10.48047/jocaaa.2024.33.08.128

A DEEP LEARNING FRAMEWORK FOR DETECTING FACE SPOOFING IN BIOMETRIC AUTHENTICATION SYSTEMS

Monika
Research Scholar (Computer Science)
School of Engineering and Technology
Shri Venkateshwara University, Gajraula, UP, INDIA
Email*: monikamaan20@gmail.com*

Dr Tarun Kumar
Research Guide (Computer Science)
School of Engineering and Technology
Shri Venkateshwara University, Gajraula, UP, INDIA
Email: *taruncdac@gmail.com*

Abstract: The ability to detect spoofed faces has become a critical concern in various applications, such as face recognition systems, banking, and security measures. This research presents a simple yet effective system designed to determine whether a face in a video stream is real or spoofed using pre-trained models for face detection and anti-spoofing. By employing a continuous loop to read each frame of the video stream, the system first detects faces using a pre-trained face detection model. It then crops and resizes the detected face image for further analysis. If the anti-spoofing model predicts that the face is fake, the system highlights the face with a red rectangle and displays the label "spoof." Conversely, if the face is real, it is marked with a green rectangle and labeled "real." This straightforward approach ensures real-time processing and provides clear visual feedback on the authenticity of the face being analyzed. The proposed system demonstrated a high accuracy rate in detecting spoofed faces, underscoring its suitability for real-world applications. Its lightweight and efficient design makes it particularly advantageous for use in mobile devices and other low-computational power environments, without the need for sophisticated hardware. This positions the system as a reliable and cost-effective solution for enhancing security in various domains, including biometric authentication, surveillance, and financial transactions.

Keywords: CNN, Biometric, Spoof, Anti-spoofing, Neural ‘Network

1. INTRODUCTION

Biometrics is one of the most widely used authentication technologies today, with facial recognition being particularly popular due to its simplicity and accuracy. This technology is prevalent across smartphones, tablets, and laptops, using cameras and algorithms to identify individuals by comparing captured images to a database. However, facial recognition systems are vulnerable to spoofing attacks, where an attacker uses photos, videos, or masks to deceive the system. Because it is easier to obtain someone’s face from social media compared to other biometrics like fingerprints, these systems are particularly susceptible to such attacks [11]. Spoofing attacks can be static, using photos or masks, or dynamic, using video replays or 3D models to mimic facial expressions.

Cybercrime is on the rise in our digitally advanced world. Many organizations are now exploring biometric face recognition as a viable security solution. This innovative technology shows a lot of promise and could revolutionize how we access sensitive information. However, despite its potential, facial recognition has its flaws. User photos can easily be found through social networks and used to spoof facial recognition software. Therefore, it is crucial for organizations to implement face anti-spoofing systems to protect sensitive data, reduce theft, and mitigate fraud. These systems enhance existing facial recognition solutions by improving their ability to detect fraud [12-13]. While this sounds promising, challenges remain. What stops someone from using a fake face to access sensitive data? This is where the need for anti-spoofing solutions comes into play. We rely on liveness detection to verify a person's identity. These checks can confirm whether an individual is actually present or using a photo to spoof the system (Figure 1) .

10.48047/jocaaa.2024.33.08.128

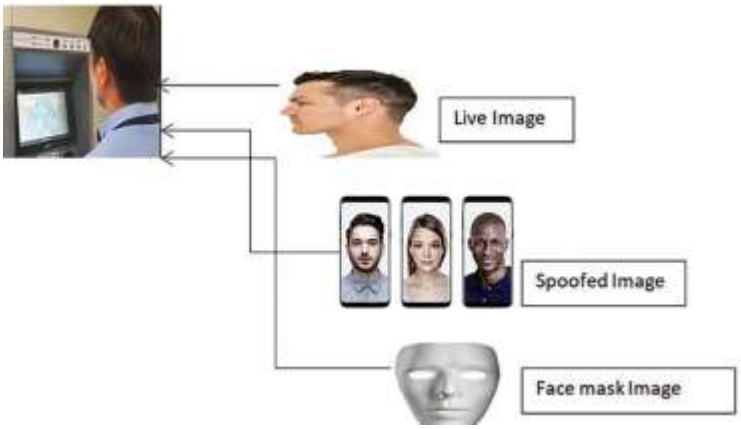

Figure 1: Types of image spoofing attacks

Liveness detection is a security feature that ensures biological identifiers are from the correct user and not someone else. Traditional methods include eye or lip movement analysis, prompted movement instructions, surface/reflection detection in video feeds, or zooming motion detection. Another recent method is 3D depth analysis. There are two approaches to liveness detection: active and passive. Active liveness detection involves the user performing an action, such as blinking, making facial movements, or keystroking, making it more difficult and time-consuming for someone to spoof the system. Passive liveness detection uses internal algorithms to detect spoofs and requires nothing from the user [14]. For example, when logging into a banking app using facial recognition, an active liveness detection system might require users to blink while it scans their face. Passive liveness detection, meanwhile, might scan a user's face to ensure a real human face with the correct depth contours is present. Many liveness detection methods, especially active approaches, take longer to identify users, reducing the speed, convenience, and simplicity of biometric ID.

