International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Image Based Steganography

Bheeshma Rao J[1], Ujwal Sai Satya Jorige[2], Sai Praneetha Katragadda[3], Pradeep Kumar .V[4]

[1]Department of Computer Science and Engineering, B V Raju Institute of Technology, Narsapur, Medak, Telangana, India
jbheeshmarao[at]gmail.com

[2]Department of Computer Science and Engineering, B V Raju Institute of Technology, Narsapur, Medak, Telangana, India
jorigeujwal16[at]gmail.com

[3]Department of Computer Science and Engineering, B V Raju Institute of Technology, Narsapur, Medak, Telangana, India
praneetha123katragadda[at]gmail.com

[4]Department of Computer Science and Engineering, B V Raju Institute of Technology, Narsapur, Medak, Telangana, India
pradeepkumar.v[at]bvrit.ac.in

Abstract: ***Steganography is a technique of hiding data in a way, such that no eavesdropper can identify the changes in original media. The methodology we proposed is Least Significant Bit Substitution to perform Steganalysis. The main idea of this technique is to directly alter LSB of the cover image with secret data. Various methods have been proposed in the literature which most of them are not capable of both preventing visual degradation and providing a large embedding capacity. With this method, it can be ensured that the embedding capacity of data can be large and also its resolution.***

Keywords: Steganography, Data Hiding, Least Significant Bit (LSB), Steganalysis

1. Introduction

a) Motivation

The immense growth in development of Web which can be referred as modern communication technology has become easier and faster. Through web, messages can be exchanged in a fast and cheap way in different areas like government workplaces, private sectors, military, and restorative regions. In most of the cases, confidentiality of the transferred messages has to be kept up. To guarantee that the message is exchanged safely and securely over the transfer, a suitable method is required. Steganography demonstrates as a trustable strategy for achieving this point. Steganography methods according to its use in various organizations to communicate between its members, as well as, it can be used for communication between members of the military or intelligence operatives or agents of companies to hide secret messages or in the field of espionage.

b) Problem Definition

Today, a lot of applications are Internet-based and their demand has led to the transfer of huge amounts of data. But public communication systems cannot be secure because of interception and manipulation of data by eavesdropping or piggybacking and many other techniques. Image Steganography is a framework where the information is safely transferred from one recipient to another using a cover file to hide the existence of secret information.

c) Objective

The security of the data being sent is our primary goal. As a result, we used steganography. To hide the hidden data, steganography uses a key and a medium called cover data. Its goal is to conceal the sender, recipient, and secret data content, leaving the secret data accessible only to the receiver. The word steganography comes from two Greek words: stego, which means hidden, and grafia, which means writing. Steganography is a technique for transferring secret data encased in cover material across a public communication channel like the Internet. An attacker cannot retrieve the secret data from the cover data using this strategy. There are mainly three important parameters for evaluating a secret data communication technique namely capacity, robustness and transparency.

d) Limitations

Undetectability of the message is one of the main criteria. That is with encryption, receiver is sure that they received a secret encrypted data; but with hidden data, they need to know that the information is concealed using a cover file. It gets tough in compressed files where most of the embedded data may be lost.

It is not possible to send large files of data with steganography; if someone knows that a message is there then it can be easily read.

2. Literature Survey

a) Introduction

Steganography is defined as a science or art of hiding the message inside some cover medium. The concept of steganography is not new; its usage can be seen from the past. From history, records depict that around 440 BC, Herodotus sent secret messages using the concept of steganography. In ancient times, Greeks also wrote messages on wood and covered them with wax. The concept of invisible ink was also used during the period of World War II. According to Greek history, secret messages were written on the bald scalp of the slaves, and after the growth of hair on their heads, they were sent as messengers.

b) Existing System

Pure Steganography is the existing system. It is the process of embedding the data into objects using various private keys. It is defined as a steganographic system which does

not require the exchange of a cipher such as stego-key. This method is not much secure because the sender and receiver can rely only upon the assumption that no other parties are aware of the secret message.

c) Disadvantages of Existing System

Few drawbacks associated with the existing system are as follows:

- It is not safe and secure for the data to be transmitted using this technique.
- The process of embedding the data is too slow.
- Stego Image Resolution is not up to the mark and it is not feasible.
- It does not come up with 100% insertion of data into the pixel.

d) Proposed System

The system we propose is called LSB, which stands for Least Significant Bit substitution.

