Deepfakes in Elections: Challenges and Mitigation

This editorial is based on **"Deepfakes in elections: They have shaken our faith in our own judgment** which was published in Indian Express on 14/05/2024. The article discusses the introduction of deep fakes in our ongoing election cycle and its associated threat to the fair election process, the challenges of deep fakes in verifying various authentic information and our own judgment.

For Prelims: Deepfakes, AI technology, The IT Act and IT Rules, Election Commission of India, AI chatbots, optical character recognition (OCR), Natural language processing (NLP), Google AI models, Deep Tech, Artificial Intelligence, Internet of Things, Big Data, quantum computing, Telecom industry, Unified Payment Interface, Space Sector, India's Semiconductor Mission, IndiaAI Mission, Mission on Advanced and High-Impact Research.

For Mains: Deepfake technologies pose risks to the functioning of democratic politics

The emergence of **deepfakes** in our **electoral process** raises significant concerns, Unlike traditional forms of misinformation, **deepfakes undermine our ability to distinguish reality from fabrication**, we can no longer rely solely on interventions or technological solutions to verify information and the real challenge lies in our **diminished trust** in our analysis.
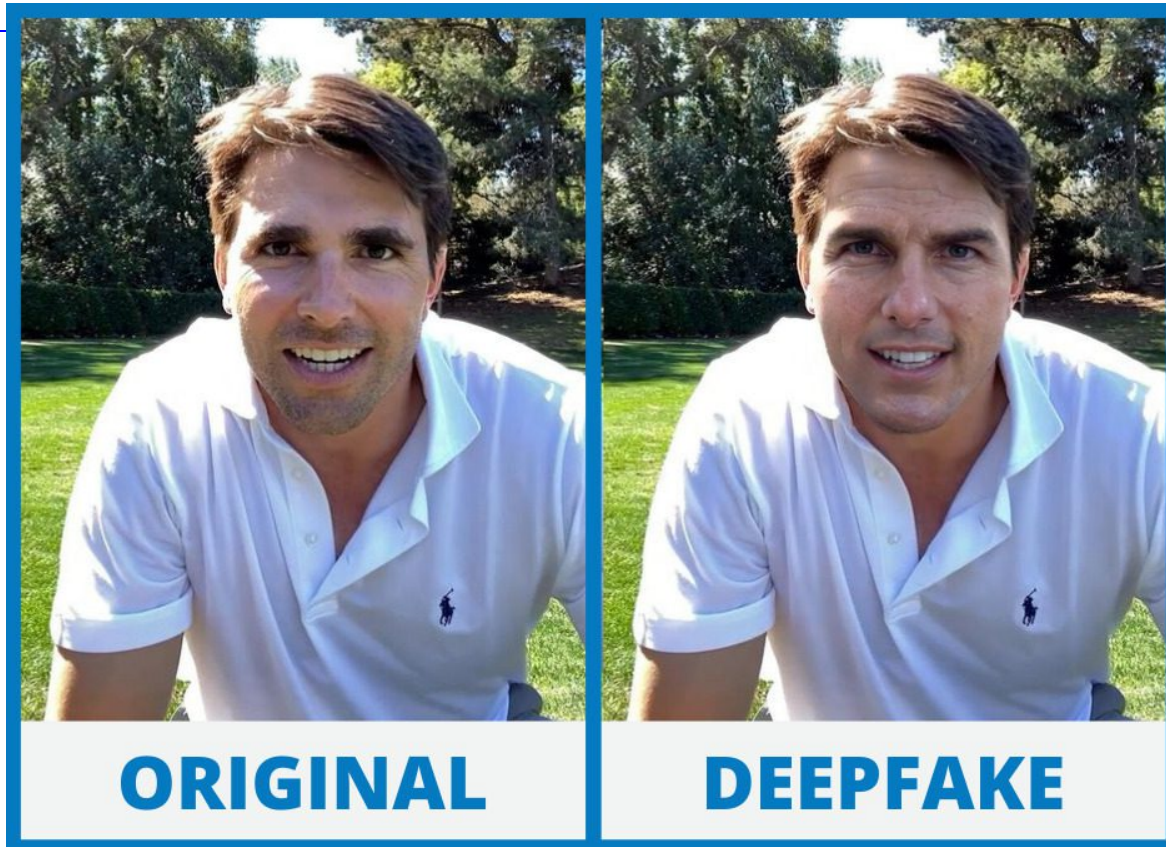
While we were accustomed to encountering manipulated information, we once had confidence in our ability to **discern** the truth, and we relied on alternative sources and trusted media institutions to verify information, However, deepfakes challenge this confidence by casting doubt on our judgment.

