International Journal of Engineering and Techniques - Volume 12 Issue 3, May-June - 2026

RESEARCH ARTICLE OPEN ACCESS

Advanced Steganography Methods in Modern Cybersecurity

Alaa Jabbar Almaliki[1], Osman Ghazali[2], Roshidi Din[3]

1,2,3(School of Computing, College of Arts and Sciences, Universiti Utara Malaysia, 06010, Sintok, Kedah, Malaysia

Email: alaa.jabbar@uum.edu.my, osman@uum.edu.my, roshidi@uum.edu.my)

Abstract:

Steganography is an information security technique that enables the concealment of data within digital objects without being detected by other users. In the current digital era, this technique is highly valuable for ensuring data security and privacy in digital communication. This paper explores the uses and applications of steganography in the digital age by analyzing existing literature and global research findings. The literature review demonstrates the importance of steganography in data protection and information security, identifying various applications such as banking information security, email communication, and the protection of medical images. The research methodology employed a systematic review of scientific literature for data collection.

The global findings indicate that steganography is a widely used technique across different domains, and its application helps maintain information privacy and security. However, its disadvantages include the potential malicious use of the technique for criminal activities. In the discussion section, the obtained results were evaluated, comparisons were made, and challenges associated with the use of steganography in the digital age were identified. In the conclusion section, the most relevant information was summarized, key findings were highlighted, and recommendations for future research were presented. In conclusion, steganography is a useful technique for protecting and ensuring information security in the digital age. Despite some disadvantages, its application can provide significant advantages in safeguarding data privacy and preventing potential cyberattacks.

Keywords — **Steganography, Digital Steganography, Information Concealment, Information Security, Privacy, Cryptography**

I. INTRODUCTION

At present, technology has become a key aspect of our daily lives. The increasing use of digital devices and access to the Internet has led to a wide range of opportunities across various domains, from communication to education and entertainment [1, 2]. However, the growth in the use of technology has also resulted in the emergence of new online threats, such as digital espionage and information theft. In this context, steganography has become an important tool for protecting the privacy and security of information in the digital age [3-5]. Steganography is a technique used to conceal information within a communication medium, in such a way that only the intended recipients can access it. Unlike cryptography, which is used to encrypt information, steganography focuses on hiding the information itself [6-8]. Consequently, this scientific article presents a literature review on the uses and applications of steganography in the digital age. It addresses the history and definition of steganography, its characteristics, types, and the techniques currently used. In addition, it analyses how steganography has been employed to protect privacy and security in various fields, including communication, copyright protection, cloud security, and information security in general. Therefore, the main objective of this study is to explore the relevance and applications of steganography in the present day, and how it can contribute to information security and privacy in the digital age [9]. The use of steganography in different domains and its potential benefits is examined. Furthermore, the ethical implications of its use and the limitations of the technique are analysed. Ultimately, this work aims to contribute to a deeper understanding and knowledge of steganography, its applications, and its benefits in the digital era.

II. LITERATURE REVIEW

Steganography is a technique used to conceal secret information within digital media while maintaining the visual or perceptual quality of the original content. Unlike cryptography, which focuses on encrypting information, steganography aims to hide the existence of the message itself, making it an essential approach in secure communication and information protection systems [10]. Over the years, steganography has evolved from traditional hidden communication methods into advanced digital techniques integrated with modern cyber security frameworks.

Recent developments in image steganography have significantly improved the capability of hiding data within multimedia content. [11] Provided a comprehensive survey of spatial-domain image steganography techniques, highlighting methods such as Least Significant Bit (LSB) substitution and their effectiveness in preserving image quality while embedding hidden information [6, 8, 12]. Their study emphasized that image steganography remains one of the most widely adopted techniques due to its simplicity, flexibility, and high embedding capacity.

With the advancement of artificial intelligence, modern steganography has increasingly incorporated deep learning and Generative Adversarial Networks (GANs). [13] Introduced invisible steganography models based on GAN architectures, demonstrating how adversarial learning can enhance imperceptibility and resistance against steganalysis. Similarly, [14] proposed the HiDDeN framework, which utilizes deep neural networks for end-to-end data hiding and extraction. Their work showed that deep learning models can significantly improve the robustness and reliability of hidden communication systems.

In addition, [15] presented a deep steganography model capable of hiding entire images within other images using neural networks. This approach represented a major advancement compared to traditional techniques because it enabled high-capacity data embedding while maintaining minimal visual distortion. These studies collectively indicate that deep learning has become a transformative factor in the evolution of modern stenographic systems.

