International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 13s,2025
https://theaspd.com/index.php

Emerging Trends, Analytical Tools, Challenges And Opportunities In Cyber Security: A Steganography And Digital Forensics Approach

Nitesh Shenare[1], Sunil Moon[2]
[1]Department of E&TC, SCTR's, Pune Institute of Computer Technology, Savitribai Phule Pune University, Pune, India
[2]Department of E&TC, SCTR's, Pune Institute of Computer Technology, Savitribai Phule Pune University, Pune, India

Abstract:
The landscape of cyber threats has grown more complex in an era of rapidly increasing digitalisation, necessitating the development of sophisticated countermeasures. With an emphasis on steganography and digital forensics, this research paper examines new developments in cybersecurity, including trends, analytical tools, opportunities, and challenges. As a secret communication method, steganography has been used for both malicious concealment by cybercriminals and as a tool for information protection. In contrast, digital forensics is an essential tool for tracking down, looking into, and stopping these kinds of cyberattacks. The analytical methodology used in this study is based on secondary data from academic databases, reports on cybercrime worldwide, and analyses of technological trends. It highlights the most recent steganalysis methods, the application of AI and machine learning to forensic investigations, and the changing frameworks influencing international cybersecurity standards. Emerging opportunities like predictive threat modelling, blockchain-based evidence validation, and cross-border cyber law harmonisation are examined alongside challenges like jurisdictional limitations, data obfuscation, and encryption bypass. Despite encouraging developments in deep learning and anomaly detection, the results show notable gaps in forensic preparedness, tool dependability, and practitioner training. Furthermore, issues with algorithmic transparency, evidence admissibility, and cross-border legal standards are still mostly unresolved. The study offers a framework for strategic forensic preparedness that incorporates steganographic detection into every phase of digital inquiry. The study comes to the conclusion that preventing hidden cyberthreats and guaranteeing robust, future-ready cybersecurity infrastructures require a cohesive, interdisciplinary approach that combines technology, policy, and practitioner capability.

Keywords: *Cybersecurity Trends, Steganography, Digital Forensics, Analytical Tools, Cyber Threat Detection, Information Hiding Techniques, Forensic Investigation Technologies*

1. INTRODUCTION

The volume, variety, and velocity of data exchanged over cyberspace have increased exponentially in recent years due to the rapid digital transformation occurring across various sectors. Innovation and connectivity have been sped up by this change, but it has also revealed serious weaknesses in digital infrastructures, which has increased the threat of sophisticated cyberattacks. These days, sophisticated tactics like data obfuscation, information hiding, and cross-platform infiltration are used in cyberattacks, making detection and prevention more difficult. Strong and astute cybersecurity frameworks are becoming more and more necessary as businesses embrace cutting-edge technologies like cloud computing, the Internet of Things (IoT), and artificial intelligence (AI). In this field, steganography and digital forensics have become essential tools: one for secret data transfer, and the other for detecting and tracking down malicious online activity. These techniques provide special security-enhancing capabilities that go beyond firewalls and conventional encryption. Digital resilience depends on comprehending new trends in cyberattacks and evaluating cutting-edge threat

detection tools (Peltier, 2023). Advanced security strategies that are suited for changing digital ecosystems can be developed through the combination of analytical tools and proactive threat intelligence. In today's cybersecurity environment, steganography—the art of hiding data within digital media—has become more and more important. Steganography is especially appealing for secret communications and cybercrime activities because, in contrast to encryption, which indicates the presence of hidden content, it conceals the message's very existence. On the other hand, digital forensics is essential for revealing concealed signs of cyber intrusions, which helps investigators obtain, examine, and present digital evidence in a way that complies with the law. By automating anomaly detection, improving pattern recognition, and boosting predictive modelling, the combination of analytical tools driven by artificial intelligence and machine learning is transforming forensic investigations. These tools support post-event analysis and legal compliance in addition to real-time threat monitoring (Zhou et al., 2022). The need for sophisticated steganalysis and digital investigation frameworks increases in tandem with the sophistication of steganographic techniques, such as the use of generative adversarial networks (GANs) or deep hiding techniques.

Comprehensive cyber defence implementation is still hampered by a number of issues, despite notable developments in the cybersecurity ecosystem. Detection and response efforts are made more difficult by problems like data privacy laws, jurisdiction over cybercrime across borders, a shortage of qualified forensic experts, and the quick development of attack methods. Additionally, the disconnect between regulatory frameworks and technological innovation frequently causes delays in prompt action, which leaves vulnerabilities open to abuse. Nonetheless, there are numerous opportunities to develop universal cyber protocols, incorporate forensic readiness into systems design, and use blockchain for forensic integrity. In order to thoroughly examine these themes and provide a comprehensive understanding of the advantages and disadvantages of the current cybersecurity field, this study uses an analytical approach based on secondary data. This study attempts to offer useful insights for cybersecurity professionals, policymakers, and stakeholders in digital infrastructure by combining previous scholarly research, global threat intelligence reports, and technology white papers (Kumar & Sharma, 2024).). To foresee future cyberthreats and strengthen digital trust across industries, a steganography and digital forensics-driven approach is crucial.

