An Enhanced Method for Least Significant Bit Image Steganography using Discrete Logarithmic Dispersion Strategy

Sreeparna Ganguly
M.Tech. Student, Dept. of CSE
JIS College of Engineering

Pranati Rakshit
Asst. Prof., Dept. of CSE
JIS College of Engineering

ABSTRACT

In this paper a novel method for information security using image steganography technique is proposed. This project simply hides a text message in an image file. 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. 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. This work intends to give an overview of image steganography, its uses and techniques. The proposed method uses the LSB (Least Significant Bit) technique to hide information in the cover image. The system enhanced the LSB technique by randomly dispersing the bits of the message in the image and thus making it harder for unauthorized people to extract the original image. Discrete logarithm calculation technique is used for determining the location of the bit into pixel to embed the message. The proposed algorithm provides a stego-key that will be used during the embedding and extracting of the message.

General Terms

Image Steganography

Keywords

Information security, Steganography, Discrete logarithmic dispersion

1. INTRODUCTION

Steganography is defined as the art and science of writing hidden messages in such a way that no one else, apart from the intended recipient knows the existence of the message. The word "steganography" is basically of Greek origin which means "hidden writing". The word is classified into two parts: "steganos" which means "secret" and "graphic" which means "writing". However, in hiding information, the meaning of steganography is hiding text or secret messages into another media file such as image, text, sound or video. The word "steganography" is often considered similar to "cryptography" and "watermarking". Whilst watermarking ensures message integrity and cryptography scrambles the message, steganography hides it. The primary objective of steganography is to avoid drawing attention to the transmission of hidden information. If suspicion is raised, then this objective that has been planned to achieve the security of the secret message because if the hackers noted any change in the sent message then this observer will try to know the hidden information inside the message.

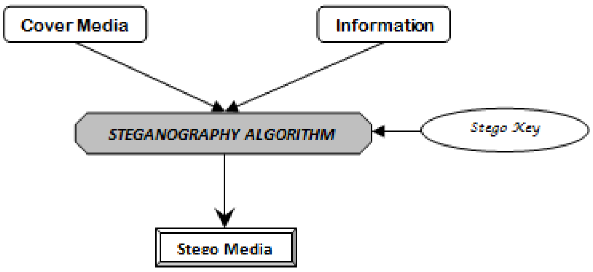


Fig 1: Basic Steganography Technique

The basic terminologies used in the steganography systems are: the cover message, secret message, the secret key and embedding algorithm. The cover message is the carrier of the message such as image, video, audio, text or some other digital media. The secret message is the information which is needed to be hidden in the suitable digital media.

1.1 Different kinds of Steganography

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. The below figure shows the four main categories of file formats that can be used for steganography.

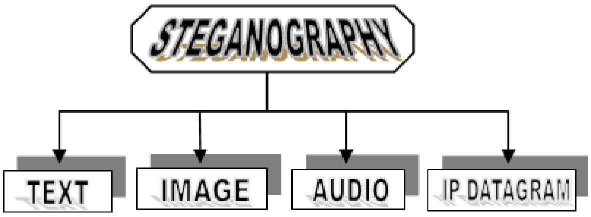


Fig 2: Different types of Steganography

1.2 Image Steganography

The most widely used technique today is hiding of secret messages into a digital image. This steganography technique exploits the weakness of the human visual system (HVS). HVS cannot detect the variation in luminance of color vectors at higher frequency side of the visual spectrum. A picture can be represented by a collection of color pixels. The individual pixels can be represented by their optical characteristics like 'brightness', 'chroma' etc. Each of these characteristics can be digitally expressed in terms of 1s and 0s. The proposed method comprehends the following objectives:

i) To generate a series of random numbers from the stego-key using Discrete Logarithm Algorithm

ii) To produce security tool based on steganographic techniques.

For example: a 24-bit bitmap will have 8 bits, representing each of the three color values (red, green, and blue) at each pixel. If we consider just the blue there will be 2^8 different values of blue. The difference between 11111111 and 11111110 in the value for blue intensity is likely to be undetectable by the human eye. Hence, if the terminal recipient of the data is nothing but human visual system (HVS) then the Least Significant Bit (LSB) can be used for something else other than color information.

2. LITERATURE REVIEW

Lots of work has been done in the field of LSB steganography. In [1] an improvement of LSB steganographic method has been suggested by randomly embedding the bits of the message in the image to produce more secure system. The proposed system goal is giving more the complexity to cryptosystems and the execution time does not differ great than the original methods then the hide the messages encrypted inside image in a way that does not allow any Attacker to even detect that there is secret message.