What are Deepfakes?

- **About:**
    - Deepfakes refer to **synthetic media** created through **AI technology**, aiming to manipulate or generate visual and audio content to **deceive or mislead individuals.**
- **Origin:**
    - The term **deepfake** was coined in **2017** by an anonymous **Reddit** user who identified as "Deepfakes."
    - This individual utilized Google's open-source **deep-learning technology** to produce and share pornographic videos.
- **Creation:**
    - The creation of deepfakes involves a technique known as **generative adversarial networks (GANs),** comprising two competing neural networks: A generator and A discriminator.
        - **The generator:** Its objective is to produce fake images or videos that closely resemble reality, while
        - **The discriminator**: Its role is to differentiate between authentic and fake content.

- **Data Synthesis:** Its creation necessitates a substantial amount of data, often sourced from the internet or social media without consent, including photos or videos of both the source and target individuals.
- **Deep Synthesis**: It constitutes a component of Deep Synthesis, an umbrella term encompassing technologies such as deep learning and augmented reality, utilized to generate text, images, audio, and video to construct virtual scenarios.

[//](#)

What are the Various Advantages of Deepfake in Elections?

- **Segmentation and targeting:**
  - Deep learning algorithms enable political parties and candidates to analyse extensive **voter data**, encompassing **demographics,** social media engagement, and voting history.
  - **Natural language processing (NLP)** algorithms enable campaigns to analyse and interpret vast amounts of textual data, including social media posts, news articles, and public forums and targeting the voters for personal benefits.
- **Real-time monitoring and adaptation:**
  - Utilising deep-powered **predictive analytics such as AI cloud,** parties can forecast election outcomes by scrutinizing diverse factors such as **polling data, economic indicators**, and sentiment analysis from social media.
  - AI algorithms continuously scan various data sources, including social media, **news outlets, and opinion polls,** to gauge public sentiment and identify emerging trends.
- **Enhanced communication strategies:**
  - **Deepfake-empowered** AI chatbots and virtual assistants engage with voters on social media platforms, addressing inquiries, disseminating information about candidates and policies, and even encouraging voter participation.
- **Security and Integrity:**
  - AI-driven deepfake tools play a crucial role in **detecting and preventing electoral fraud**, including voter suppression, manipulation of electronic voting systems, and dissemination of disinformation.
  - By analyzing data patterns and anomalies, AI algorithms contribute to upholding the integrity of elections.

- **Regulation and Oversight:**
    - Governments and electoral authorities leverage AI and deep technologies to monitor and regulate political advertising, identify breaches of campaign finance laws, and ensure adherence to electoral regulations.
    - AI-powered tools facilitate **transparency and accountability** in the electoral process.
    - For example, **In 2021**, the Bihar Election Commission collaborated with AI firm **Staqu to deploy** video analytics with **Optical character recognition (OCR)** for analyzing CCTV footage from counting booths during the panchayat elections, this system ensured complete transparency and eradicated any potential for manipulation.

What are the Various Challenges related to Deepfakes in Elections?