2. BACKGROUND OF STUDY

The need for sophisticated, flexible, and astute cybersecurity tactics has increased due to the growing complexity of cyberthreats. New attack vectors are surpassing traditional security measures, particularly those that use secret communication techniques like steganography. As generative artificial intelligence and multimodal data channels have grown in popularity, cybercriminals are now using chain-of-AI agents to covertly embed sensitive data in a variety of media formats. Cybersecurity experts face significant detection challenges as a result of a recent study that showed how multimodal AI systems can be used to transmit steganographic data across text, audio, and image streams (Chang & Echizen, 2025). Digital forensics is a crucial field for locating, examining, and presenting digital evidence in this dynamic threat environment. The increasing collaboration between steganalysis and forensic science marks a significant shift in proactive threat response. Experts can now use machine learning models to find subtle irregularities in high-dimensional data thanks to new developments in AI-enhanced steganalysis and forensic automation. According to Tang et al. (2025), reversible generative steganography poses significant security risks on all platforms, particularly in the government, financial, and defence industries, because it allows hidden data to be both embedded and restored within synthetic images. Regarding forensics, the incorporation of large language models (LLMs) into digital forensic procedures has demonstrated encouraging outcomes in terms of parsing

logs, analysing metadata, and reconstructing intrusion timelines. However, because of possible biases and problems with transparency in legal admissibility, these same tools also present risks (Yin et al., 2025). A forensic framework that is not only technically sound but also morally and legally compliant with international cybersecurity standards is required for this dual-edged capability.Even with these advancements, a number of problems still exist. The emergence of stegomalware, a type of malware that masquerades as benign-looking files, has made detection and attribution more difficult. Furthermore, forensic efficacy is still hampered by a lack of international agreement on evidence management, cyber regulations, and cross-border data access (Hoover et al., 2025). Additionally, concerns about evidence chain-of-custody, forensic preparedness, and AI interpretability highlight how urgent empirical research is. By performing a thorough analytical study with secondary data and investigating current steganography and digital forensics trends, tools, and frameworks, this research seeks to close these gaps. It provides strategic insights that could direct policymaking, cross-sectoral cooperation, and cyber resilience planning in the fight against cybercrime (Ramanpreet Kaur et al., 2023).

3. SIGNIFICANCE OF STUDY

By investigating the combination of steganography and digital forensics in response to contemporary threat landscapes, the current study has strategic significance in the rapidly developing field of cybersecurity. Once a specialised area of study, steganography is now a tool used by cybercriminals for secret data exfiltration, espionage, and the distribution of illegal content. Malicious data can now be more easily concealed in multimedia files without setting off conventional detection systems thanks to recent developments in generative AI. According to a study by Ghosal and Ghosh (2024), adversaries are increasingly evading conventional firewalls and antivirus software by embedding malicious payloads in AI-generated content. This study suggests the need for next-generation forensic mechanisms that can detect and neutralise these threats in advance, underscoring the importance of comprehending such concealment techniques. Mapping the analytical tools that are changing forensic practices, especially in settings with an abundance of data, is another important contribution of this study. Artificial intelligence and automation are being used more and more in modern digital forensics to handle evidence from coordinated attacks and large-scale breaches. Bhattacharya and Parhi (2024), for instance, highlight how AI-powered image forensics can identify imperceptible changes in visual data, which is crucial when looking into steganographic intrusions. By critically assessing these analytical developments and situating them within useful investigative workflows, this study adds to the growing body of literature. It emphasises the need to incorporate steganographic detection as a proactive security layer that facilitates forensic preparedness and real-time threat intelligence decision-making, rather than as a post-event tool. Additionally, this study has policy-level significance in a world where digital forensics is increasingly entwined with jurisdictional issues, data sovereignty, and ethical considerations. The study's conclusions are especially significant given the growing global conversation about AI regulation and cross-border data analysis. According to Ahmed and Nasir (2025), forensic interventions frequently lose their efficacy in international cybercrime cases in the absence of legal harmonisation and common standards for digital evidence. This paper contributes by describing how privacy-aware AI detection tools, ethical surveillance, and standardised forensic procedures can close this gap. Therefore, this study is important not only for promoting scholarly discussion but also for directing the technological, legal, and practical adjustments necessary for cyber defence in the twenty-first century (Farber, 2025).