- Least Significant Bit (LSB) replacement is the process of changing the carrier image's least significant bit pixels.
- It's a straightforward method of incorporating a message into an image.
- The number of bits in an image determines the Least Significant Bit insertion.
- In an 8-bit image, the least significant bit, or the 8th bit of each byte, is replaced with a secret message bit.
- The colors of each component, such as RGB (red, green, and blue), are modified for a 24-bit image.
- LSB works well with BMP images because BMP compression is lossless.

e) Abbreviations & Acronyms

Few abbreviations associated are as follows

- RGB-Red, Green, Blue colors
- LSB-Least Significant Bit
- BMP-Bit Map Image
- IQM-Image Quality Measure
- PI-Pixel Indicator

3. Analysis

a) Introduction

The user has to select the path of the image into which he or she wants to store the embedded message. Then the message must be entered that is hidden in the image displaying the image as it is which is difficult to examine that there is a message hidden in it.

b) Software Requirement Specification

Software Requirements

- Python 3.8.1
- Windows 10
- IDE/Jupiter Notebook

Hardware Requirements

- Processor –Intel Hexa-Core-i7-9750H CPU[at]2.60Hz (64-bit OS).
- Memory – 16GB RAM (Higher specs are recommended for high performance)

c) RAM: 4GB or greater

- Architecture Diagram

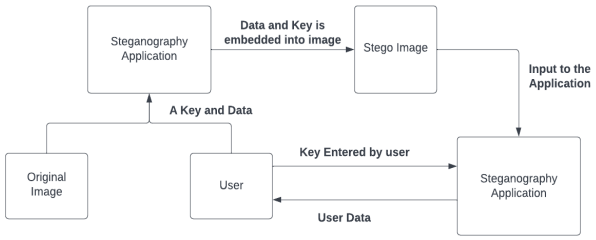

Figure 1: Architecture Diagram

The diagram displayed above is the architecture diagram of the project. Here a user embeds an image into a steganography application. The 6 data and key are used to form a stego image which is not understood by any kind of hacker.

d) Flow Charts

When a user interacts with the steganography application, he/she needs to understand two different processes. They are encoding and decoding.

Encoding

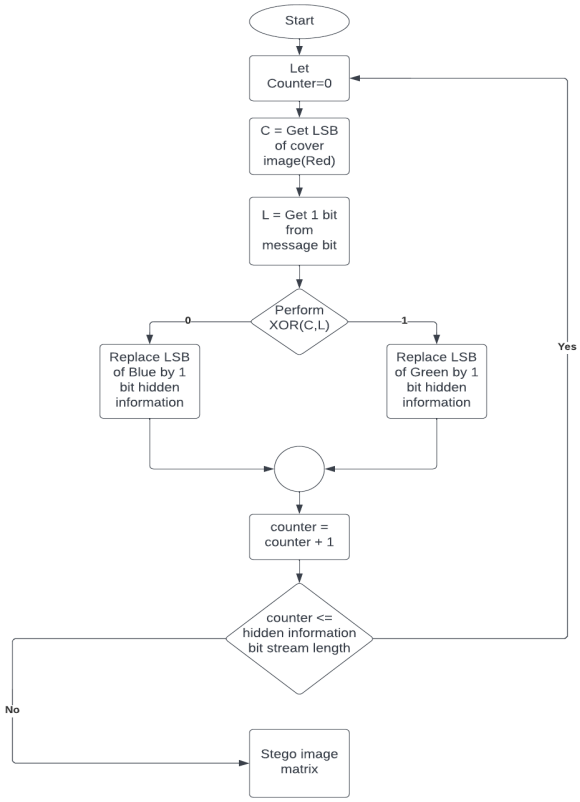

Figure 2: Flow Chart to hide information

The above flow chart is used to understand the process of encoding i. e., to hide the information and convert it into a stego image i. e., a cover image.

