Unveiling Spoofing Attempts: A DCGAN-based Approach to Enhance Face Spoof Detection in Biometric Authentication

Vuda Sreenivasa Rao[1], Shirisha Kasireddy[2], Annapurna Mishra[3],
R. Salini[4], Sanjiv Rao Godla[5], Khaled Bedair[6]

Associate Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation,
Vaddeswaram, Andhra Pradesh, India[1]
Associate Professor, Vignana Bharathi Institute of Technology, JNTUH, Ghatkesar, Hyderabad, India[2]
Associate Professor, Electronics and Communication Engineering, Silicon Institute of Technology, Bhubaneswar, India[3]
Department of CSE, Panimalar Engineering College, Chennai, India[4]
Professor, Department of AIML& Data Science, Aditya College of Engineering and Technology- Suraplem,
Andhra Pradesh, India[5]
Department of Social Sciences-College of Arts and Sciences, Qatar University, P.O. Box 2713, Doha, Qatar[6]

***Abstract*—Face spoofing attacks have become more dangerous as biometric identification has become more widely used. Through the utilisation of false facial photographs, attackers seek to fool systems in these assaults, endangering the security of biometric authentication devices and perhaps allowing unauthorized access to private information. Effectively recognizing and thwarting such spoofing attacks is critical to the dependability and credibility of biometric identification systems in a variety of applications. This research seeks to offer a unique strategy that uses Deep Convolutional Generative Adversarial Networks (DCGANs) to improve face spoof detection in order to counter the challenge provided by face spoofing assaults. In order to strengthen the security of biometric authentication systems in applications like identity verification, access control, and mobile device unlocking, the goal is to increase the accuracy and effectiveness of facial spoof detection. The training dataset is then supplemented with these artificial images, which strengthens the face spoof detection system's resilience. More accurate face spoofing is made possible by the strategy that leverages the discriminative characteristics obtained throughout the process to train the discriminator network employing adversarial learning to discriminate between actual and fake images. Experiments on the CelebFacesAttributes (CelebA) datasets show how effective the suggested method is over traditional techniques. The suggested technique outperforms conventional methods and achieves an astounding accuracy of 99.1% in face-spoof detection systems. The system exhibits impressive precision in differentiating between real and fake faces through the efficient use of artificial intelligence and adversarial learning. This effectively decreases the possibility of unwanted access and enhances the overall dependability of biometric authentication methods.**

Keywords*—Biometric authentication systems; deep convolutional generative adversarial networks; face spoof detection; synthetic image generation; unauthorized access

I. Introduction

The face of a person is essential to any visual material or communication on face spoof detection. Commonly used and easily accessible editing tools are employed to improve this visual content. The technique of manipulating facial recognition devices by posing as an authorized user with fake facial images or videos is known as face spoofing. However, through manipulating video evidence, slandering a person's credibility, and other means, its harmful use is causing division in society [1].With the widespread adoption of biometric identification systems, the threat of face spoofing attacks has become increasingly prominent. Face spoofing the technique of manipulating facial recognition devices by posing as an authorized user with fake facial images as face spoofing. As spoofing techniques continue to evolve and become more sophisticated, it is essential to develop advanced detection methods capable of identifying increasingly realistic fake faces. With the increasing use of facial recognition technology for authentication and access control, detecting spoofed or fake faces is important to prevent unauthorized access to sensitive systems, devices, or information. Face spoofing techniques, such as using printed photos or digital masks, can be exploited by threat actors to impersonate legitimate users and gain access to their accounts or personal information [2]. Traditional spoof detection methods may struggle to distinguish between real and fake faces in the presence of increasingly convincing spoofing attacks. The advancement of face spoof detection system is achieved using deep learning methods to extract highly appropriate information from facial photos and effectively train models to detect even minor differences between real and faked faces.

Face detection systems are improving, but detecting face spoofing crime remains challenging. To address this, a Generative Adversarial Network (GAN) is implemented to deliver image from the RGB as an input. It improves discriminative capability by converting live face images to depth maps and spoofing images to plain images [3]. A face anti-spoofing system that combines VIS and NIR images, achieved through a MCT-GAN for generating NIR from VIS inputs, followed by a Convolutional Neural Network (CNN) for feature fusion, aiming to improve live and spoof face classification without requiring NIR equipment during testing [4]. Deep Learning techniques can manipulate videos, potentially leading to misinformation and manipulation. Deepfake detection using GAN Discriminators is developed using Generative Adversarial Network (GAN) discriminators to identify videos of Deepfake data. The model trains a GAN and extract a discriminator module, testing different architectures and training methods. It leads to enhance the efficiency of GAN discriminators using ensemble techniques [5]. The method of CNN Detection of GAN-Generated Face Images based on Cross-Band Co-occurrences Evaluation aims to differentiate between GAN-generated and real images, particularly focusing on synthetic face images, by leveraging inconsistencies across spectral bands. By incorporating Cross-Band Co-occurrence matrices along with spatial co-occurrence matrices as input to a CNN system, it achieves superior performance compared to a detection system solely based on intra-band spatial co-occurrences, achieving an accuracy of 94% [6]. A Deepfake detection technique utilizes computer vision characteristics extracted from digital context, employing the Cascaded Deep Sparse Auto Encoder (CDSAE) trained by temporal based CNN to analyze frame changes. Subsequently, a Deep Neural Network (DNN) is employed for classification, achieving enhanced accuracies of 98.7%, 98.5%, and 97.63% for the datasets like Face2Face, FaceSwap, and DFDC, through a feature selection approach [7]. Face swapping detection employed by deep transfer learning for, achieving true positive rates exceeding 96% with minimal false alarms, and providing uncertainty estimates for each prediction, crucial for system trust. It uses dataset with the largest to date for face swapping detection using static images, with approximately 1000 real images per individual, facilitating effective model design and evaluation, resulting in an accuracy of 98% [8]. The XcepTemporalConvolutional RNN framework combines XceptionNet CNN for facial feature representation with bidirectional recurrence layers, achieving robust visual deepfake detection and gained accuracy of 99%. Additionally, a companion audio architecture with convolution modules is presented, demonstrating high accuracy on both FaceForensics++ and Celeb-DF datasets, as well as the ASVSpoof 2019 Logical Access audio datasets [9]. The NA-VGG network enhances DeepFake detection by leveraging noise features highlighted by an SRM filter layer and augmenting the noise maps to weaken face features, resulting in improved accuracy compared to advanced detectors on the Celeb-DF dataset. The results demonstrate significant performance improvements, with the SRM filter upgrading image noise by 16.8% and image augmentation improving detection accuracy by 12.5% [10].

Traditional methodologies often necessitate manual feature engineering, wherein domain experts design specific features for classification purposes. Contrastingly, deep learning has the potential to eliminate the requirement for manual feature extraction by autonomously extracting relevant and hierarchical characteristics from raw data. By using DCNN, the model is able to acquire detailed representations of facial features, allowing it to analyse spatial correlations directly from the input images. This eliminates the need for manual segmentation and it enhances the model, streamlining classification process. Various approaches, including GAN-based methods and deep learning techniques, have been developed to detect face spoofing attacks and deepfake videos. These methods employ advancements in computer vision and neural networks to enhance discriminative capabilities and attained high accuracy in detecting manipulated images and videos. The proposed framework of Face Spoof Detection Using DCGAN aims to contribute to enhancement of face spoof detection by utilizing Deep Convolutional Generative Adversarial Networks to automatically extract features for improved face spoof detection, enhancing the reliability of facial recognition system.

