

Robust GAN-Based CNN Model as Generative AI Application for Deepfake Detection

Preeti Sharma^{1,*}, Manoj Kumar^{2,3,4,5}, and Hitesh Kumar Sharma⁶

¹ School of Computer Science, University of Petroleum and Energy Studies (UPES), Dehradun, 248007 India.

² School of Computer Science, FEIS, University of Wollongong in Dubai, Dubai Knowledge Park, Dubai, UAE

³ Research Cluster Head, Network and Cyber Security, UOWD, Dubai

⁴ MEU Research Unit, Middle East University, Amman, 11831, Jordan

⁵ Research Fellow, INTI International University, Malaysia

⁶ School of Computer Science, University of Petroleum and Energy Studies (UPES), Dehradun, 248007 India.

Abstract

One of the most well-known generative AI models is the Generative Adversarial Network (GAN), which is frequently employed for data generation or augmentation. In this paper a reliable GAN-based CNN deepfake detection method utilizing GAN as an augmentation element is implemented. It aims to give the CNN model a big collection of images so that it can train better with the intrinsic qualities of the images. The major objective of this research is to show how GAN innovations have enhanced and increased the use of generative AI principles, particularly in fake image classification called Deepfakes that poses concerns about misrepresentation and individual privacy. For identifying these fake photos more synthetic images are created using the GAN model that closely resemble the training data. It has been observed that GAN-augmented datasets can improve the robustness and generality of CNN-based detection models, which correctly identify between real and false images by 96.35%.

Keywords: Deep Learning, Digital Forensics, Generative Adversarial Networks (GAN), Generative AI, CNN model, Deepfake

Received on 26 December 2023, accepted on 28 March 2024, published on 04 April 2024

Copyright © 2024 P. Sharma *et al.*, licensed to EAI. This is an open access article distributed under the terms of the [CC BY-NC-SA 4.0](https://creativecommons.org/licenses/by-nc-sa/4.0/), which permits copying, redistributing, remixing, transformation, and building upon the material in any medium so long as the original work is properly cited.

Doi: 10.4108/eetiot.5637

*Corresponding author. Email: preetiii.kashyup@gmail.com

1. Introduction

A subset of artificial intelligence known as "generative AI" can create new content, including computer code, graphics, music, writing, simulations, 3D objects, films, and more. Given its potential to revolutionize numerous industries, like entertainment, the arts, and design, it is seen as a crucial component of AI research and development. As a generative adversarial application, generative adversarial networks (GANs) are extensively employed in this field. They were first proposed by Goodfellow et al. [1] in 2014. As a result of the introduction of the family of generative models like GAN, more well-publicized examples such as systems to avoid facial recognition software or the fabrication of extraordinarily lifelike false images called Deepfakes have raised contradictory opinions from the public. Other recent applications include OpenAI-created ChatGPT, a language

model that effectively comprehends and reacts to inputs in human language. Another model created by OpenAI, called DALLE-2, can create original, high-quality images from textual descriptions [2].

GANs are a type of deep learning model that consists of two competitively trained neural networks, the generator, and the discriminator. The fundamental purpose of a GAN is to generate realistic data samples that mimic the training data, such as photos, videos, audio, or text. The generator network generates fresh samples out of random noise, whereas the discriminator network attempts to differentiate between genuine and produced data. Through adversarial training, the generator learns to enhance its output to mislead the discriminator, while the discriminator improves its ability to distinguish between real and fake. Image synthesis, video production, music composition, style transfer, data

augmentation, and other fields have found use for GANs as shown in Figure 1.

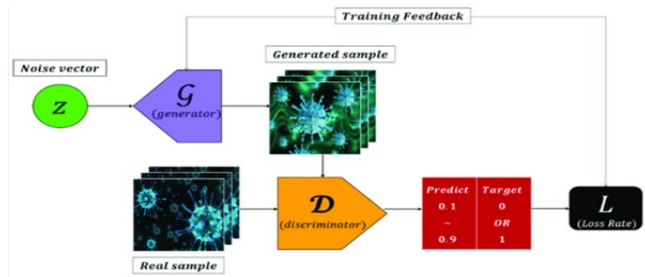


Figure 1: Working Principle of Base GAN Model [3].

