Tribhuvan University
Institute of Science and Technology

Central Department of Computer Science and Information Technology
Kirtipur, Kathmandu

In the partial fulfilment of MSc.CSIT Second Semester Seminar

"Information Hiding using Steganography"

Submitted by
Rishav Acharya
611/077

August, 2022

Tribhuvan University
Institute of Science and Technology

Supervisor Recommendation

This is to certify that Mr. Rishav Acharya (Roll no. 611/077) has submitted the seminar report on the topic **"Information Hiding using Steganography"** for the partial fulfilment of Master's of Science in Computer Science and Information Technology, second semester. I hereby, declare that this seminar report has been approved.

_____

Supervisor
Asst. Prof. Jagdish Bhatta
Central Department of Computer Science and Information Technology

Letter of Approval

This is to certify that the seminar report prepared by Mr. Rishav Acharya entitled **"Information Hiding using Steganography"** in partial fulfilment of the requirements for the degree of Master's of Science in Computer Science and Information Technology has been well studied. In our opinion, it is satisfactory in the scope and quality as a project for the required degree.

Evaluation Committee

……..…….. ……..……

Asst. Prof. Sarbin Sayami
(H.O.D)
Central Department of Computer Science
and Information Technology

Asst. Prof. Jagdish Bhatta
(Supervisor)
Central Department of Computer Science
and Information Technology

……

(Internal)

Acknowledgement

The success and final outcome of this report required a lot of guidance and assistance from many people and I am very fortunate to have got this all along the completion. I am very glad to express my deepest sense of gratitude and sincere thanks to my highly respected and esteemed supervisor **Asst. Prof. Jagdish Bhatta,** Central Department of Computer Science and Information Technology for his valuable supervision, guidance, encouragement, and support for completing this paper.

I am also thankful to **Asst. Prof. Sarbin Sayami**, HOD of Central Department of Computer Science and Information Technology for his constant support throughout the period. Furthermore, with immense pleasure, I submit by deepest gratitude to the Central Department of Computer Science and Information Technology, Tribhuvan University, and all the faculty members of CDCSIT for providing the platform to explore the knowledge of interest. At the end I would like to express my sincere thanks to all my friends and others who helped me directly or indirectly.

Rishav Acharya (611/077)

Abstract

Image steganography is the method used in transmitting secret information by hiding it in plain sight inside a cover image. The secret information is hidden in a way that it not visible to the human eyes.

This main goal of this seminar report is to present how a message or information can be embedded into an image and how the embedded message or information can be extracted or decoded from that image.

Keywords: Image steganography, Data hiding, Security

Table of Contents

List of Figures

List of Abbreviations

CNN - Convolutional Neural Network

GAN - Generative Adversarial Network

Chapter 1: Introduction

1.1 Overview

Steganography is derived from two Greek words “Stegano” means sealed and “Graphy” refers to writing which means secret writing. Simply, these two words means “covered writing” or “sealed writing”. Steganography is very old method of embedding information into other data by using some rules and techniques. In today’s modern digital world, everyone is sharing their data and information using different modern data sharing techniques so the data security issue has become very essential for everyone.

In this seminar, a discussion is done about the method of hiding information within an image by using the rules and guidelines of steganography. The information which needs to be sent to receiver is encoded within an image and the image is shared to the receiver, then the receiver will decode the image to obtain the encoded information or message that has been sent from the sender.

