International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 03 | March - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Cybercrimes in Synthetic Media: A Multidisciplinary Approach for Detection and Control

Reuben Sunil George[1], Melvin John Kurian[2], Anna Roy[3], Abel Abraham John[4], Dr.Divya K.S[5]

Student[1], Department of CS, Kristu jayanti college, Students[2,3,4], Department of Forensic Science, Assistant Professor[5], Department of CS, Kristu jayanti college

ABSTRACT:

The rapid increase in synthetic media produced or manipulated by Artificial Intelligence such as deepfakes, AI crafted images or voices, marks the beginning of a new chapter in creativity and communication. While these technological advancements bring new possibilities and opportunities in fields like entertainment and education, they also bring forward many new problems. There is an increased risk of misuse of such technologies through activities like spreading of misinformation, identity theft and fake or AI generated content. The misuse of synthetic media can also lead to cybercrimes like evidence manipulation which may affect the proper delivery of justice in cases. All this emphasizes the necessity for stricter laws and effective rules to safeguard against such threats. This research focuses on the development of synthetic media and its impact on society and also the moral dilemmas it creates. It also demonstrates the importance of regulations to manage risks and promote advancements in this field. By providing innovative solutions to the challenges, this research aims to support a balanced approach that increases the benefits of synthetic media while limiting any negative consequences.

Keywords: synthetic media, cybercrimes, deepfakes, identity theft, technology, evidence manipulation, Artificial Intelligence.

1.Introduction.

In today's digital world, the proliferation of synthetic media has reached the epitome of entertainment, advertising and education. It has emerged into a more powerful and transformative force in the digital space. Comprising of a wide range of AI generated or manipulated content, including deepfake videos, synthetic voices and facial makeovers, has proven to unlock creative possibilities and enhance creativity & imagination. However, alongside these benefits, these new-age AI manipulated content poses to significant ethical, social, security and privacy issues. The rise of synthetic media has paved the way for its misuse in the form of political or social propaganda, fake news and identity theft. If we take deepfakes for instance, we can see that it has been used to spread false narratives or impersonate individuals, robbing the trust of the public in the ethics of digital media. The rapid advancement of generative Artificial Intelligence has also outpaced the development of legal and ethical frameworks, creating a vacuum in which harmful applications can thrive. Through the growth of manipulated content, cybercrimes have skyrocketed, therefore management and detection of these synthetic contents are essential in the context of criminal investigations as manipulated image and video evidence collected during a crime can compromise the entire investigation process. By addressing these issues, this research study aims to provide a multidisciplinary approach for the detection and control of synthetic media from forensic and technological standpoints.

2.Case Studies.

Synthetic Fraud Reported in Kerala, India (2022).

Background:

In July 2022, the first case of deep fake fraud was reported in Kerala, India. This brought attention to the significant misuse of synthetic media. A 73-year-old man named Radhakrishnan was fallen into a ₹40,000 scam which involved advanced deepfake technology. [1]

Case Details:

Radhakrishnan received a call from someone who mimicked the voice of his former colleague and friend Venu Kumar. The fraudster, using AI manipulated their voice to match his friend's voice and claimed to be in urgent financial need and requested a loan of ₹40,000. Radhakrishnan, unaware that it was actually not his friend, transferred the money. When he was unable to contact the real Venu Kumar, he discovered the fraud and filed a police complaint. [1].In investigation Kerala police uncovered that sophisticated AI technology was used to mimic Venu Kumar's voice. The details about the connection between Radhakrishnan and Venu Kumar was accessed by the scammer using a social media platform. The money was traced to a bank account in Maharashtra, leading to an ongoing investigation. [1]

Deep fake videos of India's leading business personalities duped the citizens of Bengaluru.

Background Of the Case:

Bangalore City was the target of a technologically advanced cybercrime using deep fake technology in Nov 2024, in which two residents Veena KG (57 years old lady from Banashankari) and Mr. Ashok Kumar TS, (Anekal, Retired) have been swindled to the tune of approximate ₹87 lakh.