The creation of the family of algorithms known as generative adversarial networks (GANs) has been one of the most significant advancements in DL synthesis. Compared to other algorithms in the deep generative model family, GANs have several advantages. Compared to other models, they deliver an output of superior quality. The images generated by GANs are typically much sharper and more realistic than those produced by variational autoencoder (VAE). Although auto-regressive models offer a straightforward and reliable training procedure, they are not particularly effective during sampling and cannot simply produce straightforward low-dimensional picture coding. GANs are a popular choice for generating tasks due to their adaptability, and their applications are expanding as research in the field improves. However, it is critical to use GANs properly and to examine any ethical consequences, particularly when it comes to deepfakes and fake media generation.

In this research, the usability of GAN models is extensively analysed in terms of their applicational worth as Generative AI in the field of deepfakes. The underlying goal of this research is to establish the advances of GANs as effective Generative AI tools that have improved and widened the scope of traditional Generative AI concepts. Its aim is to show how GAN advancements have improved and increased the use of traditional Generative AI principles, particularly in the field of fake image classification. The research emphasizes the comparative justification of Gan’s benefits as compared to its basic model as proposed by Goodfellow and other existing models.

Rest of paper is organised with subsequent sections. Sections 2 presented related research of the domain. Section 3 defines the proposed methodology including the details about the dataset and defined architecture. Section 4 demonstrates the experimental and results section. It demonstrates various result graphs showcasing the optimised values of accuracy and loss function curve. At the end, section 5 presents the conclusion of the research paper.

2. Related Work

GANs have proven to be quite effective in a variety of tasks, like the creation of unsupervised images. Compared to the traditional machine learning method, the GAN model is more functional and has more application possibilities. Furthermore, it outperforms established algorithms like ImageNet and CIFAR-100 in large data sets [4]. Generative adversarial networks (GANs) are frequently employed in the field of computer vision (CV), particularly for data augmentation. A tabular review of literature is given below in Table 1 organized to systematically present the significant features of generative AI and the approaches included in its implicit and explicit classifications; GAN models and its evolution; GAN as potential implicit generative AI model; Efficacy of Ensemble GAN models. A comprehensive study of the Generative AI techniques with potentialities of GAN (2018-2023) is shown in Table 1 below.

3. Methodology

The methodology of the proposed approach includes the use of a newly devised GAN model for augmentation tasks and a robust CNN model for deepfake detection. GAN is used to enhance the original dataset by producing synthetic pictures. This helps to diversify the dataset and provide more training examples for the CNN. The purpose of GANs is to create new, synthetic data that mimics some existing data distribution. It is a data augmentation approach that generates new data samples. GANs use random noise from a latent space and generate unique pictures that replicate the feature distribution of the original dataset. It generates never-before-seen data by learning the distribution of photos, allowing for data augmentation that is not confined to applying alternative modifications to existing images. The augmented dataset is then used to train a Convolutional Neural Network (CNN), a deep learning model well-suited for picture categorization applications. CNN learns to discriminate between real and phoney pictures using a diversified dataset. The trained CNN is used for deepfake detection. It can detect patterns and traits that are suggestive of deepfake manipulation, giving a reliable approach for distinguishing between authentic and fake pictures. The basic steps include:

1. Data Augmentation
2. Merging of GAN-created images (Augmented) with the original dataset.
3. Training of devised CNN model with created large new dataset.
4. Detection of Real and Fake images using the CNN model.

3.1. Data Augmentation

The GAN model is used to produce additional synthetic images for image recognition. GAN-augmented datasets can improve the generalization and robustness of image recognition models by creating different images that match

the training data. We applied the Noise Injection transformation technique to the original photos for the implementation of the augmentation process. In it, we add random noise to the original images to imitate real-world defects, resulting in a more diverse and varied dataset for training. This approach teaches the model to be more resistant to changes in the data, making it more robust and capable of generalizing to previously unknown images. As this procedure is often performed in real-time during training, each batch of photos input to the model is slightly

different. This random variation during training helps the model learn to tolerate variations and improves its ability to categorize fresh, unseen images correctly. In this way, data augmentation prevents overfitting and leads to more reliable and accurate image classifiers, making the model more resilient and capable of generalizing to unseen images. The architecture of the proposed detection model is shown in Figure 2 below.

