Understanding the Impact of AI-Generated Deepfakes on Public Opinion, Political Discourse, and Personal Security in Social Media

Prakash L. Kharvi | Marymount University

With the rapid advancement in and easy accessibility of deepfake technology, there is much to comprehend about its impact on social media. This research aims to fortify trust, authenticity, and security in online communication and information sharing by analyzing deepfake impacts and scrutinizing existing strategies.

Artificial intelligence (AI) has revolutionized various facets of human life and brought transformative changes to numerous industries. However, it has also introduced new challenges and threats, one of the most notable being deepfakes. "Deepfakes" or "synthetic media" refer to the employment of manipulated digital content, such as hyperrealistic synthetic video, audio, images, or texts crafted using advanced AI techniques, to compromise targeted decision-making processes. The main epistemic threat is that deepfakes can easily lead people to acquire false beliefs.[1] This technology can fabricate information to such an extent that it becomes nearly indistinguishable from authentic material. This will influence operations targeting public opinion, social groups, political discourse, and personal as well as national security.[2]

The sophistication and prevalence of deepfakes have surged, primarily driven by advancements in AI and machine learning. These advanced tools can produce hyperrealistic manipulated videos or audio recordings that are almost impossible to differentiate from genuine content. The escalating popularity of deepfakes can be attributed to factors such as heightened media coverage, growing public awareness, and potential misuse in sectors like entertainment, politics, and even personal blackmail. Consequently, there is an urgent demand for technologies and strategies to detect and mitigate deepfakes, ensuring the integrity of digital content. A cursory analysis of search terms related to deepfakes reveals a worrisome focus on the tools facilitating their production. Google Trends shows a steady global uptick in searches for "deepfake," with a significant surge beginning in 2023, as shown in Figure 1.

Over the years, there have been significant instances of cyberthreat actors leveraging deepfake technology for cybercrime.

- In May 2018, a deepfake video appeared of former U.S. President Donald Trump advising Belgian citizens on

Digital Object Identifier 10.1109/MSEC.2024.3405963

Copublished by the IEEE Computer and Reliability Societies

criticizing their government for being part of the Paris Agreement on climate change.[3] This video created a political cover for others and restricted global efforts to cut carbon emissions.

- In September 2019, a malicious actor used audio deepfake technology to mimic an associate from a parent company, thereby deceiving the CEO of a U.K.-based organization. As a result, the CEO authorized a financial transfer of US$243,000.[4] This incident is the first recorded use of audio deepfakes in financial fraud.
- In November 2022, a Twitter user circulated a deepfake video featuring FTX founder Sam Bankman-Fried. The video falsely promoted a link for those impacted by FTX's collapse, offering free cryptocurrency as compensation. This was later exposed as a scam. More advanced giveaway scams are expected to be conducted in the near future, with a fake video of a famous person requesting donations for a giveaway in the video.[5]
- In March 2022, a Ukrainian news website was hacked to display a deepfaked video of Ukrainian President Volodymyr Zelenskyy calling for his people to surrender to Russian forces.[6] This indicates how deepfakes can propagate disinformation and manipulate public perception.
- In January 2024, a well-known incident of deepfake porn occurred when pornographic videos began circulating of Taylor Swift, a prolific songwriter.[7] Deepfakes create ethical and privacy issues that cause psychological impact to individuals, regardless of their public prominence or private status.

Deepfake Influencers

The rise of deepfake incidents has emphasized the following ideas:

- Public perceptions of deepfakes significantly influence individuals' attitudes and their capability to discern such content.
- Implementing a multipronged strategy, which includes improved detection, user education, partnerships, and legal frameworks, can effectively mitigate the spread and influence of deepfakes on social media.
- Public perceptions of deepfakes play a pivotal role in shaping individual attitudes and abilities to detect deepfakes.
- A holistic strategy involving various stakeholders and multiple approaches, such as improved technology and user awareness, is crucial to counteract the deepfake menace on social platforms.
- Current deepfake detection and mitigation strategies on social media have notable limitations. Existing technologies for deepfake detection may not effectively address cognitive biases influencing belief in deepfakes, necessitating alternative strategies.
- The spread of AI-generated content, including deepfakes, poses significant challenges to media literacy, fact checking, and trust in democratic processes. The integration of AI into democratic systems brings about heightened concerns regarding privacy, security, and political manipulation.

