ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 11, November 2013

# Use of Least Significant Bit for Text Hiding Behind Image

Salony Pandey[1]
[1]PG Student,RK UNI,Rajkot
Vinay Harsora[2]
[2]Asst. Prof. RKU UNI Rajkot

***Abstract*: Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exist a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. This paper focus on LSB method. Also various results are derived**

## I. INTRODUCTION

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. 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. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. 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 [2]. 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 [2]. The strength of steganography can thus be amplified by combining it with cryptography. Research in steganography has mainly been driven by a lack of strength in cryptographic systems. Many governments have created laws to either limit the strength of a cryptographic system or to prohibit it altogether [3], forcing people to study other methods of secure information transfer. Businesses have also started to realize the potential of steganography in communicating trade secrets or new product information. Avoiding communication through well-known channels greatly reduces the risk of information being leaked in transit [4]. Hiding information in a photograph of the company picnic is less suspicious than communicating an encrypted file.

## II. LSB AND PALETTE BASED IMAGES

Palette based images, for example GIF images, are another popular image file format commonly used on the Internet. By definition a GIF image cannot have a bit depth greater than 8, thus the maximum number of colours that a GIF can store is 256 [41]. GIF images are indexed images where the colours used in the image are stored in a palette, sometimes referred to as a colour lookup table [41]. Each pixel is represented as a single byte and the pixel data is an index to the colour palette [29]. The colours of the palette are typically ordered from the most used colour to the least used colours to reduce lookup time [30]. GIF images can also be used for LSB steganography, although extra care should be taken.

The problem with the palette approach used with GIF images is that should one change the least significant bit of a pixel, it can result in a completely different colour since the index to the colour palette is changed [30]. If adjacent palette entries are similar, there might be little or no noticeable change, but should the adjacent palette entries be very dissimilar, the change would be evident [30]. One possible solution is to sort the palette so that the colour differences between consecutive colours are minimized [16].

Another solution is to add new colours which are visually similar to the existing colours in the palette. This requires the original image to have less unique colours than the maximum number of colours (this value depends on the bit depth used) [36]. Using this approach, one should thus carefully choose the right cover image. Unfortunately any tampering with the palette of an indexed image leaves a very clear signature, making it easier to detect.

A final solution to the problem is to use grayscale images. In an 8-bit greyscale GIF image, there are 256 different shades of grey [29]. The changes

between the colours are very gradual, making it harder to detect.

## III .EVALUATION OF DIFFERENT TECHNIQUES

All steganographic algorithms have to comply with a few basic requirements. The most important requirement is that a steganographic algorithm has to be imperceptible.These requirements are as follows:

**Invisibility** – The invisibility of a steganographic algorithm is the first and foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye. The moment that one can see that an image has been tampered with, the algorithm is compromised

**Payload Capacity** – Unlike watermarking, which needs to embed only a small amount of copyright information, steganography aims at hidden communication and therefore requires sufficient embedding capacity.

**Robustness Against Statistical Attacks** – Statistical steganalysis is the practice of detecting hidden information through applying statistical tests on image data. Many steganographic algorithms leave a 'signature' when embedding information that can be easily detected through statistical analysis. To be able to pass by a warden without being detected, a steganographic algorithm must not leave such a mark in the image as be statistically significant.

**Robustness Against Image Manipulation** – In the communication of a stego image by trusted systems, the image may undergo changes by an active warden in an attempt to remove hidden information. Image manipulation, such as cropping or rotating, can be performed on the image before it reaches its destination. Depending on the manner in which the message is embedded, these manipulations may destroy the hidden message. It is preferable for steganographic algorithms to be robust against either malicious or unintentional changes to the image.

**Independent of File Format** – With many different image file formats used on the Internet, it might seem suspicious that only one type of file format is continuously communicated between two parties. The most powerful steganographic algorithms thus possess the ability to embed information in any type of file. This also solves the problem of not always being able to find a suitable image at the right moment, in the right format to use as a cover image.

**Unsuspicious Files** – This requirement includes all characteristics of a steganographic algorithm that may result in images that are not used normally and may cause suspicion. Abnormal file size, for example, is one property of an image that can result in further investigation of the image by a warden.

## IV. LEAST SIGNIFICANT BIT METHOD

The popular and oldest method for hiding the message in a digital image is the LSB method. In LSB method we hide the message in the least significant bits (LSB's) of pixel values of an image. In this method binary equivalent of the secret message is distributed among the LSBs of each pixel. For example data bits 01100101 are tried to hide into an 8 bit colour image. According to this technique 8 consecutive pixels from top left corner of the image are selected. The binary equivalent of those pixels may be like this:

00100101 11101011 11001010 00100011
11111000 11101111 11001110 11100111

Now each bit of data 01100101 are copied serially (from left hand side) to the LSB's of equivalent binary pattern of pixels, resulting the bit pattern would become:

00100101 11101011 11001011 00100010
11111000 11101111 11001110 11100111

The problem with this technique is that it is very vulnerable to attacks such as image compression and quantization of noise.

## V .RESULT & DISCUSSION

Following Table Shows the results of Simple LSB method implemented on the following image. First Column of table indicates various parameters with values.

| | Simple LSB Method | | |
|---|---|---|---|
| Image |  (8-bit, Grayscale) | | |
| Image Size | 150 x 150 | | |
| Message(number of char) | 100 | 250 | 500 |
| Number of LSB Changed | 407 | 1025 | 2026 |
| SNR of Stego Image(dB) | 57.9988 | 53.9875 | 51.0283 |
| PSNR of Stego Image(dB) | 63.8703 | 59.8590 | 56.8998 |
| Time Required to Hide (Seconds) | 0.884371 | 0.932057 | 0.935710 |
| Time Required to Extract (Seconds) | 0.007044 | 0.017437 | 0.037058 |

## VI.CONCLUSION

This experimental result concludes that as the size of message increases the change in number of LSBs also increases thus the PSNR factor decreases i.e quality of image degrades. One can improve the quality of image by decreasing the change in number of LSBs.

## REFERENCES

[1] Moerland, T., "Steganography and Steganalysis", *Leiden Institute of Advanced Computing Science*, www.liacs.nl/home/ tmoerl/privtech.pdf
[2] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", *Communications of the ACM*, 47:10, October 2004
[3] Dunbar, B., "Steganographic techniques and their use in an Open-Systems environment", *SANS Institute*, January 2002
[4] Artz, D., "Digital Steganography: Hiding Data within Data", *IEEE Internet Computing Journal*, June 2001
[5] Johnson, N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal,February 1998
[6]Johnson, N.F. & Jajodia, S., "Steganalysis of Images Created Using Current Steganography Software",Proceedings of the 2nd Information Hiding Workshop, April 1998
[7] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science,www.liacs.nl/home/ tmoerl/privtech
[8] Reference guide: Graphics Technical Options and Decisions", http://www.devx.com/projectcool/Article/19997