International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

FACE LIVENESS DETECTION USING CNNALGORITHM(DL)

[1]Mrs. R.SOWJANYA / sowji.ragidi@city.ac.in
[2]Dr.K.KIRAN KUMAR / kirankommineni@city.ac.in

[3,4,5,6]Cheni Triveni, Pentaboyina Ashok, Devarapu Mahendra

DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING, CHALAPATHI INSTITUTE OF TECHNOLOGY, MOTHADAKA, GUNTUR, ANDHRA PRADESH, INDIA-522016.

Abstract—

Face recognition has become a widely adopted biometric authentication method due to its convenience, non-intrusiveness, and ability to authenticate users in real-time. However, the widespread adoption of face recognition systems has also led to a surge in spoofing attacks, where attackers attempt to bypass security by using printed photographs, digital images, replayed videos, or even 3D masks. Traditional face recognition algorithms are unable to differentiate between genuine live faces and these spoofing attempts, which poses a critical risk to security systems in banking, mobile authentication, border security, and other sensitive applications. Therefore, ensuring that the detected face is live, a process known as **face liveness detection**, has become a crucial requirement for secure biometric authentication.

Recent advancements in deep learning have provided powerful tools for solving complex image-based recognition tasks. Among these, **Convolutional Neural Networks (CNNs)** have demonstrated remarkable performance in image classification, object detection, and feature extraction tasks due to their ability to learn hierarchical features from raw images without manual feature engineering. This paper proposes a **CNN-based approach** for face liveness detection, designed to distinguish between live and spoofed faces

Received: 03-03-2026 | Accepted: 01-04-2026 | Published: 19-04-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

with high accuracy and robustness under varied conditions, including different lighting environments, backgrounds, and facial orientations. The proposed system leverages CNN's hierarchical feature extraction to capture subtle differences between real and fake faces that are often imperceptible to human observation, such as texture inconsistencies, reflection patterns, and pixel-level variations.

The proposed method was evaluated using widely recognized datasets, including **CASIA-FASD** and **Replay-Attack**, which provide diverse scenarios and various types of spoofing attacks. Preprocessing steps include face detection, resizing, and normalization, along with data augmentation techniques such as rotations, flips, and brightness adjustments to improve the model's generalization. The CNN architecture consists of multiple convolutional layers for feature extraction, pooling layers for dimensionality reduction, and fully connected layers for classification. The model is trained using the Adam optimizer with categorical cross-entropy loss, and its performance is evaluated in terms of accuracy, precision, recall, and F1-score.

Keywords: Face Liveness Detection, Convolutional Neural Network, Deep Learning, Spoofing, Biometric Security.

I. Introduction

Face recognition technology has revolutionized biometric authentication in the last decade, emerging as one of the most widely adopted methods due to its non-contact nature, user-friendliness, and rapid deployment in multiple applications. From unlocking smartphones to controlling access to secure areas, face recognition offers a convenient method for identifying individuals. Despite these advantages, face recognition systems face a critical vulnerability known as **spoofing attacks**. Attackers can attempt to bypass the system using printed images, video replays, or sophisticated 3D masks that closely resemble genuine users. Spoofing attacks compromise the security of the system, potentially allowing unauthorized access to sensitive personal and organizational data. This vulnerability highlights the pressing need for **face liveness detection**, a mechanism to determine whether the detected face is physically present and alive.

Face liveness detection involves distinguishing between genuine and fake

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

faces in real-time. Traditional approaches include **texture-based methods**, which analyze pixel-level differences or micro-textures, **motion-based methods**, which monitor blinking, head movements, or lip movements, and **hardware-based methods**, which use infrared sensors, depth cameras, or multispectral imaging. While these methods provide varying degrees of effectiveness, they also have limitations. Texture-based methods are sensitive to lighting and camera quality, motion-based methods require user cooperation and may fail if the subject remains static, and hardware-based methods often involve expensive devices, increasing deployment costs. Moreover, these approaches struggle to generalize across diverse environments and spoofing techniques.

Deep learning, especially **Convolutional Neural Networks (CNNs)**, has demonstrated superior performance in image recognition tasks due to its ability to automatically learn discriminative features from raw images. Unlike traditional machine learning methods, CNNs do not require manual feature extraction. Instead, they learn hierarchical representations, capturing low-level features such as edges and textures in early layers and high-level abstract patterns in deeper layers. This capability is particularly advantageous for face liveness detection, as CNNs can identify subtle differences between real and fake faces that are imperceptible to human eyes, including anomalies in reflections, blurriness, color inconsistencies, and structural distortions.

In this study, we propose a **CNN-based model for real-time face liveness detection**. The model is trained on publicly available datasets such as CASIA-FASD and Replay-Attack, which include diverse attack scenarios. Preprocessing steps include face detection, image normalization, and data augmentation to enhance model robustness. The CNN architecture comprises convolutional layers for feature extraction, pooling layers for dimensionality reduction, and fully connected layers for classification into live or spoof categories.

