VAWKUM Transactions on Computer Sciences
http://vfast.org/journals/index.php/VTCS@ 2025, ISSN(e): 2308-8168, ISSN(p): 2411-6335
Volume 13, Number 1, January-June 2025 *pp:217-229*

Transformative Role of LLMs in Digital Forensic Investigation: Exploring Tools, Challenges, and Emerging Opportunities

Mashooque Ali Mahar[1], **Asad Raza**[2], **Raja Sohail Ahmed Larik**[3], **Asadullah Burdi**[4], **Muhammad Shabbir**[5*], **Mudassir Iftikhar**[5]

[1]Institute of Computer Science, Shah Abdul Latif University Khairpur, Pakistan; [2]School of Computer Science & Engineering Central South University, Changhsa, 410083, China; [3]Department of Computer Science, Ilma University, Karachi, Sindh, Pakistan; [4]Institute of Mathematics and Computer Science (IMCS), University of Sindh Jamshoro, Pakistan; [5]Department of Computer Science, Sindh Madresstual Islam University, Pakistan.

Keywords: *Digital forensic, LLMs, AI, Computer investigation, Cybercrime.*

Journal Info:
Submitted:
April 16, 2025
Accepted:
May 05, 2025
Published:
May 15, 2025

Abstract

In the evolving realm of digital forensics, the admissible nature of trustworthy digital evidence in a court of law necessitates the application of scientifically validated digital forensic investigative techniques to substantiate a suspected security event. The incorporation of LLMs represents a transformative technology, set to enhance the efficiency and accuracy of digital forensics investigations. A thorough literature analysis is conducted, including current digital forensic models, tools, large language models (LLMs), deep learning methodologies, and the application of LLMs in investigative processes. The review delineates the issues in current digital forensic methodologies and examines the barriers and potential of integrating LLMs. This study emphasizes the need of integrating LLMs into digital forensics, providing insights into their advantages, disadvantages, and wider implications for addressing contemporary cyber threats.

***Correspondence author email address:** m.shabbir1047@gmail.com
DOI: 10.21015/vtcs.v13i1.2127

1 Introduction

The evolution of digital innovative technologies has a great impact and changed the landscape of modern era. As digital equipment and tools have a substantial impact on online platforms and influence human lives and their daily life, this would be critical for civil and criminal cases [1]. This change over elevated the impact on digital forensics. As DF, it is used for information identification, information extraction, information analysis and preservation and presentation of digital evidence in such a way that legal experts can easily understand and interpret the information as per their need. The digital forensics and computer forensics words are often referred to as interchangeable. Computer forensics collect data from computers, tablet, smart phones, while DF gather data

from the any digital device [2]. DF has emerged as an essential tool for addressing hitches and challenges, from reducing fraud and cybercrime, investigating misconduct, information breaches and monitoring illegal activities. Cybercrime and activities are escalating daily, leading to an ever-increasing volume of complexity of digital data, the need development and adoption of advanced technologies to meet new demands and effectively address challenges. The DF investigations carried out the forensics specialists. and as the need for profession increases, according to Labor Statistics, employment opportunities in computer forensics are expected to rise by 31% by 2029 (link sits outside ibm.com). In recent times, the incorporation of artificial intelligence (AI) and large language models (LLMs) has major attention for their ability to transform digital forensics procedures [1, 2]. As these models are used for analyzing vast amounts of unorganized data, and offering promising applications for threat detection, evident collection, and automated reporting generation. Furthermore, their adoption also introduces challenges, for bias, privacy and the interpretability of AI generated insights [3, 4]. The AI with LLM has reformed DF by covering hidden patterns, undiscover features, automating complex tasks, and effectively processing massive amounts of digital information. AI algorithms modernize investigations by rapidly shifting through large datasets recognizing the relevant material and reducing human effort. Such as BERT, RoBERTa, ALBERT, GPT, and excel in investigating unstructured text data like chat logs, emails, social media contents, web browser history, deleted space, operating system cache. Remote store devices, semantic search, text summarization and language translation. [5, 6] Moreover, these models are helpful for authorship, interpreting tone in communication, behavioral profiling and helping investigators to understand criminal mind tactics. Furthermore, AI can also aid in the automation investigation work, much more time and efforts are currently shorthanded body of digital forensics investigators. AI supports analyzing cyber threats detection, phishing attempts, identifying vulnerabilities by monitoring information breaches [3–8].

In legal discipline, visualization methods enhanced by AI combine the data into interactive relationships, charts and timelines. Which assists in presenting legal cases. Besides, owing to the rapid escalation in the amount digital evidence. The ability to scale and comprehend context such as AI and LLMs allows investigators to conduct in-depth analysis and complicated datasets that previously seemed impossible. Thus, their integration within such domains as investigations should be considered innovative.

The main contribution of papers is as follows:

To provide an in-depth overview of existing LLMs Models, exploring frameworks and application of digital forensics.

To assess how LLMs Models are implemented to detect cyberattacks, fraud detection, malware and data breaches.

To highlight potential advancements, emerging trends, innovative approaches of LLMs for increasing the field of digital forensics.

This survey provides in depth an overview of the role of AI and LLMs methods for digital investigations or digital forensics. Moreover, this study also highlighted the application, benefits and limitations of LLMs and AI in Digital forensics. And explored the gaps and trends, tools, methods and real work scenario. and paying for future research and innovation in the critical domain.

