International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 7 4415 - 4420

Design and Implementation of Image Steganography by using LSB Replacement Algorithm and Pseudo Random Encoding Technique

Ramakrishna Hegde[1]
Dept. of Computer Science & Engineering
SDM Institute Of Technology, Ujire

Dr.Jagadeesha S[2]
Dept. of Electronics & Communication Engineering,
SDM Institute of Technology, Ujire

***Abstract*:** Steganography is the efficient technique to provide secure data transmission over the network, as the number of users increases effectively. The cryptography is also used to provide security to data over network, but transmission of secured message may be detectable to third party. From security point of view, steganography does not allow to detect the presence of hidden secret other than indeed user, over the communication channel. Here we are implementing the image steganograpgy i.e image as the master file or cover media and secrete message can be text messages. This paper presents to provide the transfer of secret data embedded into master file to obtain new image , which is practically indistinguishable from the original image, so that other than the indeed user, cannot detect the presence of the secrete data sent. Here we use the Least Significant Bit (LSB) algorithm and Pseudo Random encoding technique for hiding the secrete data by embedding the secrete data into a master file in sending station and we use reverse process of LSB and Pseudo random encoding techniques during the retrieval of the secrete data from the master file by the intended user. The PSNR of both techniques should be measured as performance characteristics of the steganography and comparing both the techniques.

Keywords: *Steganography, Peak Signal to Noise Ratio, Cover media, Master file, Least Significant Bit*

*****

I. INTRODUCTION

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. Steganography is the art and science of secret communication .It is the practice of encoding/embedding secret information in a manner such that the existence of the information is invisible. The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message it is referred to as stego-media. A stego-key is used for hiding/encoding process to restrict detection or extraction of the embedded data[2]. **Steganography** is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The first recorded use of the term was in 1499 by Johannes Trithemius in his **Steganographia** , a treatise on cryptography and steganography disguised as a book on magic.

As people become aware of the internet day-by-day, the number of users in the network increases considerably thereby, facing more challenges in terms of data storage and transmission over the internet, for example information like account number, password etc. Hence, in order to provide a better security mechanism, we propose a data hiding technique called steganography. In cryptography, the secret message that we send may be easily detectable by the attacker. But in steganography, the secret message is not easily detectable. The persons other than the sender and receiver are not able to view the secret message.

Steganography differs from cryptography[3]

- Steganography Hide the messages inside the Cover medium,Many Carrier formats.
- Breaking of steganography is known as Steganalysis.

Cryptography

- Encrypt the message before sending to the destination, no need of carrier/cover medium.
- Breaking of cryptography is known as Cryptanalysis.

Cryptography is used in many applications. Historically, cryptography was used to assure only secrecy. Wax seals, signatures, and other physical mechanisms were typically used to assure integrity of the media and authenticity of the sender. With the advent of electronic funds transfer, the applications of cryptography for integrity began to surpass its use for secrecy. Electronic cash came into being from cryptography, and the electronic credit card and debit card sprung into widespread use. The advent of public key cryptography introduced the possibility of digital signatures, and other related concepts such as electronic credentials. In the information age, cryptography has become one of the major methods for protection in all applications.

Watermarking and fingerprinting related to steganography are basically used for intellectual property protection. A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. The embedded information in a watermarked object is a signature refers the ownership of the data in order to ensure copyright protection. In fingerprinting, different and specific marks are embedded in the copies of the work that different customers are supposed to get. In this case, it becomes easy for the property owner to find out such customers who give themselves the right to violate their licensing agreement when they illegally transmit the property to other groups [1][4].

