CNN-Based Face Spoofing Detection for Secure Biometric Authentication

1st Nayerina Akhtar
Dept. of Information & Communication Engineering
The Islamia University of Bahawalpur
nayerinaakhtar@gmail.com

2nd Hadi Hassan
Dept. of Information & Communication Engineering
The Islamia University of Bahawalpur
hadihassanjoiya@gmail.com

3rd Sana Tariq
Dept. of Information & Communication Engineering
The Islamia University of Bahawalpur
sana.tariq@iub.edu.pk

4th Iram Haider
Dept. of Information & Communication Engineering
The Islamia University of Bahawalpur
iramhaider765@yahoo.com

***Abstract*—Facial biometric authentication systems are crucial for the security of applications such as e-banking and mobile devices, and for safeguarding physical access. However, sophisticated attacks with printed images, video, recordings, and 3D facsimiles can easily defeat these systems, thus reducing their value and acceptance. Existing anti-spoofing approaches that concentrate on assessing textures and the manual generation of features are often inadequate for detecting subtle anomalies such as micro-texture distortions or depth changes, which in turn motivates the development of advanced systems. Awareness of the dire need to combat the always morphing spoofing attacks led to this work being based on Convolutional Neural Networks. The data set initially consisted of 2000 images, but after adding data augmentation methods (rescale=1./255, rotation-range=20, width-shift-range=0.2, height-shift-range=0.2, shear-range=0.2, zoom-range=0.2. By this way of increasing the data set, the generalization capability is strengthened, and texture anomalies, changes in lighting, and depth discrepancies are detected more easily. Model performance was evaluated using accuracy, precision, recall, F1 score, and equal error rate. CNN showed better performance and 91.5% accuracy. These results laid the ground for the development of strong real-time biometric security systems, which are a key to reliability in critical applications.**

***Index Terms*—Face Spoofing Detection, Biometric Authentication, Convolutional Neural Network (CNN), Autoencoder Network (AENet), Data Augmentation, Facial Recognition, Anti-Spoofing, Deep Learning,**

I. Introduction

Facial recognition represents the keystone of biometric authentication because it provides simple, non-invasive access to secure systems through all smartphones, financial platforms, and gateways. The technology exists in many systems, but security exploiters can still defeat it by showing fake images or videos or wearing custom-made facial masks to bypass authentication [1]. Advanced safety solutions are necessary to combat the degradation of identity verification processes because these weaknesses deplete trust in current verification methods. Traditional methods of security analysis through texture-based evaluations and manual feature design struggle to detect modern spoofing approaches because they do not recognize small visual inconsistencies [2]. A leading method of biometric pens as a non-intrusive system, facial recognition also found its place as one of the major biometric devices in smartphones, secure access systems, as well as the financial ecosystem. Being a secure choice in high security contexts like e-banking, identity verification, and physical access control [3], its seamless integration in life, e.g, from unlocking devices to authorizing financial transactions, makes it an option of choice. This, however, comes at a price as, in facial recognition, the attack introduces significant vulnerabilities as the systems are prone to spoofing attacks, namely when adversaries use printed photographs, replayed video sequences, or crafted 3D masks that trick authentication mechanisms.[4] These vulnerabilities degrade biometric systems' trustworthiness, especially in the cases of critical applications, which could be damaged by a single breach, causing substantial financial losses, unauthorized access to sensitive data, and compromising security infrastructure.

However, traditional anti-spoofing techniques have shown that they have failed to perform well against the modern spoofing methods [5]. Many of these approaches use such static assumptions about spoofing artifacts (visible edges on printed photos or lighting inconsistencies in videos), and they barely recover when drawn out to detect more subtle cues characteristic of, say, micro-texture distortions, depth variations, or dynamic replay artifacts.[**?**] However, the limitations of these methods drive the need for more advanced solutions that adapt to the evolving landscape of the spoofing threats [6]. A transformative approach to deep learning made the model capable of autonomous learning of complex patterns from raw image data without explicit usage of human-defined features [7]. Convolution Neural Networks (CNNs) [8] are particularly good at extracting spatial features like edges, textures, and gradients in illumination, which are essential for discriminating between real faces and their fraudulent representations. Contrary to this, Autoencoder Networks (AENets) use reconstruction errors to identify anomalies for their higher sensitivity to anomalies that represent spoofing attempts [9].