2 Background of LLMs

The evolution of LLMs from early iterations like GPT to advanced versions such as GPT-4 and beyond has transformed the field of NLP, introducing unprecedented capabilities for digital forensics. The basic models have potential for text generation and context understanding. But improvements in architectures, layers, configurations, attention mechanisms and fine-tuning abilities. The main features relevant to DF include their processing of unstructured data, summarizing lengthy documents, performing semantic analysis, detect contextual nuances and

support multilingual evidence analysis. Digital forensics investigations encompass multiple steps, including investigation planning, incident detection, digital evidence identification and analysis, and report preparation and presentation, with certain operations conducted concurrently [9]. The key attributes to DF encompass the capacity to process unstructured data. Such as summarizing lengthy content, detecting contextual nuances and supporting multilingual evidence analysis. Sophisticated models like BERT and GPT-4 and LLaMA excel in interpreting content and identifying hidden pattens in massive datasets. The applications of LLMs models enhanced and encouraged us to optimize the diverse domain tasks for DF investigations. And these achievements supports DF experts to analyze the insights from the diverse digital source for addressing the challenges in the cyber field [8, 11]. An LLM is a language model developed on large amounts of text data that uses neural networks with billions of parameters. These models are designed to understand and produce human language [4, 7, 10–12]. LLMs have amazing applications and capabilities to locate pertinent artifacts and perspective evidence. By implementing GPT-41 demonstrate capabilities, Safeguards against harmful use are built into ChatGPT and other AI bots created by reputable organizations. However, rapid engineering makes it simple to get around many of these protections [13]. LLMs can be used by bad actors to increase the scope and speed of their illegal actions, such as: cybercrime, financial crime, and trafficking Creating and spreading disinformation and fake news. Recently, the FBI and Europol have warned that there are several possibilities for criminals to use generative AI and LLMs to speed up cybercrime activities: More efficient fraud, social engineering, and impersonation techniques to trick victims into divulging personal information, credentials, or money can be made possible by LLMs. Grammatical and linguistic mistakes made it reasonably easy to spot simple phishing scams in the past. Nonetheless, the intrinsic limits of the model training data can impede the model's capacity to address increasingly specialized DF cases. Additional constraints, like the absence of determinism, restrictions on context window size, and inadequate support for non-textual inputs, may hinder the use of LLMs in the reliable and predictable analysis of extensive log data or other non-textual artefacts, such as binary payloads [2, 9, 13–16].

Table 1. Model Functions Across Various Applications

Reference	Year	Function	Application	Model
Tuor et al [5]	2018	Detect	Detecting anomalous behavior in network logs with LLMs	RNN
Dutta et al [6]	2018	Detect	Chatbots assist security experts in identifying open ports	Rule Based
Ranade et al [7]	2021	Detect	CyBERT, a domain-specific BERT model to recognize specialized cybersecurity entities	BERT-based NLP Filter
Ameri et al [8]	2021	Detect	CyBERT, a cybersecurity feature claims classifier	CyBERT, GPT-2
Kereopa-Yorke et al [9]	2023	Identify	LLMs enhance cybersecurity policies	ChatGPT
Cambiaso et al [10]	2023	Respond	Replying to the scam emails using LLM	GPT-3
Chen et al [11]	2023	Detect	LLMs to perform security audits on smart contracts	GPT-3.5 Turbo, GPT-4
Deng et al [12]	2023	Detect	LLM-empowered automatic penetration testing tool	PentestGPT (GPT-3.5 & GPT-4)
Yu and Martin et al [13]	2023	Protect	Generating honeywords using LLMs	GPT-3
Gao et al [14]	2023	Detect	SecureBERT for anomaly detection	CyBERT, SecureBERT (RoBERTa)
McKee et al [15]	2023	Respond	LLM as a honeypot interface against command-line attacks	GPT-3.5
Sladić et al [16]	2023	Respond	Creating honeypots for monitoring and detecting threats	GPT-3.5 Turbo (shelLM)
Wickramasekara et al [17]	2024	Detect/Identify	LLMs for improving digital forensic investigation efficiency	LLaMA, MLLM
Scanlon et al [18]	2024	Evaluate/Interpret	ChatGPT for digital forensic investigation	ChatGPT
Bhandarkar et al [19]	2024	Detect/Identify	Digital Forensics and Incident Response	NTGs, DFIR

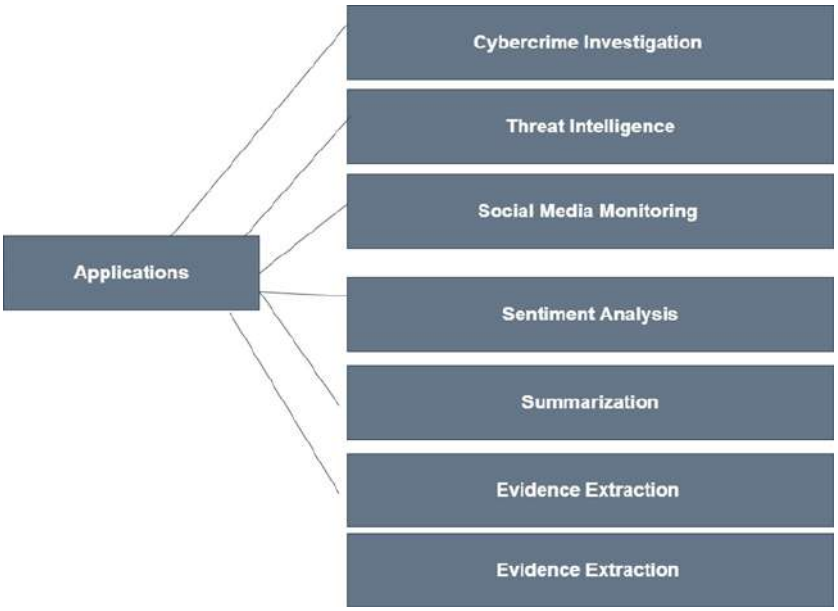

Figure 1. Applications for Digital forensic Investigation

3 Application of LLMs in DF

The combination of LLMs in DF has introduced transformative capabilities, addressing the complex challenges in different domains. In addition, the use of LLMs in the capability of DF investigator to dissect and examine sophisticated textual information as well as find concealed motifs and provide criminal intelligence. The strategies promote the automation in the traditional DF practices to allow inquiries to address the dynamics of these modern cybercrimes and the rapid growth of digital evidence [1, 6, 18, 20]. We provide a summary of a non-complete list of studies that can utilize Large LLMs in digital forensics and computer investigations in Table 1. The table shows the applications, models in use, and the functions they provide giving a systematic review of the role played by the use of the LLMs in the field of development.