Table 1. Comprehensive study of the Generative AI techniques with potentialities of GAN (2018-2023).

Year	Author	Research Approach	Technique	Application	Dataset	Experimental Result	Outcome and Future scope
2018	Lala et al.[5]	Evaluation and correction of GAN model training issues.	Ada GAN, VEEGAN, Wasserstein GAN, and Unrolled GAN	Image generation	Synthetic and Real Data (MNIST)	Ada GAN performed better than other GANs.	One evaluation measure metric was not considered sufficient to quantify mode collapse for GANs as the metrics do not give, consistent results.
2018	Lucic et al. [6]	An empirical study on evaluation measures of GAN models	MMGAN and WGAN were evaluated by using precision and recall	Image synthesis.	MNIST, CIFAR10, CELEBA	FID was found effective for mode evaluation for its robustness efficacy tests in terms of mode dropping and encoding network choices.	Budget constraints could be rectified by improving the evaluation.
2019	Groenendijk et al.[7]	Adversarial training to the task of monocular depth estimation	Vanilla GAN; LSGAN; Wasserstein GANs	Image Generation.	KITTI; Cityscapes	The research concluded that adversarial training is beneficial if and only if the reconstruction loss is not too constrained	Further development could be on state-of-the-art monocular depth estimation results, by using batch normalization and different output scales.
2019	Verbeek et al. [8]	Popular Generative Ais, such as, Generative adversarial networks. Variational autoencoder.	CNN, RNN; Image partitioning and multiple layer transformation	(CNN)Object detection, semantic segmentation, image caption, and pose estimation.	ImageNet; LSUN bedroom; CalebA; CIFAR 10	The model varied based on the latent dimension and pixel-wise detections.	Training strategies needed to be model-specific and optimized according to applications to be assessed as future scope.
2020	Kokate et al. [9]	Empirical Comparison of GANs.	FID and IS evaluation on GAN (NS-GAN and LS-GAN) and comparison done	Multiple generative efficacies were evaluated	Public Databases	The result found FID and IS as the best metrics to evaluate generated data distribution.	More evaluation of LS-GAN on the generation of data.
2021	Hughes et al.[10]	Human AI	Business-segment-	Business-specific	Standard business-	GAN applications in developing creative	Powerful tools were emerging in GAN-

		applicatio n efficacies of GANs in creative design industries	based GAN models were reviewed.	applicatio n specific datasets	specific datasets	toolboxes were found to be at their evolving stage.	based Human AI applications, such as sketch tools and others.
2021	Ruhotto et al.[11]	Deep Generati ve Modelling	Normalizing flows, Variational Autoencoder s, and Generative adversarial networks.	Image generation; Movies and Voice enhanceme nts; Deepfakes.	Public Database	Database-specific model efficacy was evaluated mathematically	The experiment provided scope and expansion areas on generative modelling and its ways of optimization.
2022	Liu et al. [12]	Evolution ary computat ion- based GAN.	EvoGAN by using Facial Action Coding System (FACS) to encode evolutionary algorithm.	Image synthesis.	Public Dataset	A good variety of images with facial expressions could be generated through EvoGAN.	The model is feasible for practical application.
2022	Chen et al. [13]	Variation al Autoenco der to improve generate d ineffectiv e images	The model with the combination of GAN and VAE.	Image correction.	Standard Dataset	The model was found to be better in utilizing resources and produce the desired result.	Extension of the model in image reconstruction could be attempted.
2022	Peters et al. [14]	An empirical comparis on of GANs and VAEs.	DCGAN and CVAE were developed for image synthesis.	Image synthesis	Fashion- MNIST dataset	DCGAN was found better than CVAE in terms of the chosen application.	DCGAN shown variable FID score while CVAE was consistent and so could be further evaluated for enhancements.
2023	Su et al. [15]	Chat GPT Evaluatio n.	A theoretical framework called IDEE on educative AI, such as ChatGPT.	Human-like texts	Text datasets available on the internet	Personalized education facilities for students, fast, quick teacher feedback generation.	Model performance was not evaluated, quality was unchecked, and ethical and safety issues were to be evaluated

