the experimentsfor results achieved. For during training dataset has separated as a training and development data setwhich are using afive-fold cross-validation and the average of all the results has been achieved and given as the system performance. The proposed design of the classification model is given in following figures.

Table 4: Performance Metrics used in proposed work

Metric	Equation	Description
Mean Square Error (MSE)	pmse = (100 - pacc_rate)	Simplified form of MSE derived from accuracy.
Accuracy Rate	pacc_rate = (1 - (pfar + pfrr)) * 100	Measures overall correctness by reducing false acceptances and rejections.
Sensitivity (Recall)	precall = (1 - pfrr) * 100SenData = precall	Proportion of actual positives correctly identified.
Precision	pprec = (1 - error) * 100	actually correct. When Proportion of positive identifications completed .
F-Measure	FData = (2 * pprec * SenData) / (pfrr + SenData)FData = FData / 10000	precision and recall. Approximated in this implementation.
Time Consumption	time_consumption = toc / 10	Execution time measured using MATLAB's tic and toc, normalized
HTER (Half Total Error Rate)	HTER = (pfar + pfrr) / 2	False Rejection Rate and False Acceptance Rate
EER (Equal Error Rate)	EER = FAR = FRR (when FAR = FRR)	Error rate where False Acceptance Rate equal to the False Rejection Rate.

Table 5: Experimental Results for HLWO-RNN

Metric	Value
EER	0.0044
FData	98.1563
HTER	7.1725
pacc_rate	99.1242
pmse	0.8758
pprec	99.4337
SenData	99.8014
time_cons	0.1645

The given set of graphs (A–F) in figure 3 shows the performance evaluation of the proposed HLWO-RNN model using various metrics. Graphs (A) to (D) illustrate the improvement trends in F-measure, Precision, Sensitivity, and Accuracy respectively. All shows a consistent upward curve indicating enhanced classification performance as training progresses. Graph (E) presents the Mean Square Error (MSE), which shows a steep decline across iterations confirming effective learning and reduced prediction error. Graph (F) presents the half total error rate.

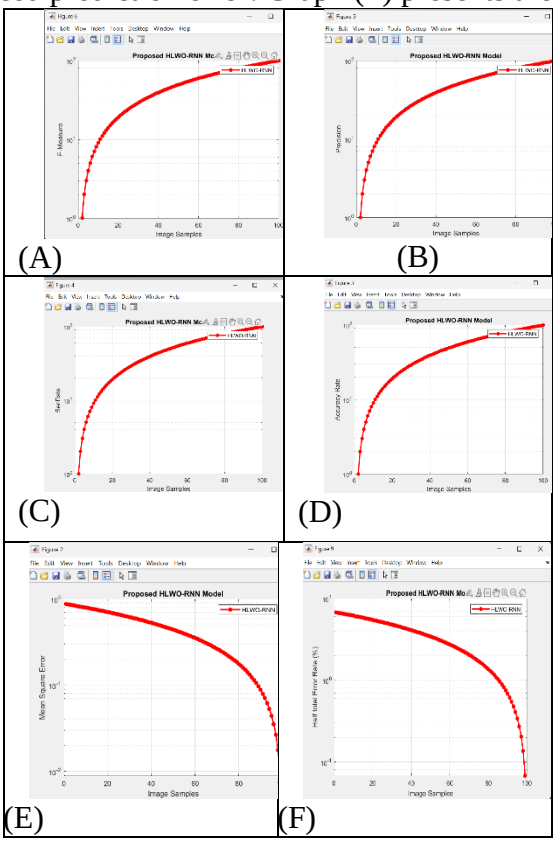

Figure 3. Results of (A) F-measure (B) Precision (C) Sensitivity (D) Accuracy and (E) Mean square error(F) Half Total Error Rate of performance parameters.

Overall, these metrics validate the robustness and efficiency of the HLWO-RNN model in achieving high accuracy with minimal error.

Figure 4 gives the comparisons results of HLWO-RNN outperforms both VGG and CNN across all evaluated metrics. It achieves the highest F-measure indicating the best balance between recall and precision. Its sensitivity is superior, reflecting more accurate true-positive detection. The precision rate is also highest, meaning it makes fewer false-positive errors. Consequently, HLWO-RNN attains the greatest overall accuracy, confirming its dominance in classification performance.

