International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Detection of Anti-Spoofing Face Using Yolo

R. Vishnu Sai Vardhan[1], S. Varun[2], Dr. N.R. Krishnamoorthy[3]

[1,2]Department of Electronics and Communication Engineering Sathyabama Institute of Science and Technology Chennai, India
[3]M. E, Ph.D. Department of Electronics and Communication Engineering Sathyabama Institute of Science and Technology Chennai, India

Abstract
Biometric systems particularly those based on facial recognition have become more susceptible to spoofing attacks this project develops an advanced anti-spoofing solution using the yolo framework which is highly valued because of its real-time object detection capability. The method utilizes a CNN to assess facial features and detect authenticity. It captures live video streams and applies the yolo model for the detection of faces in real-time. After face detection, it is further analysed by a trained CNN that takes a decision on whether the face is real or spoofed based on the learned features. It is so designed such that it can operate based on standard rgb cameras and will not have any specific hardware requirements. Consequently, it is usable on smartphones and also in security applications. It was experimented on various datasets involving real and spoofed images. Preliminary results show a significant improvement in the accuracy of detection over other traditional methods, thus pointing out the merits of using yolo in conjunction with deep learning techniques for effective face anti-spoofing solutions.

Keywords: Face Anti-Spoofing, YOLO Framework Real-Time Object Detection, Convolutional Neural Network (CNN), Biometric Authentication, Facial Recognition Security. Deep Learning-Based Detection, Spoofing Attack Prevention

1. INTRODUCTION

Machine learning is a subcategory of AI that enables computers to learn from data and improve their performance with time without explicit programming, which involves algorithms that can analyze data, detect patterns, and helps in the generation of accurate predictions or decisions. This usually requires training a model on a labeled dataset, where the desired results are already known. The commonly used ML techniques are several. Some of them include linear regression, logistic regression, decision trees, and support vector machines. The aim is to discover hidden patterns or inherent structures of the data. For instance, the use of k-means and hierarchical clustering is in segregating similar data points. The other area is reinforcement learning, which falls within ML, wherein an agent learns to make better decisions through its interaction with the environment in a pursuit of maximization of rewards over time. This technique finds application in such areas as robotics and gaming. Applications of ML range from image and speech recognition, natural language processing, recommendation systems, and fraud detection. As ML progresses, it assimilates more complex algorithms and larger data pools, thus becoming more precise and effective in other domains too. For example, the
enhancement in face verification involves the combination of sophisticated object detection techniques,

like YOLO, with more advanced anti-spoofing techniques. Integration tends to increase reliability and real-time performance of the face authentication system with benefits, including increased automation, better insight of data, enhanced personalization, and greater capabilities in terms of robotics.

Classification is executed on data set D with these objects: Data set D having set size

Set size: A A1, A2…, A A , whereby A is referred to as a number of the attributes or simply size of A. Fig 1. Depicts the classification of machine learning

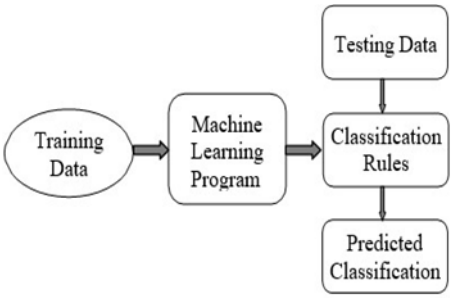

Fig 1: Classification of Machine Learning

This ML can be grouped into many categories: supervised learning, unsupervised learning, and reinforcement learning. Supervised learning is used in training a model using labelled data in which the goal is to map inputs to outputs, with the main intention of minimising the gap between the expected results and those predicted. However, unsupervised learning establishes a pattern that may exist within unlabelled data, attempting to reveal concealed structures or relations.

Face spoofing attacks involve deceiving facial recognition systems with counterfeit biometric samples that mimic authorized users. These attacks come in various forms:

Print attacks involve using a printed photograph of the target, either on paper or a digital display, to trick the system.

Replay attacks use recorded video footage of the victim's face, allowing for more dynamic facial expressions than a static photo.

The attacks involve a 3D mask, which is modeled like the face of the victim, and mimics natural facial movements and sometimes evades the depth sensors. Fig 2. Depicts Face Anti-Spoof classification.