Excel can evaluate a lot of textual information and identify the language characteristics and patterns that can help attribute writing to particular artists. Through the examination of stylistic clues like lexical choice, grammar, and syntax structures. Such models would be able to help locate the origin of suspicious documents, chat logs, and emails [2, 19]. This feature is useful when dealing with plagiarism, cybercriminal and insider threats. In addition, LLMs can search through large amounts of text data to identify latent relationships between seemingly unrelated documents, which is essential in the streamlining process during an investigation, distilling useful evidence that summarizes long documents, and pay attention to vital details. As a case in point, they may indicate relevant areas in a massive collection of emails or create summaries of critical results of technical logs. It significantly reduces the time and efforts to analyze data making LLMs indispensable for managing large-scale forensic investigations efficiently [11–16, 21]. Figure 1. Applications for Digital Forensic Investigation provides a summarized list of research papers leveraging LLMs for applications in forensics, cybercrime detection, threat intelligence, and social media monitoring

The growing sophistication of cybercrimes. Such as fraud, phishing and ransomware Cybercrime investigation involves collecting and analyzing digital evidence to create reports and present in court. Cybercrime investigators can work for law enforcement, business and work for law enforcement. LLMs are valuable for analyzing threat intelligence, specifically data regarding cyber risks, to assist in their identification, investigation, and prioritization.

Threat intelligence aids organizations in preparing for and preventing cyber-attacks by supplying information regarding attackers, their motivations, and capabilities. anticipate possible weaknesses and categories of bad content, like phishing emails and hazardous programs. Through the analysis of cybercriminal vernacular and the detection of patterns in hacker forums or the dark web, LLMs offer anticipatory insights that assist in the mitigation of cyber incidents and bolster law enforcement initiatives [22].

Social media have an integral role in the age of the day, online platforms are the critical and crucial source of digital information and evidence collection. Digital forensics can be used when profiling their state of mind or feeling, The LLMs approaches support investigators to analyze emotions, monitor hate speech, violence, cybercrime, misinformation campaign and suspicious activities with help of sentiment analysis technique [19–23]. LLMs analyze the public discussion, profile, group campaigns, events, individual and organizations, and supplying expensive context of forensic analysis. Moreover, Real time tracking of suspects can be eased by the model's ability to recognize relationships and networks on social media platforms.

The DF involve support a considerable quantity of unstructured data. Including documents, emails, multimedia assets and logs. LLMs support this approach by extracting pertinent data evidence and extensive information and empowering them to concentrate on indispensable discoveries. For instance, they can emphasize relevant areas in an extensive collection of emails and summarize insights from the technical log.

The growing complexity of cybercrimes, fraud, ransomware, phishing needs advanced tools. Such as market-oriented skills in various aspects of cybercrime investigation, threat collection methods, and use of pertinent technologies. relevant and in-demand cyber skills, including identity and access management, enterprise security architecture, computer crime, cyber fraud audit methodologies, intelligence collection, and investigations. They can detect patterns, malicious content and cyberattacks, and predict potential vulnerabilities. Moreover, LLMs also offers preemptive perceptions that help avert cyberattack and enhance law enforcement efforts by deciphering cybercriminal language and spotting patterns in hacker forums or the dark web [15, 18, 22–24].

4 Techniques and Tools Leveraging LLMs in Forensics

These methods have tractability of LLMs handling DF and finetuning was adopted to improve the performance of model. By training models on different domain datasets, and ability to identify digital communication logs, identifying patterns in phishing emails and accrediting authorship. The customization allowed for great accuracy and relevance in the results. The LLMs contains DF investigations methods to streamline projects and increase investigation efficiency. The integration can download, process and analyze digital evidence from a variety of sources, including social media platforms, emails, and file systems. They also reduce the time required for forensic investigations by facilitating the dissemination, visualization and advancement of important evidence. These methods underscored the value of LLMs in improving capabilities of digital forensics [13, 16, 21, 23, 26].

Although DF is a developing topic, the literature emphasizes that it continues to change to meet new developments and difficulties. According to Dubey et al [29], DF has several major obstacles, such as the volume and complexity of data, a lack of standardization, the insufficiency of current technologies to help investigations, and problems with timeframes. Along with the difficulties already mentioned, other problems were brought to light, including scope creep in cases because of the complexity and volume of data, the crucial tasks of choosing and prioritizing the appropriate set of evidence, and the effective use of time and investigators for the selected evidence (Kalaimannan et al [29]).

5 Challenges and Limitations of LLMs in Digital Forensics

LLMS have advanced in DF, the usage for forensic work presents several challenges and limitations that need to be tackled. Despite the promising results, LLMs still have challenges of scalability, accuracy issues, ethical and privacy concerns. Overcoming these limitations is critical for ensuring that LLMs can effectively and properly applied