Key Contributions:

- Face Spoof Detection system utilizes Deep Convolutional Generative Adversarial Networks (DCGANs) to create synthetic facial data.
- The generator, a deep architecture of neural networks, synthesizes realistic facial images resembling genuine faces and the discriminator network, trained adversarial, works with the generator to differentiate between real and spoofed images.
- The benefit of employing DCGAN for feature extraction is that it eliminates the requirement for human feature engineering by learning discriminative features directly from the raw input data.
- Enhances face spoof detection in biometric authentication systems and promotes secure access control in various applications like financial services, secure facilities, and mobile devices.

The following portion of this section is constructed as follows: The relevant work on Face Spoof Detection using DCGAN is reviewed in Section II. The problem statement of the current system is outlined in Section III. The specifics of the suggested methodology and architecture of DCGAN are explained in Section IV. The results and discussion are presented in Section V. Lastly, the conclusions and future scopes were given in Section VI.

II. Related Works

Arora et al. [11] developed a framework for the foundation of the suggested framework is the extraction of facial characteristics using dimensionality reduction and feature extraction methods using convolutional autoencoder that have been pre-trained. Subsequently, classification is performed using a softmax classifier. Evaluation conducted on three benchmark datasets - Idiap Replay Attack, CASIA-FASD, and 3DMAD - demonstrates that the framework achieves performance levels compared to advanced methods and gained accuracy of 99%. In particular, extracting features from facial visuals highlights the recent development of deep neural networks in image processing applications. Experiments carried out ondatasets such as 3DMAD, CASIA-FASD, and Idiap Replay Attack show that the suggested framework is effective in producing results that are on level with modern methods. Despite outperforming existing approaches on various benchmark datasets, the suggested face anti-spoofing framework has several limitations. When applied to diverse datasets, the methodology may be exposed to modern spoofing approaches, and by enhancing and adapting the structure to address increasing threats and crimes, such as spoofing attacks on biometric systems.

Patel et al. [12] proposed an innovative and enhanced deep-CNN (D-CNN) structure for recognizing deep fakes that is both accurate and generalizable. Data from various sources are used for training the system, thereby boosting its overall generality characteristics. The imagery is adjusted and sent into the D-CNN network. The D-CNN strategy rate of development is improved using binary-cross entropy and the Adam optimizer. It analyzed seven different datasets from the reconstructed difficulties, each including 5000 fake deep fake images and 10,000 true images. The proposed work achieves an accuracy rating of 98.33% in AttGAN, 99.33% in GDWCT, 95.33% in StyleGAN, 94.67% in StyleGAN 2, and 99.17% in StarGAN in true and fake. The framework can be upgraded by extending the model to classify video deepfake data which presents an opportunity for enhanced detection capabilities. By extracting each frame from a video, detecting and cropping faces, and then feeding them into the model, it could enable the identification of deepfake manipulations in videos.

Kumar et al. [13] proposed the framework on detecting Deepfake with metric classification for classifying deepfake videos in scenarios involving high compression through various deep learning techniques with limited data. It reveals that a proposed approach exhibits significant effectiveness in classification task based on metric learning and employs a triplet network architecture. It enhances the feature space distance between their embedding vectors for the model to learn the differentiation between real and fake videos. It validates on two datasets allows to assess their performance in diverse environments. By employing a Triplet network, it surpasses existing results using 25 frames per video. The framework achieved outstanding performance, including an AUC of 99.2% on the Celeb-DF and an accuracy of 90.71% on Neural Texture. However, the current strategy is limited by its dependence on unsupervised domain adaptation techniques to increase the model's endurance and label dependency in subsequent rounds. [13] [14] [15].

Baek et al [14] proposed Generative Adversarial Ensemble Learning for Face Forensics which involves multiple discriminative and generative networks. Unlike conventional approaches, it focuses on enhancing discrimination rather than image generate on. It is achieved by ensembling the outputs of two discriminators to improve discriminability. Additionally, it trains two generators to produce both general and hard images. The system uses produced simulated face pictures to improve the discriminators and enhances the generators based on the combination feedback of the discriminators. This is achieved by integrating input from each generator and discriminator using ensemble learning. It illustrates the efficacy of the method with a thorough analysis of the Face Forensics task and ablation tests. Two distinct discriminators and two similar generators constitute an ensemble forensic detector. An adversarial ensemble loss function and generative adversarial ensemble learning method are used in Enhancing Forensic Identification with Combined Discriminators. This causes the network topology of both generators and discriminators to become asymmetric, which enhances the framework's capacity for discrimination. It offers advantages by improving discrimination ability and addressing bias towards real or fake classes, which is applicable to existing detectors and other image forensic domains. Through extensive evaluation of the Face Forensics challenge and ablation studies, it demonstrates the effectiveness of the approach and acquired accuracy of 90%. But it requires significant computational resources and time for training multiple networks. The system needs to train two generators for both general and hard synthetic images which adds to computational burden. Ensemble learning process may require extensive tuning and optimization for optimal performance.

Ranjan et al. [15] developed a Transfer Learning-based CNNmodel for detecting DeepFakes across three prominent datasets like Deep Fake Detection (DFD), Celeb-DF, and Deep Fake Detection Challenge (DFDC). DeepFakes is curated for analysing purposes. The framework improves performance by transferring knowledge from pre-trained models to the task of DeepFake detection. While some blocks show higher accuracy without Transfer Learning, Transfer Learning consistently improves performance across most scenarios. The Celeb-DF dataset benefits significantly from Transfer Learning, with an 11.11% boost in accuracy. The model trained on the DFD dataset achieving records an accuracy of 73.20%. Conversely, the Celeb-DF model performs poorly when tested on the DFD dataset, reflecting the differences in alteration between the datasets. The cross-test accuracy is observed when the model is tested on DFDC, reaching 66.23%. The Xception Net demonstrates remarkable learning capacity by achieving impressive accuracy across all three distributions without overfitting, as evidenced by its high combined test accuracy of 86.49%. The Transfer Learning-based CNN framework for detecting DeepFakes has a potential drawback due to its reliance on pre-trained models, which may not capture the full range of features specific to DeepFake detection. While Transfer Learning consistently improves performance across most scenarios, it may not transfer relevant knowledge to the task, leading to suboptimal results.

Yavuzkilic et al. [16] presents a Multistream deep learning algorithm for identifying fake faces in videos, through a layer called fusion layer. Transfer learning is adopted, utilizing pre-trained VGG16, VGG19, and ResNet18 models for the three respective streams. The method introduces the World Politicians Deepfake Dataset (WPDD), created by extracting over 320,000 frames from videos of 20 politicians on YouTube. Various manipulations, including colour, hairstyle, structure and genuine face discrimination, are applied to both genders. This encompasses false detection like discrimination between fake and real faces, identification of seven face manipulations, and analysis of the system performance under various face manipulation. This method acquired accuracy scores of 99.98% and 99.95% for the DeepFake-TIMIT HQ and Celeb-DF datasets. The limitation of the system is its potential vulnerability to adversarial attacks and variations in face orientations.