- **Electoral Behavior Manipulation:**
    - **Creating deepfake content**, and bombarding voters with highly personalized propaganda, leading to confusion and manipulation.
    - Deepfake videos of opponents can be generated using AI, tarnishing their image and influencing voter perceptions and giving birth to the **Deep Fake Election concept.**
        - The term **"Deep Fake Elections"** refers to the use of AI software to fabricate convincing fake videos, audio, and other content, posing a serious threat to the integrity of elections and undermining public trust.
- **Spreading Misinformation:**
    - Deepfake models, particularly **Generative Artificial Intelligence(AI)**, can manipulate democratic processes by spreading disinformation
    - Examples like in the **2024 Loksabha election** where a **cloned voice** of Mahatma Gandhi has been created and shown that Gandhiji is campaigning for a particular political party.
    - **Few more examples like,** a deepfake video of the ruling party's Member of Parliament(MP), went viral on WhatsApp in the country, where he is criticizing his political opponent and encouraging voters to vote for the ruling party.
    - This risk is exacerbated by social media platforms reducing their **fact-checking** and election integrity efforts.
- **Inaccuracies and Unreliability:**
    - Deepfakes AI models, including AGI, are susceptible to inaccuracies and inconsistencies, raising concerns about their reliability.
    - Instances of **Google AI models** misrepresenting individuals have highlighted the potential dangers of unchecked AI.
    - Inconsistencies in AI models pose inherent risks to society as their usage expands.
- **Ethical Concerns:**
    - The use of deepfake in elections raises ethical questions regarding **privacy, transparency, and fairness.**
    - AI algorithms may perpetuate biases present in training data, leading to unfair treatment or **discrimination** against certain voter groups.
    - Lack of transparency in AI decision-making processes can erode public trust in electoral outcomes.
    - Unequal access to AI resources may disrupt the level playing field in elections, favouring parties with greater resources.
- **Regulatory Challenges:**
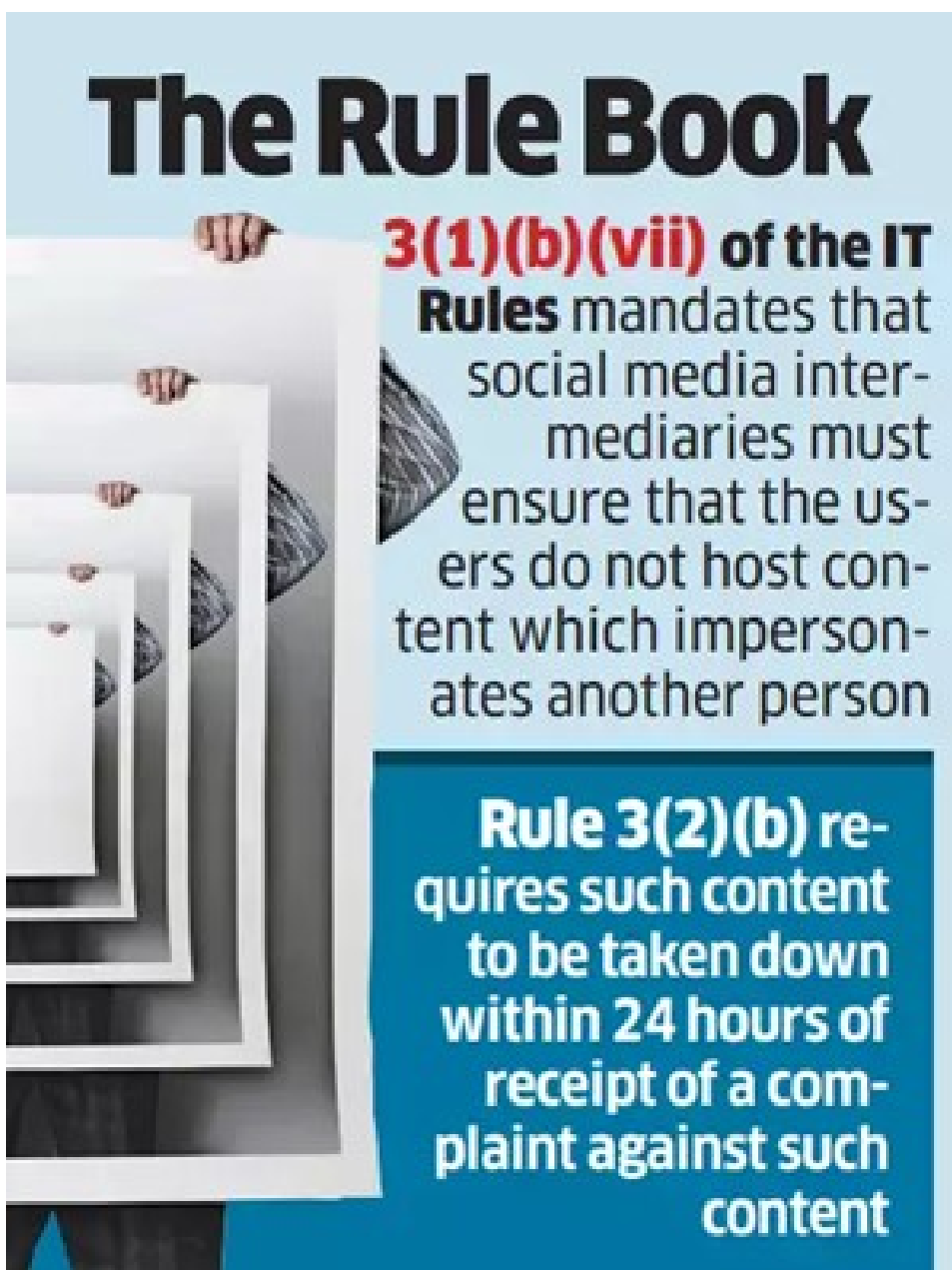   - Regulating deepfakes in electoral campaigns is challenging due to rapid technological advancements and the global nature of online platforms.
    - Governments and election authorities struggle to keep pace with evolving AI techniques and may lack expertise in regulating AI-driven electoral activities.
    - Existing laws such as the India Penal Code, of 1860**, and** the Information Technology Act, of 2000, address aspects of fake news and digital media ethics but lack specific provisions targeting AI and deepfake technology creators.