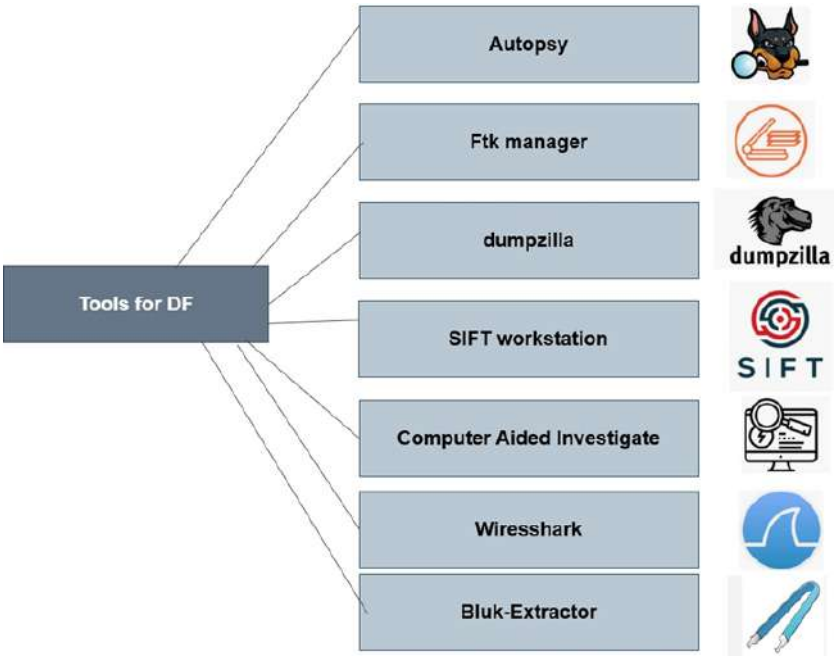

Figure 2. Tools for Digital forensic Investigation

in DF. Addition to this, the LLMs seem to have a wide variety of talents. But it's important to recognize that they have risks and limitations. Over-reliance is a prevalent problem in multimodal LLMs (Wolf et al [30]). Hadi et al identified significant drawbacks of LLMs such as biasness, explainability challenges, logical and reasoning errors, hallucinations, vulnerability to rapid injections, spelling and grammar errors, and more as reported by Hadi et al [31]. Such limitations accentuate the importance of applying the use of the LLMs in a critical and cautious manner in different contexts. One of the biggest concerns as regards to the applications in the practical aspects of DF is the scalability. Large data, such as a huge set of media data, network logs and chat records, are costly in training. Moreover, LLMs can be resource intensive, and needs high processing functionalities and vast amounts of evidence. As samples in datasets increase, load time, cost and running LLMs on such data become a limiting factor. Figure 3. LLMs Challenges for Digital Investigations highlights the key hurdles associated with the application of Large Language Models (LLMs) in digital forensic investigations, such as data privacy, model interpretability, resource requirements, and adversarial robustness.

Furthermore, statistical inconsistency, the lack of emotional characteristics in language replies, and difficulties with fact verification are some of the shortcomings in LLMs that have been documented in the literature [30–36]. These elements support a thorough comprehension of the limitations and possible drawbacks while collaborating with LLMs. According to Thapa et al. [36], LLMs can reduce the time and expenses involved in annotation jobs, but they cannot entirely replace human annotation. This is because they have trouble grasping complex linguistic structures like metaphor, idioms, irony, and sarcasm, which may affect how accurately annotations are made.

One of the key challenges in LLMs for DF ethical and data privacy . The digital forensic investigations needs personal information, private communication, emails, social media interactions. The use of LLMs by analyzing this data requires concerns about unauthorized access, misuse of information and data breaches. Although LLMs have a lot of potential, there are risks involved. Lund and Wang et al [37]; Rahman and Santacana et al [38]; and Bommasani et al [39] offer thorough summaries of the dangers associated with LLMs. One of these is the homogenization of results, in which all downstream models absorb flaws or biases from the foundation model.

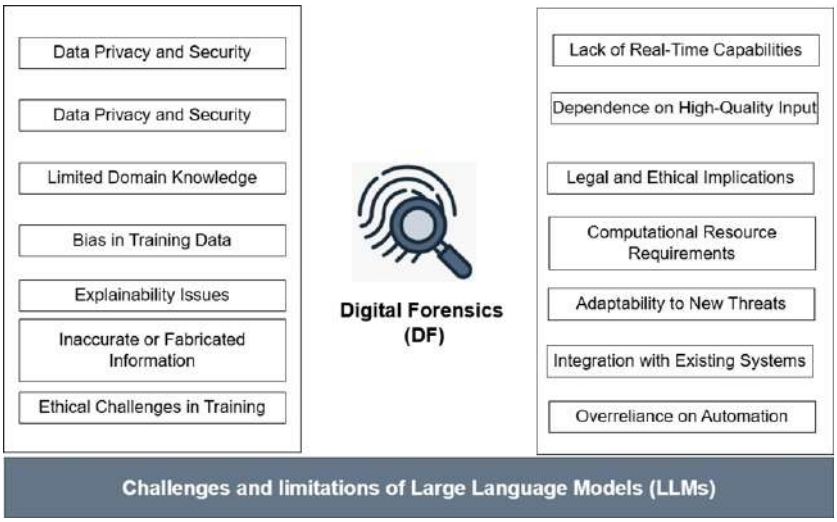

Figure 3. LLMs challenges for Digital investigations

Additionally, the owners of the foundation models run the risk of becoming a monopoly, which would enhance the concentration of power in one organization. Privacy and intellectual property issues are interwoven with ethical and legal considerations. Concerns over the possible displacement of human workers are also raised by the effects on the economy and environment. Additional difficulties are presented by the unfairness and abuse of LLMs, including the production of deep-fakes and their usage in immoral and illegal acts. Bender et al [40] have highlighted the possibility of creating social turbulence, particularly when used on social media platforms, because LLMs do not naturally prioritize the accuracy of information. Furthermore, the usage of LLMs is expensive and has a direct effect on the environment.