Sun et al. [17] introduced FCN-DA-LSA method for detection of face spoofed images. The FCN local classifier effectively utilizes face spoof distortion properties, while the domain adaptation layer enhances generalization across various domains. This preserves high-frequency spoof clues from face recapture processes. FCN-LSA gained improved performance among advanced methods, with FCN-DA-LSA further improving results. Under hybrid protocols, the FCN-DA-LSA achieves HTERs of 11.22% and 21.92%, respectively. The improvement observed in FCN-DA-LSA over the basic FCN amounts to approximately 5.67%. While it demonstrates effectiveness as a form of few-shots supervised domain adaptation, the reliance on additional data poses a constraint. It can further explore unsupervised few-shot domain adaptation methods to mitigate this limitation and enhance performance, particularly in cross-PAI or cross-camera works.

Sun et al. [18] framed a depth-based FCN approach for face spoofing detection is revised, exploring diverse supervision techniques. In response, SAPLC is proposed, comprising an FCN and an aggregation technique. The FCN evaluates pixel-level ternary labels (real foreground, fake foreground, unclassified background), which are then separated to make accurate decisions. Experimental evaluation is demonstrated and achieves competitive performance with advanced methods under various common protocols. In protocols, SAPLC achieves ACERs of 0.42%, 2.50%, 3.89%, and 9.31%, respectively. The reliance on pixel-level ternary labels and aggregation for image-level decisions could introduce computational overhead and increase processing time, which may not be feasible for real-time face spoofing detection systems.

The existing papers demonstrate various approaches to face spoofing detection, they often have limitations such as reliance on external data, computational complexity, and suboptimal generalizability. The proposed DCGAN model addresses these drawbacks by generating diverse synthetic spoofed images, augmenting the training dataset, simplifying the training process, and improving the capacity of the model to capture spoof-specific features.

III. Problem Statement

Even with improvements in facial recognition technology, biometric systems still suffer a great deal of difficulty from face spoofing attacks. This problem has been made worse by deepfake manipulations in particular, which makes the facial spoof detection techniques employed today insufficient. These approaches frequently depend on outside datasets that are computationally demanding and do not fully cover the range of real-world circumstances, which makes real-time processing more difficult. More robust and adaptable solutions are required since they might not be able to properly handle different spoofing tactics or adjust to changing attack plans [18]. To address these issues, the proposed method makes utilisation of Deep Convolutional Generative Adversarial Networks (DCGAN) in order to gain over current constraints. This technique allows for the quick and precise real-time recognition of changed images by utilizing deep learning and GAN technology, which is especially useful in situations when speed is of the essence. This capacity has important ramifications for standard applications including authentication systems, surveillance setups, and identity verification processes.

The objective of the project is to develop and evaluate a face spoof detection technique based on DCGAN to counter the rising threat of deepfake manipulations in biometric systems. It seeks to determine how well DCGAN performs in real-time processing for crucial applications like surveillance and authentication systems, examines its efficacy in a variety of real-world scenarios and spoofing techniques, and appraises its adaptability in fending off changing attack tactics. In order to improve overall security and reliability, the research also examines the practical ramifications of incorporating this technology into currently in employ biometric authentication systems.

IV. Proposed Face Spoof Detection with Deep Convolutional Generative Adversarial Network

The proposed Face Spoof Detection with Deep Convolutional Generative Adversarial Network is developed to enhance biometric authentication system using CelebA dataset. DCGAN consist of generator and discriminator networks, trained adversarial to produce realistic spoofed face images and distinguish them from genuine ones. The generator comprises multiple layers, starting with input noise vectors, and progressively up-samples them into high-dimensional representations to generate output images. Before feature extraction, the discriminator has an important role in classifying input images as genuine or generated. It trains to distinguish between real and generated images through adversarial training, guided by a loss function like binary cross-entropy. Feature extraction involves the discriminator capturing discriminative characteristics from input images, such as texture and spatial relationships, to distinguish between genuine and spoofed data. These characteristics are then used as input to a Deep Convolutional Network (DCN) for the final decision on face spoof detection. Fig. 1 depicts the block diagram of Face Spoof Detection using Deep Convolutional Network which classifies real and spoofed images from the CelebA dataset.

A. Data Description

The CelebFaces Attributes (CelebA) dataset which consists of 200,000 images of celebrity, each labelled with 40 binary attributes. The CelebA dataset consists of celebrity faces which contains 202,599 images. Every image in the dataset is annotated with labels of 40 binary attributes, covering a wide range of facial attributes such as Bald, Bangs, Black Hair, Blond Hair, Eyeglasses, Smiling, Wearing Hat, and other variations. The images in the CelebA dataset are of varying resolutions, with most images having a resolution of 178x218 pixels. The dataset includes images of celebrities from various demographics, ethnicities, ages, and genders, providing a diverse set of facial characteristics. The attribute annotations provide binary labels indicating the presence or absence of every attribute in the corresponding image. The images are typically stored in JPEG format, while the attribute annotations are provided in a text file or a structured format like CSV. The CelebA dataset is commonly used for tasks such as face recognition, attribute prediction, facial attribute editing, and face synthesis. It serves as a powerful dataset for training and evaluating deep learning systems like DCGANs for face spoof detection.

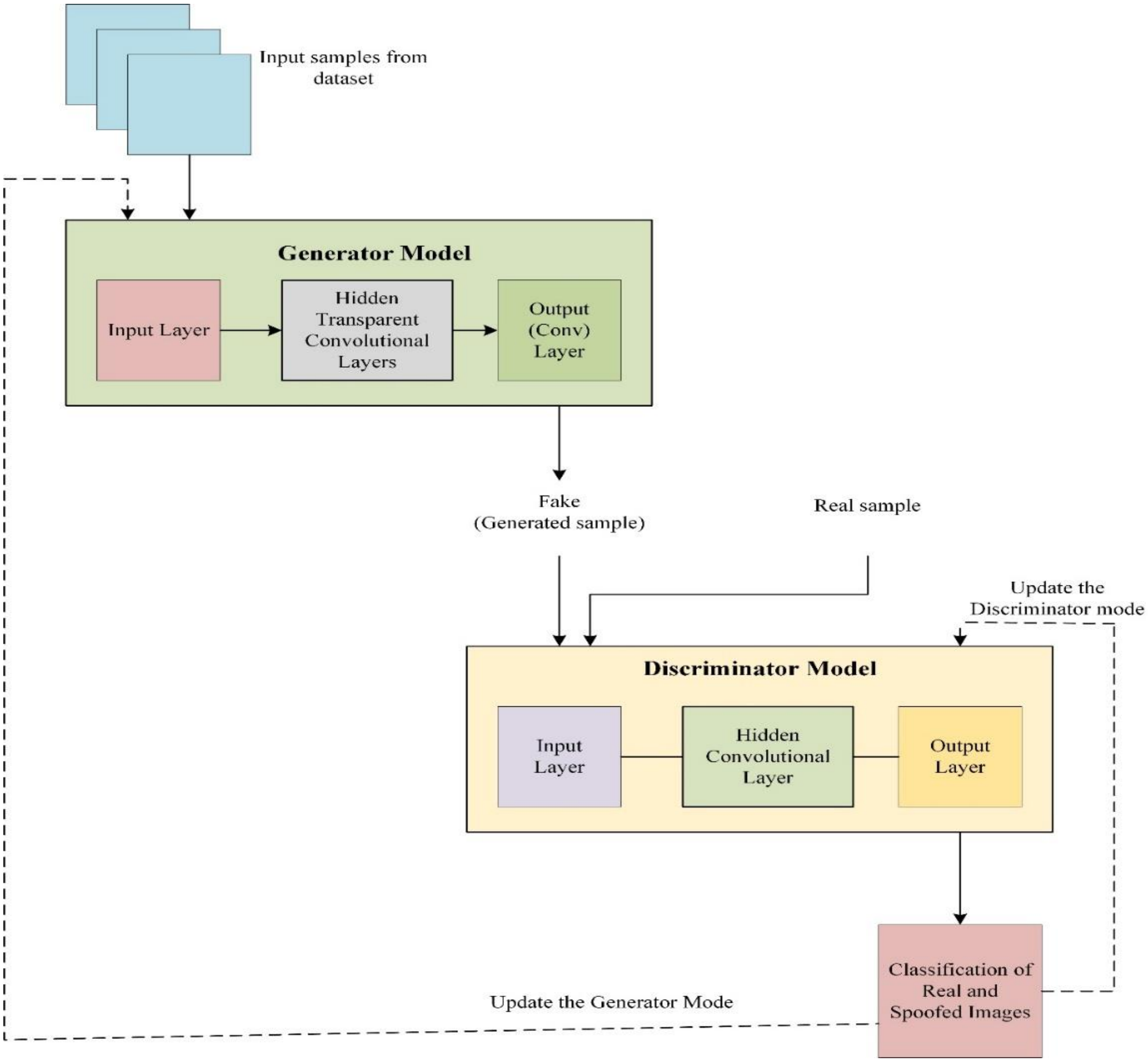
Input samples from dataset
Generator Model
Input Layer
Hidden Transparent Convolutional Layers
Output (Conv) Layer
Fake (Generated sample)
Real sample
Update the Discriminator mode
Discriminator Model
Input Layer
Hidden Convolutional Layer
Output Layer
Classification of Real and Spoofed Images
Update the Generator Mode

