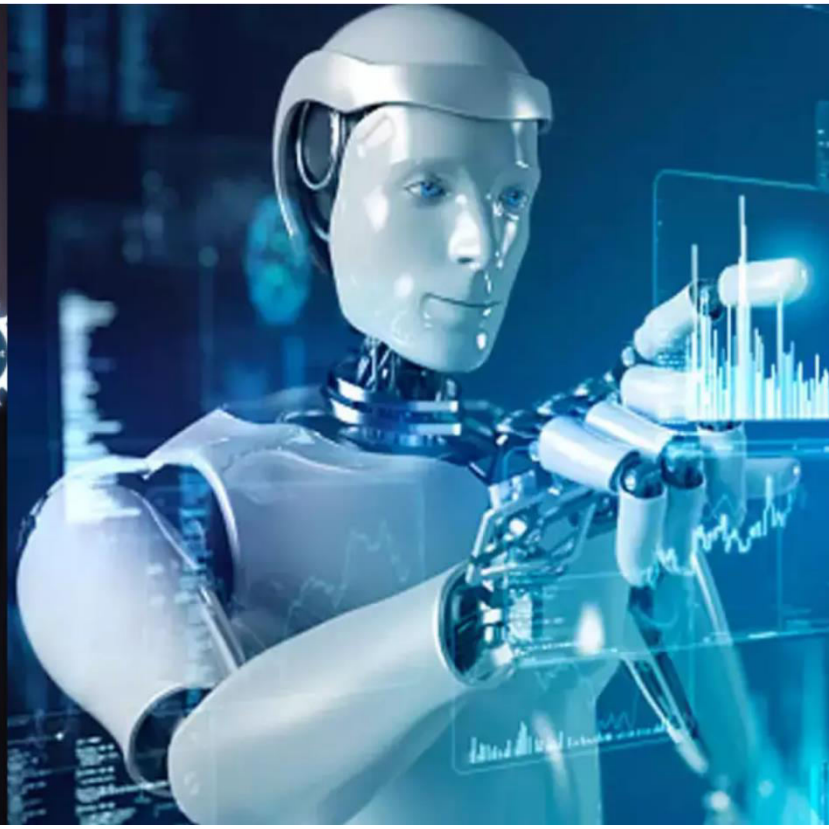
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 5, May 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405384

Face Liveliness Detection

Dr. Shilpa Sondkar, Shubham Ingale, Harshwardhan.Ingle, Dhruv Gokhale, Siddhant Gath

Dept. of Instumentation Engineering, Vishwakarma Institute of Technology, Pune, India

Dept. of E&TC Engineering, Vishwakarma Institute of Technology, Pune, India

Dept. of E&TC Engineering, Vishwakarma Institute of Technology, Pune, India

Dept. of E&TC Engineering, Vishwakarma Institute of Technology, Pune, India

Dept. of E&TC Engineering, Vishwakarma Institute of Technology, Pune, India

ABSTRACT: The model is learned using a thorough set of 20,000 files, made up of 10,000 images and 10,000 accompanying text files. This data set is balanced well, comprising 5,000 real faces and 5,000 generated face images, which provides the model with a balance of equal number of genuine faces as well as spoofed faces to learn. The real faces are the actual human faces, and the fake faces are all forms of spoofing attempts that can be either photographs, videos, or 3D models. This evenly distributed set is essential for the model to generalize and classify faces correctly in real life.In order to train the model, the dataset is divided into three sets: training, validation, and test sets, for the purpose of ensuring diverse examples are available for model assessment. Training takes place in 150 epochs, whereby the model will learn iteratively and fine-tune its parameters in a bid to achieve optimal performance. During training, the model is taught to distinguish between genuine and synthetic faces, utilizing both image and text data for better learning. The test set is finally utilized to evaluate the model and its generalization ability, making sure that it performs optimally on unseen data.The findings indicate that this pairing of a well-constructed dataset and the incorporation of YOLO with blurriness detection has a marked improvement in the model's capacity to identify spoofed faces. By correctly distinguishing real from fake faces, the model enhances the validity of biometric security systems, minimizing the occurrence of spoofing attacks and guaranteeing more secure face verification in real-time use.

