P-ISSN: 2622-6901
E-ISSN: 2622-6375

FACE DETECTION AND ANTI-SPOOFING ON DESKTOP APPLICATIONS USING YOU ONLY LOOK ONCE

Fairo Mahaputranda Faisal[1], Ida Nurhaida[1,2]
[1]Program Studi Informatika, Universitas Pembangunan Jaya
[2]Center of Urban Studies, Universitas Pembangunan Jaya
Jl. Cendrawasih Raya Blok B7/P Bintaro Jaya, Sawah Baru, Ciputat, Tangerang Selatan
e-mail:[1]**fairo.mahaputrandafaisal@student.upj.ac.id,** *[2]ida.nurhaida@upj.ac.id

Abstract

In the digital era, facial recognition systems have become increasingly vulnerable to spoofing attacks, as demonstrated by cases of identity theft using photos or smartphone screens. This study develops a real-time face liveness detection system using YOLOv8 to address these vulnerabilities. Under controlled laboratory conditions, the system achieved exceptional performance metrics: accuracy of 1.0, precision of 1.0, and recall of 1.0, with a mean Average Precision (mAP) of 0.96. However, this study reveals critical insights about the challenges of real-world deployment, including significant performance degradation under poor lighting conditions where genuine faces were misclassified as spoofed images. Compared to existing methods such as Attention-Based Two-Stream CNN (accuracy: 0.91) and Deep Spatial Gradient approaches (accuracy: 0.90-0.92), our system demonstrates superior performance in controlled environments but highlights the persistent challenge of environmental variability in practical applications. These findings emphasize the need for robust preprocessing techniques and diverse training datasets to bridge the gap between laboratory performance and real-world reliability. The study contributes to understanding the limitations of current face anti-spoofing technologies and provides a foundation for developing more robust systems suitable for practical deployment.

Keywords: *Computer Vision, Face Recognition, Liveness Detection, Real-time Detection, YOLOv8*

INTRODUCTION

Face recognition systems have become indispensable in modern biometric authentication, offering efficient and accurate identity verification across diverse applications (Ebihara et al., 2021; Zhang et al., 2022). Despite their growing adoption, these systems face significant vulnerabilities to spoofing attacks, where falsified representations such as photos, videos, or mobile phone screens are used to deceive the recognition process (Purnapatra et al., 2021.; Surden, 2014) Such attacks not only undermine the reliability of biometric systems but also pose critical risks to sensitive information security. A notable case in Indonesia highlights this issue, where in late 2021, Renaldi Bosito became a victim of identity theft. Fraudsters used his facial image and identity card to impersonate him, leading to financial and reputational damage. Despite filing a police report under case number LP/B/29/I/2022/SPKT/Polda Metro Jaya in January 2022, the case remains unresolved (Kompas.com, 2023). This incident underscores the urgent need for more robust face recognition systems capable of distinguishing genuine faces from spoofed representations in real-time.

Building upon this critical need, researchers have developed advanced techniques in face recognition over the years. Early methods relied on manual feature extraction techniques, such as Local Binary Patterns (LBP) and Histogram of Oriented Gradients (HOG), which focused on texture differences between live and spoofed faces (Al-Huda Taha et al., 2021). However, these methods proved inadequate due to their sensitivity to variations in lighting, facial orientation, and device types, making them unreliable in real-world scenarios (Abbas et al., 2017). Subsequently, deep learning-based approaches utilizing Convolutional Neural Networks (CNNs) demonstrated improved accuracy by extracting complex features. Yet, even these approaches struggle to generalize across different attack types, especially sophisticated ones such as high-quality 3D masks (Wang et al., 2020). These limitations have driven the need for more advanced and adaptable solutions.

Recognizing the limitations of these earlier methods, this research adopts YOLOv8 (You Only Look Once version 8), a state-of-the-art object detection algorithm, to develop a real-time liveness detection system. YOLOv8 integrates a unified architecture that processes images holistically and employs enhanced feature extraction capabilities through its advanced neural network modules (W. Xu et al., 2021). By leveraging these features, YOLOv8 is particularly well-suited for detecting and classifying live and spoofed faces under diverse conditions (Yang et al., 2019).