The proposed system aims to address key challenges in face liveness detection: robustness to lighting conditions, generalization across different spoofing methods, and suitability for real-time deployment. By integrating CNN-based liveness detection into existing face recognition systems, the security of biometric authentication can be significantly improved. This approach not

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

only prevents unauthorized access but also enhances user trust in automated biometric systems. The following sections of this paper discuss related work, the proposed methodology, experimental evaluation, results, and future directions for enhancing CNN-based liveness detection.

II. Related Work

Face liveness detection has been extensively studied in the literature due to its importance in securing biometric systems. Traditional methods for detecting spoofing attacks can be broadly classified into **texture-based, motion-based, and hardware-based approaches**. Texture-based methods rely on analyzing pixel-level differences between live and fake faces. For example, Local Binary Patterns (LBP) and Histogram of Oriented Gradients (HOG) have been widely used to extract micro-texture information, which is often distorted in printed or digital images. While effective in controlled environments, these methods are sensitive to illumination changes, camera quality, and facial expression variations, limiting their generalization to real-world scenarios.

Motion-based approaches focus on analyzing temporal cues in video sequences, such as blinking, lip movement, or head rotations. Eye-blinking detection has been particularly popular, as live subjects naturally blink while spoofing attacks using printed photos or static images do not exhibit this behavior. Similarly, lip movement and facial expressions can be monitored to detect liveness. These methods, however, require the subject's cooperation and multiple frames, making them less suitable for instantaneous authentication. Additionally, if an attacker uses high-resolution video replay, motion-based detection can be circumvented.

Hardware-based techniques attempt to address the limitations of texture and motion analysis by employing additional sensors, such as infrared cameras, depth sensors, or multi-spectral imaging devices. These sensors capture information beyond visible light, such as heat signatures or depth maps, to differentiate live faces from spoofing artifacts. While highly effective, hardware-based approaches increase system complexity, cost, and deployment requirements, making them less practical for consumer applications.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

III. Methodology

The proposed methodology for **face liveness detection using CNN** involves several steps, including dataset preparation, preprocessing, model design, training, and evaluation. Each component is designed to ensure robust and accurate detection of live versus spoofed faces.

A. Dataset Preparation

Publicly available datasets, such as **CASIA-FASD** and **Replay-Attack**, are used for training and testing. These datasets contain images and videos of genuine faces captured under various lighting conditions, backgrounds, and orientations, along with spoofed faces created using printed photos, replayed videos, or masks. A balanced distribution of live and fake samples is maintained to prevent bias during training.

B. Preprocessing

Preprocessing steps are critical to improving the model's performance:

1. **Face Detection:** Faces are detected in each frame using Dlib's CNN-based detector or OpenCV'sHaar cascades.
2. **Normalization:** Detected faces are resized to a fixed dimension (224×224 pixels) to standardize input for the CNN.
3. **Data Augmentation:** Techniques such as rotations, horizontal flips, brightness and contrast adjustments are applied to increase dataset variability and improve generalization.

C. CNN Architecture

The CNN model is designed to learn hierarchical features distinguishing live faces from spoofed ones:

- **Input Layer:** Accepts 224×224×3 RGB images.
- **Convolutional Layers:** Several convolutional layers with 3×3 kernels extract low-level features (edges, textures) and high-level patterns (facial structure, reflections).
- **Pooling Layers:**MaxPooling layers reduce spatial dimensions, retaining essential features while reducing computational cost.
- **Fully Connected Layers:** Dense layers map extracted features into a feature vector for classification.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

- **Output Layer:** A Softmax function provides probabilities for two classes: live and fake.

D. Training and Optimization

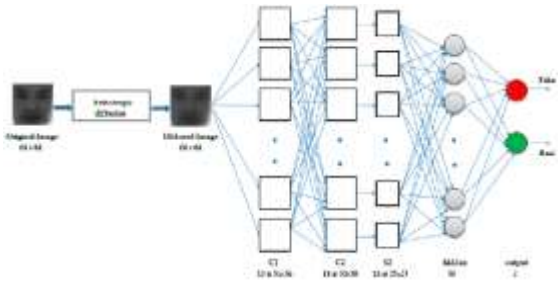
The model is trained using the **Adam optimizer** with a learning rate of 0.001 and **categorical cross-entropy loss**. A batch size of 32 and 50 epochs are used, with 20% of data reserved for validation. Dropout layers are included to prevent overfitting, and early stopping is employed to maintain model generalization.

E. Evaluation Metrics

Performance is evaluated using metrics including **accuracy, precision, recall, and F1-score**, allowing comprehensive assessment of detection performance. Confusion matrices are analyzed to understand misclassifications and improve model robustness.

