

DeepFake Detection Using Deep Learning

Mariam Rehman 1 ^(\boxtimes), Mehran Rasool¹, and Sadaf Safder²

¹ Government College University, Faisalabad, Pakistan mariamrehman@gcuf.edu.pk

² National Center in Big Data and Cloud Computing, University of Agriculture, Faisalabad, Pakistan

Abstract. A deepfake is a computer-generated video or image where one person's face is replaced with another face of a person which uses a generative adversarial network (GAN) to create and alter images that are practically impossible for humans to distinguish from authentic ones. The development of GAN technology has led to significant improvements in image generation. This progress has made it difficult for humans to differentiate between generated images and raised concerns about their misuse and also creating security threats for the society. Deepfake image detection is an essential challenge because the current methods often face inaccuracy and time-consuming issues. The research work employed GAN discriminators to address these issues. The experiment used the CelebA dataset, which contained diverse celebrity images. Moreover, the proposed model consists of components i.e., generator and discriminator. The generator creates fake data from the training images, while the discriminator distinguishes real from the fake images. The result shows that the proposed approach is out-performing with an accuracy of 95.8% in identifying deep fake images, even in the presence of various manipulations. The proposed model is helpful for enhancing trust and security in the society.

Keywords: DeepFake · GAN · Deep Learning

1 Introduction

In today's digital era, the manipulation of visual content has become incredibly advanced. Deep fake technology uses special computer programs known as Generative Adversarial Networks (GANs). These programs can create computer-generated images and videos that resemble real ones. Earlier, the technology could be used to create art and entertainment that raises serious challenges [\[1\]](#page-11-0). Deepfake technology involves the use of convolutional neural networks, particularly Generative Adversarial Networks (GANs), to create fake images or videos by replacing one person's face with another's person. Recently, social media issues have highlighted instances in which celebrities' faces were illicitly swapped into explicit content, causing damage to their reputations and long-term harm to the identities of well-known persons and common people in society [\[2\]](#page-11-1).

GAN model was first introduced by Ian J. Goodfellow in 2014 [\[2\]](#page-11-1). GAN was described as a connection between two components i.e., discriminator named as "D" and the generator named as "G." GAN method is an effective way to generate images. Over time, more advanced GANs such as BEGAN [\[3\]](#page-11-2), PGGAN [\[4\]](#page-11-3), StyleGAN [\[5\]](#page-11-4), and StyleGAN2 [\[6\]](#page-12-0)emerged. These advanced GANs have been successful in creating images for numerous purposes, such as image enhancement, translation, and image filling in missing parts.

The images generated by GANs are really hard to detect with the human eyes. This level of realism can provide an in-depth insight into particular issues especially when GAN-generated images are utilized for deception purposes. When these images are used to create fake news or to deceive ordinary people on social media by generating fake personal information, several serious challenges arise. Firstly, there are ethical problems, as the planned spread of incorrect information may affect public perception and damage trust in digital content. Secondly, there may be legal implications because these activities may violate laws governing misinformation, defamation, or identity theft. Finally, from a security aspect, GAN-generated images exploited for illicit purposes may lead to various problems, including financial scams and identity theft [\[7\]](#page-12-1).

There are various detection algorithms have been developed to address the issues mentioned earlier which can be grouped into two categories i.e., Conventional and Deep learning methods. Conventional methods have been developed for extracting image properties such as texture and structural features which rely on manually created methodologies These methods offer a simple and relatable path for detecting fake images [\[8–](#page-12-2)[11\]](#page-12-3). Although, the conventional methods have various drawbacks which require large processing resources to provide excellent performance across various scenarios. In comparison, deep learning methods have gained the interest of researchers due to their excellent outcome in image classification. Deep learning methods [\[12](#page-12-4)[–16\]](#page-12-5) have the advantage of being less computationally complex compared to conventional methods, but they lack interpretability. These methods require a large amount of data to train efficiently and are susceptible to overfitting, which can limit their practical application. Therefore, there is still a need for continual efforts to develop an efficient method for GAN-generated image detection.