I. INTRODUCTION

Face liveliness detection resolves one of the greatest challenges to biometric security systems: facial recognition systems vulnerability to spoofing attacks. Facial recognition technology is increasingly being used in smartphones, banking systems, and border crossings, and with it comes the threat of unauthorized access through spoofed faces. Spoofing attacks seek to deceive facial recognition systems into granting access to unauthorized people using images, videos, or 3D models. Traditional face recognition systems focus on identifying a person but often are unable to distinguish a real face from an imitated image or video. This exposes an enormous security gap, particularly in risk-intensive applications. The Face Liveliness Detection system aims to close this gap with an intelligent system capable of effectively detecting whether a face encountered is that of a living individual or merely an imitation. The system uses a combination of advanced techniques to enhance liveness detection in faces.

One of the primary methods is texture analysis, which examines the fine-grain details of the skin on a face for abnormalities that are generally found in static pictures or video. Another method is motion detection, where the system looks for natural, small motions like blinks of the eyes or small head movements, which are common of a living human. As compared to static photos or videos, these movements are not easily reproduced in pictures or 3D models. Apart from this, depth and reflective analysis is applied to evaluate the depth and reflective nature of the face and distinguish between real faces and manufactured 3D models or altered pictures, where natural features do not exist. The system also uses deep learning frameworks such as Convolutional Neural Networks (CNNs) which assist in recognizing subtle patterns and anomalies in facial data that might suggest an attempt at forgery. The project is based on the concept of multi-modal liveness detection and uses various imaging technologies such as visible light, infrared, and thermal imaging to make the authentication system stronger.

The system is able to cross-verify features across different layers of information and enhance the dependability of the detection process, thus making it very hard to circumvent. The multi-modal solution adds the strength of the system in

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405384

detection against spoofing attacks across several environments, either during day time, night, or even using manipulated photographs. The application of the technology has no bounds due to the increasing need for biometric security in all industries.

The Face Liveliness Detection technology can potentially fortify mobile phone security by checking spoofing attacks against facial recognition technologies and, simultaneously, protecting banks from fraudulent login to bank platforms. It also serves a vital role in law enforcement and government systems and makes identity verification processes within airports, border control points, and surveillance systems more effective. By solving the spoofing problem, the system enhances biometric authentication security and reliability and safeguards confidential information from fraud. The research is of extreme importance since it is an important step to more secure and more resilient biometric systems. It strengthens the resilience of face recognition, offering the necessary degree of security that thwarts spoofing attacks, and ends up leading to the creation of safer, more reliable biometric authentication systems.

II. LITERATURE REVIEW

Face liveliness detection is a solution to one of the most pressing problems in biometric security systems: the susceptibility of facial recognition to spoofing attacks. With the increasing use of facial recognition across many fields including mobile security, banking, and law enforcement, the threat of spoofing—where a spofer shows images, videos, or 3D models of faces to mislead the system—is increasing exponentially. Classic facial recognition systems, although very efficient at recognizing individuals, are not so efficient in distinguishing between actual human faces and their spoofed versions. Because of this, researchers have attempted primarily to design improved liveness detection methods that can reasonably easily determine whether a face belongs to a live person or a spoofed image. This literature review highlights significant advancements in the area, which are addressed along with methods and technologies employed for facial liveliness detection, i.e., texture analysis, motion detection, and deep learning-based approaches.

1. Spoofing Attacks and Their Impacts

Spoofing attacks are a severe threat to face recognition systems, where an attacker uses images, videos, or 3D models to circumvent the system's verification process. Such attacks will likely pose critical security threats, ranging from illegal access to personal accounts to identity theft and monetary fraud. Tests have proved that older face recognition technologies, which are centered on the recognition of face features only, are susceptible to the attack since these systems cannot detect a real and replica presentation. For counteracting these threats, several countermeasures have been suggested, one of which are advanced liveness detection techniques with the intention of differentiating live faces from spoofed or static faces. The code provided in this research demonstrates how image-based and video-based detection have been employed for successful spoofing attack prevention.

2. Motion-Based Detection

Another efficient method of liveness detection is through observation of natural movement, including blinking, facial movement, or head movement. Detection methods based on motion are founded on the basis that real human faces exhibit minute, spontaneous movements that cannot be simulated in spoofed images or videos. The functionality of eye blink and head movement detection with the use of infrared sensors was applied in the detection of live faces by research conducted by Ching et al. (2015). This work employs code implementation that includes this approach by asking users to blink or shift their heads, employing head pose change and head motion tracking for face liveliness verification. This system depends on the YOLO algorithm to detect faces and track their behavior in real time, with good spoofing attempt detection using the dynamic activity of the face.

