



# IJRASET

International Journal For Research in  
Applied Science and Engineering Technology



---

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

---

**Volume:** 14    **Issue:** VI    **Month of publication:** June 2026

**DOI:** <https://doi.org/10.22214/ijraset.2026.83915>

[www.ijraset.com](http://www.ijraset.com)

Call:  08813907089

E-mail ID: [ijraset@gmail.com](mailto:ijraset@gmail.com)

# Deepfake Detection Asymmetry: Generation Outpaces Detection, and What That Means for Elections

Ishan Kumar<sup>1</sup>, Bhavin Bhat<sup>2</sup>, Eshanye J<sup>3</sup>

Department of Computer Science and Engineering, RV College of Engineering

**Abstract:** *Advances in artificial intelligence (AI) have led to the creation of realistic deepfakes, including altered images, videos, and audio, that are difficult to distinguish from their original forms. Despite significant advancements in identifying synthetic media, the pace of deepfake generation is outpacing that of detection technologies, posing a threat, especially to democratic processes, by misinforming the public, discrediting political figures, and eroding confidence in elections. This paper analyses the deepening chasm between deepfake generation and detection, explores the reasons behind this imbalance, and underscores the importance of a coordinated approach to ensure the integrity of democratic institutions.*

**Keywords:** *Deepfakes, Artificial Intelligence, Election Integrity, Misinformation, Deepfake Detection, Intellectual Property Rights*

## I. INTRODUCTION

AI has dramatically changed how we create, consume, and share digital content. One remarkable application, deepfake technology, allows us to generate convincing likenesses of individuals through manipulation of their image, video, and audio. This experimental technology has swiftly evolved into a readily accessible tool that can generate impressive synthetic media using simple devices and computation power. The foundation for most deepfakes lies in the application of complex AI learning models that are trained with an enormous amount of data.

Their sophistication increases rapidly, allowing for extremely realistic synthetic media creation that closely resembles reality, thus making it incredibly challenging to identify fakes. Efforts to detect deepfakes using various methods, including the use of artificial intelligence, are ongoing; however, they are currently trailing behind the rapid developments in generative technologies. This means the technologies that can create deepfakes are progressing faster than the technologies that are able to identify them. Not only is the growing disparity in deepfake generation and detection technologies a concern in a technical sense, but its impact is far more significant on societal, legal, and political matters. It represents a critical threat to democracy and the process of democratic elections, where citizens depend on truthful and credible information.

Discredited candidates, false information spread through manipulation, and a complete loss of faith in the electoral process are just a few examples of how this technology can be abused during elections. Once a deepfake has been seen and distributed by enough individuals, any truth found later will be ignored by the majority of voters. Another major area of concern relates to intellectual property and legal implications. There are many questions and disagreements about copyright, the use of an individual's likeness without their permission, the issue of liability, and who should be responsible for creating and distributing synthetic content. Current legal frameworks predate generative AI and do not adequately address the issues surrounding deepfakes.

Governments, regulators, and technology firms are beginning to assess new strategies to manage these concerns. In this paper, the issues concerning the growing chasm between deepfake generation and detection technologies and its impact on the elections is analysed. Technological considerations that drive the chasm, as well as the limitations of present detection technologies, are explored. In addition, potential intellectual property and legal concerns arising from deepfakes are discussed. By analysing recent developments and case studies, this work aims to demonstrate the risks posed by the increasing sophistication of synthetic media and the necessity for a multidisciplinary strategy that includes technical, legislative, and institutional measures.

## II. LITERATURE SURVEY

### A. Research on deepfakes overview

Deepfakes have been a topic of intense study among AI, security, legal, and political professionals. Their generation and detection, and the more widespread social implications of their use, have been thoroughly investigated. With continuous improvement in generation technologies, academic researchers are more and more highlighting the difficulties in identifying artificial contents and limiting their influence on society and institutions.

### *B. Progression in generation of deepfakes*

In the past, Generative Adversarial Networks (GANs) have revolutionized the generation of fake content and produced remarkably realistic synthetic images by utilizing adversarial relationships between generation and discriminator models. In recent times, machine learning models are more powerful, making deepfakes with realistic lips movements, eye contact and accurate voice simulation of individuals. Diffusion-based generative models have further advanced this technology to an unprecedented level where even artificial images can rarely be detected.

