

An Intelligent Anti-Spoofing System for Face Recognition Using Machine Learning

Dr. Chinmoy Bharadwaj¹, Dr. Nayeemuddin Ahmed², Dr. Sippee Bharadwaj³

^{1,2}Department of Computer Science, University of Science and Technology, Meghalaya (USTM)

³Department of Business Analytics, International School of Business and Research, Bangalore, India

Abstract-- Face recognition systems are mostly used for authentication in many applications, such as mobile phones, security surveillance and access control. However, these systems are highly open to spoofing attacks, where an attacker can use printed photographs, digital screens, or 3D masks to mislead face recognition models. In this paper a strong anti-spoofing model using YOLO (You Only Look Once), OpenCV, and cvzone to effectively differentiate between real and fake faces in real time. This model engages a deep learning-based approach to analyses facial features and detect spoofing attempts with high accuracy. The dataset is collected and preprocessed using multiple augmentation techniques, ensuring variations in training data. The YOLOv8 model is then trained to detect faces as real or fake, exploiting advanced detection algorithms to increase security. The system is designed to work effectively in real world, providing valid and scalable anti-spoofing measures. Experimental inspection demonstrates significant improvements in detection accuracy compared to old methods, making this approach an effective solution for strengthening biometric authentication systems against spoofing threats. The findings suggest promising applications in secure access systems, financial transactions, and smart surveillance.

Keywords--Face Recognition, Anti-Spoofing, YOLO, OpenCV, Deep Learning, Biometric Security.

I. INTRODUCTION

In today's world biometric identification is the becoming the important factor in security system. Face detection playing a critical role in access control, identity verification, and surveillance applications. Face recognition has become increasingly widespread in consumer and corporate solutions as technology has advanced. Along with the increasing in the technology there is a increasing risk of vulnerability of spoofing attack. These attacks include the use of photos, videos, or masks to mislead recognition systems, this lead to unauthorized access and security issue.

Old anti-spoofing approaches, including as texture analysis, motion-based detection, and frequency analysis, have been examined to solve these issues. These techniques frequently face difficulties with real-time speed, flexibility to changing contexts, and abstraction across different attack. Deep learning-based solutions show considerable potential for addressing these restrictions by leveraging large-scale datasets and feature extraction capabilities.

This study describes a powerful anti-spoofing strategy that uses YOLO, OpenCV, and cvzone to distinguish between real and fake faces. By combining a real-time detection mechanism with deep learning-based categorization, our technique improves the security and reliability of biometric identification systems. The experimental findings show that our technique effectively mitigates spoofing attacks while retaining high detection accuracy and efficiency.

II. LITERATURE REVIEW

P. Kavitha et al.[1] completed a research on spoofing detection in facial recognition systems. They divided spoofing attacks into three categories: 2D image-based (Photo and video attacks) and 3D mask-based. Their findings highlighted the importance of effective anti-spoofing methods, pointing out that even commercial off-the-shelf (COTS) facial recognition systems are vulnerable to spoof attacks, with success rates of up to 70%. They showed creating statically efficient methods that do not require substantial picture storage.

Md. Apu Hosen et al.[2] presented facial recognition-based attendance system with anti-spoofing algorithms. Their method employs the Haar cascade classifier for face detection and the Local Binary Pattern Histogram (LBPH) for identification. They used Difference of Gaussians (DoG) filtering to enhance spoof detection. The study reported an 87% identification accuracy rate but also a 15% false positive rate. It showed a need for better system like email automation.

Aparna Sawant et al.[3] developed a facial identification attendance system with antispoofing mechanisms. Their research showed an eye blinking detection algorithm as a counter measure against spoofing attacks using printed images. By implementing OpenCV and machine learning-based approaches, their system showed enhanced security and efficiency. It reduced the risk of fraud attendance marking in educational institutions.

Minit Chitroda et al.[4] explored deep learning-based anti-spoofing techniques within facial recognition systems. Their study examined multiple plans, including anomaly detection frameworks, multi-domain learning, and liveness detection.

They appraised their model using False Acceptance Rate (FAR) and False Rejection Rate (FRR) metrics, supporting for multimodal fusion ways such as integrating depth sensing and texture analysis for improved security.

