A Minor Project Synopsis on

**Image Steganography**

Submitted to Manipal University, Jaipur

Towards the partial fulfillment for the Award of the Degree of

**BACHELORS OF TECHNOLOGY**

In Computer and Communication Engineering

2020-2024

By

Dhruv Chaudhary

209303197

LSS Jyotiraditya

209303292



Under the guidance of

Dr. Vijay Kumar Sharma

**Department of Computer and Communication Engineering**

**Manipal University Jaipur**

**Jaipur, Rajasthan**

**Introduction**

Image steganography is a technique that has gained significant attention in recent years as a means of securing communication channels. It involves the hiding of secret messages or data within an image without causing any noticeable changes to the image's quality. The use of steganography has become increasingly popular due to the increasing need for secure communication channels in various fields such as military, finance, and healthcare. This technique has led to the development of various algorithms and methods for hiding information within an image. As a result, it has become a crucial tool in maintaining privacy and security in this digital age.

In this project, we aim to explore the implementation of image steganography through Python and evaluate their performance. Our goal is to evaluate the strengths and limitations of different steganographic techniques and decide on and propose a novel method that offers better performance.

The significance of this study lies in its potential to enhance the security of communication channels by enabling the transmission of sensitive information without raising any suspicion. The results of this study can be used to inform the development of more efficient and robust steganographic methods that can be applied in various fields.

**Motivation**

There are several motivations for learning and implementing image steganography. One of the primary motivations is to maintain the privacy and security of sensitive information. With the rise of digital communication channels, it has become more critical than ever to ensure that confidential data remains private and is not intercepted by unauthorized parties. Image steganography provides an effective way to secure data transmission by hiding sensitive information within images. Attackers can steal sensitive information or manipulate data to cause harm, which can be devastating for individuals, businesses, and even governments. By implementing steganographic techniques, we can increase the resilience of digital communication channels and make it more challenging for attackers to intercept and exploit sensitive information.

Moreover, image steganography is a fascinating and challenging area of study, particularly for those interested in information security, data hiding, and cryptography. It involves the application of complex algorithms and techniques to conceal information within an image in a way that is imperceptible to the human eye. The study of steganography requires a deep understanding of image processing, data hiding, and encryption, making it an ideal area of study for those interested in computer science and related fields.

In conclusion, the motivations to learn and implement image steganography are numerous. It provides an effective way to maintain the privacy and security of sensitive information, combat cyber threats, and is a fascinating and challenging area of study. With the increasing need for secure communication channels, the demand for steganographic techniques is expected to continue to grow, making it an essential skill for those interested in information security and related fields.

**Statement of Problem**

The increasing use of digital images for communication and storage has led to a growing demand for secure ways to transmit confidential information without detection. Existing steganography techniques offer some level of protection, but they have limitations in terms of security, capacity, and quality. The challenge is to implement different image steganography systems that can effectively and securely hide information within an image while maintaining the image quality and resisting attacks. This project aims to address this challenge by exploring and improving existing steganography methods and deciding on the best approach that meets the requirements of confidentiality, robustness, and efficiency in image transmission for specific applications.

|  |  |  |
| --- | --- | --- |
| EXISTING METHODS | PROS | CONS |
| Least Significant Bit | Easy to implement, high hiding capacity | Vulnerable to attacks, noticeable reduction in image quality |
| Phase Coding | Difficult to detect, high hiding capacity | Computationally intensive, vulnerable to attacks |
| Spread Spectrum | Robust, high hiding capacity | Computationally intensive, noticeable reduction in image quality |
| Distortion-Based | Difficult to detect, high hiding capacity, small changes made | Noticeable reduction in image quality, vulnerable to attacks |

**Methodology/Planning of work**

Here are some general steps that could be followed to achieve the objective of an image steganography project:

* Research and Review Existing Techniques: Conduct a thorough review of existing image steganography techniques, including their strengths and weaknesses, to identify gaps and opportunities for improvement.
* Define Requirements: Define the specific requirements of the project, such as the parameters as well as the software and hardware requirements needed to implement the project.
* Implement the System: Implement the different image steganography system by writing code, configuring software, and testing the system to ensure that it meets the requirements.
* Test and Evaluate the System: Conduct comprehensive testing to evaluate the performance, security, and efficiency of the implemented system. Test the system under various conditions to identify any weaknesses or vulnerabilities.
* Improve the System: Based on the results of testing, identify areas for improvement and implement enhancements to the system.
* Document the Project: Document the design, implementation, and testing process, as well as any findings and recommendations, to create a comprehensive record of the project.

**Facilities required for proposed work**

Here are some general hardware and software requirements that may be needed. These might vary with time as the project development begins:

**Hardware Requirements:**

* A computer or server with sufficient processing power and memory to run the steganography software and process images quickly
* Sufficient storage space to store the image files and any intermediate results
* A high-quality monitor or display to view and analyze the images

**Software Requirements:**

* A programming language, such as Python or Java, to write the steganography software
* A steganography library or module, such as Stegano, OpenStego, or steghide, to provide the steganography functionality
* An image processing library, such as Pillow or OpenCV, to handle the image input/output, processing, and analysis
* An encryption library, such as OpenSSL or PyCrypto, to provide additional security and confidentiality of the hidden data
* A code editor or integrated development environment (IDE), such as Visual Studio Code or PyCharm, to write and debug the software

**Bibliography/References**

* <https://www.geeksforgeeks.org/image-steganography-in-cryptography/>
* <https://www.javatpoint.com/image-steganography>
* <https://www.mygreatlearning.com/blog/image-steganography-explained/>
* <https://www.cscjournals.org/manuscript/Journals/IJCSS/Volume6/Issue3/IJCSS-670.pdf>
* <https://techvidvan.com/tutorials/python-image-steganography/>