6 Future Trends in LLMs for Digital Forensics

The future of LLMs models are more effective and exciting with DF. It holds the significant promise and the use of edge computing and growth of IOT devices increased digital landscape. With ongoing expansions in models design, configuration and real time analysis, and alliance between AI and forensic experts perched to modernize investigate activity. These developments are expected to cater for the limitations and challenges and improve the effectiveness of DF in solving complex problems of cybercrime. One of the core achievements in LLMs is the evolution of Multimodal, which can analyze and interpret data from multiple sources, video, audio, image and text. The multimodal such as DALL-E and CLIP are already demonstrating promise in comprehending and producing cross domain data and incorporation into digital forensics [12, 38, 41]. Figure 4 highlights emerging trends in the application of LLMs for digital investigations, including advancements in automated Event recognition Phase, acquisition, preservation, and examination and analysis. These trends indicate a growing reliance on LLMs for their ability to process vast data sets, detect patterns, and adapt to evolving forensic challenges.

6.1 Event recognition Phase

refer to the initial stage in the Casey DF Model process. Where LLMs improve event recognition by analyzing text-based logs, network traffic, data and network dumps. This phase involves identifying the patterns, anomalies with LLMs based fine tuning models. It provides as the foundation for initiating an appropriate response for extra investigations. LLMs show promise as an Intrusion Detection System (IDS) within such systems by utilizing their capacity to spot patterns in a sequence of text data sets [151].

6.2 Data acquisition phase

The acquisition stage requires human interaction where LLMs can assist in locating possible items of evidence at the crime scene, for instance an investigator can use LLMs such as LLAVA, VisionLLM and MLLM to help examine videos and photos recording from a crime scene. These models make it easier to classify visual data by processing information included with images and text based. Time can be greatly saved by utilizing MLLM for preliminary processing, after which human agents can concentrate on the vital tasks of validation and verification.

6.2.1 Preservation and Integrity Stage

This stage maintain the integrity of data, where preserving evidence and focuses on maintaining veracity using tools FTK, Encase, DFaaS and imager. LLMs line Code LLaMA and StarCoder generate customized code for disk evidence Artifact Preservation. Autonomous agents build frameworks like AutoGen automate code generation, unit testing and event preservation. These agents combine LLMs human inputs, and tools for adaptability in forensic investigations. This automation streamlines the preservation phase, ensuring reliable and efficient handling of digital evidence [2, 4, 17, 45].

6.2.2 Examination Phase

This phase plays a crucial role and is an essential part of the investigation and aids to clarify the case, LLMs optimized for scripting can greatly support with each of these elements, predominantly large scale, within these components, LLMs can be used to complete task pattern matching, file recovering and keyword searching. LLMs provide significant assistance on these tasks. They also combine tools such as Scapy and John the Ripper to simplify the working processes. LAMs and VoT methods are efficient because the subtasks are allocated, so an investigator is able to work on the high-level analysis. Such computerization enhances the efficiency of digital forensic investigations as the investigators can focus on advanced analysis and decision-making [1, 5, 17, 45].

6.2.3 Analysis Phase

This stage involves the interpretation of the event and the conclusion of data obtained in the investigation stage. The case analysis is applicable to the LLMs with the image analysis being possible with MLLMs, which interprets images and expands the opportunities of the more comprehensive analysis of a criminal case. Specifically, the analysis of log files, email contents, chat messages, call logs, file metadata, hex dump, memory dump, and registry hives are some of the data types that are especially formatted to be analyzed by LLMs. In this way, investigators can spend significantly a lesser amount of time in analysis of audio and video data since of this specialized capability in investigations. Automated agents can be used to ensure effective work load distribution to be analyzed. Detection and implementation of the decision-making process can be made more accurate with the help of Augmented Large Language Models (ALLMs) and RAG approaches to enhance real-time information retrieval [17, 42, 44, 45].

6.2.4 Reporting phase

This stage is essential to summarizes the reliability and caliber of evidence and affects the verdict. Clarity and accuracy are crucial in DF because of the increased scrutiny. To ensure accuracy, LLMs could analyze incoming streamlines, such as emails, network traffic, and social media posts, and it help with report creation by following standards such as IEC/ISO 27043:2015. LLMs can be retrained to satisfy requirements even when they don't generate predictable results. They also make it easier to automate forensic reports in many formats, such LaTeX or HTML [17, 43–45].

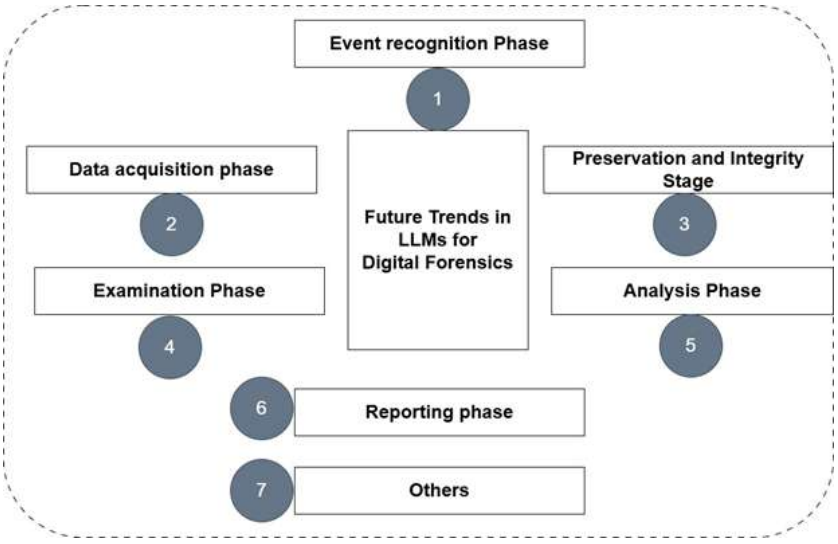

Figure 4. Future Trends of LLMs models for Digital investigations

6.2.5 Other possibilities

LLMs can apply for full automation integrated agents in all stages of the DF process paradigm. The synchronization with frameworks such as automated agents enhance the uniformity and efficiency of investigation. LLMs are also useful in the creation of synthetic content, DF educational scenarios, and agent evaluation standards. The Computer Forensics Tool Testing Program (CFTT) of the National Institute of Standards and Technology (NIST) states that depending on the automation and human knowledge required, LLMs have high, medium, and low potential across several DF phases [17, 43–45].

