International Journal of Innovations & Research Analysis (IJIRA)
ISSN :2583-0295, Impact Factor: 5.449, Volume 03, No. 04(I), October- December, 2023, pp 09-12

A CRITICAL ASSESSMENT OF STEGANOGRAPHY TECHNIQUES FOR CONCEALING INFORMATION

Sreena G Nair[*]
Dr. Rohini K[**]

ABSTRACT

In this study, we delve into the realm of steganography, an influential technique employed to conceal information within various forms of media, such as images, audio, video, and text. Steganography offers a notable advantage by enabling the covert hiding of messages, thereby avoiding the potential scrutiny that encrypted messages might invite. By utilizing this technology, we ensure not only the safeguarding of message content but also the preservation of the anonymity of those engaged in communication. This makes steganography an invaluable tool for ensuring secure communication and discreet exchange of information. The study investigates the fundamental characteristics of steganography, encompassing its security aspects, capacity for data concealment, and ability to withstand adversarial attacks. Additionally, it emphasizes the practical implications of its usage in safeguarding data, facilitating secure communication, and ensuring secrecy, particularly within corporate, governmental, and law enforcement domains. The field of steganography is constantly progressing alongside technological advancements, adapting to novel obstacles and prospects in safeguarding the confidentiality and integrity of information within our globally interconnected society.

Keywords: *Steganography, Information Concealment, Secure Communication, Data Protection, Media Formats, Covert Messaging, Information Security.*

Introduction

The protection of information has been a significant priority in the field of information technology and communication since the emergence of the Internet. The field of cryptography arose as a mechanism for guaranteeing the secrecy of messages, resulting in the advancement of diverse techniques for encrypting and decrypting data in order to safeguard it from unauthorized access. Nevertheless, there exist circumstances in which the simple act of withholding the content of information is inadequate; it becomes imperative to also conceal the actual presence of that information. The technique of concealing information, commonly referred to as steganography, can be seen as the amalgamation of artistic and scientific principles in the realm of clandestine communication. This is accomplished by the process of embedding information into unrelated data, so effectively disguising the existence of the transmitted information. The etymology of the term "steganography" may be traced back to its Greek roots, specifically the combination of "stegos" which denotes "cover," and "grafia" which signifies "writing." Consequently, the name encapsulates the concept of concealing information through the practice of covert communication.

[*] Ph.D., Research Scholar (Part time), Department of Computer Science, Vels Institute of Science Technology and Advanced Studies (VISTAS), Pallavaram, Chennai, Tamil Nadu, India.

[**] Research Supervisor and Associate Professor of Computer Science, Vels Institute of Science Technology and Advanced Studies (VISTAS), Pallavaram, Chennai, Tamil Nadu, India.

The primary emphasis in the field of steganography is the concealment of information inside digital media. The discipline of steganography has undergone significant development and has become an intriguing and intricate area of research. Its main goal is to improve the durability of concealed data against a range of signal processing procedures that are applied to the host cover media, including images, audio files, and text. A steganography technique that is deemed effective should possess the capability to offer strong safeguarding for hidden data, so ensuring its resistance against various causes such as lossy compression, resizing, interception, tampering, or deletion. Additionally, it should also provide assurance that the data contained therein remains intact and can be retrieved successfully.

Review of Literature

In the year 2010, Jing-Ming Guo, an esteemed member of the Institute of Electrical and Electronics Engineers (IEEE), collaborated with Thanh-Nam Le to provide a scholarly article entitled "Secret Communication Utilizing JPEG Double Compression." This study explores the persistent endeavor to protect privacy while disseminating information across many media platforms. Historically, cryptography has served as the predominant means of safeguarding the privacy of communications shared between individuals sending and receiving messages. Nevertheless, within modern circumstances, the utilization of steganography methods has become increasingly prominent in conjunction with encryption, so offering a supplementary level of safeguarding for covert information. This study investigates the hypothesis that the quality factor of a JPEG image can be utilized as a potential medium for information embedding. The feasibility of including messages into a JPEG image through the manipulation of JPEG quantization tables (QTs) is discussed by the authors. By utilizing specific permutation algorithms in combination with this methodology, the technology can be utilized as a mechanism for covert communication. The efficacy of the proposed methodology in decoding data is evidenced by the utilization of a direct JPEG double compression approach, which consistently produces good outcomes.

In the year 2011, a paper titled "Data Hiding" was presented by Wei-Jen Wang, Cheng-Ta Huang, and Shiuh-Jeng Wang. The paper emphasizes the importance of data concealing as a critical strategy for augmenting the security of data and communication. The present approach entails the covert embedding of data into a media carrier, hence providing a reliable mechanism for disseminating information via publicly accessible communication channels. The present study primarily examines the concept of data hiding in vector quantization (VQ) based images. It specifically focuses on the intricate task of concealing sensitive information within a cover VQ-based image, with the aim of enabling covert communication and safeguarding data. This study undertakes a thorough examination and comparison of different data-hiding techniques specifically designed for vector quantization (VQ) based images. The approaches can be classified into four discrete categories according to their reversibility and output formats. The present study proceeds to offer comprehensive insights into several representative approaches, outlining their unique characteristics, and conducting a comparative analysis of their performance using parameters such as peak signal-to-noise ratio, secret data capacity, and bit rate. The findings of the study indicate that irreversible techniques, which generate stego-images as their output, has the capability to incorporate a greater amount of confidential information compared to reversible techniques. Furthermore, this phenomenon underscores the increasing prevalence of nonstandard encoding techniques, such as joint neighboring coding, within the field of reversible data concealment. These methods have gained traction due to their capability to augment the potential for embedding confidential information.

