International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 07 July 2026
DOI: 10.47191/ijcsrr/V9-i7-39, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

Implementation of YOLOv8n-Based Liveness Detection to Enhance the Security of Facial Attendance Systems Against Real-Time Spoofing Attacks

I Putu Elba Duta Nugraha[1], Widyadi Setiawan[2]
[1,2] Udayana University, Badung, Indonesia

ABSTRACT: This research aims to develop an anti-spoofing security system based on liveness detection to address the vulnerabilities of facial attendance systems against identity manipulation using photos or videos. The methodology employed is quantitative experimental, utilizing the YOLOv8n (You Only Look Once) deep learning architecture. The research stages involved the independent collection of a dataset comprising 8,000 images, categorized into "real" and "fake" face classes. This dataset was processed using a distribution ratio of 70% for training, 20% for validation, and 10% for testing. The model training process was conducted over 50 epochs using the Google Colab platform supported by a Tesla T4 Graphics Processing Unit (GPU). The results indicate that the developed model achieves high performance, with a mean Average Precision (mAP50) of 99.4%, precision of 98.8%, and recall of 99.0%. Real-time testing demonstrated an average inference speed of 20 frames per second (FPS), ensuring system responsiveness in practical applications. Implementation on low-power hardware, specifically the NVIDIA Jetson Nano, confirmed the computational efficiency of the model for edge device deployment. The primary conclusion of this study is that the YOLOv8n-based liveness detection system is highly effective and viable for integration into automated organizational attendance systems due to its high accuracy and efficient power consumption.

KEYWORDS: anti-spoofing, computer vision, facial attendance, facial recognition, liveness detection

INTRODUCTION

Facial recognition-based attendance systems have become essential automation solutions for enhancing the efficiency and accuracy of attendance recording across various organizations. However, the implementation of these systems continues to face significant security challenges, particularly regarding their vulnerability to spoofing attacks. Users can exploit system loopholes by presenting photographs, video recordings, or masks to forge attendance, leading the system to erroneously recognize these identities as legitimate users. Consequently, the development of liveness detection security features is increasingly urgent to ensure that an individual is physically present in front of the camera.

Previous research has explored diverse approaches to addressing anti-spoofing issues. Early methods involved extracting specific facial image features to verify authenticity through relative facial movement tracking (1). As technology has advanced, the use of classifier modules based on Convolutional Neural Networks (CNN) has become dominant (2–5). Some studies combine CNNs with additional biological feature detection, such as eye blinking, to strengthen system reliability (6, 7). Efficiency in model development is also frequently achieved through transfer learning techniques using pre-trained models (3, 8–11). Regarding data requirements, researchers utilize public datasets such as CelebA-Spoof (5, 6, 12) or perform independent data collection using tools like OpenCV (13). Furthermore, there is a research trend focusing on the development of lightweight models for portable or IoT-based devices to make systems more flexible for field deployment (14, 15).

Despite the many methods developed, a gap remains in achieving an optimal balance between high accuracy and real-time processing speed, especially when implemented on low-power hardware. Most studies report accuracies ranging from 79% to 98% (2, 3, 5, 7, 8, 10, 11, 14), which still leaves a risk margin for critical security systems.

This study aims to address these challenges by implementing the YOLO (You Only Look Once) algorithm, an object detection technique capable of processing images in a single neural network pass, making it exceptionally fast and accurate for real-time applications. The primary focus of this study is to develop an anti-spoofing system capable of instantly detecting a user's physical presence with an accuracy target exceeding 99%. Additionally, this research aims to test the model's computational efficiency on NVIDIA Jetson Nano edge hardware to ensure operational viability in power-efficient, real-world environments. Through this

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 07 July 2026
DOI: 10.47191/ijcsrr/V9-i7-39, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

approach, it is expected to produce an attendance security solution that is not only robust against spoofing attacks but also responsive and resource-efficient.

MATERIALS AND METHODS

Study Design and Setting

This study employs a quantitative experimental method to develop an anti-spoofing security system. The research was conducted over a one-year period, from January to December 2025. All development and testing activities were carried out at the Computer Laboratory of the Electrical Engineering Study Program, Faculty of Engineering, Udayana University.

