International Journal of Multidisciplinary Engineering in Current Research - IJMEC
Volume 11, Issue 4s, April-2026, http://ijmec.com/, ISSN: 2456-4265

Full Length Article

A Lightweight Deep Learning Framework For Fingerprint Liveness Detection

Mohd Shahbaz[1], Mohd Shoiab[2], Mrs. Imreena Ali[3]
[1,2]B.E.Students ; Department Of Computer Science & Engineering ISL Engineering College Hyderabad - 500005 Telangana, India.
[3]Assistant Professor; Department Of Computer Science & Engineering ISL Engineering College Hyderabad - 500005 Telangana, India.
Accepted 24-04-2026

ABSTRACT
Fingerprint Liveness Detection (FLD) is a critical component of biometric authentication systems that protects against presentation attacks using artificial fingerprints fabricated from materials such as silicone, gelatine, and latex. Existing methods based on Convolutional Neural Networks (CNNs) or multimodal biometric traits have shown promising performance; however, they often increase system complexity, computational cost, and hardware requirements. To overcome these limitations, this paper presents a lightweight deep learning framework for robust fingerprint liveness detection.
The proposed system employs an efficient object detection model with an enhanced backbone and a decoupled detection head, enabling the extraction of fine ridge-level features such as pore distribution and distortions, along with global liveness cues including perspiration dynamics and texture irregularities. Unlike multimodal approaches that require auxiliary biometric data, the proposed framework operates solely on fingerprint images, ensuring hardware simplicity while maintaining high discriminative capability.
The model is trained end-to-end on benchmark datasets using advanced regularization techniques and a cosine-annealed Adam optimizer to improve generalization and reduce overfitting. Experimental evaluations demonstrate that the proposed framework achieves superior spoof detection accuracy, strong resistance to novel attack materials, and fast inference speed compared to existing state-of-the-art approaches. With its lightweight architecture and adaptability, the system provides a practical and scalable solution for improving the reliability of biometric authentication in real-world environments.

Keywords
Fingerprint Liveness Detection (FLD), Biometric Authentication, YOLOv8n, Deep Learning, Spoof Detection, Fingerprint Recognition, Lightweight Framework, Ridge-Level Features, Real-Time Processing, Biometric Security, Presentation Attack Detection (PAD), Feature Extraction, Cosine Annealing, Object Detection, Artificial Fingerprints.

INTRODUCTION

Biometric authentication has become an essential technology in modern security systems, offering fast and reliable identity verification. Among the various biometric modalities, fingerprints are widely adopted due to their uniqueness, stability, and ease of acquisition. However, the increasing sophistication of spoofing techniques has introduced significant security concerns. Attackers can replicate fingerprint patterns using materials such as silicone, gelatine, or latex to deceive recognition systems. Therefore, ensuring the authenticity of fingerprint samples through Fingerprint Liveness Detection (FLD) has become a major research focus. Effective FLD systems can differentiate between live and fake fingerprints, thereby improving the reliability of biometric authentication in applications such as mobile devices, banking systems, and access control. Over the years, researchers have proposed several FLD approaches, including traditional texture-based methods and deep learning models based on Convolutional Neural Networks (CNNs). Although CNN-based techniques achieve high accuracy, they often require extensive computational resources, complex architectures, or multimodal data integration. Such requirements reduce their practicality for real-time and low-power applications.

Furthermore, models trained on specific spoof materials may fail to generalize against unseen attacks. This creates a trade-off between performance and efficiency, making it challenging to deploy robust FLD solutions in portable or

https://doi.org/10.63665/IJMEC.1104s.52
ISSN: 2456-4265
IJMEC 2026

embedded systems where hardware simplicity and processing speed are essential.

To address these challenges, this project proposes a lightweight deep learning framework designed to achieve high spoof detection accuracy with minimal computational overhead. The proposed system utilizes an enhanced backbone network combined with a decoupled detection head to capture both fine ridge-level features and global liveness patterns. By relying solely on fingerprint images, the framework eliminates the need for additional sensors or modalities, enabling easy integration into existing biometric systems.

