SUPREMO AMICUS

INDIA'S FIRST AI INTEGRATED LAW JOURNAL

Peer Reviewed, Refereed and Open access Journal

- Available in 331+ International Libraries
- Indexed at 32 Databases

ISSN NO. 2456-9704
Volume 10 Issue 1
www.supremoamicus.org

DISCLAIMER

The information presented in this article is intended for general informational and educational purposes only. While every effort has been made to ensure that the content is accurate, up-to-date, and reliable at the time of publication, the editorial board and publisher make no representations or warranties of any kind, express or implied, regarding the completeness, accuracy, reliability, suitability, or availability of the information contained herein.

The views and opinions expressed in this article are those of the author and are based on personal research, experience, and interpretation. They do not necessarily reflect the official policy, position, or opinions of any affiliated organization, institution, or entity.

This article is not intended to serve as professional advice of any kind. The editorial board and publisher shall not be held liable for any errors or omissions in the content, nor for any losses, injuries, or damages arising from the use of or reliance on this information.

ABOUT THE JOURNAL

Supremo Amicus is an online, peer-reviewed international journal devoted to the interdisciplinary fields of law and science. In an era marked by rapid technological progress and evolving legal frameworks, the journal seeks to bridge the gap between these two dynamic domains by offering comprehensive and critical insights into their various aspects. The journal places a strong emphasis on contemporary advancements, emerging trends, and the complex challenges faced by both the legal community.

The primary objective of the journal is to encourage and promote original, high-quality research. It is committed to publishing well-researched, analytically sound, and thought-provoking articles that adhere to rigorous academic standards. Each submission undergoes a thorough peer-review process to ensure authenticity, relevance, and scholarly integrity. In doing so, the journal maintains its commitment to excellence and credibility.

In addition to fostering research, the journal aims to make complex ideas accessible and engaging for a diverse readership. It strives to present content that is not only intellectually enriching but also clearly written and reader friendly.

Furthermore, the journal is committed to promoting interdisciplinary collaboration and global engagement. It welcomes diverse perspectives from contributors across different regions and backgrounds, thereby enriching the quality and scope of discussions presented within its pages.

With this vision we proudly present Supremo Amicus to our readers.

-Editorial Team
Supremo Amicus

INTRODUCTION TO CRIMINAL LAW, THE LEGAL SYSTEM, AND THE RELEVANCE OF FORENSIC EVIDENCE IN TRIALS

By *Dr Manoj Singh*

Abstract

Criminal law is a vital branch of jurisprudence that defines crime within society and establishes rules for its punishment, thereby maintaining public order and ensuring justice. It operates through multiple components, including law enforcement, defence, prosecution, and the judiciary, each of which plays a crucial role in administering justice. Fundamental principles such as the presumption of innocence, procedural safeguards, and the burden of proof guide this system. The criminal justice mechanism comprises statutes, judicial decisions, and procedural frameworks that uphold natural justice, due process, and appropriate sentencing.

However, the complexity of criminal cases and the possibility of human error often make the reliability of witness testimony and circumstantial evidence uncertain. In this context, forensic evidence has emerged as a significant tool in modern trials. It involves the application of scientific methods—such as DNA profiling, fingerprint analysis, toxicology, and digital forensics—to collect and analyse evidence for judicial purposes. Forensic science bridges the gap between law and science by providing objective, reliable, and verifiable information that can corroborate or challenge claims made during a trial.

The use of forensic evidence enhances the accuracy of investigations, reduces dependence on subjective testimonies, and strengthens the credibility of judicial outcomes. It also serves a deterrent function, as the likelihood of scientific detection discourages criminal behaviour. Courts increasingly recognise its importance, integrating forensic methods into standard adjudicatory practices.

In conclusion, forensic science has transformed the criminal justice system by promoting fact-based adjudication and reducing the risk of wrongful convictions. Effective coordination between forensic experts and legal professionals remains essential for ensuring fairness and justice.

Keywords: Forensic evidence, prosecution, judiciary, scientific methods, burden of proof, criminal adjudication.

INTRODUCTION

The criminal justice system relies heavily on establishing truth and accountability through a complex interplay of legal principles and evidence (Rosenzweig, 2022). Forensic science has emerged as an important multidisciplinary tool that is significantly helping in the objective reconstruction of events and the identification of perpetrators in criminal cases, particularly those involving serious offences, such as murder (Arul et al., 2023). Forensic science covers broad disciplines and includes pathology, toxicology, and ballistics. This scientific methodology permits investigators to determine material truth, which increases the capability of criminal investigations and prosecutions (Bansal, 2025).

Forensic evidence facilitates criminal justice administration in many ways, such as making investigations accurate and finding crime patterns, etc. (Mohsin, 2024). It is helping the Indian legal system in many ways. It ensures justice by providing scientific insights into complex criminal cases and assisting in the identification of offenders (Chawla, 2023). Indeed, the Indian criminal justice system, governed by the Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023, and the Bharatiya Sakshya Adhiniyam, 2023, fundamentally relies on extensive investigation and trial processes to ensure credible justice delivery (Kumar & Singh, 2024). Though there is a sufficient legal landscape, there are numerous issues like low conviction rate, delayed trials and inefficient investigations. All these issues are compounded by the mismanagement of forensic evidence (Kumar & Singh, 2024).

Forensic sciences results are helpful in prosecution, investigation and acquittal (O'Brien et al., 2015). Utilisation of the various scientific streams is

significant in crime scene investigation, evidence collection, and presentation in judicial proceedings (Kothari, 2023). These streams are DNA analysis, fingerprint examination, and digital forensics. Forensic science and digital technology have enhanced the competency of criminal investigations by providing systematic approaches to disclose facts and identify suspects (Bansal, 2025).

These technological developments in surveillance and digital forensics have played an important role in evidence collection and evaluation. Still, data reliability, ethical considerations, and the risk of bias have arisen issues. It is important to emphasise the role of forensic science in fair justice because it highlights its impact on legal outcomes. The Indian criminal justice system requires reliable forensic evidence in a trial for fair justice (Kumar & Singh, 2024).

The Indian Court have accepted the importance of forensic science in investigation (V.R., 2015). Evolving forensic competence enhances the efficiency of forensic experts in their task, such as reaching reliable results, thus advancing the systematic criminal investigation process (Saxena, 2025).

These forensic techniques improve accuracy and give a basis for judicial decisions (Chango et al., 2024). Technological developments are continuously improving investigative methods, making law enforcement much easier, and helping prevent crime (Bansal, 2025). Artificial intelligence and predictive policing are also a part. These factors are significant in analysing data. Identifying patterns and forecasting potential criminal activity, thereby improving efficiency and public safety (Pica et al., 2024). The fast development of new technologies enhances the ability for real-time, On-site forensic investigations that increase the speed, including efficiency, of the criminal justice system. Spectroscopic techniques and integrated forensic platforms are examples of such Technology. (Kloosterman et al., 2015).