Fig. 1. Block diagram of face spoof detection with DCGAN.

B. Data Collection and Pre-processing

The data collection comprises celebrity face images collected from various sources, including the internet, celebrity websites, and publicly available databases. The dataset creators curated these images to ensure diversity in terms of demographics, facial attributes, and expressions. Each image in the CelebA dataset is manually annotated with a set of binary attribute labels. These annotations cover facial attributes such as age, eyeglasses, hair, gender and various facial expressions. The annotations provide valuable ground truth information for training and evaluating machine learning models. Fig. 2 depicts the pre-processing of CelebA dataset for face spoof detection.

The original images may vary in size and aspect ratio. The images are reconstructed to a standard resolution, typically 178x218 pixels. Pixel values in the images are normalized to a common scale, often ranging from 0 to 1 or -1 to 1. Normalization helps in minimizing alterations in pixel across different images. Rotation, flipping, cropping, and brightness adjustments may be applied to increase the diversity of the dataset and improve model generalization. Noise reduction techniques may be employed to enhance image quality and remove unwanted artifacts. Typically, the majority of the data is allocated to the training set, while smaller portions are used for validation and testing. Thus, the pre-processed CelebA dataset is prepared for face recognition, attribute prediction, and face spoof detection.

C. Deep Convolutional GAN Architecture

The DCGAN architecture for face spoof detection involves a combination of generator and discriminator trained adversarial to produce realistic spoofed face data and distinguish them from genuine ones. The generator typically consists of multiple layers of neural network units, organized in a deep architecture. It starts with one or more input layers, usually taking random noise vectors as input. These noise vectors serve as the seeds for generating new data samples to augment the data. The noise vectors are passed through several hidden layers, often implemented using convolutional layers, followed by ReLU to introduce non-linearity and learn hierarchical representations. The generator progressively up-samples the input noise into high-dimensional representations, which produces output images with the desired dimensions, such as grayscale or colour face images as shown in Fig. 3.

In DCGAN, the discriminator plays a crucial role in distinguishing between genuine and generated (spoofed) face images. The discriminator network is tasked with classifying input images as either genuine (real) or generated (spoofed). It takes both genuine face data from the dataset and generated face data produced by the generator as input samples. The discriminator network contains multiple convolutional layers, designed to extract features from the input and make a binary classification. During the training process, the discriminator network learns to distinguish between real and generated data by updating its parameters to minimize its classification error. It is trained in an adversarial approach with the generator, which aims to produce realistic faces that can fool the discriminator network, while the discriminator aims to accurately classify the images. The performance of discriminator is evaluated using binary cross-entropy, which evaluates the discrepancy among the predictions of the discriminator (real or generated). The loss function guides the updates to the discriminator's parameters during training, helping it improve its capability to discriminate between genuine and generated samples.

Fig. 4 depicts the learning phase of genuine and fake data by discriminator network. The discriminator and generator are trained iteratively, where the generator targets to produce data that are indistinguishable from genuine ones, and the discriminator network for accurately classifying between real and generated images. This adversarial training process helps both networks enhance over time, with the discriminator becoming better at differentiating real and generated data, and the generator becoming better at producing realistic images to fool the discriminator.

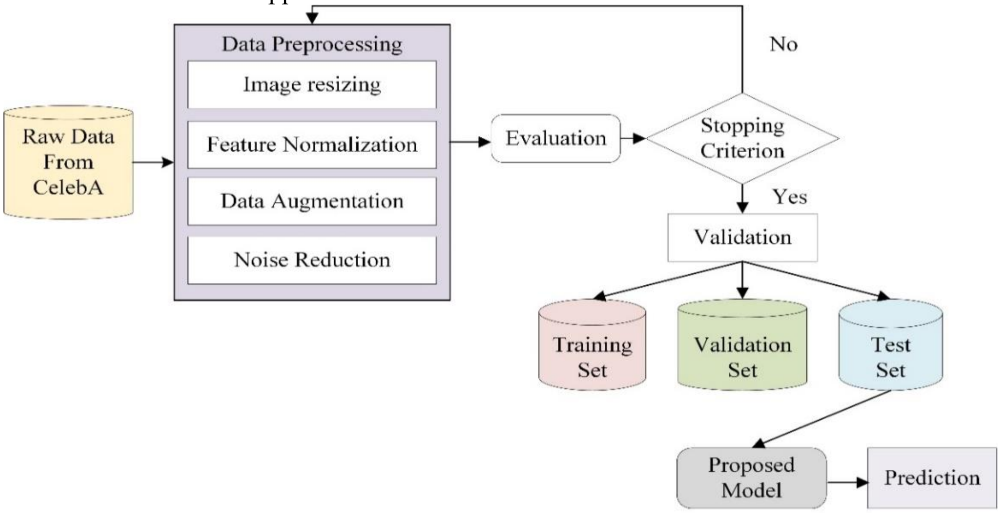

Fig. 2. Pre-processing of CelebA dataset.