7 Ethical Considerations and Legal Implications:

Legal and ethical considerations have major roles in decisive their responsible and effective progress. The LLMs models have a great role in DF. It offers powerful abilities for investigating sizable amounts of data, and ensure use aligned with ethical standards and complies with applicable laws. Besides, the reliable use of the LLMs in digital forensics to protect the fact that these models are used in a manner to assist in justice and transparency and fairness. Know that AI tools cannot substitute human judgment but may assist it, investigators ought to use LLMs applications are to be strictly defined, and they need to be able to facilitate the activities connected to the pattern analysis, data analysis, and secrets extraction instead of making their decisions on whether a person is guilty or not. Additionally, to prevent AI driven analysis from unintentionally producing incorrect results and investigators must strike a balance between human control and automation [25, 29, 44, 47]. Besides this, ethical considerations also contain the need to secure informed consent when gathering and investigating private data for DF purposes. Especially with private individuals and organizations. Jurisdiction-specific data protection rules and regulations must be followed by LLMs employed in digital forensics. For example, the European Union's General Data Protection Regulation (GDPR) requires that personal data be handled fairly, openly, and legally. Sensitive information, such private messages or private records, is frequently included in forensic investigations; any use of LLMs must guarantee that this evidence is handled in accordance with privacy rules [45–48, 59].

The investigators make sure that the data is fitting and it is anonymized and that the rights and privacy of individuals and people are not violated. Data protection protocols should be stringent to prevent access, misuse or leakage of sensitive information in the course of investigations. In order to ensure that their processes remain

to be in line with changing legal frameworks, businesses who use LLMs for forensic reasons should also perform routine audits and reviews. The risk of bias is one of the most important ethical issues with LLMs in DF, and the trained on huge datasets, LLMs can potentially represent biases that are inherent to the data they were trained with. For instance, biased. As an example, distorted data or biased language syntax can give discriminatory answers, including falsely identifying a particular group or the failure to identify the relevant information based on demographics. This bias may have severe consequences in the area of forensic research, such as false accusations or the inability to observe valuable evidence [3, 6, 8–10, 19, 45–56]. To reduce this, it is critical to ensure that LLMs are trained on representative and diverse datasets and that their accuracy and fairness is regularly evaluated to minimize this. Another significant aspect is accountability. Increasing the role of LLMs in forensic analysis creates an issue of responsibility in situations when an AI-based investigation leads to a false determination or a courtroom disaster. Human supervision and responsibility are also essential as a means of ultimately holding forensic experts responsible in the outcome of AI. Besides making sure that the use of the LLMs is based on the idea that the latter is used to aid the work of human decision-makers and not to substitute it, the investigators should be capable of explaining the reasoning behind the results provided by AI. [33, 45–50, 54–58].

8 Conclusion and Future work

Within the framework of this research study, we have presented the concept of the inseparable relationship between the LLMs model and the digital forensics with a particular focus on the abilities that these tools possess to enhance investigative capabilities using and threat intelligence, data analysis and evidence extraction. The primary conclusion of the presented research study is that the applications of LLMs are effective to support the text analysis, social media monitoring, and cybercrime investigation. They can also streamline the summarization and extraction of critical information from the complex datasets. Furthermore, numerous challenges remain, including data privacy, ethical issues, bias culpability issues. The purpose is to increase the productivity and efficiency of investigations by exploring investment opportunities for LLMs throughout the DF process. It is also hypothesized that integrating LLMs into existing DF tools may shorten user training durations because these models understand natural language input and provide output appropriately. In the ever-changing field of LLM applications in DF, exciting opportunities for additional research and development emerge.

Author Contributions

Dr. Mashooque Ali Mahar: Conceptualization, project oversight. **Asad Raza**: Methodology design, drafting, final review. **Raja Sohail Ahmed Larik:** Literature survey, validation, refinement. **Asadullah Burdi**: Investigation, visualization, technical input. **Muhammad Shabbir:** Software integration, resource coordination. **Mudassir Iftikhar:** Supervision, Data analysis, content development, proofreading.

Compliance with Ethical Standards

It is declare that all authors don't have any conflict of interest. It is also declare that this article does not contain any studies with human participants or animals performed by any of the authors. Furthermore, informed consent was obtained from all individual participants included in the study.

Conflict of Interest

No conflict of interest regarding the publication of this paper.

References

[1] E. Ullah, A. Parwani, M. M. Baig, and R. Singh, "Challenges and barriers of using large language models (LLM) such as ChatGPT for diagnostic medicine with a focus on digital pathology–a recent scoping review," *Diagn. Pathol.*, vol. 19, no. 1, p. 43, 2024.

[2] G. Michelet and F. Breitinger, “ChatGPT, Llama, can you write my report? An experiment on assisted digital forensics reports written using (local) large language models,” *Forensic Sci. Int.: Digit. Invest.*, vol. 48, p. 301683, 2024.

[3] F. Casino *et al.*, “Research trends, challenges, and emerging topics in digital forensics: A review of reviews,” *IEEE Access*, vol. 10, pp. 25464–25493, 2022.

[4] M. Al Fahdi, N. L. Clarke, and S. M. Furnell, “Challenges to digital forensics: A survey of researchers practitioners attitudes and opinions,” in *Proc. Inf. Secur. South Africa (ISSA)*, 2013, pp. 1–8.

[5] A. R. Tuor *et al.*, “Recurrent neural network language models for open vocabulary event-level cyber anomaly detection,” in *Workshops AAAI Conf. Artif. Intell.*, 2018.

