Image Steganography Using LSB Substitution and Five Modulus Technique

Swati Siddul\(^1\), Neha Surve\(^2\), Archana Vartale\(^3\), Prof.M.R.Wanjre\(^4\)
\(^1\)UG Students, Department of E&TC, AISSMS’s IOIT, Pune, India
\(^2\)siddulswati@gmail.com
\(^3\)nehasurve41@gmail.com
\(^4\)archanavartale@yahoo.com
Assst. Prof. Department of E&TC, AISSMS’s IOIT, Pune, India
mamta.wanjre@gmail.com

Abstract- Steganography is the process of hiding a secret message within a larger one in such a way that someone can not know the presence or contents of the hidden message. In LSB substitution technique least significant bits are replaced by the bits of the data to be hidden so that intruder will not be aware of existence of message. In Five modulus technique the secret message is hidden inside the 5×5 window as a non-multiples of 5. Since the modulus of non-multiples of 5 are 1, 2, 3 and 4, therefore if the reminder is one of these, then the pixel represents a secret character. This paper provides comparison between these two techniques.

Keywords: steganography ,Data hiding, LSB substitution, information hiding, five modulus method

I. INTRODUCTION

Steganography deals with hiding data into a cover media so that the observer is unable to detect the hidden content. The cover media is nothing but medium containing secret information. The main objective of Steganography is to prevent the Secret data from being stolen. The cover along with the hidden information is called as stego-object. The process of detection of secret message is called as Steganalysis. The factors to be considered here are invisibility and security.

![Fig.1: General Block Diagram of Steganography](image)

Figure 1 shows the general block diagram of Steganography. There are two inputs Message object and Carrier Object. These are given to the Steganographic Method. The Steganographic Method can be Image, Audio, Video or text Steganography. The Message object is embedded into Carrier Object by using Steganographic Method. After encoding the object obtained is called as Stego – Object. It is sent to the intended recipient so the intruder is unaware of the existence of the message in the Cover Object. The main criteria for security is no third party observer can see, listen or suspect about the message. Different type of object can be used as carrier and message object. It can be Image, Text, audio and video. Steganographic technique is mostly used in the field of secret communication. It can be used by intelligence agencies across the world to maintain confidentiality.

A. Image Steganography:

Image steganography is nothing but Embedding secret message into the cover image. Image steganography can hide the secret message in bit map image, gray scale image ,color image etc. In this paper, 8-bit gray scale images are selected as the cover media. These images are called cover images. Cover-images with the secret messages embedded within them are called stego-images. For data hiding methods, the quality of the image depends on the quality of stego-images.

II. LITERATURE SURVEY

This section gives the basic idea about background literature and describes the concept of steganography in the image. The Word steganography is originally derived from Greek words, which mean “Covered Writing”. It has been used in various forms for thousands of years. In the fifth century BC Histiaicus shaved the head of his messenger, wrote the message on his scalp, and then waited for the hair to grow again. Arriving at his destination, he shaved his head and the secret message could be easily read by the receiver. Two types of Steganography were categorised. The first on which is called fragile, this type of steganography involves embedding information into a file which is destroyed if the file is modified. On the other hand, the other type is the robust steganography which aims to embed information into a file that cannot be easily destroyed. The best known steganographic method that works in the spatial domain is the Least Significant Bit (LSB) which replaces the least significant bits of pixels selected to hide the secret information. To embed the given data secretly into the image, there are few techniques introduced earlier. The lists of methods are:

- LSB substitution
- Five Modulus Method(FMM)
- DCT (Discrete Cosine Transform)
- DWT (Discrete Wavelet Transform)

In LSB Substitution method, the least significant bits of the cover image are replaced by the secret message. In FMM image is divided into a window of particular size in which secret message is hidden.

III. PROPOSED WORK

A. LSB Substitution Technique

1) Method:
The pixel adjustment process is proposed to enhance the image quality of the stego image obtained by the simple LSB substitution method.