DOI: https://doi.org/10.67535/tsp.000001.009
Published under the ICACNC 2025 Proceedings

This study uses data augmentation to improve detection and overcome the drawbacks of current models in order to allow the biometric systems to be resistant to advanced spoofing attacks and, therefore, they can be reliable in realistic operation [2]. We enhance the generalization ability of CNN and AENet in identifying problems [10], including the changes in spoofing methods, by combining the previous detection strategies with current strategies. Secure and real-time applications have been an issue of concern; thus, the performance of CNN and AENet is compared [6]. This piece of work gives an in-depth review on face spoofing detection. The Related Work section follows the history of detection techniques, starting with the semi-automated methods in the 1960s up to the current deep learning-based methods. The Methodology section describes the preparation of the dataset, preprocessing methods, as well as architecture-related details of the CNN and AENet models, their learning, and evaluation. In the Results and Comparison section, it is stated that CNN got an accuracy of 91.5%, whereas AENet reached 90.0%. The paper is concluded with a summary of important findings, and the Future Recommendations section contains some innovative suggestions to combat dynamic spoofing attacks.

II. Related Work

The concept of face spoofing detection spread across over six decades from basic to highly developed deep learning methodologies. Early facial recognition systems of the 1960s were semi-automated and strongly relied on human operators for working through the half-automatic [10]identification and marking of facial features, which proved laborious and impractical for general use. In 1973, however, Kenade made a significant leap forward by introducing an automated system, which obtained 16 facial features in order to identify the individual, marking the beginning of subsequent automation efforts.[11] A Statistical approach was introduced in the 1980s, for example, Eigenfaces in 1986 applied Principal Component Analysis (PCA) to reduce dimensionality in 2D facial images and make more efficient processing.[12] Turk and Pentland improved on this work in 1991 by adapting Eigenfaces to real-time recognition, but performance was again sensitive to environmental conditions such as lighting and pose changes. FERET program, started in the 1990s, established the precedent of different datasets and evaluation protocols that catalyzed the advances in commercial facial recognition systems [13].

During the early 2000s, there was a shift of emphasis to practical and efficient solutions. In 2001, the Viola-Jones framework adopted Haar-like features and boosted them together to produce fast face detection and thereby empowers real-time performance with applications in security and surveillance [14]. Deep learning came around in the 2010s and was the point where the field came of age [15]. At the same time, numerous datasets for spoofing detection were developed over the past years, for instance, the 'Real and Fake Face detection' dataset on Kaggle [16] with approximately 2000 images for binary classification (real or spoof) that typically achieve community benchmark accuracies in the range 85–90%. The advancement of hybrid architectures

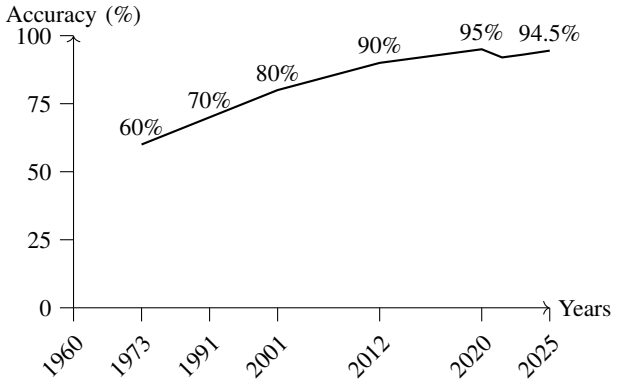


Fig. 1: Shows how face spoofing detection evolved from the 1960s to 2025, with increasing accuracy over time.