This paper provides a general overview of the following subject areas: historical cases and examples using steganography, how steganography works, what steganography software is commercially available and what data types are supported, what methods and automated tools are available to aide computer forensic investigators and information security professionals in detecting the use of steganography, after detection has occurred, can the embedded message be reliably extracted, can the embedded data be separated from the carrier revealing the original file, and finally, what are some methods to defeat the use of steganography even if it cannot be reliably detected [2].

This paper focuses on the Least Significant Bit (LSB) technique in hiding messages in an image. The system enhanced the LSB technique by randomly dispersing the bits of the message in the image and thus making it harder for unauthorized people to extract the original message [3].

The model proposed by this paper combines cryptography, steganography (taken as security layers) and along with that an extra layer of security has been imposed in between them. This newly introduced extra layer of security changes the format of normal encrypted message and the security layer followed by it embeds the encrypted message behind a multimedia cover object. [4]

In this paper we take a look to the existent methods used for embedding information into a large variety of document types: document images, audio files, image files, binary files [5].

This paper focuses on an enhanced algorithm of LSB which uses the least two significant bits of one of the channels to indicate existence of data in the other two channels [6].

Ming at, el. 2006 has made a small survey that classifies current steganography tools, according to his survey, there are many information hiding methods. Some of these are **substitution methods**, **transform methods**, and other miscellaneous methods.

Substitution methods are based on the modification of least significant bits of the cover image using the secret data and some key based random permutations. **Transform methods** are based on modification or rearrangement of transforming domain (discrete cosine, Fourier, wavelet) coefficients with secret data and some set of rules about the coefficients. Other miscellaneous methods use techniques such as **fractals, matrix decomposition** and **predictive quantization**. Some well-known steganology methodologies are the Least Significant Bit (LSB) Hiding, Regional Hiding with Segmentation (RHS) and SCAN Hiding (SH) [7].

An important point to note is that both steganography and cryptography provide secure communications and may be used concurrently. Steganography and cryptography differ in execution. In cryptography, the secret message which is the transmitted file itself cannot be recovered without the secret key; however, the encrypted file is identified as being sent. It helps to protect confidentiality but protection vanishes after decryption. In steganography the existence of the stego message is concealed in a cover file in a way that does not allow an enemy to observe that there is a message present. The stego message can be extracted with stego key as long as the stego file is identified by which embedding method is used [8].

In LSB coding, the ideal data transmission rate is 1 kbps per kHz. In some implementations of LSB coding, however, the two least significant bits of a sample are replaced with two message bits. This increases the amount of data that can be encoded but also increases the amount of resulting noise in the audio file as well. Thus, one should consider the signal content before deciding on the LSB operation to use. For example, a sound file that was recorded in a bustling subway station would mask low-bit encoding noise. On the other hand, the same noise would be audible in a sound file containing a piano solo [9].

Wang H. & Wang S. defined the **disadvantage of this method** according to the risk of detection, which is happened in the process of hiding data within the image. Therefore, the beginning of series detects storage is much possible to know the rest of the string. The reason behind the popularity of this method according to their explanation is due to the relative easiness to implement the LSB. In order to hide a secrete message inside an image, a proper cover is needed. However, this method uses bits of each pixel in the image, when using a 24 bit color image, and in this method a bit of each of the red and green and blue color component can be used. Therefore, a total of three bits can be stored in each pixel. Thus, an 800 × 600 pixel image can contain a total amount of 1.440.000 bits (180.000 bytes) of secret data [10].

3. PROPOSED ALGORITHM

In this paper, LSB (Least Significant Bit) technique is used to hide the messages in images. However, it is decided to enhance the security system by introducing a new technique comprises of randomly dispersing the message bits in images. It is proposed in this enhancement that the embedding of message bits into the image is not only in the least bit but also the other bits in the pixel in the random manner. This can be achieved by comparing the message bit to the pixel bit randomly chosen from third to the last bit. Based on this comparison, 1 is inserted in the least significant bit if the message bit identical to that of the image, whereas, 0 is inserted if the message bit didn’t match with the chosen bit from the image, see figure 3 below:

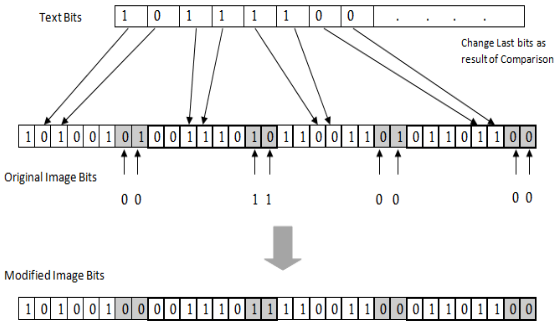
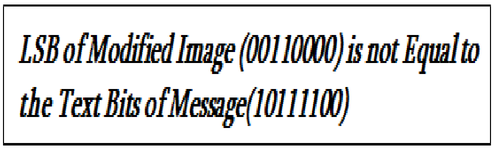


Fig 3: Embed the bits in image

It is interesting to note that the value of the least significant bit of the image is not always representing the actual value of that from the message, as expressed in the following Table 1:

Table 1: Comparison between the message with the image bit



LSB of Modified Image (00110000) is not Equal to the Text Bits of Message(10111100)

Table 2: Change in the Bits during the process of Embedding

Random Bit (1-5)	Next Bit of Random Bit(2-6)	Bit of Message	Next Bit of Message	7th Image Bit(Next to Last)	8th Image Bit(Last Bit)
0	0	0	0	1	1
		0	1	1	0
		1	0	0	1
		1	1	0	0
0	1	0	0	1	0
		0	1	1	1
		1	0	0	0
		1	1	0	1
1	0	0	0	0	1
		0	1	0	0
		1	0	1	1
		1	1	1	0
1	1	0	0	0	0
		0	1	0	1
		1	0	1	0
		1	1	1	1

The process of extracting the message from the image includes inverse comparison to that used in embedding. If the least significant bit is 1, then the actual value of the message bit is equal to that compare with image bit value, see figure 4, while if the least bit is zero then the message bit is representing the inverse value of the image bits that used in embedding comparison.

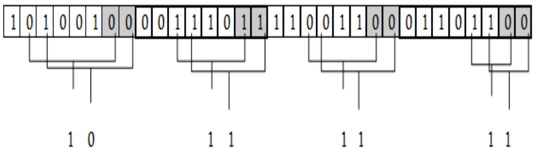


Fig 4: Extract bits from image

Table 3: Change in the Bits during the process of Extraction from image

Random Bit (1-5)	Next Bit of Random Bit(2-6)	7th Image Bit(Next to Last	8th Image Bit(Last Bit)	Value Extracted(nth Bit)	Value Extracted(n+1th Bit)
0	0	0	0	1	1
		0	1	1	0
		1	0	0	1
		1	1	0	0
0	1	0	0	1	0
		0	1	1	1
		1	0	0	0
		1	1	0	1
1	0	0	0	0	1
		0	1	0	0
		1	0	1	1
		1	1	1	0
1	1	0	0	0	0
		0	1	0	1
		1	0	1	0
		1	1	1	1

3.1 Discrete Logarithm Algorithm

Discrete logarithm calculation can be used to solve the sequence-mapping problem. The main idea here is to generate a series of random numbers of length equal to the message length that ranging from 2 to 8. These series numbers will be use in random-mapping.

Here, discrete logarithm algorithm is used to produce random numbers. These numbers depend on the value of key (k).The values are computed from the following equation, and these numbers will be limited to the length of the message, M:

$x_i = a * x_{i-1} \bmod p$ _ _ _ _ (1)

Where,

x_0= is the sum of K digits.

$a = 3 * x_0$

$p = k$

$i = 1,2,3,4 \ldots\ldots m$

The number created from the above equation is then used to generate other numbers ranging from 2 to 8.The latter is used to locate the image bit (in the pixel) that will be used in the comparison with the message bit, as expressed as follow:

$p_i = (x_i \bmod 5) + 1$ _ _ _ _ (2)

The process of stenography by the proposed system is illustrated with corresponding algorithms below. Recovering a message from a stego-image demands the corresponding decoding key, k that is used during the encoding process. Hence, both the sender and receiver have to share the stego-key during the communication. The k key is then used for selecting the positions of the pixel where the secret bits had been embedded.