What are the Government Initiatives related to Deepfakes?

- **IT Act, 2000 and IT Rules, 2021: The IT Act and IT Rules** stipulate that social media intermediaries are responsible for promptly removing deepfake videos or photos and failure to do so can result in imprisonment for up to three years or a fine of Rs 1 lakh.

- **Section 66D of IT Act:** According to **Section 66D of the IT Act, 2000**, individuals who deceive others by impersonating using a communication device or computer resource can face imprisonment for up to three years and a fine of up to one lakh rupees.
  - **Rule 3(1)(b)(vii):** This rule mandates social media intermediaries to ensure that users do not host any content impersonating another person.
  - **Rule 3(2)(b):** It requires such content to be removed within 24 hours of receiving a complaint against it.
  - The **Fact Check Unit under PIB** was established under **IT rules 2021,** in November 2019 with a stated objective of acting as a deterrent to creators and disseminators of fake news and misinformation.
    - It also provides people with an easy avenue to report suspicious and questionable information pertaining to the Government of India.
- **INDIAai.**
- **Global Partnership on Artificial Intelligence (GPAI).**
- **US India Artificial Intelligence Initiative.**
- **Responsible Artificial Intelligence (AI) for Youth.**
- **Artificial Intelligence Research, Analytics and Knowledge Assimilation Platform.**
- **Artificial Intelligence Mission.**

What Can be Done to Combat the Misuse of Depfakes in Elections?

