IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2024

DOI: 10.17148/IJARCCE.2024.13520

INVISIBLE INK OF THE DIGITAL AGE: A SURVEY OF STEGANOGRAPHY IN INFORMATION SECURITY

Bhavani B D[1], A. Rengarajan[2]

Student of MCA, Department of CS & IT, Jain (Deemed-to-be-University), Bengaluru, India[1]

Professor, Department of CS & IT, Jain (Deemed-to-be-University), Bengaluru, India[2]

Abstract: Technological advancements empower multimedia data exchange within IoT, posing security risks. Steganography, bolstered by deep learning, complements encryption, enhancing concealment and detection. Categorization, methodologies, and evaluation metrics drive innovation in image and video steganography. ISN and video techniques increase capacity while ensuring quality. Robust defences against steganalysis are imperative for safeguarding sensitive data...

Keywords: Steganography, Cryptography, Multimedia data security, Deep learning, Convolutional Neural Networks (CNNs), Generative Adversarial Networks (GANs)

I. INTRODUCTION

Advancements in technology have led to increased multimedia data exchange, especially within the Internet of Things (IoT). However, insecure networks pose significant threats to data security and privacy. To address these challenges, researchers are turning to steganography alongside traditional cryptographic methods. Steganography, the art of concealing information within seemingly innocent carriers like images or videos, has become increasingly important in complementing encryption techniques. Recent progress includes the integration of deep learning, particularly Convolutional Neural Networks (CNNs) and Generative Adversarial Networks (GANs), which have transformed both steganography and steganalysis. These techniques enhance the hiding and detection of concealed data, marking a significant shift in the field's landscape. Moreover, researchers have categorized steganography based on technical and non-technical aspects, addressing concerns such as payload capacity, image quality, and robustness. The literature also explores methodologies for image and video steganography, with a focus on enhancing payload capacity while maintaining undetectability. Notably, the proposal of the Large-Capacity Invertible Steganography Network (ISN) leverages image domain transformation to increase capacity while ensuring high-quality results. Video steganography, with its high capacity and complex structure, presents an attractive alternative, prompting extensive research into various methods, including raw and compressed domain approaches. Evaluation metrics such as PSNR, MSE, and robustness play a crucial role in assessing steganographic techniques, aiding in comparative analysis and identifying performance benchmarks. Additionally, the review discusses steganalysis attacks used to test the security of these techniques, highlighting the need for robust defenses against detection. In summary, this review provides insights into the evolving landscape of steganography and its vital role in safeguarding sensitive information. It offers valuable perspectives for researchers and practitioners, identifying research gaps and proposing future directions for advancing multimedia data security

II. BACKGROUND AND CONTEXT

The word "steganography" is derived from two Greek words, "steganos," meaning hidden, and "graphia," meaning writing. In simple words, this is the practice that shows how a message should be hidden in another medium in a way that to all appearance the existence of the message is also hidden. Examples of steganography include hiding text in an image, embedding data in audio files, or concealing messages in some apparently innocent digital files. Steganography, the ancient practice of embedding important messages in the wax tables or writing them on parchment in invisible ink, dates back to its history. The oldest known example is probably that of Herodotus, who related the story of Histiaeus who had the head of his most trusted slave shaved, had a message tattooed on his scalp after regrowth, and then sent him as a messenger. As the digital technology appeared, steganography has been extended, and by this time, one may find an entirely new range of digital media it applies to. It can be a variant of least significant bit steganography in a digital image, changing the packet timing in a network communication, or changing the very small attributes of an audio file in

 This work is licensed under a Creative Commons Attribution 4.0 International License

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2024
DOI: 10.17148/IJARCCE.2024.13520

the digital world. In recent years, steganography has regained massive interest due to its secretive use by spies and criminals, and then through varied applications such as digital watermarking, copyright protection, and covert communications in cybersecurity. It has increasingly been a part of cybersecurity practice, where both defenders and attackers adopt steganographic techniques to hide or detect sensitive information. Detection methodologies in steganography are now an increasingly important trend, placed opposite to ever more sophisticated methods of concealment. People are putting forth new algorithms and discovery tools of new ways to hide information all the time, increasing the complexity of this cat-and-mouse game between information hiders and seekers. Steganography is still such an exciting field to date, with a very rich history and developments that take place. Spy in the way of communication and a manner to date, it shows up in both ancient and modern forms of communication.