### *C. Development in Deepfake Detection Techniques*

Numerous methods of deepfake identification and detection techniques have been introduced, ranging from facial landmark analysis and checking for facial-movement and blink patterns to detecting physiological signals and performing multimodal verification. Early approaches mainly involved finding visual flaws and image anomalies, and while these early techniques had some success against older deepfakes, it had less effectiveness against the more recent deepfake techniques [6].

### *D. Limitations and Generalization Challenges in Detection Systems*

Researchers agree that despite advancements in deepfake detection technologies, they are struggling to deal with the ever-changing generation technologies [7]. It is common to discover that deepfake detection models developed against certain groups of artificial content may underperform when the input includes new forms of synthetic content that differ from previously seen examples. Many scholars see the race to develop defensive mechanisms to beat generative advancements in the fight for authentic content. [8].

### *E. Detection asymmetry and adversarial attack vulnerability*

In an attempt to break or weaken detection tools, researchers have devised techniques called adversarial attacks which involve subtle alterations to an artificial image to trick detection models into classifying them as authentic, often without making any obvious visual difference. Thus, the technological gap is widening as detection mechanisms are easily deceived.

### *F. Social and Political Implications of Deepfakes*

The social and political ramifications of deepfakes are of primary concern for academicians studying information dissemination, cybersecurity, political discourse, and societal behaviour. Synthetic media has been shown to be a potent tool for spreading misinformation and deception on a global scale [11]. There are particularly alarming implications regarding deepfakes being used for purposes of political campaigns where individuals may use synthetic media for election interference or to smear an opponent, thereby distorting public perception and potentially influencing electoral outcomes, even if these fakes may ultimately be debunked. Information researchers acknowledge that the rapid viral dissemination of digital media via social media platforms means such content spreads with lightning speed, far faster than any verification process can hope to achieve. [12].

### *G. Legal and Intellectual Property Considerations*

The intersection of deepfake technology and the legal and intellectual property realms is a subject of intense research. Studies have delved into questions of ownership of artificially generated content, misuse of one's likeness or identity, copyright issues related to synthetic media, and legal culpability for the creation or distribution of deepfakes. [15].

Researchers have noted that many existing legal frameworks were developed before the emergence of advanced generative artificial intelligence and therefore provide limited guidance for addressing contemporary deepfake-related disputes [16]. Consequently, governments and regulatory bodies in several jurisdictions have begun exploring new legislative and policy approaches aimed at reducing the risks associated with deceptive synthetic media [17].

## **III. RESEARCH GAP**

Although deepfakes have attracted significant research attention in areas such as content generation, detection techniques, misinformation, and legal regulation, less attention has been paid to the growing gap between the capabilities of deepfake generators and the systems designed to detect them. Most existing studies examine either the performance of detection methods or the broader social and political impacts of deepfakes, rather than considering how these issues are interconnected. As generative technologies continue to improve at a rapid pace, detection tools face increasing difficulty in keeping up, raising concerns about their long-term effectiveness. This imbalance presents new challenges for election integrity, particularly in environments where misleading content can spread quickly and influence public opinion. To address this issue, this paper explores the technological, legal, and intellectual property dimensions of deepfake detection asymmetry and assesses its implications for democratic electoral processes.

#### IV. PROBLEM STATEMENT

Although deepfakes have attracted significant research attention in areas such as content generation, detection techniques, misinformation, and legal regulation, less attention has been paid to the growing gap between the capabilities of deepfake generators and the systems designed to detect them. Most existing studies examine either the performance of detection methods or the broader social and political impacts of deepfakes, rather than considering how these issues are interconnected. As generative technologies continue to improve at a rapid pace, detection tools face increasing difficulty in keeping up, raising concerns about their long-term effectiveness. This imbalance presents new challenges for election integrity, particularly in environments where misleading content can spread quickly and influence public opinion. To address this issue, this paper explores the technological, legal, and intellectual property dimensions of deepfake detection asymmetry and assesses its implications for democratic electoral processes.

