Deepfakes: Detection And Creation

Adhnan Manzis[1], Prof. G Srinivasachar[2]
[1]Dept of Computer Science and Engineering
[2]Assistant Professor, Dept of Computer Science and Engineering
[1, 2] Atria Institute of Technology,Bangalore

Abstract- *Deep learning has been utilized in a large vary of applications like system vision, dialect processing and image detection. The advancement in deep learning algorithms in image detection and manipulation has led to the future of creation of deepfakes. These Deepfakes use multiple algorithms like Deep Learning algorithm to create such images that can make it to not noticeable from the real image. With the rising concern around personal privacy and security, several strategies to discover deepfake pictures have emerged, this paper mainly focuses on the utilization of deep learning for making deepfakes, this paper additionally propose the utilization of deep learning image boosting methodology to enhance the standard of deepfakes created.*

Keywords- Deepfakes, Deep Learning, Artificial Intelligence, Convolution Neural Networks

I. INTRODUCTION

The Machine visibility is evolving day by day in a variety of fields from basic image acquisition software to automotive and robots, one of the applications from Deepfake machine vision.

Deepfake is a program that uses in-depth reading algorithms to create fake images usually by changing a person's face from a source image to another person's face in the target image, with a fake image effect that is sometimes hard to find.

The basic method of creating deepfake is using deep learning encoders and decoders, which are widely used in the field of machine vision. Encoders work by extracting all the elements in an image and using decoders to create a duplicate image. Deepfake methods require a large number of photos and videos to train in deep learning models, this has been a difficult task but in our time you can easily find a large set of images on social media, this is a wide range of data. led to the development of more complex strategies, most deepfake algorithms designed using Tensorflow. TensorFlow by Google is an open source software library which uses data flow graphs to calculate numbers. It was originally developed by Google for internal research and development of machine learning and deep neural networks, but the system is common enough to work in a variety of domains and became very popular in machine learning services. after it has been made available to the public and can be used free of charge.

TensorFlow provides a way to design neural networks quickly with sufficient functionality and APIs can be used in python editing language, we can easily change CNN architecture and test various designs without changing many lines of code.

Deepfakes poses a serious risk to a future where false news is everywhere, you can watch a video of a key figure in a public speaker or a lecturer and not be sure what you see is true or false, especially since the process of creating these fake photos and videos is as easy today as you need. intended to produce false content.

Major technology companies are actively exploring ways to find deepfakes to combat the growing number of deepfakes online. Recently, Facebook, Amazon, Microsoft, and the Partnership on AI's Media Integrity Steering Committee teamed up and launched the Deepfake Detection Challenge to promote further research and development in finding and preventing deepfakes. Also, Google has released a free public database as a contribution to deepfake access. This deepfake interest from big names like Google and Microsoft shows how important a deepfake problem is.

In this paper one of the ways to get in-depth images using Mesonet CNN is explored.

II. LITERATURE SURVEY

The average videos which we see nowadays with the development of deepfake tools and the proliferation of false stories, we can understand the dangers of deepfake and it is clear and difficult to find false images and it is easy to use them with deep easy-to-use tools and false stories that can be used. such images spread online. That’s why the need for tools to find deepfakes is so important every day.

This method works best in guiding other researchers. In this case the authors continue to receive or solicit ideas from other people. Enrich your paper collection with expert

comments or promotions. And the researcher feels confident in their work and jumps in to start writing the paper.

New digital technologies are making it increasingly difficult to distinguish between real and false media. One of the most recent developments that has contributed to the problem is the emergence of deepfakes which are virtual reality videos that use artificial intelligence (AI) to show a person saying and doing things that have never happened before. Along with the reach and speed of the social media platform, convincing deepfakes can quickly reach millions of people and have a detrimental effect on our society.

While expert research on the subject is limited, this study analyzes n number ofonline articles to determine what deepfakes are and who produces them, what are the benefits and threats of deepfake technology, what examples of deepfakes exist, and how to combat them, that is deepfakes.