Beyond image-based approaches, steganography has also been applied in audio and video environments. [16] discussed various image steganography and steganalysis techniques, emphasizing the importance of multimedia security and the growing demand for secure transmission methods across digital communication systems. Their findings highlighted that multimedia steganography plays a significant role in protecting sensitive information within modern communication infrastructures.

As steganography techniques continue to advance, steganalysis methods have also evolved to detect hidden information. [17] Introduced rich models for digital image steganalysis, providing highly effective detection mechanisms capable of identifying concealed data within images. Their research demonstrated that statistical feature extraction and machine learning techniques can significantly improve hidden data detection accuracy. Consequently, the continuous competition between steganography and steganalysis has become a critical area of research in information security.

Steganography is also closely related to cyber security and cybercrime prevention. [18] Examined the role of obfuscated malware and hidden communication methods in cybercrime activities. Their work revealed that attackers may exploit data hiding techniques to evade traditional security systems, emphasizing the necessity of advanced cyber security frameworks capable of detecting concealed threats.

Another important application of steganography lies in digital watermarking and intellectual property protection. [19] Discussed the integration of digital watermarking with steganographic principles to secure multimedia ownership and prevent unauthorized duplication of digital assets. Digital watermarking has become widely used in copyright protection systems due to its ability to embed ownership information invisibly within digital content.

From a broader historical perspective, [20] explored the history of secret communication and code systems, demonstrating how information

concealment has always played a vital role in political, military, and intelligence operations. His work provides important historical foundations for understanding the evolution of modern digital steganography and secure communication technologies.

Overall, the reviewed literature demonstrates that steganography has evolved into a sophisticated field combining multimedia processing, artificial intelligence, cyber security, and privacy protection. Modern steganography techniques continue to improve in terms of robustness, imperceptibility, and embedding capacity, while advances in steganalysis continue to challenge the effectiveness of hidden communication systems. Therefore, ongoing research remains essential for enhancing secure communication and addressing emerging cyber security challenges.

III. METHODOLOGY

The methodology used to conduct this research on the uses and applications of steganography in the digital age was based on a systematic literature review. Accordingly, an extensive search was carried out for scientific articles, theses, and other academic works related to the topic across various databases, such as Scopus, Web of Science, and Google Scholar. The search terms used included "steganography," "digital steganography," "information concealment," "information security," "privacy," and "cryptography."

In addition, inclusion and exclusion criteria were applied to select the studies relevant to this research. The inclusion criteria included the relevance of the work to the research topic, the publication date. The exclusion criteria included works that were not related to steganography or did not provide relevant information for the research.

Therefore, a careful review of the selected works was conducted, and relevant information regarding the uses and applications of steganography in the digital age was extracted. A descriptive approach was employed to analyze and present the findings of the systematic literature review.

It is important to note that this methodology has limitations, and the results obtained depend on the quality and availability of the works included in the systematic literature review. However, a thorough effort was made to identify and select the most relevant studies for this research.

IV. RESULTS

The research findings suggest that steganography is a useful and widely employed technique in the digital age for concealing information within images, audio files, and video files. It has been applied across various domains, including information security, copyright protection, surveillance and espionage, and censorship.

In the field of information security, steganography has been used to hide secret messages within images and audio files to prevent the detection of confidential information. This technique has been applied in military, intelligence, and corporate environments to protect information against espionage and piracy.

In copyright protection, steganography has been used to embed digital watermarks within images, audio, and video to prevent unauthorized copying of protected content.

In surveillance and espionage, steganography has been utilized to conceal information within multimedia files to evade threat detection systems. It has been employed in espionage and surveillance activities by governments and military organizations.

In censorship contexts, steganography has been used to bypass censorship filters and enable the transmission of restricted information through government-controlled networks.

At a global level, steganography has been extensively studied in areas such as information security and digital forensics. Tools and techniques have been developed for detecting hidden messages and recovering concealed information from multimedia files. Additionally, methods have been proposed to improve the effectiveness of steganography and enhance its resistance to attacks.

In general, steganography is a versatile and useful technique for hiding information in the digital age, with applications in areas such as information security, copyright protection, surveillance and espionage, and censorship. However, it also presents challenges in terms of detection and prevention of concealed confidential information.

