Issues in Information Systems
Volume 26, Issue 4, pp. 183-194, 2025

DOI: https://doi.org/10.48009/4_iis_2025_116

Exploration of AI synthetic media and deepfake: understanding the technologies, detection software, legislation, initiatives, and curriculum

Loreen Powell, *Marywood University, lpowell@maryu.marywood.edu*
Carl Rebman, Jr., *University of San Diego, carlr@sandiego.edu*
Hayden Wimmer, *Georgia Southern University hwimmer@georgiasouthern.edu*

Abstract

Existing research regarding deepfakes has largely concentrated on the technical and legal aspects. As a result, public awareness of deepfakes amongst Americans remains limited. This research employed a qualitative desk/documentary research method to provided comprehensive exploration of the current literature focusing on artificial intelligence (AI)synthetic media with knowledge of the technologies, detection software tools, legislation, organizational initiatives, and higher education resources. It also examined the extent to which deepfake and AI synthetic media content is incorporated into business curricula across 70 AACSB and ACBSP-accredited institutions in Pennsylvania. Specifically, business courses within the course catalogs were reviewed using keyword searches for "deepfakes" and "AI synthetic media". The analysis revealed that none of the institutions offered business courses explicitly addressing these topics. Although some referenced AI or machine learning, no course content appeared to engage with the ethical, legal, or operational challenges of synthetic media. This research has practical implications for organizations, educational institutions, business instructors, and students wanting to learn more about deepfakes.

Keywords: AI synthetic media, deepfakes, business, legislation, initiatives, curriculum

Introduction

Today's deepfakes are artificial intelligence (AI) synthetic media tools used to manipulate, replace, or create highly realistic visual and audio content which does not occur in reality (Agarwal & Farid, 2021; U.S. Homeland Security, 2022; Stanford University IT, 2023; West, 2021). While doctored imagery is neither new nor rare (Rana et al., 2022; Chesney & Citron, 2019; Horaczek, 2017), the heightened interest and usage is primarily attributed to technological advancements within AI (Rana. et al, 2022).

AI-generated deepfakes pose increasing detection challenges due to the sophistication of generative models like GANs and diffusion models, which produce highly realistic visual, audio, and textual content. Detection systems struggle to keep pace with deepfake generation because deepfakes continue to evolve and bypass improvements in detection. In addition, limited training data, poor generalizability, and the emergence of cross-modal deepfakes also further reduce detection accuracy (Das et al., 2023). The widespread availability of low-cost deepfake tools allows individuals with minimal technical skills to create highly convincing synthetic content, increasing the risk of misuse in misinformation, identity theft, and

political manipulation (Rousay, 2023; Wang, 2024). As a result, it underscores how advancements in AI both enhance deepfake realism and weaken existing safeguards.

The ability to convincingly fabricate evidence, such as creating fake videos of public figures or manufacturing false narratives, poses a serious threat to trust in media and online content for individuals and businesses (Rana. et al, 2022). However, Sidoti and Vogels (2023) reported that Americans' understanding of deepfakes is still very limited. Amongst their research conducted by Pew Research Center, they specifically report that only 42% of Americans self-reflected that they know what a deepfake is. However, this statistic changes based upon education and age. Americans with college education and under the age of 30 tend to have more awareness regarding deepfakes whereas those with a high school education or over 65 years of age have little to no knowledge about deepfakes. Hence the need for continued educational awareness regarding deepfakes.

Additionally, Roe et al. (2024) examined 182 scholarly publications on deepfakes and was able to find three areas of focus such as detection methods, malicious applications, and potential benefits. They also highlighted potential positive uses of deepfakes and synthetic media in education but found consistent gaps in literature with regards to integrating deepfakes into higher education curriculum. To our knowledge there has not been a research study on whether business curriculums within higher education institutions have a course which focuses on deepfakes. The goal of this research is to provide comprehensive exploration of the current literature focusing on AI synthetic media with knowledge of the technologies, detection software tools, legislation, organizational initiatives, and higher education resources. Additionally, this research will investigate course descriptions of universities from AACSB and Accreditation Council for Business Schools and Programs (ACBSP) regarding their focus on deepfakes or AI synthetic media within their business curriculum. Based upon the results, we provide actionable recommendations for higher education Institutions to incorporate into their curriculum.