Tz-Chia Tseng et al.[5] examined smartphone-based live face authentication using deep learning. Their research focused on identifying spoofing attacks using a convolutional neural network (CNN) trained on augmented data. They compared different architectures such as VGG-16, InceptionNet, and ResNet. It demonstrated that deep learning-based ways can effectively detect 2D presentation attacks like photo and video replay attacks.

Femi Emmanuel Ayo et al.[6] presented a YOLO-based automatic face detection system for security applications. Their work focused on the role of geometric analysis in improving facial recognition accuracy while addressing challenges related to varying lighting conditions and facial expressions. Their results showed that YOLO models could provide real-time face detection with over 80% accuracy. It made them suitable for combination into spoof detection frameworks.

Viktor Dénes Huszár et al.[7] introduced a deep learning approach for spoof detection in human activity recognition (HAR) applications. Their study highlighted the effectiveness of CNN-based models in identifying video play attacks in surveillance environments. By combining real-time detection with HAR systems, they showed improved spoof detection performance, even under conditions with video compression and motion blur.

III. METHODOLOGY

Data Collection

We created a Python-based data gathering module with OpenCV and the CVZone framework. The module collects video frames from a camera and uses a face detector to identify faces in each frame. An offset is introduced to the bounding box to capture a larger region, and a blur detection look at based on the Laplacian variance is used. Only frames with proper focus (i.e., over a set blur threshold) are stored together with normalized face coordinates for labeling..

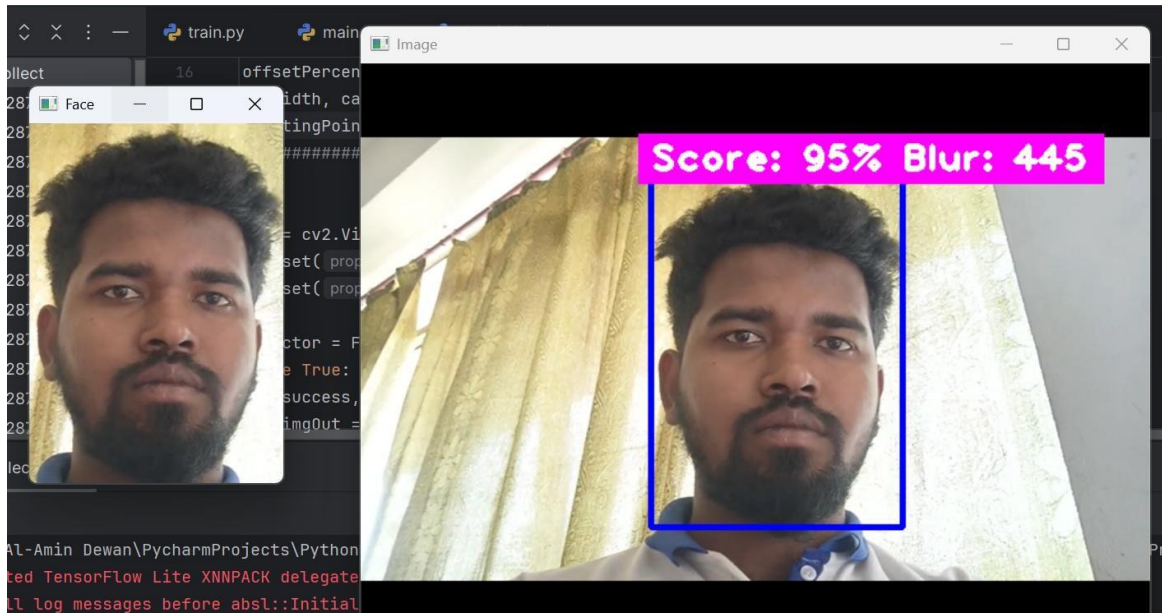


Fig: Data Collection (Image & level Capturing)

Data Splitting

The obtained dataset has been split and divided into three subsets: training, validation, and testing. The file names are randomly generated, and pictures are moved into the selected folders (i.e. train, val, test) for images and labels.

Offline Training

For model training, we employ the YOLO architecture (using a pre-trained YOLOv8 model as the base) and fine-tune it on the prepared dataset.