As a model for information concealment, steganography offers both advantages and disadvantages, which are presented below:

Advantages

- It enables the secure transmission of sensitive information, such as personal, financial, or research data, without attracting the attention of potential interceptors.
- Being invisible to the naked eye, information can be transmitted through various types of files, such as images, audio, or video, without raising suspicion.
- Steganographic techniques can be used to protect privacy on social media and online platforms by hiding information in shared messages or images.
- In the field of security, steganography is used to detect potential threats by concealing identity and location information of devices, making them difficult to trace.

Disadvantages

- Steganography can be used for illegal purposes, such as the unlawful transmission of confidential information, evasion of Internet censorship, or dissemination of extremist propaganda.
- Since it is not detectable by simple observation, it can be difficult for security systems to identify hidden information in files, potentially facilitating the spread of malware and computer viruses.
- Steganographic techniques may be used maliciously, such as inserting information into files without user knowledge, thereby compromising data integrity.
- It requires specialized technical knowledge, limiting its use to experts and potentially making it costly in terms of time and resources.

On the other hand, the research identified several significant findings, highlighting the versatility and relevance of this technique in various contexts.

The main findings are presented below:

1. Applications in Information Security:

A widespread use of steganography in information security was identified. The technique is used to hide sensitive data, such as passwords or authentication data, within multimedia files, providing an additional layer of protection against cyber threats.

2. Covert Communications:

The study revealed the use of steganography in covert communications. Government groups, intelligence organizations, and military entities utilize this technique to conceal important messages within images, videos, or even seemingly ordinary documents.

3. Copyright Protection:

An increasing use of steganography in copyright protection and digital watermarking was observed. Embedding intellectual property information within multimedia files helps track and protect ownership of digital content such as images, videos, and documents.

4. Steganography in Social Media:

The research highlighted the presence of steganography on social media platforms, where users employ this technique to hide confidential information or share messages discreetly. This raises security and privacy challenges in online environments.

5. Forensic Steganography:

A growing interest in forensic steganography was identified, particularly in recovering hidden data during criminal investigations. The technique has become an important tool for digital investigators in identifying concealed evidence.

6. Development of New Steganographic Techniques:

Continuous development of new techniques to evade conventional detection methods was observed, emphasizing the need for ongoing research in cybersecurity to keep pace with emerging threats.

7. Ethical and Legal Challenges:

Ethical and legal challenges related to the use of steganography were identified, particularly concerning privacy and potential misuse of the technology. The need for clear regulations and policies in this area was emphasized.

V. DISCUSSION AND ANALYSIS

When utilizing modern technological applications, it is essential to consider the security of the information being handled. In this regard, [3] highlights the importance of applying information

encryption mechanisms within organizations to prevent risks such as cyberattacks, plagiarism, and loss of confidentiality.

Indeed, information security has become an increasingly relevant issue in the digital age. [21] proposes a distributed cybersecurity strategy that applies the concept of intelligence operations to strengthen information protection within organizations.

Within the cybersecurity context, cyber warfare has also been widely discussed. [22] addresses this topic by analyzing different types of attacks and strategies used in such conflicts.

Furthermore, information concealment techniques such as steganography can be employed to protect sensitive data. [23] present an implementation of multiple substitution steganography using Matlab in a research workshop.

On the other hand, [24] explores the application of steganography in libraries, demonstrating that this technique can be used across diverse contexts. Additionally, despite the existence of various information protection techniques, phishing attacks remain one of the major threats. [6, 25, 26] conducted a systematic literature review to characterize these attacks and propose mitigation strategies.

Moreover, the digital age also presents challenges for social research. [27] discuss the challenges of digital ethnography in on life fieldwork.

In conclusion, the digital world presents multiple challenges in terms of information security and social research. It is essential to remain informed about the different techniques and strategies that can be used to protect information and ensure ethical and responsible research practices.

The following tables present a structured research discussion organized in comparative formats to highlight the different uses and applications of steganography in the digital age:

TABLE I
USES OF STEGANOGRAPHY IN THE DIGITAL AGE

Uses of Steganography	Description
Information Security	Conceals sensitive data to protect against cyber threats.
Covert Communications	Used by government agencies for strategic messaging.
Copyright Protection	Embeds digital watermarks to track and protect intellectual property.
Steganography in social media	Hides messages in images or text for more discreet communication.
Forensic Steganography	Used in the recovery of hidden data in criminal investigations.