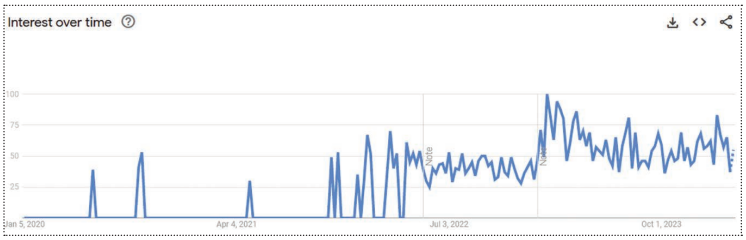

Figure 1. Google Trends data on "deepfake" since 2020. The interest in deepfake is increasing year by year.

Analysis

A study emphasizing the importance of a cybersecurity educated community sought to gauge public awareness and perceptions of deepfakes in the United States and Singapore.[8] The results indicate a need for a more comprehensive understanding and awareness of deepfakes among the public. The research utilized the third-person perception (TPP) theoretical framework, suggesting that individuals perceive others as being more susceptible to the effects of deepfakes than themselves. In essence, people believe that they are less likely to be influenced by deepfakes compared to others. The research further delved into individuals' self-assessments of their capability to detect deepfakes. Interestingly, participants generally believed they were more adept at recognizing the deceptive nature of deepfakes than their peers. The study highlighted that the perceptual gaps (differences in self-perception and others' perceptions) within the TPP are more pronounced among those with higher cognitive abilities. Such individuals are more inclined to believe that, while deepfakes can significantly sway others, they possess a superior ability to identify these manipulations. The results suggest that individuals with higher cognitive skills, especially those frequently encountering deepfakes, are better equipped to discern them and apply this discernment in real-world evaluations.

However, it is crucial to acknowledge the study's limitations. These include a reliance on a verbal ability test, a binary knowledge measure, and a sample already familiar with deepfakes. Such constraints affect the broader applicability of the findings. Further investigations are essential to better understand the interplay among cognitive ability, exposure to deepfakes, and their influence on genuine opinions.

Chesney and Citron (2019) found that deepfakes amplify the issue of misinformation in public debates.[9] They elevate the "fake news" phenomenon by producing highly realistic, yet deceptive, audio and video content. Such content can jeopardize the credibility of debate participants and erode the factual basis of policy discussions. Deepfakes diminish trust in both public and private institutions. Elected officials, judges, agencies, and other entities can be targeted, disseminating false and damaging content that becomes increasingly challenging to refute. This can intensify societal polarization and weaken confidence in pivotal institutions.

Additionally, deepfakes present threats to personal security. They can fabricate videos or audio recordings, falsely portraying individuals in actions or statements they never made. Such misrepresentations can tarnish reputations, lead to harassment, or provoke violence against those depicted. Deepfakes have systemic implications, jeopardizing democratic discourse, elections, institutional trust, and personal security on social media platforms. The study does not directly address the effectiveness of current detection and mitigation strategies against deepfakes on social media. The research suggests that, for detection software to remain effective, it must evolve in tandem with advancements in deepfake technology. Even with such advancements, the software might only mitigate systemic harms rather than eradicate them.

Kondamudi et al. (2023) discuss various aspects of fake news in social networks.[10] There is no direct mention of the influence of deepfakes on public opinion, political discourse, and personal security on social media. The study should have addressed the current strategies to counter deepfakes or how these gaps can be addressed. However, the study does mention the need for hybrid approaches and the potential of machine learning, deep learning, reinforcement learning, and blockchain-based models for more accurate outcomes in the future. Deep learning models, especially convolutional neural networks, have shown promise in detecting deepfakes. They can achieve high accuracy rates but require large amounts of labeled data for training. Moreover, as deepfake generation techniques improve, the performance of these models can degrade.

Lollia (2023) sheds light on the impact of deepfakes on public opinion, political discourse, and personal security within social media platforms.[11] Deepfakes present a formidable threat to societal security. They can be weaponized to spread misinformation and manipulate public sentiment, as observed during the 2016 U.S. elections. Furthermore, deepfakes can be crafted to concoct scandals, thereby damaging individuals' reputations and violating their privacy. The swift proliferation of these videos on social platforms magnifies their potential repercussions, posing a considerable challenge for lawmakers, social media entities, and the broader society. This scenario emphasizes the urgent need for increased vigilance and regulatory measures. Deepfakes employ AI techniques to craft compelling videos depicting individuals engaging in actions or utterances they never actually performed. This technology harnesses machine learning and neural networks to superimpose images and voices, culminating in manipulated video content. A notable instance of a deepfake is the viral video featuring former U.S. President Barack Obama, crafted by comedian Jordan Peele. Obama utters statements that he never actually made.