Real-Time Detection

The trained model is deployed in a real-time application using a webcam feed. The system processes each frame,

predicts the presence of spoof attacks, and overlays bounding boxes and confidence scores. Real-time frame rate (FPS) is calculated to ensure efficient performance:

IV. EXPERIMENTAL RESULTS AND ANALYSIS

Confusion Matrix Analysis

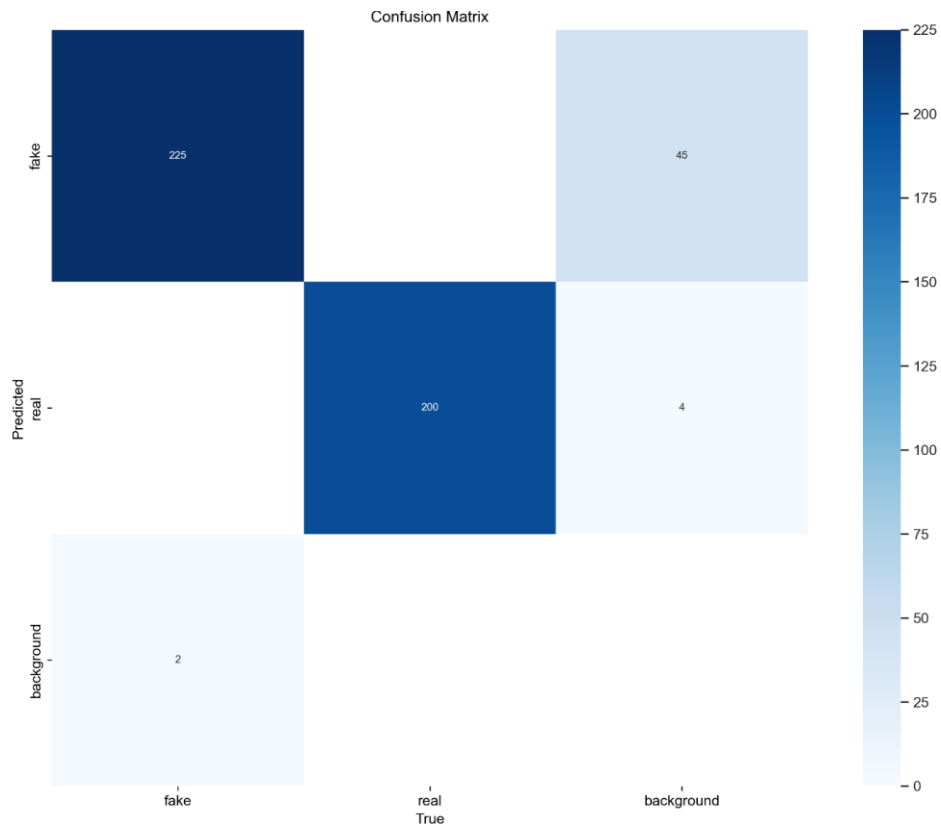


Fig: Confusion Matrix

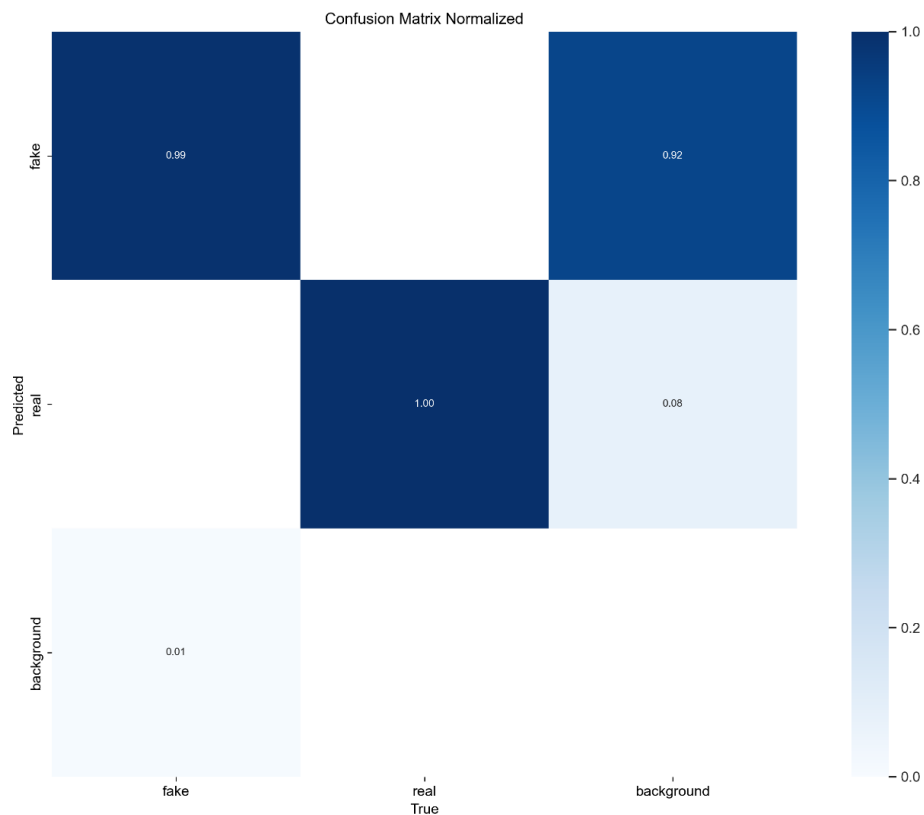


Fig: Normalized Confusion Matrix

Our confusion matrix reveals that most samples are properly identified (diagonal values close to 1.0), indicating good overall accuracy.

F1 and PR Curves:

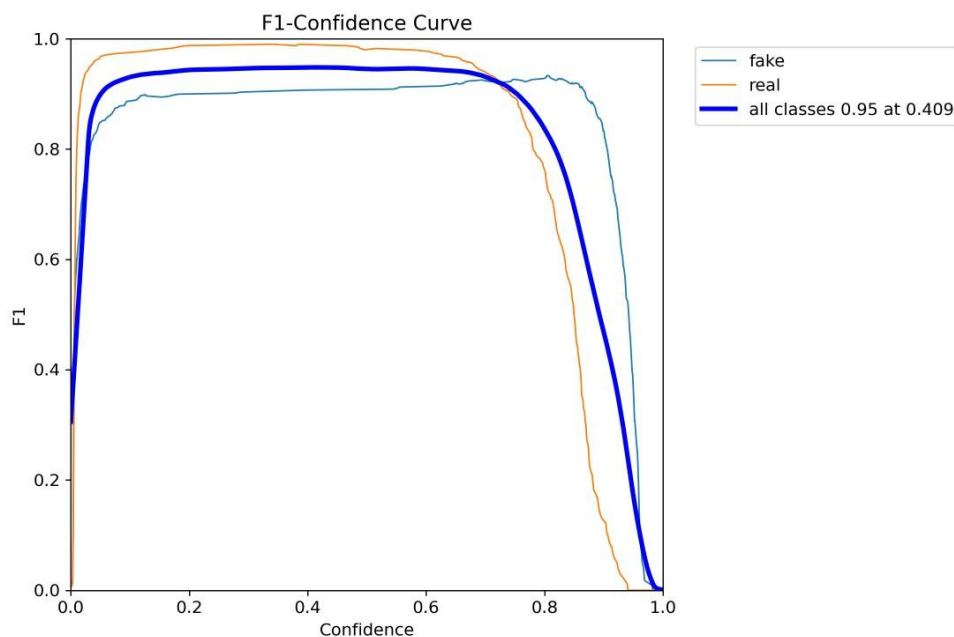


Fig: F1 Confidence Curve

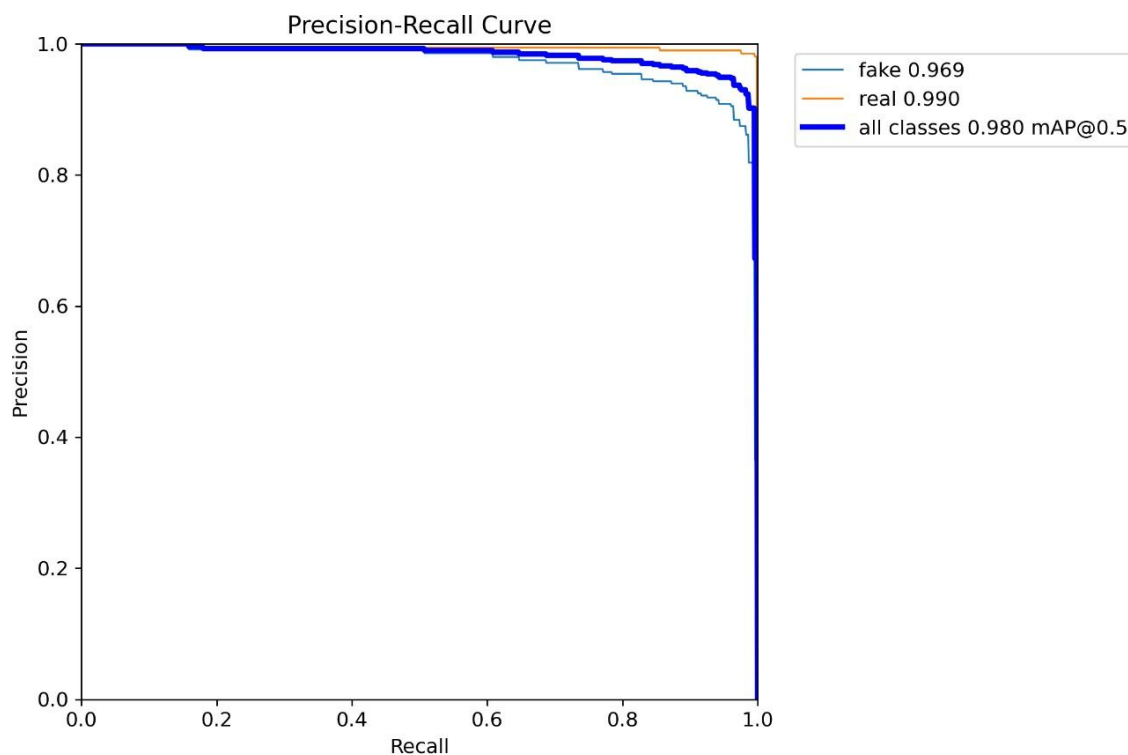


Fig: PR Curve

Fig: F1 Confidence Curve and Fig: PR Curve provide additional performance metrics across varying confidence thresholds. The F1 curve reflects the harmonic balance between precision and recall, indicating that our model

maintains a robust trade-off across the decision boundary. The PR curve further illustrates the model's precision at different recall levels, reinforcing its effectiveness in distinguishing between classes despite imbalanced data.

Qualitative Results:

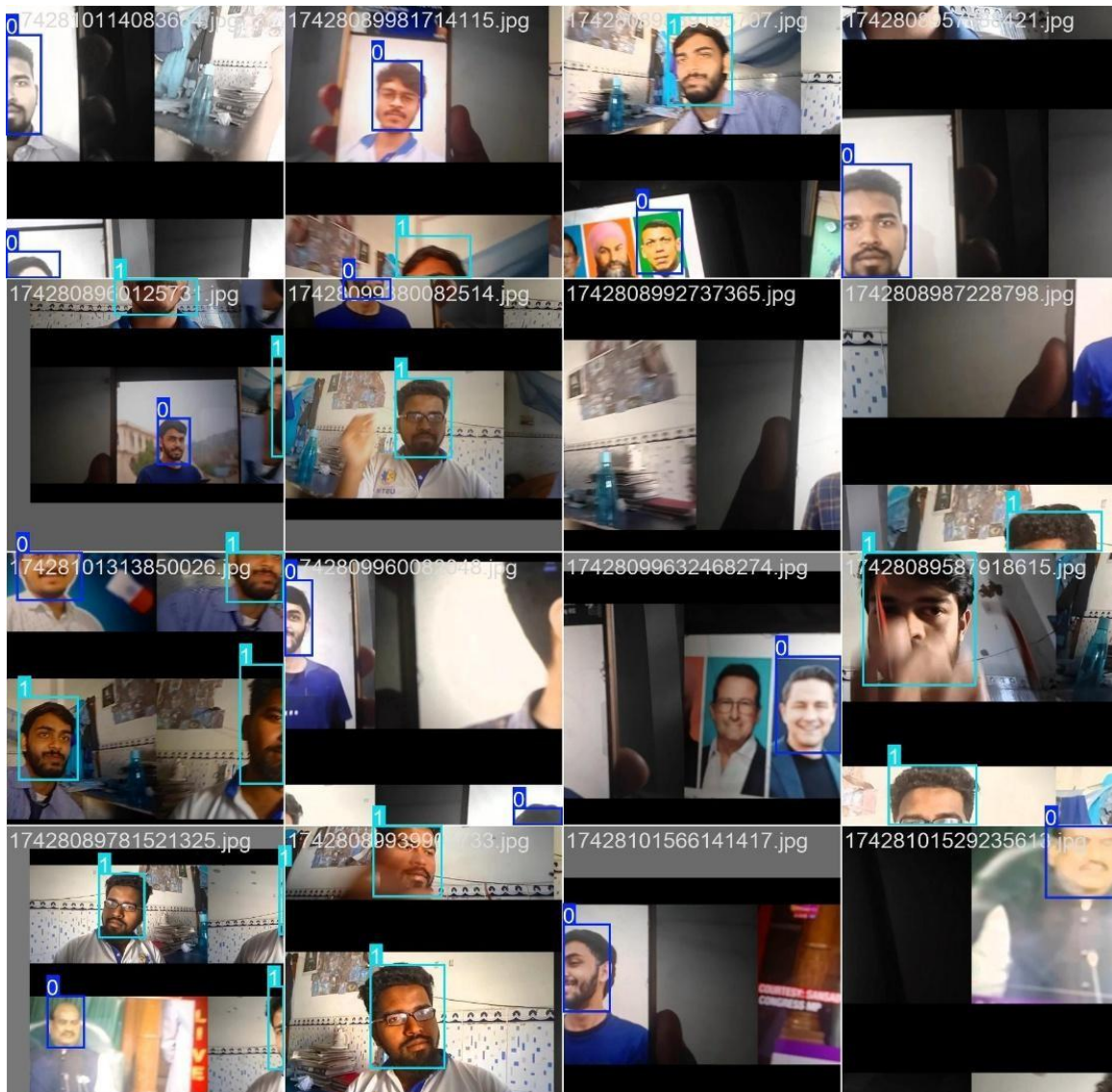


Fig: Train Batch

Fig: Train Batch shows sample output images from the training batch, highlighting real-time detection performance. These images visually validate that the model correctly localizes objects with appropriately coloured bounding boxes based on their classification (light blue or 1 for real, dark blue or 0 for fake).

Results:

The trained model's performance was assessed using standard measures. The normalized confusion matrix (*Fig: Normalized Confusion Matrix*) showed that the majority of samples were properly identified, with only a few misclassifications between the "fake" and "real" classes.

Furthermore, the F1 and Precision-Recall curves (*Fig: F1 Confidence Curve* and *Fig: PR Curve*) showed that the model maintains a good balance of accuracy and recall across different thresholds. Qualitative findings (*Fig: Train Batch*) from live inference demonstrated that the model consistently differentiates between actual and spoofed faces

in real time, as illustrated by separate color-coded bounding boxes (light blue or 1 for "real," dark blue of 0 for "fake"). These findings demonstrate that our strategy, which combines quality-driven data selection, balanced dataset partitioning, and fast real-time inference, considerably improves detection accuracy and system reliability.

