Chapter 6
Deep Learning for Digital Forensics:
Advancing Criminal Investigations

Usharani Bhimavarapu
https://orcid.org/0000-0002-0246-1420
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, India

ABSTRACT

Digital forensics has evolved significantly with advancements in artificial intelligence (AI) to enable faster, more accurate, and more scalable criminal investigation evidence collection. Traditional forensic procedures are overwhelmed by the volume, complexity, and fragility of digital evidence. AI-based forensics merges machine learning, predictive analytics, and automation in order to make digital artifact identification, preservation, and analysis better. This essay describes cutting-edge AI-based methods of forensic investigation, including deep learning-based anomaly detection, decision trees-based forensic classification, and ensemble methods to variance reduction in forensic predictions. Using AI, forensic analysts can spot patterns, follow cybercrime patterns, and relate digital evidence with greater precision. AI-based applications also assist in automating routine forensic work, reducing human errors, and improving legal investigations.

INTRODUCTION

Digital forensics is now a crucial part of contemporary investigations that allows law enforcement agencies and cybersecurity experts to process electronic evidence effectively. The widespread expansion of digital devices, cloud computing, and

DOI: 10.4018/979-8-3373-0245-4.ch006

encrypted communication streams has made evidence acquisition more complex. Conventional forensic processes are unable to cope with the sheer amount of digital data, and AI-based systems are no longer a choice but a necessity. AI-powered forensic tools are able to process large datasets, identify anomalies, and automate mundane tasks to make investigations more efficient. With machine learning algorithms, investigators can detect concealed patterns in digital evidence that would otherwise remain undetected. These technologies cut down the time taken for forensic analysis by a considerable margin while enhancing accuracy. Further, AI-driven natural language processing (NLP) helps investigate text messages, emails, and online chats for criminal intent. By automating some parts of digital forensics, the experts can give all their attention to analyzing the results and making well-informed decisions. As cybercrimes keep changing, AI is also playing a significant part in reinforcing digital evidence gathering and forensic investigations.

Ensuring the authenticity and integrity of the data is one of the greatest challenges in collecting digital evidence. AI-powered forensic tools assist in authenticating evidence by preserving digital fingerprints using cryptographic hashing methods. These instruments guarantee that the data gathered is not tampered with during the investigation process, which is a requirement of legal admissibility. Another point is that AI-based anomaly detection can detect manipulated or tampered files, guaranteeing only authentic evidence is brought under consideration. Based on AI-powered forensic imaging, investigators can recover deleted files, hidden partitions, and encrypted information from storage media. Traditional forensic methods are usually inadequate in the case of sophisticated cybercrime methods like steganography or deepfake manipulation. AI solutions employ sophisticated image recognition and deep learning algorithms to detect manipulated or forged media files. Additionally, blockchain-based forensic solutions provide a decentralized and tamper-evident method for protecting digital evidence. These technologies enhance the credibility of forensic investigations, making sure that the evidence holds up to scrutiny in court.

Artificial intelligence-based automation is essential at the early phase of digital forensic examinations. Triage tools driven by AI have the ability to rapidly scan and categorize digital evidence by relevance, minimizing effort. Automated detection of keywords and metadata extraction aid forensic examiners in finding significant information from email, documents, and chat conversations. Facial analysis and biometrics enable investigators to compare suspects to security camera imagery or social media photos. AI-powered forensic software can also scrutinize mobile geolocation data and GPS logs, offering investigators movement patterns. Speech-to-text algorithms assist in converting audio recordings to searchable text, making it simpler to analyze voice messages and phone calls. With the help of deep learning models, AI is able to identify patterns of financial cybercrimes' fraudulent transactions. These automated functions greatly minimize data-sorting time, enabling