REGULATIONS ON DETECTING,PUNISHING,PREVENTING DEEPFAKE TECHNOLOGIES BASED FORGERY

Yuan LingYun
Tashkent State University of Law
Yuanlingyun9@gamil.com
https://doi.org/10.5281/zenodo.11408227

ARTICLE INFO

Qabul qilindi: 20-May 2024 yil
Ma'qullandi: 25- May 2024 yil
Nashr qilindi: 31- May 2024 yil

KEYWORDS

deepfakes technology、*criminal law*、*cybercrime*、*The judicial system*、*investigation*

ABSTRACT

With the continuous advancement of deepfake technology, its scope and depth of application are also expanding. As an open-source code, the development of deepfake technology has promoted the popularity of AI face-swapping and AI voice-swapping services, which aim to provide convenient entertainment experiences and meet the daily needs of the general public. However, at the same time, these tools also provide new possibilities for criminals. Therefore, this paper will explore the application of deepfake technology in criminal activities, including subsequent investigation and punishment, and propose effective countermeasures against cybercrimes involving deepfakes.

IIntroduction

The Double-Edged Sword of Deepfakes

Introduction: In recent years, the rapid development of deepfakes has ushered in the era of synthetic media ahead of schedule. People can use deepfakes technology to synthesize or modify video or film content, generating high-quality synthetic videos where individuals can say, do, or express things they haven't actually said, done, or expressed. While deepfakes technology holds potential applications in entertainment, creative expression, and digital content production, it has also raised concerns in social and legal domains due to its potential for misuse in deception, dissemination of false information, fraud, and other inappropriate purposes. In judicial practice, the false evidence introduced by deepfakes poses serious challenges to the scrutiny process reliant on the high fidelity of photos and videos. Therefore, it is imperative to carefully assess the potential impact of deepfakes and take necessary measures to address possible misuse and adverse consequences. At the same time, it is essential to balance innovation and protection to ensure that technological advancements do not undermine societal interests or legal fairness. In this challenging yet opportunistic era, in-depth research and understanding of deepfakes technology are needed to effectively address the issues it brings and uphold societal stability and security.

Research methods

employ legal textual analysis method, legal policy analysis method, and case analysis method for my research.

IMain content of the disscuss and result

A.Background: Evolution and Development of Deepfakes

The emergence of "DeepFakes" marks a significant advancement in the field of facial swapping technology. It combines deep learning and fake photos, leveraging big data and artificial intelligence techniques, based on data algorithms and facial databases, to replace facial images of individuals in existing videos or photos. On the open-source platform GitHub, DeepFakes is described as "a tool that utilizes deep learning technology to identify and simulate characters in photos and videos." DeepFakes only requires sufficient image and video materials and certain hardware support to establish a matching algorithm model, thereby creating face-swapping videos. The developers of this technology directly open their algorithm code on major forums and have created an open-source project on GitHub, making DeepFakes technology easily accessible. For example, in the summer of 2017, a group of computer scientists at the University of Washington (referred to as "UW") caused a sensation by developing an algorithm that allowed them to generate a realistic yet false video based on real audio and video clips, featuring former President Barack Obama.

B.Identification of the Problem: The Dark Side of Deepfake Technology

Despite its initially benign intentions, deepfakes technology inadvertently opened Pandora's box, providing advantageous tools for deception and manipulation to criminals. The democratization of AI synthesis services has lowered the barrier of entry for cybercriminals, enabling even untrained individuals to produce highly convincing fake videos and audio recordings. Although most commercially available software services currently produce fake videos and audio recordings that can be easily identified as AI-generated, there still exists highly sophisticated and difficult-to-distinguish deepfake videos created for criminal purposes, posing the following potential threats:

1.Dissemination of False Information: Deepfake videos can create seemingly authentic scenarios and speeches, thus they may be used to spread false information, rumors, or malicious propaganda. This could lead to confusion among the public regarding authenticity and credibility, disrupting social stability and trust relationships.

2.Political Interference: Deepfake technology can be used to fabricate speeches or actions of political figures, potentially employed to manipulate voter opinions, interfere with elections, or tarnish the image of political opponents, thus posing a threat to democratic institutions and political stability.

3.Reputation Damage: Individuals or organizations may become targets of deepfake technology, with their images and reputations maliciously tarnished. False videos may be produced, leading people to believe that someone has engaged in misconduct or made inappropriate statements, thereby negatively impacting the reputation of individuals or organizations.

4.Personal Privacy Violation: Deepfake technology can be used to apply individuals' facial features to pornographic content or other inappropriate scenes without permission, infringing upon personal privacy rights. This could result in victims suffering emotional and psychological trauma, damaging their personal dignity and rights.

5.Financial Fraud: Deepfake technology may be used to deceive financial institutions or individuals, such as creating fake videos to trick users into transferring money or disclosing personal sensitive information, leading to an increase in financial fraud cases.

C.Deepfakes countermeasures

1.How to investigate Deepfakes after a crime occurs

Digital Forensics: Analyze digital evidence that may contain Deepfakes content, including videos, audio, and images. By examining metadata, analyzing pixel-level details of images or videos, detecting editing traces, etc., attempt to determine if Deepfakes technology has been used.

Technical Analysis: Utilize professionals with expertise in Deepfakes technology to conduct technical analysis and tracing, to identify the tools, software, and techniques used to create false content. This may involve collaborating with professional technical personnel to perform in-depth computer vision and machine learning analysis.

Social Media and Web Monitoring: Monitor information dissemination on social media platforms and the web, searching for signs and clues that may contain Deepfakes content. Monitor user-posted content, comments, and interactions to discover potential dissemination of false information.

