# Embedding Algorithm for Data Hiding using Steganographic Technique by File Hybridization

Akari Myint Soe, Zarli Cho
*Computer University, Pyay*
akarimyintsoe@gmail.com, chitsu2010.2@gmail.com

## Abstract

*The Internet as a whole does not use secure links, thus information in transit may be susceptible to interception as well. The important of reducing a chance of the information being detected during the transmission is being an issue now days. Some solution to be discussed is how to passing information in a manner that the very existence of the message is unknown in order to repel attention of the potential attacker. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media. In this paper, clarify what steganography is, the definition, the importance as well as the technique used in implementing steganography. It focuses on the Least Significant Bit (LSB) technique in hiding messages in an image. In this system discussed a new steganographic technique based on the file hybridization. In contrast to other methods of steganography where data embedding in image work on the principle of only one image file, the proposed method works on more than one image. The effectiveness of the proposed method is described pictorially and also has been shown that a multi-level of security of data can be achieved.*

## 1. Introduction

Steganography is the art and science of invisible communication.Hiding information into another covering media in a way that nobody except the receiver can detect the secret message and retrieve it. The word steganography is derived from the Greek words "*stegos*" meaning "cover" and "*grafia*" meaning "writing" [1] defining it as "covered writing". In image steganography the information is hidden exclusively in images. Different types of Steganographic techniques employ invisible inks, microdots, character arrangement, digital signatures, convert channel, and spread spectrum communications.

Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret [1]. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated [1]. The strength of steganography can thus be amplified by file hybridization.

The advantage of steganography over cryptography alone is that messages do not attract attention to themselves, to messengers, or to recipients. An unhidden coded message, no matter how unbreakable it is, will arouse suspicion and may in itself be incriminating, as in some countries encryption is illegal. Steganography have been many techniques for hiding information or messages in images.There are following

(i) Least significant bit insertion (LSB)

(ii) Masking and filtering

(iii) Transform techniques

Least significant bits (LSB) insertion is a simple approach to embedding information in image file. The simplest steganographic techniques embed the bits of the message directly into least significant bit plane of the *cover-image* in a deterministic sequence. Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small.

Masking and filtering techniques, usually restricted to 24 bits and gray scale images, hide information by marking an image, in a manner similar to paper watermarks.

Transform techniques embed the message by modulating coefficients in a transform domain. These methods hide messages in significant areas of the *cover-image*, which make them more robust to attack.

In this work, we consider that a stego image file may be combined with frame. This concept helps us in designing a methodology for both hiding and extracting information and is discussed in the following.

## 2. Mixing File Creation

The concept of hybridization may be used in the field of steganography, where more than one file is to be merged and a new hybrid file may consequently be generated. This hybrid file basically consists of two files, namely

· Stego image
· Supporting Frame

**Stego image:** This is a file where we can store the secret data. The basic property of this stego image file is such that even if we change the intensity of any pixel it should look like the original image. Appropriate candidate for this purpose are cartoon images, geographical images, background images of any picture or images in any chemical reaction and like others. For example, in the case of raindrops or any other nature image we can see that by an appropriate change in color of the object lying in the image can give the same impression of the original image. In order to store the secret data in such a file, the size of the container file should be proportional to the size of the secret data.

**Supporting Frame:** To make the image common, we need a supporting image frame so that the new hybrid file looks like the original one. The selection of supporting frame will depend on the feature of the stego image file to ensure the above characteristics.

There will be two options in this process; either we can put the stego image into the supporting frame or vice versa.

### 2.1 Stego image Creation

The basic model of steganography consists of *Carrier*, *Message* and *Password*. Carrier is also known as *cover-object*, which the message is embedded and serves to hide the presence of the message. Basically, the model for steganography is shown on Figure 1 [1]. Message is the data that the sender wishes to remain it confidential. It can be plain text, ciphertext, other image, or anything that can be embedded in a bit stream such as a copyright mark, a covert communication, or a serial number. Password is known as *stego-key*, which ensures that only recipient who know the corresponding decoding key will be able to extract the message from a *cover-object*. The *cover-object* with the secretly embedded message is then called the *stego-object.*