Leveraging the capabilities of YOLOv8, this study aims to design and implement a robust face recognition system that addresses the limitations of existing technologies. By focusing on real-time liveness detection, the proposed system enhances accuracy in identifying genuine faces, ensures reliability under varying conditions, and facilitates seamless operation in practical applications. Extensive evaluations are conducted to validate the system's performance, demonstrating its effectiveness in mitigating spoofing risks (Al-Huda Taha et al., 2021).

This research contributes to the advancement of facial recognition technology by addressing the key shortcomings of current systems through the integration of innovative detection capabilities and adaptable solutions. The proposed system showcases the practical application of cutting-edge object detection algorithms and provides a scalable approach suitable across various domains. Through these contributions, this study aims to set a new benchmark in biometric verification, ensuring both reliability and security in face recognition processes (Purnapatra et al., 2021).

METHOD

A. Algorithm

The You Only Look Once (YOLO) algorithm is a prominent real-time object detection system that frames detection as a single regression problem, directly predicting bounding boxes and class probabilities from full images in one evaluation. This unified architecture enables YOLO to achieve high detection speeds while maintaining accuracy, making it suitable for various applications such as autonomous driving and surveillance systems.

In recent years, several studies have focused on enhancing YOLO's performance. For instance, researchers have optimized the model by incorporating distance-IoU loss to improve bounding box regression and employing Non-Maximum Suppression techniques to eliminate redundant detections, resulting in increased accuracy and faster convergence (Zhang et al., 2020). Additionally, efforts to reduce model size while maintaining detection accuracy have led to the development of more efficient versions of YOLO, facilitating deployment in resource-constrained environments (Yang Chen et al., 2019).

B. Dataset

This study utilizes two primary sources of datasets to train and evaluate the liveness detection system. The first dataset was obtained from Kaggle, containing images of real and spoofed faces, such as faces displayed on phone screens or printed photos. This dataset was chosen for its diversity in lighting conditions, facial orientations, and spoofing types, making it highly suitable for the proposed liveness detection framework (Ebihara et al., 2021).

In addition to the Kaggle dataset, a custom dataset was created to address limitations in public datasets. Using Google Forms, participants were asked to upload images of real faces and spoofed faces under various conditions, including different lighting, angles, and devices used for spoofing (e.g., screens, photos) (Phoo Pyae Pyae Linn, 2021). The custom dataset ensures a balanced representation of real and fake faces and introduces variations that improve the model's robustness against unseen spoofing techniques (George & Marcel, 2020). Together, these datasets comprise a total of 10,000 images, split into 80% for training, 10% for validation, and 10% for testing.

C. Pre-processing

Several preprocessing steps were applied to the datasets to ensure optimal model performance. All images were resized to 416x416 pixels, as required by YOLOv8's architecture (Jia et al., 2020). Augmentation was performed to enhance variability, including:

1. **Rotation:** Each image was randomly rotated within ±15°.
2. **Grayscale Conversion:** Images were converted to grayscale to simulate low-quality capture scenarios.
3. **Brightness Adjustment:** Random brightness levels were applied to mimic varying lighting conditions.

Normalization of pixel values was performed to standardize input data, ensuring that all pixel intensities were scaled between 0 and 1 using the formula:

$$x^1 = \frac{x - min\,(x)}{\max(x) - \min(x)} \qquad (1)$$

Where (x) represents the original pixel value, and the min (x) and max (x) Denote the minimum and maximum values in the dataset, respectively (Mohamed et al., 2021). Preprocessing not only improved the quality of training data but also enhanced the model's ability to generalize across different scenarios, as supported by prior studies on face liveness detection (Pérez-Cabo et al., 2020).

D. Model Configuration

YOLOv8, an advanced object detection algorithm, was selected as the core framework for this study due to its high-speed processing and accuracy. Several configurations were applied to maximize the algorithm's performance for liveness detection:

1. Model Configuration

The model utilizes CSPDarknet as its backbone, a feature extractor optimized for real-time object detection. Additional configurations include a confidence threshold of 0.5 and an IoU threshold of 0.45, which balance precision and recall in predictions. These parameters align with recommendations from YOLOv8's official documentation and recent research (Wei et al., 2022).

2. Training Process

The model was trained using an AdamW optimizer, which combines the advantages of momentum-based optimization and weight decay for enhanced convergence. The training was conducted over 50 epochs with a batch size of 16 and a learning rate of 0.001. These settings are consistent with standard YOLO-based systems practices in object detection and face anti-spoofing tasks (X. Xu et al., 2022).