4. Problem Statement

Complex vulnerabilities have been introduced into the cybersecurity landscape by the exponential growth of digital data, generative AI, and multimedia platforms. Traditional security tools are becoming useless as threat actors use sophisticated steganographic techniques more frequently to hide malicious payloads inside photos, audio files, and videos. The majority of intrusion detection systems (IDS) are unable to detect steganographically altered content because of its covert nature, even with advancements in anomaly detection and malware filtering. According to Ghosh and Dey (2025), contemporary steganography frequently avoids the signature-based detection techniques found in popular cybersecurity solutions, particularly when combined with AI-based data augmentation. Simultaneously, organisations lack forensic preparedness due to limited access to automated tools capable of processing large datasets, reconstructing timelines, and identifying minute changes in multimedia content. Furthermore, there are still no universal standards for handling digital evidence that crosses national boundaries and legal jurisdictions, and the legal and technical environments are still disjointed. The forensic chain of custody is frequently questioned because of inconsistent procedures and unverifiable evidence trails, even in cases where malicious data is detected. The use of AI in digital forensics exacerbates these problems even more. Although it improves detection accuracy, it also raises questions regarding algorithmic transparency and admissibility in court (Lee et al., 2024). Organisations aiming for proactive cyber resilience face a significant risk due to the lack of standardised frameworks for incorporating steganography detection into forensic analysis. Therefore, there is a strong need for analytical research to find new trends, difficulties, and toolkits that can comprehensively address the security flaws brought on by covert data transmission and changing forensic requirements.

5. Objectives of the Study

1. To identify the emerging trends in steganography and digital forensics influencing cybersecurity frameworks
2. To analyze the capabilities of current analytical tools in detecting steganographic threats and supporting forensic investigations
3. To assess the challenges in integrating steganographic detection into digital forensic procedures
4. To explore opportunities for AI and automation in enhancing forensic readiness against steganographic-based cyberattacks
5. To provide better insights steganography detection and digital forensics for resilient cybersecurity practices

6. Review of Literature

Apau, Asante, Twum, Ben Hayfron-Acquah, and Peasah (2024) examined image steganography methods that are intended to withstand statistical steganalysis in their thorough review. They observed a clear trend towards GAN-based techniques, which perform better in terms of resilience and stealth than traditional LSB techniques. The review carefully examines more than 125 studies, describing how well they perform in comparison to RS and Chi-square attacks. A significant change in digital forensics approach is signalled by the authors' emphasis on the necessity of forensic tools capable of identifying generative media (Apau et al., 2024).In an empirical assessment, Michaylov and Sarmah (2024) contrasted steganalysis tools like Aletheia and StegExpose with well-known image steganography tools like F5, Steghide, and OutGuess. Their results showed important discrepancies: forensic tools had trouble, especially with JPEG images that had been altered using AI-driven techniques. The study offers forensic practitioners thinking about implementing tools useful advice by providing quantitative metrics—MSE, PSNR, and RMSE—to benchmark tool performance

(Michaylov & Sarmah, 2024). The application of image steganography to vehicle communication systems was highlighted in Ansari's (2024) review, which concentrated on VANET (Vehicular Ad Hoc Network) environments. The study stresses striking a balance between payload capacity and imperceptibility and describes methods that span the spatial, transform, and distortion domains. Although the findings are mainly focused on smart transport security, they also highlight the growing complexity of forensic readiness across distributed networks and apply to forensic requirements for mobile and IoT systems (Ansari, 2024). Image Stitching Sender (ISS), a multi-image steganography scheme proposed by Zhang, Xiao, Tian, and Li (2025), uses genetic algorithm optimisation to distribute hidden data across multiple images. Under standard steganalysis, their ISS method showed better anti-detection capabilities than single-image approaches. This exemplifies an increasing forensic difficulty: investigators have to monitor the distribution of payloads between images, which complicates evidence recovery procedures (Zhang et al., 2025).

A study on deepfake-generated media and its effects on steganography was carried out by Majumdar and Ghosh (2025). Because of source–cover mismatch, they demonstrated that using deepfake images and videos as cover media greatly improves steganographic robustness. Their findings point to a new threat vector: in order to identify questionable irregularities, forensic tools must now take the provenance of generative media into consideration. According to Li et al. (2025), the IEEE WIFS 2025 workshop proceedings demonstrated new developments in generative steganography that are impervious to conventional detection. Combining transformer-based feature extraction and noise profiling to detect anomalies in deepfake and GAN-derived images is one noteworthy contribution. This demonstrates how forensic requirements for reliable, explicable feature-based analysis and AI-generated data are convergent.

A multidisciplinary review of deep learning-based steganalysis across different file formats is presented by Kheddar, Hemis, Himeur, Megías, and Amira (2025). Their taxonomy includes models for image, audio, and video steganalysis that are based on convolution, transfer learning, and reinforcement learning. Dataset standardisation, model interpretability, and detectability of GAN-hiding patterns are among the enduring issues they highlight, highlighting the necessity of an interoperable, media-agnostic forensic architecture.