#### V. DEEPPAKE GENERATION AND DETECTION TECHNOLOGIES

##### A. Overview of Deepfake Technologies

Deepfakes leverage advanced artificial intelligence to synthesize and analyze digital media such as images, videos, and audio. The process can be divided into two closely related and inter-dependent areas: generation methods focused on producing high-quality synthetic content, and detection methods, designed to discriminate between authentic and fake content. There is an evolving dance between generation and detection capabilities where improvements in one often drive changes and improvements in the other.

##### B. GAN-Based Deepfake Generation

The generation of deepfakes has been historically driven by deep learning-based architectures. Generative Adversarial Networks (GANs) represented an early breakthrough, consisting of a generator that creates fake data samples, while a discriminator tries to distinguish between real and synthetic data. Through an adversarial process of iterative training, the generator learns to produce realistic fakes that deceive the discriminator, and this GAN-based architecture has been broadly used to generate synthetic face images, to perform face swapping, and video manipulation [1]. GAN architectures were refined with technologies such as StyleGAN, which allowed fine control over various facial attributes and generated hyper-realistic faces with very few visible flaws. These advances improved the quality of deepfake creations and significantly reduced the effectiveness of the first-generation detection methods that relied on easily detectable visual artifacts caused by synthesis failures [2].

##### C. Diffusion-Based Generation Models

Concurrently, diffusion models have emerged as another powerful technology alongside GANs. Unlike GANs, diffusion models generate data by incrementally denoising random noise until structured outputs such as images are obtained. These models have achieved excellent visual fidelity and stability and are becoming widely used in the modern generation systems, thereby decreasing the barrier for creating high-quality synthetic media [3].

##### D. Audio and Multimodal Deepfake Generation

Deepfake technology is not restricted to visual media. Audio-based deepfakes, commonly known as voice cloning, use similar deep neural networks to replicate the acoustic features of a person's voice from small audio recordings, replicating tonality, accent and speech patterns with high accuracy. When coupled with video generation, these methods can lead to highly realistic audio visual deepfake media [4].

##### E. Traditional Deepfake Detection Techniques

At the other end of the spectrum, deepfake detection technology seeks to identify synthetic or manipulated digital media. The initial detection methods largely focus on visually identifiable flaws such as unnatural blinking patterns, facial distortions or artifact caused by compression of images and videos. Such techniques are effective for low-quality, early generation deepfakes but are increasingly ineffective for high fidelity productions [5].

##### F. Modern Detection Approaches

In current detection schemes, deep learning-based approaches, including convolution neural networks (CNNs) and multimodal analytical methods, have become dominant. Such techniques examine subtle patterns in facial movements, lighting inconsistencies, or audio sync that may not be obvious to a human eye. Other detection techniques include physiological signal analysis, and biometric consistency checks which try to verify if natural physiological signatures are present in the produced content [6].

### G. Limitations and Generalization Challenges in Detection

Although considerable progress has been made in deepfake detection, challenges remain for these technologies in practice. One of the greatest limitations is that detection models perform poorly when generalizing to new generation methods to which they have not been trained. As generative techniques rapidly evolve, they create ever more sophisticated and novel means for synthetic media production, making it more difficult for existing detectors to generalize and maintain effectiveness [7].

### H. Adversarial Vulnerabilities and Detection Asymmetry

Another challenge is the extreme vulnerability of deepfake detectors to an adversarial attack. Very small modifications typically undetectable by humans-to the synthetic media are sufficient to greatly mislead even the best-performing deep fake detector, creating a sort of game of cat and mouse where robust detectors can be rendered ineffective by tiny changes in the input data [8].

### I. Overall Technological Imbalance

Overall, the relationship between deepfake generation and detection can be characterized as an ongoing imbalance. While generation techniques continue to improve in realism and accessibility, detection methods struggle to maintain consistent performance across diverse and evolving synthetic media formats. This growing gap forms the technical foundation of the asymmetry discussed in the following sections.

## VI. IMPLICATIONS FOR ELECTIONS AND DEMOCRATIC PROCESSES

### A. Overview of Electoral Risks

The increasing sophistication and accessibility of deepfake technologies pose a big risk to democratic elections and broader electoral processes. Elections are dependent on reliable access to truthful information, a trusting relationship with media sources, and the ability of voters to make informed choices.