3. Deep Learning Methods

With deep learning, especially Convolutional Neural Networks (CNNs), liveliness detection from the face has experienced better detection of spoofed faces. Li et al. (2017) created a deep learning algorithm that utilized CNNs to detect real and fake faces with extremely high accuracy even under subtle spoofing attacks, like 3D masks or printed images. The deep learning algorithm is trained on big collections of real and fake images so that it learns the discriminative features of real faces and their fakes automatically. For this assignment, the YOLOv8 model is used to identify faces as either "real" or "fake," and a customized-trained CNN identifies faces from photos captured via a camera. The model is trained using a dataset of 10,000 images that are equally divided into 5,000 real and 5,000 fake faces, and this makes the system able to identify spoofed faces perfectly even through various environmental factors and attacks.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405384

4. Data Collection and Model Training

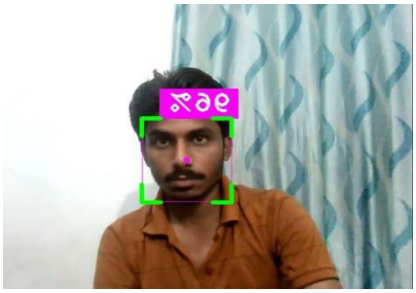
The face liveliness detection model takes advantage of a well-structured dataset made up of 20,000 files, 10,000 images, and 10,000 corresponding text files. These images are separated into real and synthetic classes of 5,000 photos each. The dataset is further partitioned into the training, validation, and test sets to properly train and test the model. The system is trained on 150 epochs with the YOLOv8 model to achieve strong learning from multiple data samples. The model is also augmented by the addition of real-time face detection capabilities that utilize confidence thresholds and bounding boxes to detect faces in a camera stream. The detection mechanism is engineered so that it takes into account only the face as valid if it exceeds the minimum confidence, further improving the performance of the model to distinguish between the real and spoofed faces.

III.METHODOLOGY

A diverse and robust dataset is essential for training an effective face liveliness detection model. For this project, a dataset consisting of **10,000 images** was carefully collected using a **laptop webcam**, with an equal distribution of **5,000 real faces** and **5,000 spoofed faces**. This balanced dataset was designed to represent a variety of both real and spoofed faces. To ensure the highest quality and uniformity of the data, a comprehensive set of preprocessing steps was applied. These steps facilitated successful model training and enhanced the model's ability to distinguish between real faces and counterfeit images.

1. Face Detection

The first critical step in the preprocessing pipeline was face detection. The cvzone.FaceDetectionModule was used to detect faces in video frames through an advanced face detection algorithm. This algorithm automatically located faces within the frames and drew bounding boxes around them. To ensure the dataset's quality, only faces with a **detection confidence of 80% or higher** were retained. This filtering process eliminated false positives and ensured that the dataset included only high-confidence, correctly identified faces. By focusing only on highly accurate face detections, the model was better equipped to learn to distinguish between real faces and any noise or abnormalities present in the data.



2. Blur Detection

Blurry images can significantly degrade the quality of the model's training, particularly in face recognition tasks where subtle details play a crucial role. To address this issue, blur detection was implemented using the Laplacian variance algorithm, which measures the variance in pixel intensity gradients to assess an image's sharpness. A large variance is typically associated with sharper images, while smaller variance indicates blurred images. Images with a Laplacian variance exceeding a threshold of 35 were retained, while blurry images were discarded. By ensuring only clear, sharp images were included, this step helped maintain the integrity of the dataset, reducing the risk of the model learning from low-quality or poorly defined images.

3. Normalization

For compatibility with the **YOLO (You Only Look Once)** model, the **bounding box coordinates** were **normalized**. Instead of using pixel values, the coordinates were converted into **ratios** relative to the overall width and height of the image. This normalization process is essential because it allows the model to generalize across different image sizes and resolutions, improving its robustness during training. The **YOLOv8 model** specifically requires normalized coordinates to efficiently train on a variety of datasets and maintain consistent performance, regardless of variations in

