Lsb Technique For Stegnography For Data Security: Review

[1]Archana garg, [2]Harmanjot Singh Dhaliwal
[1]Student,M.Tech,ECE,Punjabi university, Patiala.
[2]Assistant Professor,ECE,Punjabi university, Patiala.

Abstract

With the growth of communication technology, data hiding is becoming an important issue. For security of data, Stegnography is used. Steganography embeds the secret message in cover file and generate the stego file which is send over the internet. Various types of techniques are used in Steganography. One of the techniques which is most frequently used is LSB technique in which the secret message is embedded in the least significant bits of the cover file. In this paper, LSB Technique and various parameters including capacity, transparency and robustness are discussed.

Keywords: Steganography, Cover file, Stego file, LSB.

1. INTRODUCTION

Today by increasing use of the internet and other new technologies, the possibility of pirate access to private information of the people and companies is also increased. So it is necessary to employ novel methods for confining the accesses to these data.[1] Steganography is a powerful tool which increases security in data transferring and archiving. In the steganography scenario the covert data is first concealed within another object which is called "cover object", to form "stego object" and then this new object can be transmitted or saved. It causes the existence of the covert data and even its transmission becomes hidden. [2]

In cryptography, the structure of a message is scrambled to make it meaningless and unintelligible unless the decryption key is available. It makes no attempt to disguise or hide the encoded message. Basically, cryptography offers the ability of transmitting information between persons in a way that prevents a third party from reading it. Cryptography can also provide authentication for verifying the identity of someone or something [3].

Steganography does not alter the structure of the secret message, but hides it inside a cover image so that it cannot be seen. A message in a cipher text, for instance, might arouse suspicion on the part of the recipient while an “invisible” message created with steganographic methods will not. In other word, steganography prevents an unintended recipient from suspecting that the data exists. In addition, the security of classical steganography system relies on secrecy of the data encoding system. Once the encoding system is known, the steganography system is defeated.

The following points can be attributed to the renaissance of steganography

i. Government ban on digital cryptography. Individuals and companies who seek confidentiality look to steganography as an important complementary since combining cryptography and steganography can help in avoiding suspicion and protect privacy.

ii. The increased need to protect intellectual property rights by digital content owners, using efficient watermarking.

iii. The trend towards electronic communications and humans desire to conceal messages from curious eyes. With rapid advancement in technology, steganographic software is becoming effective in hiding information in image, video, audio or text files [4],[5],6].

Information security using steganography is the way of writing hidden messages in such a way that other than sender and intended recipient, nobody knows the existence of the message in cover object. Here the secret message and cover object may be in any format like text or image or audio file. For each format of information, steganography provides different way to hide the secret message. Only the drawback is that as per information format, steganography method is selected. [2]

2. PROCESS OF STEGNOGRAPHY

The steganography application hides different types of data within a cover file. The resulting stego also contains hidden information, although it is virtually identical to the cover file.

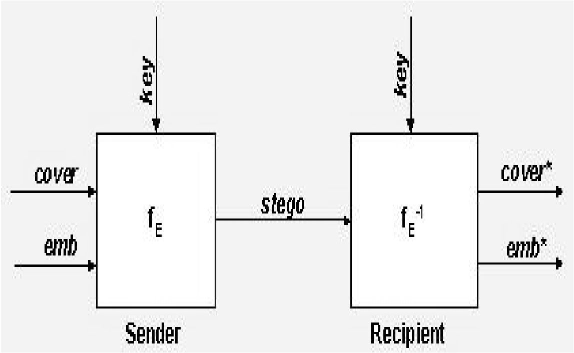

Fig1: Secure steganographic system

The components of steganographic system are:
Emb: The message to be embedded.
Cover: The data in which emb will be embedded.
Stego: A modified version of cover that contains the embedded message emb.
Key: Additional secret data that is needed for the embedding and extracting processes and must be known to both, the sender and the recipient.
fE: A steganographic function that has cover, emb and key as parameters and produces stego as output.
FE-1: A steganographic function that has stego and key as parameters and produces emb as output. FE-1 is the inverse function of fE in the sense that the result of the extracting process fE-1is identical to the input E of the embedding process fE.

