ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

A Review on Enhancement Information Hiding using LSB Technique

Brijesh Kumar[1], M.S.Dagar[2]

M.Tech, Student, Department of Computer Science and Engineering, Shri Ram College of Engineering and Management, Palwal, Affiliated to Maharishi Dayanand University, Rohtak (Haryana), India[1]

Assistant Professor, Department of Computer Science and Engineering, Shri Ram College of Engineering and Management, Palwal, Affiliated to Maharishi Dayanand University, Rohtak (Haryana), India[2]

ABSTRACT: The purpose of this tutorial is to present an overview of various information hiding techniques. A brief history of steganography is provided along with techniques that were used to hide information. This paper also deals with image steganography security issues, like complexity, and general overview of cryptography and digital watermarking approaches. Also it provides deepness discussions of stenographic algorithms like Least Significant Bit (LSB) algorithm. It also compares those algorithms in terms of speed, accuracy and security to enhance the concept of steganography. It also offers a chance to put the theory into practice by way of a piece of software designed to maximize learning in the fields. This paper gives a brief idea about the image steganography that make use of Least Significant Bit (LSB) algorithm for hiding the data into image.

KEYWORDS: LSB Technique, Steganography, Cryptography, Stego key.

I. INTRODUCTION

One of the reasons that intruders can be successful is that most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of steganography. Steganography is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exist. Steganography supports different types of digital formats that are used for hiding the data. These files are known as carriers. Depending upon the redundancy of the object, suitable formats are used. Redundancy is the process of providing better accuracy for the object that is used for display by the bits of object. The main file formats that are used for steganography are Text, images, audio and video. Steganography is also used for the less dramatic purpose of watermarking. The applications of watermarking mainly involve the protection of intellectual
property such as ownership protection, file duplication management, document authentication (by inserting an appropriate digital signature) and file annotation. A larger part of steganalysis works published so far deals with gray scale and color images. We consider a less explored area of binary image steganography, which becomes more and more important for electronic publishers, distribution, management of printed documents and electronic libraries. Note that there are two aspects of steganalysis. The first relates to the attempt to break or attack a steganography; the second uses it as an effective way of evaluating and measuring steganography security performance. In particular, we aim to carry out different levels of analysis to extract the relevant secret parameters. Steganography is an alternative method for privacy and security. Instead of encrypting, we can hide the messages in other innocuous looking medium (carrier) so that their existence is not revealed. Clearly, the goal of cryptography is to protect the content of messages, steganography is to hide the existence of messages. An advantage of steganography is that it can be employed to secretly transmit messages without the fact of the transmission being discovered. Often, cryptography and steganography are used together to achieve higher security.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

TYPE OF STEGANOGRAPHY

There are 4 different types of steganography

1. Text
2. Image
3. Audio
4. Video

- Text steganography using digital files is not used very often since text files have a very small amount of redundant data. Audio/Video steganography is very complex in use.
- Image steganography is widely used for hiding process of data. Because it is quite simple and secure way to transfer the information over the internet. Image steganography has following types:

Transform Domain

1) Jpeg
2) Spread Spectrum
3) Patch Work

Image Domain

1) LSB and MSB in BMP
2) LSB and MSB in JPG

II. LITRATURE REVIEW

One of the important requirements for LSB based steganography is maximizing the embedding capacity for each pixel. In maintaining image fidelity, the new model for image steganography is proposed on six LSB embedding given by Y.K. Lee and L.H. Chen [3]. Minimum four bits must be used for message hiding in each pixel of a gray-scale image. To achieve this message hiding three components are provided. First, the full message hiding capacity of each pixel is done according to their contrast characteristics. In the second method, to find a gray-scale to the nearest point the minimum error replacement method is adapted. The Steganography system given by M.S. Sutaone and M.V. Khandare [4], is to decode and encode any secret file from an image file using LSB embedding technique from where the secret information has been spread out randomly. This is possible with the usage of a secret key which is helpful in creating fake random numbers in helping to give out the chronology of the hidden message. A new Steganography technique with allowable modifications {-2, -1, 0, +1, +2} where the message is hidden in LSB bits in the triple layered construction is proposed by Xinpeng Zhang [5]. The cover samples to be modified are located while hiding information into the LSB. MamtaJuneja and Parvinder Singh Sandhu [6] have given a robust image Steganography method based on LSB substitution and Rivest, Shamir and Adleman (RSA) encryption techniques. For user's library based on their suitability as cover objects for some data, this paper ranks images in user's library. Xiao Yi Yu and Aiming Wang [7] proposed a new LSB steganography technique which tries to win over statistical steganalysis. For statistical detection the hiding distortion introduced to cover object is limited. This modified image pixel values for hiding is like normal image processing which easily resists all types of LSB steganalysis attacks like Chi-Square test, Optimal estimation attack etc. Hash value of the image pixels represents the secret information. C.C. Chang *et al* [8] proposed an adaptive method to the LSB insertion method. Their prime motto is to give the Correlation between adjacent pixels in estimating the intensity of smoothness. The choice of having two, three or four sided matches was discussed and the payload is high. H.C. Wu *et al* [9] proposed a new steganography technique depending on Pixel Value Differencing (PVD) and LSB replacement to give raise to an imperceptible stego-image quality, so as to increase the hiding capacity of the secret information. An alternate value from two sequential pixels by using the PVD strategy is achieved. A new polynomial-based image sharing method with two achievements was proposed by Z. Eslami and J. ZarepourAhmadabadi [10]. The block size is dynamically determined depending on the size of embedded secret information and the size of the cover images is used for information embedding. A new steganographic scheme based on the old and top numerical model was proposed by S. Geetha*et al* [11]. In this scheme, the embedded data is divided into numerals, each having variable information carrying capacity. The proposed method provides a clear visual quality apart from high payload capacity. The generated stego images get least perceptual distortion apart from high payload capacity

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

III. INFORMATION HIDING TECHNIQUES

Over the past few years, numerous steganography techniques that embed hidden messages in multimedia objects have been proposed [9]. There have been many techniques for hiding information or messages in images in such a manner that the alterations made to the image are perceptually indiscernible. Common approaches are include [10].

III.I. **Least significant bits (LSB)insertion:** It is a simple approach to embedding information in image file. The simplest steganography 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. For e.g.

Pixels:	(00100111 11101001 11001000)
	(00100111 11001000 11101001)
	(11001000 00100111 11101001)
A:	01000001
Result:	(00100110 11101001 11001000)
	(00100110 11001000 11101000)
	(11001000 00100111 11101001)

III.II. **Masking and filtering techniques:** It usually restricted to 24 bits and gray scale images, hide information by marking an image, in a manner similar to paper watermarks. The techniques performs analysis of the image, thus embed the information in significant areas so that the hidden message is more integral to the cover image than just hiding it in the noise level.

III.III. **Transform techniques**: It embeds the message by modulating coefficients in a transform domain, such as the Discrete Cosine Transform (DCT) used in JPEG compression, Discrete Fourier Transform, or Wavelet Transform. These methods hide messages in significant areas of the cover-image, which make them more robust to attack. Transformations can be applied over the entire image, to block throughout the image, or other variants.
Info Hide can enhance confidentiality of information and provides a means of communicating privately. We have also presented an image stenographic system using LSB approach. However, there are some advantages and disadvantages of implementing LSB on a digital image as a carrier. All these are defined based on the perceptual transparency, hiding capacity, robustness and tamper resistance of the method. In future, we will attempt another two approaches of stenographic system on a digital image. This will lead us to define the best approach of steganography to hide information.

IV. PROPOSED WORK

Least significant bits (LSB) insertion is a simple approach to embedding information in image file. The simplest stenographic 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.

