Deep Fakes

drishtiias.com/printpdf/deep-fakes

Why in News

Recently, cybercrime officials in India have been tracking certain apps and websites that produce nude photographs of innocent people using **Artificial Intelligence** (AI) algorithms.

Key Points

- **Deep Fake:**
  - Deep fakes or deep nudes are **computer-generated images and videos.** Cybercriminals use AI softwares to **superimpose a digital composite** (assembling multiple media files to make a final one) **onto an existing video, photo or audio.**
  - Using AI algorithms a person's words, head movements and expressions are transferred onto another person in such a seamless way that it becomes difficult to tell that it is a deep fake, unless one closely observes the media file.
- Deep fakes **first came into notice in 2017** when a Reddit user posted explicit videos of celebrities. After that several instances have been reported.

- **Concerns:**
  - The technology becomes **vulnerable** because deep fake images, audio and videos are very **realistic** and can be **used by cybercriminals to spread misinformation to intimidate or blackmail people, seek revenge or commit fraud** on social networking and dating sites.
  - It has become **one of the modern frauds of cyberspace,** along with **fake news, spam/phishing attacks, social engineering fraud, catfishing and academic fraud.**
  - It can be used to **create fake pornographic videos** and to make **politicians appear to say things they did not,** so the potential for damage to individuals, organisations and societies is vast.
  - With the **improvement in technology,** deep fakes are also getting better.
    - **Initially,** an **individual with advanced knowledge** of machine learning and access to the victim's publicly-available social media profile **could only make** deep fakes.
    - **Development of apps and websites capable** of such editing became **more frequent and easily accessible** to an average user.
- **Legality:**
  - In the US, the legality of deep fakes is **complicated.** An affected person **may claim defamation** but removing such content could be considered **censorship.** Then, it will be a **violation of the First Amendment** which guarantees Americans the freedom concerning religion, expression, assembly and the right to petition.
  - Also, **46 states in the US have revenge porn laws.** **Revenge porn** refers to the creation of sexually explicit videos or images that are posted on the Internet without the consent of the subject as a way to harass them.
  - However, the **Right to be Forgotten,** allows a user to request companies such as Facebook and Google, that have collected his/her data to take it down.
- **Protection:**
  - **Ensuring strict privacy settings on social media platforms** because keeping track of who downloads and misuses a user's pictures is impossible.
  - **Using freely available reverse image search tools** to find images that are similar to users in case it is feared that someone is using the original user's pictures.
  - **Staying mindful of virtual interactions** and **checking other user's profiles** to help determine if the person is genuine or not.

Phishing

- The email or text message carrying a link appears to come from a trusted source like a bank.

- The link takes the user to a fake website and once details like login name and passwords are entered, the login credentials reach the hacker.

Catfish Account

It refers to the practice of setting up fictitious online profiles, generally, for luring another person into a fraudulent romantic relationship.

Source: IE