Decoding

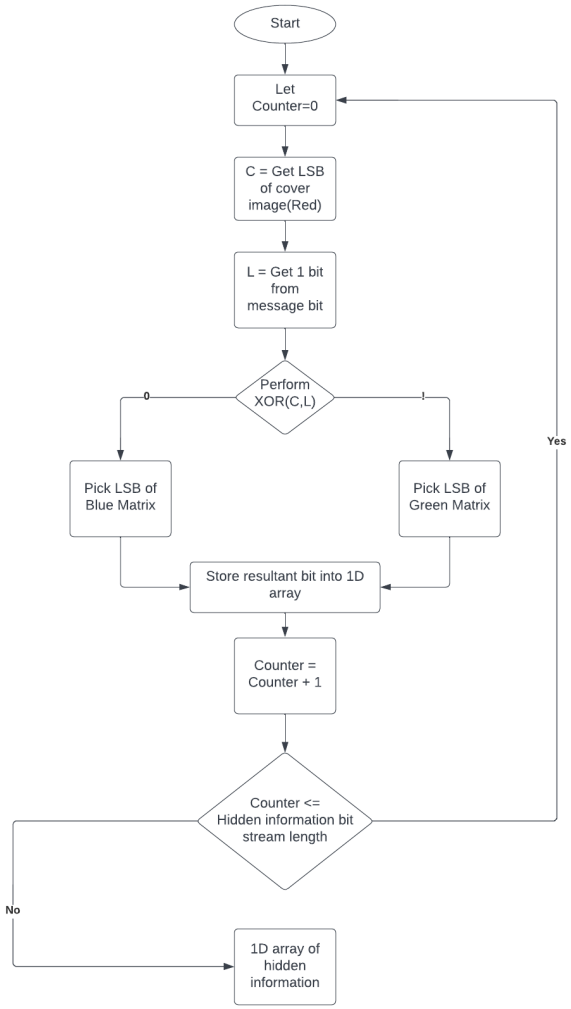

Figure 3: Flow chart to recover hidden information

The above flow chart is used to understand the process of decoding i.e. to recover the hidden information from the stego image.

Design

The attributes mainly involved are

1) Message file and
2) Image

a) Data Flow Diagram

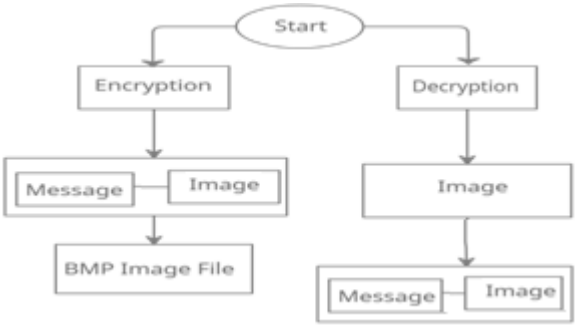

Figure 4: Data Flow Diagram

b) Module Design & Organisation

As displayed above in the data flow diagram we have mainly two modules which are encryption and decryption otherwise called as encoding and decoding processes/functions.

Module 1: Encryption: It is the process used to hide the information and form a stego image.

Module 2: Decryption: It is the process to recover the original message from stego image.

4. Implementation

Key Functions

The most important functions in our project are:

1) encode (): Here the message is encoded and stego image is formed.
2) decode (): Here the message is recovered from the stego image.

Testing

Let us consider an example to understand the functions of encoding and decoding.