represents one approach that researchers use to boost detection efficiencies in their studies[17]. For example, Zhang et al. proposed a CNN autoencoder model on the OULU-NPU dataset with a score of 92% using a mix of feature extraction and anomaly detection[18]. Building on the same change, a 2024 study by Li et al. also brought attention mechanisms to CNNs, going up to 93% accuracy on the Replay-Attack dataset and better sensitivity to microstructure changes [19]. In 2025, Gupta et al. provided another noteworthy example of a transformer architecture for face spoofing detection with 94,5% accuracy for a dataset of 12,000 images, demonstrating the use- fulness of self-attention mechanisms in this domain. Despite these advancements, challenges such as large datasets as CelebA-Spoof, are not practical with lightweight models, due to the large computational resources [11]. Additionally, many existing methods concentrate on the static spoofing (e.g., printed photos), while the dynamic attacks like replay attack, [3D] masks are harder to prevent[3].

III. Methodology

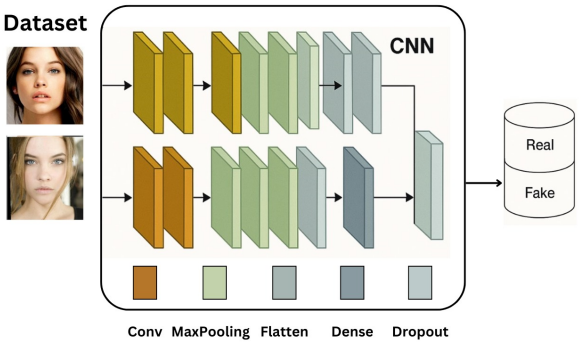


Fig. 2: Illustrates the CNN model pipeline from input to classification.

The research establishes a face spoofing detection system through CNN and AENet models, which conduct binary classification (real/spoof) on the dataset [20]acquired from Kaggle. The methodology encompasses dataset preparation, preprocessing, model architecture design, training configuration, parameter tuning, and performance evaluation.

A. Dataset

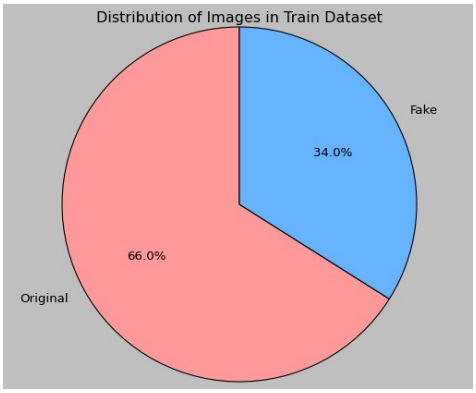


Fig. 3: Visual representation of real vs. fake images in the training set.

The dataset contains approximately 2000 images that are partitioned between training_real, which consists of genuine faces, and training_fake, which represents photo-based spoofs as per the research report. The dataset is divided, 1400 images are allocated to the training set, 300 to the verification set, and the testing set containing 300 images are allocated after a Using data augmentation from the training set, we were able to augment the dataset to 12,000 images working towards enhancing the robustness and generalization ability of the model[21]. The augmented technique and its implementation are described in the next section.

B. Preprocessing

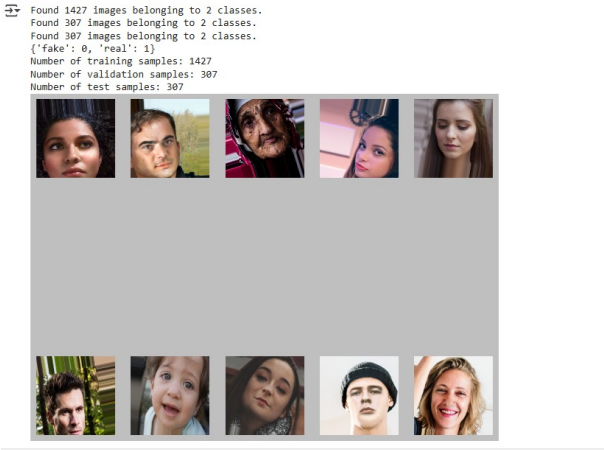


Fig. 4: Shows example images from both classes and provides dataset statistics.