[6] S. Dutta, G. Joyce, and J. Brewer, “Utilizing chatbots to increase the efficacy of information security practitioners,” in *Adv. Hum. Factors Cybersecurity*, Springer, 2018, pp. 237–243.

[7] P. Ranade, A. Piplai, A. Joshi, and T. Finin, “Cybert: Contextualized embeddings for the cybersecurity domain,” in *Proc. IEEE Int. Conf. Big Data*, 2021, pp. 3334–3342.

[8] K. Ameri, M. Hempel, H. Sharif, J. Lopez Jr., and K. Perumalla, “Cybert: Cybersecurity claim classification by fine-tuning the BERT language model,” *J. Cybersecurity Privacy*, vol. 1, no. 4, pp. 615–637, 2021.

[9] B. Kereopa-Yorke, “Building resilient SMEs: Harnessing large language models for cyber security in Australia,” *J. AI, Robot. Workplace Autom.*, vol. 3, no. 1, pp. 15–27, 2024.

[10] E. Cambiaso and L. Caviglione, “Scamming the scammers: Using ChatGPT to reply mails for wasting time and resources,” *arXiv preprint arXiv:2303.13521*, 2023.

[11] C. Chen *et al.*, “When ChatGPT meets smart contract vulnerability detection: How far are we?,” *ACM Trans. Softw. Eng. Methodol.*, 2023.

[12] G. Deng *et al.*, “PentestGPT: An LLM-empowered automatic penetration testing tool,” *arXiv preprint arXiv:2308.06782*, 2023.

[13] F. Yu and M. V. Martin, “Honey, I chunked the passwords: Generating semantic honeywords resistant to targeted attacks using pre-trained language models,” in *Int. Conf. Detection Intrusions Malware, Vulnerability Assess.*, Springer, 2023, pp. 89–108.

[14] M. Gao, “The advance of GPTs and language model in cyber security,” *Highl. Sci. Eng. Technol.*, vol. 57, pp. 195–202, 2023.

[15] F. McKee and D. Noever, “Chatbots in a honeypot world,” *arXiv preprint arXiv:2301.03771*, 2023.

[16] M. Sladić, V. Valeros, C. Catania, and S. Garcia, “LLM in the shell: Generative honeypots,” *arXiv preprint arXiv:2309.00155*, 2023.

[17] A. Wickramasekara, F. Breitinger, and M. Scanlon, “Exploring the potential of large language models for improving digital forensic investigation efficiency,” *arXiv preprint arXiv:2402.19366*, 2024.

[18] M. Scanlon, F. Breitinger, C. Hargreaves, J. N. Hilgert, and J. Sheppard, “ChatGPT for digital forensic investigation: The good, the bad, and the unknown,” *Preprints.org*, 2023.

[19] A. Bhandarkar, R. Wilson, A. Swarup, M. Zhu, and D. Woodard, “Is the digital forensics and incident response pipeline ready for text-based threats in LLM era?,” *arXiv preprint arXiv:2407.17870*, 2024.

[20] F. N. Motlagh *et al.*, “Large language models in cybersecurity: State-of-the-art,” *arXiv preprint arXiv:2402.00891*, 2024.

[21] D. Xuan-Quy, L. Ngoc-Bich, N. Bac-Bien, and P. Xuan-Dung, “LLMs’ Capabilities at the High School Level in Chemistry: Cases of ChatGPT and Microsoft Bing Chat,” 2023.

[22] M. L. Tsai, C. W. Ong, and C. L. Chen, "Exploring the use of large language models (LLMs) in chemical engineering education: Building core course problem models with Chat-GPT," *Educ. Chem. Eng.*, vol. 44, pp. 71–95, 2023.

[23] D. Glukhov, I. Shumailov, Y. Gal, N. Papernot, and V. Papyan, "LLM censorship: A machine learning challenge or a computer security problem?," *arXiv preprint arXiv:2307.10719*, 2023.

[24] S. Moore *et al.*, "Empowering education with LLMs—the next-gen interface and content generation," in *Proc. Int. Conf. Artif. Intell. Educ.*, Cham: Springer, 2023, pp. 32–37.

[25] M. Scanlon, F. Breitinger, C. Hargreaves, J. N. Hilgert, and J. Sheppard, "ChatGPT for digital forensic investigation: The good, the bad, and the unknown," *Forensic Sci. Int.: Digit. Invest.*, vol. 46, p. 301609, 2023.

[26] S. Silalahi, T. Ahmad, and H. Studiawan, "Transformer-based Sentiment Analysis for Anomaly Detection on Drone Forensic Timeline," in *Proc. 11th Int. Symp. Digit. Forensics Secur. (ISDFS)*, 2023, pp. 1–6.

[27] H. M. van Beek *et al.*, "Digital forensics as a service: Game on," *Digit. Invest.*, vol. 15, pp. 20–38, 2015.

[28] H. Henseler and H. van Beek, "ChatGPT as a Copilot for Investigating Digital Evidence," in *LegalAIIA@ ICAIL*, 2023, pp. 58–69.

[29] E. Kalaimannan, J. N. Gupta, and S. M. Yoo, "Maximizing investigation effectiveness in digital forensic cases," in *Proc. Int. Conf. Social Comput.*, 2013, pp. 618–623.

[30] Y. Wolf, N. Wies, O. Avnery, Y. Levine, and A. Shashua, "Fundamental limitations of alignment in large language models," *arXiv preprint arXiv:2304.11082*, 2023.

[31] M. U. Hadi *et al.*, "Large language models: a comprehensive survey of its applications, challenges, limitations, and future prospects," *Authorea Preprints*, 2024.

[32] Y. Qin *et al.*, "ToolLLM: Facilitating large language models to master 16000+ real-world APIs," *arXiv preprint arXiv:2307.16789*, 2023.

[33] L. Fröhling and A. Zubiaga, "Feature-based detection of automated language models: tackling GPT-2, GPT-3 and Grover," *PeerJ Comput. Sci.*, vol. 7, p. e443, 2021.

