



International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)

www.iasir.net

A Steganography Technique for Hiding Information in Image

Kamred Udham Singh

Department of Computer Science,

Faculty of Science Banaras Hindu University, Varanasi, (U.P.), INDIA

Abstract: In the area of Information Security, hiding the facts and communication from third parties is the most important factor of information technology. Security is concerned with the protection and safeguard of that information which, in its various forms can be identified Information Assets. To protect the Information from the third party we use the message hiding technique called steganography. Steganography is art and science of invisible communication. This paper deals with image steganography. For hiding secret information in images, there are number of steganographic techniques some are more complex than others and all of them have respective strong and weak points. Various steganographic algorithms like Least Significant Bit (LSB) algorithm, Jsteg and F5 algorithms, from all of these. We are going to use LSB algorithm. This paper gives a brief idea and overview of image steganography that make use of Least Significant Bit (LSB) algorithm for hiding the data into image.

Keywords: Decryption, Encryption, LSB (Least Significant Bit, Steganography), Stego key

I. Introduction

The most important factor of information technology and communication is the security of information. The idea of information hiding is not new in the history. Various methods have been developed to hide data in order to keep the message secret. Sometimes it is not enough to keep the contents of a message secret but it may also be necessary to keep the existence of the message secret. Steganography is the art and science of invisible communication of messages. It is implemented by hiding the existence of the communicated information in image, video and audio. The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing”[1] defining it as “covered writing”. The graphical representation of Steganography system presented in fig: 1.

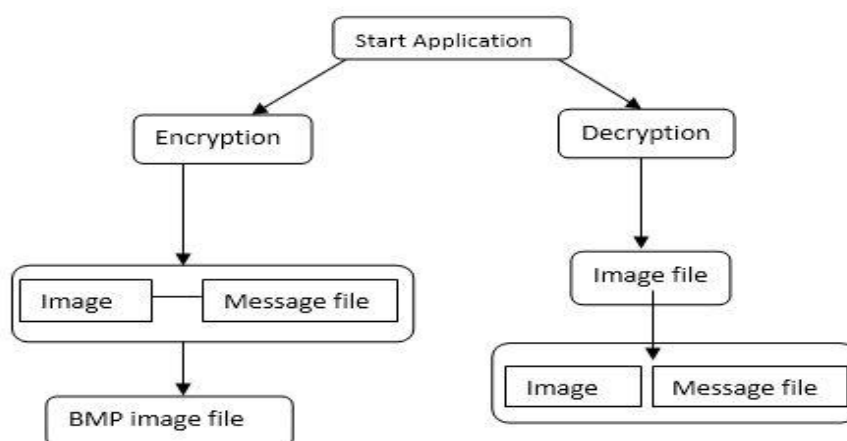


Figure: 1

The idea and practice of hiding information has a long history. In Histories the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave's scalp. When the slave's hair grew back the slave was dispatched with the hidden message [2]. The difference between Steganography and Cryptography is that the cryptography focuses on keeping the contents of a message secret whereas steganography focuses on keeping the existence of a message secret [3]. Steganography and cryptography both techniques are protecting information from undesired parties. There are two other technologies which are related to steganography are watermarking and fingerprinting. There are three components in steganography structure: Carrier image,

Message, Key. This paper describes the LSB algorithm used for image steganography to the security potential of steganography for business and personal use. In this paper, we describe the LSB algorithm used for image steganography to the security potential of steganography for business and personal use. Section II described basics of Encryption and Decryption techniques. Section III discuss about compression of image files i.e. lossy or lossless. In Section IV surveyed of least significant bit (LSB) algorithm and how it works on image files. Finally, Section V concludes the Paper.

II. Encryption and Decryption

In encryption the secret information is hiding in image file. In Decryption secret information is extract from image file. When a text message embedded with image a key is needed. This key is used to help in encryption and it decided that where the information should be hidden in the image. A short text can be use as a key.