GANs were originally designed for image creation, with a generator network producing synthetic images and a discriminator network discriminating real from fake images. Which involves training a GAN on a dataset that contains both real and GANgenerated fake images. The discriminator network is trained to distinguish between real and GAN-generated images, a process known as adversarial training. This rigorous training improves the network's capacity to identify DeepFakes precisely. Finally, the key contributions of this research are demonstrated by systematic experimentation, which evaluates the performance, accuracy, and reliability of the GAN-based detection model.

The experiment introduces a novel CNN-GAN based architecture designed to detect deep fake images. This innovative approach enhances the capacity to identify manipulated images by training on a preprocessed dataset to reduce the threats of deep fakes. Moreover, it provides an important tool for identifying the real images.

This research explores the use of celebrity image datasets in deepfake detection. The research improves the accuracy of identifying modified images by leveraging renowned celebrities. To employ these datasets provides a model for protecting celebrities from identity theft within deep fakes content.

This study contributes by thoroughly evaluating the proposed CNN-based GAN model's efficiency in detecting DeepFakes images.

The paper is organized in the following manner. Section [2](#page-2-0) provides the detailed review of literature on GAN and its types. Section [3](#page-3-0) presents the methodology and discusses the proposed detection model of the research work. Section [4](#page-8-0) provides details about results and discussion about the experiments performed. Finally, the Section [5](#page-11-5) describes conclusion and future work related to the research work.

2 Literature Review

GANs (Generative Adversarial Networks) are type of deep learning model that has revolutionized the field of generative modelling. GANs are used to create new data that is similar to a training dataset. Unlike other generative models that use explicit probability distributions, GANs learn to generate data by training two types of neural networks: a generator network and a discriminator network [\[17\]](#page-12-6).

Mirsky et al. [\[18\]](#page-12-7) examined DeepFakes by studying reenactment techniques such as manipulating facial expressions, lips, posture, or even an entire body, as well as conversion methods such as face swapping or transferring. Verdoliva et al. [\[19\]](#page-12-8) provided an overview, distinguishing between conventional methods based on sensor-based, modelbased, and supervised methods, as compared to methods based on deep learning techniques such as vCNN models. Shobhit et al. [\[20\]](#page-12-9) investigated several images and video manipulation methods i.e., popular methods, and forgery detection methods. Syed Sadaf Ali et al. [\[21\]](#page-12-10) designed advanced deep learning algorithms to detect double image compression forgeries, whereas Huang et al. [\[22\]](#page-12-11) used data augmentation and single sample clustering to improve FakeLocator's detection of various DeepFake methods.

Table [1](#page-3-1) illustrates s a comparison of several GAN types, considering their architectural structure, activation functions, number of layer, advantages, and limitations. The table demonstrates that by implementing a configuration consisting of 4 convolutional and de-convolutional layers, along with the activation functions Tanh, ReLU, and Leaky ReLU, the proposed model outperforms compared to others, achieving an accuracy of 95%.

3 Methodology

3.1 Dataset

In this research, the CelebA attributes dataset has been used. CelebA is a huge dataset including over 200,000 celebrity images annotated with 40 attributes. This extensive dataset contains a broad variety of facial data, encompassing a wide range of changes in facial emotions, positions, and backgrounds because of its thorough annotations, which include parameters such as gender, age, the presence of spectacles, and facial expressions, the dataset is widely used in computer vision and machine learning domains. Therefore, the dataset has been selected to perform DeepFakes detection in this research work.

The dataset has been distributed into training, testing and validation sets. There are total of 202,599 images in the dataset. Out of total images, 162770 belongs to training set, 19961 belongs to testing data set while 19866 images belong to validation set. Among the dataset, 80% of images are used for training, 10% for tests, and 10% for validation. The details of distribution are given in Table [2.](#page-4-0)

Data Division set	Total images
Training Set	162770
Test Set	19961
Validation Set	19866

Table 2. Distribution of training, testing, and validation dataset

3.2 Preprocessing

The GAN preprocessing stage includes three critical operations i.e. image resizing, rescaling, and normalization. The goal of rescaling is to bring the dataset values into a consistent and standardized range, specifically between -0.9608 and 0.9608, which is accomplished by increasing the pixel values of each image by 2 and then subtracting 1. The normalization step is critical for accelerating convergence during training and minimizing gradient vanishing or exploding issues. Additionally, the images are resized to 32 x 32-pixel dimensions to maintain uniformity. The dataset resulting from the preprocessing steps, serves as an input for the GAN model while aligning with the model's requirements and supporting effective training and meaningful outcomes.