Deepfakes exploit this vulnerability by allowing the production of convincingly real synthetic media that can be manipulated to misrepresent candidates or distort public perceptions of political events. When even fact-checking organizations can distinguish between real and fake news, it becomes challenging to limit the influence of a popular fabricated media. The spread of fabricated media can influence voter attitudes and public opinion, leading voters to base their choices on incomplete and false information.

### B. Misinformation and Voter Manipulation

A primary concern in the context of elections relates to the potential use of deepfakes in targeted misinformation campaigns to influence voters and disrupt electoral results. Manipulated media-videos or audio recordings of candidates may be disseminated via social media to mislead voters, create uncertainty, or damage a politician's credibility.

This phenomenon can accelerate over time as information flows more easily through various communication channels, and the speed of these developments can exceed fact-checking initiatives, making it difficult to limit the proliferation of misinformation during critical election cycles. In some instances, misinformation can exploit societal divisions by designing fake media content in ways intended to divide certain segments of the electorate. Furthermore, it can be a strategy to reduce public trust in election institutions.

### C. Erosion of Trust and the Liar's Dividend

Over time, the increasingly realism of synthetic media can lead to general public doubt regarding the authenticity of digital content in general, including legitimate recordings. When faced with credible evidence of their wrongdoing, politicians will likely attempt to deny the validity of authentic content by claiming it to be a fabrication-a phenomenon called "the liar's dividend," which undermines accountability and public trust in democratic systems. In the long run, this general erosion of public trust in media and institutions may have an adverse effect on the future functioning of democracy.

### D. Impact on Electoral Institutions and Processes

Deepfakes also present challenges to election institutions and governmental bodies tasked with ensuring fair elections. Election commissions will be under increased pressure to detect and filter fake media that has gone viral within short timelines, overwhelming any current or proposed factchecking processes. The spread of manipulated content, particularly when such content is designed to mimic real, verified media and is strategically released throughout an election, will be challenging to counter with current procedures. The ability to create an imposter version of election officials, candidates, or other influential figures-even if simply through fabricating a public statement attributed to that person-also represents a potential for electoral disruption.

### *E. Long-Term Implications for Democratic Governance*

Without robust technological solutions, legal frameworks, and institutional adaptations, the increased prevalence of deepfakes poses a systemic risk to the process by which democratic societies communicate and deliberate. The challenge posed by deepfakes to electoral processes is also a broader challenge to the ways we process information in democratic governance, and it may well expand over time as generation techniques improve and become less detectable. The “asymmetry between deepfake generation and detection” will become a greater problem as synthetic media is more readily available and sophisticated.

## **VII. PROPOSED SYSTEM FOR MITIGATING DEEPFAKE DETECTION ASYMMETRY**

### *A. Overview of Proposed Framework*

To address the growing imbalance between deepfake generation and detection, this paper proposes a conceptual framework that integrates technological, institutional, and user-level safeguards. The primary objective of the proposed system is not to eliminate deepfakes entirely, but to reduce their potential impact on electoral processes by improving early detection, verification, and response mechanisms. The framework is designed to operate across multiple stages of content creation, distribution, and consumption.

### *B. Multi-Layer Detection and Verification Pipeline*

The proposed system is based on a multi-layer pipeline that combines several complementary approaches rather than relying on a single detection method. At the first layer, incoming media content is analysed using AI-based detection models trained to identify synthetic artifacts in images, videos, and audio. This includes both traditional deep learning classifiers and models specialized for detecting inconsistencies in facial motion, voice patterns, and temporal coherence.

At the second layer, content is verified using metadata and provenance-based checks. This includes analysing digital signatures, source authenticity, and content origin tracking where available. The goal of this layer is to identify whether the media has a verified origin or has been altered after creation. The third layer incorporates cross-platform validation, where suspicious content is compared against trusted databases and known verified media sources. This helps reduce the spread of manipulated content that may have bypassed initial detection systems.