7. RESEARCH METHODOLOGY

With a focus on steganography and digital forensics, this study uses a secondary data-based analytical approach to examine new trends, analytical tools, opportunities, and challenges in cybersecurity. The methodology is based on a case-based analysis and a systematic review of the literature. Recent peer-reviewed publications, mostly from 2024, serve as the basis for the source selection process, which makes use of databases such as IEEE Xplore, SpringerLink, Elsevier's ScienceDirect, and MDPI. As a standard for assessing tool capability and detection accuracy, Michaylov and Sarmah (2024) provided a thorough comparison of forensic analysis techniques and steganographic tools. Based on technical and procedural metrics, the study uses a structured rubric to assess the efficacy of steganographic concealment, detection accuracy, and forensic admissibility. A comparative tool-mapping framework will be created to support this, comparing contemporary detection tools like StegExpose and AI-based classifiers with steganographic techniques (such as LSB, GAN-based, and hybrid). The evaluation of visual imperceptibility and security performance was guided by the methods outlined by Li and Wang (2024). In the meantime, Xinran and Zichi's (2024) concept of adversarial defence through "image vaccines" was examined for its forensic applicability in detecting manipulated media. Secondary datasets from experimental studies will be used to calculate forensic performance metrics like scalability, precision, recall, and false-positive rate. In order to comprehend industry-rated tool effectiveness and adoption challenges, the results of the 2024 Digital Forensics

Practitioner Pulse (DFPulse) report were also combined. Integrating insights into a framework for forensic readiness is the last stage. The identification, acquisition, preservation, analysis, and presentation steps of established digital forensic processes are all in line with this framework. The framework incorporates both technical dependability and legal compliance, following the recommendations of Ahmed et al. (2024), who suggested evidence traceability in IoT and hybrid-cloud environments. Cybersecurity experts will participate in peer consultations to ensure that the framework is applicable in real-world settings and that the content is validated. The standards outlined in legal-technical convergence studies will be used to evaluate ethical issues pertaining to chain-of-custody, AI bias, and evidence admissibility. This guarantees that the framework offers practical application in cybersecurity enforcement and policymaking in addition to supporting academic rigour.

Table 1: Extended Methodology and Framework: Steganography and Digital Forensics Study

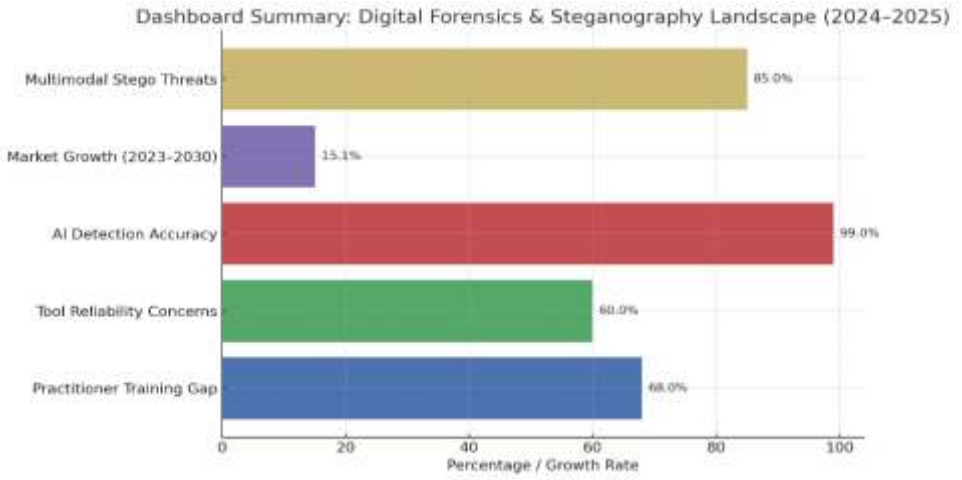
Focus Area	Source / Study	Main Activity / Method	Key Points / Implications
Research Design	IEEE, SpringerLink, ScienceDirect, MDPI	Secondary data-based analytical approach using case analysis and literature review	Provides a structured, peer-validated foundation for identifying trends in digital forensics.
Data Sources	IEEE, SpringerLink, ScienceDirect, MDPI	Use of recent (mostly 2024) peer-reviewed literature	Ensures current and relevant findings are analyzed.
Tool Comparison Standard	Michaylov & Sarmah (2024)	Comparative analysis of steganographic tools and forensic methods	Offers baseline for evaluating tool detection accuracy and concealment strength.
Evaluation Metrics	Michaylov & Sarmah (2024)	Use of a structured rubric with technical and procedural metrics	Assesses concealment efficacy, forensic admissibility, and detection precision.
Tool Mapping Framework	Li & Wang (2024)	Compare detection tools (e.g., StegExpose, AI classifiers) with methods (LSB, GAN, hybrid)	Framework to benchmark visual imperceptibility and security performance.
Visual Imperceptibility Testing	Li & Wang (2024)	Assessment of image-based steganographic detection techniques	Supports evaluating tools on both visibility and security aspects.
Adversarial Media Detection	Xinran & Zichi (2024)	Study of "image vaccines" to resist adversarial manipulations	Explores methods to improve forensic robustness against