To protect face recognition systems against spoofing attacks, many face anti-spoofing techniques have been proposed. Evaluations of these techniques on existing face anti-spoofing databases show very good performances. For instance, on the NUAA and the Replay-Attack databases, many techniques have achieved impressive performances (nearly 0% error rate) [15]. However, these face anti-spoofing databases were recorded in controlled environments, and their evaluation protocols do not reflect real-world scenarios, making the application of these techniques in real-world situations unreliable. Indeed, recent studies have revealed that the performance of state-of-the-art techniques degrades significantly under real-world variations (e.g., illumination and camera device variations), indicating that more robust face anti-spoofing methods are needed to reach the deployment levels of face biometric systems. To counter these spoofing attacks, advanced anti-spoofing techniques have been developed, including liveness detection methods such as eye-blink detection, which analyses natural blinking patterns to confirm a live face. However, as technology advances, simple blink detection is no longer sufficient against video replays. More robust methods, like 3D cameras and photoplethysmography, which analyze pixel depth, offer high precision in distinguishing real faces from flat objects. Additionally, deep learning and convolutional neural networks (CNNs) have been employed to improve anti-spoofing measures. By training CNNs to differentiate between genuine and spoofed images and combining them with traditional motion detection methods, these systems can more effectively detect spoofing in real-time, even under varied environmental conditions [16]. This combined approach enhances the resilience of facial recognition systems against a range of spoofing attacks, making them more reliable for real-world applications.

2. REVIEW OF LITERATURE

Recent advancements in facial recognition technology have spurred extensive research into anti-spoofing and liveness detection methods to enhance security against fraudulent attacks. Yuan et al. [1] leveraged Deep Convolutional Neural Networks (DCNN) and Deep Residual Networks (DRN) for

10.48047/jocaaa.2024.33.08.128

robust detection, though their complexity and overfitting remain challenges. Desktop applications using eye blink detection [2] effectively counter simple spoofing methods but are limited to desktop environments. Killioglu et al. [3] and Li et al. [4] proposed sophisticated techniques like pupil direction observation and shearlet transforms, which, despite high accuracy, require additional hardware and intensive computation. Peng and Chan [5] utilized high-frequency descriptors to improve feature detection under varied lighting, but rely heavily on high-quality cameras. Cai and Quan [6] addressed face alignment issues with a Multi-task Convolutional Neural Network (MTCNN), though its complexity poses implementation challenges. Mohamed et al. [7] and Hadiprakoso et al. [8] focused on eye and lip movement detection within CNN frameworks, effective against static spoofing but less so against dynamic attacks like 3D masks. Kumar et al. [9] and Singh et al. [10] employed neural networks and CNN-RNN models to enhance liveness detection, emphasizing depth and rPPG signal estimation, yet these methods face real-world applicability and computational demand issues.

Table 1: Revies of literature face spoofing

Reference No.	Algorithm Used	Key Features	Drawback
[1]	Deep Convolutional Neural Network (DCNN), Deep Residual Network (DRN)	Quick operation, few parameters, end-to-end self-learning, ROI extraction algorithm, adaptive learning rate adjustment	Complexity in training and potential overfitting due to deep network structure
[2]	Desktop anti-spoofing application	Counts eye blinks, liveness detection to prevent video playback and photo attacks, captures images at intervals, security countermeasures for breaches	Limited to desktop applications, may not be effective against sophisticated spoofing methods
[3]	Haar-cascade classifier, Kanade-Lucas-Tomasi (KLT) algorithm	Pupil direction observation, real-time eye region extraction and stabilization, pupil retrieval from eye region	Requires additional hardware, can be sensitive to head movements and lighting conditions
[4]	Multiscale directional transform (shearlet transform), stacked auto-encoders, softmax classifier	Effective face liveness detection and identification, tested with CASIA face anti-spoofing database, high performance	Computationally intensive, may struggle with real-time application and generalization to unseen conditions
[5]	High frequency descriptor-based approach	Reveals hair and skin features, handles lighting variations, enhances high frequency components of genuine face	Susceptible to varying lighting conditions and may require high-quality cameras
[6]	Multi-task Convolutional Neural Network (MTCNN)	Combines CNN with brightness equalization, three cascaded CNNs (P-net, R-net, O-net), precise face positioning	Complex implementation, potential issues with face alignment and varied lighting environments
[7]	Liveness detection using CNN classifier	Blinking eye and lip movement assessment, ConvNet classifier module, trains on multiple data sources	May not be effective against advanced spoofing techniques, such as 3D masks or high-quality video replays

