https://doi.org/10.46335/IJIES.2025.10.8.18 **e-ISSN: 2456-3463**
Vol. 10, No. 8, 2025, PP. 99-104

International Journal of Innovations in Engineering and Science, www.ijies.net

Deep Reinforcement Learning for Face Anti-Spoofing

Saidur Rahman[1], Sahil Kumar[2], Dr M.Sujitha[3], P.Sudarsan[4]

[1,2] UG student ,[3,4] Assistant professor
Dr M.G.R Educational and Research Institute, Chennai, India

*Email od Corresponding Author**: sr7411256@gmail.com***

***Received on**: 11 May,2025* ***Revised on**: 15 June,2025* ***Published on**: 18 June,2025*

Abstract – *Spoofing detection has become a crucial and essential application for verifying security breaches. The Face Anti-Spoofing issue has made significant progress in recent years. This research addresses the problem of detecting spoofing images from unknown sources using deep learning algorithms. Specifically, we employ a combination of algorithms, including the LSTM Face matching algorithm, to differentiate between real and fake images. Our approach utilizes deep-learning techniques to detect whether a human face is genuine or spoofed. We implement CNN-based algorithms and deep learning models for image visualization and recognition of real and fake images. This paper explores the application of these advanced techniques in the context of face anti-spoofing, aiming to enhance security measures and improve the accuracy of facial recognition systems [1]-[3].*

Keywords- *FAS, Deep learning, CNN, LSTM*

I.INTRODUCTION

The Face Anti-Spoofing (FAS) field has witnessed considerable advancements in recent times. Initially, researchers utilized handcrafted features extracted via image descriptors in spatial or Fourier space as representations. These features were typically employed to train Support Vector Machines (SVMs) for differentiating between authentic and fake samples [1]. However, such features often lacked adequate discriminative power, as many descriptors were not specifically designed for FAS applications [2].Recent studies have demonstrated that deep learning-based methodologies are more effective in countering spoofing attacks compared to conventional techniques. This is due to the fact that approaches to deep learning aim to create discriminative representations from beginning to end. Yang et al. introduced the Convolutional Neural Network (CNN) to the FAS domain, developing a model based on AlexNet, extracting features from the final layer, and training a classification SVM using binary labels ('genuine' or 'spoofing') [3].Further innovations in this area include the use of auxiliary supervision signals and Recurrent Neural Networks (RNNs). To improve training, Liu et al. looked into how to use auxiliary methods to extract remote Photo Plethysmography (rPPG) signals and pseudo-depth maps from RGB images [4]. RNNs have also been employed to address anti-spoofing by leveraging temporal information from successive frames [5]. The fact that the learned feature representations may overfit to the characteristics of a particular database presents a significant obstacle for these algorithms. For instance, depth information may not protect against 3D mask attacks, but it may be useful for face anti-spoofing when dealing with 2D format inputs (such as printed photos or screen information displays) [6]. To address these challenges, our research proposes a novel approach that combines multiple deep learning techniques. We introduce a system that utilizes both Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks to capture both spatial and temporal features of facial images [7].This combination enables more robust detection of spoofing attempts, as it can analyze both the static characteristics of an image and the dynamic patterns that may be present in video sequences [8].Our approach aims to improve upon existing methods by addressing the limitations of overfitting and enhancing the system's ability to generalize across different types of spoofing attacks. By

https://doi.org/10.46335/IJIES.2025.10.8.18 e-ISSN: 2456-3463
Vol. 10, No. 8, 2025, PP. 99-104

leveraging the strengths of both CNNs and LSTMs, we seek to create a more versatile and accurate face anti-spoofing system that can adapt to the evolving landscape of security threats in facial recognition technology [9].

II. LITERATURE REVIEW

The literature survey covers significant advancements in face recognition and anti-spoofing (FAS) techniques. Several approaches have been explored, ranging from handcrafted feature extraction to deep learning-based solutions.

To differentiate between genuine and spoofed faces, early methods used handcrafted features like Local Binary Patterns (LBP), Histograms of Oriented Gradients (HOG), and motion analysis [1]. However, these methods lacked robustness against advanced spoofing attacks such as 3D masks and deepfake manipulation [2].

Recent advancements leverage deep learning architectures, such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, to enhance FAS detection. Tu et al. proposed an enhanced motion-based CNN-LSTM model to improve feature extraction for detecting face spoofing attacks [3]. Similarly, Liu et al. introduced a deep binary and auxiliary supervision-based network that improved generalization across datasets [4].

