
Image and Video Generation Using Artificial Intelligence and its Detection

Arya J¹, M Vishnu Ganesh², Sreeraj S Nair³, Judin Thomas⁴, Dhannya J⁵

^{1,2,3,4}PG-Computer Application, Kristu Jyoti College of Management and Technology, Changanassery, Kerala

⁵Assistant Professor, Computer Application, Kristu Jyoti College of Management and Technology, Changanassery, Kerala

ABSTRACT

AI (Artificial Intelligence) is intelligence shown by machines, rather than the natural intelligence showed by creatures including people. AI allows machines to learn from experiences and situations, adapt to new information sources and perform human-like errands.

Now a days we have to make sure what we see is real or fake because development in AI and deep neural networks have prompted a rise in synthetic media, i.e., artificially generated or controlled photograph, video and audio content. Synthetic media today is exceptionally believable to such an extent that we can never again believe what we see or hear is pure and real. Among the various types of synthetic contents, the most concerning types are deepfakes and general adversarial networks (GANs).

This new reality can have critical ramifications for network protection, duplicating, counterfeit news, and border security, fake alligations etc.

Keywords - AI, Artificial Intelligence, Deepfakes, Synthetic, Media, GANs, Fake

1. Introduction

AI controlled sound, picture, and video combination has democratized access to restrictive areas or fields. From combining talk in anybody's voice, to creating picture of an imaginary character, interchanging one individual's personality with another or changing what they are talking about in a video, AI-incorporated content holds the ability to entertain and at the same time deceive.

There are organizations which sell fake individuals. We can purchase a fake individual for some dollars. If we need two or three fake individuals for just characters in a computer game, or to cause your organization site to show up more different, then we can get their photographs free of charge on a website. We can change their facial expressions and make them old or youthful and much more according to our personal preference. It is also possible if we want animated fake people, AI can do too. These mimicked individuals are beginning to make an appearance around the web, utilized as veils by real individuals with odious purpose to infiltrate the intelligence community or to take cover behind fake profiles, photograph and all and also to harass people online

2. Deepfakes

The word 'Deepfake' is plainly a blend of two regular words, 'Deep, and 'fake'. Deep says that here AI innovation included. Deepfake technology is utilized in synthetic media to make falsified content, replacing faces or combinig synthesizing faces, speech, and adjusting emotions. It is utilized to digitally impersonate an activity by an individual that the person didn't commit.

A Deepfake video seems like original substance, having the individual doing some activity or talking on a subject. And keeping in mind that making such fake recordings, numerous pictures of the designated individual from various points are utilized to superimpose the real face.

Pictures are compromised with faces and other body parts to make them look unique. While making recordings, the voice is cloned with a designated individual utilizing the AI-empowered devices to work on the process and match the lips moving as per words expressed. The Deepfake recordings influence the existences of well known personalities in our society such as politicians, actors,

actresses, other celebrities, etc. With the help of Deepfake detection services, it is possible to accurately distinguish such fake videos.

Also, Deepfake works by making exciting stories about well known individuals that people love to watch and share with others.