The fraudsters produced a doctored video that featured N.R Narayana Murthy co-founder of Infosys and Mukesh Ambani the chairman of Reliance industries impersonating these respected personalities as endorsing trading platforms. The scams were mainly perpetrated using social media platforms such as Facebook and Instagram. This shows that there is an alarming expansion of the technology synthetic media and its use in deception brought forth financial crimes. [2] [3]

Incident details:

Case 1: Veena K.G, who initially came across a deep fake footage of Mr. Narayana Murthy in which he was endorsing a platform on Facebook. Believing that this promotion is real and genuine she clicked on the malicious link which was enclosed within the video and also shared her contact information on the phishing website. Within no time, she was approached by an agent who claimed to represent the platform, explained to her the details and convinced her to invest ₹1.4 Lakh. At first, she received a small return of ₹8000, which gave her more trust in the platform. Encouragingly she invested another ₹6.7 lakh but did not receive any more returns. Following that she came across another scam on Instagram which advertised to offer the work from home opportunity. She was lured by this opportunity of earning money from easy tasks, she invested around ₹67 lakh in this scheme. Although she had received a profit of ₹55,997, which was reflected in the platform, she was asked to pay a hefty amount of taxes to withdraw the amount. Failing to get in touch with the agents representing the platform, she understood she had fallen prey to this scam and registered a complaint with the police. [2] [3]

Case 2: In a similar incident, Mr. Ashok Kumar T.S, retired Government employee, noticed a similar Facebook post which had a deep fake video of Mukesh Ambani endorsing a trading platform. Believing the authenticity of the video, he clicked open the link which was attached with the video and gave his credentials and invested a total amount of ₹19 lakh in two different bank accounts provided by the fraudsters. Similar to Veena, he got no returns or dividend and understood he was deceived and fallen as a victim for this scam after there was not contact or communication from the platform.

Both the incidents are registered under the Cyber Economic and Narcotics (CEN) south police station in Bengaluru City. Where enquiries and investigations are still in process. [2] [3]

Modus Operandi of the Fraudsters:

The fraudsters used the deepfake technology which altered and manipulated the genuine footage of Mr. Narayana Murthy and Mr. Mukesh Ambani, which probably obtained from the public appearances and events, to produce videos which seemed credible. The videos are shared in the social media platforms, embedding links which directed the victims to the imitation websites that mimicked the legitimate trading platforms. These fraudsters used psychological techniques and strategies to build their trust in investing and by providing initial payouts. This tactic convinced the victims that this scheme was genuine and authentic, leading them to invest more money. The scammers also approached the victims, impersonating agents or as a representative of the trading platforms to convince them about the further scheme's validity. [2]

Analysis:

These incidents showcase the dangerous possibilities of the synthetic media to deceive and mislead people to fall into different scams. The realistic quality of the deep fake videos have made it hard for the victims to distinguish their fraudulent intent. Public awareness campaigns are very crucial to inform and educate people about the trust of this synthetic media and the need to verify online information. Furthermore, technological solutions and interventions like creation and development of sophisticated tools to detect and identify manipulated media, which are important in preventing such cyber threats. To penalize the development and distribution of these deep fake materials, which are mostly utilized for fraudulent operations, stronger legal frameworks are necessary.

3. Methodologies.

In the modern era of Artificial Intelligence, there should also be a way of controlling and eradicating misuse of its advancements. In the context of synthetic media, there are some ways which can be used to detect & control synthetically manipulated images or videos. They are:

1. **AI-Based Detection Systems:** We can use trained AI models to recognize anomalies generated by other synthetic media generators.

2. **Quantum computing-Based Detection Systems:** Quantum algorithms can be used to analyze large datasets of real and synthetic media at unprecedented speeds, identifying subtle inconsistencies that current algorithms might miss**.**

3. **Real-Time Behavioural Analysis:** Analyse anomalies in behaviour and compare it with real and authentic data

4. **Eye Tracking and Facial Analysis:** Synthetic faces often fail to replicate natural eye movements or blinking patterns accurately. We can also use a deep learning method to identify the iris of the eye as every iris is unique and different, this will allow investigating personal to track down anyone. Analyse subtle facial movements or expressions that deepfake technology struggles to replicate convincingly.