II. LITERATURE SURVEY

The basic idea behind the steganography is to hide the secrete data into the carrier file and send it to the other party over the network. The carrier files may be text, image, audio or video. Practically in most of the cases images are taken as the carrier file. Because the digital images are very useful

and secure carrier for hiding the secret massage. Image is a collection of color pixels. In standard, 24 bit bitmap we have three color components per pixel: Red, Green and Blue. Each component is 8 bit and have 256 values. In 3 megapixel image we can hide 9 megabits of information using this technique, which is equivalent of 256 pages of book. If we only change the lowest bits of each pixel, then the numeric values can only change by a small percentage. We can only alter the original pixel color value by ±7. Such a minute alterations in the pixel value does not make any difference in the visibility of the image. The original image and embed image both looks similar to the human eye. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it

For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. The research paper [5] gives an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganographic algorithm and briefly reflects on which steganographic techniques are more suitable for which applications. The paper [6] explains that, Steganography can be a solution which makes it possible to send news and information without being censored and without the fear of the messages being intercepted and traced back to us. It is also possible to simply use steganography to store information on a location. Steganography can also be used to implement watermarking. Although the concept of watermarking is not necessarily steganography, there are several steganographic techniques that are being used to store watermarks in data. Invisible ink has been in use for centuriesfor fun by children and students and for serious undercover work by spies and terrorists [7].

Hiding information into a medium requires following elements [8]

1. The cover medium(C) that will hold the secret message.
2. The secret message (M), may be plain text, digital image file or any type of data.
3. The stegonographic techniques
4. A stego-key (K) may be used to hide and unhide the message.

In modern approach, depending on the cover medium, steganography can be divided into five types: 1. Text Steganography 2. Image Steganography 3. Audio Steganography 4. Video Steganography 5. Protocol steganography.

- **Text steganography** Hiding information in text _le is the most common method of steganography. The method was to hide a secret message into a text message.
- **Image steganography** Images are used as the popular cover medium for steganography. A message is embedded in a digital image using an embedding algorithm, using the secret key.
- **Audio steganography** Audio steganography is concerned with embedding information in an innocuous cover speech in a secure and robust manner. The different methods that are commonly used for audio steganography are LSB coding, Parity coding, Phase coding, Spread spectrum, Echo hiding.
- **Video steganography** Video Steganography is a technique to hide any kind of files in any extension into a carrying Video file.
- **Protocol steganography** The term protocol steganography is to embedding information within network protocols such as TCP/IP. We hide information in the header of a TCP/IP packet in some fields that can be either optional or are never used. [9].

III. METHODOLOGY

3.1 Network[14].

A Network is a set of devices (often referred to as nodes) connected by media links. A node can be a computer capable of sending and/or receiving data generated by other nodes on the network. The links connecting these nodes are often called communication Channels. Here we use computer network as a platform where we transfer the stego files. Computer network is allow to exchange the data between the terminals.

3.2 Least Significant Bit (LSB) Techniques[15]

The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. Digital images are mainly of two types (i) 24 bit images and (ii) 8 bit images. In 24 bit images we can embed three bits of information in each pixel, one in each LSB position of the three eight bit values. Increasing or decreasing the value by changing the LSB does not change the appearance of the image; much so the resultant stego image looks almost same as the cover image. In 8 bit images, one bit of information can be hidden. A stego-image is obtained by applying LSB algorithm on both the cover and hidden images. The hidden image is extracted from the stego-image by applying the reverse process[10]. If the LSB of the pixel value of cover image C(i,j) is equal to the message bit m of secret massage to be embedded, C(i,j) remain unchanged; if not, set the LSB of C(i, j) to m. The message embedding procedure is given below-

$S(i,j) = C(i,j) - 1$, if $LSB(C(i,j)) = 1$ and $m = 0$

 ISSN: 2321-8169
4415 - 4420

S(i.j) = C(i,j), if LSB(C(i,j)) = m

S(i,j) = C(i,j) + 1, if LSB(C(i,j)) = 0 and m = 1
where LSB(C(i, j)) stands for the LSB of cover image C(i,j) and m is the next message bit to be embedded. S(i,j) is the stego image. As we already know each pixel is made up of three bytes consisting of either a 1 or a 0.
For example, suppose one can hide a message in three pixels of an image (24-bit colors). Suppose the original 3 pixels are
(11101010 11101000 11001011)
(01100110 11001010 11101000)
(11001001 00100101 11101001)

A steganographic program could hide the letter "J" which has a position 74 into ASCII character set and have a binary representation "01001010", by altering the channel bits of pixels.