3.3 Convolutional Based GAN

A Convolutional Generative Adversarial Network is a cutting-edge deep learning model that has transformed generative modeling and image synthesis. Convolutional GANs is a version of the basic GAN architecture that are specifically designed for detecting GAN generated images. In a competitive training procedure, two neural networks i.e., the generator and the discriminator are integrated.

Fig. 1. Flow diagram of proposed Convolutional based GAN

Figure [1](#page-4-1) demonstrates the process of generating random noise to feed into the proposed model. Later, the noise vector is fed into the generator, comprising of deconvolutional layers and activation functions. The noise is transformed within the generator, eventually resulting in the generation of an image. The generator takes a stepby-step method, improving the image with a series of convolutional layers. The layers are adept at identifying and capturing intricate features in a hierarchical manner, which enable the network to produce realistic images as training progresses. Meanwhile, the discriminator acts as an evaluator, rigorously scrutinizing the generated images in order to distinguish from real ones. The adversarial training dynamic pushes both the generator and discriminator to constantly improve the network.

3.4 Architecture of Convolutional GAN

The proposed model i.e., CNN-based GAN architecture, is a variant of Generative Adversarial Networks (GANs) optimized for image generation tasks. The model combines convolutional layers into both the generator and discriminator networks, significantly improving their ability to analyze image data. The model includes several crucial elements. Firstly, convolutional layers are added into both the generator and discriminator networks, allowing for the extraction of detailed visual features from edges to higherlevel patterns. In the generator netwoek, strided convolutions are used to improve the generation of images while gradually increasing spatial resolution from lower to higher scales. In both networks, batch normalization is explicitly performed after convolutional layers, ensuring stable accelerated training via activation normalization. Secondly, there are de-convolutional layerswhich are also known as transposed convolution layers. These layers assist in the process of up-sampling. The layers play an important role in transforming low-dimensional noise vectors to higher-resolution images, gradually increasing their complexity and details. The weights of the generator are iteratively modified based on feedback from the discriminator throughout the training process. Notably, the discriminator's weights remain untrainable, ensuring that the focus is solely on refining the generator's performance. The interaction between the generator and discriminator is crucial to this process. The generator transforms random noise into realistic images by employing a series of convolutional layers, batch normalization, and activation functions such as leaky ReLU. In terms of loss computation, the generator's loss is evaluated using binary cross-entropy loss function. Simultaneously, the discriminator evaluates these generated images critically while distinguishing from real ones. The dynamic interplay is the core of adversarial training, in which the generator aims to outperform the discriminator by constantly improving its image generation capabilities. Figure [2](#page-6-0) demonstrates the structural architecture of the proposed model.

Fig. 2. Structural diagram of proposed Convolutional GAN

3.5 Parameters for Convolutional GAN

Table [3](#page-7-0) provides a detailed summary of the parameters used in the DCC-GAN model. In Table [3,](#page-7-0) there are several parameters including the kernel size, which determines the filter's coverage in terms of pixels, and the stride, a value that affects the filter's movement over the input image.. Furthermore, the table describes the features associated with each convolutional layer, defining the intricate features learnt during the training process. Besides this, another key feature is batch normalization, which is defined as a technique employed across neural network layers to accelerate training, improve stability, and enable the use of higher learning rates. Moreover, the activation functions play an essential role in assisting the neural network to detect complicated patterns in the image. Notably, the model's generator component uses these parameters to convert a 100-dimensional random noise input into a $32 \times 32 \times 3$ image. Concurrently, the discriminator analyses images with convolutional layers and provides a probability score indicating the authenticity of the input image. These parameter values are required for the Convolutional GAN model's training.