Data Sources and Dataset

The dataset for this study was independently collected using a webcam to ensure the data met the specific requirements of the model development. A total of 8,000 images were successfully collected, divided equally into 4,000 "real" face images and 4,000 "fake/spoof" face images. Real faces were captured from live human subjects with various positions, expressions, and lighting conditions. Meanwhile, fake faces were obtained by capturing face images displayed via mobile phone screens, TV screens, and printed media.

Data Processing Procedures and Software

The system was developed using the Python programming language, utilizing primary libraries such as OpenCV (cv2) and CVZone for computer vision processing. The data processing stages included:

- Detection and Filtration: Each face captured via webcam (640x480 resolution) was detected using the FaceDetector module. Only faces with a confidence score > 0.8 were processed to ensure data validity.
- Quality Check: To ensure image sharpness, the Laplacian Variance method was used. Images with a blur level below the threshold (blurThreshold = 35) were discarded.
- Annotation: The resulting detection bounding boxes were widened with a horizontal offset of 10% and a vertical offset of 20% to provide background context for the model. Data were stored in YOLO format (<class_id> <x_center> <y_center> <width> <height>).
- Data Partitioning: The dataset was shuffled to avoid bias and divided into three subsets with a ratio of 70% for training data, 20% for validation data, and 10% for testing data.

Analytical Methods and Model Training

The face authenticity detection model was built using the YOLOv8n architecture from the Ultralytics framework. The training process was conducted using two strategies:

- Online Training: Utilizing the Google Colab platform with Tesla T4 GPU support for intensive training over 50 epochs. Transfer learning techniques were applied using pre-trained weights (yolov8n.pt) to accelerate convergence.
- Training Parameters: The input image size was set at 640x640 pixels with a patience parameter of 25 epochs for early stopping to prevent overfitting.

Evaluation Metrics and Implementation

Model performance was statistically measured using metrics such as mAP50, mAP50-95, Precision, and Recall, with a performance target of 99% for each. For operational testing, inference speed was measured in milliseconds per image and Frames Per Second (FPS) to ensure real-time capability. The best model (best.pt) was then implemented and tested on NVIDIA Jetson Nano edge hardware to evaluate computational efficiency on low-power devices.

RESULTS

Dataset Acquisition and Characteristics

The data collection process through the OpenCV-based system yielded a total of 8,000 facial images, consisting of 4,000 real face samples and 4,000 spoofing attack (fake) samples. All images underwent a quality filter using the Laplacian Variance method with a blur threshold of 35 to ensure visual sharpness. This dataset was subsequently divided into a training set (5,600 images), a validation set (1,600 images), and a testing set (800 images).

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 07 July 2026
DOI: 10.47191/ijcsrr/V9-i7-39, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

Model Training Performance and Evaluation

The training of the YOLOv8n model over 50 epochs demonstrated a stable convergence trend. A consistent decrease in box loss and classification loss for both training and validation data can be observed in Figure 1. No indications of overfitting were found during the training process, as the validation curves followed the downward trend of the training curves.