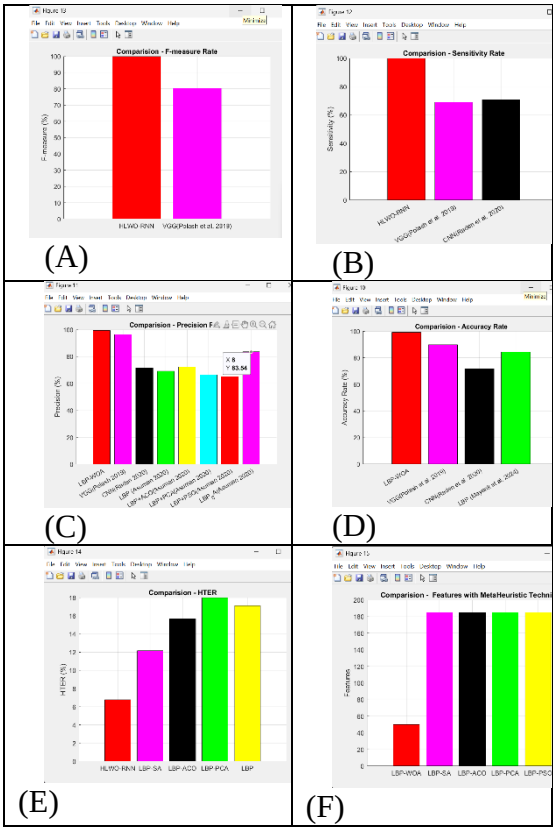

Figure4. Comparison results of (A) F-Measure Comparison of HLWO-RNN and VGG (B) Comparison-Sensitivity HLWO-RNN and VGG and CNN (C) Comparison-Precision Rate of HLWO-RNN and VGG and CNN and (D) Comparison Accuracy Rate of HLWO-RNN and VGG and CNN (E) Comparison rate of HTER (F) Comparison with Meta Heuristic Technique

Conclusions

This paper proposed is effective face anti-spoofing structure that integrates Local Binary Pattern (LBP) for texture feature extraction with the Whale Optimization Algorithm (WOA) for optimized feature selection, embedded within a hybrid component learning model. The framework presented some challenges in spoof detection, such as generalization across attack types and efficient performance under real-world conditions. By optimizing LBP parameters and selecting the most discriminative features using WOA, the model significantly reduces redundancy and enhances classification accuracy. Furthermore, combining these features with a

lightweight neural network, specifically an RNN-based classifier, enables improved detection of sophisticated spoofing techniques such as replay, print, and 3D mask attacks. Some results on benchmark datasets, including NUAA and CASIA-FASD, demonstrate superior recital in terms of accuracy, precision, sensitivity, and reduced computational complexity and analysis to traditional and deep learning-based model. The proposed HLWO-RNN system achieved high reliability while maintaining low resource requirements, making it suitable for deployment in security-critical and mobile applications. Future work may explore deeper integration with multimodal inputs and real-time deployment.

Abbreviations

FAS: Face Anti-Spoofing; LBP: Local Binary Patterns; WOA: Whale Optimization Algorithm; 3D: Three-dimensional; PA: Presentation Attack; CNN: Convolutional Neural Network; TOP: Three Orthogonal Planes; LPQ: Local Phase Quantization; HOG: Histogram of Oriented Gradients; DoG: Difference of Gaussian; PSO: Particle Swarm Optimization; GA: Genetic Algorithms; ACO: Ant Colony Optimization; EER: Equal Error Rate; ACER: Average Classification Error Rate; HTER: Half Total Error Rate; FAR: False Acceptance Rate; RNN: Recurrent Neural Network; MSE: Mean Square Error; FRR: False Rejection Rate, RNN: Recurrent Neural Network

