



The Dark Side of AI: Deepfakes and the Rise of Fake News

Dr T Vembu¹, Srinivash M², Adithya Sajosh³

¹(Associate Professor Department of English Kongunadu College of Engineering and Technology)

²(Ist year AI&DS Kongunadu College of Engineering and Technology)

³(Ist year,CSE Kongunadu College of Engineering and Technology)

Abstract: As more and more fake news articles and videos go viral in today's time, making it difficult to know what to trust, an increasing number of experts have brought deepfakes onto the agenda. If you're not in the know, a "deepfake" is a fake based on deep learning, which uses techniques to create or change a video whose outcome is as near to reality as possible. Thanks to powerful software, deepfakes are making it increasingly difficult to tell whether the audio or the video is real or fake. Earlier, to get past the facial recognition security at a government office, two men just covered their faces with a piece of cloth. With the emergence of deepfakes, though, our images can be used for this without our knowledge. The new handcraft digital print studio can develop special pieces of handloom art by Important Digits, Jewellery and Handbags. The studio was officially opened by MD Archroma India Limited, Ms Archana Sanghi. According to you, the social media being bombarded with videos of actors and models grooving to inappropriate songs are deepfakes. We can consider what she says should be true as she is a reputed star. In reality they're just being.

Keyword: Bitcoin, Ethereum, Cryptocurrency Investment, Portfolio Diversification, Risk-Adjusted Returns, Institutional Adoption, Digital Assets

I. INTRODUCTION

In the last few years, artificial intelligence has leapt from the lab into our daily lives, quietly reshaping how we see and hear the world. Among its most troubling developments are deepfakes—videos or audio that imitate real people so convincingly that it's almost impossible to tell fact from fiction. Alongside them, AI-driven fake news spreads misinformation at a speed and scale that humans alone could never match. A recent survey by Pew Research shows that nearly three-quarters of adults across 25 countries see online false information as a serious threat. For journalists, educators, and everyday users, this is more than a technological curiosity—it is a challenge to trust itself.

How Deepfakes Are Made and Spotted

Deepfakes are not magic; they are the result of sophisticated AI techniques. Generative Adversarial Networks, or GANs, pit two neural networks against each other: one generates images or sounds, while the other critiques them. Over time, this back-and-forth allows the AI to produce faces, voices, and even gestures that look disturbingly real. Today, anyone with a smartphone and an

app can swap faces in videos or mimic someone's voice convincingly, making deepfakes more accessible than ever.

Catching these forgeries, however, is a game of cat and mouse. Digital forensics teams look for tiny inconsistencies—slightly blurred edges, lighting that doesn't quite match, or subtle mismatches in eye movement. Tools like DARPA's SemaFor program use AI to flag manipulated media, while blockchain or watermarking systems can help trace content to its origin. Still, even the best systems struggle to keep pace. For many ordinary viewers, the line between real and fake has already blurred.

Real-World Consequences

The danger of deepfakes is not theoretical—it has already hit hard in corporate, political, and personal realms.

Corporate Scams

In Hong Kong in 2024, an executive at Arup, an engineering firm, was duped into wiring HK\$200 million (~£20 million) to criminals after a deepfake video call impersonated senior managers. Meanwhile, the CEO of WPP, a global advertising giant, received a fraudulent



email paired with a cloned AI voice. These incidents show that even experienced professionals can fall victim to AI-powered deception. Experts predict that such scams could escalate U.S. corporate losses from \$12.3 billion in 2023 to \$40 billion by 2027.

Political Manipulation

Politics, too, has felt the impact. In early 2026, a Republican campaign released a video showing Texas Democrat James Talarico making inflammatory statements he never actually said. Similarly, a deepfake mocking Georgia Senator Jon Ossoff circulated widely. By blurring truth and fiction, AI can manipulate public opinion and weaken democratic processes. Scholars warn that such content risks creating widespread distrust in elections and institutions.

Social and Personal Harm

Deepfakes have also found their way into schools, social networks, and even homes. Students have used them to target classmates and teachers, sometimes in explicit or harassing videos, forcing schools to rethink anti-bullying policies. Deepfake pornography is now a documented problem, harming reputations and mental health. Criminals can even use voice cloning to impersonate loved ones in emergency scams, convincing victims to send money. Medical misinformation has emerged as well, with deepfake videos of doctors promoting fake treatments, shaking public confidence in healthcare.

Repeated exposure to fabricated media can create the “illusory truth effect”—people start to believe repeated lies, and eventually even real evidence can be dismissed as fake, a phenomenon experts call the “liar’s dividend.”

How Society Is Responding

Governments, tech platforms, and educators are trying to stay ahead of this growing problem.

Legal efforts are underway worldwide. The European Union’s Artificial Intelligence Act requires clear labeling or watermarking of AI-generated content. The Digital Services Act holds platforms accountable for online disinformation. In the United States, 28 states have passed laws requiring disclosure of AI-generated political content, and federal bills like the “No Fakes Act” aim to regulate election-related deepfakes. Other nations, including China and Australia, are introducing restrictions to curb AI-driven deception, such as limiting facial recognition and enforcing age restrictions on social media.

Platform policies are evolving as well. For Australia’s 2025 election, Meta pledged to label or remove deepfakes that violate rules, and independent fact-checkers now review suspicious content. Platforms increasingly tag “synthetic content,” helping users distinguish real media from manipulated versions.

Education and media literacy are crucial. UNESCO and other organizations stress the importance of critical thinking and ethical reasoning. Students, journalists, and civil servants are learning to recognize AI-generated content, question sources, and verify facts before trusting what they see or hear. In a world flooded with information, human judgment is becoming the most important line of defense.

Practical Steps for Everyone

While technology and law adapt, individuals can take proactive steps:

Verify Before Sharing: Check claims against trusted sources or fact-checking websites like Snopes and FactCheck.org.

Watch for Inconsistencies: Spot unusual lighting, awkward movements, or robotic voices. In live calls, ask unexpected questions or actions.

Use Platform Tools: Report suspicious posts, follow warning labels, and use verification plugins when available.

Promote Media Literacy: Encourage friends, family, and colleagues to critically evaluate online content.

Support Transparency: Advocate for clear labeling of AI content and stricter enforcement by platforms.

II. CONCLUSION

AI is a tool with enormous potential, capable of both creative innovation and significant harm. Deepfakes and AI-driven fake news challenge trust, security, and social cohesion. Technical safeguards, legal frameworks, and platform policies help, but education and critical thinking remain society’s strongest defense. By verifying information, questioning plausibility, and demanding accountability, individuals can uphold the integrity of public discourse. In today’s world, where “seeing and



hearing are no longer believing,” human judgment, skepticism, and ethical reasoning are more vital than ever.