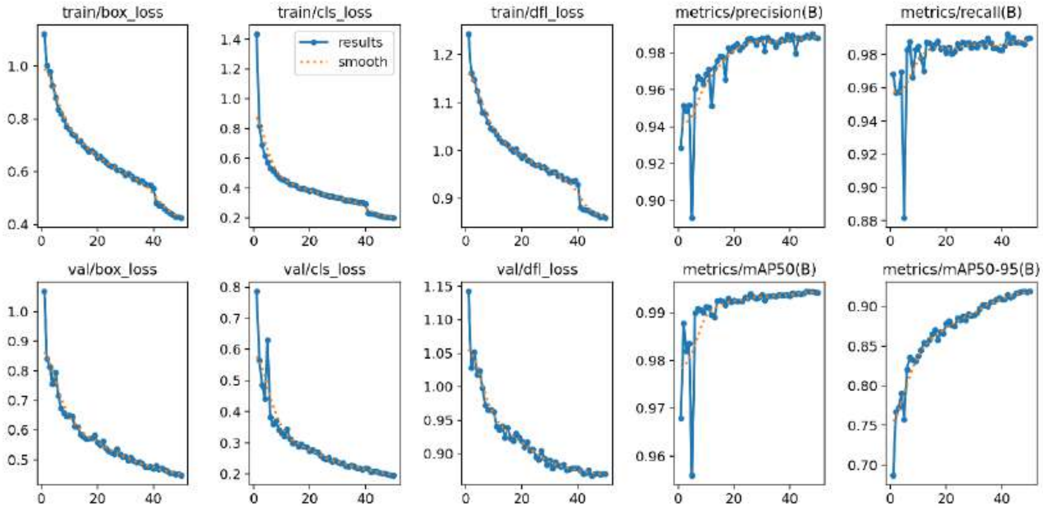

Figure 1. Main Metrics Curves

Based on the final evaluation of the validation dataset, the model achieved the quantitative results presented in Table 1.

Table 1. Summary of YOLOv8n Model Performance Metrics

Metric	Achievement Value
Precision	98.8%
Recall	99.0%
mAP50	99.4%
mAP50-95	91.9%

The balance between precision and recall for both classes is illustrated through the Precision-Recall Curve in Figure 2, which shows an Area Under Curve (AUC) approaching the maximum value.

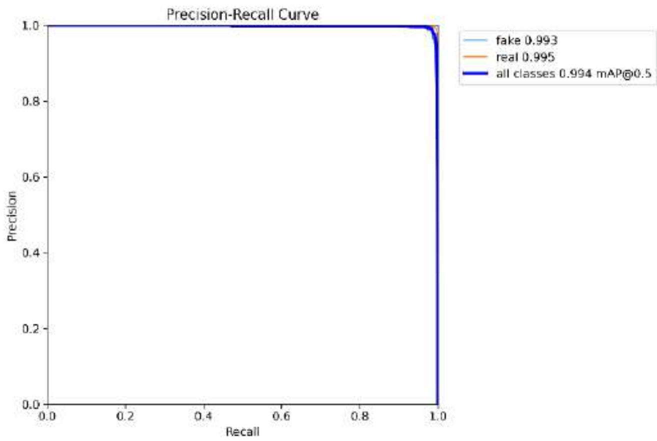

Figure 2. Precision-Recall Curve

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 07 July 2026
DOI: 10.47191/ijcsrr/V9-i7-39, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

Per-Class Classification and Detection Analysis

Detailed accuracy for each class was analyzed using the Confusion Matrix presented in Figure 3. The testing results show that the model achieved an accuracy of 100% for the real face class and 99% for the fake face class. There was only a 1% misclassification rate where fake faces were detected as background.

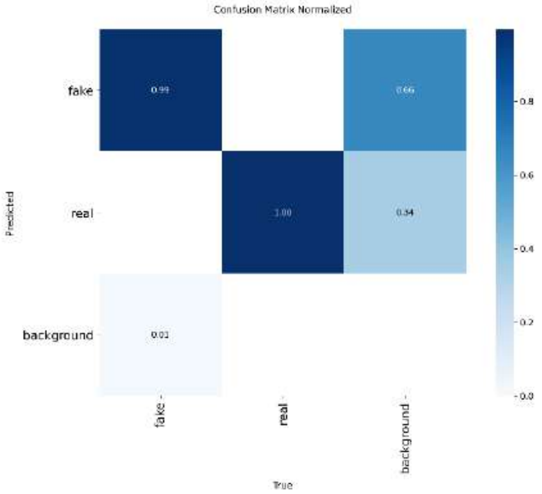

Figure 3. Confusion Matrix

Real-Time Performance and Hardware Implementation

Inference testing results demonstrated high computational efficiency, with an average processing time of 1.7 milliseconds per image. When implemented on hardware, the system was capable of operating at an average speed of 20 FPS (Frames Per Second).

Visualization of detection results in real-world conditions shows the system's ability to instantly provide a "real" label with a green frame and a "fake" label with a red frame, as shown in Figure 4. The final model has a very compact size of 6.2 MB, with a total of 3,006,038 parameters and a computational load of 8.1 GFLOPs, making it suitable for deployment on resource-constrained edge devices.

