International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

FINGERPRINT LIVENESS DETECTION VIA GLOBAL FEATURE ENCODING WITH VISION TRANSFORMERS

Dr.A.Rajesh[1], K.Venkata Shirisha[2], Kadamanchi Jyothi Bas[3], MD.Salman Pasha[4]
Associate Professor, Department of CSE[1]
Students, Department of CSE[2,3,4]
Guru Nanak Institute of Technology, Hyderabad, Telangana, India

Abstract: Fingerprint Liveness Detection (FLD) is crucial for securing biometric systems by identifying fake fingerprints made from materials like silicone, gelatine, and latex. To reduce complexity and computational cost, a lightweight deep learning framework is proposed that efficiently captures both fine ridge-level details and global texture features. The system relies solely on fingerprint images, ensuring hardware simplicity and easy deployment without additional biometric inputs. It uses an optimized architecture with advanced training techniques to improve accuracy and performance. As a result, the model achieves strong generalization and reliable performance in real-world applications.

Keywords: FLD, CNN, Spoof Detection, Biometric Authentication

I.INTRODUCTION

Biometric authentication is widely used for secure and fast identity verification, with fingerprints being the most common due to their uniqueness and ease of use. However, advanced spoofing techniques using materials like silicone, gelatine, and latex pose serious security threats. To address this, Fingerprint Liveness Detection (FLD) plays a vital role in distinguishing real fingerprints from fake ones. This improves the reliability of biometric systems in applications such as mobile security, banking, and access control. Over time, various FLD methods have been developed, including traditional texture-based techniques and deep learning approaches. CNN-based methods provide high accuracy but often involve high computational cost and complex architectures. These limitations highlight the need for more efficient and lightweight FLD solutions.

II. LITERATURE SURVEY

K. Zhang, S. Huang, E. Liu, and H. Zhao (2023) This paper presents a system that detects negative social media comments using NLP and the Random Forest algorithm, classifying them as hate, offensive, or normal. It also performs sentiment analysis, tracks user behavior, and promotes safe communication while efficiently handling large-scale real-time data.

C. Yuan, S. Jiao, X. Sun, and Q. M. J. Wu(2022) This paper introduces MFFFLD, a multimodal feature-fusion framework that improves fingerprint liveness detection by combining texture, ridge, and spectral features. Using CNNs and adaptive fusion, it captures both local and global patterns, enhancing detection of spoof fingerprints made from materials like silicone, gelatin, and latex.

III. EXISTING SYSTEM

The existing system uses a CNN-based multimodal approach that generates iris-like features from fingerprint images to improve spoof detection. This method enhances feature representation without requiring additional hardware, reducing system complexity while maintaining strong detection capability.

Existing System Disadvantages

- Prone to Overfitting
- Limited Global Feature Extraction
- High Computational Cost
- Lower Adaptability

- Longer Training Time

Proposed System

This project uses YOLOv8n, a lightweight real-time object detection model, for efficient Fingerprint Liveness Detection. It extracts both fine ridge details and global texture features to accurately classify live and spoof fingerprints. The model's optimized architecture ensures high accuracy while maintaining fast performance. This balance makes it suitable for secure and real-time biometric applications.

Proposed System Advantages:

- High Accuracy in Spoof Detection
- Better Generalization
- Real-Time Processing
- Scalable and Practical

IV. SYSTEM ARCHITECTURE

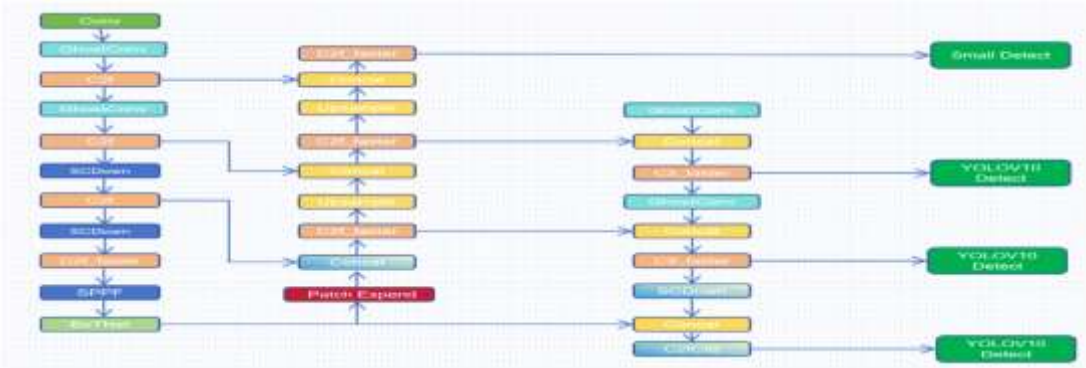

Figure 1 : SYSTEM ARCHITECTURE

This diagram shows an object detection architecture using optimized layers like GhostConv, C2f, and C3 to extract and fuse multi-scale features. It uses advanced modules and multiple detection heads to achieve accurate and fast detection of objects at different sizes.

Methodology

1. Data Collection and Preprocessing Module:

This module collects and preprocesses fingerprint images (real and spoof) using techniques like resizing, normalization, and noise removal. It applies data augmentation and splits the dataset into training, validation, and testing sets for effective YOLOv8n model training.

2. Feature Extraction:

In this module, YOLOv8n extracts both local and global fingerprint features. Its efficient architecture enables accurate, real-time liveness detection with low computational complexity.

3. Model Training and Optimization:

This module trains the YOLOv8n model to classify fingerprints as live or spoof using supervised learning. Optimization and regularization techniques ensure fast convergence, high accuracy, and strong generalization against unseen attacks.