5. **Crowdsourced Platforms:** Develop platforms where users and experts can collaboratively analyse, and flag suspected synthetic media using advanced detection tools.

6. **Legislative and Policy Innovation:** Governments and regulatory bodies could require digital media to include authenticity certifications or implement legal penalties for synthetic media misuse. Encourage the use of AI ethics frameworks that mandate transparency in synthetic media creation**.**

4.Algorithm For Detection.

Algorithm DeepfakeDetection(video_path):

Input: video_path (path to the input video)

Output: classification (Real/Fake), fake_percentage

Step 1: Load Pre-trained Model

model ← LoadPretrainedDataset()

Step 2: Initialize Frames

total_frames = 0

fake_frames = 0

Step 3: Extract Frames from Video

for frame in ExtractFrames(video_path):

total_frames = total_frames + 1

Step 4: Preprocess Frame

face_crop = DetectAndCropFace(frame)

if face_crop is None:

continue

preprocessed_frame = Preprocess(face_crop)

Step 5: Predict with Model

prediction = model.predict(preprocessed_frame)

if prediction > 0.5:

fake_frames = fake_frames + 1

Step 6: Calculate Results

Fake_percentage = (fake_frames / total_frames) × 100

```
if fake_percentage > 50:
    classification ← "Fake"
else:
    classification ← "Real"
```

Step 7: Return Results

```
return classification, fake_percentage
```

5.Cyber Jurisprudence: Emerging challenges and the need for regulations.

Deepfake technology, which is a major component in synthetic media, contributes to vast challenges in our country. The ever-evolving sector of Artificial Intelligence and Machine Learning has blurred the line between original and fabricated media. This risks the spreading of misinformation, identity theft, cyber fraud, political manipulation and violations of privacy and dignity. These challenges are not addressed properly as India lacks specific legislation to penalise deepfake related crimes.

Few of the existing legal provisions which can be used in deep fake cases are:

•The Right to Privacy, recognized as a fundamental right under Article 21 of the Indian Constitution, this right can be invoked to challenge unauthorised use of personal likenesses in deep fakes.

•Digital Personal Data Protection Bill (2022) aids in the protection of personal data and can be indirectly applied to deepfake related breaches.

Under Indian Penal Code (IPC), 1860

* Section 420 (Cheating)

* Section 468(Forgery)

These are the sections which can be used in cases of deepfakes as it can be related to cheating, fraud, impersonation or identity theft.

The Information Technology (IT) Act, 2000.

•Section 66E: Penalizes the violation of privacy through the capturing, sharing, or transmitting of an individual's visual representation without consent, with punishment of up to three years of imprisonment or a fine of 22 lakhs.

•Section 66D: Addresses impersonation using digital means, carrying penalties of up to three years of imprisonment and/or a fine of 71 lakhs.

•Section 66F: Pertains to cyber terrorism and can be applied if deepfakes are used to incite violence, disrupt government operations, or threaten national security.

Given that deep fakes are weaponised for promoting political propaganda and manipulation there is an immediate response required for this cause.

Intellectual property and Personality Rights.

The Indian Copyright Act of 1957 mainly affords protection against unauthorized creation and dissemination of deep fakes that can alter or copy copyrighted material to qualify as copyright infringement under Section 51. Deepfakes emit present problems under the Right of Publicity, which is a doctrine not created in Indian jurisprudence but also recognized in several court rulings. The Delhi High Court (ICC Development (International) Ltd v. Arvee Enterprises, 2003) established that all the publicity rights are governed by Articles 19 and 21 of the Constitution, reaffirming that people have their exclusive rights to their own personal characteristics, which includes their name, voice, image, and even likeness. In any case deepfake technology is used to commercially exploit a person's likeness without their permission, it can be challenged under the Right of Publicity.