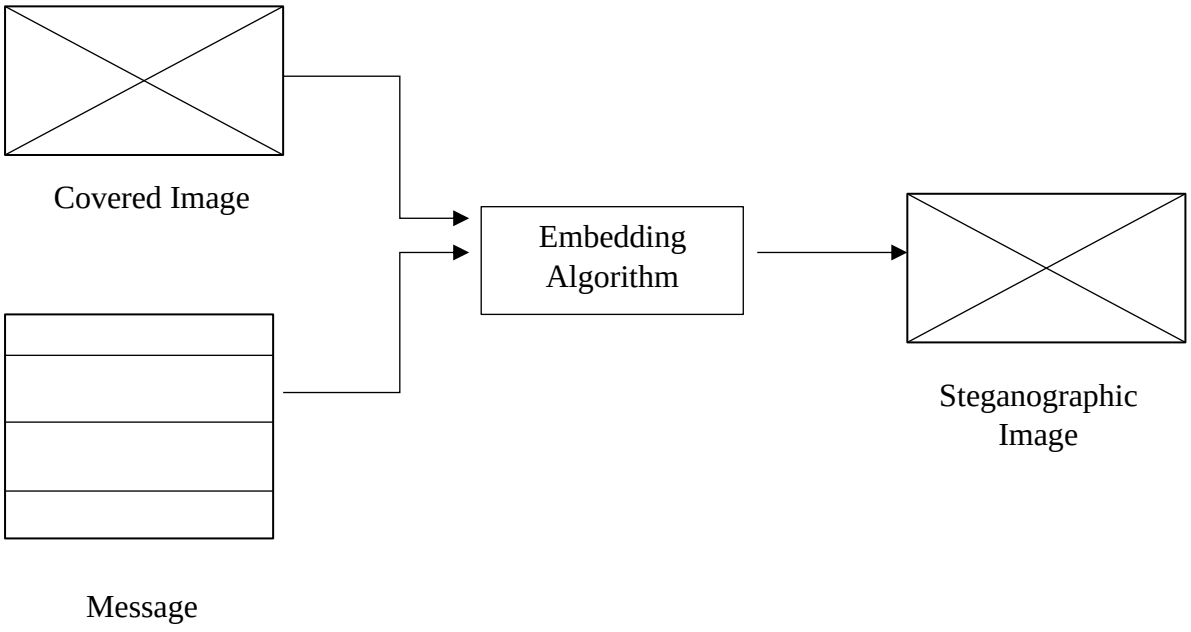

Figure 1: General Working principle of Steganography (Encoding)

In this encoding method, two inputs are taken .i.e., an image and message to encode and embedding algorithm is used to generate container image with will have the message encoded within it. The final image will be same as the image taken as the input.

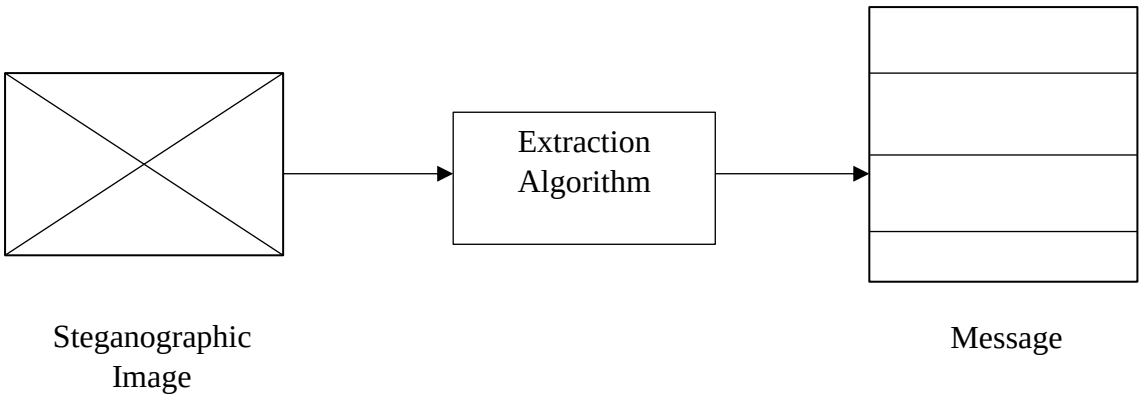

Figure 2: General Working principle of Steganography (Decoding)

In this decoding method, the encoded image is used as an input and with the extraction algorithm the encoded message is extracted by the receiver.

1.2 Some Important Definitions

Definition 1.2.1: Covered image is real image acting as a carrier for the hidden file.
Definition 1.2.2: Steganographic image is the embedded information inside the cover image.
Definition 1.2.3: Message is the information which is actually hidden into images, it can be a image or a point text.
Definition 1.2.4: Embedding algorithm is used for hiding the information inside the image.
Definition 1.2.5: Extraction algorithm is used for getting the information from steganographic image.