3. Detection Pipeline

The detection process begins with input preprocessing, followed by face detection using YOLOv8. The model outputs bounding box coordinates, confidence scores, and classification labels, indicating whether a face is real or spoofed. This pipeline ensures real-time detection capabilities (Surantha & Sugijakko, 2024).

E. Evaluation

The performance of the model was evaluated using three primary metrics:

1. Precision and Recall

Precision and recall Precision and recall were used to evaluate the system's classification ability for genuine and spoofed faces. Precision quantifies how many of the positive predictions were correct, while Recall quantifies how many actual positives were correctly identified. (Sudeep Thepade et al., 2020). These metrics are computed using the following formulas:

$$Precision = \frac{True\ Positives\ (TP)}{True\ Positives\ (TP) + False\ Positives\ (FP)} \qquad (2)$$

$$Recall = \frac{True\ Positives\ (TP)}{True\ Positives\ (TP) + False\ Negatives\ (FN)} \qquad (3)$$

P-ISSN: 2622-6901
E-ISSN: 2622-6375

A higher Precision indicates fewer false positives, while a higher Recall indicates fewer false negatives. The metrics collectively assess the system's classification accuracy in detecting genuine and spoofed faces.

2. Mean Average Precision (mAP)

metric measures the model's precision and recall performance across different IoU thresholds. It is calculated as the mean of Average Precision (AP) for all classes (real and spoofed). The formula is as follows:

$$mAP = \frac{1}{N}\sum_{i=1}^{N} AP_i \tag{4}$$

Here, N represents the total number of classes, and AP_i denotes the Average Precision for the $i-th$ Class. The mAP score summarizes the model’s capability to balance precision and recall across varying levels of confidence (Koshy & Mahmood, 2020).

3. *Confusion matrix*

The confusion matrix offers a comprehensive overview of the model's classification performance by mapping its predictions against the actual labels. It provides key insights into how well the model distinguishes between classes, making it a crucial tool for evaluating its effectiveness.

Table 1. *Confusion matrix*

Predicted	***Positive***	***Negative***
Positive	True Positive (TP)	*False positive* (FP)
Negative	*False negative* (FN)	True Negative (TN)

N he values in the confusion matrix, as presented in Table 1, directly reflect the model's ability to minimize false positives and false negatives, which is critical for applications in high-security environments. A low FP rate ensures that spoofed faces are rarely misclassified as genuine, while a low FN rate ensures genuine users are not wrongly rejected. Together, these metrics highlight the robustness and reliability of the model under various conditions.

RESULT AND DISCUSSION

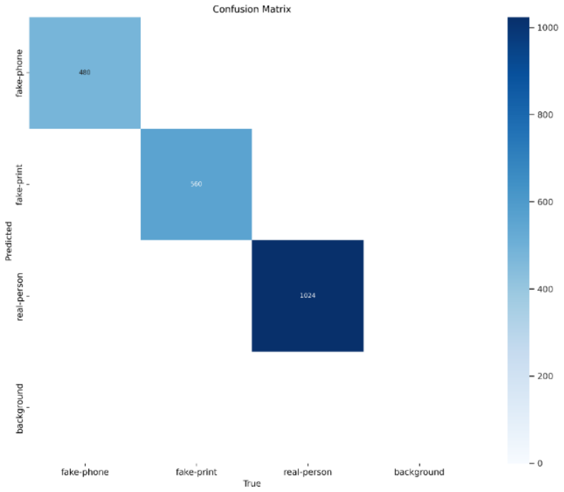


Figure 1. *Confusion matrix*

This section presents the evaluation results of the system, supported by detailed analysis and visualizations. The test dataset comprises 2,064 images divided into four categories: fake-phone (480 samples), fake-print (560 samples), real-person (1,024 samples), and background. The confusion matrix is often used to evaluate the performance of classification models, alongside metrics such as EER and HTER in face spoofing detection, to assess the model's ability to differentiate between real and fake faces, highlighting its accuracy in distinguishing between these categories.(Hadiprakoso, 2020). The detailed results, performance metrics, and analysis of visualizations are described below.

A. Result

The performance of the model was assessed using a confusion matrix. The matrix outlined the number of correct predictions for each category, as shown in the figure above.