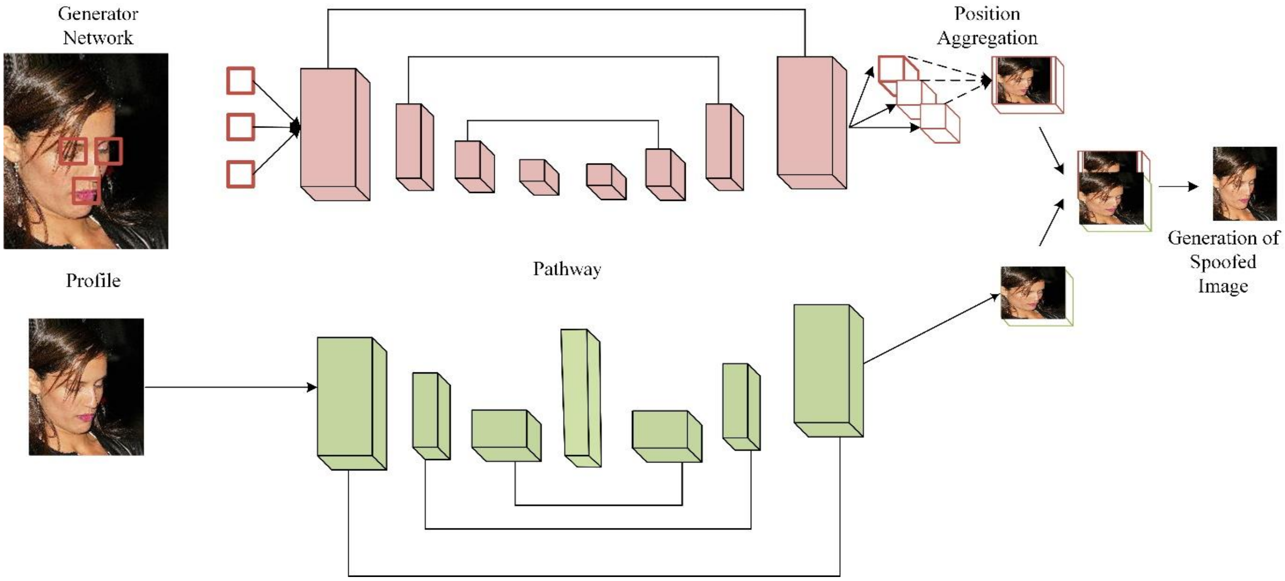

Fig. 3. Generator network in DCGAN.

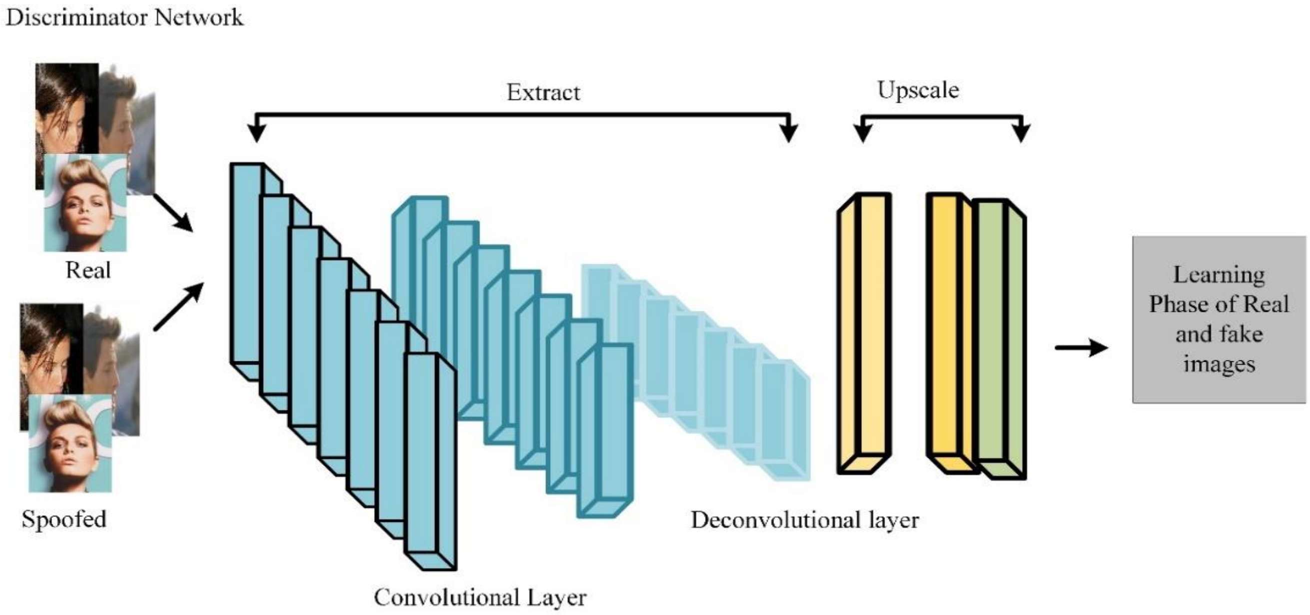

Fig. 4. Discriminator network of DCGAN.

D. Feature Extraction and Detection of Face Spoof Image using DCGAN

In face spoof detection using DCGAN (Deep Convolutional Generative Adversarial Networks), feature extraction is one of the critical steps that involves capturing discriminative characteristics from input images. The process begins with feeding genuine and spoofed face images into the discriminator network, which has been trained to differentiate between the two types of images through adversarial training. Through the adversarial training process, the discriminator becomes adept at extracting features that are discriminative for face spoof detection. These features encode subtle differences between genuine and spoofed faces, such as inconsistencies in texture, lighting, or spatial relationships. After feature extraction in face spoof detection using DCGAN, the extracted features from the discriminator capture important characteristics of both genuine and spoofed faces. These features represent high-level representations learned during the adversarial training process, where the generator is to produce realistic spoofed faces to fool the discriminator, and the discriminator learns to distinguish between genuine and spoofed faces. These features are abstracted from the raw pixel values of the input images and are encoded in a lower-dimensional feature space, making them more suitable for detection tasks. These features are then fed to a Deep Convolutional Network (DCN), which makes the final decision on whether an input image is genuine or spoofed based on the learned representations.

Fig. 5 depicts the framework of Face Spoof Detection using DCGAN in which real and spoofed images are detected. In face spoof detection using DCGAN, performance using the loss function is formulated in Eq. (1),

$$Loss = -(b\,log(a) + (1-b)\,log(1-a)) \quad (1)$$

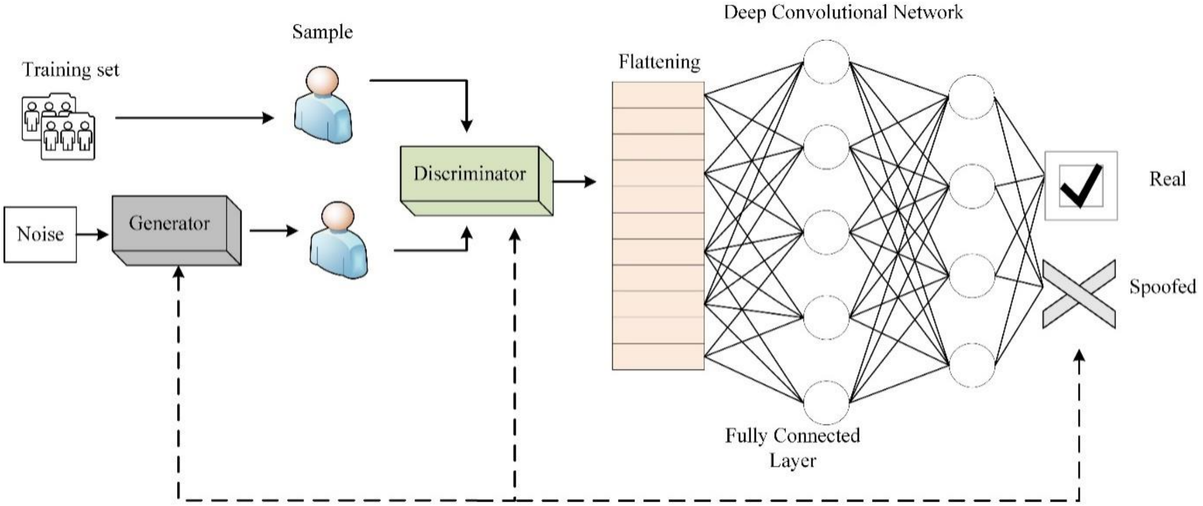

Fig. 5. Face spoof detection using DCGAN.

