Image Steganography

A

Minor Project (CC3270)

Report

Submitted in the partial fulfillment of the requirement for the award of

Bachelor of Technology

in

Computer and Communication Engineering

By:

Dhruv Chaudhary
209303197
LSS Jyotiraditya
209303292

Under the guidance of:

Dr. Vijay Kumar Sharma

Jan 2023 - May 2023

Department of Computer and Communication Engineering
School of Computer and Communication Engineering
Manipal University Jaipur
VPO. Dehmi Kalan, Jaipur, Rajasthan, India – 303007

Department of Computer and Communication Engineering
School of Computer and Communication Engineering, Manipal University Jaipur,
Dehmi Kalan, Jaipur, Rajasthan, India- 303007

STUDENT DECLARATION

*I hereby declare that this project (**Image Steganography**) is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which has been accepted for the award of any other degree or diploma of the University or other Institute, except where due acknowledgements has been made in the text.*

Place: Jaipur, Rajasthan
Date: 20/04/2023

Dhruv Chaudhary
(209303197)
B.Tech (CCE) 6th Semester

Department of Computer and Communication Engineering

School of Computing and Communication Engineering, Manipal University Jaipur,
Dehmi Kalan, Jaipur, Rajasthan, India- 303007

Date: 20/04/2023

CERTIFICATE FROM GUIDE

*This is to certify that the work entitled "**Image Steganography"** submitted by **Dhruv Chaudhary** (209303197) to **Manipal University Jaipur** for the award of the degree of **Bachelor of Technology** in **Computer and Communication Engineering** is a bonafide record of the work carried out by him under my supervision and guidance from January 2023 to May 2023*

Dr. Vijay Kumar Sharma
Department of Computer and Communication Engineering
Manipal University Jaipur

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to all those who have contributed to the successful completion of my minor project.

First and foremost, I would like to thank my project guide Dr. Vijay Kumar Sharma, who has been a constant source of inspiration and guidance throughout this project. She provided valuable feedback, suggestions, and insights that helped me immensely in achieving my project goals.

I would also like to thank the faculty members of Computer and Communication Engineering for providing me with the necessary resources and support for my project. Their encouragement and guidance were essential in shaping my project ideas and refining my research work.

I am grateful to my friends and family members for their constant encouragement and support during the course of my project work. Their emotional support and motivation have been instrumental in helping me complete my project.

Finally, I would like to extend my gratitude to all the participants who took part in my project and provided valuable feedback that helped me improve my work.

Thank you all for your support and encouragement.

Dhruv Chaudhary

LSS Jyotiraditya

ABSTRACT

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.

The significance of this project 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.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

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.

Image steganography is a technique of hiding secret information inside an image, without altering its visual quality. Various image steganography techniques have been developed to achieve this objective, and their performance varies in terms of the level of security and the amount of information that can be hidden. In this research article, we present a comprehensive performance analysis of various image steganography techniques, including Least Significant Bit (LSB), Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) essentially providing us with the analysis of Spatial Domain technique vs Transform Domain technique. The performance analysis metrics such as Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE) are discussed in the survey paper we made for this project.

We also analyze the trade-offs between security, capacity, and computational complexity for each of these techniques. Through these comparisons and research, we have devised specific use cases for the 3 algorithms we have discussed to see which one is best used where.

Problem Statement

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

Table 1: Existing Methods in Image Steganography

Methodology

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.

Working

In this project we will to two domains of image steganography techniques used: Spatial Domain techniques (LSB method) and Transform Domain Techniques (DWT/DCT methods)

Visual Representation of Image Steganography:

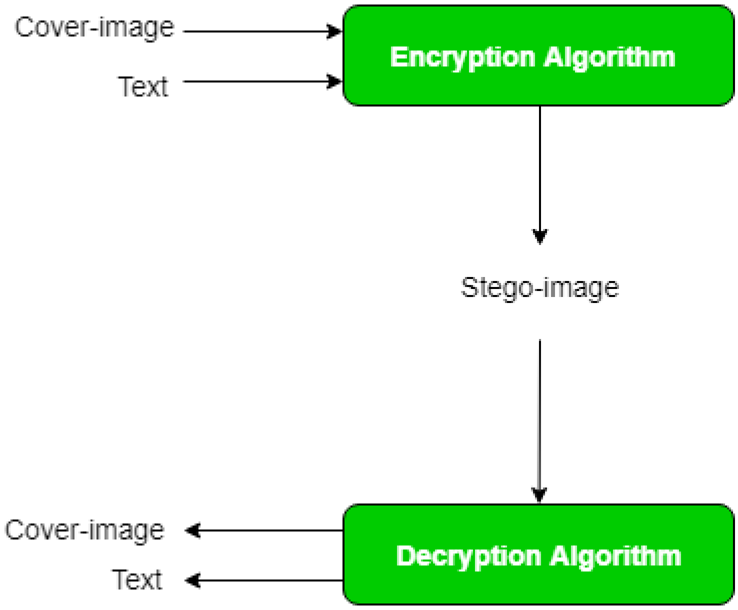
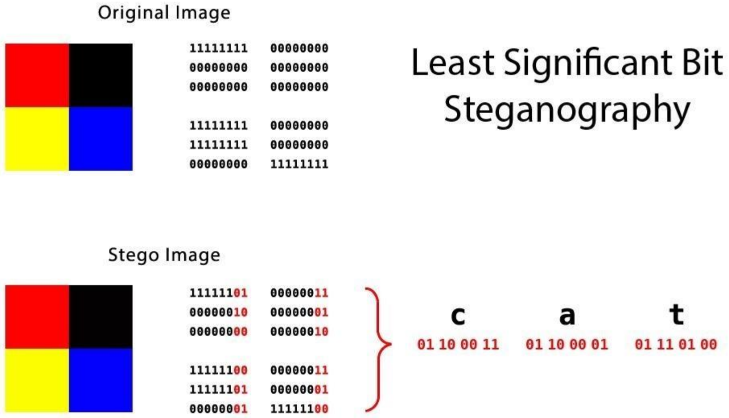


Figure 1

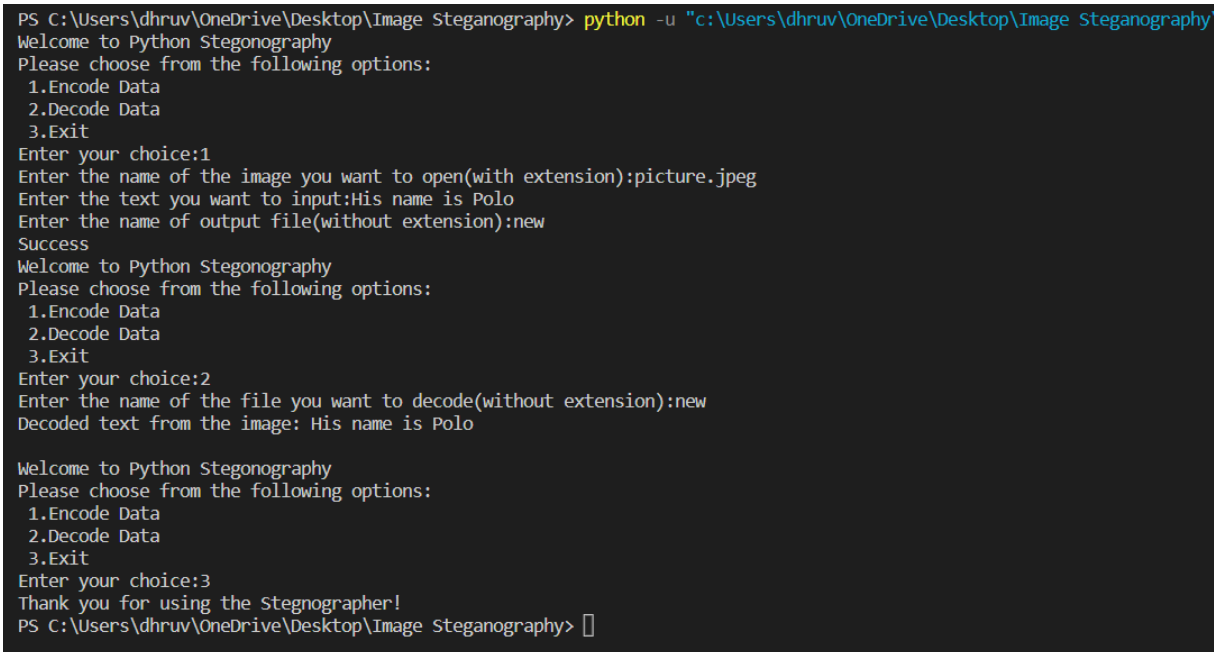
Working of least significant bit method (LSB) for image steganography:

- This technique changes the last few bits in a byte to encode a message, which is especially useful in something like an image, where the red, green, and blue values of each pixel are represented by eight bits (one byte) ranging from 0 to 255 in decimal or 00000000 to 11111111 in binary.
- Changing the last two bits in a completely red pixel from 11111111 to 11111101 only changes the red value from 255 to 253, which to the naked eye creates a nearly imperceptible change in color but still allows us to encode data inside of the picture.
- The least significant bit technique works well for media files, where slightly changing byte values creates only slight imperceptible changes, but not so well for things like ASCII text, where a single bit out of place will completely change the character. That's not to mention the fact that data hidden using LSB steganography is also easy to detect if someone is looking for it.

Visual Representation of LSB Method (Figure 2):



Code Implementation of LSB Method:



```
PS C:\Users\dhruv\OneDrive\Desktop\Image Steganography> python -u "c:\Users\dhruv\OneDrive\Desktop\Image Steganography
Welcome to Python Stegonography
Please choose from the following options:
 1.Encode Data
 2.Decode Data
 3.Exit
Enter your choice:1
Enter the name of the image you want to open(with extension):picture.jpeg
Enter the text you want to input:His name is Polo
Enter the name of output file(without extension):new
Success
Welcome to Python Stegonography
Please choose from the following options:
 1.Encode Data
 2.Decode Data
 3.Exit
Enter your choice:2
Enter the name of the file you want to decode(without extension):new
Decoded text from the image: His name is Polo

Welcome to Python Stegonography
Please choose from the following options:
 1.Encode Data
 2.Decode Data
 3.Exit
Enter your choice:3
Thank you for using the Stegnographer!
PS C:\Users\dhruv\OneDrive\Desktop\Image Steganography> 
```

Figure 3

DCT:

- The Fourier transform was originally used on heat conduction but later gain usage in various applications and became a base for other transformation like DCT. Images and videos compression algorithm uses DCT to transform into frequency domain and data compression is done through quantization. Image is divided into parts or sub-bands.
- The Discrete Cosine Transform (DCT) is a mathematical technique used to analyze signals such as images, videos, and audio. In image processing, the DCT is applied to a block of pixels in an image to transform it into the frequency domain. The resulting coefficients represent the frequency components of the image in a way that enables compression and other signal processing operations. The DCT is widely used in image and video compression algorithms such as JPEG and MPEG

DCT Image Steganography Flow:

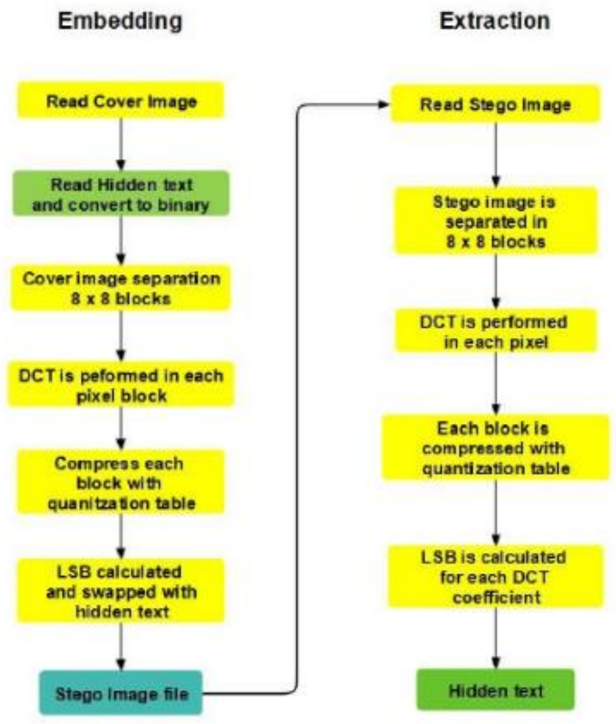

Embedding
Read Cover Image
Read Hidden text and convert to binary
Cover image separation 8 x 8 blocks
DCT is pefomed in each pixel block
Compress each block with quanitzation table
LSB calculated and swapped with hidden text
Stego Image file
Extraction
Read Stego Image
Stego image is separated in 8 x 8 blocks
DCT is performed in each pixel
Each block is compressed with quantization table
LSB is calculated for each DCT coefficient
Hidden text