Investigation and Evidence Collection: Investigate and collect evidence from individuals suspected of producing or disseminating Deepfakes, including gathering relevant evidence, witness testimonies, and other investigative leads. This may require collaboration with law enforcement agencies to conduct on-site investigations and evidence collection.

Collaboration and Information Sharing: Collaborate with international law enforcement agencies, technology companies, and academia to share information and resources, strengthening monitoring and combating of Deepfakes criminal activities. By establishing cooperation mechanisms and information sharing platforms, enhance the ability to identify and respond to Deepfakes crimes.

2.Pnalties:

Fraud Offense: If Deepfakes are used to create false vPideos or other content to deceive others, it may violate relevant laws related to fraud offenses. Fraud offenses typically involve intentionally misleading others, resulting in economic losses or other damages.

Defamation and Insult Offense: If Deepfakes videos are used to defame, insult, or disparage someone's reputation or reputation, it may violate relevant defamation and insult offenses. This behavior may be punishable by law, especially when it causes actual harm to the victim's social reputation and psyche.

False Evidence Offense: If Deepfakes are used as false evidence to interfere with judicial proceedings, it may violate the offense of false evidence. This may include forging or tampering with videos, audio, or images to influence the outcome of investigations, trials, or other judicial proceedings.

Invasion of Personal Privacy Offense: If Deepfakes videos infringe on an individual's privacy rights, such as applying their facial features to pornographic content or other inappropriate scenes, it may violate relevant laws related to invasion of personal privacy offenses.

3.Prevention:

A.Enhancing Personal Information Management: Strengthening the security of personal information collection, storage, and processing processes, including the adoption of encryption technology, access control, and data backup measures, to prevent personal information from being maliciously exploited for deepfakes.

B.Enhancing Protection of Personal Biometric Information: Particularly for biometric identification information (such as facial features, voice, etc.), enhancing the security of its collection and storage, limiting its usage scope, and preventing it from being used for creating deepfakes videos, etc.

C.Multi-channel Verification of Identity: When engaging in sensitive transactions or communications, verify identities through multiple channels, including real-time video calls, face-to-face meetings, etc., to ensure the authenticity of the other party's identity and reduce the risks associated with deepfakes.

D.Boosting Public Awareness: Through conducting promotional activities, organizing training courses, etc., raise public awareness and vigilance against deepfake threats, educate people on how to identify and respond to deepfakes, thereby effectively reducing their impact.

E.Strengthening Legal Supervision: Formulate and improve relevant laws and regulations, clarify the legal responsibilities and punishment standards for deepfake behaviors, increase efforts to crack down on infringers, and establish stricter legal boundaries for deepfakes activities.

Technological Innovation and Research: Increase research and innovation efforts in deepfake technology, develop more advanced deepfake detection and defense technologies, and enhance capabilities and levels of combating deepfakes.

F.Enhanced Network Security Protection: Strengthen network security protection measures to prevent hacker attacks and malicious software infections, safeguard the security of personal information and biometric information, and reduce potential pathways for deepfakes penetration.

IV Concluation

In the digital era, the proliferation of Deepfakes in digital media has made it increasingly difficult for the public to access the truth, diminishing trust in videos and photos and creating a crisis of trust brought about by technological advancements. This paper explores the importance of maintaining public trust in the digital age starting from the threat posed by Deepfakes, and proposes a series of response measures from investigation, punishment, to prevention.

Enhancing personal information management and protecting personal biometric information are crucial measures to prevent Deepfake manipulation. Through encryption technology, access control, and other means, the misuse of personal information can be effectively prevented. Additionally, employing multi-channel verification methods for confirming identities can mitigate the risks associated with Deepfakes.

Furthermore, intensifying publicity efforts and increasing public awareness of Deepfakes can enhance public vigilance and reduce their detrimental effects. In terms of legal supervision, establishing comprehensive laws and regulations, specifying legal responsibilities and punishment standards for Deepfake behaviors, and enforcing strict penalties are essential safeguards for maintaining integrity.

Moreover, technological innovation and research are equally crucial in combating Deepfakes. By developing more advanced detection and defense technologies, capabilities to counter Deepfakes can be enhanced. Finally, strengthening network security protection to prevent hacking attacks and malicious software infections is imperative for safeguarding personal and biometric information security.

In conclusion, only through the comprehensive application of various measures and concerted efforts can integrity be effectively maintained in the digital age, ensuring the healthy development of society and the security of individual rights.

References:

1. Deressa Wodajo,Solomon Atnafu.Deepfake Video Detection Using Convolutional Vision Transformer:Jimma University and Addis Ababa University.2102.11126v3.pdf (arxiv.org)
2. Naciye Celebi1 , Qingzhong Liu1 and Muhammed Karatoprak:A SURVEY OF DEEP FAKE DETECTION FOR TRIAL COURTS.Department of Computer Science, Sam Houston State University, Huntsville, TX, USA 2Department LLM in US Law, The University. Of Houston, Houston, TX,USAA_Survey_of_DeepFake_for_trial_courts (arxiv.org)
3. Faceapp.com.(2019).FaceApp.[online]Availableat:https://www.faceapp.com/ [Accessed 21 Oct. 2019].
4. Deepfakes policy, https://www.csis.org/analysis/trust-your-eyesdeepfakes-policy-brief, Sept.2019.
5. **林山程**. 网络冒充类诈骗犯罪的成因及防控对策研究 [J] . 网络空间安全，2022，1（3 2） ：84-88.
6. [6]Lilian Edwards.Issue: December 2022 / Categories: AI and the Bar , Justice Matters Deepfakes in the courts | COUNSEL | The Magazine of the Bar of England and Wales (counselmagazine.co.uk)