Deep Residual Learning based Discriminator for Identifying Deepfakes with Cut-Out Regularization

Sai Dheeraj Gummadi
Dept. Electronics and Communication Engineering
SRM University-AP
India
gummadi_sai@srmap.edu.in

Anirban Ghosh
Dept. Electronics and Communication Engineering
SRM University-AP
India
anirban.g@srmap.edu.in

2022 IEEE World Conference on Applied Intelligence and Computing (AIC) | 978-1-6654-7988-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/AIC55036.2022.9848964

***Abstract*—The recent development of Generative Adversarial Networks (GANs) have greatly eased the generation of deepfake images which are indistinguishable from real images. As a downside of such advancement, it is now easy to impersonate a person leading to identity theft and other malicious outcomes. In such a scenario it becomes imperative to have a robust algorithm in place which can segregate real images from the fake ones. In this study, we suggest a residual connection based convolutional neural network (CNN) architecture for detecting deepfake images and compare the results with the existing transfer learning algorithms for identifying the deepfakes. The data set used in this study is the combination of the Flickr-Faces-HQ (FFHQ) data set (Nvidia) and the deepfakes generated by the Style GAN, which is proposed by Nvidia. The data set consisting of 1,20,000 images is used for training and validating the network, while a separate set of 20,000 real world images are used for testing the performance of the model. In this current work, we test the robustness of three different algorithms - Inception Resnet V2, VGGFace2, and our customized Residual CNN with and without cut-out regularization in identifying real images. The residual architecture-based implementation in combination with cut-out architecture produces the lowest false positives rate at 0.0043% while the Inception Resnet V2 in combination with cut - regularization produces the best accuracy at 99.05%.**

Keywords—Residual Learning, Convolutional Neural Networks, Deepfakes, Transfer Learning, Cut-Out Regularization.

I. INTRODUCTION

The creation of deep fakes has become very easy due to the recent development of different types of GANs. The architecture of the GAN has been divided into two parts: (i) Generator and (ii) Discriminator where the generator generates the fake faces based on the pixels distribution of the real faces dataset and the discriminator distinguishes the images created by the generator into fake and real images. This process iterates till the discriminator fails to distinguish the fake image from the real image. So, the quality of the discriminator decides the quality of the deepfakes. DeepFake technology allows anyone with a computer and internet to make realistic images and videos of anything and everything. According to [1] published in 'The Hindu' the deepfake content on the internet has been growing year on year.

In the six months between January 2020 to June 2020, it has more than doubled from 24, 263 to 49, 081. To add to the menace as reported by deep trace labs since July 2019, 95% of the deep fake content has mimicked people in film, fashion, and sports industries. As the rate of synthetic data generation increases exponentially it is not hard to find a reason to be apprehensive of its consequences. To cite an example, as per recent reports [2], scammers have cloned the voice of bank directors embezzling money worth 35 million dollars. Privacy is another primary concern, where unsolicited usage of images or videos readily available from various social media platforms might lead to malicious usage of one's identity or even identity theft

However, just like the two faces of a coin, there are some advantages of using deep fakes. To cite an instance [3], Warner Brothers spent around 3 million dollars for just removing Henry Cavill's mustache using Computer Generated Imagery(CGI) in the Justice League. The same job could have been done inexpensively using deepfakes without significant loss in quality

Deepfakes can also help in creating huge volumes of synthetic medical data, which can help researchers to develop new methodologies for diagnosing diseases without being dependent on the original patient data which are scarcely available. In [4], the authors stated a significant improvement in performance by training the deep learning model with synthetic data in addition to 10% real data. In addition, deepfakes can significantly enhance the learning experience of students by creating synthetic interactive videos of historical figures at a low cost. Despite the above mentioned advantages of the technology there needs to be some mechanism to discriminate the real from the fake to address unscrupulous usage of the same. The current work is an attempt to design such a discriminator.