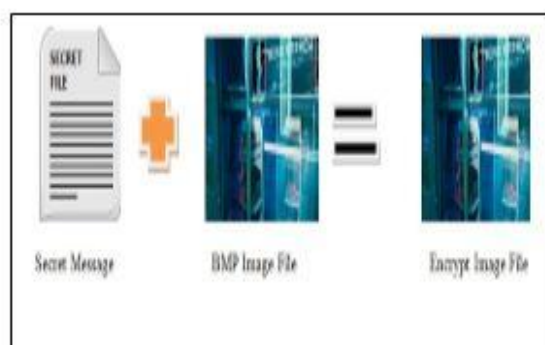


Figure 2: Encryption Process

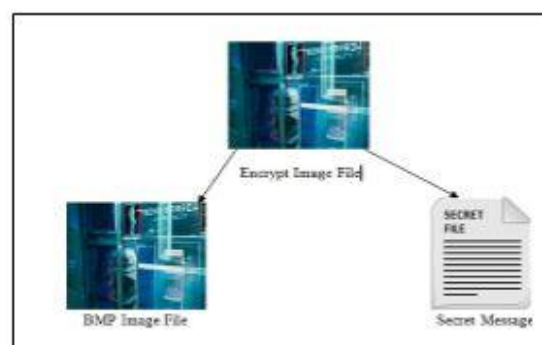


Figure 3: Decryption Process

III. Image Compressions

Image compression is a process of minimizing the size in bytes of a graphics file without demeaning the quality of the image. Microsoft Document Imaging Format (MDI) or Tagged Image File Format (TIFF), image compression is used to reduce the size of the file. There are two types of image compression: lossy and lossless [4]. These both methods are used to save storage space, but the implementing procedures are distinct. Lossy image compression creates slighter files by dumping excess image data from the original image. And it also removes that details which are too tiny for the human eye to differentiate [6]. On the other side Lossless image compression never removes any information from the original image, but instead represents data in mathematical formulas [6]. The original image's integrity is maintained and the decompressed image output is bit-by-bit identical to the original image input [4]. Lossless compression image formats are GIF (Graphical Interchange Format) and 8-bit and 24 bit BMP (Bitmap) [5]. Lossless image compression keeps the original digital image intact without the chance of lost.

IV. Concepts of Image File

An image is a collection of numbers of pixels. These pixels are displayed horizontally row by row. The number of bits in a color scheme, called the bit depth, refers to the number of bits used for each pixel. The smallest bit depth is 8, it means that there are 8 bits used to describe the color of each pixel. Grayscale images use 8 bits for each pixel and able to display 256 different colors. Digital color images are stored in 24-bit files and use the RGB color model that is known as true color. All colors of 24-bit image are most frequently represented as additive combinations of red (R), blue (B), and green (G), and each primary color is represented by 8 bits. In one given pixel, there can be 256 different quantities of red, green and blue [7]. We can represent over 16 million colors with 24 bits. The representation of RGB colors in a [R, G, B] format is [0, 0, 0] for black, and [255, 255, 255] for white. Grayscale colors will be represented by a single number for example black has a value of 0, white is 255 and light gray is 200

V. Images and Transform Domain

Image steganography techniques are two type first is Image Domain and second is Transform Domain [8]. In transform domain, images are first transformed and then the message is embedded in the image [10]. Image domain techniques cover bit-wise methods that apply bit insertion and noise manipulation [11]. Lossless image compression formats are most suitable for image domain steganography techniques are usually dependent on the image format [12]. Steganography in the transform domain involves the manipulation of algorithms and image transforms [11]. These methods hide messages in more significant areas of the cover image, making it more robust [9].

VI. LEAST SIGNIFICANT BIT TECHNIQUE

Least significant bit (LSB) insertion is a most popular and easy approach to hide information in carrier image file. In the LSB method byte is replaced with an M's bit. This technique is best for image steganography. To the human eye the stego image will look identical to the carrier image. An image file is simply a file which shows different colors on the different areas of an image. The most popular image formats that use lossless compression is 24 Bit BMP (Bitmap), use for hiding information. It is easier to hide information inside in a high quality and resolution image. Due to their size 24 Bit images are best for hiding information. But you can also choose 8 Bit BMP's or another image format such as GIF [13]. The least significant bit is used to change with the bit of secret message. In 24-bit image, one pixel can store 3 bits by changing a bit of each of the red, green and blue color components. For example we have three adjacent pixels (9 bytes) with the RGB encoding [14] (figure 4)-

10010100 00001100 11001001
10010111 00001110 11001011
10011111 00010001 11001011

Figure: 4

10010101 00001101 11001000
10010110 00001111 11001010
10011110 00010000 11001010

Figure: 5

Table 1: Advantage of LSB algorithm

Binary representation of number 400 is 110010000 embedded into the least significant bits of this part of the image. If we overlay these 9 bits over the LSB of the 9 bytes above we get the following (where bits in bold and underline have been changed) (figure5) Number 400 was embedded into the grid and LSB have changed according to the embedded message.