IV.I.**Secure Information Hiding System (SIHS):** An information hiding system has been developed for confidentiality. However, in this paper, we study an image file as a carrier to hide message. Therefore, the carrier will be known as cover-image, while the stego-object known as stego-image. The implementation of system will only focus on Least Significant Bit (LSB) as one of the steganography techniques as mentioned in previous section 2For embedding the data into an image, we require two important files. The first is the original image so called cover-image. The image (Figure 4), which in and gif format will hold the hidden information. The second file is the message itself,

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

which is the information to be hidden in the image. In this process, we decided to use a plaintext as the message. Before embedding process, the size of image and the message must be defined by the system. This is important to ensure the image can support the message to be embedded. The ideal image size is 800x600 pixels, which can embed up to 60kB messages.

The cover-image will be combined with the message. This will produce the output called stego-image. Figure 2.1 is illustrated the process. The Stego-image seems identical to the cover-image. However, there are hidden message that imperceptible. This process simply embedded the message into the cover-image without supplied any password or stego-key. At this stage, we decided to do so because we have to understand the ways of LSB insert the message bit into the image and extract the message from the stego-image produced.

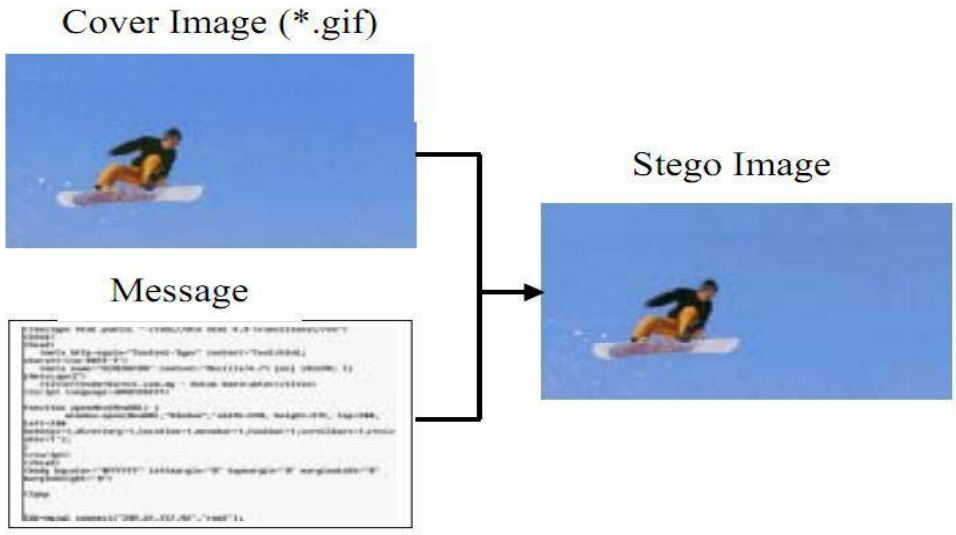
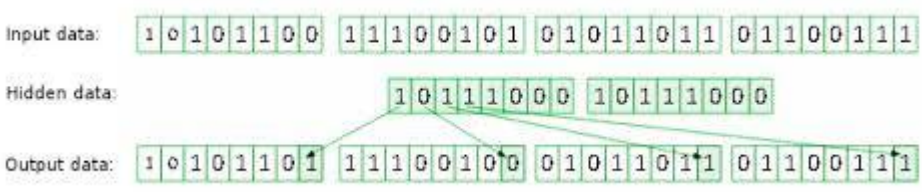


Figure IV. (a): Producing Stego-Image Process.

To illustrate this we are giving an example how to insert information in to an image. Basically an image is a matrix so in simple form we are inserting information in to an matrix. The under given example will show how to insert information into matrix.

Least Significant Bit (LSB) embedding is a simple strategy to implement Info Hide. Like all stenographic methods, it embeds the data into the cover so that it cannot be detected by a casual observer. The technique works by replacing some of the information in a given pixel with information from the data in the image. While it is possible to embed data into an image on any bit-plane, LSB embedding is performed on the least significant bit(s). This minimizes the variation in colors that the embedding creates. For example embedding into the least significant bit changes the color value by one.Embedding into the second bit-plane can change the color value by 2. If embedding is performed on the least significant two pixels, the result is that a color in the cover can be any of four colors after embedding.