(11101010 11101001 11001010)
(01100110 11001011 11101000)
(11001001 00100100 11101001)

In this case, only four bits needed to be changed to insert the character successfully. The resulting changes that are made to the least significant bits are too small to be recognized by the human eye, so the message is effectively hidden. The advantage of LSB embedding is its simplicity and many techniques use these methods [10]. LSB embedding also allows high perceptual transparency.

3.2.1 LSB insertion algorithm

Step1:The first character of the data to be hidden is taken and represented in binary format.

Step2: Next the first pixel value of the video is taken and represented in binary format.

Step3:The converted data is extracted bit by bit From the least bit. (i. e the order of left to right)

Step4: For each bit we are appending or prefixing zeros to make it a 1 byte.

Step5: After appending the zeros, if the v alue of that byte is 0, then we represent it as 2 (i.e. change the value to 2), if its 1 then we don't do any changes.

Step6: Next we take the pixel value if the pixel value is 255 or 256 then we subtract the value of the data with the pixels. If not then we add.

3.2.2 LSB Extraction algorithm (Reverse LSB)

Step1: The first value of the keyfile and the first pixel value of the steganographed video file are taken.

Step2: Next we subtract the two values that are extracted and store it in a temp array.

Step3: Step 1 and step 2 is repeated till the end of the file.

Step4: The temp file is opened and then every continuous 8 bytes are taken and they are clubbed to make them as 1 byte using the left shift operator.

Step5: The extracted byte is converted into character format and stored in a data file

Figure 3.2.1 and 3.2.2 explains the LSB insertion and LSB extraction mechanisms..

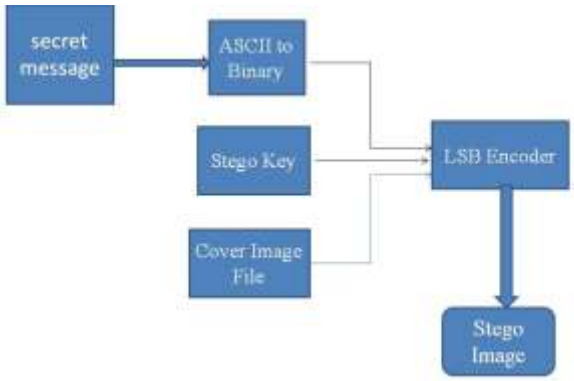

Figure 3.2.1 LSB Insertion Mechanism

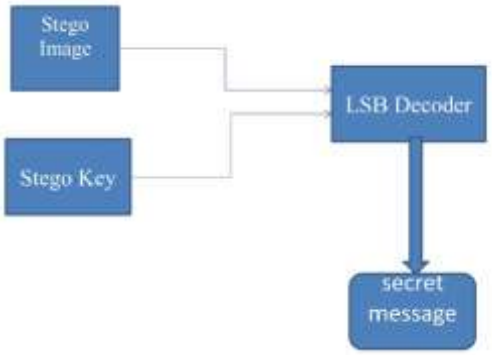

Figure 3.2.2 LSB Extraction Mechanism.

3.3. Pseudo Random Encoding Technique

In this method to choose the pixel randomly and embed the message, random key is used. This method makes it difficult to find the secrete message bits and reduces the realization of the pattern in the image[11]. Data can be hidden in the LSB of a particular colour plane (Red plane) of the randomly selected pixel in the RGB colour space[12].

3.3.1 Embedding Algorithms

In this technique, to randomized the cover image, random key is used and then hides the secrete bit of the message into the cover image using least significant bit method. Stego key

and random key is shared by transmitting and receiving ends. The random-key is usually used to seed a pseudo-random number generator to select pixel locations in an image for embedding the secret message.
Input : Cover Image, Secrete message and stego key
Ouput: Stego image

1) Read character from text file that is to be hidden and convert the ASCII value of the character into equivalent binary value into an 8 bit integer array.
2) Read the RGB colour image(cover image) into which the message is to be embedded.
3) Read the last bit of red pixel.
4) Initialize the random key and Randomly permute The pixels of cover image and reshape into a matrix.
5) Initialize the stego-key and XOR with text file to be hidden and give message.
6) Insert the bits of the secret message to the LSB of the Red plane's pixels.
7) Write the above pixel to Stego Image File.