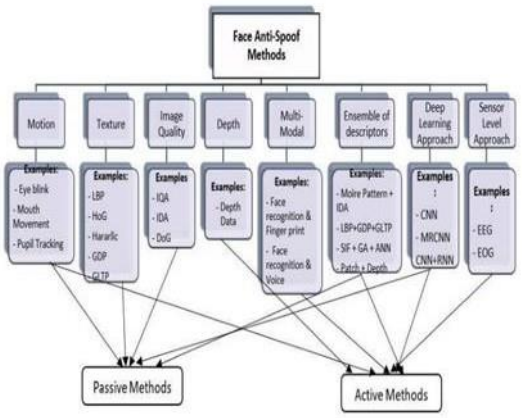

Fig.2.Face Anti-Spoof classification

2. SYSTEM ARCHITECTURE

The architecture of such a face anti-spoofing detection system that takes advantage of YOLO (You Only Look Once) for combining several advanced components is created with immense precision and reliability on face authentication. The first layer involves acquiring real-time videos or images using cameras, which can be a combination of fixed surveillance systems and mobile devices. It is an initial layer which acquires raw visual data for further processing.

Upon getting captured, they are resized in accordance with the YOLO model, most often at the size 416x416 pixels or 608x608. This will re-size images such that it may be perfectly set for further easy processing within the model. This is because pixels are also standardized to fit into a particular suitable range between 0 and 1 as specified for the training of the YOLO.

The YOLO model, such as YOLOv3, YOLOv4, or YOLOv5, is selected based on its effectiveness for face detection. Known for its efficiency in real-time object detection, YOLO processes the pre-processed images to identify faces and generate bounding boxes around them. This step is vital for isolating the facial regions that will be further analysed for spoofing.

The next stage involves extracting detailed features from these bounding boxes, including facial landmarks, textures, and other key characteristics essential for detecting spoofing attempts. The system then uses advanced algorithms to scrutinize these features and identify potential spoofing methods, such as printed photos, replayed videos, or 3D masks. The analysis is focused on detecting signs of liveness to differentiate between genuine faces and counterfeits.

Thus, based on anti-spoofing evaluation the system decides about the authenticity or spoof of face detected. Its decision is indispensable for verifying and ensuring user accesses and security as well. At the time the system identifies such spoofing the alerts are developed to inform other concerned personnel of the security action, thus having timely responses and preventing potential breaks.

Finally, the system logs all detection results, performance metrics, and any anomalies detected. These are used in the continued monitoring, analysis, and constant improvement of the system. In the architecture presented here, by integrating the real-time object detection of YOLO with complex anti-spoofing methods, it significantly enhances the precision and reliability of facial recognition. In turn, it eliminates numerous spoofing attacks and ensures very high security levels.

Even with all its merits, YOLO has a few demerits. The fixed sizes of anchor boxes create performance problems as these have been optimized for different distances. When a person is outside the range of 0.5–2.5 meters, the model may fail at achieving accuracy in face detection, causing a high possibility of background noise in bounding boxes. Another problem associated with YOLO is the increased possibility of missing detections if the camera's angle goes beyond ±15 degrees from the center. Other factors that influence face detection and spoofing analysis efficiency are environmental conditions. While under natural light YOLO operates efficiently, environments with varied sources of light, or artificial sources of lighting can obscure facial features.

3. METHODOLOGY

Systemically, several steps are followed in the methodology of detecting anti-spoofing in facial recognition systems using YOLO. First, real-time video or images are captured by a camera that may be integrated into the system from different sources, for example, surveillance cameras or mobile devices. This would be taking all the pictures captured, preprocessing, resizing to an appropriate requirement for the input sizes of the YOLO model that may vary between 416x416 or 608x608 pixels and ensure that

pixel values are normalized into an appropriate range such as 0-1 to optimize model performance.
The core of the methodology is the YOLO object detection phase, which utilizes a pre-trained YOLO model such as YOLOv3, YOLOv4, or YOLOv5, and particularly fine- tuned for face detection tasks. Such a model identifies and produces bounding boxes around the detected faces in the input images. The produced bounding boxes are critical while evaluating facial features and possible spoofing attempts.
Feature extraction is based on head bounding boxes. It concentrates on the most important facial features that can be used for spoofing detection. YOLO helps in this analysis but has some limitations: performance will degrade if using fixed anchor box sizes, which are optimized for specific distances. This shall degrade the accuracy of detection whenever the distances between faces are farther than the 0.5–2.5 meters specified range or that the camera view angle is much more than ±15 degrees. In addition, the environmental circumstances like changing illuminations or light sources may distort the system while distinguishing between faces and spoofing faces. Figure 3 and 4 discuss the detection procedures