The flow of this paper is as follows- Section II provides a gist of the related previous works, the implementation of the proposed methods is described in Section III. The results of the proposed work and its analysis are given in Section IV and Section V concludes the study.

II. RELATED WORKS

Deep fakes were relatively a new topic, yet some works have been done previously. In the initial days, deep fakes are detected based on the human eye due to pixelation during the blinking of the eye. HS Shad et al [5] used the FFHQ data set [6] collected by Nvidia corporation and presented the results of distinguishing between real and fake images using VGG-16, VGG-19, Resnet-50, Densenet-121, Densenet-169,

978-1-6654-7988-2/22/$31.00 ©2022 IEEE
DOI: 10.1109/aic.2022.26

Authorized licensed use limited to: VIT University- Chennai Campus. Downloaded on February 28,2024 at 18:20:47 UTC from IEEE Xplore. Restrictions apply.

Densenet-201 transfer learning models. The paper reported a highest accuracy of 97% using Resnet- 50 as well as Densenet-121 with 176 and 497 false positives respectively. In [5] authors proposed a CNN-based architecture and obtained 90% accuracy with 168 false positives. D Gong et al [7] extracted the fake and real images by cropping faces from videos. In this work, the authors proposed a new CNN-based architecture named Deepfake Net for classifying images into real and fake and obtained an accuracy of 96.69%. The performance of the proposed algorithm was further compared with that of VGG-19, Google Net, Xception Net, Resnet 101, and ResNeXt 50 under the optimized hyperparameters of the proposed algorithm and was found to perform better compared to the standard algorithms. S.R.A. Ahmed et al [8] on the other hand used a rationale-augmented convolutional neural network to classify images obtained from the Kaggle deep fake video data set with an accuracy of 95.77%. The architecture that was used by [8] has 3 convolution layers for extracting the features from images and the features are given to the rationale augmented CNN model for classifying them into real and fake. R Rafique et al [9] presented a highest accuracy of 88.2% using an image compression technique along with Error level Analysis (ELA). The technique however is not general and works only with lossy images in jpeg format. The images were compressed by 85% and features of images were extracted using Alexnet which is a CNN-based transfer learning model and the Shuffle Net which is designed for mobile devices with fewer computations. The extracted features were fed into SVM and KNN algorithms for classifying the real and fake images. A. Choudhary et al [10] proposed the Imagefake model which is a transfer learning based ensemble model where authors concatenated VGG-16, VGG-19, Inception V3, Squeeze net, Resnet-101 and presented an accuracy of 66% on testing data for classifying fake and real images where the training accuracy was 97%, as a result, there is a high probability of overfitting of the model. K. Chandani et al [11] presented an accuracy of 76.79% using the ResNet-152 transfer learning model with a data set of 2041 images obtained from the computational intelligence and photography lab.

S.Agarwal et al [12] on the other hand used a data set of size 320, which was generated using StyleGAN2 and CycleGAN, and proposed a capsule network for classifying fake images from real images with an accuracy of 98.4% on the CycleGAN dataset and 98.1% accuracy on StyleGAN2 dataset. In [13] Hady A. Khalil et al created the deep fake data with around 5000 images using Mesonet. As the quality of the deep fake images was very low, they have used DFDnet for improving the quality of the fake image and were able to classify the deep fake images and real images with an 80% confidence score. According to Y.Li et al [14], deep fake videos have fewer eye blinks compared to the real videos. In this work, the authors extracted features like face regions and eye areas with 6 eye landmarks. The extracted features were given to a long term recurrent convolutional neural network (LRCN). In [15] the authors used the bag of words technique to convert images into histograms of descriptors belonging to each word and classical machine learning classifier models (SVM and Random Forest) to train on various features. This implementation produced a highest accuracy of 93.55% and a precision of 93.42% using Multilayer perceptron. In [16], N. S. Ivanov et al used a data set containing 49 deepfake videos and 49 real videos and divided the process into 4 blocks. Initially, the image was passed through a face recognition module that estimates the 68 facial landmarks, then the images were passed to the super resolution block for improving the quality of the images. The processed images were then fed to the Resnet- 50 or SVM classifiers, the output of which is given to the decision maker, which announces the final judgment. This proposed model produced a maximum accuracy of 94.9% with Resnet-50. B. Malolan et al [17] obtained an accuracy of 94.33% by cropping faces from images and extracting 68 facial landmarks using dlib. The extracted features are then given to the Xception model consisting of 134 layers for segregating the deepfake images from the real images.