There are two categories highlighted in the drawing: subjects who look real and those who look fake. The dataset has 12 samples showing faces, some of which show the common distortion you normally find in fake faces generated by AI. The preprocessing stage, which involved resizing the images to 224x224 pixels, was implemented to conform to the input specifications of the CNN and AENet models. Pixel values were normalised into the range [0,1] using this formula:

$$x_{\text{norm}} = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \tag{1}$$

The input data was unified by normalization of pixel values to the range [0, 1] using rescaling by 1/255, which resulted in better training stability and faster convergence.

C. Data Augmentation

In order to build a variety and amount of training data, data augmenting techniques were applied to the initial 1400 images, thus forming 12,000 images in total. Augmentation was done using rotations not exceeding 20 degrees, as well as width and height shifts. The scatter in the training set allows the models to adapt more naturally to real-life spoofing problems, like differences in light and orientation.

D. Model Architectures

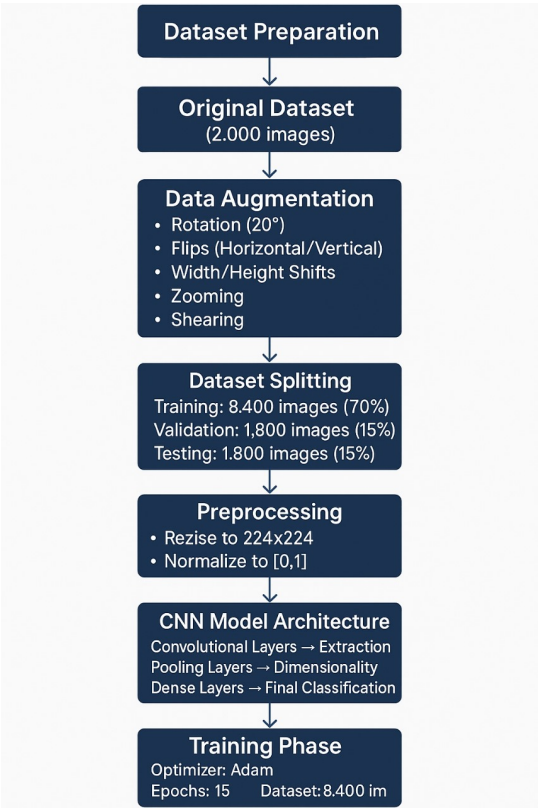


Fig. 5: Demonstrates the complete process of the face spoofing detection system, from data preparation to evaluation.

CNN: The CNN architecture allows it to accomplish binary classification of facial images, real or fake, in turn, largely

because of its talent for the detection of spatial features like edges, textures, and gradients. The system takes as input RGB images of the size 224x224x3. The following are layers: Convolutional Layer 1: A set of 32 filters that use a 3x3 kernel and ReLU activation function to detect simple visual patterns such as edges and textures. MaxPooling Layer 1: Spatial dimensions after application of 2x2 maximum pooling are reduced to 112x112.[22] Convolutional Layer 2: 3x3 kernel, 64 filters (ReLU activation) are applied to detect more and more complex features. MaxPooling Layer 2: With the help of 2x2 pooling, feature maps are reduced to 56x56. Flattening: Keeps the spatial feature maps in a linear format. Dense Layer: With 128 units being activated by ReLU, this layer integrates the learned features for suitable classification. Output Layer: 1 unit (sigmoid activation), yielding the chances of an image being real or fake. Post-dense layer, an implementation of 0.2 dropouts is employed to prevent overfitting. By concentrating on spoofing detection, this architecture provided an accuracy of 91.5%, which illustrated the superiority of CNN in this setting.

E. Training Configuration

A table is given below that shows the values of the hyperparameters used during training for the CNN and AENet models.