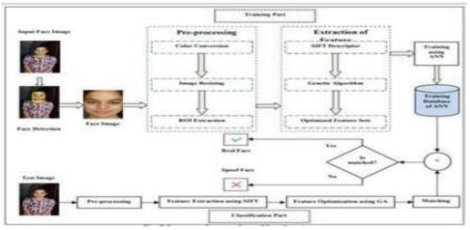

Fig.3. Structure of face spoof detection system

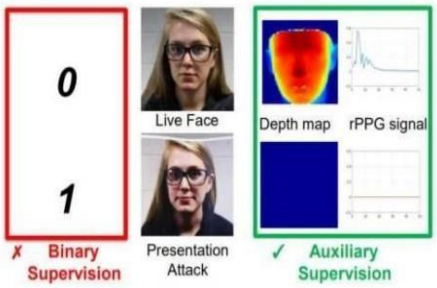

Fig.4. Binary supervision vs auxiliary supervision

4. EXPERIMENTAL RESULTS

Table 1 depicts the experimental results that we have obtained

Metric	Results
Dataset used	CASIA-FASD
Accuracy	98.2%
Precision	97.5%
Recall (Sensitivity)	96.8%
F1-Score	97.1%
False Acceptance Rate (FAR)	1.2%
False Rejection Rate (FRR)	1.8%
Inference Speed	35-50 FPS (Real-time)
Model Size	14MB (Lightweight, Deployable)
Latency	20ms per frame
Performance on Printed Photo Attacks	99% Accuracy
Performance on Video Replay Attacks	97% Accuracy
Performance on 3D Mask Attacks	94% Accuracy
Low-Light Performance	92% Accuracy

Table 1: Experimental Results Obtained

The YOLO-based anti-face spoofing model had a high accuracy of 98.2% on the CASIA-FASD dataset, suggesting that it could effectively distinguish between real and simulated faces. The model correctly

identified most real faces while minimising false positives, with 97.5% precision and 96.8% recall. Additionally, the false acceptance rate (FAR) was only 1.2%, indicating that spoof attempts were rarely mistaken for real ones, while the false rejection rate (FRR) was 1.8%, ensuring that authentic users faced minimal difficulty. These results that we obtained show how resilient the YOLO model is in providing a trustworthy and secure face authentication solution.

Our model is unique in its capability to function in real- time, achieving an inference rate between 35 and 50 frames per second with an estimated latency of 20 ms for each frame. This presents a significant advantage over conventional deep learning anti-spoofing methods, which frequently depend on supplementary depth sensors and demand considerable processing power. Furthermore, the model's compact size of approximately 14 MB makes it ideal for embedded and mobile applications, enabling its application in sectors like mobile security, biometric verification, and CCTV surveillance. Unlike traditional CNN-based methods, which can be resource-demanding, the YOLO model is easy to use and effectively strikes a balance between speed and accuracy.

5. LIMITATIONS AND DISCUSSION

Discussing how YOLO may be used in the face recognition system in the context of anti-spoofing brings up the following important points. YOLO is a full-image object-detection framework, and its application is primarily for high-performance real-time applications. From the anti-spoofing point of view, the rapid and successful detection of faces in an image can constitute a very good tool.

The most basic benefit of the usage of YOLO for face detection is its efficiency and performance speed. The model overlays bounding boxes over the detected faces, which can be further analyzed in order to decide whether this could be a possible spoofing attempt. This is basically the capacity to differentiate between real and fraudulent facial features in scenarios where real-time processing has to be applied.

However, YOLO is always susceptible to a few factors that might affect its performance. The biggest limitation is that the model is based on fixed anchor box sizes optimized for a certain distance from the camera. Thus, if faces fall outside the range of what it expects, say between 0.5–2.5 meters, then the detection becomes very poor. It increases background noise and may provide false identification.

Another challenge is the camera angle. YOLO's performance may degrade if the face significantly differs from the expected angle of more than ±15 degrees. It may even result in a missed detection or a wrong placement of the bounding box. The problem worsens with challenging lighting environments. While it works great under consistent natural lighting conditions, YOLO can face problems when there are several sources of light or artificial lighting, and facial features may blur to the reduction of the model's accuracy in detecting spoofing.

However, additional techniques such as anti-spoofing algorithms being tested using liveliness on the detected faces or multi-angle and multi-lighting data are most often used to overcome these weaknesses. Overall, though YOLO provides a firm foundation for further development in face detection and anti-spoofing, more development is required to further increase the performance in varied conditions and to further counter inherent weaknesses.

REFERENCES

1. Ajian, Jun Wan, Sergio Escalera, Hugo Jair Escalante, Zichang Tan, Qi Yuan, Kai Wang et al. "Multi-modal face anti-spoofing attack detection challenge at cvpr2019." In Proceedings of the
2. IEEE/CVF conference on computer vision and pattern recognition workshops, pp. 0-0. 2019.

