www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 8 August, 2013 Page No. 2464-2467

A Survey on LSB Based Steganography Methods

M. Pavani[1], S. Naganjaneyulu[2], C. Nagaraju[3]

[1] M. Tech, Information Technology, Lakireddy Bali Reddy College of Engineering, Mylavaram, India
pavani.mtech07@gmail.com

[2] Assoc. Professor, Information Technology, Lakireddy Bali Reddy College of Engineering, Mylavaram, India
svna2198@gmail.com

[3]Professor, Information Technology, YSR College of Engineering, Proddatur, India
nagaraju.c@lbrce.ac.in

Abstract: ***The least significant bit (LSB) based approach is a popular type of steganographic algorithms in the spatial domain. The advantage of LSB is its simplicity to embed the bits of the message directly into the LSB plane of cover-image and many applications use this method. In this paper we try to give an overview of different LSB methods and there advancements.***

Keywords: steganography, least significant bit (LSB), security, steganalysis.

1. Introduction

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message [1]. Due to growing need for security of data image steganography is gaining popularity [2]. The main goal of steganography is to communicate securely in a completely undetectable manner [3] and to avoid drawing suspicion to the transmission of a hidden data [4]. This idea of data hiding is not a novelty, it has been used for centuries all across the world under different regimes – but to date it is still unknown to most people – is a tool for hiding information so that it does not even appear to exist However Steganography operates at a more complex level as detection is dependent on recognizing the underlying hidden data.

Historical tricks include invisible inks, tiny pin punctures on selected characters, minute differences between handwritten characters, pencil marks on type written characters, grilles which cover most of the message except for a few characters, and so on. Steganography is different from cryptography. The main objective of cryptography is to secure communications by changing the data into a form so that it cannot be understand by an eavesdropper. On the other hand, steganography techniques tend to hide the existence of the message itself, which makes it difficult for an observer to figure out where exactly the message is. The information to be hidden in the cover data is known as the "embedded" data. The "steno" data is the data containing both the cover signal and the "embedded" information. Logically, the process of putting the hidden or embedded data, into the cover data, is sometimes known as embedding. Occasionally and especially when referring to image steganography, the cover image is known as the container. The term "cover" is used to describe the original, innocent message, data, audio, still, video and so on. When referring to audio signal steganography the cover signal is sometimes called the "host" signal. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement is called steganography. Steganography is a technique used to hide information within images. Using stenography, watermarks and copyrights can be placed on an image to protect the rights of its owner without altering the appearance of the image. Almost like magic, images, executable programs, and text messages can hide in images. The cover image does not appear to be altered. People look at the cover image and never suspect something is hidden. Your information is hidden in plain sight.

The traditional Image steganography algorithm is Least Significant Bit embedding, the advantage of LSB is its simplicity to embed the bits of the message directly into the LSB plane of cover-image and many applications use this method [8]. But it can be easily detected by the attackers as it embeds data sequentially in all pixels. If a steganography method causes someone to suspect that there is secret information in the carrier medium, then this method fails [9]. Instead of sequentially embedding data, data can be embedded

in random pixels, but it causes speckles in the image. The previous algorithms LSB and Random LSB concentrate on hiding data in the least significant bit position of all or some selected pixels. They are not particularly concentrating on special pixels. To overcome these problems we proposed a novel image steganography algorithm based on least significant bit embedding algorithm (LSB) for hiding secret messages in the edges of the image. Steganography is different from cryptography. The main objective of cryptography is to secure communications by changing the data into a form so that it cannot be understand by an eavesdropper [10]. On the other hand, steganography techniques tend to hide the existence of the message itself, which makes it difficult for an observer to figure out where exactly the message is.

Two aspects of attacks on steganography are detection and destruction of the embedded message. Any image can be manipulated with the intent of destroying some hidden information whether an embedded message exists or not. Detecting the existence of a hidden message will save time in the message elimination phase by processing only those images that contain hidden information. Detecting an embedded message also defeats the primary goal of steganography, that of concealing the vary existence of a hidden message.

Our goal is not to advocate the removal or disabling of valid copyright information from watermarked images, but to point out the vulnerabilities of such approaches, as they are not as robust as it is claimed. It includes a vast array of secret communications methods that conceal the message's very existence. These methods include invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum communications. Steganography and cryptography are cousins in the spy craft family. Cryptography scrambles a message so it cannot be understood. Steganography hides the message so it cannot be seen. A message in cipher text, for instance, might arouse suspicion on the part of the recipient while an "invisible" message created with steganographic methods will not.

2. Steganography Types

STEGANOGRAPHY comes from the Greek Words: STEGANOS – "Covered", GRAPHIE – "Writing". Generally the sender writes an innocuous message and then conceals a secret message on the same piece of paper. The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists.