Layers	Kernel matrix	Stride value	Features value	Batch Normalization	Activation function		
Generalization input $(100 \times 1 \times 1)$							
D-Conv	4×4	1×1	256	Yes	ReLU function		
D-Conv	4×4	2×2	128	Yes	ReLU function		
D-Conv	4×4	2×2	64	Yes	ReLU function		
D-Conv	4×4	2×2	3	N ₀	Tanh function		
Discrimination input $(32 \times 32 \times 3)$							
Conv	4×4	2×2	32	Yes	LeakyReLU function		
Conv	4×4	2×2	64	Yes	LeakyReLU function		
Conv	4×4	2×2	128	Yes	LeakyReLU function		
Conv	4×4	1×1	1	N ₀			

Table 3. Model Parameters of Proposed model

3.6 Evaluation Metrics

The model's performance was evaluated using evaluation measures such as True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN). Precision, Recall, Specificity, and Accuracy were calculated using these measures to determine the model's efficacy. The following are detailed descriptions of these measures, as well as their associated mathematical formulas:

Precision

Precision is a measure of how effectively a model predicts a positive a positive outcome, representing the proportion of correct positive predictions produced by the model out of all positive predictions made by the model.

$$
precision = True \ positive \div True \ positive + false \ positive
$$

Specificity

Specificity is a measure of a model's ability to accurately detect negative cases in the context of binary classification evaluation metrics. It evaluates the proportion of true negative predictions among all actual negative cases.

```
specificity = True negative \div True negative + false positive
```
Recall/Sensitivity

In binary classification, recall, also known as sensitivity or true positive rate, is an important evaluation parameter which measures the model's ability to correctly identify all positive instances in a dataset out of all actual positive instances.

recall or sensitivity = *True positive* \div *True positive* \div *false negatives*

F1 Score

The F1 Score is a binary classification metric that combines precision and recall to create a single score that describes a model's performance which is particularly useful when the class distribution is unequal or when false positives and false negatives have distinct costs or implications.

 $F1$ *Score* = 2 \times *percision* \times *recall* \div *percision* + *recall*

Accuracy

Accuracy is a fundamental evaluation metric used to evaluate a classification model's overall performance. Accuracy is a measure of how well a model performs and measures the ratio of correctly predicted images to the total number of images in the dataset.

 $Accuracy = True positive + True negative \div True positive + false positive$ + *false nagatives* + *true negativ*

4 Result and Discussion

The study focuses on identifying CNN-GAN generated images, demonstrating greater performance when compared to other models. The GAN uses convolutional layers to improve its efficiency. In the context of GANs, the generator uses deconvolution to generate images from random variables, while the discriminator uses CNN to identify images as either real or fake. Convolutional layers extract features from images, while de-convolutional layers expand images based on the extracted characteristics.

The experiment was carried out on large datasets using a hybrid architecture that combines the Convolutional Neural Network (CNN) layer with Generative Adversarial Network (GAN) model. The experimentation environment was built on the Jupyter Notebook utilizing the computational capability of an available NVIDIA GPU. Moreover, the Keras 2.3.1 framework, Torch, and the Python-based open-source neural network deep learning libraries were used to implement CNN-GAN. The proposed model represents an enhancement towards exploiting deep learning technology in combination with GAN for the specific dataset. The model was trained across 100 epochs with 128 batch sizes each which allowed the model to learn intricate features and patterns from the dataset. Besides this, the model improved its effectiveness to detect DeepFakes images efficiently.

4.1 Analysis of CNN-GAN Model

The primary goal of the research was to determine the effect of the CNN-GAN model on system performance. The proposed models were evaluated using a large dataset to achieve good results. Moreover, the performance of the proposed model was evaluated based on the evaluation metrics i.e., accuracy and loss. The proposed model's accuracy was measured by its ability to accurately classifying images as real or fake, whereas the loss quantifies inaccuracies throughout the training process.

Fig. 3. Comparison of Loss and accuracy of model over 50 and 100 epochs

Figure [3](#page-9-0) demonstrates that the discriminator's accuracy and loss curves are unstable at epoch 50. However, when the number of epochs is increased to 100, accuracy and loss demonstrates an upward trend before stabilizing. During the 100th epoch, the model reaches an accuracy of 95.8 percent. In Fig. [3,](#page-9-0) x-axis represents the number of training epochs, signifying the training cycle through the entire dataset. Meanwhile, the loss and accuracy are represented on the y-axis.

Fig. 4. Result of Classification Probability of Random Test Image

In the experiment, a random image has been chosen from the test dataset, and the model predicts whether the image is fake or real, as shown in Fig. [4.](#page-9-1) The method completely assesses the model's classification capabilities and capacity to generalize

across multiple DeepFakes settings. Furthermore, the model aids in gaining insights about the model's proficiency in distinguishing various aspects and attributes associated with real and fake images, as observed through the projected probabilities.