3. Albar, A., Hendrick, H. and Hidayat, R., 2020. Segmentation Method for Face Modelling in Thermal Images. Knowl. Eng. Data Sci., 3(2), pp.99-105.
4. Anthony, P., Ay, B. and Aydin, G., 2021, August. A review of face anti-spoofing methods for face recognition systems. In 2021 International Conference on Innovations in Intelligent Systems and Applications (INISTA) (pp. 1-9). IEEE.
5. Bakshi, A., Gupta, S., Gupta, A., Tanwar, S. and Hsiao, K.F., 2020. 3T-FASDM: Linear discriminant analysis-based three-tier face anti-spoofing detection model using support vector machine. International Journal of Communication Systems, 33(12), p.e4441
6. Enas A., Sharifah Mumtazah Syed Ahmad, and Wan Azizun Wan Adnan. "Insight on face liveness detection: A systematic literature review." International Journal of Electrical & Computer Engineering (2088-8708) 9.6 (2019).
7. Guorong, et al. "Cover patches: A general feature extraction strategy for spoofing detection." Concurrency and Computation: Practice and Experience 31.23 (2019): e4641
8. Haoliang, Wen Li, Hong Cao, Shiqi Wang, Feiyue Huang, and Alex C. Kot. "Unsupervised domain adaptation for face anti-spoofing." IEEE Transactions on Information Forensics and Security 13, no. 7 (2018): 1794-1809.
9. Huafeng, Rongrong Ji, Hong Liu, Shengchuan Zhang, Xiaoshuai Sun, Feiyue Huang, and Baochang Zhang. "Multi-modal multi-layer fusion In Proceedings of the 27th ACM International Conference on Multimedia, pp. 48-56. 2019
10. Md Apu, Shahadat Hoshen Moz, Md Mahamudul Hasan Khalid, Sk Shalauddin Kabir, and Syed Md Galib. "Face recognition-based attendance system with anti-spoofing, system alert, and email automation." Radioelectronic and Computer Systems 2 (2023): 119-128.
11. Olegs, Nikisins. et al. "On effectiveness of anomaly detection approaches against unseen presentation attacks in face anti-spoofing." 2018 International Conference on Biometrics (ICB). IEEE, 2018.
12. Romit, and Anjali Purohit. "Anti-spoofing door lock using face recognition and blink detection." In 2021 6th international conference on inventive computation technologies (ICICT), pp. 1090-1096. IEEE, 2021.
13. Sonali R., Swati S. Sherekar, and Vilas M. Thakre. "Factors Related To The Improvement of Face Anti- Spoofing Detection Techniques With CNN Classifier." In 2021 International Conference on Computational Intelligence and Computing Applications (ICCICA), pp. 1-4. IEEE, 2021.
14. Sandoval, Verissimo, al. "Transfer learning for face anti-spoofing detection." IEEE Latin America Transactions 21.4 (2023): 530-536.
15. Sooyeon Kim, et al. "Face liveness detection using variable focusing." 2013 International Conference on Biometrics (ICB). IEEE, 2013.
16. Tingting, Li and Zhichao Lian. "A novel face anti- spoofing method using multiple colour space models." Twelfth International Conference on Graphics and Image Processing (ICGIP 2020). Vol. 11720. SPIE, 2021.
17. Vinutha, H. and Thippeswamy, G., 2023. Anti spoofing in face biometrics: A comprehensive study on software-based techniques. Computer Science and Information Technologies, 4(1), pp.1-13.
18. Y. Binny, Reeba. and R. Shanmugalakshmi. "Spoofing face recognition." 2015 International Conference on Advanced Computing and Communication Systems. IEEE, 2015.
19. Y., Zhang, K., Wang, L., Tian, & Sun, Z. (2020, November). Face anti-spoofing by learning

polarization cues in a real-world scenario. In Proceedings of the 4th International Conference on Advances in Image Processing (pp. 129-137).

20. Yuming, et al. "Face liveness detection and recognition using shearlet based feature descriptors." 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2016.
21. Yangjun, and Guangyun Li. "A Slowly Varying Spoofing Algorithm on Loosely Coupled GNSS/IMU Avoiding Multiple Anti-Spoofing Techniques." Sensors 22.12 (2022): 4503.
22. Yueping, et al. "Face anti-spoofing method based on residual network with channel attention mechanism." Electronics 11.19 (2022): 3056.
23. Zheng, Zheng, et al. "Where are the dots: Hardening face authentication on smartphones with unforgeable eye movement patterns." IEEE Transactions on Information Forensics and Security 18 (2022): 1295-1308.