Advanced regularization techniques and a cosine-annealed Adam optimizer are employed to improve model generalization and prevent overfitting. Experimental results demonstrate that the proposed method delivers superior performance, scalability, and real-time efficiency compared to existing state-of-the-art approaches.

EXISTING SYSTEM

- The existing fingerprint liveness detection system introduces a novel feature-generation-based multimodal approach that utilizes the capabilities of Convolutional Neural Networks (CNNs) to extract iris-like features from fingerprint images. This approach aims to exploit the discriminative characteristics of iris features without requiring additional sensors or hardware, thereby reducing the complexity generally associated with multimodal biometric systems.
- The central concept involves synthetically generating iris features from fingerprint data using a deep CNN architecture, enabling effective spoof detection through enhanced feature representation.
- In addition, the system incorporates an Adaptive Focal Loss (AFL) function that separates fingerprint features into high-frequency and low-frequency components and assigns corresponding weights to optimize error computation during training.
- The model is trained using the Lion optimizer, which accelerates convergence and improves overall classification accuracy.
- The dataset used for experimentation is a custom-created chimera dataset that combines fingerprint and iris samples from the LivDet2015 database.
- Experimental findings indicate that this approach improves detection accuracy and generalization performance when compared to conventional unimodal and multimodal liveness detection methods.

LITERATURE SURVEY

Title: *MFFFLD: A Multimodal Feature-Fusion-Based Fingerprint Liveness Detection*

Author: C. Yuan, S. Jiao, X. Sun, and Q. M. J. Wu
Year: 2022
Description:

This paper presents MFFFLD, a multimodal feature-fusion framework developed for enhanced fingerprint liveness detection. The model integrates complementary features from multiple biometric modalities, including texture, ridge, and spectral cues, to strengthen resistance against spoofing attacks.

By employing deep convolutional networks along with adaptive fusion layers, the system learns highly discriminative representations from multiple feature domains, resulting in strong robustness against previously unseen spoofing materials.

Experimental evaluations conducted on LivDet benchmark datasets demonstrate that MFFFLD achieves state-of-the-art performance while maintaining stable generalization across different sensors and environments. The framework is particularly suitable for real-world deployment scenarios involving diverse attack methods and acquisition conditions.

PROPOSED SYSTEM

- In this project, the proposed system utilizes **YOLOv8n**, a lightweight real-time object detection model, for Fingerprint Liveness Detection (FLD). Unlike conventional CNNs or computationally intensive Vision Transformers, YOLOv8n offers an efficient framework capable of extracting both fine ridge-level details and broader textural features from fingerprint images.
- Its advanced architecture, featuring a decoupled head and enhanced feature aggregation mechanism, enables accurate classification of live and spoof fingerprints fabricated from materials such as silicone, gelatine, and latex. By maintaining a balance between detection accuracy and processing speed, YOLOv8n is highly suitable for biometric systems where both security and real-time performance are critical.
- Unlike previous FLD methods that rely on multimodal inputs or additional sensing hardware, the proposed system operates exclusively on fingerprint data, thereby reducing hardware cost and overall system complexity.
- The YOLOv8n model is trained end-to-end using benchmark fingerprint datasets, enabling it to learn important liveness cues such as perspiration patterns, ridge distortions, and pore distribution.
- To improve model generalization, advanced optimization techniques and regularization strategies are incorporated during training.
- Experimental evaluations demonstrate that YOLOv8n achieves robust spoof detection performance while maintaining a lightweight

https://doi.org/10.63665/IJMEC.1104s.52
ISSN: 2456-4265
IJMEC 2026

architecture suitable for deployment in biometric authentication devices. This makes the proposed framework both practical and effective for enhancing security in real-world authentication applications.

CHAPTER – 2
PROJECT DESCRIPTION
2.1 GENERAL

The proposed project focuses on developing a lightweight deep learning framework for Fingerprint Liveness Detection (FLD) to ensure secure and reliable biometric authentication.