Table 1 demonstrates the diverse applications of steganography in the digital age, particularly in information security, covert communications, copyright protection, and forensic investigations. The findings indicate that steganography has evolved into a multifunctional technology capable of supporting privacy preservation and secure digital communication across multiple domains.

TABLE II
ETHICAL AND LEGAL IMPLICATIONS OF STEGANOGRAPHY

Ethical and Legal Aspects	Considerations
Privacy	Possibility of misuse for unethical communication.
Intellectual Property	Protection of copyrights and trademarks.
Government Monitoring	Potential risks of abuse in government surveillance.
Regulation	Need for clear regulations to guide ethical use.
Ethical and Legal Aspects	Considerations

Table 2 highlights the ethical and legal implications associated with steganography technologies. The analysis reveals that while steganography enhances privacy and intellectual property protection, it may also be exploited for unethical or illegal purposes. Therefore, effective regulations and ethical frameworks are essential to ensure responsible usage.

TABLE III
CONTINUOUS DEVELOPMENT OF STEGANOGRAPHIC TECHNIQUES

Evolution of Techniques	Considerations
Technological Changes	Adoption of new technologies that influence steganographic techniques.
Continuous Research	Need for ongoing research to keep up with emerging threats.
Development of Countermeasures	Parallel development of advanced detection methods.
Evolution of Techniques	Considerations
Technological Changes	Adoption of new technologies that influence steganographic techniques.

Table 3 illustrates the continuous evolution of steganographic techniques driven by technological advancements and emerging cybersecurity threats. The findings emphasize the importance of ongoing research and the parallel development of advanced steganalysis and countermeasure techniques to address modern security challenges.

Based on the above, it can be stated that steganography in the digital age represents a versatile tool with diverse applications. However, its use raises ethical and legal challenges that must be addressed through clear regulations. Furthermore, its continuous evolution highlights the importance of ongoing research to understand and respond to emerging threats in the current digital environment.

VI. CONCLUSIONS

After analysing the existing literature and conducting this research, it can be concluded that steganography has numerous applications in the digital age, both in civilian and military domains. It can be applied in various areas such as information security, privacy protection, and intellectual property protection, among others.

Among the main advantages of steganography are its ability to transmit information secretly, the difficulty of detecting its use, and its flexibility to adapt to different types of files and information systems. However, some disadvantages have also been identified, such as the requirement for specialized technical knowledge and the possibility of misuse for illegal purposes.

It is important to emphasize that steganography must be used responsibly and ethically, as its misuse can have serious consequences for individuals' security and privacy. Additionally, further research and development of new techniques and tools are necessary to improve its effectiveness and reduce potential risks.

In conclusion, steganography is a valuable tool in the digital age, offering a wide range of applications and possibilities. However, its use must be responsible and ethical, and further research is needed to fully understand its advantages and disadvantages.

The study reveals that steganography plays a crucial role in various aspects of the digital age, ranging from information security to copyright protection and forensic investigations. Nevertheless, its use raises ethical and legal challenges that must be addressed to ensure an appropriate balance between privacy and security in the modern digital environment.

REFERENCES

[1] A. M. G. Aguirre, "Uso de recursos TIC en la enseñanza de las matemáticas: retos y perspectivas," *Entramado,* vol. 14, no. 2, pp. 198-214, 2018.

[2] A. A. J. S. Altaay, Shahrin Bin Zamani, Mazdak, "An introduction to image steganography techniques," in *2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, 2012: IEEE, pp. 122-126.

[3] Y. F. Chala, "Importancia de la aplicación del mecanismo de cifrado de información en las empresas para la prevención de riesgos como ataques, plagio y pérdida de la confidencialidad," 2019.

[4] A. J. Qasim, R. Din, F. Q. A. J. B. o. E. E. Alyousuf, and Informatics, "Review on techniques and file formats of image compression," vol. 9, no. 2, pp. 602–610, 2020.

[5] Q. Alaa Jabbar, D. Roshidi, and A. Farah Qasim Ahmed, "Extended Method of Least Significant Bits on Colour Images in Steganography," *QALAAI ZANIST SCIENTIFIC JOURNAL,* vol. 9, no. 3, pp. 1146-1158, 10/06 2024, doi: 10.25212/lfu.qzj.9.3.45.

[6] A. J. Qasim Almaliki *et al.*, "Application of the Canny Filter in Digital Steganography," *Journal of Advanced Research in Computing and Applications,* vol. 35, no. 1, pp. 21-30, 05/17 2024, doi: 10.37934/arca.35.1.2130.