In addition to this transformative impact of artificial intelligence on digital forensics and its application in combating "evil AI" with "good AI," a proactive reform of digital forensic capabilities is necessary to meet the strain brought by the dark side of digitalisation (Klasen et al., 2024). AI and forensic science use methods such as DNA analysis, pattern recognition, and crime scene reconstruction to improve the efficiency of processing and interpreting large amounts of data, thereby increasing the accuracy and speed of investigations. (El-Din, 2022). Such technological advancement is significant in the present time because digital devices and online activities generate a wide range of data, challenging traditional forensic methodologies (Mandayam, 2024).

Artificial Intelligence, machine learning, and other emerging technologies are proving their significance in criminal justice administration through various modes, such as digitising crime scenes, enabling remote analysis, improving biometric identification accuracy, and facilitating on-site analysis with small, handheld instruments (Chango et al., 2024). These technologies are reshaping digital forensics by improving data analysis capabilities, automating repetitive and time-consuming tasks, and improving efficiency, including the effectiveness of digital investigations (Mandayam, 2024). This is helpful in predicting future cyber threats and digital forensic investigations through automating the analysis and classification of these threats (Fakiha, 2023).

These technologies help quickly handle large amounts of data and uncover evidence. As a result, AI and ML play a key role in tackling the challenges of digital forensic investigations in the criminal justice system. Specifically, AI-driven solutions to improve the efficiency and accuracy of criminal investigations, particularly in cases involving extensive digital evidence (Dunsin et al., 2024). The increasing quantity of digital data with different digital devices creates a necessity for advanced tools, and AI and ML. The investigators are facing the changing nature of the digital world with increasing significance. It covers the benefits of AI and ML for image, text, and network analysis, including machine-assisted decision-making to enhance the speed and accuracy of forensic examinations.

These technologies help analysts process vast amounts of data swiftly and accurately and find crucial

evidence. The integration of AI and ML enables faster investigations. It reduces the burden on analysts by allowing them to focus on clearer, more interpretive tasks rather than exhaustive manual data sifting. It is especially helpful in cyberattack investigations, which require more robust investigative techniques (Dunsin et al., 2024). The need for advanced capabilities is growing as cybercrime rises.

Such developments are crucial because current forensic investigations, often reliant on human expertise and script-based tools, are susceptible to human error and demand considerable time and specialised knowledge. The complexity of digital forensic challenges, the large volume of data, the variety of digital devices, and the dynamic nature of the digital world necessitate the continued evolution of these AI- and ML-driven strategies.

Implementation of AI in digital forensics needs close attention to data validity and interpretability issues because it gives rise to significant challenges for researchers and practitioners. For addressing these issues, there is a need to develop standardised protocols for AI integration and foster greater transparency in algorithmic decision-making processes. Responsible utilisation of these technologies in criminal investigation is important for addressing data security and ethical issues.

METHODOLOGY

This section adopts a systematic approach to critically evaluate the existing literature on artificial intelligence (AI) and machine learning (ML) in digital forensics within the criminal justice system, identifying limitations, research gaps, and future directions. It examines how AI/ML techniques are applied across key forensic stages, including data collection, recovery, timeline reconstruction, big data analysis, pattern recognition, and maintaining the chain of custody.

While these technologies enhance efficiency by enabling rapid processing of large datasets and improving evidence detection through tools such as natural language processing and computer vision, they also raise significant challenges related to data privacy, security, integrity, and quality. Ethical and legal concerns, particularly bias and the need for explainability in court, further complicate their application. Machine learning aids in detecting anomalies and threats through predictive analytics and pattern analysis, but the overall effectiveness of current tools varies across contexts (Fattahi, 2025).

The integration of Large Language Models (LLMs) offers potential solutions to issues such as explainability and automation by analysing complex datasets and generating coherent investigative narratives. They are particularly useful for automating tasks such as report generation, anomaly detection, and sentiment analysis in forensic data, including logs and emails (Yin et al., 2025; Wickramasekara et al., 2024).

However, concerns regarding hallucinations, bias, non-deterministic outputs, and dependence on training data limit their reliability. Additional risks include data poisoning, prompt injection, and adversarial attacks, necessitating robust security measures and continuous monitoring. Compliance with legal frameworks like GDPR and CCPA is essential to ensure lawful use of AI in investigations. Despite these challenges, ongoing advancements highlight the growing importance of AI/ML and LLMs in transforming digital forensic processes, underscoring the need for cautious, regulated implementation.

DISCUSSION

This section reveals how large language models (LLMs) are useful in digital forensic workflows. It highlights their benefits and limits, exploring how LLMs are helpful in data classification, task identification and network forensics by their capacity to process and interpret huge and unstructured data.

LLMs can extract and synthesise chronological events from diverse digital artefacts and thereby. LLMs' capacity extended to advance threat intelligence. Here, they are capable of analysing global cyber threat landscapes and identifying changing patterns that may be relevant to continuous investigation, offering predictive insights (Wickramasekara et al., 2024).

LLMs have the potential to enhance the efficacy of evidence collection by detecting potential pieces of digital evidence within complex datasets, even in physical crime scene contexts. This is significant in the reservation and acquisition phase, where LLMs can generate specialised code to ensure data integrity. These models can facilitate the recovery of deleted files and expand the scope of automated forensic procedures by automating the creation of forensic images. Large Language Models (LLMs) can simplify complex legal and technical documents, expedite the reporting phase and ensure precision in findings, thereby playing a significant role in digital forensics.

Digital Forensics can be used as a service platform and thereby be useful in generating custom extraction APIs. It improves adaptability and keeps the investigation on track. Continuous improvement through retaining data with new datasets enables them to adapt to changing cybercrime trends and digital evidence. Multimodal models have become efficient by combining textual and visual data. Contrastive Language-Image Pre-training (CLIP) model learns a link between text and images, enabling deeper contextual understanding of digital evidence. This is helpful for investigators in reconstructing digital events more accurately, as they can correlate image metadata with textual communications, which helps them reconstruct digital events more accurately. Such innovations are significant in mobile forensics because large amounts of data from smartphones and messaging applications create significant analytical challenges for law enforcement agencies (Kim et al., 2025).

LLMs can analyse and interpret large amounts of conversational data, images, and hyperlinks from these applications. This ability is significant for streamlining investigations and uncovering new evidence that might otherwise be overlooked. This is true as there are now specialised systems for helping investigators in managing huge amounts of information from smartphones (Fähndrich et al., 2022). Increased processing capacity helps forensic experts better examine digital footprints and gain deeper insight into device data. These multi-models are important in detecting complicated deepfakes, thereby ensuring the integrity of evidence (Liu et al., 2024). Though AI tools achieve high accuracy, they face challenges across different crime scenes. They perform better in homicide cases compared to arson cases (Farber, 2025).