Figure 4

Algorithm of Image Steganography for text message embedding in DCT:

1. First Cover Image is read
2. Hidden message is read
3. Binary conversion of hidden message.
4. Cover Image is separated into 8x8 pixel blocks.
5. For each Pixel block DCT is performed.
6. Quantization table is used to compress each block.
7. LSB is calculated of each DCT coefficients and swapped with the hidden message.
8. Stego image is produced.

Algorithm of Image steganography for text message extraction in DCT:

1. First Stego image is read
2. Then next, through 8x8 block of pixels stego image is separated.
3. Then in each Pixel block DCT is performed.
4. Now after this step, quantization table is used to compress each block.
5. For each DC coefficient LSB is computed.
6. Convert each bits into character and retrieve the hidden message.

DWT:

- DWT is a way to transform from spatial to frequency domain. DWT is used in JPEG 2000 compression which is very popular. Wavelets are basically functions that integrate to zero waving below and above the x axis.

- For Signal and image processing, wavelets are used as the basic function like sines and cosines in Fourier transform

DWT Image Steganography Flow

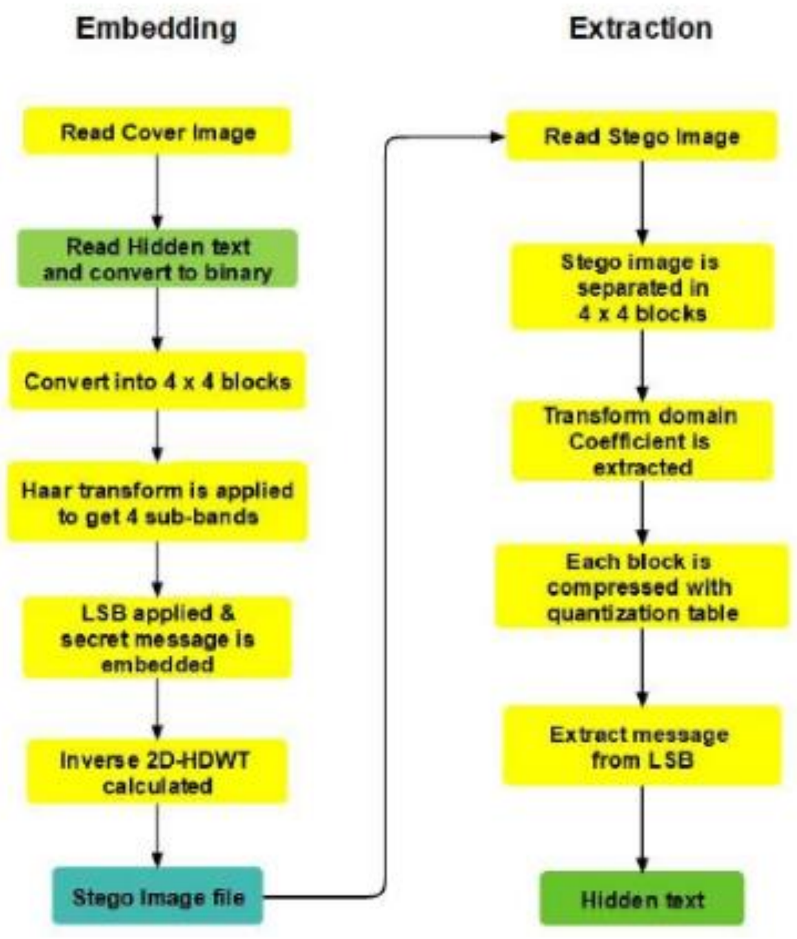

Embedding
Read Cover Image
Read Hidden text and convert to binary
Convert into 4 x 4 blocks
Haar transform is applied to get 4 sub-bands
LSB applied & secret message is embedded
Inverse 2D-HDWT calculated
Stego Image file
Extraction
Read Stego Image
Stego image is separated in 4 x 4 blocks
Transform domain Coefficient is extracted
Each block is compressed with quantization table
Extract message from LSB
Hidden text