The embedding process fE embeds the secret message E in the cover data C. The exact position (S) where E will be embedded is dependence on the key K. The result of the embedding function is slightly modified version of C: the stego data C’. After the recipient has received C’ he starts the extracting process fE-1 with the stego data C’ and the key K as parameters. If the key that is supplied by the recipient is the same as the key used by the sender to embed the secret message and if the stego data the recipient uses as input is the same data the sender has produces (i.e., it has not been modified by an adversary), then the extracting function will produce the original secret message E. [4]

3. STEGNOGRAPHY TYPES

Steganography may be classified as pure, symmetric and asymmetric. While pure steganography does not need any exchange of information, symmetric and asymmetric need to exchange of keys prior sending the messages. Steganography is highly dependent on the type of media being used to hide the information. Medium being commonly used include text, images, audio files, and network protocols used in network transmissions. Image Steganography is generally more preferred media because of its harmlessness and attraction. Additionally exchange of greetings through digital means is on the increase through the increased use of the internet and ease of comfort and flexibility is sending them. Technology advancement in design of cameras and digital images being saved in cameras and then transfer to PCs [8] has also enhanced many folds. Secondly, the text messages hidden in the images does not distort the image and there are techniques which only disturb only one bit of an image who’s effects is almost negligible on its quality. The major drawbacks of steganography are that one can hide very little information in the media selected.Some methods are following.

- Encoding secret message in text/documents
- Encoding secret message in audio
- Encoding secret message in images [7]

4. LEAST SIGNIFICANT BIT TECHNIQUE

Least significant bit (LSB) insertion is a common and simple approach to embed information in an image file. In this method the LSB of a byte is replaced with an M‟s bit. This technique works good for image steganography. To the human eye the stego image will look identical to the carrier image.. For hiding information inside the images, the LSB (Least Significant Byte) method is usually used. To a computer an image file is simply a file that shows different colors and intensities of light on different areas of an image. The best type of image file to hide information inside is a 24 Bit BMP (Bitmap) image. When an image is of high quality and resolution it is a easier to hide information inside image. Although 24 Bit images are best for hiding information due to their size. Some people may choose 8 Bit BMP‟s or possibly another image format such as GIF [10]. The reason being is that posting of large images on the internet may arouse suspicion. The least significant bit i.e. the eighth bit is used to change to a bit of the secret message. When using a 24-bit image, one can store 3 bits in each pixel by changing a bit of each of the red, green and blue color components. Suppose that we have three adjacent pixels (9 bytes) with the RGB encoding

10010101 00001101 11001001
10010110 00001111 11001011
10011111 00010000 11001011

When the number 300, can be which binary representation is 100101100 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 have been changed)

10010101 0000110**0** 1100100**0**
1001011**1** 0000111**0** 11001011
10011111 00010000 1100101**0**

Here the number 300 was embedded into the grid, only the 5 bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size. [7]

4.1 Least Significant Bit Algorithm

1. Select a cover image of size M*N as an input.
2. The message to be hidden is embedded in RGB component only of an image.
3. Use a pixel selection filter to obtain the best areas to hide information in the cover image to obtain a better rate. The filter is applied to Least Significant Bit (LSB) of every pixel to hide information, leaving most significant bits (MSB).