[7] O. G. Roshidi Din, Alaa Jabbar Qasim, "Analytical Review on Graphical Formats Used in Image Steganographic Compression," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. Vol 12, No 2, p. pp. 441~446, 2018, doi: 10.11591.

[8] A. J. Qasim and R. Din, "Capacity Performance of LSB Method On Multi-Layer Images in Steganography."

[9] J. A. Moreno Jaraba, "Estudio de la detección de ciberataques de estenografía para evitar ingreso de Software malicioso y evitar pérdidas de información en la Cámara de Comercio de Barrancabermeja," 2021.

[10] J. Fridrich, *Steganography in digital media: principles, algorithms, and applications*. Cambridge university press, 2009.

[11] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. Ho, and K.-H. Jung, "Image steganography in spatial domain: A survey," *Signal Processing: Image Communication,* vol. 65, pp. 46-66, 2018.

[12] O. G. Sunariya Utama Alaa Jabbar Qasim Almaliki, Roshidi Din, "Comparative Analysis of LSB, PVD, and EMD-Based Stenographic Methods with Hybrid Optimization in Digital Images," *International Journal of Engineering and Techniques,* vol. 11, pp. 351-357, 2025.

[13] R. Zhang, S. Dong, and J. Liu, "Invisible steganography via generative adversarial networks," *Multimedia tools and applications,* vol. 78, no. 7, pp. 8559-8575, 2019.

[14] J. Zhu, R. Kaplan, J. Johnson, and L. Fei-Fei, "Hidden: Hiding data with deep networks," in *Proceedings of the European conference on computer vision (ECCV)*, 2018, pp. 657-672.

[15] S. Baluja, "Hiding images in plain sight: Deep steganography," *Advances in neural information processing systems,* vol. 30, 2017.

[16] S. Bhattacharyya, "A survey of steganography and steganalysis technique in image, text, audio and video as cover carrier," *Journal of global research in computer science,* vol. 2, no. 4, 2011.

[17] J. Fridrich and J. Kodovsky, "Rich models for steganalysis of digital images," *IEEE Transactions on information Forensics and Security,* vol. 7, no. 3, pp. 868-882, 2012.

[18] M. Alazab, S. Venkatraman, P. Watters, M. Alazab, and A. Alazab, "Cybercrime: the case of obfuscated malware," in *International Conference on e-Democracy*, 2011: Springer, pp. 204-211.

[19] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, "Digital watermarking and steganography morgan kaufmann publishers," *Amsterdam/Boston,* 2008.

[20] D. Kahn, *The Codebreakers: The comprehensive history of secret communication from ancient times to the internet*. Simon and Schuster, 1996.

[21] I. M. Gallardo Urbini, "Estrategia de Ciberseguridad Distribuida, aplicando el concepto de Operación de Inteligencia," Universidad Nacional de La Plata, 2022.

[22] Y. Quintana, *Ciberguerra*. Los libros de la Catarata, 2023.

[23] G. S. Navas and G. Rodríguez Medina, "Esteganografía por sustitución múltiple, implementación en Matlab," in *XXI Workshop de Investigadores en Ciencias de la Computación (WICC 2019, Universidad Nacional de San Juan)*. 2019.

[24] C. Sanchís Francés, "Esteganografía y ocultación de información aplicadas a bibliotecas," 2022.

[25] S. Utama, I. S. Seger, S. M. Abd, R. Din, A. J. Qasim Almaliki, and J. Qasim Almaliki, "Analytical and Empirical Insights into Wireless Sensor Network Longevity: The Role MAC Protocols and Adaptive Strategies," *Journal of Advanced Research in Computing and Applications,* vol. 36, no. 1, pp. 52-60, 09/18 2024, doi: 10.37934/arca.36.1.5260.

[26] R. Din, A. H. Shakir, S. H. Ali, A. J. Qasim Almaliki, and S. Utama, "Exploring Steganographic Techniques for Enhanced Data Protection in Digital Files," *International Journal of Advanced Research in Computational Thinking and Data Science,* vol. 1, no. 1, pp. 1-9, 04/19 2024, doi: 10.37934/ctds.1.1.19a.

[27] K. B. Barajas and N. P. Carreño, "Desafíos de la etnografía digital en el trabajo de campo onlife," *Virtualis,* vol. 10, no. 18, pp. 134-151, 2019.