In contrast to the above mentioned works, the novelty of this study can be summarised as follows:

- The proposed work improves on the existing classification accuracy of real images from fake images using CNN-based transfer learning models with Cut out regularization.
- This study compares the performances of two transfer learning architectures: Inception Resnet-V2 [18], VGGFace2 [19], and our custom residual learning based architecture with and without Cut-Out regularization [20].
- The custom residual learning based model (Resnet-68) is interfaced with a newly developed web service [21] to spread the benefits of this work for common usage.

III. METHODOLOGY

In this section, we provide a detailed description of the proposed implementation. The dataset used for testing and validating the proposed method is described at the beginning of the section followed by an elaboration on the data preprocessing and the training phase. The functioning of the proposed deep learning based web-app is presented at the end of this section. The flow of the process is shown in fig. 1.

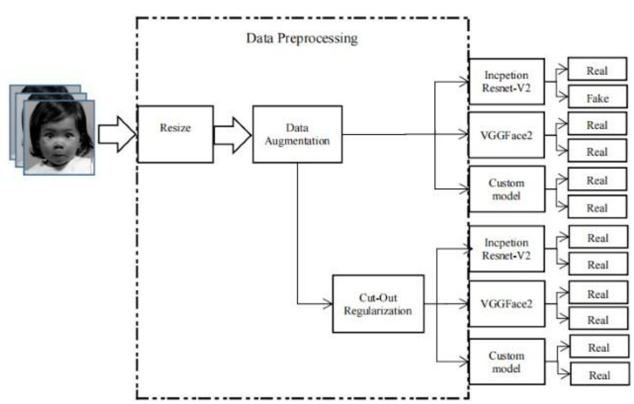


Fig. 1. Workflow of the proposed method

Authorized licensed use limited to: VIT University- Chennai Campus. Downloaded on February 28,2024 at 18:20:47 UTC from IEEE Xplore. Restrictions apply.

A. Data

The data used in this study has been gathered from Kaggle [6], where the dataset contains 1,40,000 images segregated into 70,000 real images obtained from the FFHQ dataset open-sourced by Nvidia as the benchmark for GANs and 70,000 Deepfake images created using Style based GANs by Nvidia [22]. The data set is divided into three categories - training, validation, and testing as shown in Table I. Fig. 2 show some samples of real and deepfake images from the dataset which as can be seen are hardly distinguishable.

TABLE I. OVERVIEW OF THE DATASET

Data	***Real Images***	***Deepfakes***
Data set	70,000	70,000
Training data	50,000	50,000
Validation data	10,000	10,000
Testing data	10,000	10,000

Fig. 2. Examples of Real and Deepfake Images from [6]

B. Data Pre-processing

Since the images in the dataset do not have a uniform size so they are resized into 224x224x3 for VGGFace2 [19] and our custom architecture and 299x299x3 for Inception Resnet-V2 [18] to maintain consistency in size. The resizing of images is followed by data augmentation and an optional cut-out regularization. Cut-Out regularization [20] randomly creates a patch on the images by assigning zeros to pixels. This helps in generalizing the model and in emulating real world distortion of images. Fig.3 illustrates the effect of cut-out regularization in preprocessed images from the dataset.