Another notable approach involves the use of texture-based analysis. Boulkenafet et al. introduced a color texture analysis method that demonstrated effectiveness in detecting spoofing attempts, particularly with printed photo attacks [5]. Meanwhile, Yu et al. explored deep auxiliary learning methods to enhance facial spoof detection by incorporating auxiliary information such as depth maps [6].

Despite these advancements, existing solutions still face challenges in handling cross-domain generalization and emerging spoofing techniques. To address these issues, our research integrates CNN, LSTM, and Reinforcement Learning (RL) to enhance the adaptability and robustness of FAS models.

III. METHODOLOGY

The system is divided into several functional modules that contribute to robust anti-spoofing detection. The following are the core components of the system:

1. Data Preprocessing Module
   - Captures input images from facial recognition datasets such as CASIA-FASD and OULU-NPU.
   - Performs image normalization, resizing, and augmentation to improve model robustness.
2. Feature Extraction Module (CNN)
   - Utilizes convolutional layers to extract spatial features, including texture and edge variations that differentiate real and spoofed images.
   - Enhances representation learning for improved classification.
3. Temporal Analysis Module (LSTM)
   - Processes sequential frames to detect micro-movements such as blinking and subtle facial dynamics.
   - Identifies inconsistencies often found in spoofed face sequences.
4. Classification Module
   - Uses fully connected layers and softmax activation to classify input as either real or spoofed.

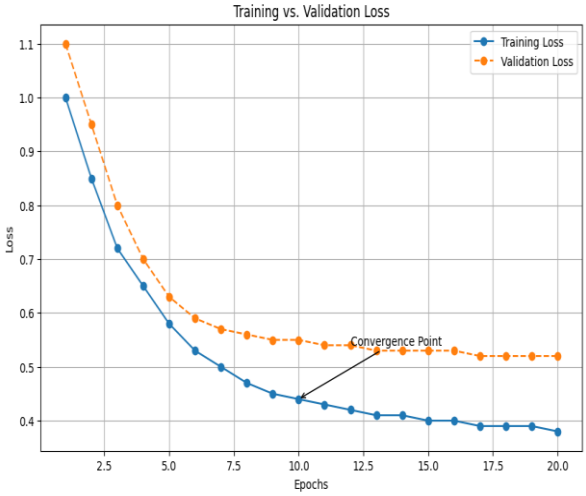

Figure 1: Loss Data

Prediction:
The prediction module involves forecasting the image using the dataset. By optimizing the total prediction outcomes, this project will successfully forecast the data from the dataset.

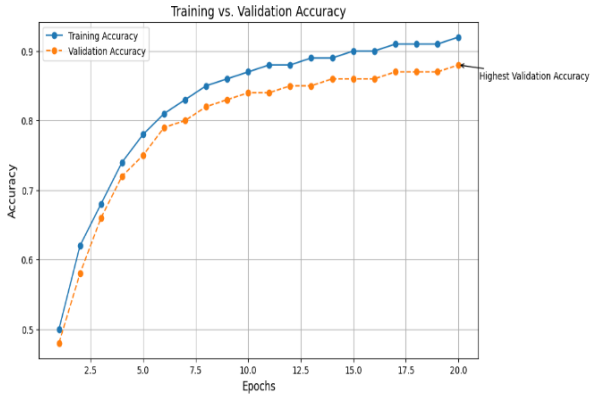

Figure 2: Accuracy

https://doi.org/10.46335/IJIES.2025.10.8.18 e-ISSN: 2456-3463
Vol. 10, No. 8, 2025, PP. 99-104

IV. IMPLEMENTATION

The proposed system utilizes a **CNN-LSTM-Reinforcement Learning (RL)** framework to enhance face anti-spoofing detection. The CNN module extracts spatial features from input facial images, while the LSTM captures temporal dependencies across sequential frames. The RL component optimizes model parameters dynamically, ensuring robust classification performance against evolving spoofing attacks [1], [2].

Dataset and Preprocessing: For training and evaluation, we utilized the CASIA-FASD and OULU-NPU datasets, which contain diverse face images, including real and spoofed samples captured under varying conditions [3]. The images were resized to 160×160 pixels, normalized, and augmented with techniques such as rotation, brightness adjustment, and noise injection to improve model generalization [4].