Figure [5](#page-10-0) compares confusion matrices produced after the model evaluations at 50th and 100th epochs. Each confusion matrix is a visual aid for evaluating the model's predictions and correspondence with actual images. The matrices provide information about the model's ability to classify images as real or fake correctly. The matrices show how many images are given to each class. Furthermore, the confusion matrices identify patterns and distribution entries that reflect the model's strengths and weaknesses, allowing for future upgrades and fine-tuning to improve overall classification performance.

Fig. 5. Comparison of Confusion Matrices Between 50 and 100 Epochs

Table [4](#page-11-6) provides an exhaustive overview of major metrics of evaluation important for measuring the effectiveness of proposed Convolutional GAN model. Accuracy, which measures the overall correctness of predictions, is 0.958, which is the ratio of properly predicted instances to entire dataset size. The model's sensitivity (recall) of 0.972 represents the ability to identify true positive instances among all actual positives, which is critical for minimizing false negatives. Specificity, at 0.943, measures the model's ability to distinguish between true negatives among all actual negatives, with a focus on reducing false positives. Precision (0.946) computes the accuracy of positive predictions, emphasizing the model's ability to avoid misclassifying negatives as positives. Finally, the F1-Score (0.958) combines precision and recall into a balanced measure, indicating a model that excels in both high precision and recall.

Dataset	Measures	Percentage
Large-scale CelebFaces Attributes (CelebA)	Accuracy	0.958
	Sensitivity	0.972
	Specificity	0.943
	Precision	0.946
	F1-Score	0.958

Table 4. Evaluation matrices measurements for the proposed model

5 Conclusion

Generative Adversarial Network i.e., GAN generates synthetic data with a realistic appearance of images by developing an algorithm in a large number of iterations. Deep-Fakes technology is a hard challenge through which the differentiation can be made between real and fake. The said challenge allows researchers to provide optimal algorithms and solutions to detect DeepFakes. The proposed model is capable of working efficiently with the large dataset. The results depict that the accuracy of the proposed model is outperforming as compared to the other models. In the research work, the loss of discriminator is minimized in a number of iterations as compared to the generator's loss. The evaluation of the proposed model is performed through sensitivity and specificity. The generalization and convergence of GAN is a promising future research area for improvements.

5.1 Future Direction

There are several limitations of the proposed model i.e., difficulties with mode collapse, issues with gradient descent and usual convergence challenges in GANs. Moreover, there are many future challenges focusing on the improvement and generalization of GAN models.