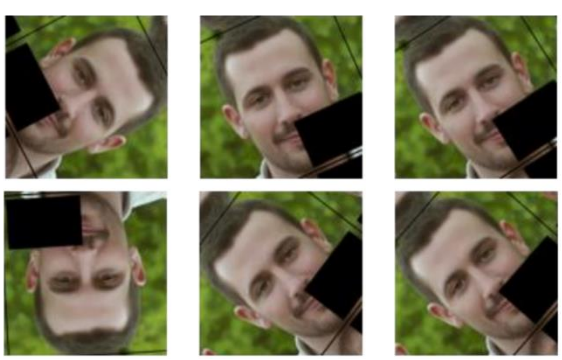


Fig. 3. Examples of the preprocessed data with cut-out

C. Inception Resnet-V2

Inception Resnet-V2 belongs to the Inception family of architectures. In this variation, residual connections replace the filter concatenation stage in the Inception network. One can have shortcuts in the model through residual connections, which helps in training a deeper neural network.

D. VGG Face-2

VGGFace2 is an advancement of the VGG Face architecture, which uses Resnet-50/Senet-50 as its backbone. VGGFace2 uses Multitask Cascade Neural Network (MTCNN) [23] for detecting the faces and calculates the face embedding, which is a vector representation of the features extracted from a face. It finds the dissimilarity between two facial images by calculating the Euclidean and Cosine distance between the feature vectors of the respective images. In addition to the feature vectors, the Resnet-50/Senet-50 models are further trained for classifying any image.

E. Custom Architecture (Resnet-68)

Our custom residual architecture has 68 layers with skip connections. The model takes as input images of size 224x224x3. The architecture of our custom residual model has been shown in fig.4. The identity block and convolution block have 3 convolution layers each with kernel shapes of (1,1), (3,3), and (1,1). We are proposing the new architecture based on the number of false positives predicted by the model. The metric can be chosen based on the use case, in this case, we are trying to reduce the errors in detecting false positives.

F. Training Phase

As mentioned earlier, the data has been divided into three parts, where 1,00,000 images are used as training data for training each model, 20,000 images are used as validation data for tuning the model, and 20,000 images are used as testing data for evaluating the performance of the model on unseen data. The optimized hyperparameters adopted for training the respective models are given in Table. II. CNN based transfer learning architectures: Inception Resnet-V2 and VGGFace2 along with our custom architecture are initially trained separately using the training set. Since the transfer learning models already have optimized weights, so we have trained them for 10 epochs, whereas our custom architecture which needs

Authorized licensed use limited to: VIT University- Chennai Campus. Downloaded on February 28,2024 at 18:20:47 UTC from IEEE Xplore. Restrictions apply.

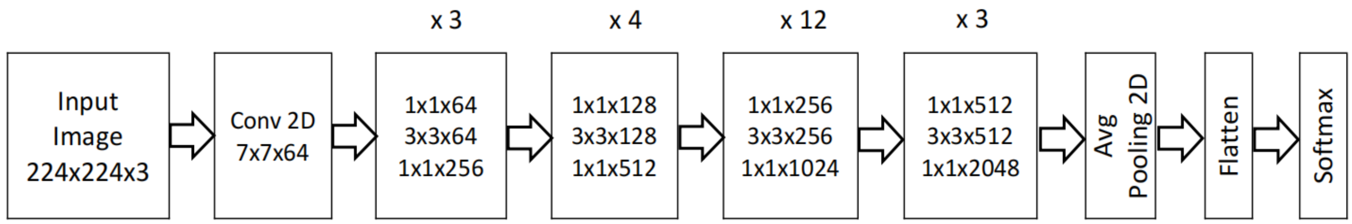


Fig. 4. Custom Architecture (Resnet-68)

training from scratch has been trained over 100 epochs with a batch size of 1000. The checkpoint method has been utilized while training the model for saving the model at its best trained weights.