Following steps are implemented for the LSB insertion:

1. Read the container file and the text byte to byte.
2. Replace the LSB of the source file with the text bit.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

3. Store the resultant byte in the steganographed file.

Following steps are implemented for the retrieval of data from a file:-

1. Read the source file byte to byte.
2. Collect the LSB of every byte.
3. Combine the LSB's to retrieve back the hidden data.

- **Algorithm for Concealing messages (Sender Side)**

Input: message, cover image

Output: stego image (containing message)

1. store location of image where message to be hidden
2. Insert the message
3. Encrypt the entered message
4. Convert the encrypted message to unsigned integer form
5. Find the length of the message inserted
6. Now convert it in to binary form
7. Store the message in a one row matrix
8. Store the message length in a predefined position of image
9. Now insert the binary format message in to image
10. Save the image
11. End

IV.II. **Extracting Message:** The same stego key is used for decoding of secret message from the stego image. The stego key is used to generate the same random number with which selection of the pixels is done and the order of block.

- **Algorithm Extraction message (Receiver side)**

Input: stego image(containing message)

Output: hidden message

1. Enter location to start(Stego key)
2. Retrieve the size of the hidden message
3. Retrieve the message by same insertion method
4. Decrypt the retrieved message
5. Display the message

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

6. End

V. CONCLUSION AND FUTURE WORK

The LSB information hiding technique provides an easy way to embed information in images, but the data can be easily decoded. We are using the Least Significant Bit algorithm in this for developing the application which is faster and reliable and compression ratio is moderate compared to other algorithm. The proposed scheme used in this paper encrypts the secret information using stego key before embedding it in the image. Certainly the time complexity of the overall process increases but at the same time the security achieved at this cost is well worth it. This cryptographic scheme can be used for other stenographic techniques also.

In this research work we reviewed many papers on steganography techniques. These papers are good enough and have wide future scope the different security and data hiding techniques are used to implement steganography using LSB, ISB, and MLSB. In further research we are going to use more advance schemes like steganography with some hybrid cryptographic algorithm for enhancing the data security.

REFERENCES

[1] Cachin, "An Information-Theoretic Model for Steganography", in proceeding 2nd Information Hiding Workshop, vol. 1525, pp. 306-318, 1998.
[2] D. Artz, "Digital Steganography: Hiding Data within Data", IEEE Internet Computing, pp. 75-80, May-Jun 2001.
[3] R. Chandramouli, N. Memon, "Analysis of LSB Based Image Steganography Techniques", IEEE pp. 1019-1022, 2001.
[4] Amirthanjan R, Akila R and DeepikaChowdavarapu, "A Comparative Analysis of Image Steganography, International Journal of ComputerApplication, Vol. 2, No. 3, pp. 2-10, 2010.
[5]Bandyopadhyay S K , "An Alternative Approach of Steganography Using Reference Image", International Journal ofAdvancements in Technology, Vol. 1, No. 1, pp. 05-11, 2010.
[6] G. Manikandan, N. Sairam and M. Kamarasan"A Hybrid Approach for Security Enhancement by Compressed Crypto-Stegno Scheme ", Research Journal of Applied Sciences, Engineering and Technology 4(6): 608-614, 2012.
[7] Shabir A. Parah, Javaid A. Sheikh, G.M. Bhat, "Data Hiding in Intermediate Significant Bit Planes, A High Capacity Blind Steganographic Technique", International Conference on Emerging Trends in Science, Engineering and Technology , pp.192-197, July 2012.
[8] Yang, Chunfang, Liu, Fenlin.,Luo, Xiangyang., and Zeng, Ying., "Pixel Group Trace Model-Based Quantitative Stegoanalysis for Multiple Least-Significant Bits Steganography", IEEE Transactions on Information Forensics and Security, Vol. 8, No. 1, January 2013.
[9] Swati Malik, Ajit "Securing Data by Using Cryptography with Steganography" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.
[10 Ishwarjot Singh ,J.P Raina," Advance Scheme for Secret Data Hiding System using Hop field & LSB" International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 7–July 2013.