1.3 Problem Statement

The purpose of this seminar report is to present how an information can be transferred from sender to receiver in the form of image. In some cases, data might be lost during the transmission process in the network or the data might be changed by the unauthorized person. This report presents the encryption and decryption technique which can be used to secure the data and information during transmission using just an image.

1.4 Objectives

The main objective of this seminar is to present a technique that can be used as cryptographic scheme during data transmission.

Chapter 2: Literature Review

There is various research done on the cryptographic scheme. Steganography is also one of the methods used by many people and researchers in order to transfer messages.

Nandhini Subramanian and co. on their paper [1], has discussed about different method used in steganography such as image steganography, GAN steganography, and CNN steganography. The authors mainly discussed about different deep learning methods available in image steganography.

Christian Bach and Ramadhan J. Mstafa on their paper [2], has discussed about information hiding in images using steganographic techniques. The authors have used the steganographic and digital watermarking methods to hide information and mix the information with other information that makes attackers difficult to recognize.

Ritu Sindhu and co. in their paper [3], has discussed about data hiding using different steganographic technique such as, image steganography, video steganography, audio steganography, text steganography, and network steganography. The authors mainly focus to present steganography overview, its demand, advantages and the techniques used in it.

Mehdi Hussain and co. in their paper [4], has provided a survey report on image steganography. The authors have provided comprehensive survey to highlight the pros and cons of existing up-to-date techniques for researchers that are involved in designing of image steganographic system. They have discussed the general structure of steganographic system and classifications of image steganographic techniques.

Jia Liu and co. in their paper [5], has discussed about the advancement of image steganography with GAN steganographic technique. The authors in their paper have reviewed the art of steganography with GANs according to the different strategies in data hiding, which are cover modification, cover selection, and cover synthesis.

Chapter 3: Methodology

3.1 Image Steganography

In image steganography, the image contains the message or information that is being transferred. As in Figure 1: General Working principle of Steganography (Encoding), the term "cover image" is the image which is used to hide the message or information. The embedding algorithm is the procedure or algorithm that is used to hide message or information inside the cover image and then steganographic image is obtained. The steganographic image contains the message or information that is being shared within the image. To get the encoded message within the image, the extraction algorithm is used as in the Figure 2: General Working principle of Steganography (Decoding). Extraction algorithm is a technique or procedure to recover the message or information from the steganographic image.

In general, the steganographic method is evaluated by two methods; embedding capacity and the image quality after embedding. So, an ideal steganography method mainly focuses on the quality of steganographic image compared to cover image, which should be very identical to each other.

3.2 Embedding Algorithm

The embedding algorithm is a method or technique that is used to embed message or information into the cover image to make it into steganographic image. In this seminar report, a passive work is done in order to acquire the image steganography. The pixels of cover image are modified according to the 8-bit binary data. The modified pixels are embedded with the message or information, and then those modified pixels are again placed into the image forming cover image into steganographic image.

Algorithm

Step 1: Get an image to encode the message or information. (Cover Image)

Step 2: Modify the pixels of image according to 8-bit binary data.

Step 3: Encode the message to the pixels by extracting 3 pixels at a time.

Step 4: Put the modified pixels in the new image. (Steganographic Image)

Step 5: Save the new image into local directory.

3.3 Decoding Algorithm

The decoding algorithm is a method or technique that is used to extract embedded message or information from the steganographic image. The pixels are extracted by 3 pixels at a time and then the data is obtained by counter process to modified 8-bit binary data in steganographic image.

Algorithm

Step 1: Get an image to decode the message or information. (Steganographic Image)

Step 2: Get image data and extract the pixels by 3 pixels at a time.

Step 3: Obtain the encoded message or information by extracting modified 8-bit binary data.

Step 4: Display the decoded message or information.

Chapter 4: Implementation

The implementation include in this seminar report is carried out in python programming. The python library used for implementation process is briefly described below:

Pillow (PIL Fork): The Image module provides a class with the same name which is used to represent a PIL image. The module also provides a number of factory functions, including functions to load images from files, and to create new images.