The data can be visible in basic formats like: Audio, Video, Text and Images etc. These forms of data are detectable by human hiding, and the ultimate solution was Steganography. The various types of steganography include:

a. Image Steganography:
The image steganography is the process in which we hide the data within an image so that there will not be any perceived visible change in the original image. The conventional image steganography algorithm is LSB embedding algorithm.

b. Audio Steganography:
Steganography can be applied to audio files i.e., we can hide information in an audio file, it can be called Audio Steganography. The audio file should be undetectable.

c. Video Steganography:
Steganography can be applied to video files i.e., if we hide information in a video file, it can be called Video Steganography. The video file should be undetectable by attacker.

d. Text files Steganography:
Steganography can be applied to text files i.e., if we hide information in a text file, it is called Text Steganography. The general process of steganography i.e., preparing a stego object that will contain no change with that of original object is prepared but using text as a source. The basic image steganography algorithm is Least Significant Bit embedding.

3. LSB METHODS

The technique converts image into shaded Gray Scale image. This image will be act as reference image to hide the text. Using this grey scale reference image any text can be hidden. Single character of a text can be represented by 8-bit. If the reference image and the data file are transmitted through network separately, we can achieve the effect of Steganography. Here the image is not at all distorted because said image is only used for referencing. Any huge amount of text material can be hidden using a very small image. Decipher the text is not possible intercepting the image or data file separately. So, it is more secure.

3.1 Least Significant Bit embedding (LSB)

In a gray scale image each pixel is represented in 8 bits. The last bit in a pixel is called as Least Significant bit as its value will affect the pixel value only by "1". So, this property is used to hide the data in the image. Here we have considered last two bits as LSB bits as they will affect the pixel value only by "3". This helps in storing extra data. The Least Significant Bit (LSB) steganography is one such technique in which least significant bit of the image is replaced with data bit. As this method is vulnerable to steganalysis so as to make it more secure we encrypt the raw data before embedding it in the image. Though the encryption process increases the time complexity, but at the same time provides higher security also. This approach is very simple.

In this method the least significant bits of some or all of the bytes inside an image is replaced with a bits of the secret message. The LSB embedding approach has become the basis of many techniques that hide messages within multimedia carrier data. LSB embedding may even be applied in particular data domains - for example, embedding a hidden message into the color values of RGB bitmap data, or into the frequency coefficients of a JPEG image. LSB embedding can also be applied to a variety of data formats and types. Therefore, LSB embedding is one of the most important steganographic techniques in use today.

3.2 Random Least Significant Bit Embedding (RLSB)

In this algorithm data is hidden randomly i.e., data is hidden in some randomly selected pixel. Random pixel is generated by using Fibonacci algorithm. The fatal drawback of LSB embedding is the existence of detectable artifacts in the form of pairs of values (PoVs). The proposed scheme breaks the regular pattern of (PoVs) in the histogram domain, increasing the difficulty of steganalysis and thereby raising the level of security. Two values whose binary representations differ only in the LSB are called a pair of values (PoVs). For example, 68(01000100)2 and 69(01000101)2 are a PoVs. If the numbers of 1s and 0s are equal and distributed randomly in the secret message that is to be embedded steganographically, the frequency of two values in each PoVs will be equal after message embedding. This regular equality pattern, called the PoVs artifact, is an unusual characteristic in the histogram domain [11]. The sample value that will be incremented or decremented depends on a series of predefined thresholds that are generated by the user-specified stego-key. The new sample value not only depends on the generated pseudorandom number but also depends on the original sample value. Using the RLSB is therefore more secure than using traditional LSB embedding techniques.

3.3 EDGE LEAST SIGNIFICANT BIT EMBEDDING (ELSB)

In ELSB, we use all the edge pixels in an image. Here, we first calculate the masked image by masking the two LSB bits in the cover image. Then we identify the edge pixels by using the Canny Edge detection method. After obtaining the edge pixels we hide the data in the LSB bits of the edge pixels only and send the stego object to the receiver. At the receiver, the stego object is again masked at the two LSB bits [12]. Then the canny edge detector is used to identify the edge pixels. We will get same edge pixels at the sender and receiver since we used the same masked image to calculate the edge pixels. Thus we identify the bits where data is hidden. So we extract data from the two LSB bits of the identified edge pixels. Thus message is obtained. The least-significant-bit (LSB)-based approach is a popular type of steganographic algorithms in the spatial domain.

However, we find that in most existing approaches, the choice of embedding positions within a cover image mainly depends on a pseudorandom number generator without considering the relationship between the image content itself and the size of the secret message. Thus the smooth/flat regions in the cover images will inevitably be contaminated after data hiding even at a low embedding rate, and this will lead to poor visual quality and low security based on our analysis and extensive experiments, especially for those images with many smooth regions. We expand the LSB matching revisited image steganography and propose an edge adaptive scheme which can select the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image.

For lower embedding rates, only sharper edge regions are used while keeping the other smoother regions as they are. When the embedding rate increases, more edge regions can be released adaptively for data hiding by adjusting just a few parameters. The experimental results evaluated on 6000 natural images with three specific and four universal steganalytic algorithms show that the new scheme can enhance the security significantly compared with typical LSB-based approaches as well as their edge adaptive ones, such as pixel-value-differencing-based approaches, while preserving higher visual quality of stego images at the same time.