Here, b represents the true label of an observation, indicating whether it is a genuine (real) image or a spoofed (fake) image. The predicted label of the observation is denoted by a. It is important to note that 'a' lies between 0 and 1, representing the probability that the observation belongs to the genuine samples. Depending on whether the system designate the real label as 0 (indicating fake images) or 1 (for real images), aim to minimize either log(1-a) or log(a), respectively. This evaluation metric helps gauge the ability of the model to distinguish between genuine and spoofed faces during training [19].

Let p denote the Gaussian noise distribution, and u represent the complex image. The generator function G (u, p) generates synthetic images, while D(u, v) represents the discrimination. Each output of the discriminator network (s = 1, 2, 3, 4) contributes to the decision process, with corresponding weights λs ensuring proper discrimination between genuine and spoofed data.The loss function of the discriminator, denoted as LD-sGAN(G, D), is formulated in eqn.2,

$$LD - sGAN(G, D) = Eu, v[logD(u, v)] + Eu, p[log(1 - D(u, G * (u, p)\ I))] \quad (2)$$

Here, the discriminator targets to maximize the loss function by accurately differentiating real and generated data. Conversely, the generator strives to minimize the loss function to generate more convincing fake images. The optimization paths of both the generator and discriminator are guided by this loss function, facilitating the adversarial training process in face spoof detection model.

V. Results and Discussion

In this research, the implementation of face spoof detection framework using python software has been successfully achieved. This study aims in accuracy improvement of face spoof detection and identification using CelebA,a large-scale face attributes dataset. The framework achieved high accuracy of 99.1% and minimised false detection. The DCGAN architecture successfully generated realistic spoofed face images, which were challenging to distinguish from genuine ones. The performance of the model was enhanced by the adversarial relationship between the discriminator and generator networks in DCGAN, which made it easier to acquire discriminative features for face spoof detection. Fig. 6 shows the detection of real and spoofed images using proposed DCGAN. The proposed DCGAN architecture is adept at detecting both real and spoof images with high accuracy. The model learns to differentiate between authentic and manipulated facial images.

A. *Performance Metrics*

1) Accuracy: In the DCGAN-based face spoof detection model, accuracy evaluates the proportion of accurately classified images (genuine and spoofed) out of all the images in the test dataset. The formula for accuracy is given in Eq. (3),

$$Accuracy = \frac{\text{RP+RN+FP+FN}}{\text{RP+RN}} \quad (3)$$

where, RP represents the number of true positive identifications (accurately classified spoofed images). RN represents the number of true negative identifications (accurately classified genuine images). FP represents the number of false positive identifications (genuine images inaccurately classified as spoofed). FN represents the number of false negative identifications (spoofed images inaccurately classified as genuine).

2) Precision: Precision is a pivotal metric in evaluating the performance of the framework based on the DCGAN-based face spoof detection architecture. It holds significant importance in classifying spoofed and genuine face images accurately. Precision measures how effectively the model can identify spoofed face images while minimizing misclassifications. The equation of precision is represented by Eq. (4),

$$Precision = \frac{AP}{AP+BP} \quad (4)$$

Here, AP denote the instances where the model correctly identifies spoofed face images, while BP represent cases where genuine face images are incorrectly classified as spoofed. Precision value from between 0 and 1, with a value of 1 indicating perfect precision, where all positive predictions are correct, and a value of 0 indicating that no correct positive predictions were made.

3) Recall: Recall in a face spoof detection model with DCGAN shows to the capacity of the model to accurately identify genuine face images as genuine. Specifically, it measures the proportion of actual genuine face images that are correctly classified as genuine by the framework, out of all genuine face images in the dataset. The formula for recallis given by Eq. (5),

$$Recall = \frac{True\ Positives}{True\ Positives + False\ Negatives} \quad (5)$$

Real Images

Fig. 6. Detection of real and spoofed images using proposed DCGAN.

where, True Positives (TP) are the number of genuine face images accurately identified as genuine and False Negatives (FN) are the number of genuine face images inaccurately identified as spoofed.

4) F1 score: In face spoof detection using DCGAN architecture, the F1 score serves as a crucial metric for evaluating performance, particularly in tasks involving the identification and categorization of spoofed and genuine face images. The F1 score is computed using eqn.6,

$$F1score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \qquad (6)$$

This equation provides an evaluation assessment of the framework in accurately classifying positive (spoofed) and negative (genuine) instances. The F1 score offers a comprehensive measure of the performance of the system by considering both precision and recall, in distinguishing between spoofed and genuine face images in face spoof detection.

Fig. 7 shows Accuracy Curve for Proposed Face Spoofed Detection using DCGAN. It achieves an impressive accuracy rate of 99.1% with an improvement of 9.056% over existing methods of Sequential CNN, ANNBBS and YOLO-CNN-XGBoost. This curve, plotted over the epochs, illustrates the learning process of the model, initially starting at lower accuracy values and gradually ascending as the model refines its capability to discern between genuine and spoofed faces. Thus, it upgrades the security and access control of biometric authentication systems in real-world applications.

Fig. 8 depicts the Losses of Training and Validation of the proposed DCGAN for face spoof detection which indicates the evolution of the performance of the technique. The training loss represents the discrepancy between the predicted and actual values for the training dataset, reflecting learning phase of the model to generate realistic spoofed face images and distinguish them from genuine ones. Ideally, both training and validation losses should decrease simultaneously, indicating that the model effectively generalize to new instances.

Table I depicts the Evaluation Metrics of the Proposed FSD-DCGAN with Existing Frameworks**.** The proposed FSD-DCGAN method stands out as the most robust and accurate among the existing techniques. The adversarial dynamic facilitated the learning of discriminative features for face spoof detection. It achieves an impressive 99.1% accuracy, when compared to all other methods. Its precision (93%) and recall (89.5%) strike a commendable balance, resulting in an F1 score of 92%. In contrast, the Sequential CNN method, while respectable, falls short in terms of recall (78.2%). ANNBBS exhibits high accuracy (94.9%) but sacrifices recall (72%) and F1 score (81%). The YOLO-CNN-XGBOOST approach performs reasonably well overall, with an accuracy of 90.73% and a balanced F1 score (86.36%).

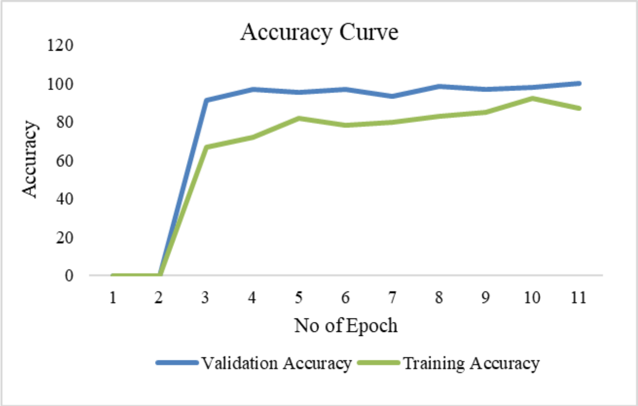

Fig. 7. Accuracy curve for proposed face spoofed detection using DCGAN.