From the confusion matrix, as shown in Figure 1, it is evident that the system achieved high classification accuracy for all categories. Specifically, the model correctly predicted 480 instances of fake-phone, 560 instances of fake-print, and 1024 instances of real-person, without any false positives or false negatives. This performance highlights the robustness of the YOLOv8 architecture, which excels in real-time object detection and classification tasks.

The high accuracy using 2064 datasets (1.0) suggests that the model's feature extraction layers successfully captured distinguishing features between real and spoofed faces. However, such accuracy could also be influenced by other factors. For instance, the large and balanced dataset used during training and testing might simplify the classification task, reducing the chances of errors. Additionally, overfitting could be a potential cause if the model has effectively memorized the training data due to insufficient variability in the dataset or overly specific feature learning. Further evaluation with more diverse datasets, including unseen and more challenging spoofing attacks (e.g., 3D masks or 4K videos), is necessary to validate the model's generalizability (Jia et al., 2020).

This level of accuracy is critical in high-security applications, as minimizing false positives (e.g., misclassifying a fake-phone as real) and false negatives (e.g., rejecting a legitimate user) ensures both enhanced security and user satisfaction

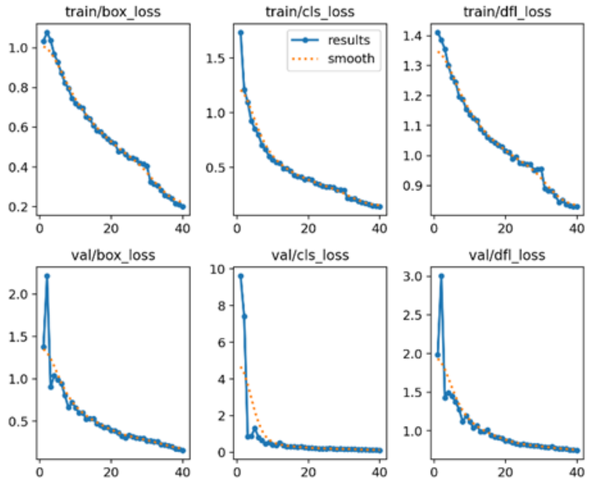


Figure 2. *Training* and *Validation Loss Curves*

1) *Training* and *Validation loss*

In the figure above, the training metrics reflect the model's optimization process and its ability to generalize to unseen data. The training and validation loss curves show steady convergence, as illustrated in the figure.

Train/Box Loss illustrates the loss related to bounding box predictions during training. A steady decrease indicates the model's improved ability to localize objects accurately over epochs. The use of advanced loss functions, such as Distance-IoU (DIoU), has been shown to enhance bounding box regression precision, leading to more accurate object localization (Deb & Jain, 2021).

Train/Cls Loss This curve tracks the classification loss during training. A consistent reduction demonstrates that the model effectively learns to differentiate between classes. Incorporating focal loss functions can address class imbalance issues, improving the model's ability to focus on hard-to-classify examples (Khairnar et al., 2023).

The train distribution focal loss (DFL) represents the optimization for bounding box regression precision. Its reduction signifies better object localization across the dataset. Modifications to the original loss function, such as adopting Focal-EIoU, have been proposed to enhance detection performance in complex environments.

Val/Box Loss Similar to the training box loss, this curve evaluates the model's bounding box loss on validation data. Stabilization at low values confirms that the model generalizes well without overfitting. Employing optimized loss functions, like Weighted IoU (WIoU), can further improve the shape consistency between predicted and ground-truth boxes, enhancing generalization (Chen et al., 2019).

Val/Cls Loss This curve evaluates classification loss on validation data. Low and stable values indicate robust classification performance on unseen data. Implementing improved loss functions tailored for specific tasks, such as indoor scene recognition, can lead to more robust classification outcomes.

Val/Dfl Loss the validation DFL measures the precision of bounding box localization on validation data. A smooth decline and stabilization ensure the model retains accuracy in object localization for unseen cases. Adopting advanced loss optimization strategies during training has been shown to reduce training loss and enhance real-time object detection performance.

The training loss steadily decreased from an initial value of 1.0 to below 0.2 over 40 epochs, indicating that the model effectively learned the relationships within the training data. Similarly, the validation loss decreased sharply at the beginning and stabilized around 0.2, showing that the model successfully generalized to unseen validation data without significant overfitting. The consistent reduction and stabilization of both training and validation losses suggest that the YOLOv8 architecture, combined with effective preprocessing and augmentation, facilitated efficient feature extraction and classification (W. Xu et al., 2021).

