Image Steganography: Concealing Information within Images

Deepti Deshmukh[1], Anshika Singh[2], Saurav Singh[3]
Mahatma Gandhi Mission's College Of Engineering & Technology, Noida,U.P.,India
[123]MGM COET, NOIDA, U.P., 201301, India

ABSTRACT

Image steganography, an age-old practice of concealing information within visual carriers, has evolved dramatically in the digital era. This research paper investigates the fundamental principles of image steganography, delves into advanced steganographic techniques, and examines the challenges and security concerns associated with this field.The findings emphasize the significance of image steganography security considerations such as detection vulnerabilities, data integrity, and payload size optimization. Looking ahead, the research points to continued advances in advanced steganographic techniques, the need for improved security in image steganography. It also emphasizes the importance of education and awareness in understanding image steganography's capabilities and limitations.This project report will provide an overview of image steganography, its applications, and techniques. It also tries to identify the requirements of a good steganography algorithm and briefly considers which steganographic techniques are better suited to which applications.This research paper also aims to add to the knowledge and understanding of image steganography and to serve as a resource for researchers, practitioners, and policymakers interested in the field's development and responsible application.

Keywords: Steganos, Least Significant Bit(LSB), Stego-key, Cryptography, Watermarking.

INTRODUCTION

Information is exchanged constantly in the modern digital age, whether it be for security, business, or personal reasons. The necessity to secure and transfer sensitive data has grown significantly with the rise in popularity of digital media and the internet. Steganography, the skill of hiding data on what appear to be innocent carrier media, has become a potent method for accomplishing this goal.

The Greek words "steganos," which means covered or concealed, and "graphie," which means writing or drawing, are the source of the word "steganography." In the field of information security, steganography occupies a unique position. Unlike traditional encryption methods, which draw attention simply by existing, steganographic techniques allow for covert communication by embedding sensitive data within digital artifacts such as images, audio files, or text documents. The carrier medium appears unchanged to the casual observer as a result of this concealment.

Image steganography is a particularly interesting and relevant domain within the broader field of steganography. Images are common in today's digital landscape, and they make an excellent cover for information concealment. It is possible to introduce hidden data into an image by changing the least significant bits (LSBs) of pixel values without affecting the image's visual quality.

This research paper explores into the fascinating topic of image steganography, exploring various techniques, methodologies, and applications. The paper will look at the history of steganography, the state of image steganography today, and its practical implications in the digital age. In addition, the paper will examine the challenges and security concerns associated with image steganography and propose future research directions. Image steganography is a testament to the ongoing fight for privacy, security, and the covert exchange of information in a digital world.

The following sections of this paper will go over image steganography techniques, advanced methods, security concerns, practical applications in detail. This comprehensive investigation will reveal a deeper understanding of the variations and significance of image steganography.

LITERATURE SURVEY

Section	Author	Publishing Year	Notes
1. Image Steganography in Spatial Domain: Current Status, Techniques, and Trends	Adeeb M. Alhomoud	2021	Explores image steganography, categorizing techniques into spatial and transform domains. Spatial methods like LSB substitution offer simplicity but are easily detectable, while transform methods provide defense against attacks but are computationally complex.
2. An image steganography approach based on k-least significant bits (k-LSB)	Omar Elharrouss, Noor Almaadeed, Somaya Al-Maadeed	2020	Introduces an image steganography approach using k-LSB to hide one image within another, addressing noise and resolution issues. Covers evaluation using PSNR metric and results of image quality enhancement.
3. Latest Trends in Deep Learning Techniques for image steganography	Vijay Kumar, Sahil Sharma, Chandan Kumar, Aditya Kumar Sahu	2023	Discusses the integration of deep learning into steganography, highlighting methods like supervised learning with CNNs and GANs. Examines challenges and critiques, ensuring a balanced approach.
4. An Extensive Survey of Digital Image Steganography: State of the Art	MA Idakwo, MB Muazu, EA Adedokun, BO Sadiq	2020	Explores the need for securing information through steganography, discussing challenges and recent achievements. Evaluates steganographic techniques in spatial, transform, and adaptive domains using various metrics, emphasizing trade-offs.

PROBLEM DEFINITION

Steganography can be considered to safeguard both messages and the parties involved. This approach included security, capacity, and robustness, the three necessary components of steganography that make it useful in the hidden flow of data via text files and secret communication. Some critical files containing secret data can be stored on the server in encrypted form, and no intruder can obtain any useful information from the original file during transmission.