III. LITERATURE REVIEW

The exchange of multimedia data, especially within the Internet of Things (IoT), has surged with the evolution of technology. However, this increased connectivity has brought forth significant concerns regarding data security and privacy due to the prevalence of insecure networks. In response to these challenges, researchers have increasingly turned to steganography, alongside traditional cryptographic methods, to safeguard sensitive information. Steganography, the practice of concealing data within seemingly innocuous carriers such as images or videos, has emerged as a powerful tool for effectively hiding information. Recent advancements in the field have been driven by the integration of deep learning techniques, notably Convolutional Neural Networks (CNNs) and Generative Adversarial Networks (GANs). These technologies have not only revolutionized steganography but have also enhanced steganalysis, the process of detecting hidden data. The utilization of deep learning algorithms has enabled significant improvements in both the concealment and detection of hidden information, marking a notable shift in the landscape of multimedia data security.

Moreover, researchers have undertaken efforts to categorize steganography methodologies based on various technical and non-technical aspects. This categorization helps address specific concerns such as payload capacity, image quality, and robustness, providing a framework for evaluating different techniques.

In the realm of image and video steganography, methodologies are continually evolving to enhance payload capacity while maintaining undetectability. One notable advancement is the proposal of the Large-Capacity Invertible Steganography Network (ISN), which leverages image domain transformation to significantly increase capacity while preserving high-quality results. Additionally, research in video steganography has gained traction due to its high capacity and complex structure, leading to the exploration of various methods, including raw and compressed domain approaches.

Evaluation metrics such as Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), and robustness play a crucial role in assessing the effectiveness of steganographic techniques. These metrics aid in comparative analysis and benchmarking performance, guiding researchers in selecting the most suitable methodologies for specific applications. Furthermore, the review underscores the importance of robust defenses against steganalysis attacks, highlighting the need for continuous advancements in data security.

In conclusion, this literature review provides insights into the evolving landscape of multimedia data security, emphasizing the growing significance of steganography in complementing encryption techniques. By addressing current challenges, identifying research gaps, and proposing future directions, this review serves as a valuable resource for researchers and practitioners in advancing the field of multimedia data security.

Additional Data:
While the literature review outlines the current state of multimedia data security and the role of steganography, additional data could further enrich the discussion. This could include:

1. Case Studies: Examining real-world applications of steganography in diverse fields such as military communication, digital forensics, and cybersecurity.
2. Technological Innovations: Highlighting recent technological advancements in steganography tools and software, as well as emerging trends in steganalysis techniques.
3. Legal and Ethical Considerations: Exploring the legal and ethical implications of employing steganography, particularly in areas such as data privacy, intellectual property protection, and compliance with regulations.
4. User Perspectives: Gathering insights from users and stakeholders on their perceptions, concerns, and preferences regarding the use of steganography for data security.

By incorporating additional data from these areas, the literature review can offer a more comprehensive understanding of the multifaceted landscape of multimedia data security and steganography.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 5, May 2024

DOI: 10.17148/IJARCCE.2024.13520

IV. METHODOLOGY

This review strictly adheres to a systematic criterion and methodology in the selection and evaluation of the literature to make it comprehensive and relevant. The search process will try to find papers that brought a major contribution to the comprehension of multimedia data security, with special focus on steganography and its applications.

Search Process: Database: Systematic searches will be performed in academic databases including IEEE Xplore, ACM Digital Library, PubMed, Scopus, and Google Scholar.

Search Strings: The search keywords used are related to security of multimedia data, steganography, cryptography, deep learning, IoT, and their related terms. For this purpose, Boolean operators and truncation were used.

Date Range: Papers published between dates appropriate to the scope of the review. English-language papers were included in most cases for purposes of increased access.

Inclusion criteria:
Relevance: Those covering multimedia data security, steganography, and related topics.

Quality: Preference was given to peer-reviewed articles, conference papers, and reputable journals in such a way that the information was of good quality and credible.

Contribution: Only novel papers with a contribution to insight, methodology, or in any other way giving a significant advance to this research field are considered.

Recency: Effort to include recent publications with the aim of covering the latest issues and trends.

Exclusion Criteria: Non-relevant: Papers that do not deal directly with multimedia data security or steganography were removed. Exclusion of sources that had not been peer-reviewed and papers that did not follow a rigorous methodology was done to maintain a level of credibility of the review. Old publications that did not add substantially to the existing information on the topic were left out.

Methodology of evaluation Comprehensive Review: Selected papers underwent a thorough review process to gather insights on information, methodologies, findings, and insights.

Comparative Study: Different steganography techniques compared through evaluation metrics like PSNR, MSE, and robustness.

Synthesizing: Information from the selected papers was synthesized to highlight the trends, gaps, challenges, and future directions in the field of multimedia data security and steganography. He will adhere to these criteria and methodologies, intending to prepare an even-handed and comprehensive review of the literature for further help in a deeper understanding of multimedia data security and steganography.