Rayhan and Rayhan (2023) highlight the potential dangers deepfakes and AI-generated content pose in politics and public opinion.[12] The ease with which this content can be disseminated across social media platforms raises severe concerns about the authenticity of information presented to the public. The challenge lies in identifying and debunking these sophisticated falsehoods to ensure the integrity of democratic processes and institutions. The study touches upon the challenges posed by deepfakes and AI-generated content. However, the specific effectiveness of current detection and mitigation strategies against deepfakes on social media needs to be explicitly detailed in the provided excerpts.

People are often motivated to believe information that aligns with their identities and beliefs, a phenomenon known as *motivated reasoning*. This is particularly evident in the context of political and social identities. According to Thaler (2024), individuals engaged in motivated reasoning will have more trust in news that aligns with their preexisting beliefs.[13] If their reasoning is politically motivated, they will see messages that support their political party as more credible and view opposing messages as less credible. Deepfake amplifies the problem by manipulating visual and auditory content to appear genuine. The believable deepfake may rate as being slightly more credible than an authentic video of the politician's speech, suggesting that the perceived credibility of deepfakes depends heavily on their alignment with the political actor's known beliefs.[14] This capability can effectively deceive viewers more than traditional misinformation, resulting in manipulating public opinion.

Sloane et al. (2022) highlight the impact of AI systems on marginalized communities.[15] There is a lack of real participation in developing AI systems, and it requires a much stronger involvement of the social sciences and humanities. AI systems often reflect societal biases, which can further marginalize vulnerable groups. Deepfakes can exacerbate these issues by creating synthetic media to discredit or otherwise harm individuals from these communities. The harms of deepfakes are not just about the technology itself

but are closely linked to existing social injustices and the marginalization of certain groups.[16] It is imperative to design AI inclusively and fairly, considering its impact on all communities, especially those already marginalized.

Van Bavel et al. (2024) have highlighted a distinction between how people believe information and how they share it.[17] Identities influence how people process information and play a role in believing and spreading misinformation. People can recognize misinformation as false but still share it regardless of its truth. Social identity goals and norms drive sharing and affect sharing directly and indirectly through beliefs.

General Findings

The "2023 State of Deepfakes" report, published by Home Security Heroes, offers a detailed examination of the current landscape of deepfake technology. This analysis is derived from an extensive study that includes 95,820 deepfake videos, 85 dedicated channels across multiple online platforms, and more than 100 websites associated with the deepfake ecosystem.[18] There has been a 550% increase in deepfakes online since 2019, as illustrated in Figure 2. This increase underscores the growing sophistication of deepfake technologies and the pressing need for improved detection and mitigation strategies to combat the spread of manipulated media.

The findings describe deepfakes as manipulated videos or images that convincingly mimic reality. They assert that deepfakes can significantly influence public opinion, political discourse, and personal security on social media. The review emphasizes that the spread of deepfakes can diminish trust in media and institutions, intensifying the polarization of political perspectives. The literature underscore the personal security threats posed by deepfakes, noting their potential use for harassment, bullying, and nonconsensual pornography. They also highlight deepfakes' challenges to verification processes, particularly within financial institutions, and discuss their potential role in facilitating criminal activities. The literature acknowledges the stringent legislation introduced by governments and the moderation policies enforced by social media platforms in response to deepfake-related risks. It concludes that enhancing public awareness is crucial in mitigating the threats posed by deepfakes.

Furthermore, it delves into the limitations of current detection and mitigation strategies, spotlighting challenges related to cognitive biases and the integration of technological solutions. It also provides a broader context on AI-generated content and deepfakes, underscoring their ramifications for democratic systems, political manipulation, and associated ethical dilemmas.