Government and law enforcement agencies can communicate privately by using Steganography Corporation. The primary goal of steganography is to connect privately in an entirely unnoticeable manner and to avoid causing confusion in the transfer of secret information. It is not to prevent others from understanding the secret data, but rather to prevent them from believing that it exists at all. If a steganography technique causes someone to mistrust the carrier medium, the method will fail.

OBJECTIVES

Steganography's objective is to facilitate covert communication. As a result, a basic requirement of this steganography system is that the hider message transmitted by stego-media be inaccessible to humans.

The other purpose of steganography is to avoid raising suspicions about the existence of a secret message.

This information-hiding technology has recently gained popularity in a variety of applications.

This project aims to develop security tools using steganography techniques.

- Study data hiding techniques using the project's encryption module.
- Learn how to extract hidden data using the decryption module.

Steganography sometimes is used when encryption is not permitted. Or, more commonly, steganography is used to supplement encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen.

SOFTWARE & HARDWARE REQUIREMENTS:

1. Software Requirements

- JDK
- Apache Netbeans(OR any IDE)

2. Hardware Requirements

- i5 10th Generation
- 4Gb ram (minimum)

3. Supportive Operating System

- This program is coded in Java which is Platform independent, it can run in any operating system.

METHODOLOGY

Once the application has been launched. The user has two tabs: encrypt and decrypt. If the user selects encrypt, the application displays a screen with options to select an image file, information file, and save the image file. If the user picks decrypt, the application displays a screen allowing the user to select only the image file and specify the folder where the secret file will be saved. This project uses two methods: encrypt and decrypt.
Encryption hides secret information in any sort of image file.
Decryption is the process of extracting secret information from an image file.

SYSTEM ARCHITECTURE

An input image is used as the carrier for the hidden information at the beginning of the architecture. JPG, PNG, or BMP are just a few examples of common digital image formats that can include the input image. The pieces of information in the form of text that must be hidden within the picture are known as the secret data.

1.Embedding Process: This procedure involves embedding the encrypted data into the carrier picture. Usually, this procedure entails the following steps:

a. Pre-processing:

- If required, resize or normalize the input image to a certain size or format.
- Transform the secret data (such as text to binary representation) into a format that is appropriate for embedding.

b. Selecting the Embedding Method:

- Select the right embedding method according to the required degree of resilience, capacity, and security.
- LSB replacement, spread spectrum, and transform domain approaches are examples of common strategies.

c. Secret Data Embedding:

- Apply the selected embedding technique to hide the secret data within the carrier image.
- Modify specific pixels or frequency coefficients of the image according to the embedding algorithm.
- Ensure that the embedded data does not significantly alter the visual appearance of the image.

A steganography key may be used to enhance security and control access to the embedded information. The key is a secret parameter or password known only to the sender and receiver, enabling them to extract or decipher the hidden data.

2. Extraction Process: The stegano image's concealed information is recovered using the extraction method. This procedure is used by the image's recipient to get the hidden data. The following are the steps in the extraction process:

a. Initial processing:

- If required, resize and convert the format of the stego-image in order to prepare it for extraction.

b. Extraction Technique Selection:

- Choose the extraction technique that best fits the employed embedding approach.
- Verify that the method corresponds with the steganography key (if any).

c. Extraction of Secret Data:

- Utilize the selected extraction method to extract the stego-image's hidden data.
- Reconstruct the original secret data by extracting the modified pixels or frequency coefficients.

The recovered secret data is what the image steganography technology produces.

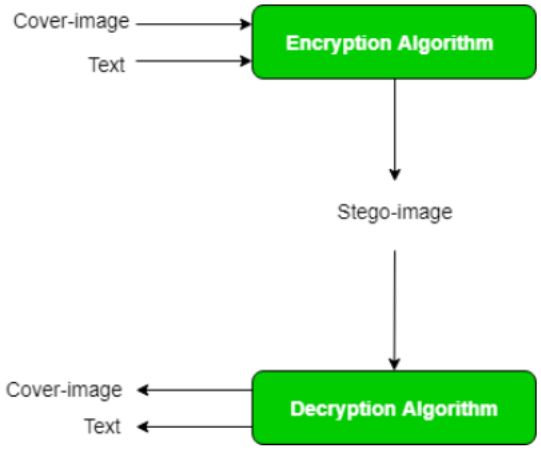

Fig: System Architecture of Image Steganography

APPLICATIONS

Image steganography has a wide range of practical applications due to its ability to conceal information within digital images. These applications use steganography's covert nature to achieve specific goals, such as protecting intellectual property or ensuring the integrity of medical images. In this section, we will look at some of the most important applications of image steganography.