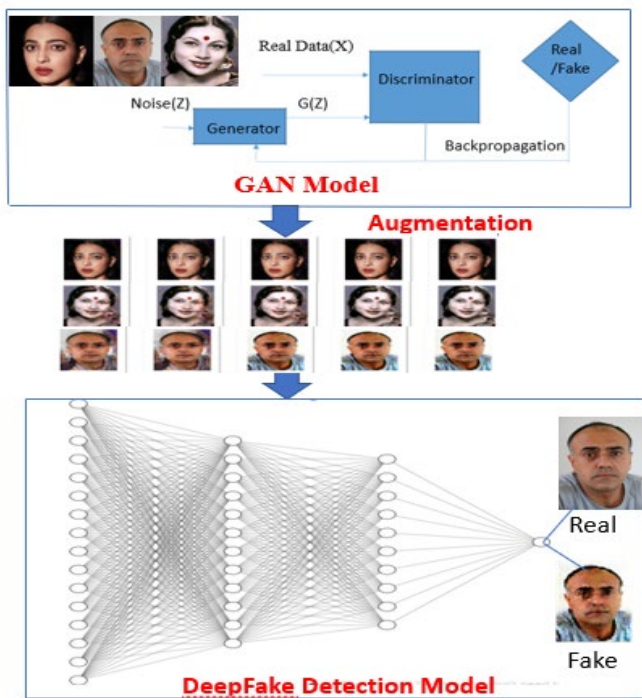


Figure 2: Architecture of the proposed Deepfake Detection Model.

3.2 Dataset

Indian Actor Images Dataset is used for training and testing the model. This collection contains 6750 photos of Indian actors (male and female), grouped into 135 unique categories or groupings. Ajay Devgan, Akshay Kumar, Amitabh Bachchan, Amjad Khan, Amol Palekar, Amrish Puri, Anil Kapoor, and others are among the Indian superstars whose images have been utilized. The dataset was created via Google Images. These datasets contain big-scale and heterogeneous facial picture information that has been pre-processed with the necessary improvements to optimize model training and acquire improved accuracy with the least amount of time consumption. The data set [16] can be downloaded: <https://www.kaggle.com/datasets/iamsouravbanerjee/indian-actor-images-dataset>.

3.3 Deepfake Detection Using CNN Model

The architecture of the proposed Convolutional Neural Network (CNN) is designed with weights 16,12,10,1 in subsequent layers used for deepfake detection. CNN's weights and architecture correctly characterise its performance [17]. It learns and discovers features that discriminate between real and fake images. The CNN architecture is often made up of several layers, each with its own set of learnable weights. The weights are applied to the incoming data to convolve it, extracting essential features, and finding patterns. The output of the last layer is utilized to determine if the input is authentic or fraudulent.

1. Input Layer: The raw image data is delivered into the network through the input layer. The size of the input would be determined by the resolution of the photographs used for deepfake detection.

2. Convolutional Layers (with a total of 16 filters):

The first convolutional layer is made up of 16 filters (sometimes referred to as kernels). Each filter is applied to the input image and extracts certain features. During the training phase, the weights associated with these filters are learned.

3. Pooling Layer: A pooling layer is often added after each convolutional layer to minimise the spatial dimensions of the feature maps while retaining critical information. A frequent pooling technique is max pooling, which takes the maximum value inside a given region of the feature map.

4. Convolutional Layers (with 12 Filters): The second convolutional layer has 12 filters that convolve over the previous layer's pooled feature maps, extracting higher-level features.

5. Pooling Layer: To minimize the spatial dimensionality, a pooling layer is added after the second convolutional layer.

6. Convolutional Layers (with 10 Filters): The third convolutional layer contains 10 filters that convolve over the preceding layer's pooling feature maps, extracting more abstract information.