10.48047/jocaaa.2024.33.08.128

[8]	CNN-based liveness detection	Focuses on eye blinking and lip movement, effective against video-based replay attacks, combines blinking eye module with ConvNet classifier	Limited effectiveness against sophisticated dynamic attacks, potential for high false positives/negatives
[9]	Neural network-based detection	Prevents spoofed faces from accessing, addresses photo, video replay, and 3-D attacks, ensures genuine live face images	High computational requirements, potential difficulties in real-time application and generalization
[10]	CNN-RNN model with auxiliary supervision	Estimates face depth and rPPG signals, pixel-by-pixel and sequence-by-sequence supervision, distinguishes between live and spoof faces	Complex training and implementation, may be prone to errors in varied real-world scenarios

3. RESEARCH METHODOLOGY

This study aims to develop an advanced anti-spoofing model incorporating three primary modules: face anti-spoofing detection, liveness detection, and criminal identification using a Convolutional Neural Network (CNN) classifier. The operational flow of this model is straightforward yet robust. Initially, the face anti-spoofing module processes input data to detect fraudulent attempts using photos, posters, masks, or smartphones. Upon detecting a face, the input is forwarded to the CNN classifier, which determines the authenticity of the face. If the face passes this check, it is then subjected to the liveness detection module, which verifies the presence of eye blinks and lip movements to ensure the face is live. Inputs that successfully pass through both modules are confirmed as real faces. Subsequently, these authenticated inputs are examined by the criminal identification module, which identifies whether the detected face belongs to a criminal based on pre-existing facial recognition data.

The methodology for developing the CNN classifier modules involves several critical steps: data collection, data pre-processing, model training, model evaluation, and testing. These steps ensure that the classifier is well-equipped to distinguish between real and spoofed faces accurately. Face spoofing is a type of attack where an unauthorized person attempts to breach a security system by using a photo, video, or 3D mask of an authorized person's face, aiming to steal their identity. To counteract this, an anti-spoofing face detection system is designed to distinguish between a spoofed face used by an attacker and the real face of an authorized person. This methodology outlines the steps and processes involved in developing such a system, along with the necessary libraries and tools.

Our methodology for developing the face anti-spoofing system involves several critical steps, ranging from capturing the initial input image to evaluating the system's effectiveness using a test set. Below is a detailed description of each step:

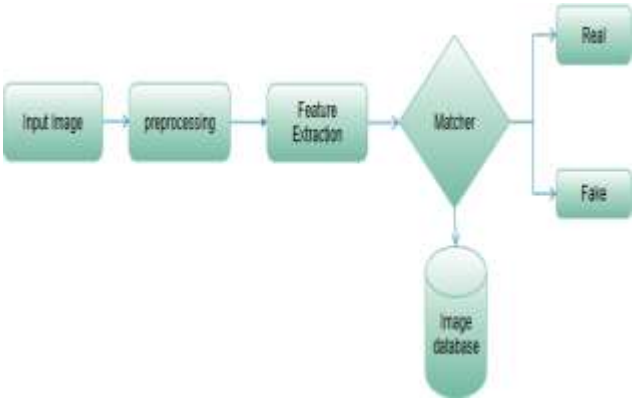

Figure 2: Research methodology

10.48047/jocaaa.2024.33.08.128

STEP 1: Input Image - Facial Image: The first step involves capturing a digital image of the face with sufficient resolution and quality to ensure accurate biometric matching. This image serves as the foundation for the entire process, and it must be of high enough quality to allow for effective facial spoofing detection. Advanced sensors are used to capture these images, ensuring that the data is suitable for subsequent analysis.

STEP 2: Pre-processing: Pre-processing is a crucial initial step that prepares the captured facial image for further analysis. This step includes several sub-processes:

- *Pixel Brightness Conversion/Brightness Correction:* Adjusting the brightness levels to ensure uniformity and enhance the image quality.
- *Geometric Transformation:* Correcting the image geometry to standardize the facial features and make them comparable across different images.
- *Image Filtering and Segmentation:* Applying filters to remove noise and segmenting the image to isolate the facial region from the background.

These pre-processing techniques enhance the quality of the facial image, making it suitable for the subsequent feature extraction phase.

STEP 3: Feature Extraction: Feature extraction is a critical step that involves creating combinations of variables that accurately represent the data. This process is essential for developing a robust model. Techniques employed here aim to optimize the representation of the facial image by identifying key features that distinguish between real and spoofed faces. Optimized feature extraction is considered a cornerstone of developing the best-performing machine learning models.