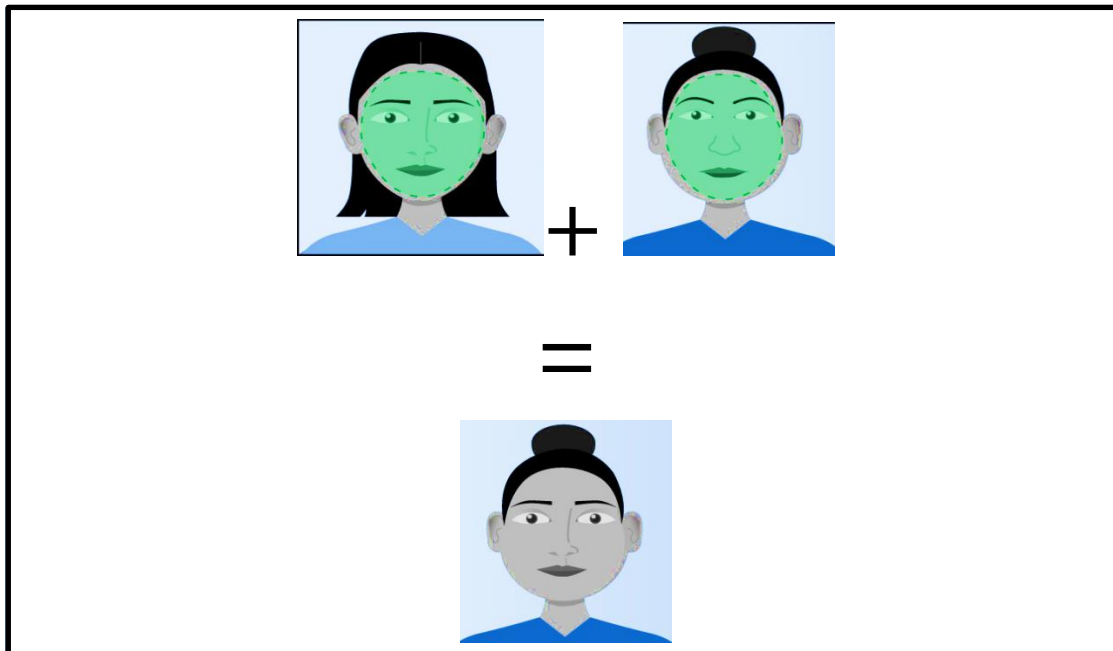


Fig.1. Deepfake

2.1 How Does Deepfake Works?

There are a few methods for making Deepfake content utilizing AI calculations. Basically, these are algorithms that can create content in light of the information input. To make fake face or replace a piece of an individual's face, it should initially be trained. Then the trained data is fed to huge amount of data, at that point, uses to figure out how to make its own, new information. Fundamentally they depend on autoencoders and some of the time on generative adversarial networks (GAN).

Autoencoders : They are a group of self-supervised neural networks, fundamentally based on dimensionality reduction, that figure out how to duplicate their own input. Autoencoders can compress the data like what they have been trained on. Other than this, the autoencoder's result will not be identical to its input.

An autoencoder has 3 parts: an encoder, a code, and a decoder. The encoder compresses the input data and produces the code after the decoder reconstruct the input based upon the code.

GAN : GAN is a way to deal with generative modeling from the input dataset. These understand from input information to create new information. The framework is prepared by two particular neural networks: a generator and a discriminator. The generator finds regularities or patterns in the input dataset and figures out how to reproduce them. The produced information is sent to the discriminator combined with genuine data for assessment. The reason for the generator is to trick the discriminator. You need to train system until the discriminator no longer confuses with the created information with the genuine information. GANs are hard to train and require more resources, so they are frequently utilized for producing photographs instead of video.

3. GANs

The making of fake images just became possible because of another kind of AI called a generative adversarial network (GAN). We feed a computer lots of photographs of genuine individuals. It studies them and attempts to create its own photographs of individuals.