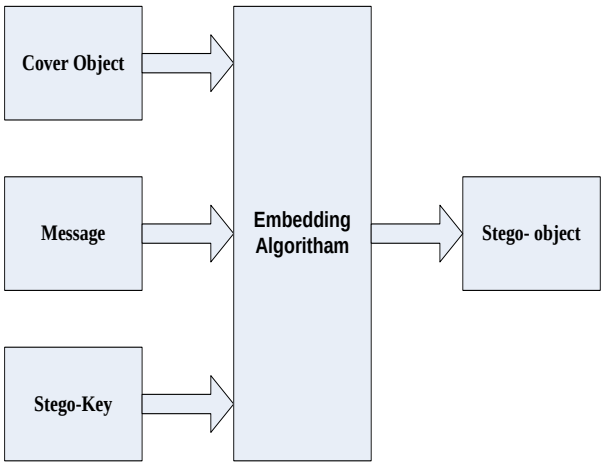



Fig.1 Basic Model for Stego-image files Creation

## 3. Proposed Embedding Algorithm

The purpose technique of hiding data inside images are either 4-LSB or pixel indicator technique(PIT).

In Fig. 2. ***4-LSB Technique*** which use for the data that is inserted into the Stego object file is the sentence" steganography mean covered writing".

In Fig 3. ***Pixel Indicator Techniue (PIT)*** uses the least significant bits of one of the channels to indicate existence of data in the other two channels.We propose this pixel indicator technique for RGB images steganography.

If consider the size of an image as M x N, and Z be the amount of secret data that to be sent through this image then, the relation between the size of data and the place in the container file may be defined as follows.

For the former case, certainly we have

$Z < 3 \times M \times N$

Consider P as the maximum space required for storing the secret data of size is Z, we explain the following cases.

**Case I when Z<P**

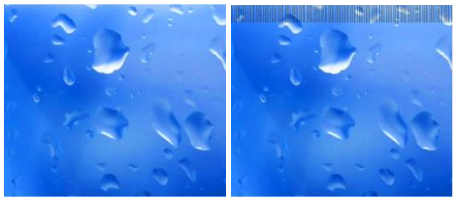
- Use to the Pixel indicator technique(PIT) or 4-LSB of our secret message by simply overwriting the data

**Case II when Z>P**

- If the secret message is more than the image space, then it is not possible to store all the secret message into the image file

### 3.1. 4-LSB

4-Least Significant Bit method involves utilizing four least significant bits of one of the RGB bytes of a 24-bit image for message concealment. It use 8-bit true color image to hold 4-bit of our secret message by simply overwriting the data.



a) b)

a)Cover image file before inserting the data
b)Stego image file

Fig.2 Creation of Stego image files using 4-LSB

### 3.2. Pixel Indicator Technique in 1-LSB

The technique uses least significant bits of one of the channels Red, Green or Blue as an indicator of data existence in the other two channels. The indicator bits are set randomly (based on the image nature) in the channel. Table 1 shows the relation between the indicator and the hidden data inside the other channels. To improve security, the indicator channel is not fixed. The indicators are chosen based on a sequence.

In the first pixel Red is the indicator, while Green is channel **1** and Blue is the channel **2**.

In the second pixel, Green is the indicator, while Red is channel **1** and Blue is channel **2**.

In third pixel Blue is the indicator, while Red is channel **1** and Green is channel **2**.

**Table 1.** Meaning of indicator values

| Indicator | Channel 1 | Channel 2 |
|---|---|---|
| 0 | No hidden data | No hidden data |
| 1 | No hidden data | 1 bit of hidden data |

These techniques by using one of the channels as an indicator for data existence in the other two channels and the indicator are set randomly by nature.

a) b)

a) Cover image file before inserting the data
b) Stego image file

Fig.3 Creation of Stego image file using PIT

After creation of the Stego image file the next step is to create the hybrid file.

## 4. Hybrid file Creation

After combining frame by the stego-image we get the resultant hybrid or mixed image (Fig. 4).

b) Hybrid Image File after merge of a) and Fig. 3 b)

Fig. 4 Formation of Hybrid Image File

## 5.Data Capacity

Capacity is the amount of information that can be hidden in the cover medium. The most basic of LSBs insertion for 24-bit pictures insert 3bit/pixel. Since every pixel is 24 bits, we can hide. Acquiring a data rate of 3 embedded bits every 8 bits of the image.The image size of 800 × 600 (480,000 pixels), have been used to hide text message of 144,0000 Bytes . Data Capacity in 800×600 cover image is shown in Table 2.