Common Themes

Several common themes emerge after analyzing the preceding studies from the literature review. A recurring theme is the influence of deepfakes on public perceptions, individual attitudes, and the ability to discern manipulated content. Challenges are tied to detecting and mitigating deepfakes, particularly as the technology behind deepfakes evolves. A consistent theme across the research is the critical role of user education and awareness. The studies stress the importance of informing users about the existence, dangers, and identification methods for deepfakes. The importance of creating partnerships, sharing resources, and setting industry standards is highlighted. It underlines the need to develop legal structures and policies that address the creation, dissemination, and evil use of deepfakes. The role of fact-checking initiatives in verifying media content authenticity is also highlighted.

Mitigating the Deepfake Problem

With the rise of synthetic media content along with generative AI, there is a need to protect trustworthy content creators and content consumers. There is a need to establish trust in digital content between these two personas.

Implement Digital Watermarking

There must be a standard for content creators to watermark their software digitally. "Digital watermarking" refers to the process of concealing or embedding data behind an image or video that is invisible to the naked human eye.[19] Content creators must digitally watermark every piece of content their software produces, whether video, audio, images, or text. Table 1 shows the types of digital watermarking techniques that have evolved over time that content creators can use to protect the

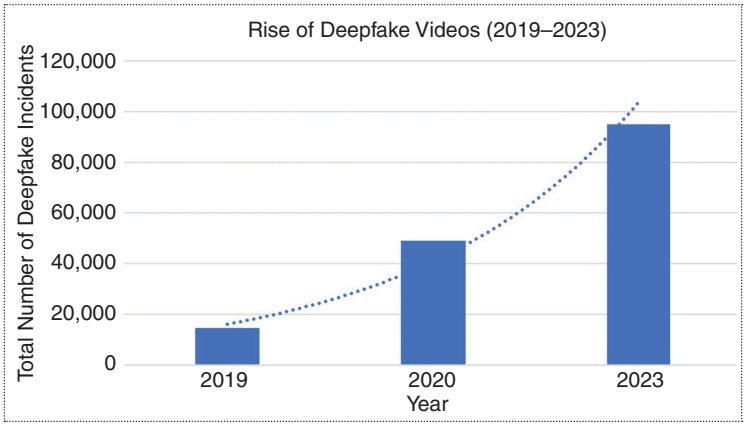

Figure 2. Deepfake incidents (2019–2023). The number of deepfake incidents is expected to increase in the coming years.

integrity of their content. Digital watermarking also protects the content from robust attacks and allows easy downstream detection.

Authenticate Real Digital Content Using the Coalition for Content Provenance and Authenticity

Apart from understanding ways to mitigate harm from synthetic media, there should be a call on how to authenticate accurate and trusted digital content. With the help of the Coalition for Content Provenance and Authenticity (C2PA), downstream consumers can certify the source and history of content.[20] The C2PA is an open source effort to build a specification that allows the devices of content creators, at the point of recording, to log the date, time, and location of all pixels, which are recorded and cryptographically signed into a compact signature. That signature is then put into an immutable ledger, such as blockchain. When the content leaves that device, it goes to social media and shows up to the consumer. The consumer device can return to the ledger and validate the digital content.

Blockchaining Social Media Platforms

Many social media platforms are centralized, necessitating a regulatory framework to integrate these platforms into blockchain networks. Such platforms should operate as part of a distributed ledger, enhancing transparency, trust, and data security, as illustrated in Figure 3. Beyond exploring methods to mitigate harm from synthetic media, it is imperative to address the authentication of accurate and trustworthy digital content. The C2PA aids downstream consumers in verifying the source and history of content and determining the authenticity of images, videos, or text. C2PA is an open source initiative aiming to develop a standard that enables the devices of content creators to log details, such as date, time, location, and a cryptographically signed record of all pixels at the point of recording, embedding these data into a compact signature stored on an immutable ledger like blockchain. Content creators are thus empowered to distribute digital content across social media platforms on blockchain networks, incorporating watermarking techniques and C2PA metadata. When content consumers access this digital content through transaction submissions in the ledger, these transactions are verified within the peer-to-peer network. New blocks are added to the existing blockchain, ensuring that transactions are completed with verification according to C2PA specifications.

Now, What Should We Do About the Bad Actors?

In today's world, there are no restrictions on creating synthesized media, nor is there guidance to prevent bad actors from producing deepfake content. Bad actors need access to cloud computing services to develop and deploy deepfake content. To minimize the risks posed by such actors, cloud service providers should take steps to limit their Internet access.