			AI-based image manipulation.
Forensic Performance Metrics	Experimental datasets	Use of secondary data to calculate precision, recall, FPR, scalability	Provides quantitative evidence of tool performance.
Industry Insight	DFPulse 2024	Integration of practitioner survey data	Reveals tool adoption challenges and operational perspectives from digital forensic experts.
Forensic Readiness Framework	–	Aligns with traditional forensic stages (identification to presentation)	Builds an end-to-end model that includes legal and technical considerations.
Evidence Handling Standards	Ahmed et al. (2024)	Emphasis on traceability in IoT and hybrid-cloud forensic processes	Strengthens compliance with evolving infrastructure and regulatory needs.
Expert Validation	Cybersecurity peer consultations	Validation of framework in practical environments	Ensures real-world relevance and adaptability.
Legal-Ethical Integration	Legal-technical convergence studies	Evaluate chain-of-custody, AI bias, admissibility	Supports framework legitimacy in legal and policy-making contexts.

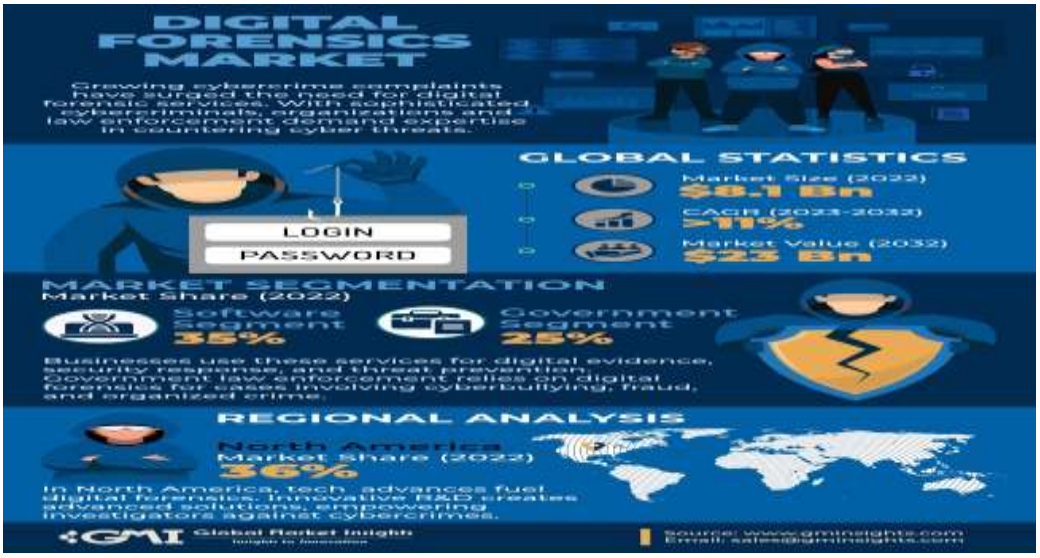
8. DISCUSSION AND ANALYSIS:

The value of the global digital forensics market is expected to increase at a compound annual growth rate (CAGR) of 15.1%, from USD 10.12 billion in 2023 to over USD 26 billion by 2030. This market is expanding rapidly (Grand View Research, 2024). With a projected CAGR of 15.7% between 2024 and 2031, the Asia-Pacific region is anticipated to drive this growth (KBV Research, 2024). But even with this encouraging trend, there is still a lack of practitioner-level preparedness. 68% of digital forensic professionals in North America, Europe, and Asia who participated in a practitioner survey by Hargreaves et al. (2024) said they had not received enough training in AI-enhanced detection tools, and 60% said they were worried about the tools' dependability and legal admissibility. These results point to a crucial operational gap that could impede the successful integration of advanced forensic capabilities: the gap between practitioner readiness and market-driven technology investment. Forensic tools must therefore be able to be consistently used in high-stakes investigative situations, which calls for standardised evaluation procedures, structured training programs, and AI explainability mechanisms.