LMs and a database can increase data analysis efficiency. Their ability to process huge amounts of unstructured data identifies correlations and anomalies that might escape human investigators. Human expertise and AI's computational skill improve the accuracy and efficiency of cyber forensic investigations. LLMs trained on recent datasets could improve data analysis and help identify patterns (Daungsupawong & Wiwanitkit, 2023). Their special feature for processing large amounts of unstructured data helps identify connections and anomalies that human investigators may miss. This human expertise and data-processing capability can enhance the efficiency and accuracy of cyber forensic investigations, thereby improving overall cybersecurity. These advances provide significant potential, but there are still limitations, such as the technology's chance of "hallucinations" or generating factually incorrect information on LLMs. It makes it necessary to be careful in forensic applications.

LLMs and a database can increase data analysis efficiency. Their ability to process huge amounts of unstructured data identifies correlations and anomalies that might escape human investigators. Human expertise and AI. Despite having advanced capabilities, the issue of hallucinations in LLM responses occurs. It raises credibility and accuracy issues of AI systems and highlights the importance of validation mechanisms to reduce errors and improve decision-making quality (Kumamoto et al., 2023). To resolve these limitations, some measures need to be adopted, such as an extensive validation framework, explainable AI methodologies, including a human-in-the-loop system for assuring forensic integrity and AI-derived insights. This emphasises a regular feedback system between forensic practitioners and AI developers for refining models and mitigating

erroneous outputs (Hassanin & Moustafa, 2024; Zangana et al., 2024).

The development of explainable AI is important for enabling forensic experts to understand the reasons behind an AI's conclusions and ensuring transparency in crucial decision-making processes. The legal and ethical implications of deploying AI in digital forensics, including concerns regarding data privacy, bias in training data, and the potential for misuse, also demand careful consideration and the development of comprehensive regulatory frameworks. This framework should address the challenges of ensuring alignment across modalities and optimising multimodal fusion strategies, particularly as deepfake detection techniques become more sophisticated (Liu et al., 2024).

Further research could take into consideration holistic, theoretically-grounded approaches, especially getting advantage from Multimodal Large Language Models to enhance detection robustness, interpretability, and generalisation across modalities. We need to focus on advanced multi-modal fusion systems for enhancing single-modal detection methods. These can use cross-modal attention system contrastive multi-modal learning techniques, and unified multi-modal transformers. Future investigations must be centred on hybrid architectures able to combine localised spatial-frequency cues with multimodal semantic representations for enhancing the credibility of deepfake detection systems.

Such developments are crucial because of increasing sophistication in deepfake generation techniques, which use weaknesses in unimodal detection by changing multiple modalities simultaneously (Sharma et al., 2024). It is necessary to detect manipulated content for maintaining the integrity of digital evidence in legal proceedings (Verdoliva, 2020). This necessitates extensive benchmarking for text and visual interactions, including the development of focused cross-modal alignment strategies.

It is essential to improve the interpretability of multimodal models for real-world forensic use because it is helpful for experts in understanding model decisions and building trust (Wang et al., 2024; Mansoor & Iliev, 2025). It is important to maintain proper alignment within base LLMs and achieve accurate cross-modal coordination for ensuring stability in multimodal inference because it is key to reliable analysis (Zhang et al., 2024). This needs techniques such as adversarial domain alignment and meta-learning that enable models to adapt quickly to new manipulation methods and deepfake threats.

Combining robust multimodal analysis, explainable AI, and strict validation helps create trustworthy and legally sound forensic systems. Embedding invisible signals into media at the time of creation could serve as a proactive defence, though privacy and scalability remain issues. Future research should focus on defences for Diffusion Models targeting latent encoding and attention layers, and on hybrid detection methods that combine statistical patterns, generative inconsistencies, and semantic reasoning for stronger, more adaptive deepfake detection (Liu et al., 2024; Wang et al., 2024).

Proactive approaches are significant for disrupting deceptive attacks by leveraging technologies such as natural language processing and anomaly detection to identify and block complex adversarial strategies (Schmitt & Flechais, 2024). This arms race between generative AI and detection highlights the importance of continuous innovation in forensic AI. This continuous development must also consider the scalability and deployment efficiency of these detection systems, bottlenecked by teacher quality and domain alignment. This highlights the need for broad access to high-quality, diverse training datasets and experts who can mitigate bias and enhance the generalizability of forensic AI models across various digital crime scenarios.

It is important to integrate understandable artificial intelligence so that people can understand these systems. This helps human operators grasp how algorithms make decisions in complicated forensic investigations. The rise of highly realistic synthetic media known as deepfakes produces serious issues for the credibility of digital evidence and people's confidence in multimedia content (Amerini et al.,

2025; Ferrara, 2024). These synthetic media forms, generated through sophisticated artificial intelligence techniques such as generative adversarial networks and diffusion models, are capable of producing highly convincing but entirely fabricated images, audio, and video (Xu et al., 2024).

Deepfakes can affect criminal justice administration as they can be used to fabricate evidence, spread misinformation, and impersonate individuals, thereby highlighting the fairness of the judicial processes (Babaei et al., 2025). The growing issues make it necessary to develop extensive deepfake detection methodologies to ensure the authenticity of digital evidence presented in court. The availability of generative AI tools will likely face issues related to AI-generated content (Linna et al., 2024). This creates dual issues: the presentation of fabricated AI-generated evidence and the false accusation. Both issues contribute to the unreliability and bias of current AI detection technologies.

Legal frameworks and forensic protocols need to adopt a technique capable of distinguishing between authentic and synthetic content while accounting for AI detection limitations (Sandoval et al., 2024). Addressing algorithmic biases and interpretability issues in AI models is crucial for validating AI-generated evidence (Anand & Thakur, 2025; Fähndrich et al., 2022).

Explainable AI systems can enhance transparency and reduce distrust in AI-based digital forensics (Solanke, 2022). This involves developing standardised evaluation protocols for AI detection results and making legal precedent for their acceptance in the increasing prevalence of synthetic media. (Cooke et al., 2025; Mahara & Rishe, 2025; Babaei et al., 2025; Abbasi et al., 2025). The rise in digital counterfeiting due to advanced generative artificial intelligence necessitates a collective effort to develop a state-of-the-art detection method that can differentiate between trusted media and synthetic fabrications (Khan et al., 2025).

The rapid growth of deepfake technology makes it difficult to verify media. Differentiating real content from fake content becomes increasingly difficult, posing a threat to the integrity of evidence in legal situations (Buo, 2020). However, there is a lack of transparency in these detection systems, which often operate as "black boxes" that adversely affect human understanding of their decision-making processes (Mansoor & Iliev, 2025). It is necessary to research into Explainable Artificial Intelligence, focusing on making opaque AI models into transparent "glass box" models, thereby enhancing stakeholder understanding and trust in their output (Vu et al., 2024; Kelly et al., 2020). This increased transparency is crucial for establishing the admissibility and credibility of AI-driven forensic analysis in legal proceedings due to the rise of deepfakes. (Moreno, 2024).