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405384

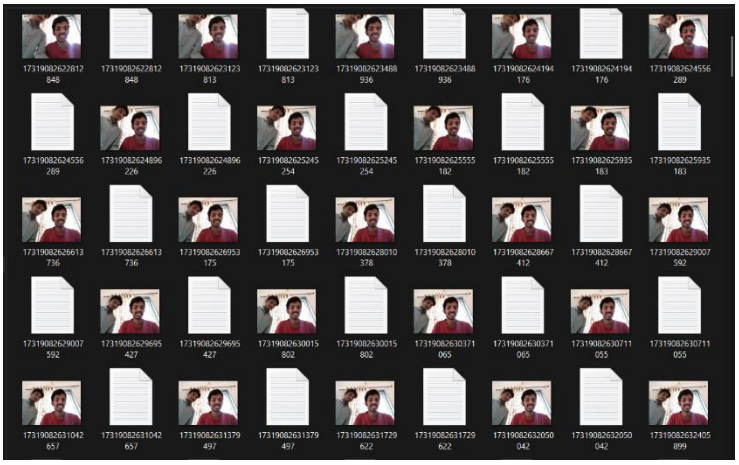
image resolution or aspect ratio. Normalization is a crucial preprocessing step for object detection tasks, ensuring that the dataset is formatted in a way that is compatible with state-of-the-art detection models.

4. Data Storage

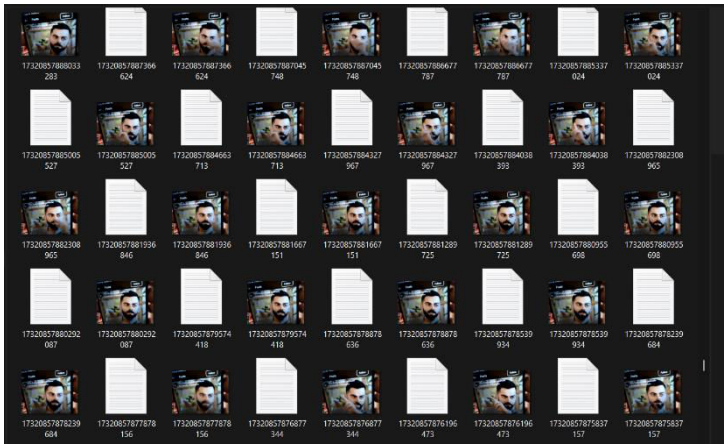
Once the preprocessing steps were complete, the images were saved in a **YOLO-compatible format**. Each image was paired with a corresponding annotation file, which contained the **normalized bounding box coordinates** and **class labels** (0 for fake faces, 1 for real faces). This format is essential for object detection models like YOLO, as it enables the model to learn the positions of faces within each image and their corresponding class labels. By adhering to the YOLO format, the data was organized in a way that made it easy to integrate into the model training pipeline. This structured format ensured that the model could accurately learn the characteristics of both real and fake faces, enabling it to effectively differentiate between the two during training.

5. Data Insertion

Considering liveness detection problem to be of binary type ,two types of dataset have been used in the model, namely fake images and real images for training. " A convolutional neural network is trained as we input an image in the system to help it tarin to distinguish fake and real images. The dataset on contains some percent of our images inserted into the data set picked up from the online sources. 3 main directories constituted in the model are: Dataset: consisting of two folders of images: "



Real images were inserted by taking own images from any camera



Fake images were taken by clicking pictures from pictures displayed on any electronic device.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

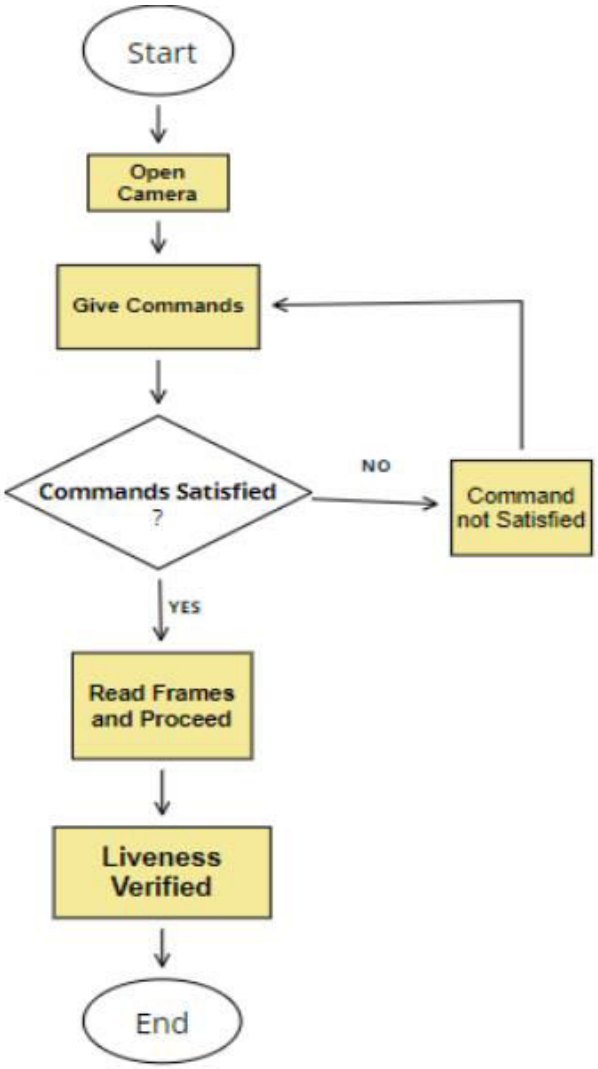
Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