[34] W. Wang *et al.*, "VisionLLM: Large language model is also an open-ended decoder for vision-centric tasks," *Adv. Neural Inf. Process. Syst.*, vol. 36, 2024.

[35] H. Dubey and S. Bhatt, "Digital forensics techniques and trends: A review," *Int. Arab J. Inf. Technol.*, vol. 20, pp. 644–654, 2023.

[36] S. Thapa, U. Naseem, and M. Nasim, "From humans to machines: can ChatGPT-like LLMs effectively replace human annotators in NLP tasks," in *Workshop Proc. 17th Int. AAAI Conf. Web Social Media*, 2023.

[37] B. D. Lund and T. Wang, "Chatting about ChatGPT: how may AI and GPT impact academia and libraries?," *Library Hi Tech News*, vol. 40, no. 3, pp. 26–29, 2023.

[38] N. Rahman and E. Santacana, "Beyond fair use: Legal risk evaluation for training LLMs on copyrighted text," in *ICML Workshop Generative AI and Law*, 2023.

[39] R. Bommasani *et al.*, "On the opportunities and risks of foundation models," *arXiv preprint arXiv:2108.07258*, 2021.

[40] E. M. Bender, T. Gebru, A. McMillan-Major, and S. Shmitchell, "On the dangers of stochastic parrots: Can language models be too big?," in *Proc. 2021 ACM Conf. Fairness, Accountability, and Transparency*, 2021, pp. 610–623.

[41] Y. Qin *et al.*, "Toolllm: Facilitating large language models to master 16000+ real-world APIs," *arXiv preprint arXiv:2307.16789*, 2023.

[42] Q. Wu *et al.*, "Autogen: Enabling next-gen LLM applications via multi-agent conversation framework," *arXiv preprint arXiv:2308.08155*, 2023.

[43] G. Michelet and F. Breitinger, "ChatGPT, Llama, can you write my report? An experiment on assisted digital forensics reports written using (local) large language models," *Forensic Sci. Int.: Digit. Invest.*, vol. 48, p. 301683, 2024.

[44] J. Sundman and W. Hedenskog, "Evaluating the usability of large language models as tools in cybersecurity: A comparison of censored and uncensored models in penetration testing and digital forensics," 2024.

[45] A. Wickramasekara and M. Scanlon, "A framework for integrated digital forensic investigation employing AutoGen AI agents," in *Proc. 2024 12th Int. Symp. Digital Forensics and Security (ISDFS)*, pp. 01–06, IEEE, Apr. 2024.

[46] A. Nikolakopoulos *et al.*, "Large language models in modern forensic investigations: Harnessing the power of generative artificial intelligence in crime resolution and suspect identification," in *Proc. 2024 5th Int. Conf. Electron. Eng., Inf. Technol. Educ. (EEITE)*, pp. 1–5, IEEE, May 2024.

[47] D. B. Oh, D. Kim, and H. K. Kim, "volGPT: Evaluation on triaging ransomware process in memory forensics with large language model," *Forensic Sci. Int.: Digit. Invest.*, vol. 49, p. 301756, 2024.

[48] J. Adkins, A. Al Bataineh, and M. Khalaf, "Identifying persons of interest in digital forensics using NLP-based AI," *Future Internet*, vol. 16, no. 11, p. 426, 2024.

[49] S. Jia *et al.*, "Can ChatGPT detect deepfakes? A study of using multimodal large language models for media forensics," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, pp. 4324–4333, 2024.

[50] M. M. Al Mahdi and S. Baror, "Proof of concept of a digital forensic readiness cybercrime language as a service," in *Int. Conf. Cyber Warfare and Security*, vol. 19, no. 1, pp. 191–199, Mar. 2024.

[51] M. Ivanova and S. Stefanov, "Regarding artificial intelligence in digital forensic investigation: Applications and solutions," in *Proc. 2024 XXXIII Int. Sci. Conf. Electronics (ET)*, pp. 1–6, IEEE, Sep. 2024.

[52] S. Qi *et al.*, "What is the limitation of multimodal LLMs? A deeper look into multimodal LLMs through prompt probing," *Inf. Process. Manag.*, vol. 60, no. 6, p. 103510, 2023.

[53] K. Chugh and P. Ahuja, "A forensic approach: Identification of source printer through deep learning," *Int. J. Electron. Secur. Digit. Forensics*, vol. 16, no. 6, pp. 775–798, 2024.

[54] Y. Yao *et al.*, "A survey on large language model (LLM) security and privacy: The good, the bad, and the ugly," *High-Confidence Comput.*, p. 100211, 2024.

[55] S. H. Kamtam, H. S. Lallie, and M. A. Azad, "The application of AI techniques for firearm detection in digital forensic investigation," *Int. J. Electron. Secur. Digit. Forensics*, vol. 16, no. 3, pp. 372–396, 2024.

[56] Z. Ji *et al.*, "Towards mitigating LLM hallucination via self reflection," in *Findings Assoc. Comput. Linguist.: EMNLP 2023*, pp. 1827–1843, Dec. 2023.

[57] I. A. Kandhro, U. Khan, S. Memon, and M. Yasir, "Discover and safe: An automated security management system for educational institutions," *Int. J. Electron. Secur. Digit. Forensics*, vol. 15, no. 2, pp. 158–176, 2023.

[58] D. Patrick *et al.*, "A novel comparison of data analytics and business intelligence tools: An information preservation and ledger management solution," *Int. J. Electron. Secur. Digit. Forensics*, vol. 15, no. 4, pp. 387–412, 2023.

[59] F. Y. Loumachi and M. C. Ghanem, "Advancing cyber incident timeline analysis through rule based AI and large language models," *arXiv preprint arXiv:2409.02572*, 2024.