References

[1] Määttä A, Hadid A, Pietikäinen M. Face spoofing detection from single images using micro-texture analysis. In: 2011 International Joint Conference on Biometrics (IJCB); 2011; Washington (DC), USA. p. 1–7. doi: 10.1109/IJCB.2011.6117510.
[2] Chingovska G, Anjos A, Marcel S. On the effectiveness of local binary patterns in face anti-spoofing. In: IEEE BIOSIG; 2012; Darmstadt, Germany. p. 1–7. Available from: https://publications.idiap.ch/downloads/papers/2012/Chingovska_IEEEBIOSIG2012_2012.pdf
[3] Anthony P, Ay M, Aydin N. A review of face anti-spoofing methods for face recognition systems. J Inf Secur Appl. 2021;58:102730. doi: 10.1016/j.jisa.2021.102730.
[4] Zhou J, Ge C, Yang J, Yao H, Qiao X, Deng P. Research and application of face anti-spoofing based on depth camera. In: 2019 2nd China Symposium on Cognitive Computing and Hybrid Intelligence (CCHI); 2019 Sept; Beijing, China. p. 225–9.
[5] Wu X, Zhou J, Liu J, Ni F, Fan H. Single-shot face anti-spoofing for dual pixel camera. IEEE Trans Inf Forensics Secur. 2020;16:1440–51. doi: 10.1016/j.jksuci.2023.101871.
[6] Yu L, Li X, Li Y, Zhao G. Face anti-spoofing with deep learning: A survey. IEEE Trans Pattern Anal Mach Intell. 2022;44(11):7607–26. doi: 10.1109/TPAMI.2022.3155508.
[7] Mirjalili S, Lewis A. The whale optimization algorithm. Adv Eng Softw. 2016;95:51–67. doi: 10.1016/j.advengsoft.2016.01.008.
[8] Spencer J, George M, Lee SH. Presentation attack detection using CNNs and LBP features. arXiv preprint arXiv:2312.00041. 2023. Available from: https://arxiv.org/abs/2312.00041
[9] Li Y, Wang Y, Zhang Z. Face anti-spoofing based on DWT-LBP-DCT features. J Vis Commun Image Represent. 2020;73:102930. doi: 10.1016/j.jvcir.2020.102930.

[10] Alvarez R, Vera-Rodriguez J, Fierrez J, Ortega-Garcia J. Presentation attack detection: A systematic literature review. ACM ComputSurv. 2022;55(5):1–38. doi: 10.1145/3526021.
[11] Madanan M, Akhmal N, Velayudhan NC. Optimal face spoof detection based on improved whale optimization algorithm and dual-stage CNN. J King Saud UnivComput Inf Sci. 2023;35(2):101871. doi: 10.1016/j.jksuci.2023.101871.
[12] Xing H, Tan SY, Qamar F, Jiao Y. Face antispoofing based on deep learning: A comprehensive survey. Appl Sci. 2025;15(12):6891. doi: 10.3390/app15126891.
[13] Wang Z, Yu Z, Zhao C, Zhu X, Qin Y, Zhou Q, Zhou F, Lei Z. Deep spatial gradient and temporal depth learning for face antispoofing. arXiv preprint arXiv:2003.08061. 2020. Available from: https://arxiv.org/abs/2003.08061
[14] Liu S, Zhang KY, Yao T, Bi M, Ding S, Li J, et al. Adaptive normalized representation learning for generalizable face antispoofing. arXiv preprint arXiv:2108.02667. 2021. Available from: https://arxiv.org/abs/2108.02667
[15] Shao R, Lan X, Yuen PC. Regularized fine-grained meta face antispoofing. arXiv preprint arXiv:1911.10771. 2019. Available from: https://arxiv.org/abs/1911.10771
[16] Zhang KY, Yao T, Zhang J, Tai Y, Ding S, Li J, et al. Face antispoofing via disentangled representation learning. arXiv preprint arXiv:2008.08250. 2020. Available from: https://arxiv.org/abs/2008.08250
[17] De Freitas Pereira L, Anjos A, De Martino JM, Marcel S. LBPTOP based countermeasure against face spoofing attacks. In: Proc Asian Conf Computer Vision; 2012. p. 121–32.
[18] Shao S, Xiang T, Loy CC. Domain generalization for face anti-spoofing. IEEE Trans Inf Forensics Secur. 2020;15:3243–57. doi: 10.1109/TIFS.2020.2993545.
[19] Yang J, Lei Z, Liao S, Li SZ. Learn convolutional neural network for face anti-spoofing. arXiv preprint arXiv:1408.5601. 2013.
[20] Liu Y, Ju Y, Jourabloo A, Liu X. Disentangling spoof trace for generic face anti-spoofing. In: Proc IEEE/CVF Conf Computer Vision and Pattern Recognition (CVPR); 2021. p. 6812–21. doi: 10.1109/CVPR46437.2021.00674.
[21] Kim HJ, Kwon SK. Anti-Spoofing Method by RGB-D Deep Learning for Robust to Various Domain Shifts. Electronics. 2025;14(11):2182.
[22] Yu Z, Yang X, Li S, Zhao G. Remote heart rate measurement from face videos under realistic conditions using spatio-temporal networks. IEEE Trans Image Process. 2021;30:954–67. doi: 10.1109/TIP.2020.3038924.
[23] Atoum Y, Liu Y, Jourabloo A, Liu X. Face anti-spoofing using patch and depth-based CNNs. In: Proc IEEE Int Joint Conf Biometrics; 2017. p. 319–28.
[24] Larey A, Rond E, Achrack O. A Multi-Modal Approach for Face Anti-Spoofing in Non-Calibrated Systems using Disparity Maps. arXiv preprint arXiv:2410.24031. 2024.
[25] Yang J, Li Y, Luo J, Tan T. Face anti-spoofing: Model matters, so does data. In: Proc IEEE/CVF Conf Computer Vision and Pattern Recognition (CVPR); 2019. p. 3507–16.
[26] Patel K, Han H, Jain AK. Cross-database face antispoofing with robust feature representation. Neurocomputing. 2016;197:25–38.
[27] George A, Marcel S. Deep pixel-wise binary supervision for face presentation attack detection. In: Proc Int Conf Biometrics (ICB); 2019. p. 1–8.