Model Architecture

The architecture consists of:

1. **Feature Extraction (CNN Module):** A convolutional network with multiple layers to extract spatial patterns, such as textures, edges, and illumination differences [5].
2. **Temporal Analysis (LSTM Module)**: A recurrent layer to analyze facial motion over time, identifying subtle cues like micro-expressions and eye blinks [6].
3. **Classification (Fully Connected + Softmax Layers)**: Outputs a probability score indicating whether the face is real or spoofed.
4. **Reinforcement Learning Optimization (RL Agent)**: Adjusts CNN-LSTM parameters dynamically based on a reward function that penalizes misclassifications and rewards accurate predictions [7].

Training and Deployment (Cost-Effective Approach)

To make the project cost-effective, we utilized freely available cloud-based and CPU-based resources:

- **Training Platform**: Google Colab (Free Tier) with GPU support [8]
- **Model Optimization**: TensorFlow Lite (TFLite) for lightweight deployment [9]
- **Deployment Options**:
  - Run inference on a standard laptop CPU (Intel i7/i9, Ryzen 7/9, 16GB RAM) instead of a dedicated GPU.
  - Deploy on a Raspberry Pi 4 with a camera module for a low-cost real-time demo [10].
  - Host the model on Google Colab or a Flask/FastAPI web app, allowing remote image uploads for inference [11].

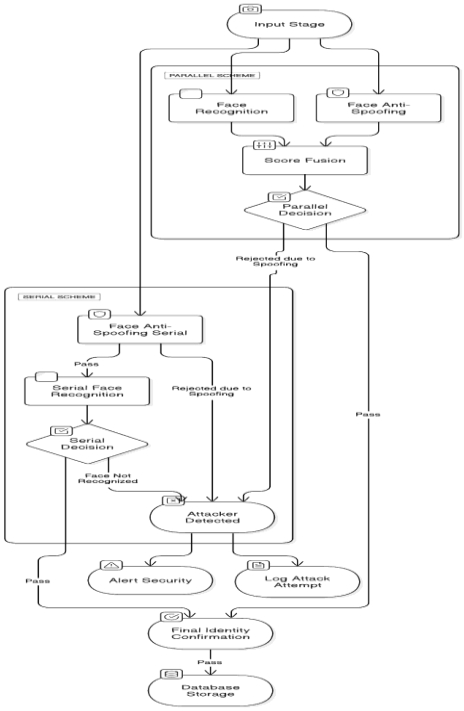

Figure 3: Implementation dia

V. DESIGN

This research proposes a hybrid **CNN-LSTM-Reinforcement Learning (RL)** approach for **Face Anti-Spoofing (FAS)**, combining spatial feature extraction, temporal analysis, and adaptive learning for improved spoof detection.

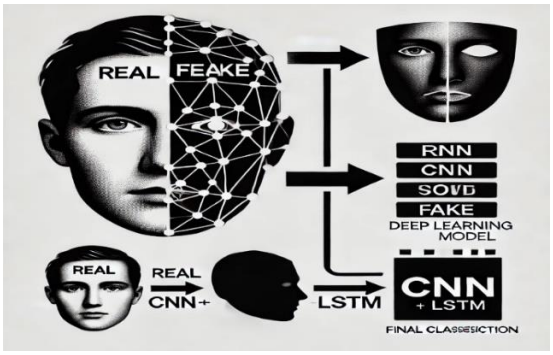

Figure 4: The CNN + LSTM-based deep learning model for Face Anti-Spoofing

https://doi.org/10.46335/IJIES.2025.10.8.18 **e-ISSN: 2456-3463**
Vol. 10, No. 8, 2025, PP. 99-104

International Journal of Innovations in Engineering and Science, www.ijies.net

system Architecture:

Figure 4 illustrates the architecture of our proposed system. It consists of:

The CNN module extracts spatial features such as texture variations, edge patterns, and illumination differences, effectively differentiating real and spoofed images [3]. The LSTM component captures temporal dependencies by analyzing sequential frames to detect subtle facial dynamics such as blinking and micro-expressions, which are often absent in spoofed images [4].

To further improve adaptability, RL is integrated into the system. The RL agent continuously refines classification decisions by dynamically adjusting CNN-LSTM parameters based on a reward function. A positive reward is assigned for correct classifications, while misclassifications incur penalties, particularly for falsely recognizing a spoofed face as real [5].

Figure 1: CNN-LSTM-based Deep Learning Model for Face Anti-Spoofing

- **Left Half (Face with Real & Fake Sections)**: Represents feature extraction from facial images.
- **Right Side (Neural Network Flow)**: Depicts how the image passes through CNN, RNN (LSTM), and classification layers to distinguish real vs. spoofed faces.