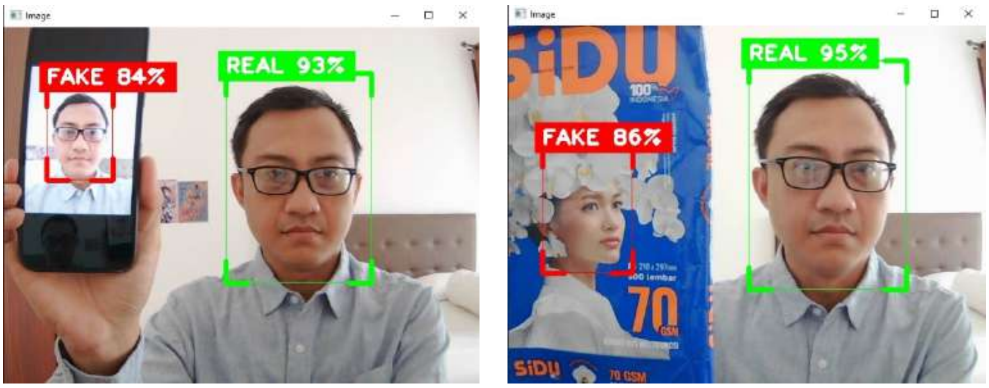

Figure 4. Visualization of Detection Results

DISCUSSION

The results of this research indicate that the implementation of the YOLOv8n architecture for liveness detection provides a significant performance enhancement compared to previous studies. The developed model achieved an mAP50 of 99.4% with a precision rate of 98.8% and a recall of 99.0%. This achievement exceeds the accuracy ranges reported in earlier literature, which were between 79% and 98%. This high accuracy can be attributed to the use of transfer learning techniques on the pre-trained YOLOv8n model combined with a high-quality independent dataset of 8,000 images. Unlike manual feature extraction methods (1) or the use of standard CNNs (2–5, 7, 9, 11, 12) which often require substantial computational power or multi-pass processing, YOLOv8n is capable of processing the entire image in a single neural network pass, resulting in faster detection without sacrificing accuracy.

These findings advance the security practices of attendance systems by proving that a very high security level (>99%) can be achieved in real-time. The use of an independently collected dataset with strict blur detection filtering and a high confidence score (0.8) proved effective in minimizing false positives. This provides a practical solution for organizations requiring an attendance system robust against spoofing attacks using photos, mobile screens, or printed media.

The primary strength of this study lies in the balance between detection accuracy and resource efficiency. The resulting model is highly compact, measuring only 6.2 MB, yet extremely responsive with an inference speed of 1.7 milliseconds per image. The system's ability to operate at an average of 20 FPS on NVIDIA Jetson Nano edge devices confirms the feasibility of implementation on low-power hardware. This represents a significant advancement over research that focused solely on accuracy in desktop computer environments (2, 3, 10, 13). However, this study also has limitations, as the dataset used is still restricted to laboratory environments and may require more extreme variations in lighting conditions as well as a broader variety of spoofing device types to enhance robustness in dynamic, real-world operational environments.

The implication of this research is the availability of a prototype ready to be integrated into existing facial attendance system infrastructures to prevent attendance manipulation. For future research, it is recommended to expand the dataset with more complex facial pose variations and explore continuous learning mechanisms so the model can automatically adapt to new, evolving spoofing techniques. Additionally, the integration of extra security features such as multi-factor authentication could be considered to create a more comprehensive biometric security ecosystem.

CONCLUSION

This research successfully developed a liveness detection security system based on the YOLOv8n architecture to mitigate spoofing attacks in facial attendance systems. Based on the evaluation results, the developed model achieved very high performance, with an mAP50 of 99.4%, precision of 98.8%, and recall of 99.0%.

The primary contribution of this study is the provision of a face authenticity detection solution that is not only highly accurate in distinguishing between real faces and fake faces but is also optimal for real-time implementation. Testing on NVIDIA Jetson Nano hardware confirmed the system's feasibility for operation on low-power hardware with an average speed of 20 FPS. Overall, this research demonstrates that the integration of the YOLOv8n algorithm is capable of providing reliable and efficient protection for automated attendance systems against various spoofing attack media.