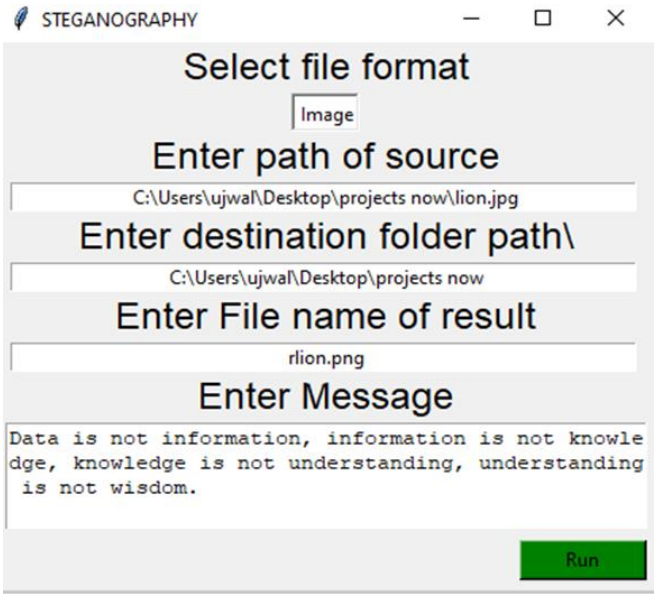

Figure 5: Input Screen

As we have two modules, we are going to use encoding and enter the message to be hidden. For this we need to enter the path of the image which we are using for encoding the message. In the next step we need to enter the path where we want to store our stego image. In the next step we need to enter the desired name of our stego image. In the last step of encoding process, we need to add the message which we want to encrypt.

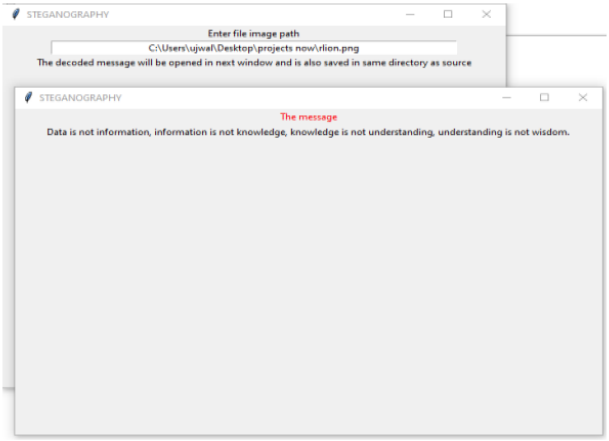

Figure 6: Output Screen

By using the decoding module, the message hidden is displayed to the user. To get the message which we encrypted we need to enter the path of our stego image. After the decryption process, we can see the message which we have encrypted.

The image used to hide the message and the stego image created are quite similar that it is hard to identify. For the above example the image used is a lion and we have two images displayed before and after the creation of a stego image.

Figure 7: Image used to hide information

5. Conclusion & Future Work

5.1 Conclusion

The scope of the project is to limit unauthorized access and provide better security during message transmission. In this project, we mainly concentrated on embedding the data into an image.

5.2 Future Extension

This project can be further extended to a level such that it can be used for the different types of image formats like. gif,. tif etc., and also use other formats like video, audio in the future.

References

[1] Jayaram P, Ranganatha H R, Anupama H S, " Information Hiding Using Audio Steganography – A Survey" in The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011.
[2] Jammi Ashok, Y. Raju, S. Munishankaraiah, K. Srinivas "Steganography: An Overview" in International Journal of Engineering Science and Technology Vol.2 (10), 2010.
[3] K. P. Adhiya and Swati A. Patil, "Hiding Text in Audio Using LSB Based Steganography" in Information and Knowledge Management Vol.2, No.3, 2012.
[4] Pratap Chandra Mandal Modern "Steganographic technique: A survey" in International Journal of Computer Science & Engineering Technology (IJCSET).
[5] Cheddad, A., Condell, J., Curran, K., Mc Kevitt, P.: Digital image steganography: survey and analysis of current methods. Signal Process.90 (3), 727–752 (2010).