TABLE II. OPTIMIZED HYPERPARAMETERS

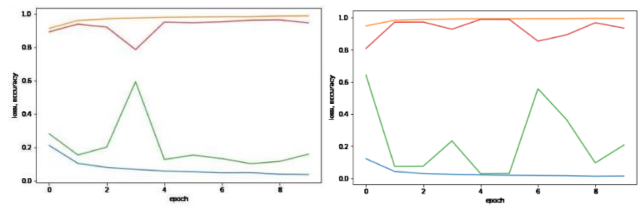
Hyperparameters	***Inception Resnet-V2***	***+ Cut Out***
Learning Rate	0.001	0.0001
Optimizer	Adam	Adam
Cost Function	Binary Cross Entropy	Binary Cross Entropy
Epoch	10	10
	VGG Face-2	***+ Cut Out***
Learning Rate	0.0002	0.0001
Optimizer	Adam	Adam
Cost Function	Binary Cross Entropy	Binary Cross Entropy
Epoch	10	10
	Custom Arch (Resnet-68)	***+ Cut Out***
Learning Rate	0.0001	0.0001
Optimizer	Adam	Adam
Cost Function	Binary Cross Entropy	Binary Cross Entropy
Epoch	100	10

G. *Web Application*

Since deepfake content is increasing on the internet, we intend to make the algorithm accessible to common people and reduce the adverse impact of synthetic images. To fulfill our endeavour we have developed a website [21] with HTML, CSS, and Java Script where the end user only needs to upload a picture or an image taken from a video to the application. All the necessary preprocessing and computation runs in the background of the application which displays the result of an input image being classified as real or fake along with the accuracy of the prediction.

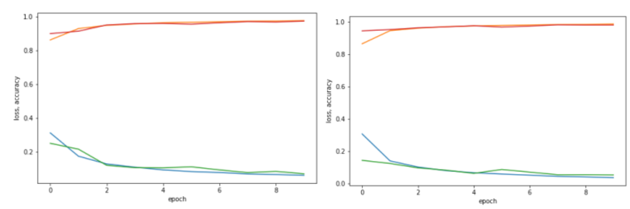
IV. RESULTS

In this section, the performance of the proposed algorithms is presented and analysed. We also present some sample outputs from the newly developed website to validate its working. In the learning curves (fig. 5 - 7) above the blue and



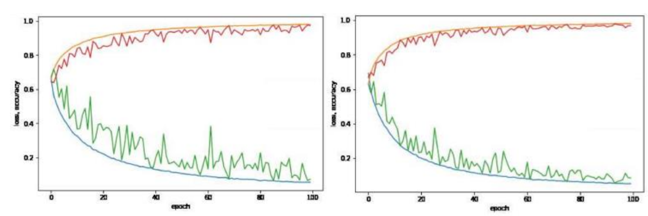
(a) Without out regularization (b) With Cut-Out Regularization

Fig. 5. Learning Curves of Inception Resnet-V2



(a) Without regularization (b) With Cut-Out Regularization

Fig. 6. Learning Curves of VGG Face-2



(a) Without regularization (b) With Cut-Out Regularization

Fig. 7. Learning Curves of Custom Architecture

green lines represent the training and validation loss respectively whereas the orange and red curves represent the training and validation accuracy respectively

In the case of Inception Resnet-V2 fig.5a and 5b show that the model is unable to extract the generalized set of feature vectors. As a result, the validation loss (the green curve) fluctuates and is higher than the training loss. This could happen either due to a change in the distribution of the data or the validation data being barely representative of the training data. However, from accuracy graphs, it is clear that by the end of the training, the training accuracy is very close to one in both the scenarios of with and without cut out. Since there are fluctuations in loss, we cannot trust the model even if it shows better accuracy

In general, we consider the model with the least distance between training loss and validation loss as a good model. In the case of VGGFace2, fig. 6a and 6b illustrates close coincidence of the two curves and more so in the case of

Authorized licensed use limited to: VIT University- Chennai Campus. Downloaded on February 28,2024 at 18:20:47 UTC from IEEE Xplore. Restrictions apply.

scenario with cut out. As before, the accuracy graphs in both the cases grow slowly and settle on a value very close to one as is expected.