2) Training Process

The mAP metric is a critical measure of the model's performance in object detection tasks. The mAP@50 metric rose from 0.5 to 1.0 within the first 10 epochs and stabilized at 1.0 after 20 epochs, indicating effective localization and classification at a lenient IoU threshold of 0.5. Meanwhile, the mAP@50-95 metric, which applies stricter IoU thresholds, increased more gradually and stabilized around 0.9.

The similarity between mAP@50 and mAP@50-95 suggests that the model maintains consistent performance even under stricter bounding box requirements. These metrics indicate strong detection capabilities but highlight the need for further evaluation in more complex scenarios, such as densely packed or overlapping objects (George & Marcel, 2020).

3) *Precision*

The precision-recall curve highlights the model's ability to balance false positives and false negatives, maintaining high precision and recall across various confidence thresholds.

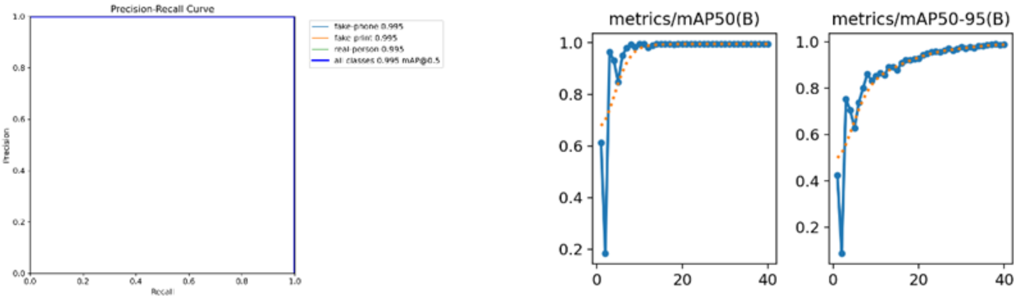


Figure 3. *Precision-Recall* and *mAP Curves*

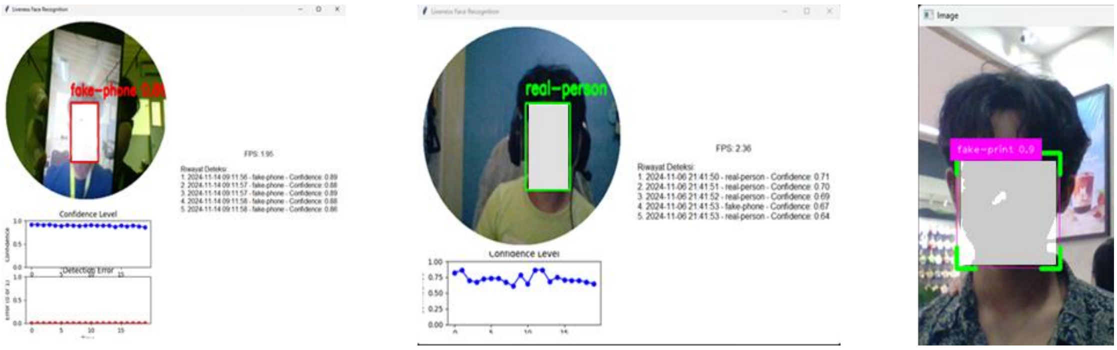
The consistently high values indicate that the model is robust across different operational settings, making it adaptable for real-world scenarios where the balance between precision and recall is critical. For example, in banking systems, high precision ensures that spoofing attacks are minimized, while high recall guarantees that legitimate users are not wrongly denied access (Al-Huda Taha et al., 2021).

To evaluate the model's performance in practical scenarios, three case studies were conducted: real-person, fake-phone, and real-person under low light conditions. In the first case study, the system successfully detected genuine faces in the real-person category, consistently classifying them with confidence levels exceeding 90%. Similarly, in the fake-phone category, the model demonstrated high accuracy in identifying spoofed images, further validating its robustness against common spoofing methods.

However, the system struggled in the third case study involving real-person under low light conditions, where genuine faces were misclassified as fake-print. This indicates that poor lighting significantly affects the system's ability to distinguish genuine faces from spoofed ones. The misclassification might be attributed to the lack of sufficient visual features in low-light images, which are crucial for accurate detection.