The format of this study is as follows. First is a discussion relevant literature review followed by the methodology. Next is a discussion of higher education resources, organizational and legislation issues. The discussion is followed by the results of deepfake technology and detection tools, as well as actionable recommendations. The last two sections are the conclusion followed by imitations and future research possibilities.

Literature Review

Initially, victims of doctored imagery often knew the individual behind the creation of the altered content. In many cases, these manipulations stemmed from personal motivations such as revenge or a failed relationship, where the intent was typically to embarrass or harm an individual personally. These types of incidents were frequently localized to personal conflicts, and the scale of the harm was often limited. However, the landscape of doctored imagery has evolved significantly in recent years. Today, deepfakes represent a far broader and more alarming category of emerging cybercrimes affecting organizations. The advent of advanced technology, particularly AI, has not only accelerated the creation of such content but has also made the tools for generating these forgeries widely available to the public. As a result, deepfakes are no longer confined to personal vendettas or isolated instances; instead, they have become a tool for larger, more dangerous forms of exploitation amongst organizations (Rana et al., 2022, Rousay, 2023; Vig, 2024; Wang, 2024).

In 2019, the CEO of an unnamed UK-based energy firm was targeted for fraud involving voice cloning technology. Specifically, AI was used to mimic the voice of the company's German parent firm's chief executive, instructing the UK CEO to transfer around $243,000 to a Hungarian supplier. Unfortunately, the

UK CEO thought the request was real and authorized the transfer. The bad actors made three phone calls to the UK CEO before anything became suspicious (Damiani, 2019).

Nguyen et al. (2021) argued that deepfakes are contributing to a crisis of trust in media, where visual confirmation no longer assures authenticity. They believed the implications are profound, extending beyond skepticism to encompass significant societal impacts. Individuals and organizations targeted by malicious deepfakes face distress and potential harm, while these fabricated media can exacerbate disinformation or fraudulent activity, amplify hate speech for many organizations. For example, cybercriminals tricked a finance professional into transferring $25 million by impersonating a CFO via video call. In another case, within three months of time eight stolen IDs were used in Hong Kong to file 90 loan applications and open 54 bank accounts (Chen & Magramo, 2024).

Similarly, Westfall (2024) also reported that deepfakes pose a significant malicious threat to businesses, individuals, and governments. Current AI-generated deepfakes, particularly those featuring Elon Musk, are being leveraged to deceive consumers, resulting in an estimated loss of $12 billion in global fraud. Furthermore, it is projected that fraud losses linked to AI deepfakes will more than triple to $40 billion within the next three years. As a result, businesses, individuals, educational institutions, and governments must begin to develop mitigation strategies, robust technological solutions and legislation, and educational awareness to detect and protect themselves against deepfake threats.

Methodology

This research has two goals. The first goal of this research is to provide comprehensive exploration of the current literature focusing on AI synthetic media with knowledge of the technologies, detection software tools, legislation, organizational initiatives, and higher education resources. Thus, this research employed a qualitative desk/documentary research methodology. Public secondary data which heavily focused upon existing published research studies, relevant US laws and regulations, current software tools, and curriculum resources were used to provide condensed collections and summary tables. This study chose a qualitative desk/documentary method due to its effectiveness in analyzing institutional documents, course catalogs, and policy standards related to AI synthetic media in higher education. This approach is appropriate for identifying patterns, gaps, and representations within existing curricular materials without requiring direct interaction with participants (Bowen, 2009).

The second goal of this research is to investigate course descriptions of universities from AACSB and Accreditation Council for Business Schools and Programs (ACBSP) regarding their focus on deepfakes or AI synthetic media within their business curriculum. Consequently, this research conducted a systematic analysis of course descriptions of Business classes from AACSB and Accreditation Council for Business Schools and Programs (ACBSP) throughout Pennsylvania (PA). Publicly available secondary data from the AACSB and ACBSP websites were used to provide a list of schools within PA. Next, publicly available secondary data from each university's course catalog regarding the business curriculum was downloaded into a Microsoft Excel file. Once all files were downloaded a simple word search was completed on the data. Specifically, the author's searched for the following two terms: "deepfakes" and "AI synthetic media". Results were tallied and summarized.