REFERENCES

1. Srivastava D, Shukla P, Sahani AK. Face Verification System with Liveness Detection. In: 2021 IEEE 18th India Council International Conference (INDICON). 2021. p. 1–5.
2. Koppikar U, Sujatha C, Patil P, Hiremath PS. Face Liveness Detection to Overcome Spoofing Attacks in Face Recognition System. In: Sharma MK, Dhaka VS, Perumal T, Dey N, Tavares JMRS, editors. Innovations in Computational Intelligence and Computer Vision. Singapore: Springer Singapore; 2021. p. 351–60.
3. Koshy R, Mahmood A. Enhanced deep learning architectures for face liveness detection for static and video sequences. Entropy. 2020;22(10):1–27.
4. Zuo Y, Gao W, Wang J. Face Liveness Detection Algorithm based on Livenesslight Network. In: 2020 International Conference on High Performance Big Data and Intelligent Systems (HPBD&IS). 2020. p. 1–5.
5. Mohamed AA, Nagah MM, Abdelmonem MG, Ahmed MY, El-Sahhar M, Ismail FH. Face Liveness Detection Using a sequential CNN technique. In: 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC). 2021. p. 1483–8.
6. Hadiprakoso RB, Setiawan H, Girinoto. Face Anti-Spoofing Using CNN Classifier & Face liveness Detection. In: 2020 3rd International Conference on Information and Communications Technology (ICOIACT). 2020. p. 143–7.
7. Potdar A, Barbhaya P, Nagpure S. Face Recognition for Attendance System using CNN based Liveliness Detection. In: 2022 International Conference on Advances in Computing, Communication and Materials (ICACCM). 2022. p. 1–6.

8. Omara M, Fayez M, Khalid H, Ghoniemy S. A Transfer Learning Approach for Face Liveness Detection. In: 2023 Eleventh International Conference on Intelligent Computing and Information Systems (ICICIS). 2023. p. 122–7.
9. Jafri S, Chawan S, Khan A. Face Recognition using Deep Neural Network with "LivenessNet." In: 2020 International Conference on Inventive Computation Technologies (ICICT). 2020. p. 145–8.
10. Santoso JT, Sediyono E, Hartomo KD, Sembiring I. Optimizing Attendance System : Integrating Liveness Detection and Deep Learning for Reliable Face Recognition. JUITA J Inform. 2024;12(2):207–16.
11. Wei Y, Machica IKD, Dumdumaya CE, Arroyo JCT, Delima AJP. Liveness Detection Based on Improved Convolutional Neural Network for Face Recognition Security. Int J Emerg Technol Adv Eng. 2022;12(8):45–53.
12. Garg S, Mittal S, Kumar P, Anant Athavale V. DeBNet: Multilayer Deep Network for Liveness Detection in Face Recognition System. In: 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN). 2020. p. 1136–41.
13. Mandol S, Mia S, Ahsan SMM. Real Time Liveness Detection and Face Recognition with OpenCV and Deep Learning. In: 2021 5th International Conference on Electrical Information and Communication Technology (EICT). 2021. p. 1–6.
14. Surantha N, Sugijakko B. Lightweight face recognition-based portable attendance system with liveness detection. Internet of Things (Netherlands) [Internet]. 2024;25(January):101089. Available from: https://doi.org/10.1016/j.iot.2024.101089
15. Zhang Y, Zheng L, Thing VLL, Zimmermann R, Guo B, Yu Z. FaceLivePlus: A Unified System for Face Liveness Detection and Face Verification. In: Proceedings of the 2023 ACM International Conference on Multimedia Retrieval [Internet]. New York, NY, USA: Association for Computing Machinery; 2023. p. 144–152. (ICMR '23). Available from: https://doi.org/10.1145/3591106.3592289

Cite this Article: Duta Nugraha, I.P.E., Setiawan, W. (2026). Implementation of YOLOv8n-Based Liveness Detection to Enhance the Security of Facial Attendance Systems Against Real-Time Spoofing Attacks. International Journal of Current Science Research and Review, 9(7), pp. 3980-3985. DOI: https://doi.org/10.47191/ijcsrr/V9-i7-39