STEP 4: Matcher: The matcher component uses a search distance method to find matching features between two images. One image serves as the source image, and the other as the target image. The matcher identifies features in the source image and attempts to find corresponding features in the target image. This process is vital for detecting similarities and differences between real and spoofed faces.

STEP 5: Dataset and Training Image Database: An organized image database is used to manage and process queries efficiently. This database comprises a large collection of digital images, specifically compiled for machine learning projects. The datasets include both real and spoofed facial images, which are used to train, test, and evaluate the performance of our anti-spoofing model. These datasets are essential for ensuring that the model can generalize well to new, unseen images.

STEP 6: Spoof / Real: The "Spoofed/Real" classification is the critical outcome generated by our face spoofing detection algorithm. This algorithm is meticulously trained to distinguish between spoofed and genuine facial images. Utilizing advanced machine learning techniques, it analyses various features of the input image to determine its authenticity. When an image is processed, the algorithm assesses whether the facial features correspond to those of a real person or a spoofed attempt, such as a photo, video, or 3D mask. The result is then presented, indicating whether the image is "Spoofed" or "Real," thus ensuring robust security against identity theft and unauthorized access.

STEP 7: System Effectiveness: The effectiveness of our system is gauged using a test set. The test set includes a balanced mix of real and spoofed facial images, separate from the training data, to provide an unbiased evaluation of the model's performance. The evaluation test set is used to evaluate the model's performance. If the model predicts a face as fake (spoof), the system draws a red rectangle around the face and labels it as "spoof." Conversely, if the model predicts the face as real, it draws a green rectangle around the face and labels it as "real."

4. PROPOSED WORK

Our face anti-spoofing system is composed of two main components: a pre-trained face detection model and a deep learning anti-spoofing model. The face detection model identifies faces in video streams and extracts the relevant face regions for further analysis. We employed the Haar Cascade classifier for this purpose, which is known for its efficiency and effectiveness in real-time face detection.

a) Face Detection

10.48047/jocaaa.2024.33.08.128

The Haar Cascade classifier, provided by OpenCV, is utilized to detect faces within the video stream. This method uses a series of simple classifiers that are applied in stages to the image, ensuring rapid and accurate face detection. Once a face is detected, the model extracts and crops the face region, preparing it for the anti-spoofing analysis.

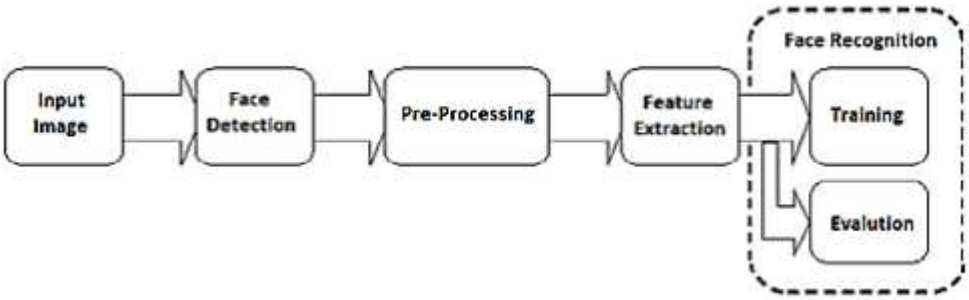

Figure 3: Basic steps of automated face recognition systems

b) Anti-Spoofing Model

The anti-spoofing component of our system is built on a convolutional neural network (CNN) architecture, chosen for its proven effectiveness in image recognition tasks. This deep learning model is trained to differentiate between spoofed and real faces. The input for the anti-spoofing model is the cropped face image from the face detection model, and the output is a probability score indicating whether the face is real or fake. We trained our anti-spoofing model using a dataset that includes images of both real and fake faces. The model employs binary cross-entropy loss and accuracy as the training objectives, and it is optimized using the Adam optimizer. The effectiveness of the model is enhanced through backpropagation and gradient descent techniques during the training phase.

The dataset used in this study is divided into two parts: the training set and the test set, following an 80:20 ratio. This allocation ensures that 80% of the data is used for training the model, providing it with ample examples to learn effectively, while the remaining 20% is reserved for testing to evaluate the model's performance unbiasedly. The training set optimizes the convolutional neural networks (CNNs) and fully connected networks through backpropagation and gradient descent techniques. Backpropagation involves propagating the model's prediction error back through the network to update weights, while gradient descent moves the weights in the direction of the negative gradient of the loss function, minimizing error and enhancing model performance. This method enables the model to learn complex patterns from the data, refining its ability to distinguish between spoofed and real faces. The model's efficacy is then assessed using the test set, which it has not seen during training, ensuring an accurate measure of its generalization capability and real-world applicability.