- **image. open ():** This function identifies the file, but the file remains open and the actual image data is not read from the file until we try to process the data.
- **image. copy ():** This function copies the image as the original one.
- **image. size ():** This function gets the image size in pixels. The size is given as 2 -tuple width and height.
- **image. putpixel ():** This function modifies the pixels at given position.
- **image. save ():** This is function is used to save the image.

```
img = input("Enter image name(with extension) : ")
image = Image.open(img, 'r')


data = input("Enter data to be encoded : ")
if (len(data) == 0):
    raise ValueError('Data is empty')

newimg = image.copy()
encode_enc(newimg, data)

new_img_name = input("Enter the name of new image(with extension) : ")
newimg.save(new_img_name, str(new_img_name.split(".")[1].upper()))
```

Figure 3: Code Snippet

Chapter 5: Results and Finding

This seminar report demonstrates how message or information can be embedded into an image and extracted from the image. At first, an image is taken and message is given to the embedding algorithm. The embedding algorithm embeds the message into the given image by modifying the pixels of the image. The pixels of cover image are modified according to the 8-bit binary data. The modified pixels are embedded with the message or information, and then those modified pixels are again placed into the image forming cover image into steganographic image.

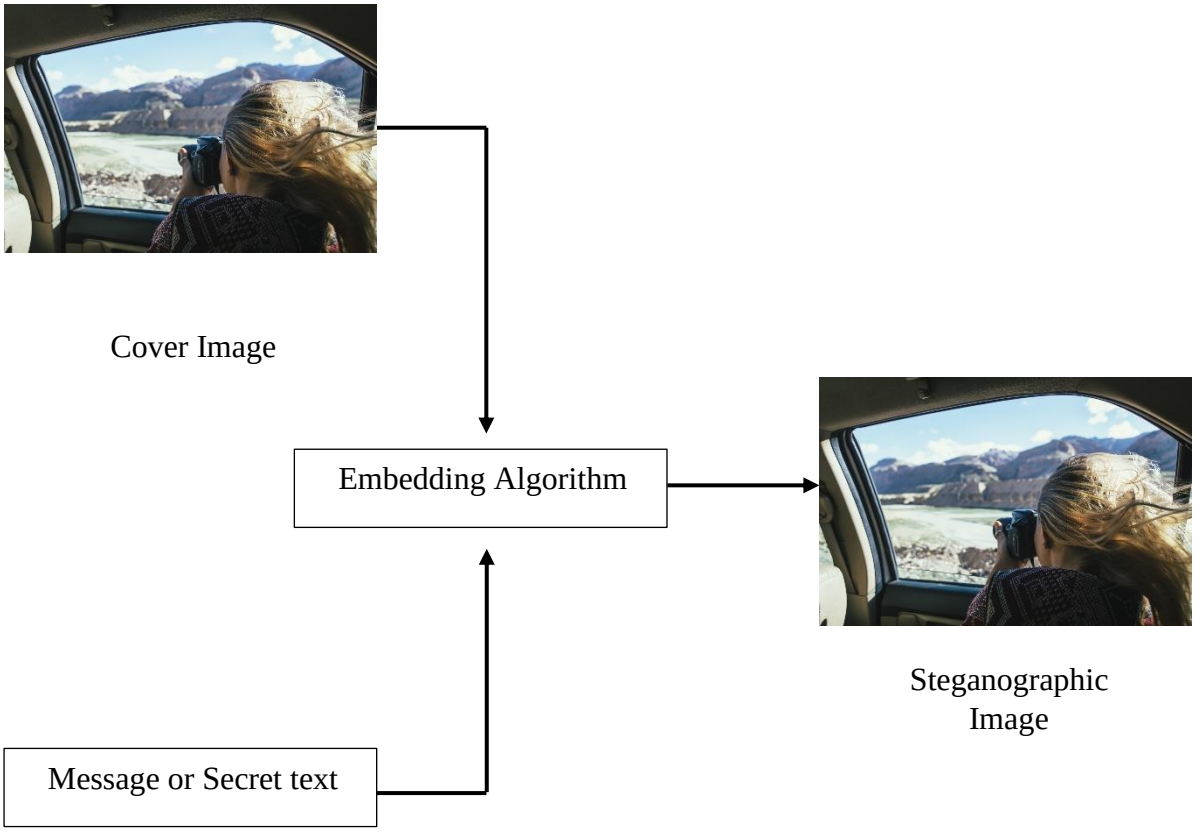

Figure 4: Embedding message to image

While extracting the message or information form steganographic image, counter embedding procedure is used. The decoding algorithm is a method or technique that is used to extract embedded message or information from the steganographic image. The pixels are extracted by 3 pixels at a time and then the data is obtained by counter process to modified 8-bit binary data in steganographic image.