V. ANALYZING AND COMPARING THE FINDINGS

1. Use of Deep Learning Technologies: A common thread running through the reviewed literature is that the use of deep learning technologies has brought revolutionary changes in the area of steganography. In the related works, researchers mentioned how this revolution works in breakthroughs for steganography processes and steganalysis in better ways of both the capacity to conceal and to detect hidden data.

2. Emphasis on High Payload Capacity and Quality: Another consistent theme is the looking for high payload capacity with the least compromise on the quality of image and video outputs in steganography. A number of approaches, for instance, the ISN architecture, concern increasing the capacity of a steganography scheme and simultaneously preserving the image's integrity.

3.Categorization and Evaluation Metrics: Such techniques in the literature are often categorized based on their techniques or non-techniques such as payload capacity, image quality, and robustness. Besides, the performance evaluation criteria that are constantly being used for the measurement of steganographic techniques are PSNR, MSE, and robustness, allowing comparison and benchmarking.

DOI: 10.17148/IJARCCE.2024.13520

VI. LIMITATIONS AND GAPS IN EXISTING LITERATURE

Limited Real-World Attention: The literature is full of the discussions of methodologies and techniques, but, on the flip side, relatively less work has been done in the direction of real-world applications and case studies regarding steganography. Exactly how steganography is applied to real-life practical scenarios across domains can help better in gaining insight about its effectiveness and challenges.

2. Ethical and Legal Issues: Another significant gap is in the field of ethical and legal issues, and details linked to the use of steganography during major discussions. They could be applied in potential wrongdoings like terrorism and other illegal activities; surely there is a need to pursue research that will deal with ethical and legal issues, which incorporate regulatory compliance and privacy issues.

3. User perspective and usability. In most cases, the literature is void of the user perspective and experience on the usability and practicality of steganography tools and techniques. It could encompass user-centered research that is going to avail such an understanding of user interests, and concerns about usability challenges, and therefore even drive the design and development of steganographic systems.

4. Standardization and Benchmarking: Steganographic techniques are never appraised with standard benchmarks and evaluation frameworks. Setting standards and benchmarks for this means that the results of different studies are compared and that rigor and reliability of research are ensured in this field.

In short, the reviewed literature does offer valuable insight into the developments and challenges of multimedia data security and steganography. However, important limitations and some gaps that need further attention in the future include real-time applications of steganography, ethical and legal considerations, user perspectives, and standardization of the available benchmarks for better understanding and role of steganography in data security.

VII. CONCLUSION

In this regard, this survey paper gives an overall view of the changing scenario of steganography within the scope of multimedia data security. Advancement in the area of technology, and that too in the domain of Internet of Things (IoT), has left the gate of media data in exchange to be opened at an exponential rate. Contrary to that, insecure networks encompass and threaten every possible movement of data for security and privacy. In order to fight against these challenges, the current researchers are applying steganographic methods among other cryptographic approaches to protect confidential information.

To conclude, the survey paper serves as an important source of information for the research community and practitioners in the domain of multimedia data security and steganography. Therefore, the paper contributes to better enlightenment about the current challenges, identifies the research gaps, and proposes the future direction of steganography's vital role in hiding sensitive information in this digital era.

REFERENCES

[1]. Dhawan, S., & Gupta, R. (2021). Analysis of various data security techniques of steganography: A survey. In Information Security Journal (Vol. 30, Issue 2, pp. 63–87). Bellwether Publishing, Ltd. https://doi.org/10.1080/19393555.2020.1801911.

[2]. Dalal, M., & Juneja, M. (2021). A survey on information hiding using video steganography. Artificial Intelligence Review, 54(8), 5831–5895. https://doi.org/10.1007/s10462-021-09968-0.

[3]. Kunhoth, J., Subramanian, N., Al-Maadeed, S., & Bouridane, A. (2023). Video steganography: recent advances and challenges. Multimedia Tools and Applications, 82(27), 41943–41985. https://doi.org/10.1007/s11042-023-14844-w.

[4]. Lu, S.-P., Wang, R., Zhong, T., & Rosin, P. L. (n.d.). Large-capacity Image Steganography Based on Invertible Neural Networks.

[5]. Zhou, H., Zhang, W., Chen, K., Li, W., & Yu, N. (2022). Three-Dimensional Mesh Steganography and Steganalysis: A Review. In IEEE Transactions on Visualization and Computer Graphics (Vol. 28, Issue 12, pp. 5006–5025). IEEE Computer Society. https://doi.org/10.1109/TVCG.2021.3075136.

[6]. Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). Image Steganography: A Review of the Recent Advances. IEEE Access, 9, 23409–23423. https://doi.org/10.1109/ACCESS.2021.3053998.

 This work is licensed under a Creative Commons Attribution 4.0 International License