### *C. Early Warning Mechanism*

The system acts in real-time, continuously monitoring social media and news channels during an election period, assigning a risk score based on detection confidence. If it exceeds a particular threshold, relevant authorities, or platform moderators receive an alert for further verification. This approach is crucial in election periods where misinformation might quickly spread faster than factchecking. Our system offers a real-time early warning advantage, allowing for immediate action to curb the spread of misinformation. This layer is particularly important during election cycles, where the speed of information dissemination often exceeds the speed of fact-checking. Early identification can significantly reduce the reach and impact of manipulated content before it becomes widely circulated.

### *D. Human-in-Loop Verification System*

To improve reliability, the proposed framework includes a human-in-the-loop verification stage for high-risk cases. Content flagged by automated systems is reviewed by trained analysts or fact-checking teams who assess its authenticity using contextual and domain knowledge. This hybrid approach helps reduce false positives and improves decision making in cases where automated systems alone may not be sufficient.

### *E. User Awareness and Reporting Mechanism*

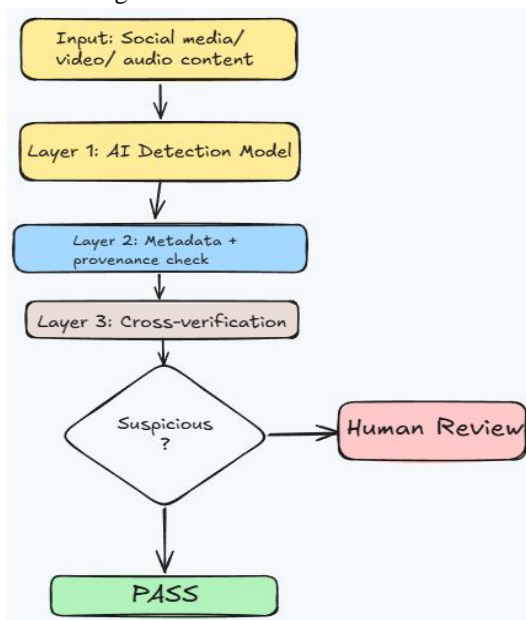
In addition to technical components, the system incorporates a user-facing awareness layer. This includes simplified indicators that signal whether content has been verified, is under review, or has been flagged as potentially synthetic. Users are also provided with reporting mechanisms to flag suspicious media for further investigation. This participatory approach helps distribute responsibility across platforms and end users.

### *F. Conceptual Flow of the System*

The overall workflow of the proposed system begins with content ingestion, followed by AI-based detection, metadata verification, and cross-platform validation.

If content is flagged as suspicious, it moves to a human review stage and is either labelled, restricted, or removed depending on severity. Verified content is allowed to circulate without restriction. This layered approach ensures multiple checkpoints before potentially harmful content reaches a wide audience. A detailed flowchart representing this process is provided in Fig. 1.

Fig 1: Detailed flow of the model



## VIII. INTELLECTUAL PROPERTY RIGHTS CONSIDERATIONS

### A. Ownership of AI-Generated Models and Training Frameworks

The creation of deepfake generation and detection systems heavily relies on pre-existing datasets, machine learning architectures and publicly available frameworks. Modern artificial intelligence models are generally trained on large scale datasets that consist of images, videos and audio samples collected from diverse sources.

For example, if the original content is copyrighted or contains identifiable people. For the proposed framework, it is assumed that the detection and analysis models are constructed utilizing standard machine learning libraries and pre-trained architectures commonly available in open-source environments. But even so, there are questions about ownership of model outputs, the influence of training data, and works derived through finetuning processes.

### B. Dataset Usage and Licensing Concerns

Deepfake detection systems typically rely on datasets containing both authentic and synthetic media samples. These datasets are often compiled from publicly available sources or generated using existing deepfake tools. A key intellectual property concern is whether the use of such datasets for training purposes constitutes fair use or requires explicit licensing agreements.

Additionally, datasets used in training may contain copyrighted visual or audio content, raising questions about unauthorized reproduction and redistribution. In many jurisdictions, the legal framework governing the use of data for machine learning purposes is still evolving, and there is limited clarity on how existing copyright laws apply to training large-scale artificial intelligence systems.

### C. Rights Over Synthetic Media Outputs

A critical issue in deepfake technology is the ownership of synthetic outputs generated by artificial intelligence systems. Since deepfakes often involve the replication of real individuals' faces, voices, or expressions, questions arise regarding personality rights, likeness rights, and moral rights of individuals whose features are replicated.