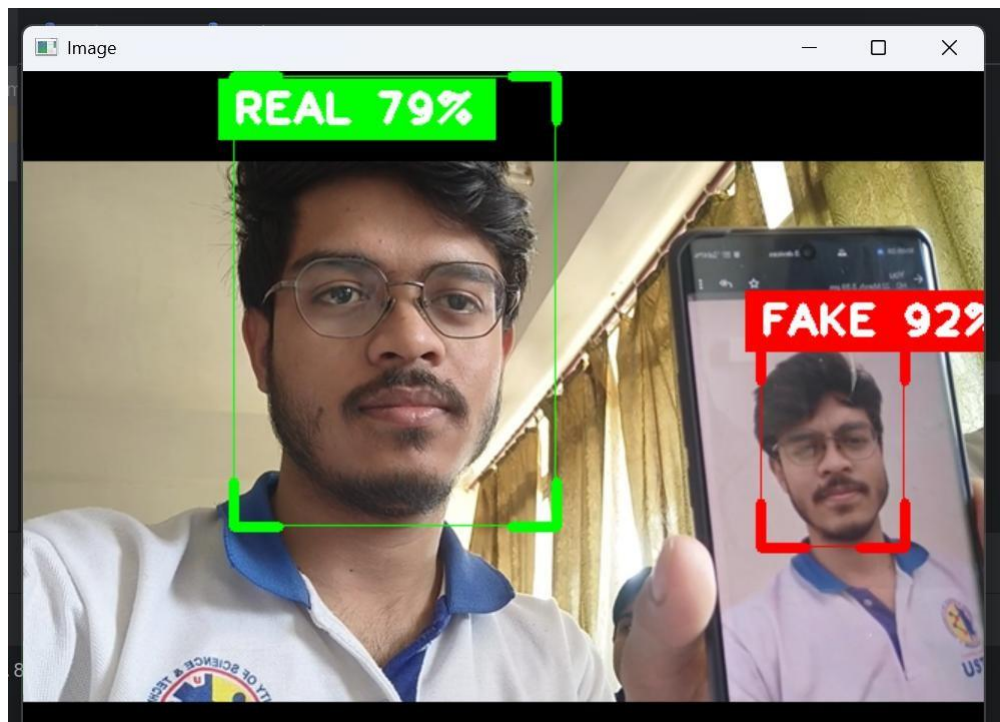