Deepfake technology continuously creates challenges to maintaining effective detection capabilities because of its adversarial nature. (Wahab et al., 2025). This ongoing technological arms race highlights the importance of dynamic and adaptive forensic tools capable of evolving the sophistication of generative models (Gu et al., 2023). Due to this reason, a multidimensional approach to digital forensics, combining technical detection with strong law and policy frameworks, is necessary for resolving the multifold challenges created by generative AI (Ferrara, 2024). These developments make fabricated media highly realistic, including images, videos, and audio, which can be easily and inexpensively generated, thus posing significant challenges for forensic analysis and legal authentication (Banh & Strobel, 2023).

The development of explainable artificial intelligence for digital forensics is crucial because it offers a promising pathway to mitigate the opacity of complex AI algorithms by transforming "black box" models into more interpretable "glass box" systems (Kelly et al., 2020; Mansoor & Iliev, 2025). This change is crucial for building trust among legal practitioners and the public, who often lack confidence in AI-based digital evidence extraction due to concerns about transparency and credibility (Solanke, 2022). This approach is vital for ensuring that AI-driven insights can be effectively presented and scrutinised in a court

of law, thereby upholding the principles of justice and fairness. Deployment of explainable AI in forensic science requires rigorous validation across diverse datasets to ensure generalizability and resilience against adversarial attacks (Boneh et al., 2019).

Combining multimodal large language models with specialised forensic prompts is important for analysing and interpreting forensic cues, providing explanations that align with human thinking processes for detecting AI-generated images (Tan et al., 2025). This integration improves the use of AI in forensics by enabling detection and clear explanations of evidence, thereby increasing the credibility of AI-driven results in legal contexts. Many advanced deep learning models are very accurate but lack transparency, which is required for legal scrutiny, thereby necessitating explainable AI frameworks (Chellappan, 2024; Tariq et al., 2025).

Clear processes are necessary for effective use of AI in the judicial system (Zhang & Zhang, 2023). Explainable AI revealing too much could create vulnerabilities (Díaz et al., 2023). Combined use of multi-modal learning models like CLIP and large language models for deepfake detection by providing thorough explanations (Guo et al., 2025). For example, combining insights from GPT-4o with visual data enhances the system's robustness against attacks and improves deepfake detection (Liu et al., 2024; Ji et al., 2025).

The advancement of more robust and explainable deepfake detection methods uses the contextual understanding and analytical power of large language models to change raw forensic data into actionable legal intelligence. This integration is further enhanced by knowledge-guided forgery-adaptation modules that utilise contrastive learning, enabling more accurate detection and explanation of forged elements. This is crucial as digital forensic laboratories are handling more data, and traditional manual methods are insufficient (Yin et al., 2025; Wickramasekara et al., 2025). This shift towards AI-augmented forensic analysis is not without its own set of challenges, including the need to address potential biases in AI models and the complex ethical and legal considerations surrounding their deployment in judicial systems.

Despite these challenges, the ongoing development of explainable AI in digital forensics provides a way to bridge the gap between technical advancement and legal requirements by enabling AI decision-making processes to be transparent and verifiable, thereby fostering greater trust and acceptance of AI-driven evidence in courtrooms. This capability produces clear explanations and detects slight irregularities, improving human expertise in forensic work. It moves beyond the detection of simple anomalies to deeper insights (Tariq et al., 2025). For instance, Large Vision-Language Models can be used for deepfake detection by linking image features with fine and deepfake image descriptions. It enables classification and localisation of forgeries. These models, using knowledge-guided forgery prompts and lightweight prompt tuning, achieve better detection and localisation with less effort, marking a vital advancement in addressing the complex nature of modern deepfakes.

However, issues remain regarding the computational resources required to process large volumes of digital evidence and the inherent limitations of current LLMs, such as an inclination toward hallucinations and language dependency, which necessitate continuous human oversight. Future research should focus on optimising Large Vision-Language Models to mitigate these issues (Jiang et al., 2024).

It is essential to develop solid evaluation methods to ensure the reliability and accuracy of the LLM-generated forensic analyses, as matching human investigators' interpretative skills is a serious challenge. The integration of Large Language Models and digital forensics necessitates addressing issues of standardisation, interpretability, and validation of LLM-generated outputs to ensure their accuracy and confidence in investigations.

The efficacy of these models in forensic contexts is often affected by their over-reliance on training data and the inputs they receive, as well as their sensitivity to extraneous knowledge. It is necessary to improve

reliability, including the applicability of LLMs in digital forensic investigations, by developing robust prompt engineering methods and integrating diverse, representative datasets. There is a persistent issue of statistical inconsistency and a lack of emotional content in linguistic responses, which complicate their application in scenarios that require human-like interpretation. LLMs with automated agents pose new challenges for digital forensics regarding accountability and the potential for autonomous decision-making in legal contexts.

The existing challenges further extend to the absence of standard procedures, a large volume of data during investigations and the inadequacy of current tools in comprehensive analyses. For addressing these issues, it is necessary to develop an advanced computational system that can handle large volumes of data and create a tool capable of integrating various forensic analysis techniques.

Large Language Models and Generative AI provide an opportunity in handling these complex challenges, especially in improving the efficiency and accuracy of forensic investigations. LLMs can automate tasks such as keyword list creation, incident narration and code generation, which assists investigators in the digital forensic process. This automation includes incident recognition, where LLMs can streamline the initial identification of digital events requiring forensic scrutiny. LLMs can improve the quality and clarity of forensic reports, automate script generation, provide access to technical and procedural knowledge, and facilitate multilingual and sentiment analysis. In this way, they can significantly enhance investigative capabilities (Scanlon et al., 2023). LLMs can be used for code generation to preserve disc evidence. LLMs like StarCoder and Code LLaMA are useful in creating customised scripts and code.

In addition to analysis, LLMs are useful in different phases, such as reporting and examination. At the reporting phase, LLMs are useful by producing comprehensive reports, summarising complex findings, and translating technical data into accessible language for non-specialists, such as judges. During the examination phase, LLMs can help with data collection, recovery, and classification by performing file recovery, keyword searching, and pattern identification. They are also helpful for tasks such as cloud data extraction, deleted file recovery, and forensic media preparation.

This feature significantly streamlines the acquisition phase of digital forensics. LLMs can help in improving the efficiency and accuracy of evidence collection and digital forensic investigations analysis processes. They can improve real-time knowledge retrieval and decision-making. It is helpful in rapid responses to unfolding digital incidents. LLMs like Mobile-LLaMA are significantly useful in network forensics by detecting unusual patterns in network traffic.