From an intellectual property perspective, synthetic media challenges traditional definitions of authorship and originality. If a deepfake is generated using a trained model, it becomes difficult to determine whether ownership lies with the developer of the model, the user generating the content, or the entity whose data was used during training.

#### *D. Attribution and Model Accountability*

Another important aspect of intellectual property rights in this domain is attribution. Machine learning models are often trained using architectures and datasets developed by multiple contributors. Ensuring proper attribution of these components is essential for maintaining transparency and legal compliance.

However, as models become more complex and incorporate multiple layers of pre-trained components, tracing the contribution of individual datasets or algorithms becomes increasingly difficult. This creates challenges in assigning accountability for both detection failures and misuse of generative models.

#### *E. Intellectual Property Implications in Detection Systems*

In the proposed framework, the detection system itself relies on a combination of machine learning classifiers, temporal analysis modules, and metadata verification tools. Each of these components may be derived from or influenced by existing research models. As such, the intellectual property rights associated with the detection framework are distributed across multiple technological components.

This raises additional concerns regarding licensing, reuse of academic models, and compliance with open-source software regulations. In practical deployment scenarios, organizations implementing such systems must ensure that all underlying components adhere to appropriate licensing agreements.

### **IX. CASE STUDY: GLOBAL LEGAL RESPONSES TO DEEPFAKE REGULATION**

#### *A. Overview of Global Regulatory Approaches*

Different countries are starting to tackle the deepfake threat, from implementing various election, data privacy and criminal legislation to specific artificial intelligence (AI) laws. There is currently no one global deepfake law, however the recent trends and policies enacted or proposed appear to lean towards tighter regulation of synthetic media, especially around the context of elections, misleading or false information, and misuse of identity.

#### *B. United States Approach*

Currently, no specific federal law is addressing the threat posed by deepfakes in the US. Yet, various US states have enacted specific legislation regarding misuse of deepfakes, especially in elections. California, Texas, amongst other states, have passed legislation prohibiting the use of deceptive synthetic media involving a political candidate during an election campaign. The main intent of these laws is to prevent any manipulation of the voters during elections and promote honesty in political communications. The US has introduced bills such as DEEPFAKES Accountability Act, which would mandate labels for and disclosures of synthetic media. These bills have not yet been fully implemented. Hence, US regulation on deepfakes is fragmented and largely state specific.

#### *C. European Union Framework*

The EU is using a more holistic regulatory approach, as embodied in the EU Artificial Intelligence Act. This framework imposes certain transparency obligations upon AI generated media, including a duty to disclose that the media has been synthetically generated or manipulated. Furthermore, the law regards certain AI applications as a “high-risk use of AI, particularly those impacting democratic processes. In addition, The General Data Protection Regulation (GDPR) provides indirect protection against the misuse of personal information to create deepfakes. This particularly apply when an individuals’ likeness is used without their consent.

#### *D. China’s Regulatory Model*

China has been the first nation to implement strict regulation in synthetic media, through its Deep Synthesis Provisions. The provisions require mandatory labelling of all AI generated content and imposing serious compliance requirements on platforms hosting synthetic media. The framework seeks to regulate the use of synthetic media as an instrument for political interference, to combat false information and ensure social stability. Under this model, platform provider is also held liable to supervise and control the dissemination of synthetic media.

#### *E. United Kingdom and Australia*

The United Kingdom regulates deepfakes primarily through the Online Safety Act, which requires digital platforms to take action against illegal and harmful content, including manipulated media.

While there is no dedicated deepfake legislation, existing laws on harassment, fraud, and malicious communications are applied to address misuse. Australia has also introduced amendments to its criminal code to specifically address non-consensual deepfake content, particularly in relation to synthetic explicit material. Additionally, electoral authorities are actively reviewing frameworks to manage AI-generated misinformation during political campaigns.

## X. FUTURE SCOPE

Future research in deepfake detection can focus on improving real-time detection systems that are capable of adapting to rapidly evolving generative models. The integration of blockchain-based content provenance and digital watermarking may provide stronger verification of media authenticity. Advances in multimodal detection, combining audio, visual, and textual analysis, can further enhance accuracy in identifying synthetic content. Additionally, the development of standardized global regulations and AI governance frameworks will be essential to address cross-border challenges posed by deepfake technologies, especially in sensitive domains such as elections and public communication.