4. SECURITY MODEL

Steganography is used to hide the very existence of a message from a third party. Due to growing need for security of data, image steganography is gaining popularity.

ELSB aims that more secure than LSB and RLSB, storage capacity is decreased and Data transmission rate is increased.

a. Goals

The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists.

b. Threats

The algorithms LSB and Random LSB concentrate on hiding data in the least significant bit position of all or some selected pixels. They are not particularly concentrating on special pixels. To overcome these problems we proposed a novel image steganography algorithm based on least significant bit embedding algorithm (LSB) for hiding secret messages in the edges of the image.

5. FUTURE ENHANCEMENTS

Our future research efforts will be focused on putting together a new method that has a greater hiding capacity than the 4-LSBs method and can maintain such stego-image quality as to meet the demand of human visual sensitivity. The following are some directions for future research. Make better use of edge areas to hide more data: If 5 bits of secret data were to be hidden in every pixel, and then the visual artifacts on the stego-image would be obviously visible. That is to say, not every pixel can afford to hold so many secret data bits without clearly showing the modification. In our opinion, the whole image should at least be broken down to smooth areas and edge areas, and data hiding can then be done to different kinds of areas differently. In smooth areas, for example, we can hide 4 bits of secret data in each pixel; in edge areas, each pixel can afford to hold as many as 5 bits of secret data. However, it is necessary but more challenging to try to maintain the local properties of the pixels, making them stay the same after hiding data, because, say, if some smooth area is changed into a non-smooth area after hiding data, it will result in judging errors in the recovery phase. Therefore, the extracting algorithm must be blind.

Utilize more surrounding pixels to determine the local complexity of the image pixel: In Wu and Tsai's method, the local characteristic of the image is determined by two pixels [13]. In Zhang and Wang's method, the local variation of each pixel depends on its three surrounding pixels. In our opinion, within a reasonable limit, more surrounding pixels mean more accurate local variation. For instance, we can compute the local variation based on a sub-block design.

6. CONCLUSION

In the Least Significant Bit embedding algorithm (LSB) and Random Least Significant Bit embedding algorithm (RLSB) an attacker can easily detect the presence of hidden image. To overcome these problems, this new algorithm is implemented based on least significant bit embedding algorithm (LSB) for hiding secret messages in the edges of the image. The algorithm ELSB hides data in edge pixel. The implemented algorithm is applicable to all kinds of images and can be used in covert communication, hiding secret information like copyrights, trade secrets and chemical formulae.

7. REFERENCES

[1] R. Chandramouli and N. Memon,"Analysis of LSB based Image Steganography", IEEE ICIP, pp. 1022-1022, Oct. 2001.

[2] R.J. Anderson, F.A.P. Petitcolas, "On The Limits of Steganography", IEEE Journal ofSelected Area in Communicafions, pp. 474-481, May 1998.

[3] N.F. Johnson, S. Jajodia, "Staganalysis: The Investigation of Hiding Information", IEEE, pp. 113-116, 1998.

[4] H. Hastur, Mandelsteg, ftp://idea.sec.dsi.unimi.it/pub/security/crypt/code/

[5] Niels Provos, "Probabilistic Methods for Improving Information Hiding", Technical report 01-1, January 31, 2001.

[6] R. Anderson, (ed.), Information hiding: first international workshop, Cambridge, UK. *Lecture Notes in Computer Science*, vol. 1174, Berlin Heidelberg New York: Springer-Verlag, 1996.

[7] W. Bender, D. Gruhl, N. Morimoto, A. Lu, "Techniques for Data Hiding", *IBM Systems Journal* Vol. 35, No. 3&4. MIT Media Lab, pp. 313-336, 1996.

[8] N.F. Johnson &S. Jajodia, "Steganalysis of Images Created Using CurrentSteganography Software", in Proceeding for the Second Information Hiding Workhop, Portland 0 regon, USA, April 1998, pp. 273-289.

[9] F.A.P. Petitcolas, R.J. Anderson and M.G. Kuhn,"Information Hiding - A Survey", IEEE Proc., SpecialIssue on Protection of Multimedia Content, 87(7),pp. 1062-1078, July 1999.

[10] K. Rabah, "Steganography- the Art of Hiding Data", Information Technology of Journal, 3(3), pp.245-269, 2004.

[11] Yeuan-Kuen Lee, Graeme Bell, Shih-Yu Huang, Ran-Zan Wang,and Shyong-Jian Shyu, "An Advanced Least-Significant-Bit Embedding Scheme for Steganographic Encoding", Springer-Verlag Berlin Heidelberg 2009.

[12] K. Naveen BrahmaTeja, Dr. G. L. Madhumati, K. Rama Koteswara Rao, "Data Hiding Using EDGE Based Steganography", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 11, November 2012.

[13] Wu, D.C. and Tsai, W.H. (2003). "A steganographic method for images by pixel value differencing", *Pattern Recognition Letters*. Vol. 24 (9-10), 1613-1626.