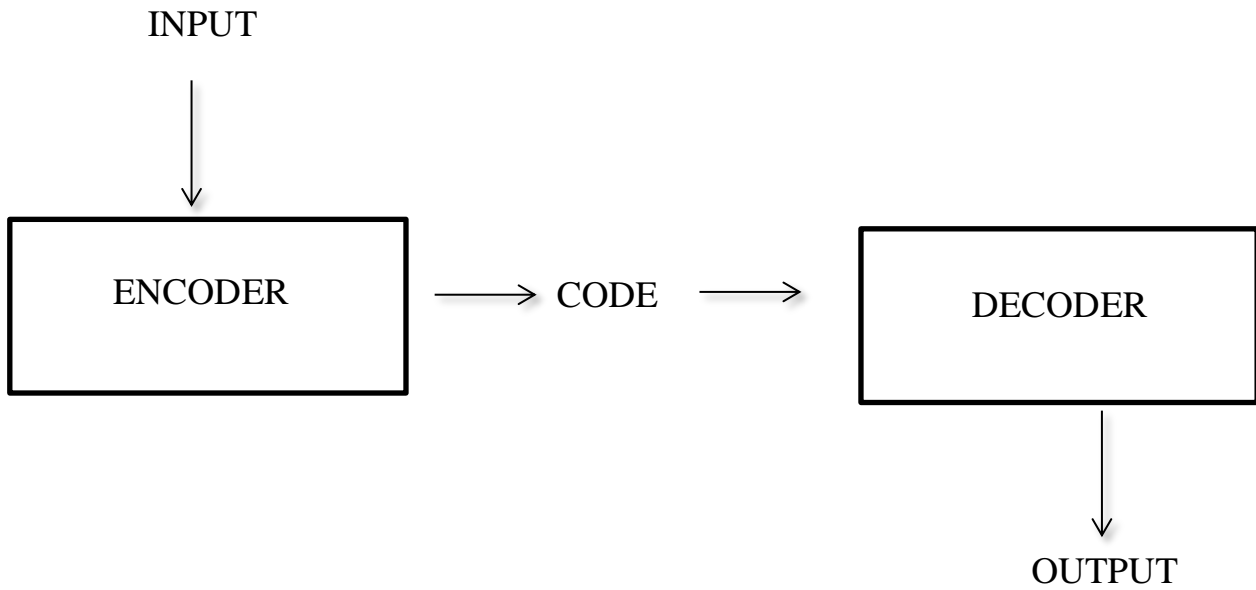


Fig.2.Autoencoder components

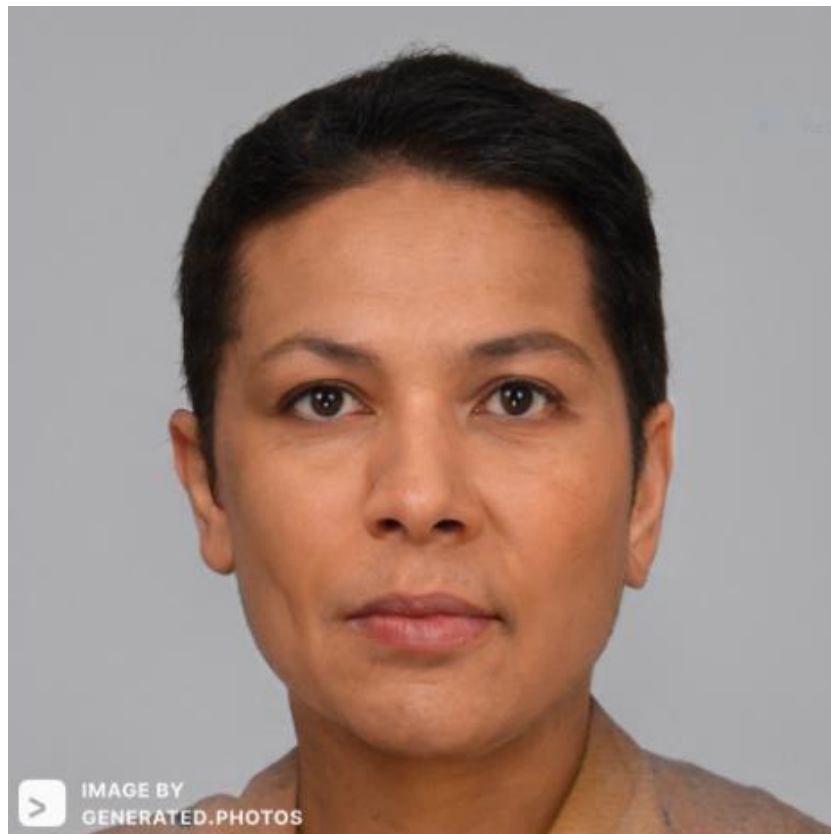


Fig.3.A synthetic face

3.1 How GANs Works?

GANs comprises of two networks- a Generator $G(x)$, and a Discriminator $D(x)$. Generator creates new data instances, while the discriminator, assesses them for legitimacy; for example the discriminator concludes whether each instance of data that it surveys belongs to the real training dataset or not.