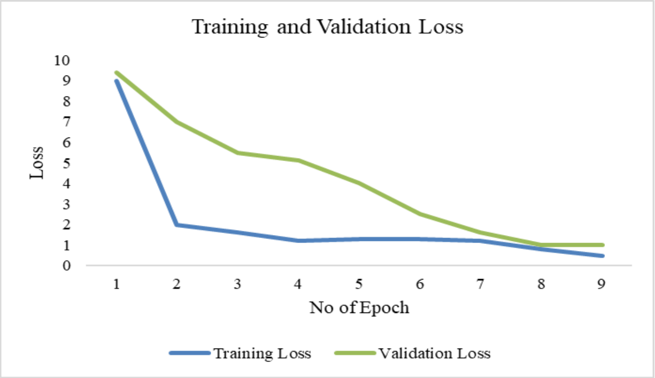

Fig. 8. Training and validation loss of proposed DCGAN.

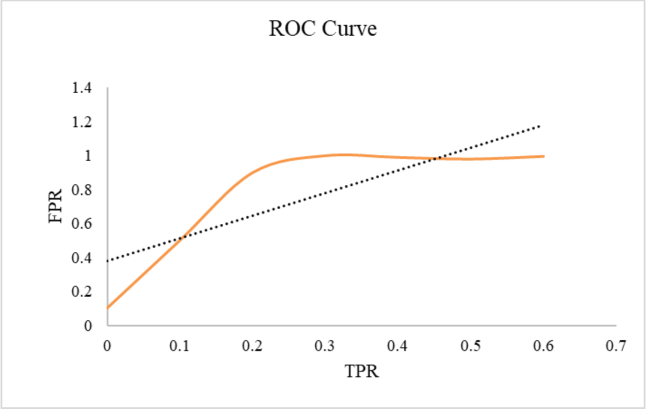

Fig. 9. ROC curve for the proposed face spoof detection using DCGAN.

TABLE I. EVALUATION METRICS OF THE PROPOSED METHOD WITH EXISTING FRAMEWORKS

Methods	Accuracy	Precision	Recall	F1 score

Sequential CNN [20]	87%	93.6%	78.2%	86.8%
ANNBBS [21]	94.9%	90%	72%	81%
YOLO-CNN-XGBOOST [22]	90.73%	87.36%	85.39%	86.36%
Proposed FSD-DCGAN	99.1%	93%	89.5%	92%

The Area Under the Curve (AUC) in face spoof detection model using DCGAN indicates to the area under the Receiver Operating Characteristic (ROC) curve. A higher AUC value, shows superior discrimination and better overall accuracy in distinguishing between real and spoofed faces. The formula for calculating the Area Under the Curve (AUC) in a ROC curve is given in Eq. (7),

$$AUC = \sum i = 1n - 12(xi + 1 - xi) \cdot (yi + yi + 1) \quad (7)$$

where, (xi,yi) are the points of the ROC curve, and n is the total number of points. The AUC shows the integral of the ROC curve, which measures the overall evaluation of a binary classification approach.

Fig. 9 shows ROC Curve for the Proposed Face Spoof Detection using DCGAN. The Receiver Operating Characteristic (ROC) for the proposed face spoof detection using DCGAN illustrates the exchange between True Positive and False Positive Rates across different decision limits. A higher area under the ROC curve shows superior discriminatory evaluation, with the model achieving high true positive rates while minimizing false positive rates.

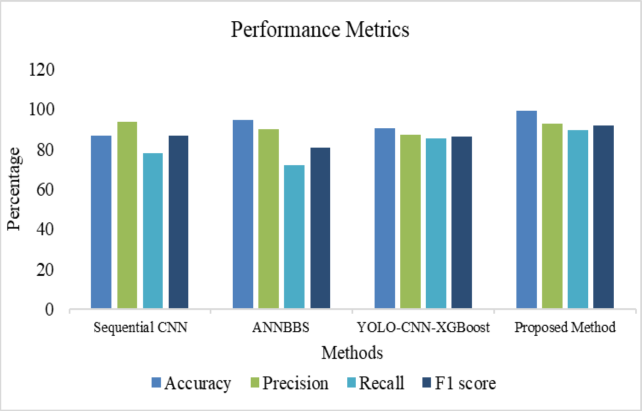

Fig. 10. Performance metrics of proposed face spoof detection using DCGAN.

Fig. 10 depicts performance metrics of proposed system with existing framework. The precision of the proposed framework DCGAN(99.1%) is greater than the existing approaches of Sequential CNN(87%), ANNBBS(94.9%) and YOLO-CNN-XGBoost (97.22%). The recall of the suggested method DCGAN (89.5%) is higher than the existing approaches of Sequential CNN (78.2%), ANNBBS (72%) and YOLO-CNN-XGBoost (85.39%). The F1-score of the suggested method DCGAN (92%) is higher than the existing approaches Sequential CNN (86.8%), ANNBBS (81%) and YOLO-CNN-XGBoost (86.36%).

B. *Discussion*

The discourse pertaining to the diverse frameworks utilised for identifying deep fakes and face spoofing highlights the diverse methodologies that researchers are implementing to tackle this critical challenge. The structure of Arora et al. [11], which focuses on the extraction and categorization of face characteristics, shows encouraging levels of accuracy but could run into problems with changing spoofing techniques and a variety of datasets. With potential for improvement, Patel et al. [12] improved deep-CNN structure has great accuracy rates for a variety of false image types, including video deepfake detection. Although there are certain restrictions in domain adaptation strategies, Kumar et al. [13] focus on metric classification and triplet network design emphasises the significance of feature space differentiation. The Generative Adversarial Ensemble Learning method by Baek et al. [14] prioritises discrimination enhancement and achieves respectable accuracy at the cost of training time and computational resources. The CNN model developed by Ranjan et al. [15] using Transfer Learning exhibits better performance on various datasets; nonetheless, its dependence on pre-trained models could result in less-than-ideal outcomes. The above discussions collectively highlight the continuous attempts, each with unique advantages and disadvantages, to counter the spread of face spoofing and deepfakes.

In the domain of face spoof detection leveraging deep learning techniques, a significant advancement was achieved by integrating Deep Convolutional Generative Adversarial Networks (DCGAN), resulting in an outstanding accuracy of 99.1%, exceeding the capabilities of conventional approaches like Sequential CNN [20]. The interplay between the model's training dynamics and its effectiveness in discerning between genuine and spoofed faces is depicted through graphical representations of training and testing accuracy, loss, and ROC curves. Using samples from CelebFaces Attributes (CelebA), the model shows its ability to distinguish between authentic and spoofed facial images. Discriminative features may be learned from raw input data using DCGAN, which eliminates the requirement for human feature engineering and is a benefit for employing it for feature extraction. The outcomes generated by the proposed framework illustrate its efficacy in recognizing the subtle differences between genuine and spoofed facial features. Thus, it promotes secure access control in various applications like financial services, secure facilities, and mobile devices.

