Deepfake Technology

Published On: 08-11-2023

Why is in news?

A popular Indian actor entering an elevator in revealing clothes. Football fans in a stadium in Madrid holding an enormous Palestinian flag. These unrelated events have something in common: they never happened.

And yet, they were some of the most viral pieces of content on various social media platforms. Thanks to artificial intelligence (AI), which has improved greatly over the past year, there are now platforms that allow nearly anyone to create a persuasive fake by entering text into popular AI generators that produce images, video or audio.

About deepfakes:

A deepfake is a **digitally forged image or video of a person** that makes them appear to be someone else.

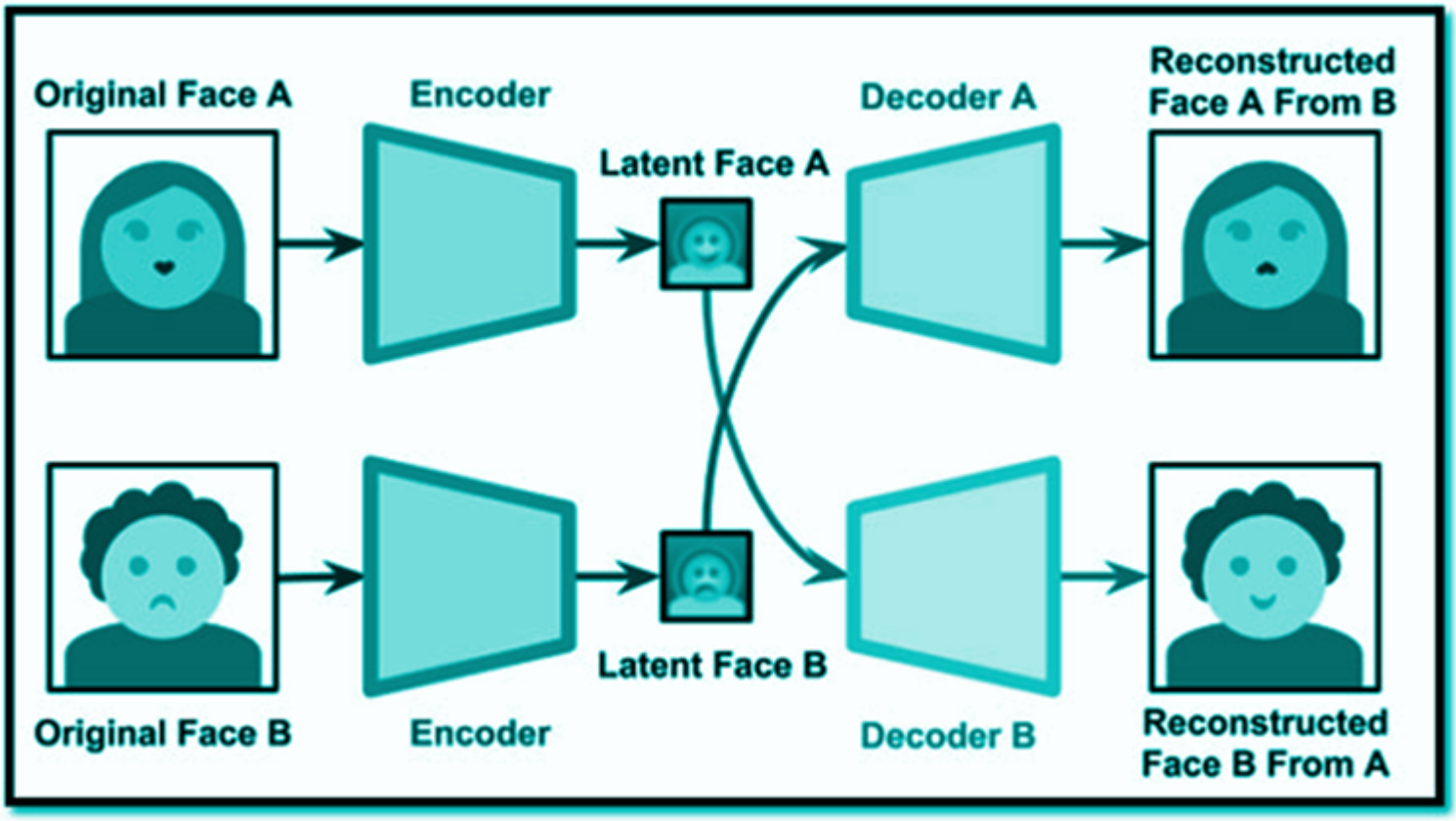
It is the **next level of fake content creation** that takes **advantage of Artificial Intelligence** (AI).

Artificial intelligence refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions.

It can create people who do not exist and it can fake real people saying and doing things they did not say or do.

The application of a technology called **Generative Adversarial Networks (GAN),** which uses two AI algorithms — where one generates the fake content and the other grades its efforts, teaching the system to be better — has helped come up with more accurate deepfakes.

A Generative Adversarial Network (GAN) is a **deep learning architecture** that consists of two neural networks competing against each other in a zero-sum game framework.