Fig.7, represents the learning graphs of our custom residual architecture where the training loss graphs are consistently decreasing over the epochs and reached 0.05 by end of training with Cut-out Regularization and 0.08 without cut out regularization. Fig.7a and 7b also illustrate the training and validation accuracy of our residual architecture where, as is expected the graphs slowly approach one with an increase in the number of epochs.

TABLE III. CONFUSION MATRIX OF DEEPFAKES CLASSIFICATION

	Actual labels		
Predicted labels	***Inception Resnet-V2***		
		Real Images	***Deepfakes***
	Real Images	9,862	133
	Deepfakes	138	9,867
	VGGFace - 2		
		Real Images	***Deepfakes***
	Real Images	9,341	49
	Deepfakes	659	9,951
	Custom Architecture (Resnet-68)		
		Real Images	***Deepfakes***
	Real Images	8,451	72
	Deepfakes	1549	9,928

The learning curves provide an idea about the convergence of the algorithms in terms of accuracy or loss. However, it does not exactly quantify the efficacy of the algorithms. To gauge the performance of the models on real world unseen test data we create their respective confusion matrices which provide the number of True Positives (TP). False positives (FP), True Negatives (TN), and False Negatives (FN) for calculating performance metrics like accuracy, f1-score, sensitivity/recall, precision, and false positive rate. In our implementation, the fake images are considered the negative while the real images are the positive. So a correctly identified fake image will be defined as a true negative in our model. Table.III presents the confusion matrix of the models without regularization whereas Table.IV represents the confusion matrix of the models trained with cut out regularization. When the matrices are compared, it can be seen that there is a significant reduction in the number of false predictions when our custom residual model is used in conjunction with cut out regularization. In case of the transfer learning models with cut-out regularization, on the other hand, the reduction is only in the number of false negatives-from 138 to 7 accounting for 95% change in Inception Resent V2 and from 659 to 338 resulting in a 51% drop.

Table. V presents the consolidated performance of the different algorithms with and without cut out regularization. The results are calculated using equations presented in [24]. The proposed custom residual architecture based model is interfaced with the web application since the custom model is specifically designed to reduce the number of false positives. In our implementation, a deepfake image wrongly classified as a real image is considered a false positive which is considered as a metric of interest since identifying a false image as real can have graver consequences compared to the other scenario. The interfaced web application was deployed in the cloud and is freely available for use by common people. The end-user just needs to upload an image or a screenshot from a video to the web application and within a matter of seconds can know whether the person in the image or video is real or not with a certain confidence. Some sample outputs from the website are presented in fig. 8 and fig. 9 where a fake image is correctly identified with 69.74% confidence and a real image is correctly tagged with a confidence of 99.92%.

TABLE IV. CONFUSION MATRIX OF DEEPFAKES CLASSIFICATION WITH CUT-OUT REGULARIZATION

	Actual labels		
Predicted labels	***Inception Resnet-V2***		
		Real Images	***Deepfakes***
	Real Images	9,993	183
	Deepfakes	7	9,817
	VGGFace - 2		
		Real Images	***Deepfakes***
	Real Images	9,661	173
	Deepfakes	339	9,827
	Custom Architecture (Resnet-68)		
		Real Images	***Deepfakes***
	Real Images	9,452	43
	Deepfakes	548	9,957