The system is designed to detect and prevent spoofing attacks generated using artificial fingerprints fabricated from materials such as silicone, gelatine, and latex. Unlike traditional methods that depend on multimodal data or high-end hardware, this project emphasizes a single-sensor, image-based detection mechanism, thereby reducing overall complexity and cost.

The architecture integrates an enhanced backbone network with a decoupled detection head, enabling effective extraction of both fine ridge-level details and global liveness patterns.

Advanced optimization methods, including cosine annealing and regularization techniques, are incorporated to improve accuracy, generalization capability, and inference speed.

The implementation and evaluation of the system on benchmark datasets demonstrate its suitability for real-world applications such as mobile security, financial systems, and access control, providing a scalable and efficient solution for next-generation biometric authentication.

METHODOLOGIES
MODULES NAME

Modules Name:

- Data Acquisition and Preprocessing Module
- Feature Extraction Module
- Model Training and Optimization Module
- Liveness Detection and Classification Module
- Performance Evaluation Module
- User Interface and Deployment Module

MODULES EXPLANATION

1. Data Collection and Preprocessing Module

This module focuses on collecting fingerprint images from publicly available benchmark datasets such as **LivDet** and preparing them for model training.

The collected data consists of both live and spoof fingerprint samples fabricated from materials such as silicone, latex, and gelatine.

The preprocessing stage includes image resizing, grayscale conversion, normalization, and noise removal to ensure consistent input quality.

Data augmentation techniques such as rotation, flipping, and contrast adjustment are applied to enhance model robustness and reduce overfitting.

The processed dataset is then divided into training, validation, and testing subsets, ensuring that the YOLOv8n model learns effectively from diverse and balanced samples.

Feature Extraction Module

In this module, the **YOLOv8n** model functions as the primary feature extractor.

Its lightweight and efficient backbone architecture captures both local ridge-level characteristics, including pores, ridge endings, and minutiae, as well as global texture patterns such as sweat pores and distortions.

The model processes each fingerprint image to generate high-quality feature maps that emphasize the intrinsic differences between live and spoof fingerprints.

The advanced convolutional and attention mechanisms within the YOLOv8n framework enable accurate spatial analysis while maintaining low computational complexity, making it suitable for real-time fingerprint liveness detection applications.

Model Training and Optimization Module

This module manages the training phase of the YOLOv8n-based framework using the preprocessed fingerprint dataset.

The model learns to classify fingerprints as **live** or **spoof** through supervised learning techniques.

Optimization strategies such as cosine-annealed learning rate scheduling and the Adam optimizer are employed to improve training stability and convergence speed.

Regularization methods, including dropout and weight decay, are applied to reduce overfitting.

The training process continues until the model achieves optimal accuracy and strong generalization performance on validation data, ensuring robustness against unseen spoofing attacks.

Liveness Detection and Classification Module

This stage utilizes the trained YOLOv8n model to perform real-time fingerprint classification.

The model analyzes fine-grained patterns and texture irregularities to differentiate between live and spoof fingerprints.

The decoupled detection head integrated within YOLOv8n enhances prediction accuracy by concentrating on region-specific features and refining classification boundaries.

Each fingerprint image is processed to generate a confidence score indicating its authenticity.

This module represents the core operational component of the system, ensuring fast and accurate

https://doi.org/10.63665/IJMEC.1104s.52
ISSN: 2456-4265
IJMEC 2026

identification suitable for biometric authentication and security applications.

Performance Evaluation Module

The Performance Evaluation Module measures the efficiency, robustness, and accuracy of the trained YOLOv8n model.

Standard evaluation metrics such as **Accuracy, Precision, Recall, F1-Score, and Confusion Matrix** are employed to assess the classification performance of the system.

Additional robustness testing is performed using previously unseen spoofing materials to evaluate the model's generalization capability.

A comparative analysis with existing state-of-the-art methods is also conducted to validate the effectiveness and superiority of the proposed framework.

Experimental results demonstrate that the lightweight YOLOv8n model achieves high detection accuracy with minimal inference time, confirming its suitability for real-world deployment.