Layer of Collection:

7. Add another layer of pooling to minimize the spatial dimensions.

8. Fully Connected Layer (with 1 Neuron): The remaining feature maps are flattened and processed through a fully connected layer with a single neuron after multiple convolutional and pooling layers. This layer functions as a binary classifier, returning a value between 0 and 1, with 0 indicating a genuine image and 1 indicating a false image.

9. Output Layer: The output layer applies a suitable activation function (e.g., sigmoid) to the fully connected layer's output, mapping the value to the range [0, 1], allowing it to be interpreted as the likelihood of the input being real or fake.

3.4 Algorithm

Algorithm: Robust Deepfake Detection

Step 1: Gathering Data

- Collect an "Indian Actor Images Dataset" with real photos and associated labels (0 for real, 1 for fraudulent). Let $D(\text{real})$ represent the dataset. Train the defined Generative Adversarial Network (GAN) model with $D(\text{real})$. The GAN generates fictitious images, and the resulting dataset is designated by $D(\text{fake})$.

Step 2: Addition of Augmented Images

- Adding the D-Fake with $D(\text{real})$ dataset to create a large dataset for CNN model for better fake detection.

Step 3: CNN Architecture

- Define the CNN architecture by specifying the appropriate hyperparameters (number of filters,

kernel sizes, pooling layers, and so on). In this example, we will employ the previously specified architecture with weights 16, 12, 10, and 1.

Step 4: Deepfake Detection Model Training

- Create a CNN model with random weights. Let W_l represent the CNN weights, where l is the layer.
- Train the CNN model by following these steps:
For each epoch:
 - Iterate over the real ($D(\text{real})$) and GAN-generated ($D(\text{fake})$) image datasets.
 - Let l denote the batch index for each batch of real and GAN-generated photos.
 - Run the CNN model on the l batch of actual images and compute the output probability $P(\text{real})_l$ for each image in the batch. The anticipated probability for the image in the j batch is represented by $P(\text{real})_l(j)$.
 - Run the CNN model on the l batch of GAN-generated images, then calculate the output probability $P(\text{fake})_l$ for each image in the batch. The projected probability for the j image in the l batch is represented by $P(\text{fake})_l(j)$.
 - For each real image in the l batch, compute the binary cross-entropy loss $L(\text{real})_l(j)$ between the predicted probability $P(\text{real})_l(j)$ and the matching ground truth label $Y(\text{real})_l(j)$.
 - For each GAN-generated image in the l batch, compute the binary cross-entropy loss $L(\text{fake})_l(j)$ between the predicted probability $P(\text{fake})_l(j)$ and the accompanying ground truth label $Y(\text{fake})_l(j)$.
 - To compute the gradients, backpropagate the total loss $L(\text{total})_l(j) = L(\text{real})_l(j) + L(\text{fake})_l(j)$ through the CNN model.
 - Update the CNN model's weights with an optimisation technique called stochastic gradient descent (SGD). Let η be the learning rate.

Step 5: Testing

- After training, run the CNN model on a separate test dataset that includes both genuine and false images. Let $D(\text{test})$ represent the test dataset.
- Let l denote the index of the test image in the dataset for each test image.
- Calculate the output probability $P(\text{test})_l$ by running the l test picture through the trained CNN model. The projected probability for the j test picture is represented by $P(\text{test})_l(j)$.
- $P(\text{test})_l(j)$ output probability compared to a preset threshold (e.g., 0.5). If $P(\text{test})_l(j) > 0.5$, the image is real (label 0); else, it is fake (label 1).

Step 6: Performance Assessment

- Using the test dataset $D(\text{test})$, compute performance metrics accuracy, precision, recall, and F1 score to evaluate the model's performance in detecting deepfake images.