Table 2: Training and testing datasets

	Training Datasets	**Testing Datasets**
REAL	1800	500
SPOOF	2200	450
TOTAL	4000	950

The face anti-spoofing system's training dataset consists of 4000 images, including 1800 real face images and 2200 spoofed face images, which encompass a range of deceptive inputs like photographs, video replays, and 3D masks. This diverse training set enables the model to effectively learn the distinguishing features of genuine and fake faces. The testing dataset, comprising 950 images with 500 real and 450 spoofed faces, is used to evaluate the model's performance, ensuring its ability to accurately identify real versus spoofed faces in practical scenarios. This comprehensive approach aims to create a robust and reliable anti-spoofing system.

c) CNN Model

10.48047/jocaaa.2024.33.08.128

A deep convolutional neural network (CNN) for spoof detection is designed to differentiate between real and fake facial images with high accuracy. The architecture typically consists of multiple layers, including convolutional layers, pooling layers, and fully connected layers, each serving a specific function in feature extraction and classification (Figure 4 and 5).

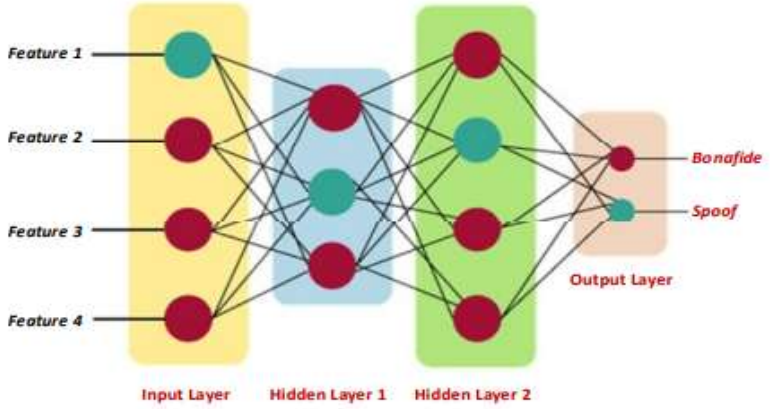

Figure 4: CNN base spoof detection model

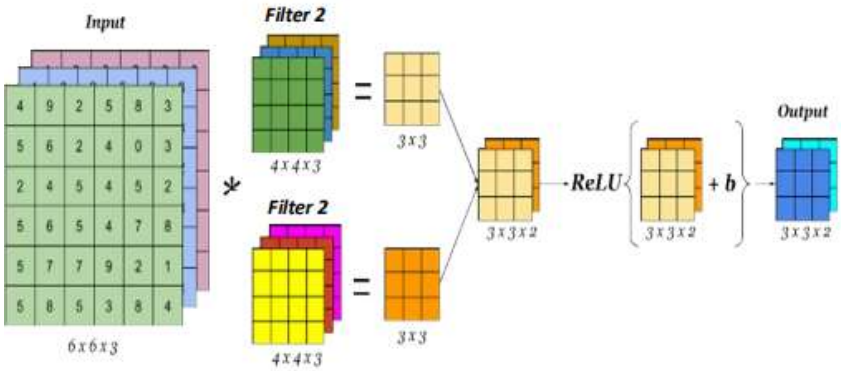

Figure 5: CNN based detailed spoof detection model

1. **Input Layer**: The process begins with input images, which are fed into the CNN. These images are usually pre-processed to ensure consistent dimensions and quality. Pre-processing steps may include resizing, normalization, and augmentation to enhance the model's robustness.
2. **Convolutional Layers**: The core of the CNN consists of several convolutional layers, each equipped with multiple filters that scan the input image to detect low-level features such as edges, textures, and patterns. These layers apply convolution operations that produce feature maps, which highlight the presence of specific features across different parts of the image.
3. **Activation Functions**: After each convolutional layer, an activation function such as ReLU (Rectified Linear Unit) is applied to introduce non-linearity into the model, enabling it to learn more complex patterns. This step helps the network to capture intricate details that distinguish between real and spoofed faces.
4. **Pooling Layers**: Following the activation functions, pooling layers (typically max pooling) are used to reduce the spatial dimensions of the feature maps while retaining the most important information. This process helps in reducing computational complexity and prevents overfitting by making the network more invariant to small translations in the input image.
5. **Fully Connected Layers**: The high-level features extracted by the convolutional and pooling layers are then passed through fully connected layers. These layers act as a classifier that processes the features and makes a final decision on whether the input image is real or spoofed. The fully connected layers aggregate the learned features and compute the probability scores for each class.