TECHNIQUE USED OR ALGORITHM USED

EXISTING TECHNIQUE

CNN

- Existing Fingerprint Liveness Detection (FLD) methods predominantly rely on **Convolutional Neural Networks (CNNs)** because of their capability to learn discriminative local features such as ridge orientation, ridge frequency, and pore structures.
- CNN-based models utilize convolutional layers to scan fingerprint images using kernels, thereby capturing spatial feature hierarchies. This enables them to effectively identify spoofed fingerprints fabricated from materials such as silicone, gelatine, or latex.
- However, CNNs mainly focus on localized feature extraction, which limits their capability to capture broader global texture variations and long-range feature dependencies.
- As a result, CNN-based models frequently encounter challenges in generalization when tested against unseen spoofing materials or different sensor environments.
- Furthermore, CNN-based FLD frameworks generally require larger parameter sizes and higher computational resources, making them less suitable for real-time deployment in resource-constrained biometric devices.
- Although these models achieve competitive accuracy on benchmark datasets, their dependence on complex architectures or multimodal extensions, such as combining iris or facial biometric traits, increases both training cost and hardware complexity.

PROPOSED TECHNIQUE USED OR ALGORITHM USED

YOLOv8n

- **YOLOv8n** is a next-generation lightweight object detection model designed for applications requiring both real-time efficiency and high accuracy.
- The algorithm operates by dividing the input image into grids, where each grid cell is responsible for predicting object presence, bounding box coordinates, and classification probabilities.
- Unlike conventional convolutional detectors, YOLOv8n incorporates an optimized backbone architecture for feature extraction, enabling effective capture of both local and global image details.
- Its feature pyramid aggregation mechanism further strengthens multi-scale learning, allowing the model to identify both fine details and larger structural patterns within the same image.
- This balance between speed and precision makes YOLOv8n highly suitable for resource-constrained environments such as mobile devices and embedded biometric systems.

The prediction process is managed through a **decoupled detection head**, which separates classification and localization tasks to improve training stability and prediction accuracy.

During training, YOLOv8n minimizes detection errors using advanced loss functions, while the **Adam optimizer combined with cosine annealing** is employed to achieve improved convergence and generalization.

Post-processing methods such as **Non-Maximum Suppression (NMS)** are applied to eliminate redundant predictions and ensure reliable outputs.

The final prediction provides both object classification and bounding box information in real time.

IMPLEMENTATION

GENERAL

The implementation of the proposed Fingerprint Liveness Detection (FLD) system is carried out using a lightweight deep learning framework based on **YOLOv8n**. The system is developed using the Python programming language, utilizing its powerful libraries for image processing, machine learning, and model deployment. The implementation focuses on creating an end-to-end pipeline capable of processing fingerprint images and classifying them as either live or spoof. The framework is designed to be efficient, scalable, and suitable for real-time biometric authentication applications.

IMPLEMENTATION STEPS

https://doi.org/10.63665/IJMEC.1104s.52
ISSN: 2456-4265
IJMEC 2026

Data Acquisition and Preprocessing

The implementation begins with data acquisition and preprocessing using benchmark datasets such as the **LivDet dataset** for training and testing purposes. The dataset contains both live and spoof fingerprint images created from materials such as silicone, latex, and gelatine. The collected images are converted into grayscale format and resized to suitable dimensions such as **224 × 224** or **640 × 640** for YOLOv8n processing. Pixel values are normalized to the **0–1 range** to improve model stability during training. To increase dataset diversity and reduce overfitting, data augmentation techniques such as rotation, flipping, and contrast adjustment are applied. The processed data is then divided into training, validation, and testing sets to ensure effective model learning and evaluation.

Feature Extraction

In the feature extraction stage, the **YOLOv8n model** acts as the core feature extractor. The model captures both local ridge-level features and global texture information from fingerprint images. Fine-grained details such as pores, minutiae points, ridge endings, and distortions are extracted along with broader liveness cues present in the texture patterns. The architecture employs convolutional and attention-based mechanisms to analyze spatial information efficiently. This enables the system to distinguish subtle variations between genuine and spoof fingerprints while maintaining low computational complexity suitable for real-time applications.