Suppose we're attempting to accomplish something more hackneyed than mimic the Mona Lisa. We will produce numerals written by hand like those found in the MNIST dataset, which is taken from this present reality. The objective of the discriminator, when shown an example from the genuine MNIST dataset, is to identify those that are authentic.

Meanwhile, the generator is making new, synthetic pictures and it passes to the discriminator. It does as such in the expectations that they, as well, will be considered authentic, despite the fact that they are fake.

The objective of the generator is to create acceptable manually written digits: to lie without being gotten.

T

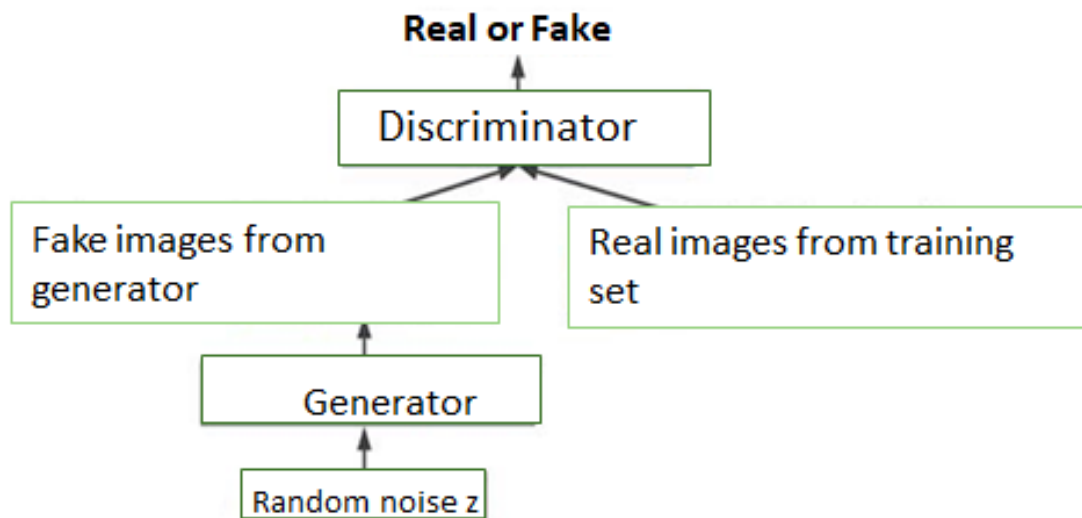


Fig.4.GAN working

4. Benefits and Limitations Of AI Media

4.1 Benefits

- Art: Deepfake innovation can be utilized to make AI symbols for use in preparing recordings. Synthesia have been standing out from the corporate world during the COVID pandemic since lockdowns and wellbeing concerns have made video shoots affecting genuine individuals considerably more challenging to pullof.
- Research: Outside the fields of diversion and preparing, deepfake tech can likewise be utilized to make personal avatars. These can then be utilized in applications that permit individuals to try new garments or new haircuts at home, or in training applications in various professions.
- Personality protection: Maybe more critically, AI-created symbols have been utilized to safeguard the personality of interviewees in news reports about the abuse of LGBTQ individuals in Russia.
- Monetary saving: Others bring up that generative innovation might actually democratize various enterprises. By permitting the modest making of everything from recordings, to commercial and games, generative innovation could permit people and organizations to enter these fields with less venture.
- Awareness: One more benefit is that it makes us mindful of such fake media, and we shouldn't completely accept that all that we see around us. When we observe that it is fake, we learn, and next time when such contents comes, we take time to trust it or do a research to verify the news.
- Fashion Field: We can create unique and customized models for fashion industries as they wish.
- Diversity: Fake images of different gender can be added to websites to show diversity.

- Training: Fake images can be used for training people on various subjects without involving real people images.