Origin of the term:

The term **deepfake originated in 2017**, when an anonymous Reddit user called himself “Deepfakes.”

This user manipulated Google’s open-source, deep-learning technology to create and post pornographic videos.

The videos were doctored with a technique known as face-swapping. The user “Deepfakes” replaced real faces with celebrity faces.

Benefits of Deepfake Technology:

Entertainment:Deepfake technology can be used to **create realistic special effects in movies and TV shows**It can also be used to create personalized entertainment experiences, such as virtual reality simulations that allow users to interact with their favourite celebrities.

Education:Deepfake technology can be used to **create more engaging and interactive educational experiences** For example,it could be used to create simulations of historical events or to allow students to interact with virtual characters.

Activism: Deepfake technology can be used to **raise awareness of social issues**For example,it could be used to create videos that show the impact of climate change or to give a voice to marginalized groups.

Impact of Deepfake Technology:

The primary victims of malicious deepfake technology are women, with over **96% of deepfakes being pornographic** videos. This type of content threatens, intimidates, and psychologically harms individuals.

Deepfakes contribute to a **decline in trust in traditional media**. This erosion can lead to a culture of factual relativism, damaging civil society.

Malicious nation-states can use deepfakes to **undermine public safety**, create chaos, and sow uncertainty in target countries. This technology can also **undermine trust in institutions and diplomacy**.

Insurgent groups and terrorist organizations can use deepfakes to manipulate and spread inflammatory speeches or provocative actions to incite anti-state sentiments among the public.

The existence of deepfakes can lead to the **dismissal of genuine information** as fake news. Leaders may use deepfakes and alternative facts to discredit actual media and truths.

These fakes can be used to **impersonate individuals** for fraudulent activities.

Measures to combat deepfakes:

European Union:

The EU has an updated **Code of Practice** to stop the spread of disinformation through deepfakes.

The revised Code requires tech companies including Google, Meta, and Twitter to take measures in countering deepfakes and fake accounts on their platforms.

They have six months to implement their measures once they have signed up to the Code.

If found non-compliant, these companies can face ?nes as much as 6% of their annual global turnover.

United States:

In July 2021, the US introduced the bipartisan **Deepfake Task Force Act** to assist the Department of Homeland Security (DHS) to counter deepfake technology.

The measure directs the DHS to conduct an annual study of deepfakes — assess the technology used, track its uses by foreign and domestic entities, and come up with available countermeasures to tackle the same.

China:

China has implemented a policy that requires deepfake content to be labeled and traceable to its source. Users need consent to edit someone’s image or voice, and news from deepfake technology must come from government-approved outlets.

India:

In India, currently, there are **no legal rules** against using deepfake technology.

However, specific laws can be addressed for misusing the tech, which include Copyright violation, Defamation, etc.

Legal protection available in India:

IPC & IT Act:

Currently, very few provisions under the Indian Penal Code (IPC) and the Information Technology Act, 2000 can be potentially invoked to deal with the malicious use of deepfakes.

Section 500 of the IPC provides punishment for defamation.

Sections 67 and 67A of the Information Technology Act punish sexually explicit material in explicit form.

IT Act of 2000 – Section 66E: This section is applicable in cases of deepfake crimes that involve capturing, publishing, or transmitting a person's images in mass media, violating their privacy.

Offenders can face imprisonment for up to three years or a fine of up to ?2 lakh.

IT Act of 2000 – Section 66D: This section allows for the prosecution of individuals who use communication devices or computer resources with malicious intent to cheat or impersonate someone.

It can result in imprisonment for up to three years and/or a fine of up to ?1 lakh.

Copyright Protection:

The Indian Copyright Act of 1957 provides copyright protection for works, including films, music, and other creative content.

Copyright owners can take legal action against individuals who create deepfakes using copyrighted works without permission.

Section 51 of the Copyright Act provides penalties for copyright infringement.

RPI:

The Representation of the People Act, 1951, includes provisions prohibiting the creation or distribution of false or misleading information about candidates or political parties during an election period.

ECI Guidelines:

The Election Commission of India has set rules that require registered political parties and candidates to get pre-approval for all political advertisements on electronic media, including TV and social media sites, to help ensure their accuracy and fairness.

Way Ahead:

The Union government should **introduce separate legislation** regulating the nefarious use of deepfakes and the broader subject of AI.

The proposed Digital India Bill can also address this issue. Tech firms are also working on detection systems that aim to flag up fakes whenever they appear.

India can consider **establishing a dedicated research and development entity** similar to DARPA, which has been at the forefront of deepfake detection technologies.

Media literacy efforts must be enhanced to cultivate a discerning public. Media literacy for consumers is the most effective tool to combat disinformation and deepfakes.

Develop accessible and user-friendly technology solutions to detect deepfakes, authenticate media, and promote authoritative sources.

Every **individual should take responsibility** for being critical consumers of online media. Before sharing content on social media, pause and think about its authenticity.

Encourage **social media platforms to take action against deepfakes**. Many platforms have already established policies or acceptable terms of use for deepfakes.