4. Liveness Detection and Classification:

This module uses the trained YOLOv8n model for real-time classification of fingerprints as live or spoof. It analyzes fine patterns and outputs an authenticity score, ensuring fast and accurate biometric authentication.

5. Performance Evaluation:

This module evaluates the YOLOv8n model using metrics like Accuracy, Precision, Recall, F1-Score, and Confusion Matrix. It also tests robustness and compares with other methods, showing high accuracy and fast performance for real-world use.

6. Deployment and User Interface:

This module deploys the trained YOLOv8n model into a user-friendly application for real-time fingerprint authentication. It ensures fast, portable, and efficient performance with an easy GUI for practical use in security systems.

V. IMPLEMENTATION

The implementation phase converts the conceptual design of the Fingerprint Liveness Detection system into a real-time working application. This stage involves setting up the development environment, preprocessing fingerprint datasets, training the deep learning model, and integrating the system for real-time detection. The system is designed to accurately distinguish between live and spoof fingerprints using advanced deep learning techniques.

Algorithm Used

Existing Algorithm

CNN

Existing FLD methods use CNNs to detect spoof fingerprints by extracting local features, but they struggle with global patterns and generalization to unseen attacks. They also require high computational resources and complex architectures, leading to overfitting and highlighting the need for lightweight and efficient solutions.

Proposed Algorithm

YOLOv8n:

YOLOv8n is a lightweight object detection model designed for real-time performance and high accuracy, predicting object locations and classes from image grids. It uses an optimized backbone and multi-scale feature learning to capture both fine and global details, making it suitable for resource-constrained environments like mobile and embedded systems.

VI. EXPERIMENTAL RESULTS

REGISTRATION PAGE :

Figure 2: REGISTRATION PAGE

This page provides a registration interface with fields for email, password, and confirmation, along with a register button and a login link for existing users.

DETECTION PAGE :

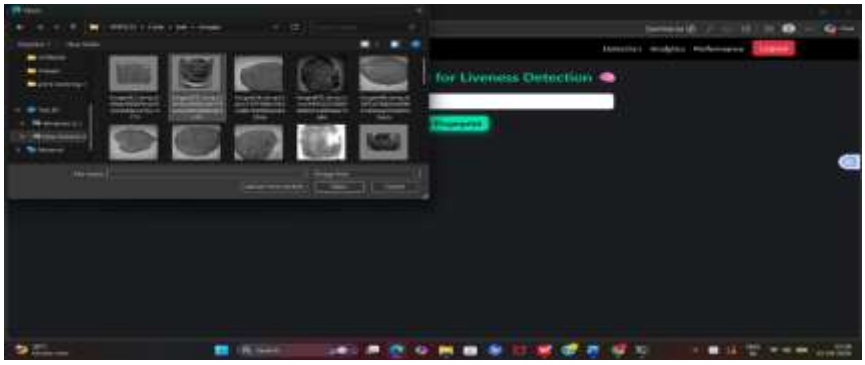

Figure 3: DETECTION PAGE

This page represents a fingerprint liveness detection system where users can upload or capture fingerprint images to verify if they are real or fake. It includes options for detection, analytics, and performance, ensuring secure and reliable fingerprint authentication.

VERIFICATION PAGE:

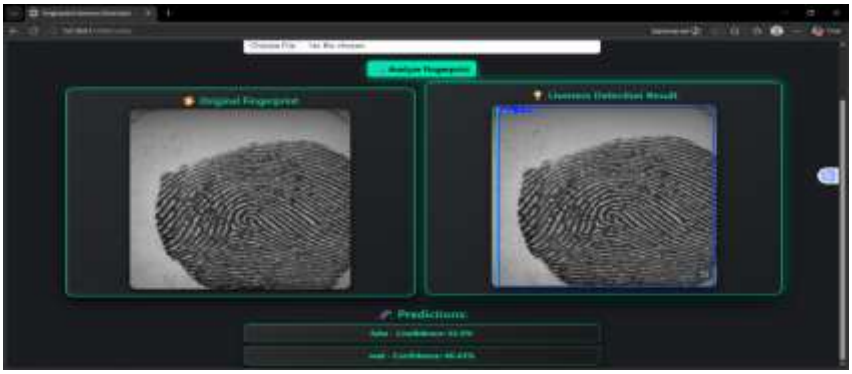

Figure 4: VERIFICATION PAGE

This page demonstrates the fingerprint liveness detection process where users upload an image and analyze whether it is real or spoofed. It displays both the original and processed results with confidence scores, ensuring accurate and secure authentication.

VII. CONCLUSION

The proposed fingerprint liveness detection system uses a lightweight YOLOv8n model to accurately distinguish between real and spoofed fingerprints. It combines efficient preprocessing, feature extraction, and classification while maintaining low computational cost. The system captures fine ridge and pore-level features, improving reliability against spoofing attacks. Its end-to-end design enables real-time performance, making it suitable for practical biometric applications. Overall, it provides a scalable and secure solution with potential for future enhancements like adaptive learning and edge optimization.

VIII. FUTURE ENHANCEMENT

In the future, the fingerprint liveness detection system can be enhanced by integrating multimodal biometrics like iris, face, or voice recognition to improve accuracy and security. It can also adopt advanced models such as transformers or VLMs to better capture complex fingerprint patterns and resist sophisticated attacks. Deploying optimized versions on edge devices like Raspberry Pi or Jetson can make the system scalable and cost-effective for real-time applications. Incorporating continuous learning methods like federated or incremental learning will help the model adapt to new spoofing techniques. Additionally, features like explainable AI and cloud-based monitoring can improve transparency, reliability, and system maintenance.

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.