VI. Conclusion and Future Works

Biometric security has advanced significantly with the use of Deep Convolutional Generative Adversarial Networks (DCGANs) for face spoof detection. The suggested framework shows improved accuracy in differentiating between real and fake face photos thanks to the cooperation of discriminator and generator networks. Based on adversarial training, the discriminator network outperforms conventional convolutional approaches in extracting discriminative features necessary for accurate spoof detection, as demonstrated by studies conducted on the CelebFaces Attributes (CelebA) dataset. This development raises the bar for future improvements in spoof detection technologies while simultaneously strengthening the security of biometric identity systems. Looking ahead, our study points to a number of interesting directions that warrant further investigation. First and foremost, it's imperative to strengthen the model against spoofing techniques that are getting more and more complex, like deepfake videos, by investigating innovative architectures and feature integration. Moreover, the real-time use of the model in real-world settings, such mobile authentication apps or surveillance systems, is very valuable for quick threat identification and reaction. To ensure that the model architecture and training process are flexible enough to adapt to a variety of datasets and changing spoofing techniques, it is imperative that they be continuously improved and optimised. Furthermore, strengthening the security and effectiveness of the model in practical applications requires reducing adversarial assaults on the model itself. The efficacy and practicality of DCGAN-based face spoof detection could be further strengthened by pursuing these future research avenues, which will additionally contribute to progress biometric security and create more robust authentication systems.

REFERENCES

[1] "Sci-Hub | Detecting DeepFake, FaceSwap and Face2Face facial forgeries using frequency CNN. Multimedia Tools and Applications, 80(12), 18461–18478 | 10.1007/s11042-020-10420-8." Accessed: Feb. 08, 2024. [Online]. Available: https://sci-hub.ee/10.1007/s11042-020-10420-8.

[2] D. Gong, O. S. Goh, Y. J. Kumar, Z. Ye, and W. Chi, "Deepfake Forensics, an AI-synthesized Detection with Deep Convolutional Generative Adversarial Networks," 2020.

[3] Y. Wang, X. Song, T. Xu, Z. Feng, and X.-J. Wu, "From RGB to Depth: Domain Transfer Network for Face Anti-Spoofing," IEEE Trans. Inf. Forensics Secur., vol. 16, pp. 4280–4290, 2021, doi: 10.1109/TIFS.2021.3102448.

[4] F. Jiang, P. Liu, X. Shao, and X. Zhou, "Face anti-spoofing with generated near-infrared images," Multimed. Tools Appl., vol. 79, no. 29–30, pp. 21299–21323, Aug. 2020, doi: 10.1007/s11042-020-08952-0.

[5] S. A. Aduwala, M. Arigala, S. Desai, H. J. Quan, and M. Eirinaki, "Deepfake Detection using GAN Discriminators," in 2021 IEEE Seventh International Conference on Big Data Computing Service and Applications (BigDataService), Aug. 2021, pp. 69–77. doi: 10.1109/BigDataService52369.2021.00014.

[6] M. Barni, K. Kallas, E. Nowroozi, and B. Tondi, "CNN Detection of GAN-Generated Face Images based on Cross-Band Co-occurrences Analysis," in 2020 IEEE International Workshop on Information Forensics and Security (WIFS), New York, NY, USA: IEEE, Dec. 2020, pp. 1–6. doi: 10.1109/WIFS49906.2020.9360905.

[7] S. B. Balasubramanian, J. K. R, P. P, V. K, and P. Trojovský, "Deep fake detection using cascaded deep sparse auto-encoder for effective feature selection," PeerJ Comput. Sci., vol. 8, p. e1040, Jul. 2022, doi: 10.7717/peerj-cs.1040.

[8] X. Ding, Z. Raziei, E. C. Larson, E. V. Olinick, P. Krueger, and M. Hahsler, "Swapped face detection using deep learning and subjective assessment," EURASIP J. Inf. Secur., vol. 2020, no. 1, p. 6, Dec. 2020, doi: 10.1186/s13635-020-00109-8.

[9] A. Chintha et al., "Recurrent Convolutional Structures for Audio Spoof and Video Deepfake Detection," IEEE J. Sel. Top. Signal Process., vol. 14, no. 5, pp. 1024–1037, Aug. 2020, doi: 10.1109/JSTSP.2020.2999185.

[10] X. Chang, J. Wu, T. Yang, and G. Feng, "DeepFake Face Image Detection based on Improved VGG Convolutional Neural Network," in 2020 39th Chinese Control Conference (CCC), Shenyang, China: IEEE, Jul. 2020, pp. 7252–7256. doi: 10.23919/CCC50068.2020.9189596.

[11] S. Arora, M. P. S. Bhatia, and V. Mittal, "A robust framework for spoofing detection in faces using deep learning," Vis. Comput., vol. 38, no. 7, pp. 2461–2472, Jul. 2022, doi: 10.1007/s00371-021-02123-4.

[12] Y. Patel et al., "An Improved Dense CNN Architecture for Deepfake Image Detection," IEEE Access, vol. 11, pp. 22081–22095, 2023, doi: 10.1109/ACCESS.2023.3251417.

[13] A. Kumar, A. Bhavsar, and R. Verma, "Detecting Deepfakes with Metric Learning," in 2020 8th International Workshop on Biometrics and Forensics (IWBF), Porto, Portugal: IEEE, Apr. 2020, pp. 1–6. doi: 10.1109/IWBF49977.2020.9107962.

[14] J.-Y. Baek, Y.-S. Yoo, and S.-H. Bae, "Generative Adversarial Ensemble Learning for Face Forensics," IEEE Access, vol. 8, pp. 45421–45431, 2020, doi: 10.1109/ACCESS.2020.2968612.

[15] P. Ranjan, S. Patil, and F. Kazi, "Improved Generalizability of Deep-Fakes Detection using Transfer Learning Based CNN Framework," in 2020 3rd International Conference on Information and Computer Technologies (ICICT), San Jose, CA, USA: IEEE, Mar. 2020, pp. 86–90. doi: 10.1109/ICICT50521.2020.00021.

[16] S. Yavuzkilic, A. Sengur, Z. Akhtar, and K. Siddique, "Spotting Deepfakes and Face Manipulations by Fusing Features from Multi-Stream CNNs Models," Symmetry, vol. 13, no. 8, Art. no. 8, Aug. 2021, doi: 10.3390/sym13081352.

[17] W. Sun, Y. Song, H. Zhao, and Z. Jin, "A Face Spoofing Detection Method Based on Domain Adaptation and Lossless Size Adaptation," IEEE Access, vol. 8, pp. 66553–66563, 2020, doi: 10.1109/ACCESS.2020.2985453.

[18] W. Sun, Y. Song, C. Chen, J. Huang, and A. C. Kot, "Face Spoofing Detection Based on Local Ternary Label Supervision in Fully Convolutional Networks," IEEE Trans. Inf. Forensics Secur., vol. 15, pp. 3181–3196, 2020, doi: 10.1109/TIFS.2020.2985530.

[19] Kevin, "Generating Human Faces with DCGANs," Medium. Accessed: Feb. 12, 2024. [Online]. Available: https://medium.com/@dungwoong/generating-human-faces-with-dcgans-7a4d54eaa89b.

[20] 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), NV, USA: IEEE, Jan. 2021, pp. 1483–1488. doi: 10.1109/CCWC51732.2021.9376030.

[21] S. Kumar et al., "Face Spoofing, Age, Gender and Facial Expression Recognition Using Advance Neural Network Architecture-Based Biometric System," Sensors, vol. 22, no. 14, Art. no. 14, Jan. 2022, doi: 10.3390/s22145160.

[22] A. Ismail, M. Elpeltagy, M. S. Zaki, and K. Eldahshan, "A New Deep Learning-Based Methodology for Video Deepfake Detection Using XGBoost," Sensors, vol. 21, no. 16, Art. no. 16, Jan. 2021, doi: 10.3390/s21165413.