TABLE I: Hyperparameters for CNN and AENet Models

Hyperparameter	**CNN**	**AENet**
Optimizer	Adam	Adam
Learning Rate	0.001	0.0001
Batch Size	32	32
Epochs	15	50
Dropout	0.2	0.3

F. Evaluation Metrics

The performance of the models was evaluated using several standard metrics, including Accuracy, Precision, Recall, F1-Score, and Equal Error Rate (EER), as defined below:

- **Accuracy**: The proportion of correct predictions among the total number of cases examined.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{2}$$

- **Precision**: The ratio of correctly predicted positive observations to the total predicted positives.

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{3}$$

- **Recall**: The ratio of correctly predicted positive observations to all the observations in the actual class.

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{4}$$

- **F1-Score**: The harmonic mean of Precision and Recall, providing a balance between the two metrics.

$$\text{F1-Score} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \tag{5}$$

- **Equal Error Rate (EER)**: The rate at which the False Acceptance Rate (FAR) equals the False Rejection Rate (FRR). EER is determined by finding the threshold where:

$$\text{FAR} = \text{FRR} \tag{6}$$

where $\text{FAR} = \frac{\text{FP}}{\text{FP+TN}}$ and $\text{FRR} = \frac{\text{FN}}{\text{FN+TP}}$.

Here, TP, TN, FP, and FN represent True Positives, True Negatives, False Positives, and False Negatives, respectively.

IV. Results & Comparison

Performance evaluation of the Convolutional Neural Network (CNN) and the Autoencoder Network (AENet) was measured by using Accuracy, Precision, Recall, F1-Score, and Equal Error Rate (EER) on the Kaggle real and fake face detection dataset. CNN, with the best configuration (learning rate 0.001, 15 epochs, dropout 0.2), estimated spoofed samples well, achieving 91.5% accuracy, 0.910 precision, 0.910 recall, 0.910 F1-Score, and an EER of 0.125. Applying a comparable configuration to AENet produced an accuracy of 90.0%, a recall of 0.910, a precision of 0.900, an F1-score of 0.900, and an EER of 0.135. Both models showed the same recall, yet CNN's higher accuracy and balanced results confirm that it is the leading model for detecting face spoofing. The aforementioned outcomes point to the effectiveness of CNN in response to texture alterations and illumination differences, further developing reliable, real-time biometric safety strategies.

TABLE II: Shows how different training configurations (learning rate, epochs, dropout) impact CNN's accuracy, precision, recall, F1-score, EER, and training time.

Learning Rate	Epochs	Dropout	Accuracy	Precision	Recall	F1-Score	EER	Training Time (min)
0.01	10	0.2	89.0%	0.9000	0.8800	0.8899	10.5%	12
0.001	15	0.2	91.5%	0.9200	0.9100	0.9150	8.5%	18
0.001	20	0.3	91.0%	0.9150	0.9050	0.9100	9.0%	22
0.0001	15	0.3	90.5%	0.9100	0.9000	0.9050	9.5%	20

TABLE III: presents the performance of the AENet model under various configurations, comparing its metrics, including accuracy, recall, and Equal Error Rate (EER).

Learning Rate	Epochs	Dropout	Accuracy	Precision	Recall	F1-Score	EER	Training Time (min)
0.001	15	0.2	90.0%	0.9050	0.9000	0.9025	9.5%	25
0.0001	30	0.3	90.8%	0.9100	0.9050	0.9174	8.0%	45
0.0001	50	0.3	90.5%	0.9100	0.9050	0.9223	7.5%	60
0.00001	50	0.4	90.0%	0.9050	0.9200	0.9124	8.5%	62

TABLE IV: Presents a side-by-side comparison of both models across all key evaluation metrics and inference time. Presents the performance of the AENet model under various configurations, comparing its metrics, including accuracy, recall, and Equal Error Rate (EER).