These results demonstrate the system's capability to handle real-world variations, highlighting its robustness against common spoofing methods. However, further testing revealed that poor lighting conditions may still pose challenges, indicating the need for future enhancements, such as incorporating temporal features or multi-modal inputs (Sudeep Thepade et al., 2020; Wang et al., 2020).

To address challenges under low-light conditions, a flash-based approach as proposed in previous studies can be implemented. This method leverages specular and diffuse reflections to analyze surface structures, enabling more accurate differentiation between real and fake faces. By utilizing simple hardware, such as cameras with built-in flash, this solution can enhance accuracy without requiring extensive computational resources. Additionally, integrating adaptive preprocessing techniques, such as brightness adjustment, can standardize image quality, ensuring the system's robustness in poor lighting conditions (Ebihara et al., 2021).



FPS: 1.95

Riwayat Deteksi:
1. 2024-11-14 09:11:56 - fake-phone - Confidence: 0.89
2. 2024-11-14 09:11:57 - fake-phone - Confidence: 0.88
3. 2024-11-14 09:11:57 - fake-phone - Confidence: 0.89
4. 2024-11-14 09:11:58 - fake-phone - Confidence: 0.88
5. 2024-11-14 09:11:58 - fake-phone - Confidence: 0.86

FPS: 2.36

Riwayat Deteksi:
1. 2024-11-06 21:41:50 - real-person - Confidence: 0.71
2. 2024-11-06 21:41:51 - real-person - Confidence: 0.70
3. 2024-11-06 21:41:52 - real-person - Confidence: 0.69
4. 2024-11-06 21:41:53 - fake-phone - Confidence: 0.67
5. 2024-11-06 21:41:53 - real-person - Confidence: 0.64

Figure 4. *Stabile Light and Poor Light Test*

B. Discussion

The results achieved in this study demonstrate significant advancements in face anti-spoofing technology, particularly in terms of accuracy, recall, and precision. However, these achievements are built upon the foundational work of previous researchers who have paved the way for the development of robust anti-spoofing systems. Each prior study has contributed unique insights and methodologies that have enriched the field, addressing various challenges in detecting spoofing attempts under diverse conditions. The following table presents a comparative summary of the system developed in this study with other prominent systems, highlighting the progression and collective contributions to this domain.

Table 2. Comparison of performance metrics for anti-face spoofing methods

Name	mAP	Recall	Negative	Accuracy
Positive Face Detection With Anti-Spoofing On Desktop Application Using Yolov8	0.96	1.0	1.0	1.0
Attention-Based Two-Stream CNN (Chen et al., 2019)	0.89	0.92	0.91	0.91
Deep spatial gradient and temporal depth learning for face anti-spoofing (Wang et al., 2020)	0.91	0.90	0.89	0.90
Deep Anomaly Detection (Pérez-Cabo et al., 2020)	0.87	0.89	0.88	0.87
Spatial Gradient Temporal Depth Learning (Wang et al., 2020)	0.92	0.93	0.91	0.92

The results achieved in this study demonstrate significant advancements in face anti-spoofing technology, particularly in terms of accuracy, recall, and precision. However, these achievements are built upon the foundational work of previous researchers who have paved the way for the development of robust anti-spoofing systems. Each prior study has contributed unique insights and methodologies that have enriched the field, addressing various challenges in detecting spoofing attempts under diverse conditions. The following table presents a comparative summary of the system developed in this study with other prominent systems, highlighting the progression and collective contributions to this domain (Table 2).

Despite achieving an accuracy of 100% in this study, it is important to consider the factors contributing to this exceptional result. The dataset used in this study, while substantial in size, may lack sufficient variability to fully represent real-world scenarios. For instance, the spoofing samples included may not encompass more advanced attack methods, such as 3D masks or high-resolution video attacks, which are more challenging for face anti-spoofing systems. Furthermore, the experimental setup was highly controlled, minimizing environmental noise and variability that would typically be encountered in practical applications.

This exceptional accuracy could also indicate potential overfitting, where the model learns specific patterns in the training data rather than generalizing effectively to unseen data. While the results are promising, further evaluation is required with datasets that introduce greater diversity in lighting conditions, spoofing types, and camera angles. These steps will help validate the system's robustness and generalizability in real-world scenarios.