Large Action Models and Voice of the Technician techniques optimise investigation by reducing routine tasks. It helps investigators concentrate on complex analysis and critical decision-making. This multidisciplinary approach combines numerous techniques and models. This approach highlights the rapidly evolving landscape of digital forensics, where advanced AI tools are crucial for handling the complexity of ongoing cybercrime investigations. This change shows a move towards automated and intelligent forensic frameworks, highlighting the crucial role of AI in tackling the limitations of traditional investigative methods. As a result, digital forensics is rising into a domain where AI-driven automation and smart analysis are necessary to maintain investigation efficiency and address the complexity of cyber threats (Loumachi & Ghanem, 2024).

CONCLUSION

These models are helpful in improving efficiency and minimising human error in complicated digital investigations in forensic frameworks. It also helps in the standardisation of the forensic procedures and reporting, which enhances trustworthiness and permissibility of the digital evidence in legal proceedings. This standardisation is important in growing complexity and volume of digital evidence.

The rising difficulty creates issues for conventional forensic methods, which make AI-enabled solutions

for maintaining investigation efficiency. AI, machine learning, and digital forensics face challenges regarding data volume, ethical considerations, and the limitations of existing models. Further research should focus on extensive AI/ML techniques which can manage vast and diverse datasets and develop frameworks for ethical AI implementation in the forensic context. One such challenge involves computational resources for processing the massive data inherent in digital forensics.

Lack of standardisation and interpretability within AI models present obstacles to their adoption and application in forensic analyses. Such issues necessitate developing more effective algorithms and explainable AI models to ensure forensic conclusions are accurate and understandable to experts.

The dynamic nature of digital evidence is another hurdle, as it changes frequently due to encryption or anti-forensic techniques, and further complicates AI-driven analysis. Machine learning and artificial intelligence capacity enhance digital forensic investigations by automated analysis and classification of cyber threats. The vast amount of data can overload even an advanced system. It necessitates a new method for processing and reducing data effectively.

Reliance on AI in digital forensics needs careful consideration of data validity because some effective methods need validation of the massive datasets processed by these systems. It poses a significant challenge to the reliability and admissibility of AI-driven forensic findings in legal contexts. Future research should develop frameworks to address training data biases and ensure the accuracy of AI-driven forensic results. These developments can address shortcomings of existing AI applications in digital forensics. The disparity of present tools and the complexity of digital data present serious issues.

The ethical use of AI in digital forensics, particularly regarding data privacy and algorithmic bias, warrants examination to maintain public trust and ensure fairness in judicial proceedings. This is the reason why transparent and interpretable AI models are essential to build confidence in their forensic utility and ensure their responsible deployment in legal frameworks.

The continuous increase in the quantity of digital data and the rise of advanced communication technologies necessitate the integration of artificial intelligence methods to effectively manage and process forensic evidence. This integration can significantly enhance the efficiency and accuracy of investigations by automating tasks such as data triage, incident detection, and forensic analysis.

Limitations of manual approaches are time-consuming and susceptible to human error, leading to the need to streamline the investigation. This problem can be resolved by AI digital forensic investigations. AI algorithms are capable of rapidly scanning vast volumes of data, including previously closed cases, leading to quicker, more accurate, and streamlined digital forensics, which also frees up investigators to concentrate on other critical matters.

AI and machine learning can make datasets more useful for forensic investigators. It will maintain accessibility, including safety, for databases of solved, unsolved, and pending cases. This highlights the need for digital solutions such as Artificial Intelligence, which can process and analyse the vast data generated by criminal activities. These tasks would otherwise be time-consuming for human investigators. In this context, AI and machine learning are useful in digital forensics, which involves the acquisition, processing, and analysis of large volumes of digital data for criminal investigations.

Despite the advantages, the existing manpower and government resources allocated to investigate cybercrimes are often insufficient, and existing digital investigation procedures still rely on human interaction, which slows the process considerably, given the rapid pace of digital offences (Iqbal & Alharbi, 2020). This highlights the need for advanced technological solutions provided by AI and ML to bridge the gap between investigative capacity and the increasing volume and complexity of cybercrime.

The fast-growing technology and integration of AI and ML technologies are ready to revolutionise digital

forensics by enabling more efficient and precise analysis of digital evidence. This is crucial in managing the increasing workload in digital forensic laboratories. These techniques offer a way to speed up investigations by automating data collection, analysis, and pattern recognition, leading to the saving of time in traditional digital forensic methods. Machine learning algorithms can be employed to swiftly sift through heterogeneous and voluminous datasets, addressing the challenges posed by the scale and complexity of modern digital environments that often overwhelm human investigators.

The emerging stages of AI and ML in digital forensics are very much crucial as they offer future research for enhancing their efficiency in cybercrime timeline reconstruction, data collection, and complex pattern identification. This enhanced capacity is significant in ensuring that forensic practitioners have developed tools to combat digital criminality. Machine learning is effective in automating the classification and analysis of cyber threats, enhancing the efficiency of cyber forensic investigations by identifying and categorising malicious activities .AI and ML have a special ability to learn from past data to create predictive models that can anticipate future cybercrime trends and potential attack vectors. This proactive feature accelerates incident response and strengthens preventative measures against emerging digital threats.

The integration of AI-driven tools into digital forensics helps alleviate the burden on investigators, who are often overwhelmed by the volume of cases and the vast amounts of data requiring processing. The technological development, especially in mobile device forensic tools, enables extensive data acquisition from diverse devices and supports advanced social media and program analysis, thereby expanding the scope and depth of forensic examinations. These sophisticated tools leverage AI to analyse intricate data patterns, leading to more accurate and efficient evidence extraction from complex digital ecosystems.

Challenges for real-time cybercrime investigations necessitate advanced machine learning techniques. This capability helps in identifying unusual threats in large databases and improves the precision and speed of forensic investigations. This improvement is significant as cybercrime is continuously changing. This improvement is significant as cybercrime is continuously changing. Advanced analytical capabilities are required to identify new threats and behavioural patterns.

Continuous evolution of mobile security threats necessitates ongoing study and improvement in mobile device forensic analysis to effectively counter malicious actors. An understanding of existing research in AI and ML applications to digital forensics and incident response is important for developing tactics against cyber threats and an effective investigation procedure. This paper is focused on examining how Artificial Intelligence and Machine Learning are capable of enhancing cybersecurity, focusing on improving detection and response capabilities for security purposes, including new malware and zero-day exploits.

Enhancing AI and ML applications has made it possible to manage increased data volumes, leading to streamlining incident management and enhancing overall cybersecurity resilience. This analysis encompasses an in-depth review of prevalent trends, potential applications, challenges, and future directions for AI and ML in digital forensics and incident response to offer an understanding of the field's current state and future prospects.

The paper highlights AI-driven methods in forensic analysis and malware investigation. Such methods are rule-based reasoning, genetic algorithms, and memetic algorithms. These computational techniques provide enhanced forensic capabilities against cyber threats through automation and analytical depth.