Observations and Key Issues

We recognize the following concerns:

- The human psyche's vulnerability to deepfakes means people can be easily influenced or deceived, making discernment difficult. This affects both public perception and individual attitudes.

Table 1. Types of digital watermarking techniques based on embedding digital content domains.[19]

Type	Usage
Invisible watermarking	Used for content authentication, tracking, and copyright protection
Fragile watermarking	Used for tamper detection, authentication, and integrity of digital content
Robust watermarking	Used to trace unauthorized distribution, employ copyright protection, and content authentication
Spatial-domain watermarking	Used to modify the pixel values of the digital content to embed the watermark
Frequency-domain watermarking	Used to modify the frequency components of the content to embed the watermark
Quantization-based watermarking	Used to adjust quantization levels of the digital content while minimizing perceptual distortion

- The continuous evolution of deepfake technology challenges the effectiveness of detection tools and methods. As creators enhance their strategies, detectors are in a perpetual race to keep up.
- Despite the growing menace of deepfakes, many individuals remain uninformed about their existence, the potential harm they can cause, and how to identify them.
- The battle against deepfakes requires a concerted effort from tech companies, social media platforms, policymakers, and users. Fragmented approaches may lack efficacy in addressing the multifaceted challenges posed by deepfakes.
- All social media platforms are required to adhere to the C2PA technical specification, which includes metadata. The current practice of stripping off the metadata results in a lack of effective downstream detection capability.
- Existing legal and regulatory frameworks may not fully address the nuances and ramifications of deepfake technology, creating potential loopholes for malicious actors.
- Relying solely on technological solutions like detection algorithms may not be sufficient, especially as deepfake creation methods evolve. A comprehensive approach that includes policy measures, public awareness, and robust verification methods is needed to effectively combat the threat of deepfakes.
- Traditional fact-checking methods may be insufficient to tackle the challenges posed by deepfakes, necessitating new tools and methodologies.
- Deepfakes can erode public trust in democratic institutions and processes, potentially manipulating political discourse and influencing elections, leading to societal discord.
- The use and spread of deepfakes present profound ethical challenges, especially when they infringe on personal privacy or are used to disseminate misinformation, challenging the fundamental principles of truth and authenticity in the digital era.

Future Research

Addressing the challenges posed by deepfakes necessitates a comprehensive approach. Future research advocates establishing a trusted framework between content creators and consumers. A framework should integrate social media platforms into the blockchain network to ensure transparency, data security, and foster partnerships. All stakeholders, including content creation companies, researchers, social media entities, and policymakers, should collaborate to share insights and best practices. Additionally, an agreement among governments and social media platforms should be reached to adopt C2PA specifications and include metadata for effective downstream detection. Governments and international bodies should collaboratively draft regulations that