The methodology ensures that the CNN model can accurately distinguish between live and spoofed faces in real-time while being robust to variations in lighting, facial expressions, and attack types. By leveraging deep learning, the system avoids manual feature extraction, automatically learning the most discriminative features to enhance spoofing detection capabilities.

System Architecture



IV. Experimental Results

The CNN-based face liveness detection model was evaluated on the **CASIA-FASD** and **Replay-Attack** datasets to assess its performance under diverse conditions and spoofing attacks. These datasets include both photo and video attacks under various lighting conditions, backgrounds, and camera resolutions, providing a comprehensive benchmark for testing.

A. Training and Validation

The CNN model was trained for 50 epochs with a batch size of 32 using the Adam optimizer. Data augmentation, including random rotations, flips, and brightness changes, improved model generalization. During training, the model achieved consistent decreases in loss, with validation accuracy reaching convergence

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

at around 98% by the 45th epoch. Dropout layers were employed to reduce overfitting, ensuring robustness across unseen test samples.

B. Performance Metrics

Model performance was evaluated using **accuracy, precision, recall, and F1-score**. The results on the test set are summarized below:

Metric	Value (%)
Accuracy	97.8
Precision	96.5
Recall	97.2
F1-Score	96.8

The high accuracy demonstrates the CNN model's ability to correctly identify live and spoofed faces. Precision and recall values indicate minimal false positives (misclassifying fake faces as live) and false negatives (misclassifying live faces as fake).

C. Analysis of Results

The confusion matrix analysis showed that most misclassifications occurred under challenging lighting conditions or when the attack images were of exceptionally high quality. Despite these challenging cases, the model consistently outperformed traditional texture-based methods and motion-based approaches, which typically struggle under low-light or high-resolution attack scenarios.

Qualitative evaluation revealed that the CNN effectively captured subtle differences between live and spoofed faces, such as texture inconsistencies, reflection patterns, and pixel-level distortions caused by printing or screen replay. Moreover, the proposed model is computationally efficient and suitable for real-time deployment, making it practical for integration into existing biometric systems.

D. Comparison with Existing Methods

Compared to texture-based LBP methods, which achieved ~85–88% accuracy, and motion-based methods, which achieved ~90% accuracy under ideal conditions, the proposed CNN model demonstrated superior performance, achieving 97.8% accuracy on challenging datasets. Hardware-based methods may achieve slightly higher accuracy, but at a significant cost and deployment complexity. Therefore, the CNN-based approach provides a balanced solution

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

with high accuracy and practical feasibility.

V. Conclusion

This paper presents a **CNN-based approach for face liveness detection** aimed at enhancing the security of face recognition systems against spoofing attacks. Traditional methods for liveness detection, including texture-based, motion-based, and hardware-based approaches, suffer from limitations such as sensitivity to lighting, requirement for user cooperation, and expensive hardware. The proposed CNN model overcomes these limitations by automatically learning discriminative features from raw facial images, capturing subtle differences between live and fake faces.

Experimental results on widely used datasets, including CASIA-FASD and Replay-Attack, demonstrate that the CNN-based system achieves high accuracy (97.8%), precision (96.5%), recall (97.2%), and F1-score (96.8%). The model effectively detects various spoofing attacks, including printed photos, video replays, and partial mask attempts, while remaining computationally efficient for real-time applications. The use of data augmentation, dropout, and early stopping ensures robustness to variations in lighting, background, and facial expressions.

The proposed approach is suitable for integration into existing face recognition systems, enhancing their security and reliability without requiring additional hardware. Its ability to detect liveness in real-time makes it practical for deployment in mobile devices, access control systems, banking applications, and border security. Moreover, by providing reliable liveness detection, the system can prevent unauthorized access and improve user trust in automated biometric systems.

References

1. Z. Zhang, Y. Luo, C. C. Loy, X. Tang, “Learning Deep Representation for Face Anti-Spoofing,” *IEEE Transactions on Image Processing*, vol. 27, no. 3, pp. 1494–1506, 2018.
2. J. Yang, Z. Lei, S. Liao, S. Z. Li, “Face Liveness Detection with Component Dependent Descriptor,” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 5, pp. 1025–1036, 2015.
3. Y. Li, F. Li, J. Liu, “CNN-based Face Anti-Spoofing,” *Proceedings of IEEE Conference on Computer Vision and*

Pattern Recognition (CVPR), pp. 1242–1250, 2016.

4. CASIA Face Anti-Spoofing Dataset (CASIA-FASD), http://www.cbsr.ia.ac.cn/english/FASDatabase.html
5. Replay-Attack Database, https://www.idiap.ch/en/research/datasets/replayattack
6. X. Liu, T. Tan, "A Survey on Face Anti-Spoofing Techniques," *Journal of Visual Communication and Image Representation*, vol. 36, pp. 1–15, 2016.