Figure 5

Algorithm of Image steganography for text message embedding in DWT:

1. Cover Image is read.

2. The hidden message is read

3. Binary conversion of hidden message.

4. Convert the cover image into 4 x 4 blocks.

5. 2D-Haar transform is applied to get 4 sub-bands LL, HL, LH & HH.

6. LSB of each sub-band is changed and secret hidden message is embedded into it.

7. Inverse 2D-HDWT (Haar Discrete Wavelet Transform) is calculated for each 4 x 4 block.

8. Stego image is produced.

Algorithm of Image steganography for text message extraction in DWT:

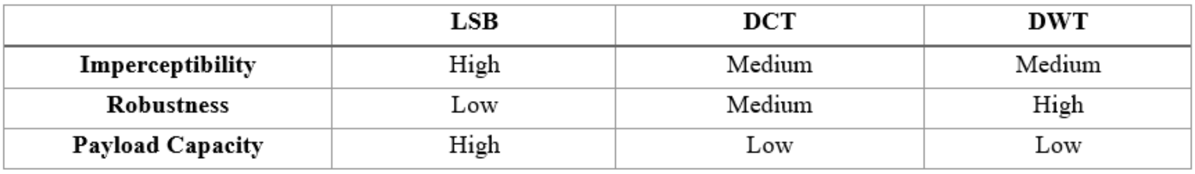
1. The Stego image is read.
2. Stego image is divided into 4 x 4 blocks
3. Transform domain coefficient is extracted by using 2D Haar Discrete Wavelet Transform (HDWT) for each block.
4. Extract message from LSB in each pixel
5. Hidden message is extracted

Qualitative analysis parameters:

- Parameters such as imperceptibility, capacity, and robustness are evaluated.
- (a) Imperceptibility: It refers the stego file quality post embedding the secret text. This is a significant factor in steganography wherein if the stego file doesn't retain its quality, it can be suspected to have hidden information.
- (b) Capacity: It refers to the size of the secret message that can be embedded in the carrier or cover file.
- (c) Robustness: It refers to withstand manipulation of the stego file such that the embedded secret information can be retrieved after various attacks like scaling, cropping, compression, rotation, blurring, noise adding, filtering and re-mastering.

Results

Qualitative Analysis/comparison table



	LSB	DCT	DWT
Imperceptibility	High	Medium	Medium
Robustness	Low	Medium	High
Payload Capacity	High	Low	Low

Table 2

Use Case (LSB):

- Possible Use Case: Digital Watermarking for Copyright Protection
- Justification: LSB has good imperceptibility, which means that it can embed data in an image without causing noticeable changes to the image. In the case of digital watermarking, the watermark is usually a small piece of data, such as a logo or a copyright notice. LSB is capable of embedding this data in a way that is not noticeable to the human eye. Additionally, LSB has high payload capacity, which means that it can embed a large amount of data in an image. This is useful in cases where multiple watermarks need to be embedded in the same image or where the watermark needs to be resistant to attacks that attempt to remove or alter the watermark.

Use Case (DCT):

- Use Case: Medical Imaging for Patient Information Embedding
- Justification: DCT has moderate imperceptibility, which means that it can embed data in an image without causing noticeable changes to the image in some parts of the image, but in some cases, it can be noticeable in certain parts of the image. In the case of medical imaging, patient information needs to be embedded in a way that is not noticeable and does not interfere with the diagnosis or interpretation of the image. DCT is capable of embedding this data in the frequency domain, which is less perceptible to the human eye. Additionally, DCT has good robustness, which means that the embedded data can survive image compression or other manipulations that might occur during the transmission or storage of the image.