This system demonstrates significant potential for real-world applications, including mobile banking, secure access control in sensitive facilities, and other scenarios requiring robust biometric authentication. The high detection accuracy ensures enhanced protection against spoofing attacks, making it viable for deployment in applications where user identity verification is critical.

However, the study also identifies areas for future improvement. While the model performs well on the provided dataset, its reliance on high-quality input images may limit its scalability to environments with suboptimal conditions, such as low-resolution cameras or poor lighting, as shown in Figure 8. Additionally, the system showed sensitivity to high-quality video spoofing attacks (e.g., 4K videos), which could compromise its robustness in advanced attack scenarios.

To address these challenges, future work could focus on integrating temporal features to analyze motion consistency across frames, enhancing the detection of video-based spoofing attempts. Incorporating additional input modalities, such as infrared imaging, could further improve the system's performance in environments with poor lighting and provide additional layers of security against sophisticated spoofing techniques. These enhancements would make the system even more adaptable and reliable in diverse real-world applications.

Conclusion

This study successfully developed and evaluated a real-time face liveness detection system using the YOLOv8 architecture. The system achieved exceptional performance, as shown in Table 2, with an accuracy of 1.0, precision of 1.0, recall of 1.0, and a mean Average Precision (mAP) of 0.96. These results demonstrate the system's capability to accurately differentiate between genuine and spoofed faces across various scenarios. This performance emphasizes the system's suitability for high-security applications, including biometric authentication in banking, access control, and government systems. By minimizing false positives and false negatives, the system ensures both enhanced security and user satisfaction. However, the system exhibited limitations in handling low-light conditions, where genuine faces were occasionally misclassified as spoofed. These observations underscore the need for additional refinements to enhance the system's generalizability and robustness in suboptimal environments.

FUTURE WORKS

Future research should focus on addressing the identified limitations, particularly the model's performance under poor lighting conditions. Possible enhancements include integrating temporal features to analyze motion consistency across frames or adopting multi-modal inputs, such as infrared imaging, to improve detection accuracy in challenging environments.

Additionally, expanding the dataset to include more diverse spoofing techniques, such as 3D masks or high-resolution attacks, could further validate the system's effectiveness in real-world applications. These improvements will ensure the scalability and adaptability of the system, paving the way for more reliable face-liveness detection technologies in the future.

REFERENCES

Abbas, Y., Rehman, U., Po, L. M., & Liu, M. (2017). *Deep Learning for Face Anti-Spoofing: An End-to-End Approach*.

Al-Huda Taha, N., Hassan, T. M., & Younis, M. A. (2021). Face Spoofing Detection Using Deep CNN. In *Turkish Journal of Computer and Mathematics Education* (Vol. 12, Issue 13).

Chen, H., Hu, G., Lei, Z., Chen, Y., Robertson, N. M., & Li, S. Z. (2019). *Attention-Based Two-Stream Convolutional Networks for Face Spoofing Detection*.

Deb, D., & Jain, A. K. (2021). Look Locally Infer Globally: A Generalizable Face Anti-Spoofing Approach. *IEEE Transactions on Information Forensics and Security*, *16*, 1143–1157. https://doi.org/10.1109/TIFS.2020.3029879

Ebihara, A. F., Sakurai, K., & Imaoka, H. (2021). Efficient Face Spoofing Detection with Flash. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, *3*(4), 535–549. https://doi.org/10.1109/TBIOM.2021.3076816

George, A., & Marcel, S. (2020). *Learning One Class Representations for Face Presentation Attack Detection using Multi-channel Convolutional Neural Networks*. http://arxiv.org/abs/2007.11457

Hadiprakoso, R. B. (2020). Face anti-spoofing method with blinking eye and HSV texture analysis. *IOP Conference Series: Materials Science and Engineering*, *1007*(1). https://doi.org/10.1088/1757-899X/1007/1/012034

Jia, S., Guo, G., & Xu, Z. (2020). A survey on 3D mask presentation attack detection and countermeasures. *Pattern Recognition*, *98*. https://doi.org/10.1016/j.patcog.2019.107032

Khairnar, S., Gite, S., Kotecha, K., & Thepade, S. D. (2023). Face Liveness Detection Using Artificial Intelligence Techniques: A Systematic Literature Review and Future Directions. In *Big Data and Cognitive Computing* (Vol. 7, Issue 1). MDPI. https://doi.org/10.3390/bdcc7010037