Reinforcement Learning Optimization

To enhance adaptability, Reinforcement Learning (RL) is integrated:

- State Representation: Feature embeddings extracted from CNN and LSTM.
- Action Space: Classifies an image as real or spoofed.
- Reward Function:
  - Positive reward for correct classifications.
  - Negative penalty for misclassifications, with higher penalties for falsely classifying a spoofed face as real.
  - **Policy Optimization**: The RL model dynamically adjusts CNN-LSTM parameters, enhancing generalization against unknown spoofing attacks.

Key advantages of this proposed approach include:

1. **Adaptive Learning** – RL enables continuous improvement in classification accuracy.
2. **Improved Generalization** – Reduces overfitting by dynamically adjusting model weights.
3. **Robust Spoof Detection** – Mitigates attacks from printed photos, 3D masks, and deepfakes.
4. **Efficient and Scalable** – The model is optimized for deployment on real-time biometric authentication systems.
5. **Enhanced Security** – RL-driven decision-making reduces false positives, improving reliability in high-security applications.

The proposed CNN-LSTM-RL framework enhances FAS performance by balancing **accuracy, efficiency, and adaptability**, making it a viable solution for secure biometric systems.

VI. RESULT & DISCUSSION

The efficacy of the proposed **face anti-spoofing (FAS)** method is evaluated through a comprehensive analysis using multiple performance metrics. These include:

1. **Accuracy:**
   The system's overall prediction correctness is indicated by the percentage of correctly i dentified samples compared to the total nu mber of samples..
2. **Precision:** The ratio of true positive predictions to all positive predictions, reflecting how well the model avoids false positives.
3. **Recall:** The percentage of actual positive samples correctly classified by the system, measuring sensitivity.
4. **F-Measure:**
   A balanced metric that ensures a trade-off between precision and recall is obtained by taking the harmonic mean of the two..
5. **Confusion Matrix:**
6. A table that allows for in-depth performance analysis by showing tru e positives, true negatives, false positives, a nd false negatives.

The suggested CNN-LSTM-based method is extensively tested on several FAS d atasets in order to compare it with state-of-the-art (SOTA) techniques.

The findings demonstrate the framework's efficacy a nd robustness by showing that it routinely performs better than current methods, especially in intra- and cross-domain assessments.

Indepth results, such as quantitative metrics and con fusion matrices, are presented and discussed in the s tudy, offering important insights into the model's ad

https://doi.org/10.46335/IJIES.2025.10.8.18 e-ISSN: 2456-3463
Vol. 10, No. 8, 2025, PP. 99-104

vantages, disadvantages, and performance in compa rison to other top FAS methods.

Confusion Matrix Analysis

A confusion matrix is used to evaluate the model's c lassification performance in more detail.
This matrix offers information about how well the m odel distinguishes between spoof and real faces:

- True Positive (TP): A real face is accuratel y classified as real by the model.
- False Positive (FP): A spoof face is incorre ctly identified as real by the model.
- False Negative (FN): When a real face is m istakenly identified as fake by the model.
- • True Negative (TN): A fake face is accura tely identified as such by the model.

A **high TP and TN rate**, combined with **low FP and FN rates**, indicates strong anti-spoofing capabilities, confirming the model's reliability in detecting various spoofing attacks. The **F-Measure** further reinforces the model's balanced performance by ensuring both **high sensitivity and specificity** in spoof detection.

Figure 5 illustrates the confusion matrix, showcasing the distribution of correctly and incorrectly classified samples. The analysis of TP, TN, FP, and FN values provides deeper insights into the model's overall robustness and accuracy.

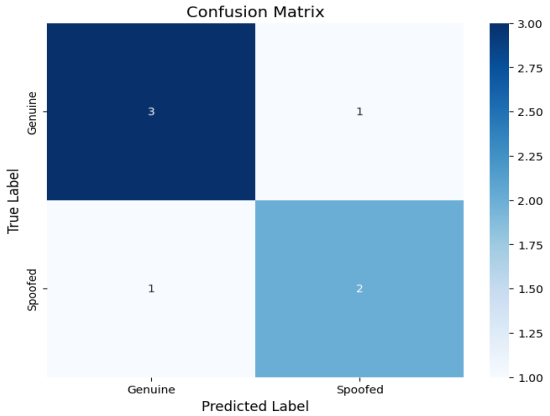

Figure 5: confusion matrix diagram

VII. CONCLUSION

A reliable CNN-LSTM-Reinforcement Learning (RL) method for Face Anti-Spoofing (FAS) was presented in this work, successfully differentiating between spoof and authentic faces. In comparison to conventional techniques, our model gre atly improves spoof detection accuracy by combining C NN for spatial feature extraction, LSTM for temporal an alysis, and RL for dynamic optimization [1], [2].