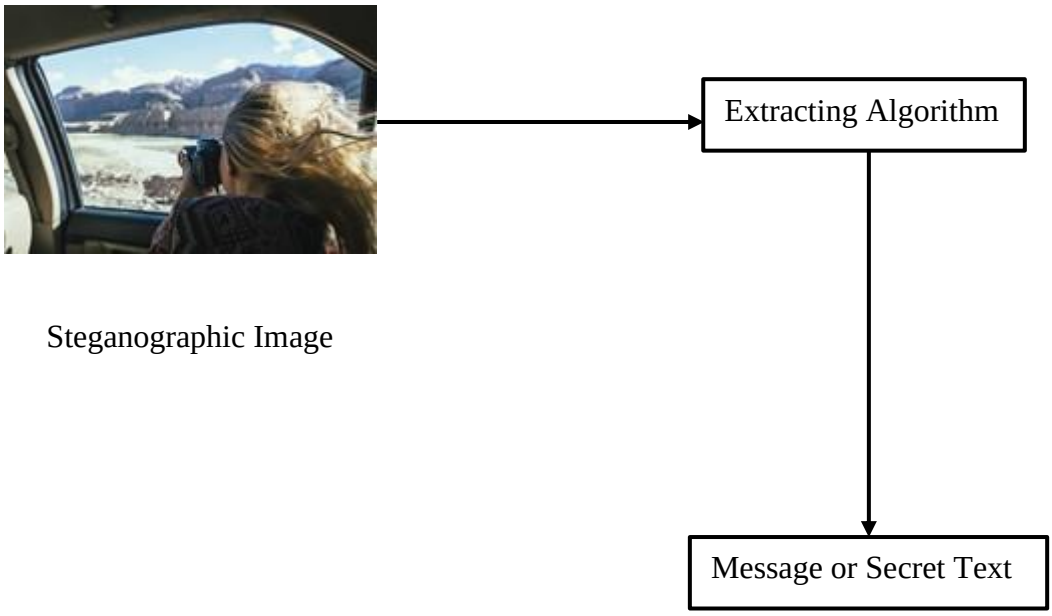

Figure 5: Extracting message from image

Chapter 6: Conclusion

Image steganography is the method used in transmitting secret information by hiding it in plain sight inside a cover image. The secret information is hidden in a way that it not visible to the human eyes. This seminar mainly presents how a message or information can be embedded into an image and how the embedded message or information can be extracted or decoded from that image.

References

[1] O. E. S. A.-M. a. A. B. N. Subramanian, "Image Steganography: A Review of the Recent Advances," *IEEE Access*, vol. 9, pp. 23409 - 23423, 2021.

[2] C. B. Ramadhan J. Mstafa, "Information Hiding in Images Using Steganography Techniques," *American Society for Engineering Education*, 2013.

[3] P. S. Ritu Sindhu, "Information Hiding using Steganography," *International Journal of Engineering and Advanced Technology (IJEAT*, vol. 9, no. 4, p. 2249 – 8958, 2020.

[4] A. W. Y. I. B. I. K.-H. J.-H. J. Mehdi Hussain, "Image steganography in spatial domain: A survey," *Signal Processing: Image Communication*, vol. 65, p. 10.1016/j.image.2018.03.012, 2018.

[5] Y. K. ,. Z. Z. ,. Y. L. J. L. M. Z. A. X. Y. JIA LIU, "Recent Advances of Image Steganography With Generative Adversarial Networks," *IEEE Access*, vol. 8, no. 10.1109/ACCESS.2020.2983175., pp. 60575-60597, 2020.