4. Results and Discussion

The results are based on the loss and accuracy numbers for each epoch of the model's training procedure. Loss is a metric that measures how well the model performs during training. It indicates the difference between predicted and actual ground truth labels. The purpose of deep learning is to minimise the loss function. The loss should ideally decrease as the training goes, showing that the model is learning to generate more accurate predictions. The percentage of correctly categorised samples in the overall dataset is measured by accuracy. A higher accuracy means that the model predicts more correctly. However, when working with imbalanced datasets, it is critical to interpret accuracy in conjunction with other performance indicators. The different tendencies in the loss and accuracy values in our case are shown in table 2.

As shown in Figure 3, in the early epochs (e.g., 10), the loss is rather large (4.3714), showing that the model's performance is not yet optimal. The loss diminishes with time as training progresses (e.g., 1.965 at epoch 30, 1.1657 at epoch 60, and 0.1035 at epoch 100).

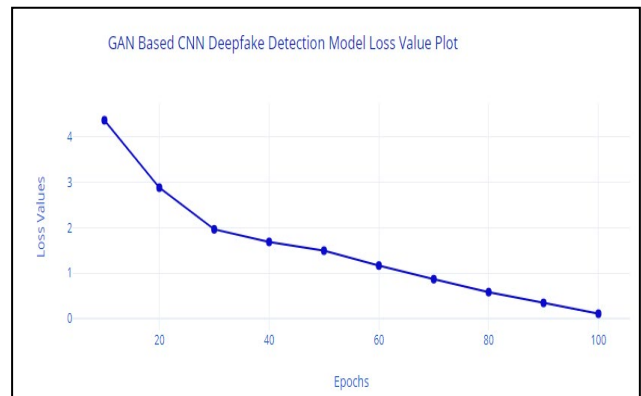


Figure 3: Loss Value Plot of GAN Based CNN Deepfake Detection Model.

This diminishing trend is a good indication as it indicates that the model is learning and improving its predictions.

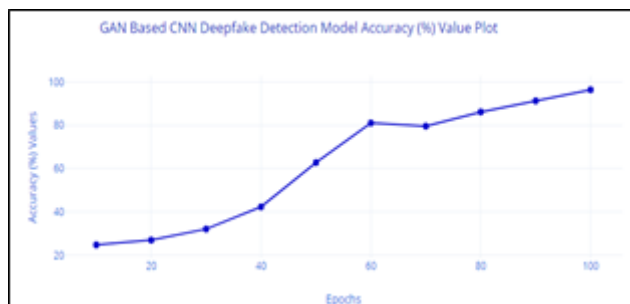


Figure 4: Accuracy Value (%) Plot of GAN Based CNN Deepfake Detection Model.

Similarly, in accuracy case as shown in Figure 4, the accuracy begins at a rather low value (24.82%) in the first epochs (e.g., 10) of training, showing that the model is not performing well at the start. It improves with time as training advances (e.g., 32.12% at epoch 30, 81.02% at epoch 60, and 96.35% at epoch 100). This rising accuracy trend is encouraging, indicating that the model is learning to identify data more accurately.

Table 2. shows the different tendencies in the loss and accuracy values in our case.

Epoch	Loss	Accuracy
10	4.3714	24.82
20	2.8845	27.01
30	1.965	32.12
40	1.6878	42.34
50	1.4939	62.77
60	1.1657	81.02
70	0.8653	79.56
80	0.5801	86.13
90	0.3418	91.24
100	0.1035	96.35

So, based on these provided performance metrics, it appears that the CNN Deepfake detection model is improving over time as shown in Figure 5. The loss is consistently decreasing, which means the model is learning to make better predictions. Additionally, the accuracy is increasing, indicating that the model is becoming more proficient at distinguishing between real and fake images.

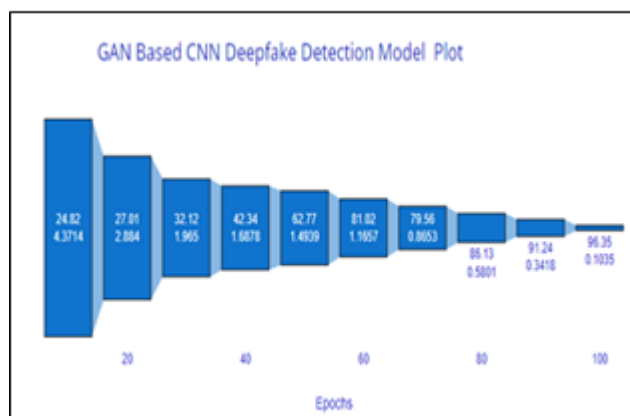


Figure 5: Deepfake Detection Plot of GAN Based CNN Model.