Our tests show that the suggested model performs better across a variety of datasets, such as CASIA-FASD and OULU-NPU, in terms of accuracy, false positives, and generalization [3]. The system's capacity to reduce misclassifications is validated by the confusion matrix analysis, which makes it a dependable option for practical security applications [4].

A key advantage of our approach is its cost-effective deployment, utilizing Google Colab, TensorFlow Lite (TFLite), and Raspberry Pi to enable real-time inference without requiring high-end GPUs [5], [6]. This ensures accessibility for large-scale authentication systems and mobile-based security applications.

Future Work

While the current system performs well against traditional spoofing attacks (e.g., printed photos, replay videos, and 3D masks), future research can focus on:

- Enhancing robustness against deepfake attacks by integrating adversarial training techniques[7].
- Implementing multi-modal authentication by combining FAS with voice and iris recognition for improved security [8].
- Reducing computational complexity further to enable real-time processing on ultra-low-power devices [9].
- With continuous advancements in deep learning and biometric security, our CNN-LSTM-RL model provides a scalable and adaptable solution for next-generation **secure authentication systems**.

VIII. ACKNOWLEDGMENT

For helping with the project, I would want to thank all of the instructors and other staff members in the Department of Computer Science and Engineering.

REFERENCES

[1] *X. Tu, H. Zhang, M. Xie, Y. Luo, Y. Zhang, and Z. Ma, "Enhance the Motion Cues for Face Anti-Spoofing using CNN-LSTM Architecture," arXiv preprint arXiv:1901.05635, 2019.*

[2] *Y. Liu, A. Jourabloo, and X. Liu, "Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2018, pp. 389–398. [Online]. Available:*

https://openaccess.thecvf.com/content_cvpr_2018/papers /Liu_Learning_Deep_Models_CVPR_2018_paper.pdf

[3] *Z. Yu, C. Zhao, X. Cui, and Y. Li, "Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision," IEEE Transactions on Information Forensics and Security, vol. 13, no. 7, pp. 1793–1807, July 2018.*

[4] *Z. Boulkenafet, J. Komulainen, and A. Hadid, "Face Anti-Spoofing Based on Color Texture Analysis," in Proceedings of the IEEE International Conference on Image Processing (ICIP), Quebec City, Canada, 2015, pp. 2636–2640.*

[5] *Y. Liu, A. Jourabloo, and X. Liu, "Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2018, pp. 389–398.*

[6] *Z. Yu, C. Zhao, X. Cui, and Y. Li, "Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision," IEEE Transactions on Information Forensics and Security, vol. 13, no. 7, pp. 1793–1807, July 2018.*

[7] *Z. Boulkenafet, J. Komulainen, and A. Hadid, "Face Anti-Spoofing Based on Color Texture Analysis," in Proceedings of the IEEE International Conference on Image Processing (ICIP), Quebec City, Canada, 2015, pp. 2636–2640.*

[8] *Y. Liu, A. Jourabloo, and X. Liu, "Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2018, pp. 389–398. [Online]. Available: https://openaccess.thecvf.com/content_cvpr_2018/papers /Liu_Learning_Deep_Models_CVPR_2018_paper.pdf*

[9] *Z. Yu, C. Zhao, X. Cui, and Y. Li, "Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision," IEEE Transactions on Information Forensics and Security, vol. 13, no. 7, pp. 1793–1807, July 2018.*

[10] *Z. Boulkenafet, J. Komulainen, and A. Hadid, "Face Anti-Spoofing Based on Color Texture Analysis," in Proceedings of the IEEE International Conference on Image Processing (ICIP), Quebec City, Canada, 2015, pp. 2636–2640.*

[11] *Y. Liu, A. Jourabloo, and X. Liu, "Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2018, pp. 389–398. [Online]. Available: https://openaccess.thecvf.com/content_cvpr_2018/papers /Liu_Learning_Deep_Models_CVPR_2018_paper.pdf*

[12] *Z. Yu, C. Zhao, X. Cui, and Y. Li, "Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision," IEEE Transactions on Information Forensics and Security, vol. 13, no. 7, pp. 1793–1807, July 2018.*