References

- 1. Nguyen, T.T., et al.: Deep learning for deepfakes creation and detection: a survey. Comput. Vision Image Understand. **223**, 103525 (2022). <https://doi.org/10.1016/j.cviu.2022.103525>
- 2. Goodfellow, I., et al.: Generative adversarial networks. Commun. ACM **63**(11), 139–144 (2020). <https://doi.org/10.1145/3422622>
- 3. Li, Y., Xiao, N., Ouyang,W.: Improved boundary equilibrium generative adversarial networks. IEEE Access **6**, 11342–11348 (2018). <https://doi.org/10.1109/ACCESS.2018.2804278>
- 4. Karras, T., Aila, T., Laine, S., Lehtinen, J.: Progressive growing of GANs for improved quality, stability, and variation. In: 6th International Conference on Learning Representations, ICLR 2018 - Conference Track Proceedings, pp. 1–26 (2018)
- 5. Karras, T., Laine, S., Aila, T.: A style-based generator architecture for generative adversarial [networks. IEEE Trans. Pattern Anal. Mach. Intell.](https://doi.org/10.1109/TPAMI.2020.2970919) **43**(12), 4217–4228 (2021). https://doi.org/ 10.1109/TPAMI.2020.2970919
- 6. Karras, T., Laine, S., Aittala, M., Hellsten, J., Lehtinen, J., Aila, T.: StyleGANv2, Cvpr, pp. 8107–8116 (2020)
- 7. Hany, H.: Creating, using, misusing, and detecting deep fakes. J. Online Trust Safety **1**(4) (2022). <https://doi.org/10.54501/jots.v1i4.56>
- 8. Deng, J., Zhang, X., Chen, H., Wu, L.: BGT: a blind image quality evaluator via gradient and [texture statistical features. Sign. Process. Image Commun.](https://doi.org/10.1016/j.image.2021.116315) **96**, 116315 (2021). https://doi.org/ 10.1016/j.image.2021.116315
- 9. Li, H., Li, B., Tan, S., Huang, J.: Identification of deep network generated images using [disparities in color components. Sign. Process.](https://doi.org/10.1016/j.sigpro.2020.107616) **174**, 107616 (2020). https://doi.org/10.1016/ j.sigpro.2020.107616
- 10. Tang, G., Sun, L., Mao, X., Guo, S., Zhang, H., Wang, X.: Detection of GAN-synthesized [image based on discrete wavelet transform. Secur. Commun. Networks](https://doi.org/10.1155/2021/5511435) **2021**, 1 (2021). https:// doi.org/10.1155/2021/5511435
- 11. Agarwal, B.: 1209: RECENT ADVANCES ON SOCIAL MEDIA ANALYTICS AND MUL-TIMEDIA SYSTEMS : ISSUES AND CHALLENGES Financial sentiment analysis model utilizing knowledge-base and domain-specific representation, pp. 8899–8920 (2023)
- 12. Mi, Z., Jiang, X., Sun, T., Xu, K.: GAN-generated image detection with self-attention mechanism against GAN generator defect. IEEE J. Sel. Top. Signal Process. **14**(5), 969–981 (2020). <https://doi.org/10.1109/JSTSP.2020.2994523>
- 13. Yang, J., Xiao, S., Li, A., Lan, G., Wang, H.: Detecting fake images by identifying potential [texture difference. Futur. Gener. Comput. Syst.](https://doi.org/10.1016/j.future.2021.06.043) **125**, 127–135 (2021). https://doi.org/10.1016/ j.future.2021.06.043
- 14. Zhao, S., Zhang, M., Ding, H., Cui, X.: MFF-Net: deepfake detection network based on multi-feature fusion. Entropy **23**(12), 10–13 (2021). <https://doi.org/10.3390/e23121692>
- 15. Chen, B., Ju, X., Xiao, B., Ding, W., Zheng, Y., de Albuquerque, V.H.C.: Locally GANgenerated face detection based on an improved Xception. Inf. Sci. (Ny) **572**, 16–28 (2021). <https://doi.org/10.1016/j.ins.2021.05.006>
- 16. Hsu, C.-C., Zhuang, Y.-X., Lee, C.-Y.: Deep fake image detection based on pairwise learning. Appl. Sci. **10**(1), 370 (2020). <https://doi.org/10.3390/app10010370>
- 17. Wang, X., Guo, H., Hu, S., Chang, M.-C., Lyu, S.: GAN-generated Faces Detection: A Survey and New Perspectives (2022). <http://arxiv.org/abs/2202.07145>
- 18. Mirsky, Y., Lee, W.: The creation and detection of deepfakes: a survey. ACM Comput. Surv. **54**(1), 1–41 (2021). <https://doi.org/10.1145/3425780>
- 19. Verdoliva, L.: Media forensics and DeepFakes: an overview. IEEE J. Sel. Top. Signal Process. **14**(5), 910–932 (2020). <https://doi.org/10.1109/JSTSP.2020.3002101>
- 20. Tyagi, S., Yadav, D.: A detailed analysis of image and video forgery detection techniques. Vis. Comput. **39**(3), 813–833 (2023). <https://doi.org/10.1007/s00371-021-02347-4>
- 21. Gupta, P., Rajpoot, C.S., Shanthi, T.S., Prasad, D., Kumar, A., Kumar, S.S.: Image forgery detection using deep learning model. In: 3rd International Conference on Smart Electronics [and Communication ICOSEC 2022 - Proceedings, pp. 1256–1262 \(2022\).](https://doi.org/10.1109/ICOSEC54921.2022.9951952) https://doi.org/10. 1109/ICOSEC54921.2022.9951952
- 22. Huang, Y., Juefei-Xu, F., Guo, Q., Liu, Y., Pu, G.: FakeLocator: robust localization of GAN[based face manipulations. IEEE Trans. Inf. Forensics Secur.](https://doi.org/10.1109/TIFS.2022.3141262) **17**, 2657–2672 (2022). https:// doi.org/10.1109/TIFS.2022.3141262