Discussion and Results

The rapid development of deepfake technology, fueled by AI, has had profound implications for cybersecurity and privacy. In the past, creating high-quality doctored imagery or videos required a high

level of technical expertise, limiting its use to a small group of individuals or specialized professionals. However, the situation has dramatically changed due to the proliferation of easily accessible and user-friendly tools (Rousay, 2023; Wang, 2024).

A simple google search for free deepfake software immediately yielded over 10 free or open-source software tools for creating deepfakes. Popular open-source tools like DeepFaceLab, and FaceSwap which require little technical skills are readily available for anyone to use. Thus, the widespread accessibility and user-friendly tools and software for deepfake creation has made it possible for individuals with minimal technical expertise to generate sophisticated forgeries, raising significant concerns about potential misuse in misinformation, identity theft, and political manipulation (Chesney et al., 2019). Table 1 provides a list of the top five deepfake software tools that can be easily accessed and used.

Table 1. Deepfake Software Tools

Name	URL	Cost
FaceApp	https://github.com/topics/faceapp	Free – Open Source
Faceswap-GAN	https://github.com/shaoanlu/faceswap-GAN	Free – Open Source
DFaker	https://github.com/dfaker/df	Free – Open Source
DeepFaceLab	https://github.com/iperov/DeepFaceLab	Free – Open Source
HeyGen	https://www.heygen.com/	Free & Plans ranging from $24 - $69/month
Synthesia	https://www.synthesia.io/?r=0	Free & Plans ranging from $18 - $64/month
Veed	https://www.veed.io/tools/ai-video	Free & Plans ranging from $12-29/month

This democratization of deepfake technology, combined with its affordability, means that anyone with internet access and a computer can generate sophisticated manipulations of some sort of reality (Vig, 2024). While there are some instances where the deepfake software can be detected as not realistic, it is important to note that technological advancements are occurring within the sector.

Deepfake Detection

Particularly, generative adversarial networks (GANs), which consist of two neural networks, the generator and the discriminator, compete to produce increasingly realistic images or videos. The generator network creates fake data, while the discriminator network evaluates its authenticity. It is this adversarial relationship which drives the generator to produce increasingly convincing images or videos, while the discriminator becomes better at identifying fakes (Goodfellow et al., 2014). As a result of iterative process, deepfakes have evolved to the point where it is extremely difficult to distinguish them from real media content (Agarwal et al., 2021b). Additionally, AI-generated deepfakes further compound the challenges to accurately detect deepfakes (Das et al., 2023).

Today many technological detection solutions are focusing on identifying inconsistencies or anomalies that may not be evident through simple observation. Researchers are developing tools that can watermark digital media to verify its authenticity and trace its origins (Rana et al, 2022; Nguyen et al., 2021). To summarize existing deepfake detection methodologies, Rana et al. (2022) conducted a systematic literature review of 112 articles published between 2018 and 2020. They categorized the detection approaches into four main types: deep learning-based techniques, classical machine learning methods, statistical approaches, and blockchain-based solutions. Deep learning models, for instance, are commonly trained to detect subtle visual artifacts—such as irregular blinking, unnatural facial movements, or lighting inconsistencies—that may indicate manipulation (Matern et al., 2019). Biometric-based methods also play a key role in analyzing physiological features to distinguish genuine from altered content (Agarwal et al., 2019, 2021b). Another

line of research focuses on identifying the unique "fingerprints" left by different generative models (Yang et al., 2019). Additionally, Verdoliva (2020) proposed the use of blockchain technology to establish immutable records that verify media authenticity.

