Research Exhibition in Mathematics and Computer Sciences (REMACS 6.0)/
ISBN: 978-629-97440-5-4

IMAGE STEGANOGRAPHY WEB APPLICATION

Muhammad Nur Harith Shariffudin and Nor Arzami Othman
College of Computing, Informatics and Mathematic
Universiti Teknologi MARA Perlis Branch, Malaysia
harith.shariffudin@gmail.com and arzami@uitm.edu.my

ABSTRACT - This study for a final year project with the title Image Steganography Web Application presented in this abstract offers a user-friendly interface for securely embedding and extracting secret information within digital images. The application utilizes an advanced steganographic algorithm, which is Randomized Least Significant Bit (RLSB), to ensure robust data concealment while maintaining the visual integrity of the cover image. Users can upload their desired image, select the preferred steganographic algorithm, and encode the hidden data for added security. The web application supports encoding and decoding images for concealing data in images. To evaluate its performance, extensive testing was conducted, including embedding and extracting data using different image formats. The results demonstrated the application's effectiveness in hiding information while preserving image quality. The web application proved to be a versatile and practical tool with applications in various fields such as cryptography and digital forensics. In conclusion, the Image Steganography Web Application provides a convenient and secure solution for individuals and organizations needing to transmit sensitive data covertly within images, ensuring data privacy and integrity in an intuitive and user-friendly manner.

Keywords: Image Steganography, Web Application, RLSB (Randomized Least Significant Bit)

1. INTRODUCTION

Image steganography plays a crucial role in various real-life situations where secure communication is vital. For example, in the field of journalism, journalists may employ steganographic techniques to transmit sensitive information or evidence while protecting their sources. In the field of cybersecurity, steganography can be used to hide encryption keys or confidential data within images, making it harder for malicious actors to detect and intercept them. Additionally, law enforcement agencies can utilize steganography to embed watermarks or hidden identification markers in digital images for copyright protection or forensic purposes. Image steganography offers a powerful tool for covert communication and secure information exchange in a wide range of practical scenarios.

2. METHODOLOGY

The Image Steganography Web Application is developed using the Waterfall Model of the Software Development Life Cycle (SDLC). This model follows a sequential approach, starting with requirements gathering, followed by system design, development, testing, deployment, and maintenance. Each phase is completed before moving to the next, ensuring a structured and comprehensive development process for the web application. By adhering to the Waterfall Model, the application undergoes thorough planning, design, and testing to meet the specified requirements and ensure a successful and well-organized development journey.

3. RESULTS AND DISCUSSION

The Image Steganography Web Application was tested using the RLSB (Random Least Significant Bit) algorithm for embedding hidden data within cover images. The performance was evaluated based on metrics such as embedding capacity, visual quality, and robustness against detection. The results demonstrated that the RLSB algorithm effectively concealed data within the cover images while preserving visual quality. It provided a reasonable embedding capacity, allowing for a moderate amount of hidden data to be stored. The algorithm also exhibited good resistance against detection techniques, making it challenging for unauthorized users to detect the presence of hidden information.

4. NOVELTY OF RESEARCH / PRODUCT

In recent research, the focus of image steganography has shifted towards developing innovative methods that offer enhanced robustness against steganalysis and enable the concealment of larger amounts of data (Das et al., n.d.). Some noteworthy approaches that have been proposed include deep learning-based steganography, which utilizes deep learning techniques to embed secret data in images in a manner that is challenging to detect (Pevný & Fridrich, 2008). Spread spectrum steganography is another novel method that spreads the secret data across a wider range of pixels within the image, thereby increasing the difficulty of detection. Transform domain steganography, on the other hand, embeds the secret data in the transform domain of the image, further complicating its detection (Subramanian et al., 2021).

5. CONCLUSION

In conclusion, the Image Steganography Web Application offers a user-friendly interface for securely embedding and extracting hidden data within images. With advanced steganographic algorithms and options for concealing data, it ensures privacy and data integrity, making it a valuable tool for secure information transmission.

6. REFERENCES

Das, S., Das, S., Bandyopadhyay, B., & Sanyal, S. (n.d.). *Steganography and Steganalysis: Different Approaches*.

Pevný, T., & Fridrich, J. (2008). Novelty detection in blind steganalysis. *Proceedings of the 10th ACM Workshop on Multimedia and Security*, 167–176. https://doi.org/10.1145/1411328.1411357

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