When compared to other deepfake detection methods shown in Table 3, our suggested model, which used the Indian Actor Images Dataset and a GAN-based CNN technique, achieved the greatest accuracy (96.35%).

As it can be viewed in Figure 5 that Marra et al. [18] achieved an accuracy of 95.07% using their own dataset created with Cycle GAN and a CNN model. With the Face Forensics++ dataset and a CNN model, Afchar et al. [19] achieved an accuracy of 94.05%. Finally, Zhou et al. [20] attained an accuracy of 92.90% using the Face Forensics++ dataset.

Thus, in our suggested model, the CNN strategy based on GAN-generated data augmentation performed well, surpassing alternative methods that relied on various datasets or variants of CNN models.

Table 3. Comparison of the GAN-based CNN deepfake detection model with Existing models.

Author	Dataset	Detection Model	Accuracy
Ours	Indian Actor Images Dataset	GAN Based CNN	96.35%
Marra et al.[18]	Own dataset (Cycle GAN)	CNN	95.07%
Afchar et al.[19]	Face Forensics++	CNN	94.05%
Zhou et al.[20]	Face Forensics++	CNN	92.90%

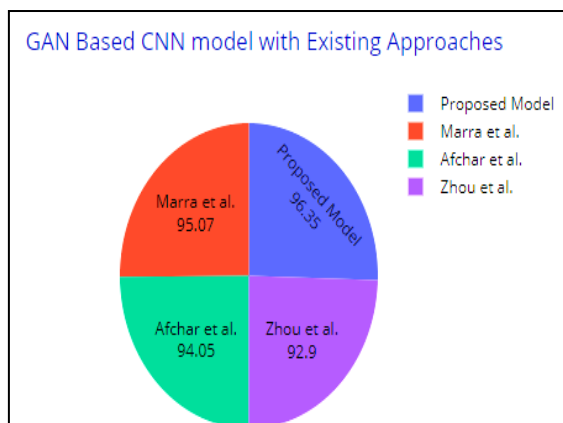


Figure 6: Comparative Study Plot of the GAN Based CNN Model with Existing Models.

Additionally, it's crucial to evaluate the model's performance on a few different difficult datasets to guarantee the model's robustness and generalizability to several deepfake scenarios and real-world applications.

5. Conclusion

The proposed GAN-based CNN deepfake detection approach is proved a promising technique for identifying deepfake images. The model successfully differentiates between real and fake images by using the strength of convolutional neural networks (CNNs) to learn important features from real and GAN-generated images. Large datasets, including the augmented dataset produced by the GAN model, are useful to train the model. Through backpropagation and optimisation techniques like stochastic gradient descent (SGD), loss is seen to be minimised to 0.1035. Also, it is observed that proposed model achieved the highest accuracy of 96.35% compared to other studies using different datasets and CNN models ensuring its better detection quality. Additionally, to ensure the model's robustness and generalizability to multiple deepfake scenarios, it essential to validate the model's performance on a variety of other challenging datasets. Furthermore, the deepfake detection algorithm is continually being improved to combat new threats rising in synthetic media.

