World Bulletin of Social Sciences (WBSS)
Available Online at: https://www.scholarexpress.net
Vol. 52 November 2025
ISSN: 2749-361X

METHODS FOR DETECTING AND INVESTIGATING CRIMES INVOLVING DEEPFAKES

Djamatov Mustafa Xatamovich,
Senior lecturer, Department of digital technologies and information security, Academy of the ministry of internal affairs of the Republic of Uzbekistan
Gulomova Dilxumor Baxtiyorxuja qizi,
Cadet of the Academy of the Ministry of Internal Affairs

Article history:

Received: 30th August 2025
Accepted: 26th September 2025

Abstract:

In the modern digital society, artificial intelligence technologies, particularly deepfakes, have become not only creative tools but also means of committing crimes. This paper examines the main types of crimes associated with the use of deepfakes, including the dissemination of defamatory materials, fraud, invasion of privacy, and political manipulation. Special attention is given to the methods of detecting and investigating such offenses. The study analyzes current deepfake detection algorithms, forensic video and computer-technical examination techniques, as well as issues of legal regulation and international cooperation in this field. The problems of identifying the sources of fake content and collecting digital evidence are highlighted. The conclusion emphasizes the need for a comprehensive approach combining technical, legal, and forensic methods to effectively counter crimes based on the use of deepfake technologies.

Keywords: deepfake, artificial intelligence, digital forensics, fake detection, investigation, cybercrime, digital evidence.

INTRODUCTION:

With the advancement of artificial intelligence (AI) technologies and generative neural networks, the emergence of deepfakes has become a new threat to society and the state. These highly realistic digital fabrications can be used for fraud, blackmail, disinformation, and interference in political processes. Deepfakes represent a serious challenge to public security: they can be employed to compromise individuals and institutions, disseminate false information, and manipulate social or political narratives. The effective detection and investigation of such crimes require a systematic approach that integrates technological, legal, and organizational measures. The purpose of this article is to examine in detail modern methods of deepfake detection, stages of forensic investigation, and the implementation of these practices within law enforcement activities.

The term deepfake (from "deep" and "fake") refers to digital content—video, audio, or image—created using AI and machine learning technologies. In essence, a neural network reconstructs a video or photograph pixel by pixel based on existing samples. The primary goal of deepfakes is to imitate a person's appearance, voice, and facial expressions as realistically as possible. With the rise of generative neural networks, deepfake creation has become relatively accessible, while their quality has reached a level where it is difficult to distinguish a fake from the original with the naked eye. Deepfakes are typically generated using deep neural networks—most often Generative Adversarial Networks (GANs). The principle of GANs is straightforward: one neural network generates synthetic content, while another evaluates its realism, forcing the generator to produce increasingly authentic results.

METHODS:

A comprehensive investigation of crimes involving deepfakes requires a robust legal framework recognizing digital evidence. In Uzbekistan, the 2024 Law on Digital Evidence established the legal status of audio, video, and other electronic files; requirements for maintaining their integrity and authenticity; and mandatory expert participation in seizure and examination procedures. This law enables the use of digital evidence in courts, provided that all procedural requirements are strictly observed—a particularly critical factor in deepfake-related cases, where even minor breaches in the chain of custody may render the material inadmissible. To support law enforcement agencies, specialized digital forensics centers have been established. In Uzbekistan, the Research Institute of Digital Forensics was created under the Academy of Law Enforcement Agencies. Its main functions include:

- conducting examinations of digital materials;
- training personnel in methods of forgery detection;

World Bulletin of Social Sciences (WBSS)
Available Online at: https://www.scholarexpress.net
Vol. 52 November 2025
ISSN: 2749-361X

– building databases for digital evidence analysis; and
– facilitating the introduction of electronic systems for evidence exchange (e.g., E-forensics).

The effectiveness of investigations depends not only on technology but also on strict procedural compliance: maintaining a verifiable chain of custody, ensuring file authenticity, and protecting data from alteration during transfer and storage. Without adherence to these standards, even the most sophisticated detection methods may be ruled inadmissible in court. Modern methods of deepfake detection fall into several categories: metadata analysis, visual analysis, audio analysis, and AI-based detection. File metadata contains information such as recording date and time, device type, and camera settings. Inconsistencies between these data and the claimed source may indicate manipulation. Common techniques include:

– verification of photo EXIF data;
– analysis of digital signatures and watermarks;
– tracking file transmission and modification history.

The goal of metadata analysis is to identify traces of editing, inconsistencies, and potential tampering.

Video deepfakes often contain subtle artifacts detectable through careful analysis:

– facial and blinking irregularities: generative models sometimes create unnatural eye or lip movements;
– lighting and shadow anomalies: mismatched light direction or unrealistic shading;
– motion discontinuities: abrupt frame transitions or inconsistent facial positioning;
– frequency artifacts: irregular smoothing patterns detectable through frequency-domain analysis.

