

SECURE DATA TRANSFER OVER INTERNET USING IMAGE STEGANOGRAPHY.

Problem Statement:

The exchange of information over the Internet raises significant concerns about the security and privacy of sensitive data. While encryption is a powerful tool for protecting sensitive information by rendering it unreadable, it can also inadvertently signal to attackers that valuable data is being transmitted. This awareness can lead to targeted attacks, making the data vulnerable. As a result, new methods of secure communication have emerged, among which steganography has gained increasing attention [1].

Steganography, derived from the Greek word meaning “covered writing,” refers to the technique of hiding messages within other non-secret data, such as images, audio files, or video files. The primary goal of steganography is to conceal the existence of the information rather than just protecting it from unauthorized access. This distinction makes steganography different from encryption, which focuses solely on transforming data into an unreadable form. By embedding data within a transmission medium, steganography provides an additional layer of security, rendering the hidden message invisible to potential attackers [2].

Historically, the concept of steganography dates back centuries, such as the use of invisible ink, or tattooed messages hidden under hair [3]. Steganography in digital media: principles, algorithms, and applications. In the digital age and technological advancement, steganography has also evolved significantly, using complex algorithms and digital media to hide information. One of the most common methods is to use digital images as a carrier medium. This is due to the duplicate information present in images, where pixel values can be slightly altered to store hidden data without noticeable changes in the image quality [4].

Specifically, steganography involves embedding data within the pixel values of an image by manipulating the least significant bits (LSB) of the pixel data. Small amounts of information can be encoded into an image without being visibly altered, making the human eye unable to detect such subtle changes, which has made this method highly effective for covert communications. Furthermore, by combining steganography with encryption techniques, even if the hidden message is discovered, it will remain unreadable without the decryption key, further enhancing security[5].

Using information steganography technology to securely transmit data over the Internet addresses modern cybersecurity challenges by providing an effective way to protect sensitive data. This research focuses on implementing image steganography as a means of secure data transmission, with the aim of enhancing confidentiality and protecting data from eavesdropping during transmission over the Internet.

In this research, we will implement LSB technology to embed data within images to develop an information steganography system during transmission over the Internet. This report will demonstrate how to securely transmit sensitive information over the Internet while keeping it hidden from potential eavesdroppers. In addition, we will discuss the integration of encryption and steganography together to further secure the embedded message, providing a comprehensive solution for secure data transmission.

Research Objectives

The primary aim of this research is to develop a secure and efficient method for covert data transmission over the internet using image steganography. The research seeks to leverage the redundancy in digital images to conceal sensitive data, ensuring that the existence of the hidden message remains undetected while maintaining the quality of the image. By integrating encryption techniques with steganography, the research aims to provide a dual-layer security mechanism that protects both the content and the existence of the message during transmission

- To implement an algorithm that hides data inside digital images using the least significant bit (LSB) method.
- To incorporate encryption techniques such as (asynchronous encryption) to secure the hidden data before embedding it in the image. This ensures that the data will remain secure even if the data is discovered, and the data cannot be discovered.
- To maintain the integrity of the visual image after embedding the hidden data so as not to raise any suspicions among attackers that there is confidential data in the image.
- To implement a reliable extraction algorithm that retrieves the embedded message from the image without changing the data.
- To design a simple and intuitive user interface that allows users to upload images and enter the message to be hidden.

1. Computational Complexity vs. Simple Solutions

Approaches that advocate simple encryption, as in the Nunna and Krishna study, may conflict with those that require more computationally intensive techniques, such as the discrete wavelet transform (DWT). While simple solutions aim for efficiency, they may not provide the same level of security as heavier algorithms, creating a conflict in application suitability.

References

- [1] D. Watermarking, S. Katzenbeisser, and F. A. P Petitcolas, *Recent Titles in the Artech House Computer Security Series Rolf Oppliger, Series Editor Information Hiding Techniques for Security Technologies for the World Wide Web, Rolf Oppliger*, 1st ed., no. 112. Artech House, 2015. [Online]. Available: <http://www.ifi.unizh.ch/~oppliger/serieseditor.html>.
- [2] N. Jhonson, Z. Duric, and S. Jajodia, *Information Hiding Steganography and Watermarking : Attacks and Countermeasures, Advanced in Information Security*. New York: Springer Science-Business Media, 2001. doi: 10.1007/978-1-4615-4375-6.
- [3] J. Fridrich, *Steganography in digital media: Principles, algorithms, and applications*, vol. 9780521190. Cambridge university press, 2012. doi: 10.1017/CBO9781139192903.
- [4] M. M. Taher, A. R. B. H. J. Ahmad, R. S. Hameed, and S. S. Mokri, “a Literature Review of Various Steganography Methods,” *J. Theor. Appl. Inf. Technol.*, vol. 100, no. 5, pp. 1412–1427, 2022.
- [5] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, “Image Steganography: A Review of the Recent Advances,” *IEEE Access*, vol. 9, pp. 23409–23423, 2021, doi: 10.1109/ACCESS.2021.3053998.