VII. LSB algorithm

- Select an image of size M*N for an input.
- The message to be hidden in RGB component only of an image.
- Use a pixel selection filter to obtain the best areas to hide information in the cover image to obtain an enhanced rate. The filter is applied to Least Significant Bit (LSB) of every pixel to hide information, leaving most significant bits (MSB).
- After that Message is hidden using Bit Replacement method.

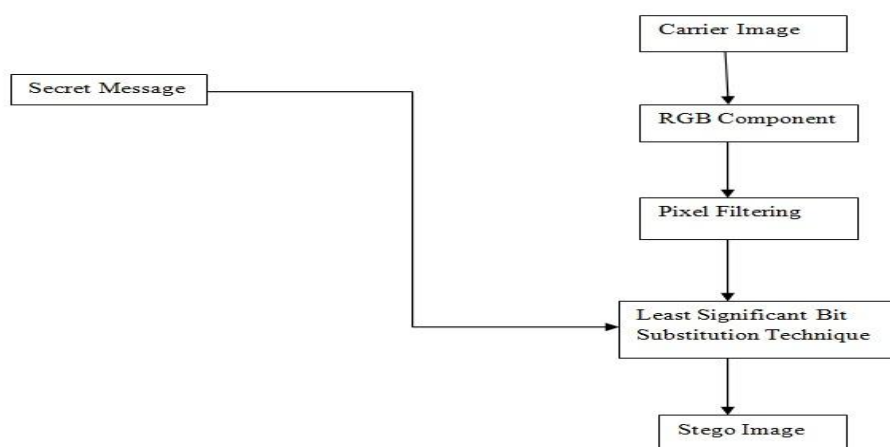


Fig: 6 Algorithm of Least Significant Bit

Benefits of LSB Algorithm: There are two main advantage of Least Significant Bit algorithm which described in following table:

Message Security	Reduce Distortion Rate
A least significant bit technique uses 24 bit BMP images, because it is a lossless compression image formats. In a 24 bit BMP image for hiding the secret data, there is the need of large cover image. Before embedding it in digital image message data is converted in digital image in to byte. So this approach is secure, prevent from liability.	Mostly images are used in steganography as a cover objects. 24 bit BMP (Bitmap) is use for hiding information because it is a lossless compression image formats. To hide the message in image, first it is converted into byte format and then stored in byte array. After that message is encrypted and then embeds each bit into the LSB position of each pixel position. This approach involves change in least significant bit (LSB) of each pixel byte. Hence reduces the distortion rate that is look of original image.

VIII. Result and conclusion

In this paper the existing Least Significant Bit Algorithm has been analyzed and found can effectively hide a message inside a digital image file. There are many applications of image steganography which are used for secretly and covertly communication. Main use of image steganography is, communication of high-level or top-secret documents between international governments. Image steganography has many illegal uses as it can be used by hackers to send viruses and Trojans. Image steganography increase the security of the message by hiding it in a less obvious location. IT also describes the benefits from approach like security of message increases and distortion rate has reduced.

References

- [1] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/tmoerl/privtech.pdf
- [2] Silman, J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001
- [3] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, October2004
- [4] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/tmoerl/privtech.pdf
- [5] Johnson, N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998
- [6] "Reference guide: Graphics Technical Options and Decisions", <http://www.devx.com/projectcool/Article/19997>
- [7] Owens, M., "Adiscussion of covert channels and steganography", SANS Institute, 2002
- [8] Silman, J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001
- [9] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October2004
- [10] Lee, Y.K. & Chen, L.H., "High capacity image steganographic model", Visual Image Signal Processing, 147:03, June 2000
- [11] Johnson, N.F. & Jajodia, S., "Steganalysis of Images Created Using Current Steganography Software", Proceedings of the 2nd Information Hiding Workshop, April1998
- [12] Venkatraman, S., Abraham, A. & Paprzycki, M., "Significance of Steganography on Data Security", Proceedings of the International Conference on Information Technology: Coding and Computing, 2004
- [13] V. Lokeswara Reddy, Dr.A.Subramanyam, Dr.P. Chenna Reddy, "Implementation of LSB Steganography and its Evaluation for Various File Formats", Int. J. Advanced Networking and Applications 868 Volume: 02, Issue: 05, Pages: 868-872 (2011)
- [14] T. Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in Proceeding of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sand to South Africa, June/July 2005