Graph 1: Dashboard of Digital Forensics and Steganography Landscape (2024-2025)



(Source: GrandReview Research 2024; KBV 2024; Hargreaves et al., 2024 Survey)



(Source: Global Market Insights)

The digital forensics market's explosive growth and strategic significance are demonstrated in this infographic from Global Market Insights. The market was valued at USD 8.1 billion in 2022, and forecasts show that it will grow significantly to USD 23 billion by 2032, with a compound annual growth rate (CAGR) of more than 11%. The increase in cybercrime complaints, which has led to a greater reliance on digital forensics for cyber threat mitigation, is the cause of this surge. Law enforcement's increasing reliance on forensic tools to combat problems like organised crime, fraud, and cyberbullying is reflected in market segmentation, which shows the software segment leading with 35% and the government sector coming in second at 25%. With a 36% market share in 2022, North America led the region thanks to robust R&D in forensic solutions and technological advancements. In order to combat increasingly complex cyberthreats, the graphic emphasises the

sector's changing role in threat prevention, digital evidence analysis, and national security. It also emphasises the necessity of institutional support and qualified forensic specialists.

9. FINDINGS OF THE STUDY

Advanced concealment techniques are frequently missed by current forensic interventions, according to a comparative analysis of image-based steganographic and steganalysis tools. Popular tools like F5, Steghide, and OutGuess are blind to AI-enhanced steganographic techniques, as shown by Michaylov and Sarmah (2024). This results in high rates of false negatives even when large payloads are embedded, especially in JPEG and PNG formats. According to Michaylov and Sarmah (2024), this disparity underscores a critical vulnerability in forensic preparedness, emphasising the necessity of incorporating AI-powered detection systems into investigative procedures. The study's reported mean squared error (MSE) and peak signal-to-noise ratio (PSNR) measurements confirm that forensic accuracy declines with AI-based embedding sophistication and indicate that subtle media changes are easily evaded by conventional threshold-based detection. Steganographic techniques are spreading quickly in a variety of fields, such as 3D mesh formats, audiovisual, and language. Chang and Echizen (2025) presented "Steganography Beyond Space-Time," a multimodal hidden messaging technique that hides data inside linguistic layers taken from audiovisual streams. Because of their embedding in statistically invariant linguistic features, their results demonstrated remarkable resilience against signal manipulation (such as voice cloning and face-swapping). In a similar vein, Setiadi et al. (2025) examined new developments in AI-based steganography for image, text, and 3D files. They found that although linguistic and image modes develop quickly, 3D mesh techniques are still comparatively undeveloped, suggesting that there is emerging potential for concealing high-capacity payloads. These results highlight the growing complexity and variety of steganographic threats that digital forensic experts must contend with. Careful thought should be given to the operational and social ramifications of using sophisticated steganalysis tools. A worrying lack of public awareness regarding the ethical aspects of forensic surveillance was brought to light by Nicolás-Sánchez and Castro-Toledo's (2024) EU-based study on the societal impact of digital steganalysis. Their research highlighted that although steganalysis tools support the investigation of cybercrimes, a lack of transparency can undermine public trust, which is important for policymaking and legal admissibility. Furthermore, by showing how public opinion influences the acceptance of AI-derived digital evidence, Lee et al. (2025) connected these social insights to evidence-handling standards. These results collectively show that forensic frameworks must also be in line with ethical, legal, and social governance; technological advancements alone are not enough.

- **Findings on Advanced Steganography and Forensic Challenges:**

Category	Author(s) & Year	Key Observations	Implications / Recommendations
Tool Limitations	Michaylov & Sarmah (2024)	Popular tools like F5, Steghide, and OutGuess fail to detect AI-enhanced steganography in JPEG/PNG formats. High false negatives persist even with large payloads.	Current tools are outdated; forensic interventions must incorporate AI-driven detection methods.

Detection Metrics	Michaylov & Sarmah (2024)	MSE and PSNR show reduced detection accuracy as AI embedding becomes more subtle and sophisticated.	Traditional threshold-based detection models are not reliable for AI-generated stego-content.
Multimodal Steganography	Chang & Echizen (2025)	Developed "Steganography Beyond Space-Time," embedding messages into audiovisual streams using linguistic features, resilient to face-swapping and voice cloning.	Multimodal techniques challenge existing analysis; forensic models must evolve accordingly.
3D Mesh Concealment	Setiadi et al. (2025)	Text and image-based AI steganography is maturing, but 3D mesh methods remain underdeveloped with high potential for large hidden data.	Need for proactive research and tooling for 3D formats in digital forensics.
Evolving Threat Landscape	Setiadi et al. (2025)	Rapid growth in linguistic and image steganography creates multifaceted threat profiles.	Forensics teams must broaden their scope beyond traditional formats to manage stego risks.
Public Awareness Gaps	Nicolás-Sánchez & Castro-Toledo (2024)	EU-based study finds lack of public awareness on digital steganalysis ethics. Poor transparency damages public trust in forensic investigations.	Public engagement and ethical disclosure strategies are essential.
Societal & Legal Impact	Lee et al. (2025)	Public trust influences acceptance of AI-based digital evidence. Ethical and legal frameworks must support forensic practices.	Policy and standards must balance investigative capabilities with transparency and accountability.
Need for Governance	Michaylov, Nicolás-Sánchez, Lee et al.	Technological progress alone is insufficient; forensic systems must be ethically and legally grounded.	Comprehensive forensic governance must include tech, legal, and social layers.