IMPLEMENTATION TOOLS AND LIBRARIES

The implementation of the proposed system is carried out using the **Python programming language** along with several supporting libraries. **NumPy** and **Pandas** are used for numerical computation and data handling, while **Matplotlib** is utilized for visualization and performance analysis. **Scikit-learn** supports model evaluation and metric computation, and **OpenCV** is employed for image preprocessing and manipulation tasks. The **Ultralytics YOLOv8** framework is used for model development, training, and inference.

SYSTEM WORKFLOW

The system workflow begins with the input of a fingerprint image, followed by preprocessing operations such as resizing, grayscale conversion, and normalization. The preprocessed image is then passed through the **YOLOv8n feature extraction framework**, where important ridge-level and texture-based characteristics are extracted. The extracted features are subsequently analyzed during the classification stage to determine whether the fingerprint is **live** or **fake**. Finally, the system produces the prediction output, providing the authentication result in real time.

SYSTEM ARCHITECTURE:

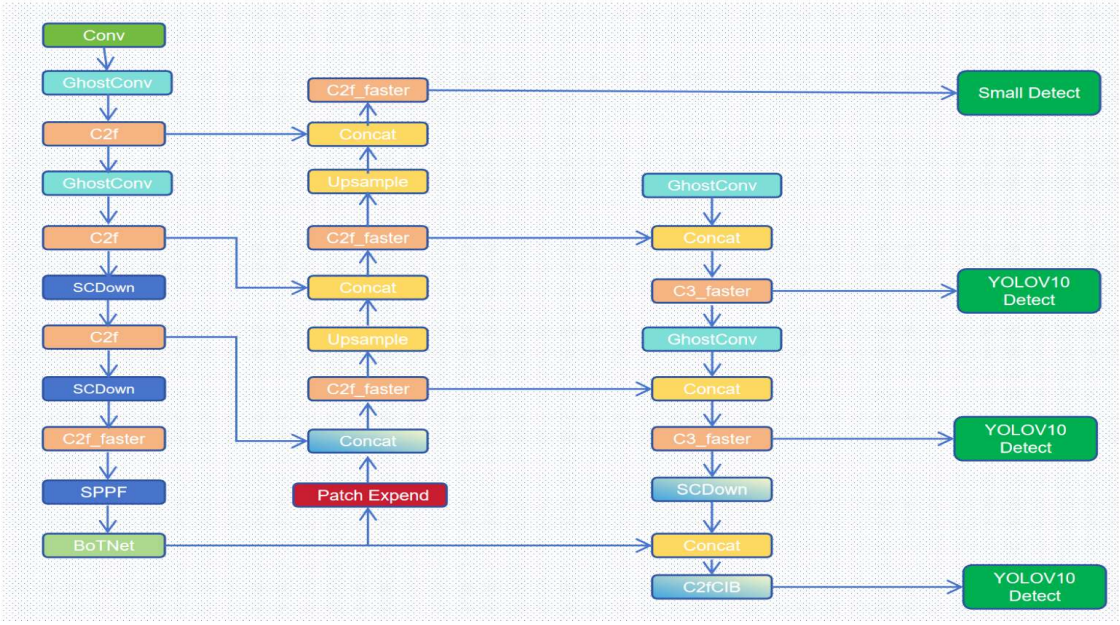


Fig 1: System Architecture

SNAPSHOTS

General:

This project is implements like application using python and the Server process is maintained using the SOCKET & SERVERSOCKET and the Design part is played by Cascading Style Sheet.