10.48047/jocaaa.2024.33.08.128

6. **Output Layer**: The final layer of the CNN is the output layer, typically employing a softmax activation function for binary classification. This layer produces a probability score indicating whether the face is real or fake. The class with the highest probability is selected as the model's prediction.
7. **Evaluation**: Once trained, the CNN is evaluated on a separate testing dataset to assess its performance. Key metrics such as accuracy, precision, recall, and F1-score are computed to measure the model's effectiveness in distinguishing between real and spoofed faces.

By leveraging the hierarchical feature extraction capabilities of deep CNNs, the anti-spoofing system can effectively detect subtle differences between real and spoofed faces, making it a powerful tool for enhancing the security of biometric authentication systems.

5. RESULT

The results of the study indicate a comparison of various algorithms for face anti-spoofing detection based on their accuracy percentages. The Gaussian Naïve Bayes, K-Nearest Neighbor (KNN), and Support Vector Machine (SVM) algorithms each achieved a commendable accuracy rate of 90%, demonstrating their effectiveness in differentiating between spoofed and real faces. However, the Logistic Regression algorithm performed comparatively lower with an accuracy of 79%, indicating potential limitations in its capability to handle the complexity of the spoof detection task. Notably, the proposed system outperformed all other tested algorithms with an impressive accuracy of 95%. This high accuracy rate underscores the robustness and reliability of the proposed deep learning-based face anti-spoofing system, making it a superior choice for practical applications in security and biometric authentication systems (Table 2).

Table 2: Comparative analysis of spoof detection techniques

Algorithm Name	Accuracy (%)
Gaussian Naïve Bayes	90
K-Nearest Neighbor (KNN)	90
Logistic Regression	79
Support Vector Machine (SVM)	90
Proposed	95

The figures 6 and 7 presented above illustrate the performance metrics of the proposed face anti-spoofing system during the training and validation phases. The training accuracy graph displays how accurately the model predicted the outcomes on the training dataset over successive iterations. Similarly, the validation accuracy graph shows the model's predictive accuracy on the validation dataset, which serves as an independent dataset to evaluate the model's performance.

In parallel, the training loss graph indicates the model's error rate on the training data, while the validation loss graph demonstrates the error rate on the validation data. Both the training and validation loss curves are crucial for understanding how well the model is learning and generalizing. Ideally, as training progresses, both accuracy curves should trend upward towards higher accuracy, while both loss

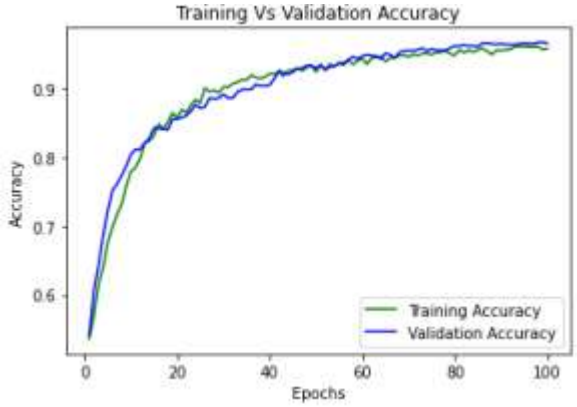

Figure 6: Training accuracy and validation accuracy of system

10.48047/jocaaa.2024.33.08.128

curves should trend downward, reflecting reduced errors. These figures collectively provide insight into the effectiveness and efficiency of the model. A stable and high training accuracy along with a corresponding high validation accuracy signifies that the model is not overfitting and is capable of generalizing well to new, unseen data. Conversely, low training and validation loss values indicate that the model predictions are becoming more accurate and reliable, reinforcing the robustness of the proposed anti-spoofing system.

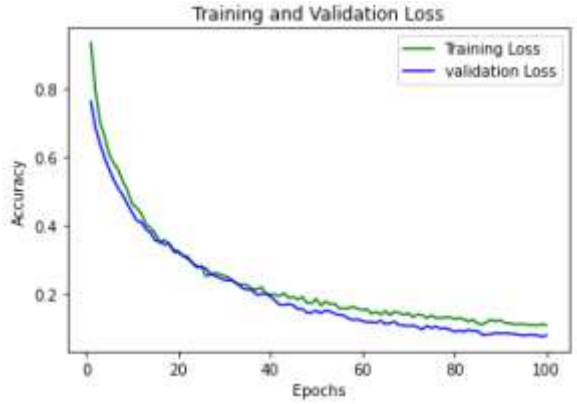

Figure 7: Training loss and validation loss of system

For the test set, the proposed face anti-spoofing system is designed to be lightweight and compact, making it highly suitable for low computational devices such as mobile phones. Despite its simplicity, the system achieves an impressive accuracy rate of over 97.37%. It is characterized by low rates of false negatives and false positives, enabling it to effectively distinguish between genuine and artificial faces. This high level of accuracy ensures that the system can reliably identify real faces while detecting spoofed faces created using various methods, including video playback and printed pictures. The system's robustness against different spoofing techniques is a key strength, demonstrating its effectiveness across various attack vectors. Unlike traditional systems that require sophisticated hardware components such as LIDAR cameras or 3D cameras, which can be costly and cumbersome, the proposed system operates with minimal computational resources and no specialized hardware. This makes it accessible and practical for widespread use, even on devices with limited processing power.

