**PROJECT REPORT**

**on**

**IMAGE STEGANOGRAPHY**

**(CSE III Semester Mini project)**

**2023-2024**



**Submitted to:**  **Submitted by:**

Dr Susheela Himanshu Negi

(CC-CSE-F2-III-Sem) Roll. No:2218853

**Guided by:** CSE-F2-III-Sem

Mr. AKASH RAWAT Session: 2023-2024

**DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY**

**GRAPHIC ERA HILL UNVERSITY, DEHRADUN**

**CERTIFICATE**

### Certified that Mr. Himanshu Negi (Roll No.- 2218853) has developed mini project on “Image steganography” for the CS III Semester Mini Project Lab in Graphic Era Hill University, Dehradun. The project carried out by Students is their own work as best of my knowledge.

Date: Oct 2023-Dec 2023

Dr Susheela

**Class Co-ordinator**

**CSE-F2-III-Sem**

(CSE Department)

GEHU Dehradun.

**ACKNOWLEDGMENT**

We would like to express our gratitude to The Almighty Hare Krishn, the most Beneficent and the most Merciful, for completion of project.

We wish to thank our parents for their continuing support and encouragement. We also wish to thank them for providing us with the opportunity to reach this far in our studies.

We would like to thank particularly our project Co-ordinator Dr Susheela and our Project Guide Mr. Akash Rawat for his patience, support and encouragement throughout the completion of this project and having faith in us.

At last, but not the least We greatly indebted to all other persons who directly or indirectly helped us during this work.

**Mr Himanshu Negi**

**Roll No.- 2218853**

**CSE-F2-III-Sem**

**Session: 2023-2024**

**GEHU, Dehradun**

## **TABLE OF CONTENTS**

1. **Introduction**
2. **Methodology**

**2.1 Image Selection**

**2.2 Python Libraries**

**2.3 Steganographic Techniques**

**2.3.1 LSB Substitution**

**2.3.2Frequency Domain Techniques**

## **3. Implementation**

### **3.1 LSB Substitution**

### **3.2 Frequency Domain Techniques**

## **4. Results**

## **5. Conclusion**

**6. Future Work**

## **7. Acknowledgments**

## **8.References**

## **Abstract**

Steganography is the art and science of hiding information within other non-secret data to prevent detection. In the digital age, image steganography has become an essential technique for secure communication. This report explores the implementation of image steganography using Python, focusing on embedding and extracting hidden messages within digital images.

## **1. Introduction**

Steganography plays a crucial role in information security by concealing the existence of communication. Unlike cryptography, which focuses on securing the content of a message, steganography is concerned with hiding the message itself. In this report, we delve into the realm of image steganography and demonstrate how Python can be utilized for this purpose.

## **2. Methodology**

### **2.1 Image Selection**

For this project, we selected various digital images in different formats (JPEG, PNG, etc.) to assess the flexibility of the steganographic technique across multiple file types.

### **2.2 Python Libraries**

The implementation of image steganography is facilitated by the use of Python libraries. We employed the popular **PIL** (Python Imaging Library) for image manipulation and **numpy** for efficient numerical operations.

### **2.3 Steganographic Techniques**

Two main techniques were explored:

#### 2.3.1 LSB Substitution

The Least Significant Bit (LSB) substitution involves replacing the least significant bit of each pixel's color channel with the bits of the hidden message. This method is simple but effective for concealing information without perceptible changes to the image.

#### 2.3.2 Frequency Domain Techniques

Frequency domain steganography involves manipulating the frequency components of an image. We utilized the Discrete Cosine Transform (DCT) to embed and extract information in the frequency domain.

## **3. Implementation**

### **3.1 LSB Substitution**

The LSB substitution involved the following steps:

* Convert the message to binary.
* Iterate through each pixel of the image.
* Replace the least significant bit of each color channel with the corresponding bit from the binary message.

### **3.2 Frequency Domain Techniques**

The frequency domain techniques included:

* Convert the image to the frequency domain using DCT.
* Embed the message in the frequency coefficients.
* Reverse the DCT to obtain the steganographic image.

## **4. Results**

The implemented techniques were successful in hiding messages within the images. The LSB substitution method demonstrated good concealment with minimal visual distortion. Frequency domain techniques, while more complex, provided higher security with a lower likelihood of detection.

## **5. Conclusion**

Image steganography using Python proved to be a viable method for secure communication. The choice between LSB substitution and frequency domain techniques depends on the desired level of security and the permissible distortion in the image.

## **6. Future Work**

Future work could involve optimizing the algorithms for better performance, exploring advanced steganographic techniques, and developing tools for real-world applications. Additionally, research could focus on the robustness of these methods against various attacks.

## **7. Acknowledgments**

We acknowledge the contributions of the open-source community, particularly the developers of the **PIL** and **NumPy** libraries, which significantly facilitated the implementation of image steganography in Python.

## **8.References**

* Python Imaging Library (**PIL**)
* [**NumPy**](https://numpy.org/)
* Anderson, R. (1998). Information hiding in digital signals. Proceedings of the IEEE, 86(4), 673-679.
* <https://networksimulationtools.com/steganography-network-security-projects/>