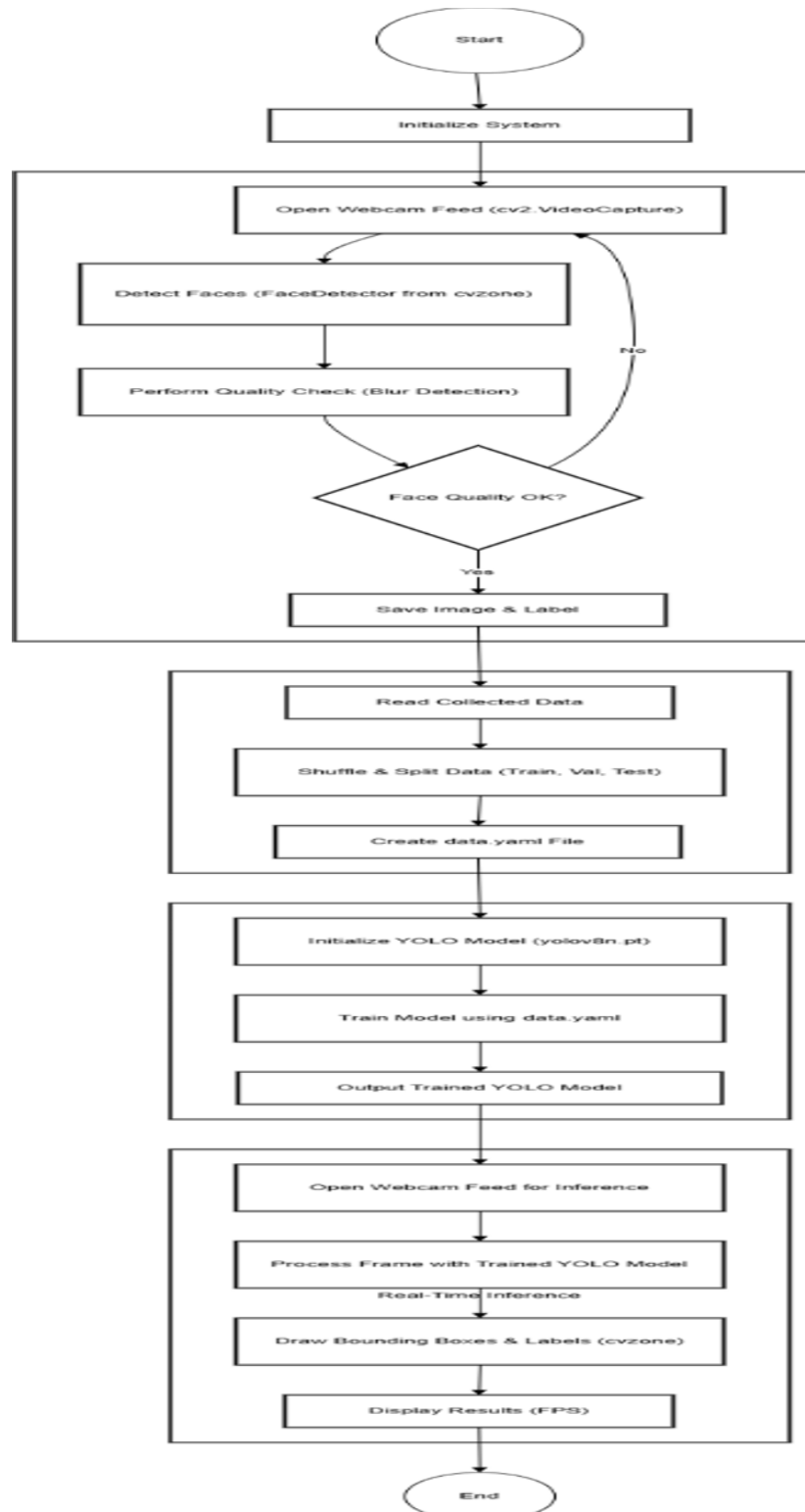