[28] Agarwal P, Gupta P. Face anti-spoofing using multi-feature CNN. Multimed Tools Appl. 2019;78(3):3617–32. doi: 10.1007/s11042-018-6269-z.
[29] Zhang Z, Yan J, Liu S, Lei Z, Li SZ. A face antispoofing database with diverse attacks. In: Proc 5th IAPR Int Conf Biometrics (ICB); 2012. p. 26–31.
[30] Liu Y, Jourabloo A, Liu X. Learning deep models for face anti-spoofing: Binary or auxiliary supervision. In: Proc IEEE Conf Computer Vision and Pattern Recognition (CVPR); 2018. p. 389–98. doi: 10.1109/CVPR.2018.00047.
[31] George B, Aithal HKS, Babu AV. Deep learning-based face anti-spoofing: A survey. Inf Fusion. 2021;76:252–75. doi: 10.1016/j.inffus.2021.05.004.
[32] Bhatia R, Kumar A. Adaptive face anti-spoofing using residual CNNs with LBP-enhanced input. Multimed Tools Appl. 2025;84:9111–30. doi: 10.1007/s11042-024-17723-1.
[33] Li Y, Feng Z, Zhao G. Face anti-spoofing via deep local binary patterns. In: Proc Int Conf Image Processing (ICIP); 2017; Beijing, China. p. 3220–4. doi: 10.1109/ICIP.2017.8296907.
[34] Boulkenafet Z, Komulainen J, Hadid A. Face spoofing detection using colour texture analysis. IEEE Trans Inf Forensics Secur. 2016;11(8):1818–30. doi: 10.1109/TIFS.2016.2555283.
[35] Tarasov AA, Denisova AY, Fedoseev VA. Detection of presentation attacks on facial authentication systems using Intel RealSense depth cameras. In: Int Conf Hybrid Intelligent Systems; 2022 Dec; Cham, Switzerland. Springer; 2022. p. 1303–14.
[36] De Freitas Pereira T, Anjos A, De Martino JM, Marcel S. Can face anti-spoofing be properly benchmarked? In: Proc IEEE Int Conf Biometrics: Theory, Applications and Systems (BTAS); 2012; Arlington (VA), USA. p. 1–8. doi: 10.1109/BTAS.2012.6374579.