In LSB Substitution Method, the gray scale image is used as cover image. Each pixel of gray scale image is made of 8-bits. The LSBs of each pixels are found by using Mod function. Also the secret message to be sent is converted from the textual format to the binary values by ASCII values of each character in the message. Then these values and the LSB matrix which was obtained earlier are compared element by element. If they are same then there will be no change. If LSB value is ‘0’ and the binary value is ‘1’ then the value ‘1’ is added to the pixels value and if LSB is ‘1’ and binary value is ‘0’, the value ‘1’ is subtracted from the pixels value.

In this way the least significant bit (LSB) of each pixel is replaced by the secret message. Since only LSB’s are replaced the Stego image will look same as that of the original image, because majority of the image information is contained in the most significant bits.

2) Result
It is observed that the cover image is not changed. As we see in Following two figures Figure 2a. shows the original cover image before embedding the secret message into it. Figure 2b shows the Stego image in which the secret message is hidden by encoding process. There is no difference between two images below.

![Fig. 2a: Original Cover Image](image1)

![Fig. 2b: Stego Image](image2)

B. Five Modulus Method:

1) Method:
The basic idea behind FMM is based upon the following concept: in most of the images the neighboring pixels are correlated. Therefore for bi-level images, the adjacent of a pixel tend to be similar to the original pixel. Hence, FMM consists of dividing the given image into blocks of k x k pixels each. In binary level grey images we know that each pixel is a number between 0 and 255. Therefore, if we can change each number in that range into a number divisible by 5, according to theory of FMM then this will not affect the Human Visual System (HVS). The basic idea in FMM is to check each and every pixels in the k x k block and transform each pixel into a number divisible by 5 according to the following algorithm.

If Pixel mod 5 = 4
Pixel = Pixel + 1
Else if Pixel mod 5 = 3
Pixel = Pixel + 2
Else if Pixel mod 5 = 2
Pixel = Pixel - 2
Else if Pixel mod 5 = 1
Pixel = Pixel - 1

where Pixel is the digital image representation of the k x k block. According to table (1), the transformation of the FMM could be shown.

<table>
<thead>
<tr>
<th>Old</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>254</td>
<td>255</td>
</tr>
<tr>
<td>255</td>
<td>255</td>
</tr>
</tbody>
</table>

Table 1: FMM transformation

Here, FMM could transform any number in the range 0-255 into a number that when divided by 5 the remainder is always 0, 1, 2, 3, or 4 (e.g., 20 mod 5 is 0, 11 mod 5 is 1, 202 mod 5 is 2, and so on). Mathematically the new values for the k x k block will always be as follows: 0, 5, 10, 15, 20, 25, 30, 35, 40, ..., 200, 205, 210, 215, ..., 250, 255 (i.e., multiples of 5).

![Fig. 5a: Original Image](image3)

![Fig. 3b: FMM Transformation](image4)
and the transformed FMM images. There is no difference between the images.

2) Determination of Window Size
The determination of the suitable size of the window used for steganography is very important procedure. The smaller window size is better to increase number of secret message characters hidden in the cover image. The general formula to determine the suitable window size has been derived as follows:
Window size=√n/4
where n gives the number of distinct characters used in the secret text message.
Also, a general formula to extract the ASCII character value from the steganography image has been derived as follows:
Character value=(position+(remainder-1)×k²)+(starting index-1)

3) Result
In order to illustrate proposed steganography algorithm, FMM has been implemented to the bitmap test image (i.e. Lena) which is used as a cover image. The cover image is 512×512 bitmap image. Since the text message used contain the 95 common ASCII characters a window of size 5×5 have been used for FMM technique.

Fig. a) original image  b) stego image

IV. CONCLUSION
In this paper, a method for steganography based on the LSB substitution and FMM method has been represented. Many research have been done on different techniques but image quality problem exists in every method. So, in order to achieve good quality of the image, the implementation of the FMM into steganography produces better results than LSB substitution method that do not have a noticeable distortion on it by the human eye. Hence, FMM steganography algorithm is very efficient to hide the secret text inside the image. FMM is not an absolute steganographic algorithm and has some limitations. There are issues that need to be resolved.

REFERENCES
[1] Chi-Kwong Chang, L.M. Cheng, “Hiding data in images by simple LSB substitution”, Department of Computer Engineering and Information Technology, City University of Hong Kong, Hong Kong, Received 17 May 2002; received in revised form 11 July 2003; accepted 11 August 2003.