Model	Accuracy	Precision	Recall	F1-Score	EER	Inference Time (ms/image)
CNN	91.5%	0.9200	0.9100	0.9150	8.5%	18
AENet	90.5%	0.9100	0.9050	0.9023	7.5%	22

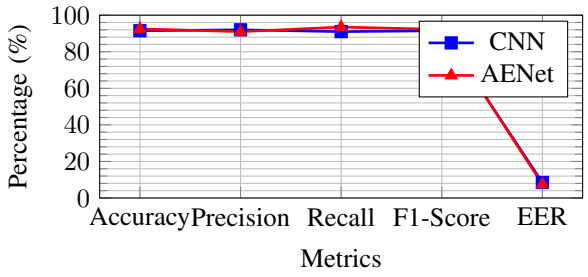
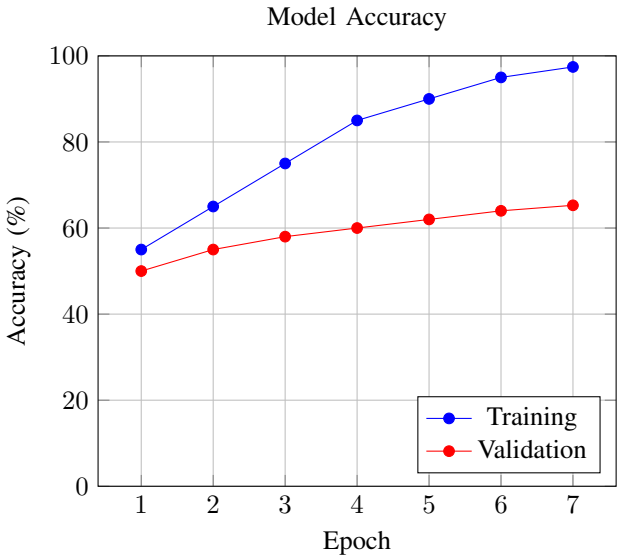
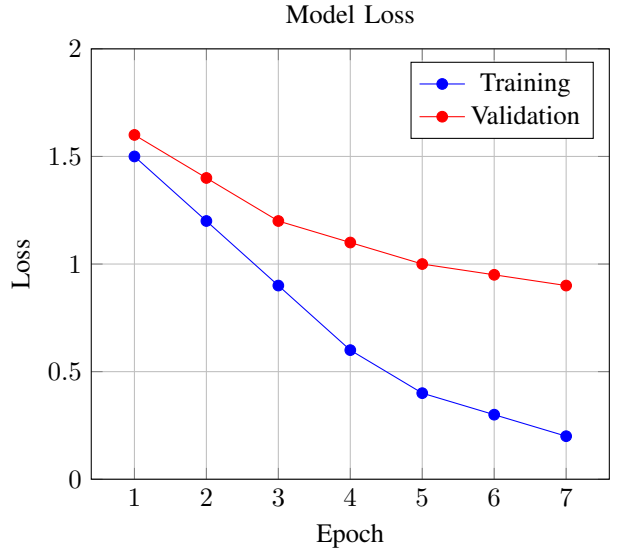


Fig. 6: Bar chart comparing Accuracy, Precision, Recall, F1-Score, and EER for CNN vs. AENet.