Despite these advancements, detection methods often fuel the development of more sophisticated deepfakes, as detection and generation technologies continue to evolve in a mutually adversarial cycle (Agarwal et al., 2021b). Thus, the creation of robust technological solutions for detecting deepfakes is very challenging (Das et al., 2023). Currently, reverse image search is a widely used tool for verifying the authenticity of suspicious images or videos. By uploading a screenshot to platforms like Google's reverse image search, users can check for matches online. Identical results may support the content's authenticity, while discrepancies can indicate manipulation. However, more effective use of this tool depends on future improvements in search result accuracy and quality (Helmus, 2022). Table 2 provides the top 3 trending technology detection tools used to help identify deepfakes.

Table 2. Trending Technology Detection Tools Used to Help Identify Deepfakes

Tool	Cost	URL
FaceForensic	Free – Open Source	https://github.com/ondyari/FaceForensics
Sentinel	Fee based	https://thesentinel.ai
Witness Media Lab	Free – Website of Recommended Verification Tools	https://lab.witness.org/portfolio_page/verification/

Realistically, there are no technological solutions available to stop deepfakes, it is crucial to aid in digital literacy to individuals, organizations, and the public (U.S. Department of Homeland Security, 2022). A study by Vaccari and Chadwick (2020) utilized a mixed-methods approach consisting of an experimental design where participants were exposed to both authentic and deepfake videos, a survey, and educational training on digital literacy and critical thinking skills regarding deep fake detection. Since their research focused on the impact of deepfakes on political engagement, trust, and the effectiveness of educational interventions, the Jordan Peele deepfake video regarding United States Former President Barack Obama was used. A diverse population of 2,005 adults participated in the study. One of the many things their study found was that exposure to educational materials regarding deepfakes enhanced participants' ability to discern fake from real videos, thereby reducing their susceptibility to misinformation.

Legislation

A major problem for business leaders is maintaining trust and credibility with all constituents. For example, in business, the foundation of effective collaboration often relies on confidence in both messages and messengers. As deepfakes continue to escalate, seeing (or hearing) is no longer believing instead, trust must be viewed with skepticism until it is verified as a credible source. Currently, it is reported that the best deepfake detection tools only have success identifying deepfakes 75% of the time (Westfall, 2024). Thus, government help is still needed. In fact, many celebrities effective by deepfakes have been pushing for legislation to help stop and protect individuals against deepfake misuse (Gold, 2025).

There are some significant U.S. federal legislation or legal frameworks which address individual or organizational misuse of deepfakes are amid development or approval. For example, there are four well known U.S. federal initiatives such as the Take It Down Act, the No AI Fraud Act, the Deepfakes Accountability Act, and the Disrupt Explicit Forged Images and Non-Consensual Edits (DEFIANCE) Act. However, only some of these initiatives have passed through both chambers of Congress. Therefore, the lagging legal framework presents a challenge for many effected individuals and organizations looking for some legal actions and consequences for the misuse of deepfake technology (Chesney et al., 2019b; Owen, 2024). As a result, within the United States (US), a few states have individually enacted legislation aimed to protect individuals' privacy, uphold the integrity of electoral processes, and prevent the spread of harmful

misinformation (Alanazi et al., 2024). For example, Texas enacted SB 751 (2019) which makes use of deepfakes for deceptive purposes in an election a legal crime (Texas Legislature Online, 2019). Currently, there are many proposed legislations. As a result, it is important to keep track of the process of the proposed legislation within each state. Table 3 contains a list of three popular Deepfake legislation trackers.

Table 3. Deepfake Legislation Trackers

Name of Legislation Tracker	URL
Ballotpedia AI Deepfake Legislation Tracker	https://legislation.ballotpedia.org/ai-deepfakes/overview
Public Citizen's Deepfake Legislation Tracker	https://www.citizen.org/article/tracker-intimate-deepfakes-state-legislation
National Conference of State Legislatures (NCSL) Tracker	https://www.ncsl.org/technology-and-communication/deceptive-audio-or-visual-media-deepfakes-2024-legislation

It is also important to note that on April 28, 2025, the President of the United States issued an Executive Order *Advancing Artificial Intelligence Education for American Youth*, emphasizing the need to prepare students for an AI-driven future (Federal Register, 2025). The order promotes early AI education in K–12, professional development for educators, and collaboration between schools and industry. Its goal is to foster innovation, critical thinking, and workforce readiness to maintain U.S. leadership in AI which includes deepfake detection.