3.3.2 Extraction of the Hidden message

In this process of extraction, the process first takes the key and then random-key. These keys takes out the points of the LSB where the secret message is randomly distributed [13]. Decoding process searches the hidden bits of a secret message into the least signi_cant bit of the pixels within a cover image using the random key.
In decoding algorithm the random-key must match i.e. the random-key which was used in encoding should match because the random key sets the hiding points of the message in case of encoding. Then receiver can extract the embedded messages exactly using only the stego-key.

3.3.3 Message Extraction Algorithm[16]

Input : Stego Image file, Stego-key and random-key
Output : Secrete Message

1) Open the Stego image file in read mode and from the Image file, read the RGB colour of each pixel.
2) Extract the red component of the host image.
3) Read the last bit of each pixel.
4) Initialize the random-key that gives the position of the message bits in the red pixel that are embedded randomly.
5) For decoding, select the pixels and Extract the LSB value of red pixels.
6) Read each of pixels then content of the array Converts into decimal value that is actually ASCII value of hidden character.
7) ASCII values got from above is XOR with stego-key and gives message file, which we hide inside the cover image.

IV. EXPERIMENTAL RESULTS

4.1 Performance Analysis

As a performance measure for image distortion due to hiding of message, the well-known peak-signal-to noise ratio (PSNR), which is categorized under difference distortion metrics, can be applied to stego images. It is defined as:

$PSNR = 10\log (Cmax)^2 / MSE.$

MSE = mean - square – error,
which is given as:
$MSE = 1 / MN((S-C)^{2.}$
Cmax = 255.
Where M and N are the dimensions of the image, S is the resultant stego-image, and C is the cover image.

PSNR values below 30 dB indicate low quality (i.e., distortion caused by embedding is high). A high-quality stego image should strive for a PSNR of 40 dB, or higher.

There are several parameters are used to measure the performances and some of them are explained below.

Perceptibility: It does embedding information distort cover medium to a visually unacceptable level.

Capacity: How much secrete data can be hidden.

Robustness to attacks: It is attack on the stego medium in an effort to destroy, remove, or change the embedded data.

Table 4.1 Comparison of the characteristics in the above two techniques.

Technique	Imperceptibility	Capacity	Robustness
LSB algorithm	High*	High	Low
Pseudo Random Encoding	High*	High	High

***** Indicates depends on the used cover image.

Figure 4.1 Grey Scale Image (Cover media)

 ISSN: 2321-8169
4415 - 4420

Figure 4.2 RGB Image. (Cover media)

We consider grey scale and RGB image as cover media (before the embedding of the secrete message) as shown in figure 4.1 and 4.2 respectively. Text file / image taken as secrete message for both the techniques. Figure 4.3 and Figure 4.4 are the grey scale image with text file and RGB image with text file respectively. By referring the Figures from 4.1 to 4.4, we notice that human eyes cannot distinguish images before embedding the secrete message and after embedding the secrete message.

Figure 4.3 Grey Scale image with text file

Figure 4.4 RGB image with text file

Table 4.2. PSNR of Least Significant bits technique

Sl. No	Cover Image	Secrete Message	Stego Image	SNR (dB)	MSE	PSNR (dB)
1	Grey Image	Text file	Grey Images	60.534	0.045	61.80
2	RGB Image	Text file	Images	62.098	0.012	68.25
3	RGB Image	Image	Images	54.027	0.094	58.67

Table 4.3 PSNR of Pseudo Random Encoding technique.

Sl. No	Cover Image	Secrete Message	Stego Image	SNR (dB)	MSE	PSNR (dB)
1	Grey Image	Text file	Grey Image	60.734	0.045	62.10
2	RGB Image	Text file	Images	62.198	0.012	69.35
3	RGB Image	Image	Images	54.227	0.094	59.67

It is possible to embed more secrete information into the RGB image compare to the grey scale images. PSNR of RGB image with text file as secrete message is more than the grey scale image with text file and distortion rate is also less in RGB images. Since RGB image is better in terms of quality , PSNR is also higher compare to the grey image.