4.2 Limitations

- Humiliation: Instead of helping anybody, this AI-based innovation has problems influencing various groups of our society. Aside from making counterfeit news and sharing, these media is utilized predominantly for vengeance, criticizing defaming famous people. When fake recordings turn into a web sensation, individuals accept them at first and continue to share them to other people. This makes the designated individual humiliated.
- Trust: AI generated media challenges people trust because how people can believe their own eyes. They will face trust issues.
- Scamming: One more area of concern is financial scams. Sound Deepfakes have proactively been utilized to clone voices and persuade individuals they are conversing with somebody trusted and defraud them.
- Blackmailing: People use fake images, videos and sounds to blackmail others. This can affect individual's mental health.
- Data Privacy: GANs can produce clone of a person. So it is serious threat connected to facial recognition and data privacy.
- Misinformation spreading: AI can easily create realistic fake media and it will prompt people to spread fake information.
- Chance of losing jobs: In many field now a days we are using AI media. This will led to less usage of man-power. For example, in the case of fashion field fashion models are created using AI. So people can lose their opportunity in this field.

5. How to detect GANs and Deepfakes?

AI are now able to generate fake medias. But it can harm many people if it is misused. As the technology is evolving these fake faces can be very dangerous. So it is necessary to understand how to detect AI generated media. People without technical knowledge(i.e. common people) should also know about detecting these synthetic faces. Below given are few methods to detect fake images and videos.

5.1 GAN image detection

- Face asymmetries: Synthetic faces are in many cases portrayed by unnatural asymmetries. For instance, GAN pictures at times present eyes with various tones, or awry specular reflections, various hoops, or just on studs, or ears with extraordinarily various qualities.
- Landmark locations: All individual face parts are created with an elevated degree of authenticity and with many details, yet their relative locations are unnatural. In view of this perception, the strategy utilizes the areas of the facial landmark points, like the tips of the eyes, nose, and the mouth, as discriminative elements for recognition.
- Color features: GANs produce by design just a restricted scope of intensity values, and do not create saturated and/or under-exposed regions. While this is a decent property to ask of a photograph, countless normal face pictures really do introduce outrageous esteemed pixels, and their absence recommends a synthetic occurrence.
- Blob artifacts: For instance, the normalization strategy utilized in GAN triggers blob artifacts and color bleed in generated images. This uncovers the fake pictures easily.

5.2 Deepfake video detection

- Blurry: Faces in numerous Deepfake recordings are surprisingly blurry. There are two main reasons. one, the new face needs to mix well with the other pictures. Accordingly, filters are applied which will blur the face slightly. Two, some budget productions use low-resolution photos of the faces to learn the encoder.
- Skin tone: In some swapped face, the skin complexion looks un-nature.

- **Flicking:** One of the significant shortcomings of Deepfakes is that video frames are created frame-by-frame independently. Such independence might produce video frames with recognizable various tones, lighting, and shadow contrasted with the last frame. At the point when it is playing back, flicking happens.
- **Teeth:** One of the vital setbacks of most Deepfakes recordings is the teeth region. It is difficult for the decoder to remake a little region that has an detailed and well-defined design. Normally, the teeth in Deepfakes are blurry. In other cases, the teeth are misaligned teeth, or the singular tooth is extended or shrank.
- **Glare and reflection:** A portion of the glare or reflection in Deepfakes looks exaggerated, missing or without the legitimate complexity. This is the issue for Deepfakes to deliver little designs.
- **Eye Blinking:** For instance, numerous early Deepfakes recordings have faces gathered from still pictures. This makes a gross imbalance of training class. Normally, there will be an absence of side images and images that are blinking.

6. Future of AI Generated Media

Faces and videos generated using AI has a very big future ahead. AI-driven characters might in any case be in their earliest stages, with long stretches of improvement yet ahead before they arrive at development, now they are leaving an imprint on our lives, and their utilization is quickly edeveloping.