3.2 Embedding Algorithm

1. Read the RGB cover image.
2. Enter the string.
3. Store length of string in the variable len.
4. Store equivalent 8 bit ASCII value of each character of the string into str[ ] array.
5. Enter the Stego-key.
6. Reserve last two pixels for sending the Stego-key and length of the string.
7. Generate a sequence of random numbers between 1 and 5 using Discrete Logarithm Algorithm.

```
    8.  Embedding will be started from red channel of the 1st pixel (row index 1 and column index 1).
    9.  For i= 1 to (len*8) step 2
    10. Get the random number from the sequence.
    11. Store the bit value of the generated random number position from the current pixel into bitpos_1 variable.
    12. If str[i] == bitpos_1
    13. Set 7th bit of current pixel '1'.
Else
    14. Set 7th bit of current pixel '0'.
End If.
    15. Store the bit value of the (generated random number+1) position from the current pixel into bitpos_2 variable.
    16. If str[i+1] == bitpos_2
    17. Set 8th bit of current pixel '1'.
Else
    18. Set 8th bit of current pixel '0'.
End If
    19. Go to the next channel.
End For
    20. End.
```

3.3 Retrieval Algorithm

```
    1.  Get the stego image.
    2.  Extract the Stego-key and length of the string from the image.
    3.  Store length of the string in the variable len.
    4.  Generate a sequence of random numbers between 1 and 5 using Discrete Logarithm Algorithm.
    5.  Retrieval will be started from red channel of the 1st pixel (row index 1 and column index 1).
    6.  For i= 1 to (len*8) step 2
    7.  Get the random number from the sequence.
    8.  Store the bit value of the generated random number position from the current pixel into bitpos_1 variable.
    9.  If 7th bit of current pixel == bitpos_1
    10. Insert value '1' into retrieve_str[i].
Else
    11. Insert value '0' into retrieve_str[i].
End If
    12. Store the bit value of the (generated random number+1) position from the current pixel into bitpos_2 variable.
    13. If 8th bit of current pixel == bitpos_2
    14. Insert value '1' into retrieve_str[i+1].
Else
    15. Insert value '0' into retrieve_str[i+1].
End If
    16. Go to the Next channel.
End For
    17. Print the extracted string retrieve_str[ ] .
End.
```

4. IMPLEMENTATION AND RESULTS

The proposed algorithm is implemented using uncompressed images of .png format. Instances of execution are shown below. In this example, a 198 x 135 image called 'onion.png', key value 1221 and a message string 'JIS College of Engineering' are used. From figure 5.4 it can be seen that the recovery rate is 100% if cover image is clean and noise-free. If noise is inserted in the cover image, the decrement of recovered message quality will be directly proportional to the error percentage.

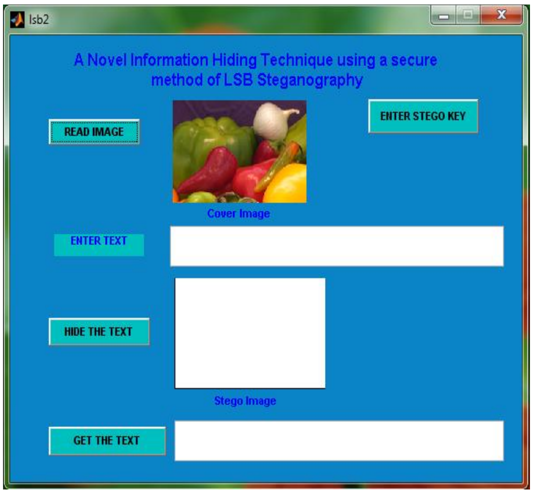
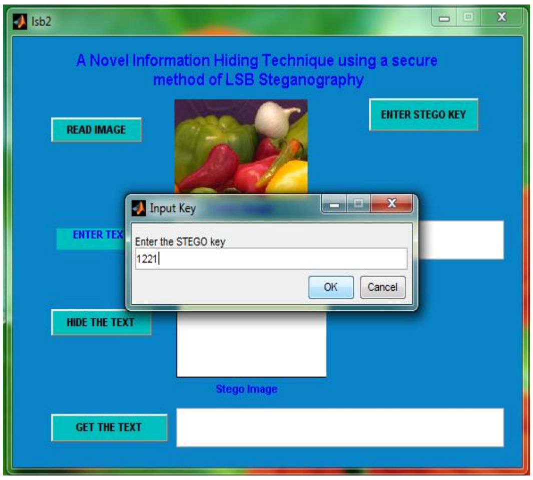
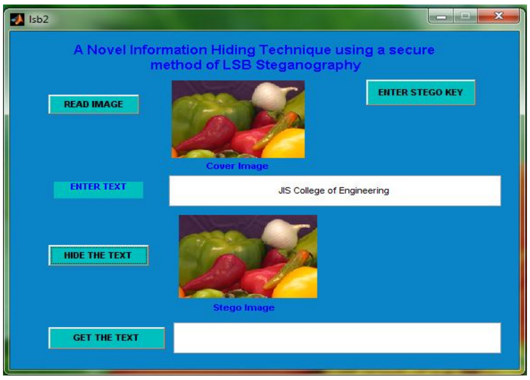