Organizational Initiatives

Instead of waiting for state, federal, or international legislation, many organizations enacted their own initiatives to help combat deepfakes. For example, Facebook, the Partnership on AI, Microsoft, and academics from Technical University of Munich, University of Naples Federico II, Cornell Tech, MIT, University of Oxford, UC Berkeley, University of Maryland, College Park, and University at Albany–SUNY to start a global deepfake detection challenge (DFDC) encouraging the creation of advanced algorithms capable of identifying manipulated content with high accuracy (Dolhansky et al., 2020). This initiative aimed to leverage the collective expertise of the AI community to develop robust and effective detection methods DFDC had 2,114 participants and over 35,000 detection models submitted. Thus, the DFDC showed that deepfake detection is extremely difficult and still an unsolved issue facing the world, but technological solutions can aid in the detection process (Canton Ferrer et al., 2020).

Similarly, another nonprofit organization, AIandYou (2025) launched to provide free educational information for individuals and organizations to help them understand AI synthetic media. Their website (https://aiandyou.org/) is extensive with tons of resources and examples. For example, they provided information and a link to the Toys"R"Us AI TV commercial. The establishment for collaboration between educational institutions and businesses is needed to disseminate information and keep each other informed regarding deepfakes.

Finally, it is important to note that many universities have faculty starting to publicly educate via organized talks and discussions regarding deepfakes (Arizona State University News, 2024) or collaborating with other outside organizations regarding deepfakes. For example, Columbia University and Sciences Po in Paris have joined forces in collaboration via an innovation lab to research AI influence and challenges toward world democracies (Quintanar & Zuloaga, 2023).

Higer Education Deep Initiatives

Currently, some universities provide educational content to their faculty, staff and students to better equip them in navigating the challenges posed by deepfake technology. For example, Stanford University

provides a comprehensive website for responsible AI practices and usage (https://uit.stanford.edu/security/responsibleai#section_2970). Their website provides an overview, safety measures and risk factors for data privacy and security when using third-party AI platforms and tools, a few best practices, tools, resources and guidelines when working with generative AI, and newsletters which focus on trending topic such as deepfakes (Stanford University IT, 2023). However, it is important to note that just like legislation and detection methods, not all universities have a comprehensive information website for addressing deepfakes. Table 4 provides a comprehensive list of resources for higher education institutions to learn more about responsible AI practices and usage.

Table 4. Resources for Educators Regarding Responsible AI Practices

Tool	Website
International Society for Technology in Education (INSITE) Artificial Intelligence in Education Website	https://iste.org/ai
Microsoft's Responsible use of artificial intelligence in education	https://learn.microsoft.com/en-us/training/paths/responsible-use-of-artificial-intelligence-in-education/
MIT's OpenCourseware Course on Media Literacy in the Age of Deepfakes	https://ocw.mit.edu/courses/res-cms-001-media-literacy-in-the-age-of-deepfakes-spring-2021/pages/syllabus/
Stanford University Website on Responsible AI Practices and Usage	https://uit.stanford.edu/security/responsibleai#section_2970
Teach AI	https://www.teachai.org/
The Association of California School Administrator's Navigating Responsible AI in Education Resource Hub	https://www.teachai.org/policy

Additionally, many accredited universities include a technology course as part of their business core for a bachelor's degree in business administration (B.S.B.A) or Master of Business Administration (MBA) degree programs. For example, Association to Advance Collegiate Schools of Business (AACSB) Accreditation body (2023) states "technology will be ever important, and all AACSB-accredited schools will be expected to have processes in place to ensure that both learners and faculty are competent with current and emerging technologies" (p. 22). They also have it embedded under 4.1 curriculum standards that "Current and emerging technology is appropriately infused throughout each degree program as appropriate for that degree and level of program (i.e., bachelor's, master's, doctoral). A learn-to-learn expectation is instilled in learners to facilitate agility in adaptation to emerging technologies in the future" (p.43). Thus, one would expect that deepfakes would be included among the content address in these technology courses for business degrees.