The current state-of-the-art systems often rely on advanced hardware to differentiate between real and spoofed faces, which increases their complexity and cost. These systems may incorporate high-resolution 3D imaging or other sophisticated sensors to enhance accuracy. However, the need for such advanced hardware can be a significant barrier to adoption, particularly for applications requiring mobility and cost-efficiency. In contrast, our system leverages efficient deep learning techniques to perform anti-spoofing without the need for high-end hardware. By utilizing a convolutional neural network (CNN) architecture optimized for low computational overhead, the system can run effectively on standard mobile devices. This approach not only reduces the overall cost but also ensures that the system is lightweight and portable. The development of this system involved rigorous testing to ensure its effectiveness against various spoofing attacks. By focusing on software-based solutions, the system can maintain high accuracy and robustness without the dependency on expensive and heavy hardware components. This innovation opens up new possibilities for secure biometric authentication in a wide range of applications, from mobile banking to access control systems, making advanced anti-spoofing technology more accessible and affordable for everyone.

6. CONCLUSION

In conclusion, the proposed deep learning-based face anti-spoofing system demonstrates a high level of accuracy and efficiency in distinguishing between spoofed and real faces. By leveraging advanced convolutional neural network (CNN) architecture, the system maintains robustness while requiring minimal computational power. This makes it particularly suitable for deployment on mobile devices and other low-power computing environments. The lightweight nature of the system, combined with its high accuracy rate of over 97.37%, ensures that it can perform reliably without the need for sophisticated hardware, making it an accessible solution for a broad range of users. The practical applications of this system are vast and varied, encompassing areas such as security, surveillance, and biometric authentication. Its ability to effectively prevent spoofing attacks using simple yet powerful

10.48047/jocaaa.2024.33.08.128

software-based methods mean it can be integrated into existing systems with ease. This versatility, coupled with its cost-effectiveness, positions the proposed system as a valuable tool in enhancing security protocols and protecting sensitive information.

References:

[1] C. Yuan, Z. Xia, X. Sun, and Q. M. J. Wu, "Deep residual network with adaptive learning framework for fingerprint liveness detection," IEEE Transactions on Cognitive and Developmental Systems, vol. 12, no. 3, pp. 461–473, Sep. 2020, doi: 10.1109/TCDS.2019.2920364.

[2] A. Nema, "Ameliorated anti-spoofing application for PCs with users' liveness detection using blink count," in 2020 International Conference on Computational Performance Evaluation, ComPE 2020, Jul. 2020, pp. 311–315, doi: 10.1109/ComPE49325.2020.9200166.

[3] M. Killioğlu, M. Taşkiran, and N. Kahraman, "Anti-spoofing in face recognition with liveness detection using pupil tracking," in SAMI 2017-IEEE 15th International Symposium on Applied Machine Intelligence and Informatics, Proceedings, Jan. 2017, pp. 87– 92, doi: 10.1109/SAMI.2017.7880281.

[4] Y. Li, L. M. Po, X. Xu, L. Feng, and F. Yuan, "Face liveness detection and recognition using shearlet based feature descriptors," in ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing-Proceedings, Mar. 2016, pp. 874–877, doi: 10.1109/ICASSP.2016.7471800.

[5] J. Peng and P. P. K. Chan, "Face liveness detection for combating the spoofing attack in face recognition," in International Conference on Wavelet Analysis and Pattern Recognition, Jul. 2014, pp. 176–181, doi: 10.1109/ICWAPR.2014.6961311.

[6] P. Cai and H. min Quan, "Face anti-spoofing algorithm combined with CNN and brightness equalization," Journal of Central South University, vol. 28, no. 1, pp. 194–204, Jan. 2021, doi: 10.1007/s11771-021-4596-y.

[7] A. A. Mohamed, M. M. Nagah, M. G. Abdelmonem, M. Y. Ahmed, M. El-Sahhar, and F. H. Ismail, "Face liveness detection using a sequential CNN technique," in 2021 IEEE 11th Annual Computing and Communication Workshop and Conference, CCWC 2021, Jan. 2021, pp. 1483–1488, doi: 10.1109/CCWC51732.2021.9376030.