Fig: Result

V. WORK FLOW DIAGRAM





International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 09, September 2026)

VI. CONCLUSION

In this research, we developed a robust face anti-spoofing system integrating YOLO-based deep learning with OpenCV and CVZone for real-time detection. The model follows a structured pipeline, starting from data collection and pre-processing to model training and real-time inference. By implementing blur detection and bounding box normalization, our approach ensures high-quality data input for training. The trained YOLO model efficiently distinguishes between real and spoofed faces using a confidence threshold.

Experimental results demonstrate that our system can effectively detect spoofing attempts while maintaining real-time performance. The integration of blur detection, dataset organization, and efficient training enhances the model's ability to generalize across different face spoofing techniques. However, future improvements can focus on incorporating additional modalities, such as infrared imaging, to further enhance spoof detection accuracy. Additionally, optimizing computational efficiency for deployment on edge devices would improve scalability.

Overall, this study contributes to the advancement of secure and reliable face recognition systems, reinforcing biometric authentication against spoofing threats

VII. FUTURE WORK

We presented a comprehensive face anti-spoofing system that integrates data collection, dataset preparation, YOLO-based model training, and real-time detection using widely available hardware. The literature review confirms that our approach—leveraging deep learning and traditional image processing techniques—addresses many of the challenges in spoof detection. Future research will focus on expanding the dataset, incorporating additional modalities (e.g., infrared), and optimizing the deep network architecture for even faster real-time performance.

REFERENCES

- [1] A. Sawant, R. Daga, S. Salvi, M. Shaikh, S. Dagwar, and O. Surve, "Facial Identification Based Attendance System with Anti-Spoofing," *International Journal of Innovative Science, Engineering & Technology*, IJSET - International Journal of Innovative Science, Engineering & Technology, Vol. 11 Issue 05, May 2024 ISSN (Online) 2348 – 7968 | Impact Factor – 6.72 , url <http://www.ijiset.com/>
- [2] M. Chitroda, P. Bhagat, H. Gupta, and N. Vispute, "Automated Face Recognition System with Spoof Detection," *International Journal of Research Publication and Reviews*, International Journal of Research Publication and Reviews, Vol 5, no 3, pp 949-953 March 2024, ISSN 2582-7421 url: <http://www.ijrpr.com/>
- [3] Md. A. Hosen, S. H. Moz, M. M. H. Khalid, S. S. Kabir, and S. M. Galib, "Face Recognition-Based Attendance System with Anti-Spoofing, System Alert, and Email Automation," *Journal of Biometric Security*, doi: 10.32620/reks.2023.2.10 , UDC 004.93'12.056.523
- [4] Femi Emmanuel Ayo "Geometric Analysis and YOLO Algorithm for Automatic Face Detection System in a Security Setting," *Journal of Physics: Conference Series*, 2022 J. Phys.: Conf. Ser. 2199 012010, url: <https://doi.org/10.1088/1742-6596/2199/1/012010>
- [5] T.-C. Tseng, T.-F. Shih, and C.-S. Fuh, "Anti-Spoofing of Live Face Authentication on Smartphone," *JOURNAL OF INFORMATION SCIENCE AND ENGINEERING* 37, 605-616 (2021) DOI: 10.6688/IJSE.202105_37(3).0007
- [6] V. D. Huszár and V. K. Adhikarla, "Live Spoofing Detection for Automatic Human Activity Recognition Applications," *Sensors*, vol. 21, no. 7339, 2021, url: <https://doi.org/10.3390/s21217339>
- [7] K. Kavitha and K. Vijaya, "A Study on Spoofing Face Detection System," *SN Computer Science*, vol. 117, no. 22 2017, 205-208, ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version), url: <http://www.ijpam.eu/>
- [8] X. Li et al., "Early Study on Face Spoof Detection," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 500–508, 2004.
- [9] V. Chaudhari et al., "Video-Based Facial Recognition System for Attendance," *International Journal of Computer Vision*, vol. 102, no. 2, pp. 150–158, 2014.
- [10] M. Ramasane et al., "Real-Time Face Recognition System Under Varying Conditions," *Journal of Real-Time Image Processing*, vol. 9, no. 3, pp. 333–341, 2014.