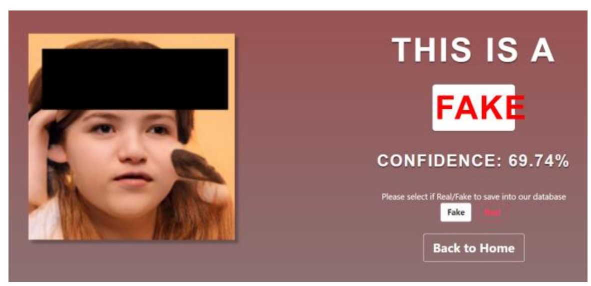


Fig. 8. Web application detecting deepfake image with Cut-Out

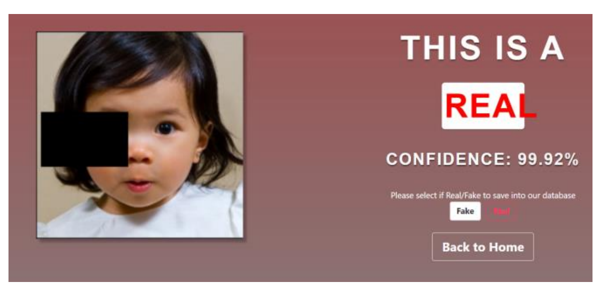


Fig. 9. Web application detecting real image with Cut-Out

Authorized licensed use limited to: VIT University- Chennai Campus. Downloaded on February 28,2024 at 18:20:47 UTC from IEEE Xplore. Restrictions apply.

TABLE V. PERFORMANCE OF THE MODELS

Metrics	Without Cut Out			With Cut-Out		
	Inception Resnet-V2	***VGGFace - 2***	***Custom Architecture***	***Inception Resnet-V2***	***VGGFace - 2***	***Custom Architecture***
Accuracy	98.65%	96.46%	91.92%	99.05%	97.44%	97.05%
F1 Score	98.64%	96.35%	91.25%	99.04%	97.42%	96.97%
Precision	98.67%	99.48%	99.16%	98.17%	98.24%	99.55%
Specificity	98.67%	99.51%	99.28%	98.20%	98.27%	99.57%
Sensitivity	98.62%	93.41%	84.51%	99.93%	96.61%	94.52%
False positive rate	0.0133%	0.0049%	0.0072%	0.018%	0.017%	0.0043%

V. CONCLUSION

This study proposes a new CNN-based residual architecture with and without cut out regularization to reduce the number of false predictions in image classification. The results from the new architectures are then compared with the performance of two existing transfer learning models - Inception Resnet V2 and VGGFace2. The proposed architecture on both occasions is found to present a significant reduction in false positive rate while always maintaining a healthy accuracy. Inception Resnet V2 on the other hand produces a superior accuracy and F1 score in both the scenarios with and without cut-out regularization and can be readily used when the mentioned metrics are of interest. The new deep learning model was further interfaced with a web application and was made available for use by common people [21]. As a future extension of the work, we would like to develop a self-learning model where given an input pre-tagged image for classification the model can further learn from it while providing its prediction.

REFERENCES

[1] J. Xavier, “Deepfake content is doubling every six months, trend to grow in asia,” https://www.thehindu.com/sci-tech/technology/deepfake-content-is-doubling-every-six-months-trend-to-grow-in-asia/ article32064299.ece, 2020

[2] T. Brewster, “Fraudsters cloned company director’s voice in 35 million bank heist, police find,” https: //www.forbes.com/sites/thomasbrewster/2021/10/14/ huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=7ac209047559, 2021.

[3] J. Vincent, “Cheap ai is better at removing henry cavill’s superman mustache than Hollywood special effects,” https://www.theverge.com/tldr/2018/2/7/16985570/superman-mustache-ai-deepfakes-henry-cavill, 2018.

[4] H.-C. Shin, N. A. Tenenholtz, J. K. Rogers, C. G. Schwarz, M. L. Senjem, J. L. Gunter, K. P. Andriole, and M. Michalski, “Medical image synthesis for data augmentation and anonymization using generative adversarial networks,” in International workshop on simulation and synthesis in medical imaging. Springer, 2018, pp. 1–11

[5] H. S. Shad, M. Rizvee, N. T. Roza, S. Hoq, M. Monirujjaman Khan, A. Singh, A. Zaguia, S. Bourouis, et al., “Comparative analysis of deep- fake image detection method using convolutional neural network,” Computational Intelligence and Neuroscience, vol. 2021, 2021.

[6] Cthulululu, “140k real and fake faces,” https://www.kaggle.com/c/deepfake-detection-challenge/discussion/122786, 2020.