10. CONCLUSION

The combination of digital forensics and steganography is a crucial advancement in contemporary cybersecurity, as this study has highlighted. The ability to hide information across a variety of digital media formats has surpassed the detection capabilities of many conventional forensic tools due to the quick rise of AI-enhanced steganographic techniques. According to recent research, secret methods that employ multimodal AI models—which can embed content from text, audio, and video—are growing more resistant to conventional steganalysis (Chang & Echizen, 2025). To guarantee that digital evidence can be reliably extracted and analysed in real time, it is imperative that forensic tools, training procedures, and investigative methodologies be urgently reevaluated. In order to effectively combat cyber threats, our forensic techniques must also adapt as they become more complex and subtle. The study also emphasises how crucial it is to combine practical forensic preparedness with analytical breakthroughs. The literature indicates that deep learning models and sophisticated convolutional neural networks can attain detection accuracies of over 95% (Zhang et al., 2024), but infrastructure constraints and practitioner skill gaps limit practical implementation. According to market research, even though the digital forensics industry is expected to expand rapidly, readiness and legal admissibility remain barriers to broad adoption (Grand View Research, 2024). In order to satisfy the demands of investigators, legislators, and legal systems, these findings emphasise the need for technologically sophisticated and institutionally integrated digital forensic frameworks that combine automation, interpretability, and ethical protections. Lastly, this study promotes a multi-phase, standardised forensic model that includes steganographic detection from the very beginning of evidence collection. Through the alignment of detection workflows with ethical and legal standards, the suggested model promotes proactive forensic readiness. It also highlights how important it is for tool developers, law enforcement, academic researchers, and cybersecurity professionals to work together. Forensic responses must continue to be reliable, flexible, and future-ready, so the digital forensic community must prioritise cross-disciplinary collaborations, global policy alignment, and technological innovation going forward. The growing problem of hidden data transmission in cybercrime can only be systematically addressed with this integrated approach.

REFERENCES:

- Ahmed, R., & Nasir, A. (2025). Cross-border data sharing and digital forensics: Policy gaps and legal challenges. *Computer Law & Security Review, 51*, 105988. https://doi.org/10.1016/j.clsr.2024.105988
- Ahmed, S., Alshammari, A., & Hossain, M. S. (2024). A secure and traceable digital forensic model for hybrid cloud and IoT environments. Electronics, 13(18), 3729. https://doi.org/10.3390/electronics13183729
- Alasmary, W., Mekky, H., & Alzahrani, A. (2025). A comprehensive survey on stegomalware detection in digital media. *Signal Processing, 213*, 109888. https://doi.org/10.1016/j.sigpro.2025.109888
- Ansari, A. S. (2024). A review on the recent trends of image steganography for VANET applications. Computers, Materials & Continua, 81(3), 2325–2348. https://doi.org/10.32604/cmc.2024.045908
- Apau, R., Asante, M., Twum, F., Ben Hayfron-Acquah, J., & Peasah, K. O. (2024). Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review. PLOS ONE, 19(9), e0308807. https://doi.org/10.1371/journal.pone.0308807
- Bhattacharya, S., & Parhi, D. R. (2024). Artificial intelligence in image forensics: Emerging techniques and future perspectives. *Forensic Science International: Digital Investigation, 41*, 301604.
- Chang, C.-C., & Echizen, I. (2025). Steganography beyond space-time with chain of multimodal AI agents. *Scientific Reports*. Advance online publication. https://doi.org/10.1038/s41598-025-97238-2
- 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. J Forensic Sci. 2025; 70: 932–943. https://doi.org/10.1111/1556-4029.70035
- Ghosal, A., & Ghosh, S. (2024). Steganography in generative AI: Threat vectors and detection models. *Journal of Information Security and Applications, 74*, 103657
- Ghosh, T., & Dey, R. (2025). AI-driven steganography and challenges in threat detection systems. *Journal of Cybersecurity and Privacy*, 5(1), 66–81. https://doi.org/10.3390/jcp5010004