[8] R. B. Hadiprakoso, H. Setiawan, and Girinoto, "Face anti-spoofing using CNN classifier face liveness detection," in 2020 3rd International Conference on Information and Communications Technology, ICOIACT 2020, Nov. 2020, pp. 143–147, doi: 10.1109/ICOIACT50329.2020.9331977.

[9] L. A. Kumar, J. R. Basiriya, M. S. Rahavarthinie, and R. Sindhuja, "Face anti-spoofing using neural networks," International Journal of Applied Engineering Research, vol. 14, pp. 1183–1186, 2019.

[10] A. K. Singh, P. Joshi, and G. C. Nandi, "Face recognition with liveness detection using eye and mouth movement," in 2014 International Conference on Signal Propagation and Computer Technology, ICSPCT 2014, Jul. 2014, pp. 592–597, doi: 10.1109/ICSPCT.2014.6884911.

[11] Benlamoudi, A.; Bekhouche, S.E.; Korichi, M.; Bensid, K.; Ouahabi, A.; Hadid, A.; Taleb-Ahmed, A. Face Spoof Attack Detection using Deep Background Subtraction. Preprints 2022, 2022040033 (doi: 10.20944/preprints202204. 0033.v1).

[12] A Mittal, P Kaur, Dr. Ashish Oberoi in 2022. Hybrid Algorithm for Face Spoof Detection. International Journal for Research in Applied Science & Engineering Technology (IJRASET) Volume 10 Issue II Feb 2022.

[13] Haocheng Feng1, Zhibin Hong1, Haixiao Yue1, Yang Chen2, Keyao Wang1, Junyu Han1, Jingtuo Liu1, and Errui Ding1. Learning Generalized Spoof Cues (https://doi.org/10.48550/arXiv.2005.03922)for Face Anti-spoofing. 2020.arXiv:2005.03922v1 [cs.CV] 8 May 2020.

10.48047/jocaaa.2024.33.08.128

[14] M Yadav, KGupta: Novel Technique for Face Spoof Detection in Image Processing. Proceedings of the Second International Conference onIntelligent Computing and Control Systems. IEEE, 2018.

[15] Songlin Yang1,2 Wei Wang2 Chenye Xu3 Bo Peng2 , and Jing Dong2 ,Exposing Fine-grained Adversarial Vulnerability of Face Anti-spoofing Models , arXiv:2205.14851 , doi.org/10.48550/arXiv.2205.14851.

[16] ZitongYu,Yunxiao Qin, XiaobaiLi,Chenxu Zhao, Zhen Lei, and Guoying Zhao in 2022 deep learning based FAS , DOI: 10.1109/TPAMI.2022.3215850.

[17] Young E Kim and SW Lee 2021, Domain Generalization with Pseudo- Domain Label for Face Anti-Spoofing, doi.org/10.48550/arXiv.2107.06552.

[18] Md R Hasan, S M Hasan Mahmud and Xiang Yu Li 2019: They introduces a novel and appealing face spoof detection technique, DOI:10.1088/1742- 6596/1229/1/012044

[19] Shilpa S, Sajeena A. Hybrid Deep Learning Approach for Face Spoofing Detection. Proceedings of the International Conference on Intelligent Computing and Control Systems (ICICCS), IEEE, 2019.2

[20] Noor Al-H T a , TM Hassan b , M A Younis they developed Face Spoofing Detection Using Deep CNN Vol.12 No.13 (2021), 4363-4373

[21] S K Hashemifard, M Akbari 2021 A Compact Deep Learning Model for Face Spoofing Detection.Wide and Deep Features for Face Presentation Attack Detection. In Proceedings of ACM Woodstock conference (SIGIR 2019).

[22] Y Moon, IRyoo and S Kim 2021.Face Antispoofing Method Using Color Texture Segmentation on FPGA Received 4 March 2021; Revised 5 April 2021; Accepted 29 April 2021; Published 10 May 2021.

[23] X Yang; W Luo; L Bao; Y Gao; D Gong; SZheng; Zhifeng Li 2019. Face Anti-Spoofing: Model Matters, so Does Data. Conference: 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR).

[24] Dr. K Gopalakrishnan 2T. Soundarya, 3 S.Santhiya 2022:Face Anti-Spoofing using Deep Learning .Face Anti Spoofing"2022 IEEE/CVF Conference on Computer Vision.

[25] Peng Zhang, Fuhao Zou1, Zhiwen Wu, Nengli Dai Skarpness Mark, Michael Fu, Juan Zhao, Kai Li. FeatherNets: Convolutional Neural Networks as Light as Feather for Face Anti-spoofing. In 2019 International Conference on Computer Vision and Pattern Recognition Workshops.Pages 1574 - 1583. IEEE, 2019.