The results suggest that while deepfakes are a major threat to our society, political and business systems, they can be fought through law and order, business and voluntary policies, education and training, and the development of deep, content-based technology. authenticity, and deepfake prevention. This study provides a comprehensive review of deepfakes and provides cybersecurity and AI entrepreneurs with business opportunities in the fight against media lies and false news.

III. DETECTION OF DEEPFAKES USING MESONET CNN

Mesonet is a neural network specifically designed to detect deepfakes. Deepfakes videos are commonly found on all social media. The type of videos on social media like Instagram that are compressed low quality videos so small analysis based on image sound is not possible and MesoNet takes that into account, and finds deepfake at a high semantic level as difficult as even and people sometimes struggling to find deepfakes.

MesoNet relies on a centralized approach using a deep neural network with a small number of layers. This network starts with a four-layer pattern of sequencing and merging and is followed by a dense network with a single hidden layer. Convolution and merging is used to extract image elements. A common pattern using a convolution layer followed by merging. Layer as the convolution layer releases features and the integration layer creates a lower sample version of the feature map.

To improve normal performance, convolutional layers use ReLU unlocking functions that introduce non-linearity and Batch Normalization for normal output, and fully integrated layers use Dropout to customize and improve their durability.

Successfully building a strong neural network capable of finding complex deepfakes requires a large data set of training images. thanks to social media this type of image can be easily accessed and companies like google provide great databases to help speed up research on security in deepfakes. MesoNet has used a database of more than 5000 images, images separated by real images and in-depth images.

IV. CREATION OF DEEPFAKES

Deepfakes are created using in-depth learning methods where they aim to insert the target's face into another person's face in a photo or video. This process was developed by engineers and online communities to significantly create easy-to-use online applications such as FakeApp and FaceSwap.

Deepfake relies on the autoencoder-decoder pipeline. Encoders are widely used in image compression relying on deep neural networks and by introducing a bottle to the network and this forces a compressed representation of the actual input. With the introduction of highly advanced encoders, high-quality image compression is possible which can simplify deepfake operation as it requires lesser compact strength. The task of creating deepfake by training two autoencoders.

These principles can be used to produce in-depth images and (or) videos, obviously, images are faster to produce as they require less processing and are smaller in size comparedto videos. With the development of deepfake tools and the proliferation of false stories, we can understand the danger of deepfake and it is obvious and difficult to find fake images and it is easy to do with easy-to-use deepfake tools and fake stories that can use such images spread online. That is why the need for tools to find deepfakes becomes so important every day.

This approach works the best in guidance of fellow researchers. In this the authors continuously receives or asks inputs from their fellows. It enriches the information pool of your paper with expert comments or up gradations. And the researcher feels confident about their work and takes a jump to start the paper writing.

V. CONCLUSION AND FUTURE WORK

In this paper deepfake creation and detection was explored as well as the integration of deep learning image enhancement method to increase Deepfake detection in the case of face-swapping deepfakes, they are hard to detect when the person is facing straight towards to camera.

- We believe that to further improve the performance of deepfake detectors, the focus should be on using datasets of difficult conditions like this.

- Future works include using generating deepfakes with reduced imperfection and using better enhancement tools.
- The quality of deepfakes created can be improved.
- Use image enhancement methods gave higher-quality look deepfake images.

ACKOWLEDGEMENT

The preferred spelling of the word ―acknowledgment‖ in American English is without an ―e‖ after the ―g.‖ Use the singular heading even if you have many acknowledgments.

REFERENCES

[1] Deepfakes - https://en.wikipedia.org/wiki/Deepfake
[2] MesoNET CNN– Deepfake Detection Tool - https://github.com/MalayAgr/MesoNet-DeepFakeDetection
[3] DFDNet – AI Image Reconstruction tool - https://github.com/csxmli2016/DFDNet
[4] Examples of Deepfakes - https://www.creativebloq.com/features/deepfake-examples
[5] Auto-Encoding and Decoding Pipeline - https://www.researchgate.net/figure/Creation-of-a-Deepfake-using-an-auto-encoder-and-decoder-The-same-encoder-decoder-pair_fig2_349703826