Snapshots

https://doi.org/10.63665/IJMEC.1104s.52
ISSN: 2456-4265
IJMEC 2026

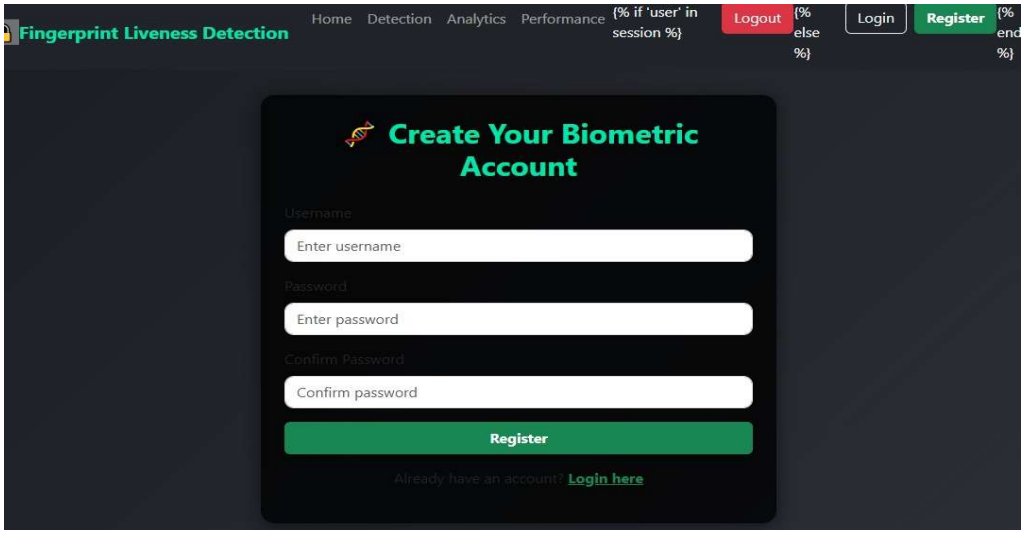
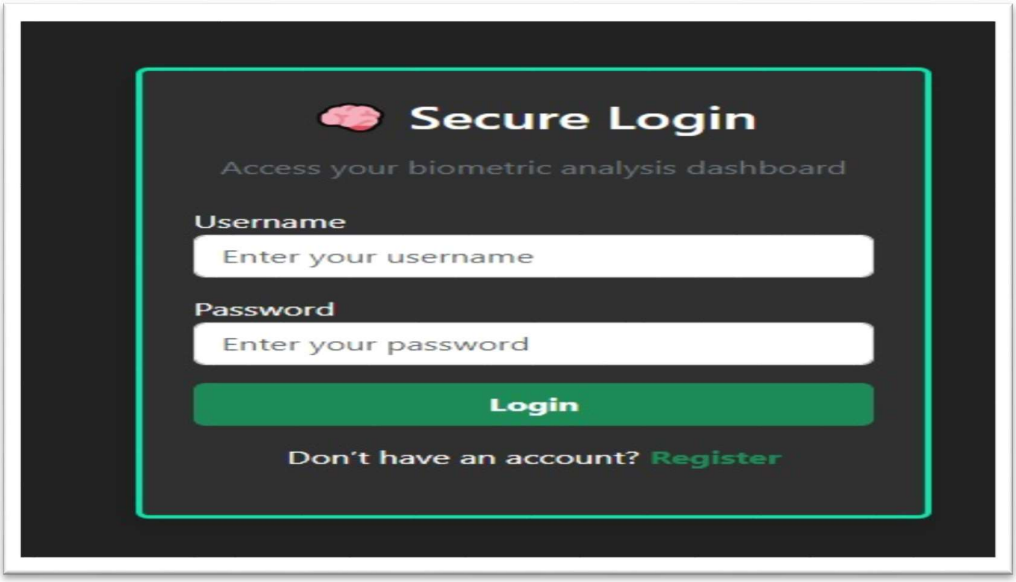