4. After that Message is hidden using Bit Replacement method. [7]

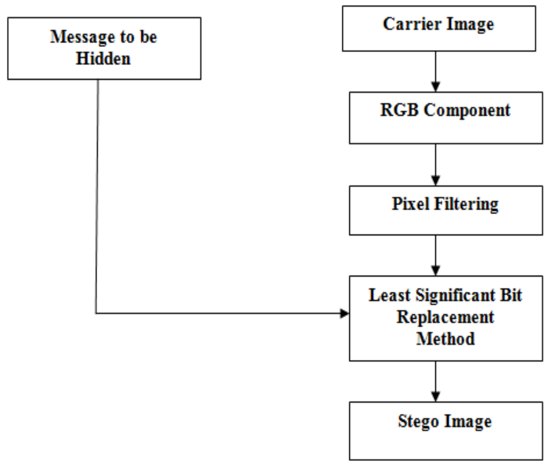

Fig 2: LSB algorithm

5. Analysis

Most researchers use Peak Signal to noise Ratio (PSNR), Mean Square Error (MSE) and Hiding Capacity as performance parameters to measure the quality of image.

1. **MSE:** It is defined as square of error between cover & stego image. The error indicates the distortion in an image. MSE can be calculated by using 2-D mathematical equation described as follows:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

Where I(i,j) = The value of pixel in cover image
K(i,j) = The value of pixel in stego image
N=Size of image

2. **PSNR**: It is measure of quality of image. PSNR can be calculated by using mathematical equation given below:

$$PSNR = 10.\log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

$$= 20.\log_{10}\left(\frac{MAX_I}{MSE}\right)$$

3. **Capacity:** Steganographic capacity is the maximum no of bits that can be embedded in a cover image with a negligible probability of detection by an adversary [11]. It is the size of the data in a cover image that can be modified without deteriorating the integrity of the cover image. The steganographic embedding operation needs to preserve the statistical properties of the cover image in addition to its perceptual quality. Capacity is represented by bits per pixel (bpp) and the Maximum Hiding Capacity (MHC) in terms of percentage.

6. CONCLUSION

Stegnography is a process used for the security of data. The message to be secured is embedded in the cover file which can either be text, image or audio file. In stegnography, LSB technique is applied in spatial domain to embed data in cover file.

LSB is easy and commonly used technique. Future work can be done to improve this technique by embedding the message into other bits except MSB to enhance the security. The security can be measured in terms of PSNR, MSE and capacity in bits per pixel.

Refernces:

1. Mohammad Pooyan, Ahmad Delforouzi “LSB-based Audio Steganography Method Based on Lifting Wavelet Transform” International Symposium on Signal Processing and Information Technology, PP.600-603,2007 IEEE

2. Bhagyashri A. Patil, Vrishali A. Chakkarwar “Review of an Improved Audio Steganographic Technique over LSB through Random Based Approach” IOSR Journal of Computer Engineering Volume 9, Issue 1 (Jan. - Feb. 2013), PP 30-34

3. Robert Krenn, "Steganography and steganalysis", An Article, January 2004.

4. Jayaram P, Ranganatha H R, Anupama H S "Information hiding using audio steganography – a survey" The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011

5. R.A. Santosa and P. Bao, "Audio-to-image wavelet transform based audio steganography," Proc. Of 47th Int Symposium ELMAR, June 2005, pp. 209- 212.

6. W. Bender, W. Butera, D. Gruhl, R. Hwang, F. J. Paiz, S. Pogreb, "Techniques For Data Hiding", IBM Systems Journal, Volume 39 , Issue 3-4, July 2000, pp. 547 – 568.

7. Shaveta Mahajan, Arpinder Singh "A Review of Methods and Approach for Secure Stegnography" International journal of advanced research in computer science and software engineering Volume 2, Issue 10, October 2012

8. Haz Malik, Steganalysis of qim steganography using irregularity measure, Proc. of the 10th ACM workshop on Multimedia and security, ACM Press, pp. 149-158, 2008.

9. Shilpa gupta, geeta gujral and neha aggarwal "Enhanced least significant bit algorithm for image steganography" ijcem international journal of computational engineering & management, vol. 15 issue 4, july 2012

10. 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)

11. Neha Batra, Pooja Kaushik, "Implementation of Modified 16×16 Quantization Table Steganography on Colour Images", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue10,October2012.