Neural networks and machine learning algorithms are also employed:

– CNNs and autoencoders trained on large deepfake datasets to recognize hidden indicators of forgery;
– GAN-specific detection models that identify artifacts typical of generative synthesis;
– multimodal approaches comparing video and audio synchronization—discrepancies between lip movements and speech often suggest falsification;
– interpretable models that visualize detection features, facilitating the judicial use of technical evidence.

Audio deepfakes are detected through:

– spectrogram analysis revealing anomalies in high and low frequencies;
– phonetic cues such as unnatural breathing, pauses, or background noise;
– robustness testing by altering playback speed or adding noise to observe changes.

Crimes involving deepfakes exhibit several distinctive characteristics:

– concealment and scalability: falsified materials can spread instantly and anonymously online;
– high content realism: fakes are nearly indistinguishable from authentic recordings without expert analysis;
– international dimension: sources are often located abroad, complicating legal jurisdiction;
– legal complexity: digital evidence must meet strict admissibility standards in court.

These factors make investigation particularly challenging and necessitate specialized methodologies.

The investigation of deepfake-related crimes is a complex, multi-stage process requiring coordination across law enforcement departments and the use of advanced technologies. The initial stage begins with the filing of a complaint by individuals, organizations, or state bodies, or with the detection of suspicious content online or on digital devices. It is essential at this stage to assess the nature and scale of the threat in order to determine subsequent actions.

RESULTS AND DISCUSSION

The next stage involves the seizure and documentation of evidence. Original files must be preserved in their unaltered form with full documentation of the chain of custody to ensure admissibility and prevent tampering. Particular attention is given to secure data transfer channels and protected storage media. The subsequent technical analysis stage is central to the investigation. Here, specialists examine file metadata, analyze visual and audio cues, and detect anomalies in facial expressions, blinking, lighting, and lip–voice synchronization. AI-based algorithms are applied to uncover hidden generative artifacts. Machine learning enables the identification of even highly refined forgeries. The materials are then submitted for expert evaluation. In controlled laboratory settings, qualified specialists perform an in-depth analysis using professional digital forensics tools. The resulting expert report provides detailed methodologies and confirms the fact of manipulation—an essential element for judicial proceedings. The following stage involves inter-agency and international cooperation. In cases of cross-border dissemination, law enforcement agencies collaborate with international partners, as well as with social media platforms, messaging services, and hosting providers to obtain logs and additional data. All such actions must comply with legal and privacy requirements.

World Bulletin of Social Sciences (WBSS)
Available Online at: https://www.scholarexpress.net
Vol. 52 November 2025
ISSN: 2749-361X

The final stage is the judicial presentation of evidence. Expert reports must be clearly structured and comprehensible to non-specialist judges and legal professionals. It is important not only to prove the fact of falsification but also to explain the technical aspects of the detection process in a transparent and convincing manner. Only through compliance with all procedural steps can the investigation be considered complete and effective.

CONCLUSION

Deepfakes are becoming one of the most serious digital threats of modern society. Their ability to generate audio and video materials virtually indistinguishable from reality opens new avenues for criminal activity—from fraud and extortion to the destabilization of political systems. Effective counteraction to such threats is possible only through a comprehensive approach that integrates advanced technological tools, rigorous procedural standards, and a mature legal framework. The use of cutting-edge AI algorithms, forensic methodologies, and analytical systems makes it possible to detect hidden signs of manipulation, preserve the integrity and authenticity of digital evidence, and present it properly in court.

The key factor in this process is the professionalism and expertise of specialists capable of not only detecting deepfakes but also presenting their findings in a legally sound manner. Continuous improvement of detection techniques, adoption of innovative technologies, training of law enforcement personnel, and active collaboration with international experts are all essential components of an effective strategy. Thus, the combination of technological expertise, legal precision, and professional competence creates a reliable system for countering deepfake-related crimes, ensuring the protection of citizens' rights, the security of the digital environment, and the public's trust in the rule of law.

REFERENCES:

1. Закон Республики Узбекистан "О кибербезопасности" №ЗРУ–660 от 15 апреля 2022 года // Lex.uz..
2. INTERPOL Cybercrime Strategy 2022–2025. Lyon: Interpol General Secretariat, 2022..
3. Семёнов П. А. Правовые основы противодействия киберпреступности: монография. – Санкт-Петербург: Изд-во СПбГУ, 2020.
4. Mahamadov, R. (2022). Prospects for the application of artificial intellectual technologies in education. *Technika [tecHnka]*, *1*(7), 1-10.
5. Рустам Хабибуллаевич Махамадов, & Мустафа Хатамович Джаматов (2022). Кибержиноятчилик ва кибертерроризм таҳдидларига қарши кураш. Central Asian Research Journal for Interdisciplinary Studies (CARJIS), 2 (5), 103-108.
6. Makhamadov Rustam Khabibullayevich, & Djamatov Mustafa Khatamovich. (2025). Modern intellectual systems: status, functions, technologies and development tendencies. American Journal Of Applied Science And Technology, 5(02), 52–55. https://doi.org/10.37547/ajast/Volume05Issue02-13