- **Regulatory Measures:**
  - Implement strict laws and regulations that specifically address the creation, dissemination, and use of deepfake content for electoral manipulation.
  - **Example:** Amendments to the **Information Technology Act, India Penal Code, of 1860,** or enact new legislation to **criminalize the creation and dissemination of deepfake** content during election periods.
- **Election Commission Guidelines:**
  - In the context of the **Lok Sabha elections 2024,** one possible solution to **deepfaked and AI-fueled misinformation** would be guidelines issued by the **Election Commission of India.**
  - There is a need to implement regulations that require transparency in the use of AI algorithms for political purposes.
    - This includes **disclosing sources of funding** for political advertisements and requiring platforms to disclose how algorithms determine the content users see.
- **Technology-Based Solutions:**
  - Develop advanced AI algorithms and tools to detect and authenticate deep fake content in real-time.
  - **For example** likes **DeepTrust Alliance**, a coalition of tech companies and research institutions, developed DeepTrust Analyzer, a tool that uses machine learning to identify deepfake videos and images.
  - Indian tech companies could collaborate with research institutions to develop **deep fake detection** algorithms tailored to Indian languages and cultural contexts.
- **Awareness and Education Campaigns:**
  - **Launch public awareness campaigns** to educate voters about the existence and potential impact of deepfake technology on elections.
  - **Example** such as the Government of India could partner with **media organizations** and celebrities to **create public service** announcements raising awareness about deepfakes and urging vigilance during elections.
- **Enhanced Fact-Checking:**
  - Establishing a **Rapid Response Team** to address the dissemination of fake news, deep fakes, and other forms of misinformation during elections is crucial.
  - While it's inevitable that fake videos and misinformation will arise, the key lies in **swiftly addressing** them before they escalate and spread widely.
- **Collaborative Efforts:**
  - Foster collaboration among governments, tech companies, and civil society organizations to develop coordinated responses to deepfake threats.
  - A few examples like, **The Deepfake Detection Challenge, organized by Facebook, Microsoft,** and several universities, invites researchers to develop tools to detect and combat deepfake videos.
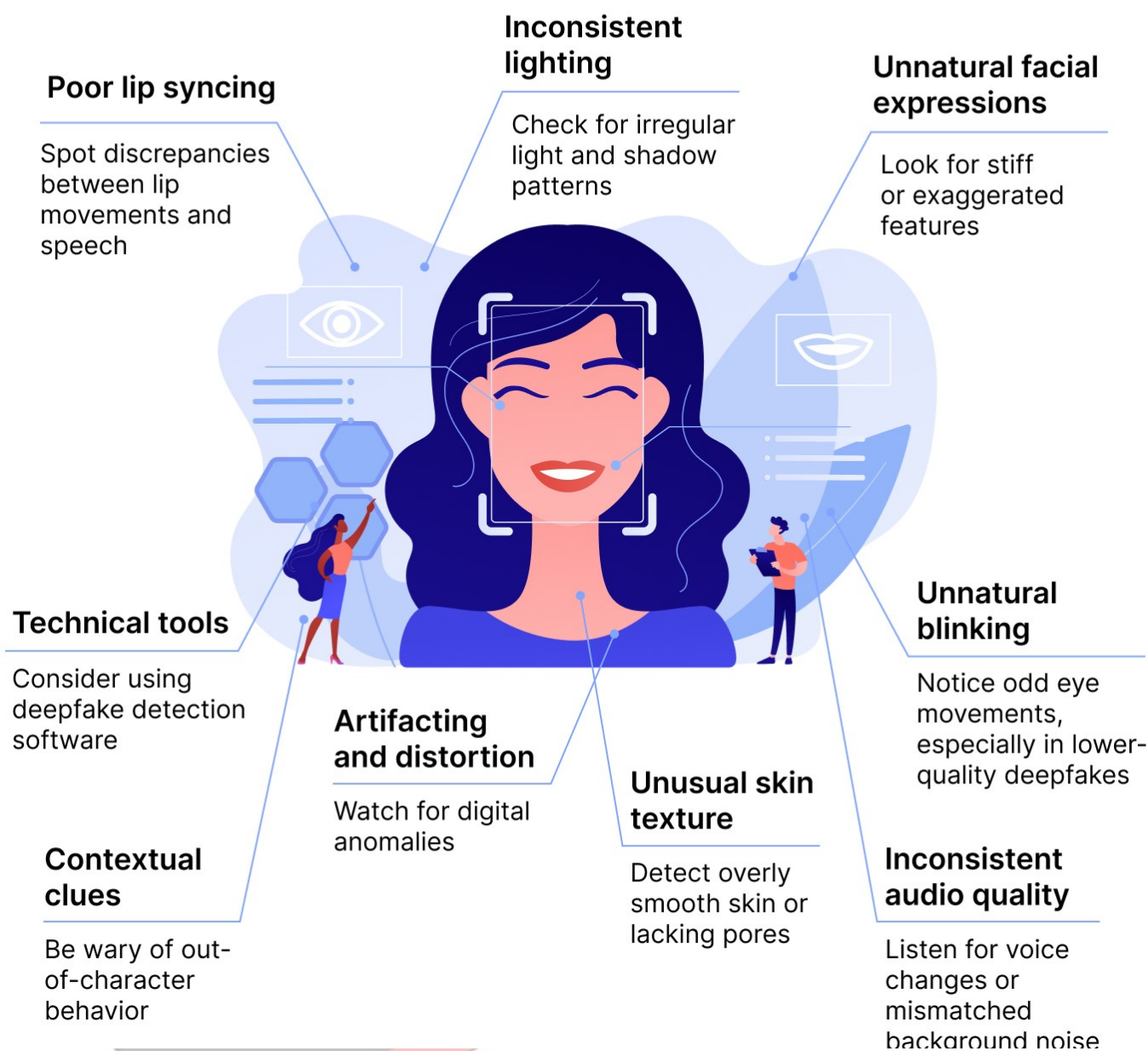- **Drawing Insights from International Practices:**
  - **China's Regulatory Strategy**: China emphasizes **obtaining consent** and verifying identities in the use of deepfake technologies, providers of such technologies are mandated to secure consent from depicted individuals and **authenticate user identity** and moreover, measures are in place to facilitate recourse for individuals adversely affected by deepfake content.
  - **Canada's Preventative Approach:** Canada focuses on preemptively addressing the harms of deepfakes through **widespread public awareness campaigns** and prospective legislation and these campaigns aim to educate the populace about the risks associated with deepfake technology.
- **Promoting Ethical AI:**
  - Foster the advancement of AI technologies with ethical principles at the forefront, prioritizing objectives like **mitigating bias, safeguarding privacy, and fostering transparency.**
  - Institutional norms and protocols delineating the judicious application of AI within **political domains.**