Regulatory Measures and IT guidelines.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, has made it mandatory in social media platforms to identify and remove deep fakes. The enforcement is a bit patchy, however, and platforms conveniently invoke the issues of free speech and privacy. The 2022 amendment to these IT Rules compulsorily made mandatory for deep fakes or morphed videos to be removed within 24 hours of receipt of the complaint.A formal advisory has been released directing that the intermediaries like Instagram, Facebook, YouTube, X (formerly Twitter), and Google has to effectively inform their users about the dangers and effects of publishing or sharing deep fakes, which comes as the same is an offense under the Indian Penal Code and is punishable by the law. According to Minister of State for IT & Electronics, Rajeev Chandrasekhar, in the event of legal violations of the IT Rules being observed or reported, legal actions regarding the issue will be initiated.

All Platforms also need to ensure that content that is prohibited under the Rule 3(1)(b) of the IT Rules is effectively communicated to all users in the language of their own choice at the time of first their registration and on every subsequent occasion of login.

Recent Legal Cases:

There has been a significant rise in the popularity of deepfake cases as several celebrities are being targeted, causing public outrage. Landmark cases include celebrities such as Anil Kapoor, Rashmika Mandana, Sachin Tendulkar, N R Narayan Murthy etc.Measures to combat the threats needs a multi-pronged approach that includes legal, technological and digital literacy initiatives. Specific deepfake legislation that clearly defines synthetic media should be imposed. Moreover, social media platforms should moderate and actively remove deepfake content. India currently relies on fragmented laws; the increasing sophistication demands immediate legal reforms.

6.Conclusion

While the rising use of deepfakes and other synthetic media offer many new opportunities, they also present considerable issues. They raise several moral and security concerns, as they can be used in various cybercrimes such as fraud, evidence manipulation, identity theft, and other scams. The case study demonstrates an urgent need for rules and regulations to combat such cybercrimes. They also show the dangers of technologies such as artificial intelligence and specify the need for strict and effective measures to reduce and control the misuse of synthetic media. AI-based detection, quantum computing, eye-tracking analysis, and crowdsourced verification platforms can be used to identify and prevent cybercrimes associated with synthetic media. In addition, the public needs to be made aware of such cybercrimes and the dangers of deepfakes and other synthetic media.

This research emphasizes the necessity of effective detection and ethical guidelines for reducing the risks regarding the misuse of synthetic media.

7.References

1. *Squad, I. C. (2023, November 27). Case Study: Kerala's first deepfake fraud. Indian Cyber Squad. https://www.indiancybersquad.org/post/case-study-kerala-s-first-deepfake-fraud*
2. *Desk, T. T. (2024, November 4). Bengaluru residents duped of Rs 95 lakh by deepfake videos of Narayana Murthy and Mukesh Ambani. The Times of India. https://timesofindia.indiatimes.com/technology/tech-news/bengaluru-residents-duped-of-rs-95-lakh-by-deepfake-videos-of-narayana-murthy-and-mukesh-ambani/articleshow/114955868.cms*
3. *HT News Desk. (2024, November 4). Two Bengaluru people fell prey to Narayana Murthy and Mukesh Ambani deep fake videos, loses close to ₹90L: Report. Hindustan Times. https://www.hindustantimes.com/cities/bengaluru-news/two-bengaluru-people-fell-prey-to-narayana-murthy-and-mukesh-ambani-deep-fake-videos-loses-close-to-rs-90l-report-101730688063694.html*
4. *Vig, S. (n.d.). Regulating Deepfakes: An Indian perspective. Digital Commons @ University of South Florida. https://digitalcommons.usf.edu/jss/vol17/iss3/5/*
5. *Bhaumik, A. (2023, December 4). Regulating deepfakes and generative AI in India | Explained. The Hindu. https://www.thehindu.com/news/national/regulating-deepfakes-generative-ai-in-india-explained/article67591640.ece*
6. *Drishti IAS Coaching in Delhi, Online IAS test series & study material. (n.d.). https://www.drishtiias.com/printpdf/perspective-combating-deepfakes*