V. CONCLUSION

Steganography transmits secrets through apparently innocuous covers in an effort to conceal the existence of a secret. In areas where cryptography and strong encryption are being outlawed, citizens are looking at steganography to circumvent such policies and pass messages covertly. Steganography might also become limited under laws, since governments already claimed that criminals use these techniques to communicate. In this project we have used steganography and cryptography both.

In this paper, we have used Least Significant Bit (LSB) algorithm and Pseudo Random encoding technique for steganography. The secrete text message is embedded successfully with the master file (carrier file) and transmitted to intended user. Image or video file or audio file can be used as master file. And also we successfully embedded the data file with the master file and transmitted to intended party. The secrete text message or secrete data file is retrieved back by the intended user from the master file. The negligible changes in the master file after embedding the secrete text message or secrete data file (stego file) cannot identify by the human beings. Our results shows that PSNR of Pseudo Random technique is better than the LSB technique and PSNR of both techniques are above 60 dB i..e superior image quality and also distortion rate is reduced. A high-quality stego image should strive for a PSNR of 40 dB and here by using both techniques, we have achieved PSNR more than 60 dB.

REFERENCE

[1] R.Anderson and F. Petitcolas, "On the limits of steganography" IEEE Journal of Selected Areas in Communications, Vol. 16, No. 4, May 1998.

[2] Niels Provos, Peter Honeyman, "Hide and Seek: An Introduction to Steganography," IEEE computer society,2003.

[3] Hiding data in images by simple LSB substitution by Chi-Kwong Chan, L.M. Cheng Department of Computer Engineering and Information Technology, City University of Hong Kong, Hong Kong Received 17 May 2002.

[4] Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, "Hiding data in images by optimal moderately significant-bit replacement" IEE Electron. Lett. 36 (25) (2000) 20692070.

[5] T. Morkel 1, J.H.P. Eloff 2, M.S. Olivier 'AN OVERVIEW OF IMAGE STEGANOGRAPHY', Information and Computer Security Architecture (ICSA) Research Group. Department of Computer Science, University of Pretoria, 0002, Pretoria, South Africa.

[6] Arvind Kumar Km. ' Steganography- the data hiding technique', International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010.

[7] "A Tutorial Review on Steganography" by Samir K Bandyopadhyay , Debnath Bhattacharyya1, Debashis Ganguly1, Swarnendu Mukherjee1 and Poulami Das, Heritage Institute of Technology.

[8] Niels Provos, Peter Honeyman, " Hide and Seek: An Introduction to Steganography," IEEE computer society,2003.

[9] Pratap Chandra Mandal Asst. Prof., Department of Computer Application B.P.Poddar Institute of Management Technology . "Modern Steganographic technique: A Survey" , International Journal of Computer Science Engineering Technology (IJCSET).

[10] A. Cheddad, J. Condell, K. Curran and P.M. Kevitt. (2010). "Digital image steganography: survey and analysis of current methods." Signal Processing Journal.

[11] A Tutorial Review on Steganography" by Samir K Bandyopadhyay, Debnath Bhattacharyya1, Debashis Ganguly1, Swarnendu Mukherjee1 and Poulami Das, Heritage Institute of Technology.

[12] International journal of computer engineering technology (ijcet) "steganography based on random pixel selection for efficient data hiding'.Shamim Ahmed Laskar and Kattamanchi Hemachandran (Research Scholar, Department of Computer Science, Assam University).

[13] Journal of Theoretical and Applied Information Technology 15th February 2012. Vol. 36 No.1. A steganography algorithm for hiding image in Image by improved lsb substitution by minimize Detection by vijay kumar sharma, 2vishal shrivastava M.Tech. scholar, Arya college of Engineering IT, Jaipur , Rajasthan (India).

[14] http://www.studytonight.com/computer-networks/overview-of-computer-networks

[15] "http://www.ijarcce.com/upload/2014/august/IJARCCE3I%20a%20p%20anu%20A%20Secured%20Communication%20Based%20on%20Adaptive%20Steganography.pdf "

[16] Shamim Ahmed Laskar 1 and Kattamanchi Hemachandran," INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING & TECHNOLOGY (IJCET)" Volume 4, Issue 2, March – April (2013), pp. 31-44