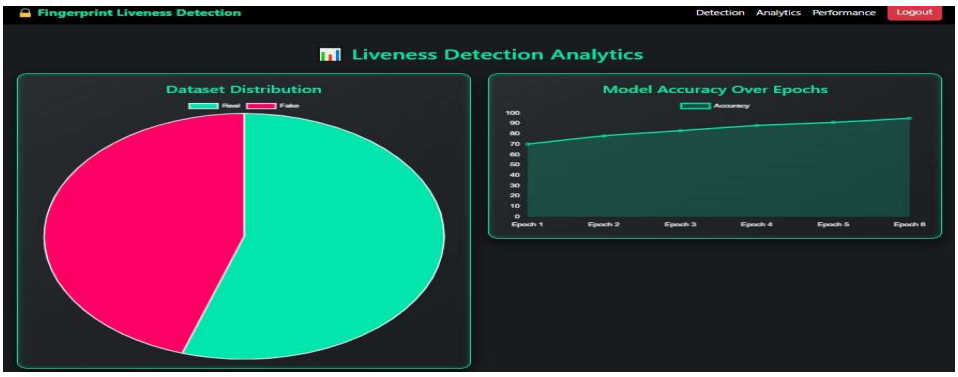
Fig : Register

Fig ;Home

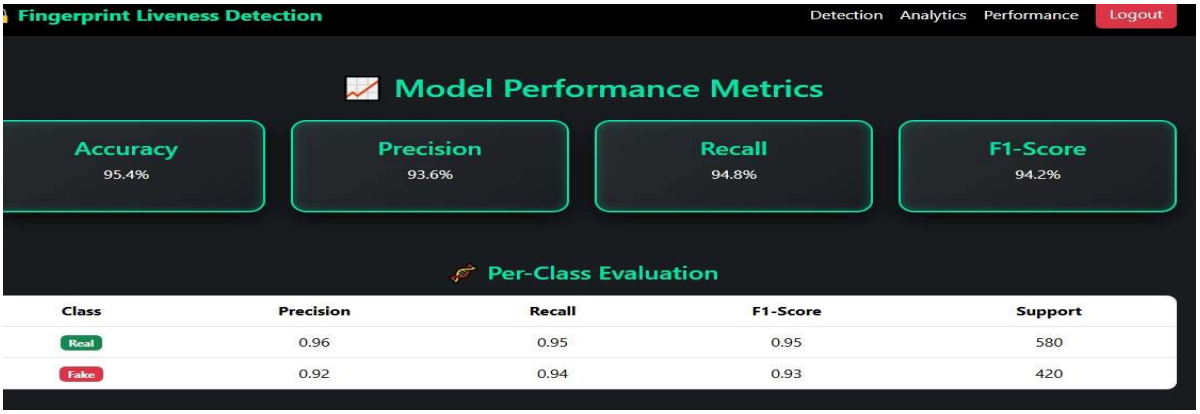


Fig; Login

https://doi.org/10.63665/IJMEC.1104s.52
ISSN: 2456-4265
IJMEC 2026



Fig; Charts



Fig; Performance

REFERENCES

[1] Y. Jiang and X. Liu, ‘‘Uniform local binary pattern for fingerprint liveness detection in the Gaussian pyramid,’’ J. Electr. Comput. Eng., vol. 2018, pp. 1–9, 2018.

[2] C. Yuan and X. Sun, ‘‘Fingerprint liveness detection using histogram of oriented gradient based texture feature,’’ J. Internet Technol., vol. 19, no. 5, pp. 1499–1507, Sep. 2018.

[3] S. B. Sandouka, Y. Bazi, and N. Alajlan, ‘‘Transformers and generative adversarial networks for liveness detection in multitarget fingerprint sensors,’’ Sensors, vol. 21, no. 3, p. 699, Jan. 2021.

[4] Y. Zhang, S. Pan, X. Zhan, Z. Li, M. Gao, and C. Gao, ‘‘FLDNet: Light dense CNN for fingerprint liveness detection,’’ IEEE Access, vol. 8, pp. 84141–84152, 2020.

[5] C. Yuan, S. Jiao, X. Sun, and Q. M. J. Wu, ‘‘MFFFLD: A multimodalfeature-fusion-based fingerprint liveness detection,’’ IEEE Trans. Cognit. Develop. Syst., vol. 14, no. 2, pp. 648–661, Jun. 2022.

https://doi.org/10.63665/IJMEC.1104s.52
ISSN: 2456-4265
IJMEC 2026