Use of Deepfake videos can be extend to many fields other than film industry and gaming , like medical field, fashion field etc. This AI generated synthetic content can save time and cost in many ways. Deepfakes depend on augmented reality and keep on being a marker of technology breakouts. Deepfakes will proceed to develop and spread further, and issues like the absence of details in the synthesis will be survived, and with lighter-weight neural network designs and advances in hardware, training and producing time will be altogether decreased. We have already seen new calculations that can deliver progressively more significant levels of authenticity and run in near real time. According to experts, GANs (generative adversarial networks) will be the main drivers of Deepfakes advancement in the future.

CONCLUSION

AI media generation can cause real harm. We are now seeing the utilizations of this innovation to infringe upon individuals' securities, make havoc by showcasing people creating false statements, fooling individuals into duplicity, committing fraud and cybercrime.

Going ahead, to limit duplicity and control the sabotaging of trust, technical experts, writers, and policymakers will play a critical part in standing up and teaching the general population about the capacities and risks of synthetic media. New fake detection which is more accurate and reliable methods need to be developed. If people can teach ourselves to just believe content from trustworthy sources, we might find that synthetic media could actually overweigh the bad. With expanded public mindfulness, we could figure out how to restrict the adverse consequence of fake photos or videos, find approaches to co-exist with them, and even reap benefits from them later on.

References

1. Karras T, Laine S, Aila T (2019) A style-based generator architecture for generative adversarial networks. In: IEEE/CVF conference on computer vision and pattern recognition (CVPR), pp 4396–4405
2. Travis L. Wagner and Ashley Blewer (2019): “The Word Real Is No Longer Real”: Deepfakes, Gender, and the Challenges of AI-Altered Video
3. Stamatis Karnouskos (2020): Artificial Intelligence in Digital Media: The Era of Deepfakes

4. Karras T, Laine S, Aittala M, Hellsten J, Lehtinen J, Aila T (2020) Analyzing and improving the image quality of StyleGAN. In: IEEE/CVF conference on computer vision and pattern recognition (CVPR), pp 8110–8119.
5. Jonathan Hui (2020) Article: <https://jonathan-hui.medium.com/detect-ai-generated-images-deepfakes-part-1-b518ed5075f4>
6. Wang R, Juefei-Xu F, Ma L, Xie X, Huang Y, Wang J, Liu Y (2020) FakeSpotter: a simple yet robust baseline for spotting AI-synthesized fake faces. In: International joint conference on artificial intelligence (IJCAI), pp 3444–3451
7. Lucas Whittaker; Tim C. Kietzmann; Jan Kietzmann; Amir Dabirian (2020) “All Around Me Are Synthetic Faces”: The Mad World of AI-Generated Media
8. Stijn Kas, Thomas Hes, Brian Jansen, Ruben Post, (2020): Do you know if I'm real? An experiment to benchmark human recognition of AI-generated faces
9. Cristian Vaccari, Andrew Chadwick (2020): Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News
10. Yuru Lin, Krishnaveni Parvataneni (2021): Deepfake Generation, Detection, and Use Cases: A Review Paper
11. Andrei O. J. Kwok, Sharon G. M. Koh (2021): Deepfake: a social construction of technology perspective
12. Giandomenico DiDomenico, Jason Sit, Alessio Ishizaka, Daniel Nunan (2021): Fake news, social media and marketing: A systematic review
13. Loreto Corredoira, Ignacio Bel Mallén, Rodrigo Cetina Presuel (2021): The Handbook of Communication Rights, Law, and Ethics: Seeking Universality, Equality, Freedom and Dignity
14. Xin Wang, Hui Guo, Shu Hu, Ming-Ching Chang, Siwei Lyu (2022): GAN-generated Faces Detection: A Survey and New Perspectives (2022)
15. Sophie J. Nightingale s.nightingale1@lancaster.ac.uk and Hany Farid (2022): AI-synthesized faces are indistinguishable from real faces and more trustworthy
16. Christian Rathgeb, Ruben Tolosana, Ruben Vera-Rodriguez, Christoph Busch (2022): Book: Handbook of Digital Face Manipulation and Detection