This work highlights the importance of AI and ML in reshaping cybersecurity by enhancing threat detection and response in the context of complex cyberattacks such as those seen in the SolarWinds and Colonial Pipeline incidents. This integration is particularly vital as traditional security measures frequently prove

insufficient against the escalating complexity and volume of modern cyber threats.

Such complicated methodologies that combine rule-based AI with large language models offer a strong framework for improving incident timeline analysis and automating threat assessment processes in digital forensics. This synergistic approach enables a more precise reconstruction of cyber incidents and a more efficient identification of malicious activities. The increasing volume and variety of digital evidence in cybercrime cases require an advanced automated tool for timeline analysis. Which AI. Particularly through rule-based systems and large language models, it is uniquely positioned to provide. Additionally, the increasing workload in digital forensic labs, coupled with the rising complexity of cases, underscores the need to adopt advanced AI-driven solutions, such as Large Language Models, to enhance the efficiency and speed of the investigative process.

*****

Reference

Abbasi, M., Váz, P., Silva, J., & Martins, P. (2025). Comprehensive Evaluation of Deepfake Detection Models: Accuracy, Generalisation, and Resilience to Adversarial Attacks. *Applied Sciences*, *15*(3), 1225. https://doi.org/10.3390/app15031225

Amerini, I., Barni, M., Battiato, S., Bestagini, P., Boato, G., Bruni, V., Caldelli, R., Natale, F. G. B. D., Nicola, R. D., Guarnera, L., Mandelli, S., Wani, T. M., Marcialis, G. L., Micheletto, M., Montibeller, A., Orrù, G., Ortis, A., Perazzo, P., Puglisi, G., … Vitulano, D. (2025). Deepfake Media Forensics: Status and Future Challenges. *Journal of Imaging*, *11*(3), 73. https://doi.org/10.3390/jimaging11030073

Anand, K., & Thakur, S. (2025). Challenges and Limitations of AI in Forensic Science: A Critical Review [Review of *Challenges and Limitations of AI in Forensic Science: A Critical Review*]. *International Journal of Research Publication and Reviews*, *6*(6), 5621. https://doi.org/10.55248/gengpi.6.0125.0672

Arif, M., Abdaud, F., & Huzaiman, H. (2023). The Role of Forensic Science in Proving Murder Cases at the Investigation Stage. *AL-MANHAJ Jurnal Hukum Dan Pranata Sosial Islam*, *5*(1), 1019. https://doi.org/10.37680/almanhaj.v5i1.2989

Babaei, R., Cheng, S., Duan, R., & Zhao, S. (2025). Generative Artificial Intelligence and the Evolving Challenge of Deepfake Detection: A Systematic Analysis. *Journal of Sensor and Actuator Networks*, *14*(1), 17. https://doi.org/10.3390/jsan14010017

Banh, L., & Strobel, G. (2023). Generative artificial intelligence. *Electronic Markets*, *33*(1). https://doi.org/10.1007/s12525-023-00680-1

Bansal, S. (2025). *The Role of Forensic Science and Digital Technology in enhancing Investigation Efficacy: An Analytical Study*. *54*(2), 2566. https://doi.org/10.48047/ecrbvn26

Boneh, D., Grotto, A., McDaniel, P., & Papernot, N. (2019). How Relevant Is the Turing Test in the Age of Sophisbots? *IEEE Security & Privacy*, *17*(6), 64. https://doi.org/10.1109/msec.2019.2934193

Buo, S. A. (2020). The Emerging Threats of Deepfake Attacks and Countermeasures. *arXiv (Cornell University)*. https://doi.org/10.48550/arXiv.2012.07989

Chango, X., Flor-Unda, O., Gil-Jiménez, P., & Gómez-Moreno, H. (2024). Technology in Forensic Sciences: Innovation and Precision. *Technologies*, *12*(8), 120.

https://doi.org/10.3390/technologies12080120

Chawla, Mr. D. S. (2023). The Role of Forensic Evidence in Criminal Investigations in India. *International Journal for Research in Applied Science and Engineering Technology*, *11*(10), 760. https://doi.org/10.22214/ijraset.2023.56099

Chellappan, R. B. (2024). From Algorithms to Accountability: The Societal and Ethical Need for Explainable AI. *Research Square (Research Square)*. https://doi.org/10.21203/rs.3.rs-5277731/v1

Cooke, D., Edwards, A., Barkoff, S., & Kelly, K. (2025). As Good as a Coin Toss: Human Detection of AI-Generated Content. *Communications of the ACM*. https://doi.org/10.1145/3729417

Daungsupawong, H., & Wiwanitkit, V. (2023, October 6). ChatGPT and forensic science: comment. In *Forensic Science Medicine and Pathology* (Vol. 20, Issue 2, p. 761). Springer Science+Business Media. https://doi.org/10.1007/s12024-023-00731-1

Díaz, M., Ferrer, M. A., & Vessio, G. (2023). Explainable offline automatic signature verifier to support forensic handwriting examiners. *Neural Computing and Applications*, *36*(5), 2411. https://doi.org/10.1007/s00521-023-09192-7

Du, X., Hargreaves, C., Sheppard, J., Anda, F., Sayakkara, A., Le-Khac, N., & Scanlon, M. (2020). SoK. *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 1. https://doi.org/10.1145/3407023.3407068

Du, X., Hargreaves, C., Sheppard, J., Anda, F., Sayakkara, A., Le-Khac, N.-A., & Scanlon, M. (2020). SoK: Exploring the State of the Art and the Future Potential of Artificial Intelligence in Digital Forensic Investigation. *arXiv*. https://doi.org/10.48550/ARXIV.2012.01987

Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V. (2024). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. *Forensic Science International Digital Investigation*, *48*, 301675. https://doi.org/10.1016/j.fsidi.2023.301675

El-Din, E. A. A. (2022). ARTIFICIAL INTELLIGENCE IN FORENSIC SCIENCE : INVASION OR REVOLUTION? *Egyptian Society of Clinical Toxicology Journal*, *10*(2), 20. https://doi.org/10.21608/esctj.2022.158178.1012

Fähndrich, J., Honekamp, W., Povalej, R., Rittelmeier, H., & Berner, S. (2022). Special Issue on Application of AI in Digital Forensics. *KI - Künstliche Intelligenz*, *36*(2), 121. https://doi.org/10.1007/s13218-022-00777-3

Fakiha, B. (2023). Enhancing Cyber Forensics with AI and Machine Learning: A Study on Automated Threat Analysis and Classification. *International Journal of Safety and Security Engineering*, *13*(4), 701. https://doi.org/10.18280/ijsse.130412

Fakiha, B. (2024). Unlocking Digital Evidence: Recent Challenges and Strategies in Mobile Device Forensic Analysis. *Journal of Internet Services and Information Security*, *14*(3), 68. https://doi.org/10.58346/jisis.2024.i2.005