A systematic review course descriptions of Business classes from AACSB and Accreditation Council for Business Schools and Programs (ACBSP) throughout Pennsylvania was completed. A total of 37 ACBSP universities were ACBSP accredited, and 33 universities were found to be AACSB accredited in PA. Upon examination of their course descriptions publicly available on their websites and course catalogs, not one AACSB or ACBSP university had a business course which specifically focused on deepfakes, or AI synthetic media. There were a few courses found at multiple universities which focused on AI or ML Learning (ML) found amongst 23 AACSB universities and 17 ACBSP universities. However, the course descriptions did not seem to reflect that the focus would shift to include deepfakes impacts on business.

Actionable Recommendations for Higher Education to Integrate into Their Curriculum

As indicated above, the lack of higher education courses focused on deepfakes, or AI synthetic media suggests a critical gap in preparing future business professionals with the tools to navigate the ethical, legal,

and operational complexities introduced by deepfake technologies. As a result, businesses cannot assume that new graduates may have knowledge and awareness about deepfakes to aid businesses in establishing or updating their policies, frameworks, and overall awareness.

In fact, these results suggest that graduates entering the workforce may be unprepared to identify, analyze, or respond to synthetic media threats. As a result, businesses may be vulnerable to manipulated content that can impact brand trust, operational security, stakeholder relationships, and employee identity safety and security. As such, there is a growing consensus that business schools must do more to equip students with the competencies needed to navigate these emergent risks.

To address this gap, Table 5 provides a detailed list of actionable recommendations for integrating deepfake awareness and related topics into business and IT curricula. These recommendations are grounded in best practices from AI ethics, cybersecurity education, and interdisciplinary pedagogy, offering institutions options for updating their educational models in line with technological change.

Table 5. Detailed Actionable List of Recommendations to Integrate Deepfake Awareness into Business and Technology Curricula

Action	Recommendation	Implementation Strategy
Update Existing Courses	Embed deepfake content into core business and/or IT courses	• Update syllabi in courses like Business Ethics, Information Systems, Cybersecurity, and Management Information Systems (MIS) to include content on deepfakes • Introduce Deepfake tools in lectures, labs, and/ or assignments • Explore the ethical, strategic, or legal implications of synthetic media in business contexts
	Develop deepfake content into freshman seminars	• Create a module for first-year seminars to cover misinformation, AI bias, and verification skills
	Integrate deepfake topics into case studies and capstone projects	• Use real-world case studies and simulations involving deepfakes
	Incorporate experiential learning activities	• Include guest lectures, webinars, or panel discussions with professionals from cybersecurity, journalism, and legal fields • Included fieldtrips to explore an organization's AI and deepfake policies
Develop New Courses	Develop interdisciplinary electives on deepfakes, synthetic media, and AI ethics	• Create courses heavily focused on Deepfakes • Foster partnerships between business, IT, law, and communication departments to team-teach models to address deepfake topics from ethical, technical, and social perspectives

Conclusion

Mitigating the impact of deepfakes requires a coordinated, multi-pronged response that includes continuous technological innovation, comprehensive legislative action, corporate accountability, and robust public and academic education. As deepfakes become more difficult to detect and more dangerous in potential misuse, initiative-taking education and awareness are essential for fostering a digitally resilient and informed society. Additionally, the lack of deepfake literacy among large segments of the American population, especially those without higher education or within older age groups, further reinforces the need for deepfake literacy awareness and resources.

This research highlighted how low-cost, accessible deepfake creation tools make it easier than ever for bad actors to exploit AI, while existing detection technologies, legislation, organizational initiative, and educational efforts struggle to keep pace. Additionally, this research conducted a review of business curricula in Pennsylvania's AACSB and ACBSP higher education institutions for deepfake literacy courses. The results reveal that topics related to deepfakes and AI-generated synthetic media are absent from current instructional content. This omission suggests a critical gap in preparing future business professionals with the tools to navigate the ethical, legal, and operational complexities introduced by deepfake technologies.