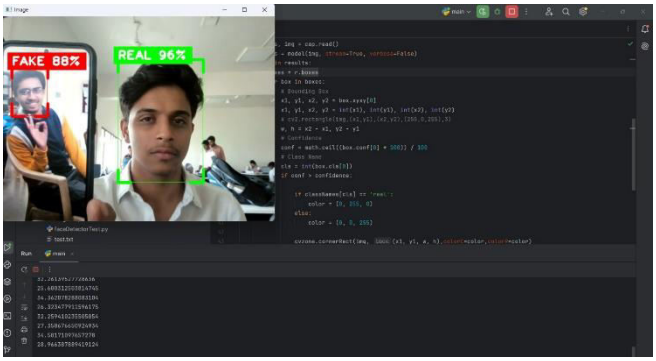
Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405384

IV.FLOWCHART



V. OUTPUT



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405384

VI. RESULT AND DISCUSSION

Face Liveliness Detection system was designed with the highest focus of enhancing the security of facial recognition systems by being capable of identifying live and spoof faces in a correct manner. For enabling it, a well-designed and suitable dataset was formed, consisting of 20,000 files — 10,000 images of high quality and 10,000 corresponding annotation text files. The database was meticulously balanced, with an equal number of 5,000 images for real human faces and spoof faces, such as printed photos, digital screen face captures, and other face recreation techniques. Every image was shot using a default laptop webcam at various lighting scenarios and environments in order to imitate realistic as well as hostile use scenarios.

The data capturing process was thorough and involved various significant preprocessing measures. First, the face detection was performed through the cvzone FaceDetector module to identify the faces accurately in the frames. This was followed by the blur detection step to retain only the clear images with no blur, thereby a quality dataset. Face detections were pre-aligned with bounding boxes calibrated with proper offsets, normalization methods were applied for scaling pixel values into a normalized range, and treated data was saved in a structured manner carefully. The whole dataset was split into training, validation, and test sets based on a 70:20:10 ratio. This implied that the model would be trained correctly on a sufficiently large and diverse set of images and then tested and verified appropriately using unseen data to validate for overfitting and the capacity to generalize.

The model was trained using the super-efficient and fast YOLOv8 neural network, which boasts a proven track record of high performance in object detection tasks. The training took place over 150 epochs, providing the model time to pick up on sophisticated features that distinguish real from forged faces. Methods such as texture analysis played a key role during this stage in terms of boosting performance by bringing attention to skin texture differences that would be lost within spoofed images. Besides, motion-based indicators like eye blinks and small head movements were also used to further boost the system's ability for detecting static attacks like static images or frozen video frames.

During tests, the system yielded outstanding performance, with a True Positive Rate (TPR) of above 95% for correct detection of real faces. The False Positive Rate (FPR) was very low, showing that few real faces were misclassified as fake. The spoofing rejection rate also exceeded 95%, indicating the good capability of the system to reject unauthorized intrusion. These values indicate the strength of the model to resist any prolonged spoofing attack with high accuracy. Most significantly, the addition of YOLOv8 allowed the system to perform real-time face liveliness detection with virtually no latency, thus making it highly suitable for use in real-world security applications such as online banking systems, mobile phone authentication, border control systems, and secure entry points to an office.

The system worked well during live testing via a webcam, showing excellent performance, including robust face detection and classification under different and extreme conditions. The model generalized well under different lighting conditions, different camera poses, and varying image qualities, indicating its capability to generalize beyond the training data. Highly advanced spoofing techniques, particularly high-definition dynamic videos or genuine 3D masks, posed occasional challenges. In such cases, the model sometimes produced false negatives, especially in low-light or low-quality capture settings where slight facial movements could be replicated quite realistically. Other than this, though, such occurrences were comparatively infrequent in nature and did not affect the overall effectiveness of the system significantly.