Fig 5.1: Cover Image is taken



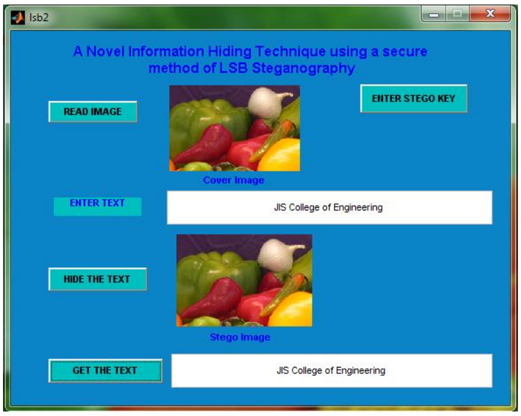
Enter the STEGO key
1221

Fig 5.2: Key value is given for generating pseudo-random dispersion sequence


A Novel Information Hiding Technique using a secure method of LSB Steganography

JIS College of Engineering

Fig 5.3: Text message is hidden with cover image


A Novel Information Hiding Technique using a secure method of LSB Steganography

JIS College of Engineering

JIS College of Engineering

Fig 5.4: Secret message is recovered

Fig 5: Step by Step Implementation Procedure

5. CONCLUSION AND DISCUSSION

In this paper, an enhancement of the image steganography system is devised using LSB approach to provide a means of secure communication. It is proposed in this enhancement that the embedding of message bits into the image is not only in the least bit but also the other bits in the pixel in the random manner. This can be achieved by comparing the message bit to the pixel bit randomly chosen from third to the last bit. Based on this comparison, 1 is inserted in the least significant bit if the message bit identical to that of the image, whereas, 0 is inserted if the message bit didn't match with the chosen bit from the image. The advantage of the proposed method is that the change will not be made to all considered LSB positions of the cover image .Using the proposed method change in the image bits can be minimized. In this proposed method two consecutive message bits have been compared with two consecutive bits in the image pixel. The two LSB values will be determined based on the comparison between the message bits and randomly generated image bits. To improve security discrete logarithm algorithm has been used to generate a sequence of random numbers. Due to this complexity in the process of embedding, it is difficult for an attacker to retrieve the value of the original text without knowing the key; the equation configured to generate random numbers, and the method of embedding. In this way, the system is strengthened using LSB approach to provide a means of secure communication.

The strength of Steganography lies in the sheer amount of information that changes hands every day. It is very simple using digital technology to conceal any given digital information within other information, so virtually anything could contain a hidden meaning. There is no practical way to check it all. However, none of steganography methods we examined could resist a concerted attack if someone knew that there was a message in a given document.

6. REFERENCES

[1] Jassim Mohmmed Ahmed and Zulkarnain Md Ali, **“**Information Hiding using LSB technique” , IJCSNS International 18 Journal of Computer Science and Network Security, VOL.11 No.4, April 2011

[2] Shawn D. Dickman,”An Overview of Steganography**”,** Computer Forensics Term Paper, James Madison University

[3] M. M. Amin, et al., "Information hiding using steganography," in Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference on, 2003, pp. 21-25.

[4] Debnath Bhattacharyya, Poulami Das,Samir Kumar Bandyopadhyay, and Tai-hoon Kim, “Text Steganography: A Novel Approach” International Journal of Advanced Science and TechnologyVol. 3, February, 2009.

[5] Richard Popa “An Analysis of Steganographic Techniques”.

[6] Adnan Gutub, Mahmoud Ankeer, Muhammad Abu-Ghalioun, Abdulrahman Shaheen,Aleem Alvi “Pixel Indicator High Capacity Techniquefor Rgb Image Based Steganography”.

[7] C. Ming, et al., "Analysis of Current Steganography Tools: Classifications & Features," in Intelligent Information Hiding and Multimedia Signal Processing, 2006. IIH-MSP '06. International Conference on, 2006, pp. 384-387.

[8] F. A. P. Peticolas, et al., "Information hiding–a survey," Proceedings of the IEEE, vol. 87, pp. 1062-1078, 1999.

[9] Padmashree G, Venugopala P S ,“International Journal of Engineering and Innovative Technology (IJEIT)” .Volume 2, Issue 4, October Audio Stegnography and Cryptog raphy: Using LSB algorithm at 4th and 5thLSBlayers

[10] R. J. Anderson and F. A. P. Petitcolas, "On the limits of steganography," Selected Areas in Communications, IEEE Journal on, vol. 16, pp. 474-481, 1998.