Limitations and Future Research

It is important to note that this paper is not without limitations. First, it is limited to a literature review and secondary data analysis. Second, as stated above, we only analyzed data secondary data publicly available on the internet. Third, our data is limited course descriptions from AACSB and ACSBP accredited universities. Fourth, our work is limited to geographical locations of AACSB and ACSBP universities in Pennsylvania. Future research studies should address the limitations described above and reevaluate the content as needed. This research has practical impacts for organizations, individuals, educators, and educational institutions wanting to learn more about deepfakes. Furthermore, it is the authors' hope this paper serves as a foundation for educational institutions to begin to develop more robust business courses to help in education and awareness regarding deepfakes.

References

Agarwal, S., & Farid, H. (2021). Detecting deep-fake videos from aural and oral dynamics. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition (pp. 981-989).

Agarwal, S., Farid, H., Gu, Y., He, M., Nagano, K., & Li, H. (2019). Protecting world leaders against deep fakes. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, 38-45. https://doi.org/10.1109/CVPRW.2019.00009

Agarwal, S., Hu, L, Ng, E., Darell, T., Li, H., & Rohrbach, A. (2021b). Watch those words: video falsification detection using word-conditioned facial motion. https://www.dropbox.com/scl/fi/7jh4t0dmltk9sz0wjtfzi/arXiv22.pdf?rlkey=wufxcnbjcfkflugwo7h1rrx32&e=1&dl=0

AIandYou (2025). https://aiandyou.org

Alanazi S, Asif S, Moulitsas I. (2024) Examining the societal impact and legislative requirements of deepfake technology: a comprehensive study. *International Journal of Social Science and Humanity*, 14 (2), 58-64. https://doi.org/10.18178/ijssh.2024.14.2.1194

Arizona State University News (2024). ASU researchers discuss the implications of deepfakes. https://news.asu.edu/20240628-science-and-technology-asu-researchers-discuss-implications-deepfakes

Association to Advance Collegiate Schools of Business (2023). 2020 Guiding Principles and Standards for Business Accreditation. https://www.aacsb.edu/-/media/documents/ accreditation/2020-aacsb-business-accreditation-standards-june-2023.pdf

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, *9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Canton Ferrer, C., Dolhansky, B., Pflaum, B., Bitton, J., Pan, J. & Lu, J. (2020). Deepfake detection challenge results: an open initiative to advance AI. https://ai.meta.com/blog/deepfake-detection-challenge-results-an-open-initiative-to-advance-ai/

Chen, H. & Magramo, K. (2024). Finance worker pays out $25 million after video call with deepfake 'chief financial officer'. *Cable News Network*. https://edition.cnn.com/2024/02/04 /asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

Chesney, R., & Citron, D. (2019). Deepfakes and the new disinformation war: the coming age of post-truth geopolitics. *Foreign Affairs*, 98(1), 147-155. https://www.jstor.org/stable/26798018

Chesney, R., & Citron, D. K. (2019b). Deepfakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753-1820. https://doi.org/10.15779/Z38RV0D15J

Citizen.org (2025). Tracker: state legislation on deepfakes in elections. https://www.citizen.org/article/tracker-legislation-on-deepfakes-in-elections/

Damiani, J. (2019, September). A voice deepfake was used to scam A CEO out of $243,000. Forbes. https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/

Dolhansky, B., Howes, R., Pflaum, B., Baram, N., & Ferrer, C. C. (2020). The deepfake detection challenge dataset. https://arxiv.org/abs/2006.07397

Das, A.K., Mukhopadhyay, S., Dalui, A., Bhattacharya, R., Naskar, R. (2023). A multi-stage multi-modal classification model for deepfakes combining deep learned and computer vision oriented features. In: Muthukkumarasamy, V., Sudarsan, S.D., Shyamasundar, R.K. (eds*) Information Systems Security*. ICISS 2023. *Lecture Notes in Computer Science*, vol 14424. Springer, Cham. https://doi.org/10.1007/978-3-031-49099-6_13

Federal Register. (2025, April 28). Advancing artificial intelligence education for American youth [Executive Order]. https://www.federalregister.gov/documents/2025/04/28/2025-07368/advancing-artificial-intelligence-education-for-american-youth

Gold, H. (2025). Celebrity AI deepfakes are flooding the internet. Hollywood is pushing Congress to fight back. https://www.cnn.com/2025/03/08/tech/hollywood-celebrity-deepfakes-congress-law/index.html

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. *Advances in Neural Information Processing Systems*, 27, 2672-2680.