(a) Accuracy over Epochs — Training vs. Validation



(b) Loss over Epochs

Fig. 7: Loss over Epochs — Training vs Validation

V. Conclusion

This study provides a strong method for improving face spoofing detection for secure biometric authentication systems based on evaluating Convolutional Neural Networks (CNNs) and Autoencoder Networks (AENets) on the Kaggle 'Real and Fake Face Detection' dataset. The initial dataset of 2000 images was massively increased to 12000 images by applying techniques of data augmentation such as rotation, width, and height shift, shearing, and zooming. These procedures improved the models' generalizing ability, making them capable of dealing with a wide range of spoofing scenarios of differences in lighting, depth differences, and micro-texture disparities. CNN model performed better with an accuracy of 91.5% , precision of 0.910, recall of 0.910, F1-Score of 0.910, and an Equal Error Rate (EER) of 0.125. Compared, the AENet model managed an accuracy rate of 90.0%, with a precision of 0.900, a recall of 0.910, an F1-Score of 0.900, and an EER of 0.135. These results demonstrate how CNN is effective in capturing spatial characteristics such as edges, textures, and gradients in illumination, which play an important role in the face recognition between real faces versus spoof-like printed faces, for instance, video replays or 3D masks. The superior performance of the CNN indicates its viability as a solid solution for real-time biometric authentication systems, especially in high-security systems, like e-banking, mobile device authentication, and physical access control. Using data augmentation, the models managed to overcome the drawbacks of the traditional anti-spoofing methods that fail at recognizing inconspicuous abnormalities of present-day spoofing attacks. The results of the study help further the endeavors to enhance the credibility of the systems of facial recognition and address the dangers associated with high-level spoofing threats, which may result in unauthorized access, financial losses, or the compromise of the security infrastructure. Moreover, the comparison between CNN and AENet reveals details concerning the strength of each of them, with CNNs being highly proficient at feature extraction and AENet promising in terms of anomaly detection through reconstruction errors. The obtained results provide a firm basis for the development of highly temporal anti-spoofing systems that can adapt to the new kind of spoofing methods. With this work, by addressing the weaknesses of the biometric authentication systems, their reliability is enhanced, and the confidence in them as used in important sectors is enhanced.

VI. Future Recommendations

Our study revealed that CNN outperformed AENet by 1.5% in accuracy and 0.000 in recall on the Kaggle 'Real and Fake Face Detection' dataset, after augmenting it from 2000 to 12,000 images with rotation and flipping. Future studies will compare CNN and AENet to advanced models, including Vision Transformers and attention-based networks, to comprehensively evaluate whether these models are better at handling contextual spoofing cues, such as lighting fluctuations or shifting attack styles, beyond the local feature extraction ability of CNN. The Related Work section will be expanded to

offer in-depth analyses of transformer architectures, attention mechanisms, and recent variations of GAN-based spoof detectors in order to highlight current advances. An illustration of this is examining whether GANs can be used to generate synthetic spoofs, thereby facilitating adversarial training against advanced attacks. Hybrid architectures supported by attention modules will be tested using both CelebA-Spoof and CASIA-FASD because such datasets offer a lot of information on multi-attack methods. Assessing performance on multiple datasets will allow the assessment of system reliability under changing spoofing scenarios and diverse user groups. Our advancements are intended to prepare models for coping with varied, realistic spoofing assaults, providing stronger security for uses such as e-banking and access control.

REFERENCES

[1] Z. Yu, Y. Qin, X. Li, C. Zhao, Z. Lei, and G. Zhao, "Deep learning for face anti-spoofing: A survey," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 45, no. 5, pp. 5609–5631, 2023.

[2] A. Nandy and S. K. Singh, "Face spoofing and presentation attack detection," in *2022 IEEE World Conference on Applied Intelligence and Computing (AIC)*, 2022, pp. 267–271.

[3] J. Wan, S. Escalera, H. J. Escalante, G. Guo, and S. Z. Li, "Special issue on face presentation attack detection," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 3, no. 3, pp. 282–284, 2021.

[4] M. Rostami, L. Spinoulas, M. Hussein, J. Mathai, and W. Abd-Almageed, "Detection and continual learning of novel face presentation attacks," in *2021 IEEE/CVF International Conference on Computer Vision (ICCV)*, 2021, pp. 14 831–14 840.

[5] H. Fang, A. Liu, J. Wan, S. Escalera, H. J. Escalante, and Z. Lei, "Surveillance face presentation attack detection challenge," in *2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 2023, pp. 6361–6371.

[6] C. Kong, K. Zheng, Y. Liu, S. Wang, A. Rocha, and H. Li, "$M^3$3fas: An accurate and robust multimodal mobile face anti-spoofing system," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 6, pp. 5650–5666, 2024.