[7] D. Gong, Y. J. Kumar, O. S. Goh, Z. Ye, and W. Chi, “Deepfakenet
an efficient deepfake detection method,” International Journal of Advanced Computer Science and Applications, vol. 12, 2021.

[8] S. R. A. Ahmed and E. Sonuç, “Deepfake detection using rationale-augmented convolutional neural network,” Applied Nanoscience, pp. 1–9, 2021.

[9] R. Rafique, M. Nawaz, H. Kibriya, and M. Masood, “Deepfake detection using error level analysis and deep learning,” in 2021 4th International Conference on Computing & Information Sciences(ICCIS). IEEE, 2021, pp. 1–4.

[10] A. Choudhary and A. Arora, “Imagefake: An ensemble convolution models driven approach for image based fake news detection,” in 2021 7th International Conference on Signal Processing and Communication (ICSC). IEEE, 2021, pp. 182–187.

[11] K. Chandani and M. Arora, “Automatic facial forgery detection using deep neural networks,” in Advances in Interdisciplinary Engineering. Springer, 2021, pp. 205–214.

[12] S. Agarwal, N. Girdhar, and H. Raghav, “A novel neural model based framework for detection of gan generated fake images,” in 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence). IEEE, 2021, pp. 46–51.

[13] H. A. Khalil and S. A. Maged, “Deepfakes creation and detection using deep learning,” in 2021 International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC). IEEE, 2021, pp. 1–4.

[14] Y. Li, M.-C. Chang, and S. Lyu, “In ictu oculi: Exposing ai created fake videos by detecting eye blinking,” in 2018 IEEE International Workshop on Information Forensics and Security (WIFS). IEEE, 2018, pp. 1–7.

[15] Y. Zhang, L. Zheng, and V. L. Thing, “Automated face swapping and its detection,” in 2017 IEEE 2nd International Conference on Signal and Image Processing (ICSIP). IEEE, 2017, pp. 15–19.

[16] N. S. Ivanov, A. V. Arzhskov, and V. G. Ivanenko, “Combining deep learning and super-resolution algorithms for deep fake detection,” in 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). IEEE, 2020, pp. 326–328.

[17] B. Malolan, A. Parekh, and F. Kazi, “Explainable deep-fake detection using visual interpretability methods,” in 2020 3rd International Conference on Information and Computer Technologies (ICICT). IEEE, 2020, pp. 289–293.

[18] C. Szegedy, S. Ioffe, V. Vanhoucke, and A. A. Alemi, “Inception-v4, inception-resnet and the impact of residual connections on learning,” in Thirty-first AAAI conference on artificial intelligence, 2017.

[19] Q. Cao, L. Shen, W. Xie, O. M. Parkhi, and A. Zisserman, “Vggface2:A
dataset for recognising faces across pose and age,” in 2018 13th IEEE international conference on automatic face & gesture recognition (FG 2018). IEEE, 2018, pp. 67–74.

Authorized licensed use limited to: VIT University- Chennai Campus. Downloaded on February 28,2024 at 18:20:47 UTC from IEEE Xplore. Restrictions apply.

[20] T. DeVries and G. W. Taylor, “Improved regularization of convolutional neural networks with cutout,” arXiv preprint arXiv:1708.04552, 2017.

[21] G. Dheeraj, “deepfakedetectionwithai,” https:// deepfakedetectionwithai.herokuapp.com/, 2021.

[22] T. Karras, S. Laine, and T. Aila, “A style-based generator architecture for generative adversarial networks,” in Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, 2019, pp. 4401–4410.

[23] K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, “Joint face detection and alignment using multitask cascaded convolutional networks,” IEEE signal processing letters, vol. 23, no. 10, pp. 1499–1503, 2016.

[24] S. D. Gummadi and A. Ghosh, “A transfer learning based approach for detecting covid-19 with radiography images,” in 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT). IEEE, 2021, pp. 1–5

Authorized licensed use limited to: VIT University- Chennai Campus. Downloaded on February 28,2024 at 18:20:47 UTC from IEEE Xplore. Restrictions apply.