References

- [1] I. Goodfellow et al. (2020), "Generative adversarial networks," *Commun. ACM*, vol. 63, no. 11, pp. 139–144, Doi: 10.1145/3422622.
- [2] Islam. A. (2023). A Hist. Gener. AI From gan to GPT-4. Mark Tech Post. <https://www.marktechpost.com/2023/03/21/a-history-of-generative-ai-from-gan-to-gpt-4/>.
- [3] Park. S.-W., Ko, J.-S., Huh, J.-H., Kim, J.-C. (2021). Rev. Gener. Adverse. Networks Focus. *Comput. Vis. its Appl. Electron.* 10(10), 1216. <https://doi.org/10.3390/electronics10101216>.
- [4] Jin, L., Tan, F., Jiang, S. (2020). Gener. Adverse. Network. *Technol. Appl. Comput. vision. Comput. In tell. Neurosis.* 2020, 1–17. <https://doi.org/10.1155/2020/1459107>.
- [5] Lala, S., Shady, M., Belyaeva, A., Liu, M. (2018). Eval. Mode Collapse Gener. Adverse. Networks. *IEEE*.
- [6] Lucic, M., Kurach, K., Michalski, M., Bousquet, O., Gelly, S. (2018). Are GANs Create. Equal. A Large-Scale Study. <https://proceedings.neurips.cc/paper/2018/file/e46de7e1bcaaced9a54f1e9d0d2f800d-Paper.pdf>.
- [7] Groenendijk, R., Karaoglu, S., Gevers, T., Mensink, T. (2020). benefit Adverse. Train. monocular depth Estim. *Comput. Vis. Image Understanding*, 190, 102848. <https://doi.org/10.1016/j.cviu.2019.102848>.
- [8] Verbeek, J. (2019). Deep Gener. Model. INRIA.
- [9] Kokate, P., Joshi, A. D., Tamizharasan, P. S. (2020). An Empir. Comp. Gener. Adverse. Network. *Meas. Lect. Notes Electr. Eng.* 1383–1396. https://doi.org/10.1007/978-981-15-5341-7_105.
- [10] Hughes, R. T., Zhu, L., Bednarz, T. (2021). Gener. Adverse. networks-enabled human-artificial in tell. *Collab. Appl. Create. Des. Ind. A Syst. Rev. Curr. approaches Trends. Front. Artificial*
- [11] Ruhotto, L., Haber, E. (2021). An Introduction to Deep Gener. Model. *GAMM-Mitteilungen*, 44(2). <https://doi.org/10.1002/gamm.202100008>.
- [12] Liu, F., Wang, H., Zhang, J., Fu, Z., Zhou, A., Qi, J., Li, Z. (2022). EvoGAN An Evo. Comput. Assist. gan. *Neurocomputing*, 469, 81–90. <https://doi.org/10.1016/j.neucom.2021.10.060>.
- [13] Chen, J., Song, W. (2022). GAN_VAE Elev. Gener. ineffective image through Var. autoencoder. 2022 5th Int. Conf. Pattern Recognit. Artif. Intell. (PRAI). <https://doi.org/10.1109/prai55851.2022.9904067>.
- [14] Peters, H., Celis, N. C. (2022). An Empir. Comp. Gener. Capab. GAN vs VAE. *KTH R. Inst. Technol.*
- [15] Su (苏嘉红), J., Yang (杨伟鹏), W. (2023). Unlocking power ChatGPT a Framew. Appl. Gener. AI Educ. *ECNU Rev. Educ.* 209653112311684. <https://doi.org/10.1177/20965311231168423>.
- [16] <https://www.kaggle.com/datasets/iamsouravbanerjee/indian-actor-images-dataset>.
- [17] Prasad Koyyada, S., & Singh, T. P. (2023). An explainable artificial intelligence model for identifying local indicators and detecting lung disease from chest X-ray images. *Healthcare Analytics*, 100206.
- [18] F. Marra, D. Gragnaniello, D. Cozzolino, L. Verdoliva, "Detection GAN-generated fake images over Soc. networks," *Proc. IEEE Conf. Multimed. Inf. Process. Retrieval*, 2018, pp. 384–389.
- [19] Afchar, D., Nozick, V., Yamagishi, J., Echizen, I. (2018). MesoNet A Compact facial video Forg. Detect. network. *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Work.* 2122–2131. <https://openaccess.thecvf.com/co>.
- [20] Zhou, W., Huang, Y., Wang, W., Wang, W., Tan, T. (2020). Learn. to Detect fake face videos wild. *Proc. IEEE Conf. Comput. Vis. Pattern Recognition*, 5205–5214. https://openaccess.thecvf.com/content_CVPR_2020/papers.