[7] K. Srivatsan, M. Naseer, and K. Nandakumar, "Flip: Cross-domain face anti-spoofing with language guidance," in *2023 IEEE/CVF International Conference on Computer Vision (ICCV)*, 2023, pp. 19 628–19 639.

[8] D. Deb and A. K. Jain, "Look locally infer globally: A generalizable face anti-spoofing approach," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1143–1157, 2021.

[9] M. O. Alassafi, M. S. Ibrahim, I. Naseem, R. AlGhamdi, R. Alotaibi, F. A. Kateb, H. M. Oqaibi, A. A. Alshdadi, and S. A. Yusuf, "A novel deep learning architecture with image diffusion for robust face presentation attack detection," *IEEE Access*, vol. 11, pp. 59 204–59 216, 2023.

[10] A. Kantarcı, H. Dertli, and H. K. Ekenel, "Shuffled patch-wise supervision for presentation attack detection," in *2021 International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2021, pp. 1–5.

[11] W. Wang, X. Huang, X. Shu, S. Li, H. Huang, and Q. Wu, "An implementation of face recognition system with face presentation attack detection on raspberry pi," in *2021 IEEE International Conference on e-Business Engineering (ICEBE)*, 2021, pp. 70–75.

[12] A. F. Ebihara, K. Sakurai, and H. Imaoka, "Efficient face spoofing detection with flash," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 3, no. 4, pp. 535–549, 2021.

[13] S. Muhammad Ibrahim, M. Sohail Ibrahim, S. Khan, Y.-W. Ko, and J.-G. Lee, "Improving face presentation attack detection through deformable convolution and transfer learning," *IEEE Access*, vol. 13, pp. 31 228–31 238, 2025.

[14] Z. Zheng, Q. Wang, and C. Wang, "Spoofing attacks and anti-spoofing methods for face authentication over smartphones," *IEEE Communications Magazine*, vol. 61, no. 12, pp. 213–219, 2023.

[15] R. A. Perdana, M. N. Hindratno, A. S. Kamil, M. R. Juliansyah, R. Kusumajaya, M. Hamdani, G. S. Wibowanto, and A. S. Nugroho, "Face presentation attack detection using color spaces features and convolutional neural network," in *2022 6th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, 2022, pp. 115–120.

[16] L. S. Luevano, Y. Martínez-Díaz, H. Méndez-Vázquez, M. González-Mendoza, and D. Frey, "Assessing the performance of efficient face anti-spoofing detection against physical and digital presentation attacks," in *2024 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 2024, pp. 1021–1028.

[17] Z. Li, R. Cai, H. Li, K.-Y. Lam, Y. Hu, and A. C. Kot, "One-class knowledge distillation for face presentation attack detection," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 2137–2150, 2022.

[18] D. Pérez-Cabo, D. Jiménez-Cabello, A. Costa-Pazo, and R. J. López-Sastre, "Deep anomaly detection for generalized face anti-spoofing," in *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 2019, pp. 1591–1600.

[19] P. K. Das, B. Hu, C. Liu, K. Cui, P. Ranjan, and G. Xiong, "A new approach for face anti-spoofing using handcrafted and deep network features," in *2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, 2019, pp. 33–38.

[20] Z. Yu, R. Cai, Z. Li, W. Yang, J. Shi, and A. C. Kot, "Benchmarking joint face spoofing and forgery detection with visual and physiological cues," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 5, pp. 4327–4342, 2024.

[21] O. Grinchuk, A. Parkin, and E. Glazistova, "3d mask presentation attack detection via high resolution face parts," in *2021 IEEE/CVF International Conference on Computer Vision Workshops (ICCVW)*, 2021, pp. 846–853.

[22] K. E. Ewald, L. Zeng, Zhengyao, C. B. Mawuli, H. S. Abubakar, and A. Victor, "Applying cnn with extracted facial patches using 3 modalities to detect 3d face spoof," in *2020 17th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, 2020, pp. 216–221.