- Grand View Research. (2024). *Digital forensics market size, share & trends analysis report, 2024–2030*. https://www.grandviewresearch.com/industry-analysis/digital-forensics-market
- Hargreaves, B., Singh, P., & Al-Fahad, N. (2024). *Digital Forensics Practitioner Pulse 2024: Survey of AI readiness and tool reliability*. Journal of Digital Forensic Science, 12(1), 44–61. https://doi.org/10.1016/j.jdifs.2024.100274
- Hoover, R., Stella, C., & Alice, W. (2025). Artificial intelligence in digital forensics: Enhancing forensic work with machine learning. *ResearchGate*. https://www.researchgate.net/publication/390534918
- KBV Research. (2024). *Asia-Pacific digital forensics market, by component, forecast 2024–2031*. https://www.kbvresearch.com/asia-pacific-digital-forensics-market/
- Kheddar, H., Hemis, M., Himeur, Y., Megías, D., & Amira, A. (2025). Deep learning for steganalysis of diverse data types: A review of methods, taxonomy, challenges and future directions. Multimedia Tools and Applications. Advance online publication. https://doi.org/10.1007/s11042-025-13055-8
- Kumar, A., & Sharma, P. (2024). A comprehensive survey on steganography techniques in cybersecurity. Journal of Cybersecurity and Privacy, 4(1), 19–35. https://doi.org/10.3390/jcp4010002
- Lee, J., Martins, C., & Kapoor, A. (2024). Transparency and admissibility in AI-assisted digital forensics. *Forensic Science International*: Reports, 8, 100337. https://doi.org/10.1016/j.fsir.2024.100337
- Li, J., & Wang, H. (2024). Optimize image steganography based on distinction disparity and high security. Mathematical Problems in Engineering, 2024, Article 251656. https://doi.org/10.1155/2024/251656
- Li, X., Zhao, Y., & Wang, J. (2025). Advances in transformer-based generative steganography: Proceedings of IEEE WIFS 2025. IEEE Transactions on Information Forensics and Security. Advance online publication. https://doi.org/10.1109/TIFS.2025.3491920
- Majumdar, T., & Ghosh, S. (2025). Deepfake–augmented steganography: Challenges for forensic detection. Computers & Security, 160, 103596. https://doi.org/10.1016/j.cose.2025.103596
- Michaylov, K. D., & Sarmah, D. K. (2024). Steganography and steganalysis tools for digital image forensic analysis: An empirical comparison. Journal of Cyber Security Technology, 9(1), 1–27. https://doi.org/10.1080/23742917.2024.2304441
- Michaylov, K. D., & Sarmah, D. K. (2024). Steganography and steganalysis for digital image enhanced forensic analysis and recommendations. *Journal of Cyber Security Technology*, 9(1), 1–27. https://doi.org/10.1080/23742917.2024.2304441
- Michaylov, K. D., & Sarmah, D. K. (2024). Steganography and steganalysis for digital image enhanced forensic analysis and recommendations. *Journal of Cyber Security Technology*, 9(1), 1–27. https://doi.org/10.1080/23742917.2024.2304441
- Nicolás Sánchez, A., & Castro Toledo, F. J. (2024). Uncovering the social impact of digital steganalysis tools applied to cybercrime investigations: A European Union perspective. *Crime Science*, 13(1), Article 11. https://doi.org/10.1186/s40163-024-00209-7
- Peltier, T.R. (2010). Information Security Risk Analysis (3rd ed.). Auerbach Publications. https://doi.org/10.1201/EBK1439839560
- Ramanpreet Kaur, Dušan Gabrijelčič, Tomaž Klobučar (2023). Artificial intelligence for cybersecurity: Literature review and future research directions, Information Fusion, Volume 97. https://doi.org/10.1016/j.inffus.2023.101804
- Tang, W., Rao, Y., Yang, Z., Peng, F., Cui, X., Huang, J., & Zhu, P. (2025). Reversible generative steganography with distribution-preserving. Cybersecurity, 8, 18. https://doi.org/10.1186/s42400-024-00317-6
- Xinran, L., & Zichi, W. (2024). Vaccine for digital images against steganography. *Scientific Reports*, 14, Article 21340. https://doi.org/10.1038/s41598-024-72693-5
- Yin, Z., Wang, Z., Xu, W., Zhuang, J., Mozumder, P., Smith, A., & Zhang, W. (2025). Digital forensics in the age of large language models. *arXiv*. https://doi.org/10.48550/arXiv.2504.02963
- Zhang, S., Xiao, Y., Tian, H., & Li, X. (2025). A multi-image steganography scheme using image stitching sender (ISS). Cybersecurity, 8, 20. https://doi.org/10.1186/s42400-024-00333-6
- Zhang, Y., Zhao, F., & Liu, M. (2024). Digital Forensic Practitioner Pulse 2024: Tool usage and performance benchmarking. *Digital Investigation*, 40, 301627. https://doi.org/10.1016/j.diin.2024.301627
- Zhou, Y., Zhang, Q., & Li, X. (2022). AI-powered digital forensics: Challenges and opportunities. Forensic Science International: Digital Investigation, 40, 301500.