Farber, S. (2025). AI as a decision support tool in forensic image analysis: A pilot study on integrating large language models into crime scene investigation workflows. *Journal of Forensic Sciences*. https://doi.org/10.1111/1556-4029.70035

Fattahi, J. (2025). *Machine Learning and Deep Learning Techniques used in Cybersecurity and Digital Forensics: a Review*. https://doi.org/10.48550/ARXIV.2501.03250

Firdonsyah, A., Purwanto, P., & Riadi, I. (2023). Framework for Digital Forensic Ethical Violations: A Systematic Literature Review. *E3S Web of Conferences*, *448*, 1003. https://doi.org/10.1051/e3sconf/202344801003

Gu, J., Xu, Y., Sun, J., & Liu, W. (2023). Exploiting Deepfakes by Analyzing Temporal Feature Inconsistency. *International Journal of Advanced Computer Science and Applications*, *14*(12). https://doi.org/10.14569/ijacsa.2023.0141291

Guo, X., Song, X., Zhang, Y., Liu, X., & Liu, X. (2025). Rethinking Vision-Language Model in Face Forensics: Multi-Modal Interpretable Forged Face Detector. *2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 105. https://doi.org/10.1109/cvpr52734.2025.00019

Hassanin, M., & Moustafa, N. (2024). A Comprehensive Overview of Large Language Models (LLMs) for Cyber Defences: Opportunities and Directions. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2405.14487

Iqbal, S., & Alharbi, S. (2020). Advancing Automation in Digital Forensic Investigations Using Machine Learning Forensics. In *IntechOpen eBooks*. IntechOpen. https://doi.org/10.5772/intechopen.90233

Ji, Y., Hong, Y., Zhan, J., Chen, H., lan, jun, Zhu, H., Wang, W., Zhang, L., & Zhang, J. (2025). *Towards Explainable Fake Image Detection with Multi-Modal Large Language Models*. https://doi.org/10.48550/ARXIV.2504.14245

Jiang, Y., Yan, X.-Y., Ji, G.-P., Fu, K., Sun, M., Xiong, H., Fan, D.-P., & Khan, F. S. (2024). Effectiveness assessment of recent large vision-language models. *Visual Intelligence*, *2*(1). https://doi.org/10.1007/s44267-024-00050-1

Katiyar, N., Tripathi, Mr. S., Kumar, Mr. P., Verma, M., Sahu, A. K., & Saxena, S. (2024). *AI and Cyber-Security: Enhancing threat detection and response with machine learning.* https://doi.org/10.53555/kuey.v30i4.2377

Kelly, L., Sachan, S., Ni, L., Almaghrabi, F., Allmendinger, R., & Chen, Y. (2020). Explainable Artificial Intelligence for Digital Forensics: Opportunities, Challenges and a Drug Testing Case Study. In *IntechOpen eBooks*. IntechOpen. https://doi.org/10.5772/intechopen.93310

Khan, N., Nguyen, T., Bermak, A., & Khalil, I. (2025). *Unmasking Synthetic Realities in Generative AI: A Comprehensive Review of Adversarially Robust Deepfake Detection Systems*. https://doi.org/10.48550/ARXIV.2507.21157

Kim, K., Lee, C. K., Bae, soeun, Choi, J., & Kang, W. (2025). *Digital Forensics in Law*

Enforcement: A Case Study of Llm-Driven Evidence Analysis. https://doi.org/10.2139/ssrn.5110258

Klasen, L. M., Fock, N., & Forchheimer, R. (2024). The invisible evidence: Digital forensics as key to solving crimes in the digital age. *Forensic Science International*, *362*, 112133. https://doi.org/10.1016/j.forsciint.2024.112133

Kloosterman, A., Mapes, A., Geradts, Z., Eijk, E. van, Koper, C., Berg, J. van den, Verheij, S., Steen, M. van der, & Asten, A. C. van. (2015). The interface between forensic science and technology: how technology could cause a paradigm shift in the role of forensic institutes in the criminal justice system [Review of *The interface between forensic science and technology: how technology could cause a paradigm shift in the role of forensic institutes in the criminal justice system*]. *Philosophical Transactions of the Royal Society B Biological Sciences*, *370*(1674), 20140264. Royal Society. https://doi.org/10.1098/rstb.2014.0264

Kothari, P. (2023). Exploring the Role of Forensic Science in Indian Criminal Justice System. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4565177

Kumamoto, T., Yoshida, Y., & Fujima, H. (2023). Evaluating Large Language Models in Ransomware Negotiation: A Comparative Analysis of ChatGPT and Claude. *Research Square (Research Square)*. https://doi.org/10.21203/rs.3.rs-3719038/v1

Kumar, V., & Singh, Y. (2024). Investigation and trial: Analyzing procedural challenges in the Indian criminal justice system. *International Journal of Criminal Common and Statutory Law*, *4*(2), 196. https://doi.org/10.22271/27899497.2024.v4.i2c.106

Li, T., Huang, Z., Wen, H., He, Y., Lyu, S., Wu, B., & Cheng, G. (2025). *RAIDX: A Retrieval-Augmented Generation and GRPO Reinforcement Learning Framework for Explainable Deepfake Detection*. https://doi.org/10.48550/ARXIV.2508.04524

Linna, D. W., Dalal, A., Gao, C., Grimm, P., Grossman, M. R., Pulice, C., Subrahmanian, V. S., & Tunheim, Hon. J. (2024). *Deepfakes in Court: How Judges Can Proactively Manage Alleged AI-Generated Material in National Security Cases*. https://doi.org/10.2139/ssrn.4943841

Liu, P., Tao, Q., & Zhou, J. T. (2024). Evolving from Single-modal to Multi-modal Facial Deepfake Detection: A Survey. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2406.06965

Loumachi, F. Y., & Ghanem, M. C. (2024). *Advancing Cyber Incident Timeline Analysis Through Rule-Based Ai and Large Language Models*. https://doi.org/10.2139/ssrn.4972795

Mahara, A., & Rishe, N. (2025). *Methods and Trends in Detecting Generated Images: A Comprehensive Review*. https://doi.org/10.48550/ARXIV.2502.15176

Mandayam, R. (2024). *The Impact of Artificial Intelligence on Digital Forensic*. *3*(6), 1. https://doi.org/10.47363/jaicc/2024(3)414

Mansoor, N., & Iliev, A. I. (2025). Explainable AI for DeepFake Detection. *Applied Sciences*, *15*(2), 725. https://doi.org/10.3390/app15020725

Mohsin, K. (2024). *The Significance of Forensic and Scientific Evidence and Their Admissibility in Criminal Law*. https://doi.org/10.2139/ssrn.4960559

Moreno, F. R. (2024). *Deepfake Fraud Detection: Safeguarding Trust in Generative Ai*. https://doi.org/10.2139/ssrn.5031627