Use Case (DWT):

- Use Case: Military and Intelligence Applications for Secure Data Transmission
- Justification: DWT has good imperceptibility and high robustness, which makes it suitable for applications where high security is required. In the case of military and intelligence applications, the data that needs to be transmitted or stored is sensitive and needs to be protected from unauthorized access. DWT is capable of embedding data in an image in a way that is not detectable and is resistant to attacks that might attempt to remove or alter the embedded data. Additionally, DWT has high payload capacity, which means that it can embed a large amount of data in an image, making it suitable for applications where a large amount of data needs to be transmitted or stored securely.

USE CASE (Texting App):

- For a simple implementation of adding an image steganography feature in a text messaging app, the LSB technique would be suitable.
- The LSB technique is the simplest and most widely used image steganography technique. It involves modifying the least significant bit of each pixel in an image to embed the secret data. This technique is relatively easy to implement and has low computational complexity, making it suitable for applications with limited resources.
- In the case of a text messaging app, users may want to embed a small amount of data, such as a short message or a small image, in the cover image. The LSB technique has high payload capacity and can embed a relatively large amount of data in the image, making it suitable for this type of application.
- Additionally, the LSB technique has good imperceptibility, which means that the modified image is visually similar to the original image, making it difficult for an attacker to detect the presence of the embedded data.
- Overall, for a simple implementation of adding an image steganography feature in a text messaging app, the LSB technique is a good choice because it is easy to implement, has high payload capacity, and good imperceptibility.

Challenges

During the course of this minor project, several challenges were encountered that posed significant hurdles in the pursuit of the research objectives. These challenges can be broadly classified into four categories, as discussed below:

1. Time Duration for Research: Researching all aspects of all the domains of image steganography and all the methods for each of these domains required a lot of time duration (more than expected) and literature review for this task was extensive.

2. Code Implementation: While LSB Code Implementation was not the toughest piece of work, it turned out so that implementation of Transform Domain techniques was out of our scope due to its very computationally extensive requirements. Nonetheless, we found appropriate results through research and survey.

3. Numerical Analysis: While it is arguably possible to implement and calculate numerical analysis for image steganography despite being a mere team of 2 with laptop computers as resource, time duration played a role in not being able to do thorough numerical analysis of all the methods considered in this project.

Considering these challenges, a number of strategies were employed to mitigate their impact, including the use AI resources, referring with guide mentor, seniors and fellow classmates. Despite these efforts, the challenges encountered during this project underscore the need for continued research and development in the field of data science and machine learning.

Future Prospects

- Implement a GUI Application for a steganography GIF feature to be implemented in a texting social application
- Implement a new unique method of image steganography by tweaking existing methods such as LSB or by creating a working combination of two existing techniques combing the pros of both

Individual Contribution

- Both team members made a significant contribution to the project and its completion in ideation if not grunt work as well
- Research was mainly spear-headed by me. I, under the guidance of my mentor, provided direction to my partner who then further assisted in the research portion
- Code implementation of LSB method was handled by me
- Writing of survey paper was done by me but research was done by both
- Synopsis was written by my partner
- End term Report compilation was done mainly by me but with a helping hand provided by my partner
- Making the PPT for End Term presentation was my contribution

Bibliography and 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/

[1] Sharma, V.K., Srivastava, D.K. and Mathur, P. (2018), Efficient image steganography using graph signal processing. IET Image Processing, 12: 1065-1071. https://doi.org/10.1049/iet-ipr.2017.0965

[2] Khalili M., and Asatryan D.: 'Colour spaces effects on improved discrete wavelet transform-based digital image watermarking using Arnold transform map', *IET Signal Process.*, 2013, **7**, pp. 177–187

[3] Prabakaran G., and Bhavani R.: 'A modified secure digital image steganography based on discrete wavelet transform'. Int. Conf. Computing, Electronics and Electrical Technologies, March 2012, pp. 1096–1100

[4] Ms. Shubhangi Hiwe, Prof. S. I. Nipanikar, 2014, An Analysis of Image Steganography Methods, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 03, Issue 02 (February 2014),

[5] Hamid, Nagham, et al. "Image steganography techniques: an overview." *International Journal of Computer Science and Security (IJCSS)* 6.3 (2012): 168-187.

[6] Hussain, Mehdi, 2013, A Survey of Image Steganography Techniques. *International Journal of Advanced Science and Technology. (2013):* 113-125