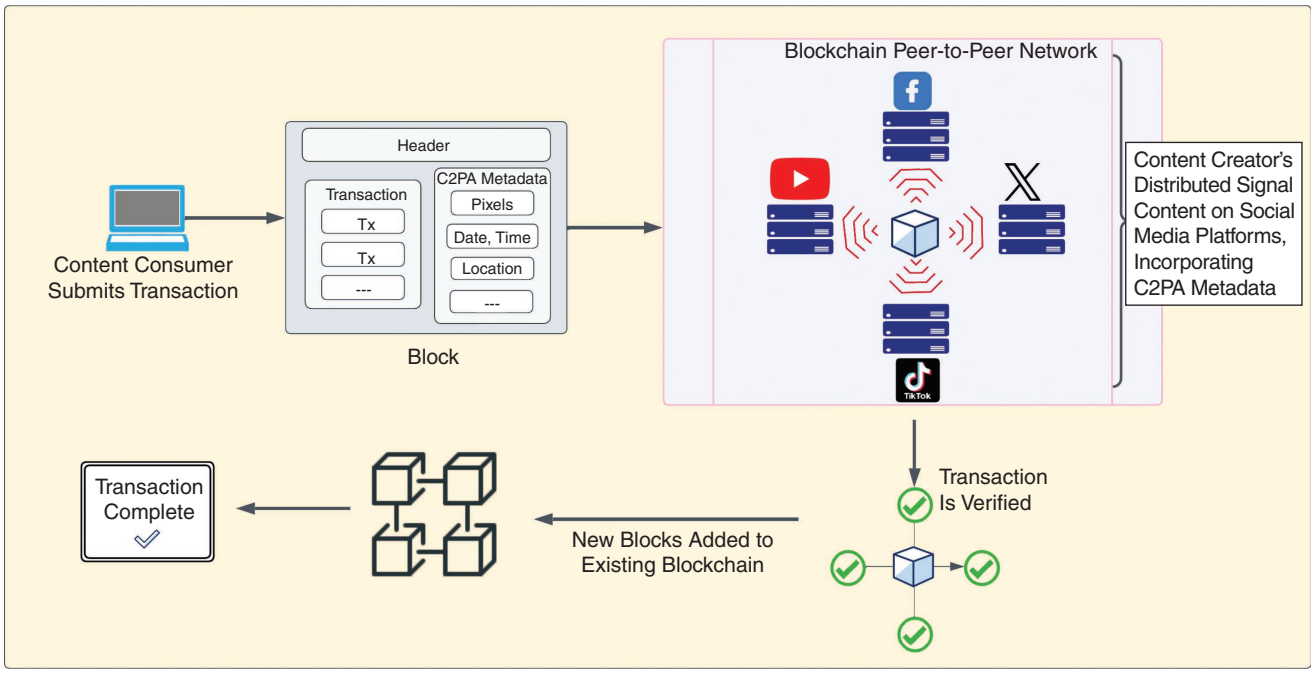

Figure 3. The decentralization of social media platforms with the intent to protect and validate content creators' media. Downstream consumers can certify the source using C2PA metadata. Tx: transmission.

address the challenges and ethical implications of deepfakes.

Research should be focused on how to promote the creation of open source tools and platforms where researchers and developers can collaborate on deepfake detection and mitigation techniques. Platforms should have easy-to-use interfaces that allow users to report suspected deepfakes. People should also advocate for creating global standards that define the ethical creation and dissemination of synthetic media. There should be research on establishing a network of fact checkers globally to verify the authenticity of viral content quickly. News outlets should partner with fact checkers and technologists to ensure the dissemination of accurate information.

The rapid evolution and proliferation of deepfakes present a multidimensional challenge with significant societal implications. These artificially crafted media pieces can easily manipulate individual and collective perceptions, putting trust in democratic processes, personal privacy, and media authenticity at risk. At the core of this challenge is a cognitive vulnerability in humans, making them susceptible to misinformation. This vulnerability is further exacerbated by a lack of widespread awareness and education on deepfakes, underscoring the importance of enhancing public knowledge about them. The technological arms race, wherein detection methods continually try to catch up with ever-evolving deepfake creation techniques, further complicates the issue. Relying solely on technology to detect and mitigate deepfakes isn't a comprehensive solution. Legal and policy measures need to evolve, closing potential loopholes and penalizing malicious use.

Furthermore, multistakeholder collaboration is paramount. Tech companies, social media platforms, policymakers, fact checkers, and users must all work together to devise holistic strategies. Deepfakes represent a formidable challenge in the digital age, intertwining technological, psychological, societal, and ethical aspects. Addressing this threat requires a concerted, multifaceted approach encompassing public awareness, technological innovation, policy formulation, and cross-industry collaboration. ■