## XI. CONCLUSIONS

The quick progress in deepfake generation has led to an increasingly asymmetric relation between its production and detection capability. This article analysed this asymmetry through exploring development trends of generation technology, constraints of existing detection systems and socio-economic impacts on election integrity, intellectual property and legislative. This research identified that current generation approaches like GAN-based frameworks, diffusion models and voice synthesizing systems has achieved new levels in realism and availability of synthetic media.

On the one hand, although detection approaches are getting more mature, they are still encountering problems of generalization capability, vulnerability to adversarial attacks and deployment in real world environment, on the other hand, which gives rise to a continuous gap where detector technology cannot catch up with the fast-developing generation technology. On the social aspect, election process, especially democratic election, has suffered the severe consequences from deepfake generation technology, for instance, to spread misinformation, personate politicians, and pollute social discourse by which the

## XII. ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to R.V. College of Engineering (RVCE) for providing a conducive academic environment and the resources necessary for carrying out this work. We are especially grateful to Dr. Chitra B. T., Professor, Department of Industrial Engineering and Management (IEM), for her invaluable guidance, encouragement, and insightful suggestions throughout the development of this paper.

Her expertise in Engineering Intellectual Property Rights (EIPR) and continuous support greatly contributed to shaping our understanding of the subject and improving the quality of this work. We also thank the faculty and staff of the Department of Industrial Engineering and Management for their support and cooperation during the course of this study.

## REFERENCES

- [1] I. J. Goodfellow et al., "Generative Adversarial Nets," Advances in Neural Information Processing Systems (NeurIPS), 2014.
- [2] T. Karras, S. Laine, and T. Aila, "A Style-Based Generator Architecture for Generative Adversarial Networks," Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2019.
- [3] J. Ho, A. Jain, and P. Abbeel, "Denoising Diffusion Probabilistic Models," Advances in Neural Information Processing Systems (NeurIPS), 2020.
- [4] S. Rana et al., "Deepfakes: A Survey of Detection Techniques," IEEE Access, vol. 10, pp. 123456–123478, 2022.
- [5] Y. Mirsky and W. Lee, "The Creation and Detection of Deepfakes: A Survey," ACM Computing Surveys, vol. 54, no. 1, pp. 1–41, 2021.
- [6] A. van den Oord et al., "WaveNet: A Generative Model for Raw Audio," arXiv preprint arXiv:1609.03499, 2016.
- [7] L. Li et al., "Deepfake Video Detection Using Convolutional Neural Networks," Pattern Recognition Letters, vol. 146, pp. 1–8, 2020.
- [8] R. Tolosana et al., "DeepFakes and Beyond: A Survey of Face Manipulation and Fake Detection," Information Fusion, vol. 64, pp. 131–148, 2020.
- [9] P. Neekharu et al., "Adversarial Deepfakes: Evaluating Vulnerability of Deepfake Detectors," arXiv preprint, 2021.
- [10] S. Westerlund, "The Emergence of Deepfake Technology: A Review," Technology Innovation Management Review, vol. 9, no. 11, pp. 40–53, 2019.
- [11] M. Vaccari and A. Chadwick, "Deepfakes and Disinformation: Exploring the Impact on Democracy," Social Media + Society, vol. 6, no. 1, 2020.
- [12] H. Chesney and D. Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," California Law Review, vol. 107, no. 6, pp. 1753–1820, 2019.
- [13] A. Paris and M. Donovan, "Deepfakes and Cheap Fakes," Data & Society Research Institute Report, 2019.
- [14] European Union, "Artificial Intelligence Act," Official Legislative Text, 2024.
- [15] China Cyberspace Administration, "Deep Synthesis Provisions," Government Regulation, 2023.
- [16] OECD, "Artificial Intelligence Principles," OECD Publishing, 2019.
- [17] World Intellectual Property Organization (WIPO), "AI and Intellectual Property Policy Report," 2024.



10.22214/IJRASET



45.98



IMPACT FACTOR:  
7.129



IMPACT FACTOR:  
7.429



# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24\*7 Support on Whatsapp)