In the year 2012, a research article was given by Fangjun Huang, a member of the Institute of Electrical and Electronics Engineers (IEEE), Jiwu Huang, a senior member of IEEE, and Yun-Qing Shi, a fellow of IEEE. The paper introduced a new channel selection rule for steganography in the context of the Joint Photographic Experts Group (JPEG) format. This regulation functions as a mechanism for discerning discrete cosine transform (DCT) coefficients that result in little visible distortion during the concealment of data. The suggested regulation considers three essential variables: the perturbation error (PE), the quantization step (QS), and the amount of the quantized discrete cosine transform (DCT) coefficient intended for alteration (MQ). The experimental findings presented in the research illustrate that the implementation of this novel channel selection method has a substantial impact on enhancing security within the domain of JPEG steganography, resulting in higher performance outcomes.

The various classifications of steganography techniques

- **Image Steganography**

JPEG compression is a widely adopted technique for reducing an image's size while preserving its visual quality to the extent that it remains imperceptible to the human eye. In essence, it retains all the details in an image that are beyond human perceptibility, making their absence virtually unnoticed.

- **Audio Steganography**

Audio Steganography is the technology that involves embedding information within an audio channel. This method finds application in digital copyright protection. Watermarking, a related technique, conceals one piece of information (message) within another piece of information (carrier). It is commonly employed in various applications, including audio clips.

- **Video Steganography**

Video files are essentially compilations of images and audio, allowing many of the techniques employed in image and audio steganography to be adapted for use in video files. What makes video particularly advantageous is its capacity to conceal a substantial amount of data, given its dynamic stream of images and sounds. Consequently, any minor distortions or alterations that might be otherwise noticeable can often escape human detection due to the continuous flow of information.

- **Text Steganography**

One of the most challenging forms of steganography is text steganography, also known as linguistic steganography. This is due to the limited redundancy present in text compared to images or audio. Text steganography involves using natural language in written form to hide a secret message. The advantage of choosing text steganography over other mediums lies in its minimal memory usage and simplified communication.

Key Benefits

Steganography offers a distinct advantage over cryptography alone, as it ensures that messages remain inconspicuous. Clearly visible encrypted messages, no matter how secure they may be, can raise suspicions and could even be deemed incriminating in regions where encryption is prohibited. Consequently, while cryptography safeguards the content of a message, steganography can be seen as providing protection for both the messages themselves and the parties involved in communication.

This approach encompasses security, capacity, and robustness, three essential attributes of steganography that render it valuable for covert information exchange through textual documents and the establishment of clandestine communication.

Crucial files containing sensitive information can be stored on a server in an encrypted format. This ensures that no unauthorized intruder can glean any meaningful data from the original file during transmission.

Employing steganography, corporations, government entities, and law enforcement agencies can engage in covert and confidential communication.

Conclusion

In summary, steganography stands as a versatile and robust technique for concealing information within a variety of media formats, including images, audio, video, and text. Its key attribute lies in its ability to discreetly embed communications within everyday content, avoiding the attention that encrypted signals might typically attract. This dual safeguarding of message content and the anonymity of communicating parties makes it an invaluable tool in the realm of secure communication and information exchange. The significance of steganography is underscored by its capacity to offer security, data-carrying capability, and resilience, rendering it suitable for a wide range of applications, including covert communication and data protection. In situations where data confidentiality is of paramount importance, steganography proves to be an immensely valuable tool. It allows for the secure storage of sensitive information in encrypted formats on servers, effectively thwarting unauthorized access and reducing the risk of data exposure during transmission. Furthermore, steganography plays a critical role in enhancing the confidentiality and integrity of communication for various entities, including corporations, government agencies, and law enforcement bodies. This ensures the preservation of sensitive information in a secure and undisclosed manner. As technology continues to advance, the field of steganography evolves, presenting new challenges and opportunities for safeguarding information and facilitating secure interactions within an increasingly interconnected global context

References

1. Chung, Y. Y., & Xu, F. F. (2006). Development of video watermarking for MPEG2 video.
2. Craver, S., & Rezgui, A. (2003). A survey of software protection techniques and tools. Technical Report, Johns Hopkins University
3. Cummins, J., Diskin, P., Lau, S., & Parlett, R. (2011). Steganography and digital watermarking.
4. Fridrich, J. (2001). Steganography in digital media: Principles, algorithms, and applications. Cambridge University Press.
5. Fridrich, J., Goljan, M., & Du, R. (2001). Detecting LSB steganography in color, and gray-scale images. In Multimedia and Security Workshop (pp. 16-30).
6. Guo, J. M., & Le, T. N. (2011). Secret Communication Using JPEG Double Compression.
7. Johnson, N. F., &Jajodia, S. (1998). Exploring steganography: Seeing the unseen. IEEE Computer, 31(2), 26-34.
8. Liao, H. M., & Fan, K. (2012). Real-time MPEG2 video watermarking in the VLC domain.
9. Lu, C., Chen, J., & Fan, K. (2005). Real-time frame-dependent video watermarking in VLC domain.
10. Petitcolas, F. A., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding—a survey. Proceedings of the IEEE, 87(7), 1062-1078.
11. Shah, R., Agraval, A., & Ganesham, S. (2011). Frequency domain real-time digital image watermarking.
12. Shirali-Shahreza, M. (2006). A new method for real-time steganography.
13. Westfeld, A., & Pfitzmann, A. (1999). Attacks on steganographic systems: Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools. Lecture Notes in Computer Science, 1768, 61-75.

□❍□