O'Brien, É., Daéid, N. N., & Black, S. (2015). Science in the court: pitfalls, challenges and solutions [Review of *Science in the court: pitfalls, challenges and solutions*]. *Philosophical Transactions of the Royal Society B Biological Sciences*, *370*(1674), 20150062. Royal Society. https://doi.org/10.1098/rstb.2015.0062

Pica, E., Ross, D. F., & Pozzulo, J. (2024). The Impact of Technology on the Criminal Justice System. In *Routledge eBooks*. Informa. https://doi.org/10.4324/9781003323112

Rijsbosch, B., van Dijck, G., & Kollnig, K. (2025). *Adoption of Watermarking Measures for AI-Generated Content and Implications under the EU AI Act*. https://doi.org/10.48550/ARXIV.2503.18156

Rosenzweig, G. (2022). Scientific Thinking About Legal Truth. *Frontiers in Psychology*, *13*. https://doi.org/10.3389/fpsyg.2022.918282

Sandoval, M.-P., Vau, M. de A., Solaas, J., & Rodrigues, L. F. D. (2024). Threat of deepfakes to the criminal justice system: a systematic review [Review of *Threat of deepfakes to the criminal justice system: a systematic review*]. *Crime Science*, *13*(1). BioMed Central. https://doi.org/10.1186/s40163-024-00239-1

Saxena, R. R. (2025). *AI-Driven Forensic Image Enhancement*. https://doi.org/10.36227/techrxiv.174672975.55187402/v1

Scanlon, M., Breitinger, F., Hargreaves, C., Hilgert, J.-N., & Sheppard, J. (2023). *ChatGPT for Digital Forensic Investigation: The Good, The Bad, and The Unknown*. https://doi.org/10.20944/preprints202307.0766.v1

Schmitt, M., & Fléchais, I. (2024). Digital deception: generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*, *57*(12). https://doi.org/10.1007/s10462-024-10973-2

Sharma, V. K., Singh, S. N., & Caudron, Q. (2024). Combating Deepfakes Using an Integrated Framework forAudio and Video Deepfake Detection. *Research Square (Research Square)*. https://doi.org/10.21203/rs.3.rs-4861782/v1

Solanke, A. A. (2022). Explainable digital forensics AI: Towards mitigating distrust in AI-based digital forensics analysis using interpretable models. *Forensic Science International Digital Investigation*, *42*, 301403. https://doi.org/10.1016/j.fsidi.2022.301403

Tan, C., Wang, J., Ming, X., Tao, R., Wei, Y., Zhao, Y., & Lu, Y. (2025). *ForenX: Towards Explainable AI-Generated Image Detection with Multimodal Large Language Models*. https://doi.org/10.48550/ARXIV.2508.01402

Tariq, S., Nguyen, D., Chamikara, M. A. P., Wu, T., Abuadbba, A., & Moore, K. (2025). *LLMs Are Not Yet Ready for Deepfake Image Detection*. https://doi.org/10.48550/ARXIV.2506.10474

Tariq, S., Woo, S. S., Singh, P., Irmalasari, I., Gupta, S., & Gupta, D. (2025). *From Prediction to Explanation: Multimodal, Explainable, and Interactive Deepfake Detection Framework for Non-Expert Users*. https://doi.org/10.48550/ARXIV.2508.07596

Verdoliva, L. (2020). Media Forensics and DeepFakes: An Overview. *IEEE Journal of Selected Topics in Signal Processing*, *14*(5), 910. https://doi.org/10.1109/jstsp.2020.3002101

V.R, D. (2015). Forensic scientific evidence: problems and pitfalls in India. *International Journal of Forensic Science & Pathology*, 79. https://doi.org/10.19070/2332-287x-1500020

Vu, T.-H., Jagatheesaperumal, S. K., Nguyen, M.-D., Huynh, N. V., Kim, S., & Pham, Q. (2024). Applications of Generative AI (GAI) for Mobile and Wireless Networking: A Survey. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2405.20024

Wahab, H., Ugail, H., & Jaleel, L. (2025). *Ensemble-Based Deepfake Detection using State-of-the-Art Models with Robust Cross-Dataset Generalisation*. https://doi.org/10.48550/ARXIV.2507.05996

Wang, S., Lin, H., Luo, Z., Ye, Z., Chen, G., & Ma, J. (2024). MFC-Bench: Benchmarking Multimodal Fact-Checking with Large Vision-Language Models. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2406.11288

Wang, S., Long, Z., Fan, Z., & Wei, Z. (2024). From LLMs to MLLMs: Exploring the Landscape of Multimodal Jailbreaking. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2406.14859

Wickramasekara, A., Breitinger, F., & Scanlon, M. (2024a). Exploring the Potential of Large Language Models for Improving Digital Forensic Investigation Efficiency. *arXiv*. https://doi.org/10.48550/ARXIV.2402.19366

Wickramasekara, A., Breitinger, F., & Scanlon, M. (2024b). Exploring the Potential of Large Language Models for Improving Digital Forensic Investigation Efficiency. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2402.19366

Wickramasekara, A., Breitinger, F., & Scanlon, M. (2025). Exploring the potential of large language models for improving digital forensic investigation efficiency. *Forensic Science International Digital Investigation*, *52*, 301859. https://doi.org/10.1016/j.fsidi.2024.301859

Xu, X., Zhao, T., Zhang, Z., Li, Z., Wu, J., Achille, A., & Srivastava, M. (2024). Principles of Designing Robust Remote Face Anti-Spoofing Systems. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2406.03684

Yin, Z., Wang, Z., Xu, W., Zhuang, J., Mozumder, P., Smith, A., & Zhang, W. (2025). *Digital Forensics in the Age of Large Language Models*. https://doi.org/10.48550/ARXIV.2504.02963

Yu, P., Fei, J., Gao, H., Feng, X., Xia, Z., & Chang, C. H. (2025). *Unlocking the Capabilities of Large Vision-Language Models for Generalizable and Explainable Deepfake Detection*.

https://doi.org/10.48550/ARXIV.2503.14853

Zangana, H. M., Mustafa, F. M., & Li, S. (2024). Large Language Models in Cybersecurity. In *Advances in information security, privacy, and ethics book series* (p. 277). IGI Global. https://doi.org/10.4018/979-8-3373-1102-9.ch009

Zhang, N., & Zhang, Z. (2023). The application of cognitive neuroscience to judicial models: recent progress and trends [Review of *The application of cognitive neuroscience to judicial models: recent progress and trends*]. *Frontiers in Neuroscience*, *17*. Frontiers Media. https://doi.org/10.3389/fnins.2023.1257004

Zhang, Y., Huang, Y., Sun, Y., Liu, C., Zhao, Z., Fang, Z., Wang, Y., Chen, H., Yang, X., Wei, X., Su, H., Dong, Y., & Zhu, J. (2024). Benchmarking Trustworthiness of Multimodal Large Language Models: A Comprehensive Study. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2406.07057