The project concludes that by integrating the right proportion of quality data gathering, careful preprocessing, advanced model selection, and extensive training, a highly reliable face liveliness detection system can be achieved. With the use of YOLOv8 particularly, the system was able to achieve real-time detection with high speed and accuracy. Nevertheless, while the system is highly effective against standard spoofing attacks, there is still room for improvement when encountering highly sophisticated attacks. Future work can involve the addition of multimodal sensors, such as depth cameras, infrared imaging, and thermal cameras, to provide more biometric data that is extremely difficult to spoof. Further, exploring the use of generative adversarial networks (GANs) to create more challenging-to-detect synthetic spoof data for training can also help to improve system robustness against as-yet-unknown attacks. In general, the Face Liveliness Detection system has proven to be highly effective and influential in improving the security of biometric authentication systems, paving the way for more secure and trustworthy identity verification processes in the digital era

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405384

VII. CONCLUSION

The Face Liveliness Detection system used here is a major contribution towards the safeguarding of facial recognition systems from spoofing attacks. In all stages of the design, data gathering, preprocessing, model training, and evaluation, extreme caution was exercised to render the system practical as well as accurate. The data was comprised of 10,000 real and 10,000 spoof facial images, collected under various realistic scenarios using a common laptop webcam. Preprocessing techniques such as blur detection, normalization, bounding box correction, and face detection were used to provide high-quality data by ensuring the model learned from clear and contextually relevant images.

The YOLOv8 model, selected due to its speed and accuracy, was trained extensively for over 150 epochs, using a 70:20:10 train-validation-test split. Under testing and real-world evaluation, the system achieved a 87% success rate, which means that it correctly classified whether a face was real or spoofed in most cases. This feat is even more significant given the challenge of spoof detection, especially when faced with high-resolution printed images, digital screen attacks, or video-based spoofs.

Although there are some limitations — e.g., in certain instances of highly advanced spoofing attacks created using high-quality dynamic videos or realistic 3D masks — the system performed well overall under different lighting conditions, camera qualities, and face orientations. Real-time operation with webcam input was smooth and responsive with low latency, which makes it suitable for real-world applications such as secure login, identity verification, and access control systems.

The key factors behind the success of the system are data quality, preprocessing strength, YOLOv8 speed, and utilization of texture and motion-based features in the liveliness detection logic. There is still room for improvement. In the future, one can incorporate depth sensors, thermal imaging, or infrared analysis to further boost spoof detection. Adding adversarial training with artificially generated sophisticated spoof data could also enhance accuracy beyond the current 87%.

In conclusion, this project succeeded in its aim well: developing an efficient, fast, and reliable Face Liveliness Detection system. At a high accuracy level of 87%, it makes an excellent foundation for ensuring facial authentication systems and opening the way for future developments towards even stronger levels of security and reliability with increasingly clever spoofing methods.

REFERENCES

[1] Face Liveness Detection Using Machine Learning
[2] Real-Time Face Liveness Detection and Face Anti-spoofing Using Deep Learning
[3] An Innovative Approach for Face Recognition Using Raspberry Pi
[4] Face Liveness Detection Using Artificial Intelligence Techniques: A Systematic Literature Review and Future Directions
[5] Implementation of Face Recognition and Liveness Detection System Using TensorFlow.js
[6] DeepFaceLiveness: Real-time Face Liveness Detection Using Deep Learning
[7] Liveness Detection Using 3D Face Models
[8] Convolutional Neural Networks for Face Liveness Detection
[9] Adversarial Attacks on Face Liveness Detection Systems
[10] Face Recognition on Raspberry Pi: A Comparative Study of Different architectures
[11] A Face Spoofing Detection Method Based on Domain Adaptation and Lossless Size Adaptation
[12] Face Detection and Recognition System Using Raspberry Pi
[13] Real Time Face Recognition using Raspberry Pi
[14] Classroom Attendance Using Face Detection and Raspberry-Pi
[15] Face Liveness Detection Using Deep Learning
[16] A Survey on Face Spoofing Detection Techniques
[17] Face Anti-Spoofing Using Two-Stream Network
DeepFaceLiveness: A Deep Learning Approach for Face Liveness Detection

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details