Helmus, T.C. (2022, July 6). Artificial intelligence, deepfakes, and disinformation. The RAND Corporation. https://www.rand.org/pubs/perspectives/PEA1043-1.html

Horaczek, S. (2017). Spot faked photos using digital forensic techniques, Popular Science. https://www.popsci.com/use-photo-forensics-to-spot-faked-images

Matern, F., Riess, C., & Stamminger, M. (2019). Exploiting visual artifacts to expose deepfakes and face manipulations. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*, 39-48.

Nguyen, T. T., Nguyen, C. M., Nguyen, D. T., Nguyen, D. T., & Nahavandi, S. (2021). Deep learning for deepfakes creation and detection: A survey. https://arxiv.org/abs/1909.11573

Owen, A. (2024). Deepfake laws: is AI outpacing legislation? https://onfido.com/ blog/deepfake-law/

Quintanar S. & Zuloaga, J. (2023). SIPA launches new lab to tackle overlap of AI and democracy. https://www.columbiaspectator.com/news/2023/10/16/sipa-launches-new-lab-to-tackle-overlap-of-ai-and-democracy/

Rana, M. S., Nobi, M. N., Murali, B., & Sung, A. H. (2022). Deepfake detection: A systematic literature review. IEEE access, 10, 25494-25513. https://doi.org/10.1109/access.2022.3154404

Roe, J., Perkins, M. & Furze, L. (2024). Deepfakes and higher education: a research agenda and scoping review of synthetic media. *Journal of University Teaching and Learning Practice*, V 21(10), 1-22. https://doi.org/10.53761/2y2np178

Sidoti, O.& Vogels, E. A. (2023, August 17). What Americans know about AI, cybersecurity and big tech. *Pew Research Center*. https://www.pewresearch.org/internet/ 2023/08/17/what-americans-know-about-ai-cybersecurity-and-big-tech/

Stanford University IT (2023). Dangers of deepfake: what to watch for. https://uit.stanford.edu/news/dangers-deepfake-what-watch

Texas Legislature Online. (2019). SB 751: Relating to the creation of a criminal offense for fabricating a deceptive video with intent to influence an election. https://capitol.texas.gov/BillLookup/History.aspx?LegSess=86R&Bill=SB751

U.S. Department of Homeland Security (2022). Increasing threats of deepfake identities. https://www.dhs.gov/sites/default/files/publications/increasing_threats_of _deepfake_identities_0.pdf

Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: exploring the impact of synthetic political video on deception, uncertainty, and trust in news. *Social Media and Society*, 6(1), 1-13. https://doi.org/10.1177/2056305120903408

Vig, S. (2024). Regulating deepfakes: an Indian perspective. *Journal of Strategic Security*, 17(3), 70-93. https://doi.org/10.5038/1944-0472.17.3.2245

Wang, J. (2024). It starts with deepfakes–When you no longer need to believe to see. You can now just see what you want to see. The latest advancement in image-based sexual abuse where deepfakes are only the beginning for future exploits of artificial intelligence. https://researchspace.auckland.ac.nz/server/api/core/bitstreams/78ad1dc6-04e1-4a58-bd67-66fd9483e7de/content

West, D. M. (2021). How to combat deepfakes and fake news. Brookings Institution. https://www.brookings.edu/research/how-to-combat-deepfakes-and-fake-news/

Westfall, C. (2024, November, 29). AI deepfakes on the rise causing billions in fraud losses. Forbes. https://www.forbes.com/sites/chriswestfall/2024/11/29/ai-deepfakes-of-elon-musk-on-the-rise-causing-billions-in-fraud-losses/

Yang, X., Li, Y., & Lyu, S. (2019). Exposing deep fakes using inconsistent head poses. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*, 53-59.