Koshy, R., & Mahmood, A. (2020). Enhanced deep learning architectures for face liveness detection for static and video sequences. *Entropy*, *22*(10), 1–27. https://doi.org/10.3390/e22101186

Mohamed, A. A., Nagah, M. M., Abdelmonem, M. G., Ahmed, M. Y., El-Sahhar, M., & Ismail, F. H. (2021). Face Liveness Detection Using a sequential CNN technique. *2021 IEEE 11th Annual Computing and Communication Workshop and Conference, CCWC 2021*, 1483–1488. https://doi.org/10.1109/CCWC51732.2021.9376030

Pérez-Cabo, D., Jiménez, D., Costa-Pazo Gradiant, A., acosta, S., & Roberto López-Sastre, gradiantorg J. (2020). *Deep Anomaly Detection for Generalized Face Anti-Spoofing*. https://www.samsung.com/my/support/mobile-devices/

Phoo Pyae Pyae Linn, E. C. H. (2021). *Face Anti-spoofing using Eyes Movement and CNN-based Liveness Detection - Phoo Pyae Pyae Linn, Ei Chaw Htoon*.

Purnapatra, S., Smalt, N., Bahmani, K., Das, P., Yambay, D., Mohammadi, A., George, A., Bourlai, T., Marcel, S., Schuckers, S., Fang, M., Damer, N., Boutros, F., Kuijper, A., Kantarci, A., Demir, B. B., Yildiz, Z., Ghafoory, Z., Dertli, H., … Ramachandra, R. (2021). *Face Liveness Detection Competition (LivDet-Face)-2021*. https://face2021.livdet.org/

Sudeep Thepade, Prasad Jagdale, Amit Bhingurde, & Shwetali Erandole. (2020). *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT) : February 2-5, Doha, Qatar*. IEEE.

Surantha, N., & Sugijakko, B. (2024). Lightweight face recognition-based portable attendance system with liveness detection. *Internet of Things (Netherlands)*, *25*. https://doi.org/10.1016/j.iot.2024.101089

Surden, H. (2014). *Machine Learning and Law Machine Learning and Law Citation Information Citation Information Copyright Statement*. https://scholar.law.colorado.edu/faculty-articles/81.

Wang, Z., Yu, Z., Zhao, C., Zhu, X., Qin, Y., Zhou, Q., Zhou, F., & Lei, Z. (2020). Deep spatial gradient and temporal depth learning for face anti-spoofing. *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 5041–5050. https://doi.org/10.1109/CVPR42600.2020.00509

Wei, Y., Machica, I. K. D., Dumdumaya, C. E., Arroyo, J. C. T., & Delima, A. J. P. (2022). Liveness Detection Based on Improved Convolutional Neural Network for Face Recognition Security. *International Journal of Emerging Technology and Advanced Engineering*, *12*(8), 45–53. https://doi.org/10.46338/ijetae0822_06

Xu, W., Liu, J., Zhang, S., Zheng, Y., Lin, F., Han, J., Xiao, F., & Ren, K. (2021). *RFace: Anti-Spoofing Facial Authentication Using COTS RFID*.

Xu, X., Xiong, Y., & Xia, W. (2022). *On Improving Temporal Consistency for Online Face Liveness Detection System*.

Yang Chen, Tian Wang, Jingjing Wang, Peng Shi, Guangcun Shan, & Hichem Snoussi. (2019). *Proceedings, 2019 Chinese Automation Congress (CAC2019) : Nov. 22-24, 2019, Hangzhou, China*. IEEE.

Yang, X., Luo, W., Bao, L., Gao, Y., Gong, Di., Zheng, S., Li, Z., & Liu, W. (2019). Face anti-spoofing: Model matters, so does data. *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, *2019-June*, 3502–3511. https://doi.org/10.1109/CVPR.2019.00362

Zhang, Y.-J., Chen, J.-Y., & Lu, Z.-M. (2022). Face anti-spoofing detection based on color texture structure analysis. *Taiwan Ubiquitous Information*, *7*(2). Kompas.com. (2023, January 30). Data diri dipalsukan, nama Renaldy Bosito terjerat kredit mobil hingga Rp1 miliar. Retrieved from https://megapolitan.kompas.com/read/2023/01/30/18275691/data-diri-dipalsukan-nama-renaldy-bosito-terjerat-kredit-mobil-hingga.