- **Digital Watermarking**

Digital watermarking is a well-known example of image steganography. It entails incorporating ownership or copyright information into digital images. Photographers, artists, and content creators frequently use watermarks to protect their intellectual property. This type of image steganography allows the original creator to be identified and discourages unauthorized use or distribution of copyrighted materials.

- **Digital Forensics**

Image steganography is critical in the field of digital forensics for uncovering hidden information within images that may be relevant to criminal investigations. Investigators use steganalysis techniques to detect and extract hidden data from images, such as hidden messages or

encrypted content. This application assists law enforcement agencies in the investigation and prosecution of cybercrime.

- **Covert Communication**

Steganography is frequently used for covert communication in applications where confidentiality is critical. Image steganography can be used by intelligence agencies, military organizations, and security agencies to exchange classified information discreetly. Steganography can make covert communication difficult to detect, making it a valuable tool for espionage and national security.

- **Secure Data Transmission**

Image steganography can be used to improve data transmission security over public or unsecured networks. Organizations can protect their data from interception or eavesdropping by embedding sensitive information within images. The application is useful in areas like secure messaging, email communication, and online privacy.

- **Medical Imaging**

The healthcare industry can benefit from medical image steganography. Medical records and diagnostic images of patients frequently contain sensitive information that must be kept secure. Steganography can be used to embed patient data within medical images, keeping the data private and accurate. This application helps to protect patient privacy and the accuracy of medical records.

- **Copyright Protection**

Image steganography, in addition to digital watermarking, can be used to protect the copyrights of visual content. To discourage unauthorized use in the digital age, where images are easily shared and reproduced, content creators can embed copyright information within their work. This application is important for intellectual property protection in the creative and media industries.

- **Secure Messaging and Cryptography**

To improve the security of messaging and communication, steganography can be combined with cryptographic techniques. Individuals and organizations can create a dual-layered security approach by combining encryption and steganographic methods. This ensures that the hidden content remains private even if a message is intercepted.

- **Privacy-Preserving Social Media Sharing**

Individuals may want to share personal or sensitive images on social media while maintaining their privacy. Image steganography can be used to conceal personal information within photographs, protecting the privacy of the people in the photographs. This application is especially useful in the context of online social networks.

These applications demonstrate the versatility and significance of image steganography in a variety of domains. While it offers practical solutions for data security and secure communication, it also emphasizes the importance of responsible and ethical use. Image steganography's incorporation into these applications improved data security, privacy, and copyright protection, making it a valuable tool in today's digital landscape.

CONCLUSION

In conclusion, this research paper has provided a comprehensive exploration of image steganography, its historical roots, advanced techniques, and the associated challenges and security concerns. The study emphasizes the critical considerations in image steganography, including detection vulnerabilities, data integrity, and payload size optimization. As we navigate the digital landscape, the findings underscore the need for heightened security measures and continued advancements in steganographic techniques. The paper also highlights the practical applications of image steganography across diverse domains, from digital forensics to privacy-preserving social media sharing. In the evolving landscape of information security, this research contributes to the understanding of image steganography and encourages responsible and ethical applications of this powerful concealment tool.

REFERENCES

[1] Alhomoud, A. (2021). Image Steganography in spatial Domain: current status, techniques, and trends. *Intelligent Automation and Soft Computing*, *27*(1), 69–88. https://doi.org/10.32604/iasc.2021.014773

[2] Elharrouss, O., Almaadeed, N., & Al‐Maadeed, S. (2020). An image steganography approach based on k-least significant bits (k-LSB). *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*. https://doi.org/10.1109/iciot48696.2020.9089566

[3] Kumar, V., Sharma, S., Kumar, C., & Sahu, A. K. (2023). Latest Trends in Deep learning techniques for Image Steganography. *International Journal of Digital Crime and Forensics (Print)*, *15*(1), 1–14. https://doi.org/10.4018/ijdcf.318666

[4] Idakwo, M. A., Mu'azu, M. B., Adedokun, E. A., & Sadiq, B. O. (2020). An extensive survey of digital image steganography: State of the art. *ATBU Journal of Science, Technology and Education*,*8*(2),40–54.http://www.atbuftejoste.com/index.php/joste/article/download/972/pdf_638

[5] T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005.

[6] H. Shi, X.-Y. Zhang, S. Wang, G. Fu and J. Tang, "Synchronized detection and recovery of steganographic messages with adversarial learning", *Proc. Int. Conf. Comput. Sci.*

[7] Silman, J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001

[8] Neil F. Johnson and Sushil Jajodia, "Steganalysis of Images Created using Current Steganography Software/' in Proceedings of 2nd International Workshop on Information Hiding, April 1998, Portland, Oregon, USA.