**Table 2.** Compare data capacity for PIT and 4-LSB

| Embedding Technique | Data Capacity |
|---|---|
| 4-LSB | 720,000 Bytes |
| 1-LSB | 180,000 Bytes |
| PIT | 360 Bytes |

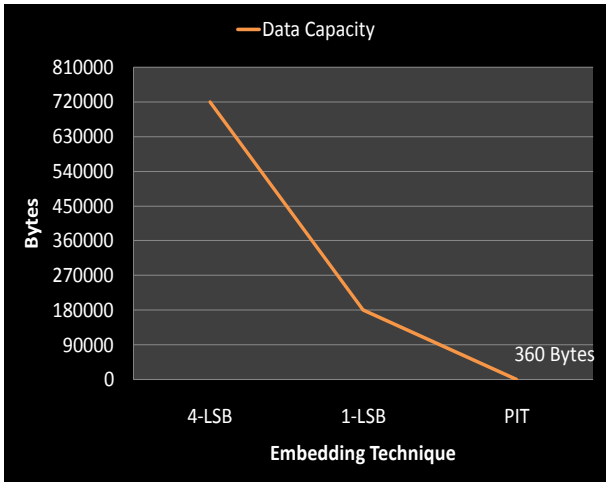



Fig.5 The Embedding data capacity graph for **800×600** Cover Image

**Table 3: Evolution results details**

| Visual Inspection of the image | Score | | 4bit-LSB | PIT |
|---|---|---|---|---|
| | Not Susceptible | | | - |
| | Susceptible | Low | | |
| | | High | - | |

## 6. Comparison Result

The performance of the proposed technique has been highlighted here with the concept being used Least Significant Bits (LSB) methods. 4-LSB considered to compare with pixel indicator technique (PIT). The advantages of 4-LSB are clear. 4-LSB methods use 1 pixel per 1byte message. So, it can be accept many amount of message. Disadvantages of 4-LSB is the visual change between the original image and stego-image can be forecast in fig2 b).PIT embedded data can easily be implemented and do not visually degrade the image to the point of being noticeable in fig 3 b). The evolutional results are pointed out in Table 3. Note that the proposed PIT showed better results when compared to 4bits-LSB are considered. But, the disadvantages of PIT cannot embed many data.

## 7. Conclusion

The rise of the Internet, one of the most important factors of information technology and communication has been the security of information. Steganography applications for digital image including copyright protection,feature tagging, and secret communication.In this system we give an idea to enhance the security of system by combining the two techniques. Here message is first embedded in using PIT or 4-LSB technique and then merge in frame to provide double layer protection. The study considered PIT techniques to compare with 4-LSB technique. PIT is more security because it has not susceptible.

## 8. References

[1] N.F. Johnson and S. Jajodia, " Exploring Steganography: Seeing the Unseen ", Computer, vol. 31, No. 2, Feb 1998, pp. 26-34.

[2] Donovan Artz " Digital Steganography: Hiding Data within Data", IEEE Internet computing, pp.75-80 May –June 2001.

[3] Niels Provos and Peter Honeyman, "Hide and Seek : An Introduction to Steganography", IEEE 1540-7993, June 2003'

[4] Alkhraisat Habes, "Information Hiding in BMP image Implementation, Analysis and Evaluation" , Saint Petersburg Institute for Informatics and Automation, Russian Academy of Sciences, Saint Petersburg, Russia

[5] G. Sahoo1 and R. K. Tiwari2, "Designing an Embedded Algorithm for Data Hiding using Steganographic Technique by File Hybridization, Department of Computer Science &Engineering. , B.I.T., Mesra, Ranchi, Jharkhand, India

[6] F.A.P Peticolas, R.J. Anderson and M.G.Kuhn, "Information Hiding –A Survey", and Proceedings of IEEE, pp. 1062-1078, July 1999.

[7] Adnan Gutub, Ayed Al-Qahtani, Abdulaziz Tabakh,"Triple-A: Secure RGB Image Steganography Based on Randomization" Computer Engineering Department, KFUPM, Dhahran 31261, SAUDI ARABIA