References

1. D. Fallis, "The epistemic threat of deepfakes," *Philos. Technol.*, vol. 34, no. 4, pp. 623–643, Dec. 2021, doi: 10.1007/s13347-020-00419-2.
2. M. E. Bonfanti, "The weaponisation of synthetic media: what threat does this pose to national security?" Elcano Royal Institute, Madrid, Spain, 2020. [Online]. Available: https://media.realinstitutoelcano.org/wp-content/uploads/2021/11/ari93-2020-bonfanti-weaponisation-of-synthetic-media-what-threat-does-this-pose-to-national-security.pdf
3. M. Chawki, "Navigating legal challenges of deepfakes in the American context: A call to action," *Cogent Eng.*, vol. 11, no. 1, Dec. 2024, Art. no. 2320971, doi: 10.1080/23311916.2024.2320971.
4. N. Kshetri, J. F. DeFranco, and J. Voas, "Is it live, or is it deepfake?" *Computer*, vol. 56, pp. 14–16, Jul. 2023, doi: 10.1109/MC.2023.3252059.
5. I. Vakilinia, "Cryptocurrency giveaway scam with Youtube live stream," in *Proc. IEEE 13th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, New York, NY, NY, USA: IEEE, Oct. 2022, pp. 0195–0200, doi: 10.1109/UEMCON54665.2022.9965686.
6. J. Twomey, D. Ching, M. P. Aylett, M. Quayle, C. Linehan, and G. Murphy, "Do deepfake videos undermine our epistemic trust? A thematic analysis of tweets that discuss deepfakes in the Russian invasion of Ukraine," *Plos One*, vol. 18, no. 10, Oct. 2023, Art. no. e0291668, doi: 10.1371/journal.pone.0291668.
7. T. Goss, Deepfakes and Societal Impacts. 2024. doi: 10.13140/RG.2.2.12829.49128.
8. N. Ahmad, P. A. Laplante, J. F. DeFranco, and M. Kassab, "A Cybersecurity Educated Community," *IEEE Trans. Emerg. Topics Comput.*, vol. 10, no. 3, pp. 1456–1463, Jul./Sep. 2022, doi: 10.1109/TETC.2021.3093444.
9. B. Chesney and D. Citron, "Deep fakes: A looming challenge for privacy, democracy, and national security," *California Law Rev.*, vol. 107, no. 6, pp. 1753–1820, 2019.
10. M. R. Kondamudi, S. R. Sahoo, L. Chouhan, and N. Yadav, "A comprehensive survey of fake news in social networks: Attributes, features, and detection approaches," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 6, Jun. 2023, Art. no. 101571, doi: 10.1016/j.jksuci.2023.101571.
11. F. Lollia, "At the heart of social networks: influence, disinformation and societal risk," Jun. 2023. Accessed: Aug. 06, 2023. [Online]. Available: https://hal.science/hal-04134028
12. S. Rayhan and S. Rayhan, "The Role of AI in Democratic Systems: Implications for Privacy, Security, and Political Manipulation," 2023. doi: 10.13140/RG.2.2.31121.61281.
13. M. Thaler, "The fake news effect: Experimentally identifying motivated reasoning using trust in news," *Amer. Econ. J., Microecon.*, vol. 16, no. 2, pp. 1–38, May 2024, doi: 10.1257/mic.20220146.
14. M. Hameleers, T. G. L. A. van der Meer, and T. Dobber, "Distorting the truth versus blatant lies: The effects of different degrees of deception in domestic and foreign political deepfakes," *Comput. Human Behav.*, vol. 152, Mar. 2024, Art. no. 108096, doi: 10.1016/j.chb.2023.108096.
15. M. Sloane, E. Moss, O. Awomolo, and L. Forlano, "Participation is not a design fix for machine learning," in *Proc.*

2nd ACM Conf. Equity Access Algorithms, Mechanisms, Optim., Arlington VA USA: ACM, Oct. 2022, pp. 1–6, doi: 10.1145/3551624.3555285.

16. J. Habgood-Coote, "Deepfakes and the epistemic apocalypse," *Synthese*, vol. 201, no. 3, Mar. 2023, Art. no. 103, doi: 10.1007/s11229-023-04097-3.
17. J. J. Van Bavel, S. Rathje, M. Vlasceanu, and C. Pretus, "Updating the identity-based model of belief: From false belief to the spread of misinformation," *Current Opinion Psychol.*, vol. 56, Apr. 2024, Art. no. 101787, doi: 10.1016/j.copsyc.2023.101787.
18. "2023 state of deepfakes: Realities, threats, and impact." Home Security Heroes. Accessed: Mar. 11, 2024. [Online]. Available: https://www.homesecurityheroes.com/state-of-deepfakes/#key-findings
19. A. Palani and A. Loganathan, "Digital image and video watermarking: Methodologies, attacks, applications, and future directions," *Multimedia Tools Appl.*, vol. 83, pp. 1–61, Jun. 2023, doi: 10.1007/s11042-023-15806-y.
20. R. K. Hill and C. Baquero, "Pondering the ugly underbelly, and whether images are real," *Commun. ACM*, vol. 67, no. 3, pp. 8–10, Mar. 2024, doi: 10.1145/3639711.

Prakash L. Kharvi is pursuing a doctor of science degree in cybersecurity from Marymount University, Arlington, VA 22207 USA. His research interests include security in artificial intelligence and machine learning, security and privacy in the metaverse, and detection and mitigation of deepfake technologies. Kharvi received a master of professional studies in cybersecurity from Fort Hays State University. He is a Graduate Student Member of IEEE. Contact him at plk78754@marymount.edu.