How to Recognize Deepfake Content

Poor lip syncing

Spot discrepancies between lip movements and speech

Inconsistent lighting

Check for irregular light and shadow patterns

Unnatural facial expressions

Look for stiff or exaggerated features

Technical tools

Consider using deepfake detection software

Contextual clues

Be wary of out-of-character behavior

Artifacting and distortion

Watch for digital anomalies

Unusual skin texture

Detect overly smooth skin or lacking pores

Unnatural blinking

Notice odd eye movements, especially in lower-quality deepfakes

Inconsistent audio quality

Listen for voice changes or mismatched background noise

Drishti mains Questions:

How can deepfake technology impact the integrity of election campaigns, and what measures can be implemented to mitigate its influence?"

UPSC Previous Year Questions

Prelims

Q. With the present state of development, Artificial Intelligence can effectively do which of the following? (2020)

1. Bring down electricity consumption in industrial units

2. Create meaningful short stories and songs
3. Disease diagnosis
4. Text-to-Speech Conversion
5. Wireless transmission of electrical energy

Select the correct answer using the code given below:

(a) 1, 2, 3 and 5 only
(b) 1, 3 and 4 only
(c) 2, 4 and 5 only
(d) 1, 2, 3, 4 and 5

Ans: (b)

Mains:

Q. What are the main socio-economic implications arising out of the development of IT industries in major cities of India? **(2021)**

PDF Refernece URL: https://www.drishtiias.com/printpdf/deepfakes-in-elections-challenges-and-mitigation