A STEGANOGRAPHY METHOD TO HIDE DATA IN EDGES OF AN IMAGE

M. Pavani#1, S. Naganjaneyulu*2

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

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

Abstract— **In this paper An LSB method is proposed to provide security for data using steganography method. Steganography is the art of hiding information in other information in such a way that the eavesdropper doesn't know the existence of a message. The traditional image steganography algorithm is Least Significant Bit embedding, but it can be easily detected by the attackers as it embeds data sequentially in all pixels. Instead of sequentially embedding data, data can be embedded in random pixels, but it causes speckles in the image. A better approach is to hide the data in the regions like edges. A novel least significant bit embedding algorithm for hiding encrypted messages in nonadjacent and random pixel locations in edges of images is proposed. It first encrypts the secret message, and detects edges in the cover image. Message bits are then, embedded in the least significant bits and random locations of the edge pixels. It ensures that the eavesdroppers will not have any suspicion that message bits are hidden in the image and standard steganography detection methods can not estimate the length of the secret message correctly.**

***Keywords*—Steganography, Least Significant Bit (LSB), Security, Cryptography,**

I. Introduction

The word steganography is of Greek origin from which steganos means 'covered' graphei means 'writing', means the art and science of covered communication; a steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion. In the past, people used hidden tattoos or invisible ink to convey steganographic content. Today, computer and network technologies provide easy-to-use communication channels for steganography. Essentially, the information-hiding process in a steganographic system starts by identifying a cover medium's redundant bits. The embedding process creates a *stego medium* by replacing these redundant bits with data from the hidden message.

Modern steganography's goal is to keep its mere presence undetectable, but steganographic systems because of their invasive nature leave behind detectable traces in the cover medium. The main goal of steganography is to communicate securely in a completely undetectable manner [1] and to avoid drawing suspicion to the transmission of a hidden data [2]. It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists. Steganography operates at a more complex level as detection is dependent on recognizing the underlying hidden data. It also includes a vast array of methods of secret communications that conceal the very existence of the message. In Steganography, data is hidden inside a vessel of container that looks like it only, but contains something else. A variety of vessels are possible, such as digital images, sound clips, and even executable files.

In this modern era, internet offers great convenience in transmitting large amounts of data in different parts of the world. However, the safety and security of long distance communication remains an issue. In order to solve this problem has led to the development of steganography schemes. 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. 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. It is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret [3]. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated [4]. The strength of steganography can thus be amplified by combining it with cryptography. Two other technologies that are closely related to steganography are watermarking and fingerprinting [5]. These technologies are mainly concerned with the protection of intellectual property, thus the algorithms have different requirements for steganography.

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. The original image is called a *cover image* in steganography, and the message-embedded image is called a *stego image* [6]. Your information is hidden in plain sight. The advantage of steganography over cryptography alone is that messages do not attract attention to themselves. Plainly visible encrypted messages no matter how unbreakable will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

Steganography encompasses methods of transmitting secret messages through innocuous cover carriers in such a manner that the very existence of the embedded messages is undetectable. Creative methods have been devised in the hiding process to reduce the visible detection of the embedded messages. 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.

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 [7]. 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 [8]. 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 [9]. 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.

II. Traditional data hiding methods

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. 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. 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.

A. Least Significant Bit (LSB) Method

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)[7][10] 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.

Algorithm

- Take the input image and secret message.
- Convert each image pixels and message into binary form.
- Mask last two LSB bits of image pixels with first two MSB bits of message.
- Convert this binary form into image.
- That image is the stego object.

B. 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.

Algorithm

- Take the input image and secret message.
- Convert random (using Fibonacci series) image pixels and message into binary form.
- Mask last two LSB bits of image pixels with first two MSB bits of message.
- Convert this binary form into image.
- That image is the stego object.

III. PROPOSED METHOD

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.

Algorithm

- Take the input image and secret message.
- Convert each image pixels and message into binary form.
- Mask last two LSB bits of each image pixels with ‘0’.
- Convert this binary form into stego image, by using Sobel operator convert this into edge pixels.
- Hide message in edge pixels.

IV. EXPERIMENTALRESULTS

The experimental results presented in this section describe the performance of our proposed technique. For steganography we use LSB based well known embedding methods. To conduct our experiments, we have tested our scheme ELSB embedding & sobel operator. The results were 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.

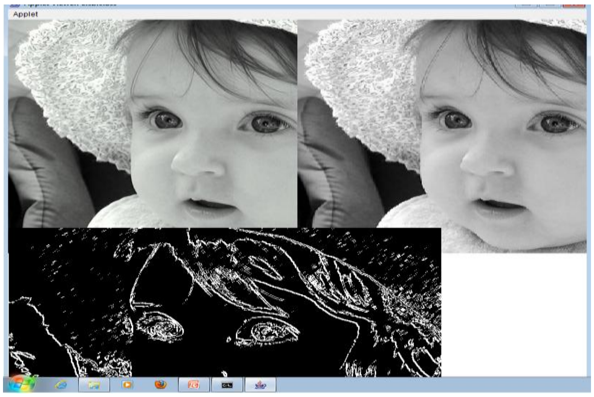
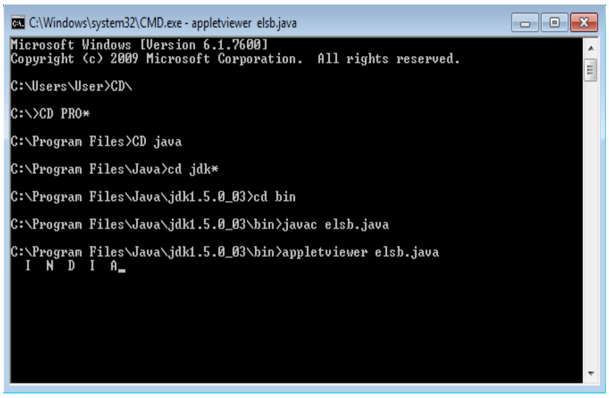


Fig. 1 Output after encoding ELSB.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\User>CD\

C:\>CD PRO*

C:\Program Files>CD java

C:\Program Files\Java>cd jdk*

C:\Program Files\Java\jdk1.5.0_03>cd bin

C:\Program Files\Java\jdk1.5.0_03\bin>javac elsb.java

C:\Program Files\Java\jdk1.5.0_03\bin>appletviewer elsb.java
  I  N  D  I  A_
```

Fig. 2 Output after decoding

V. FUTURE ENHANCEMENT

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. By observation 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.

VI. CONCLUSION

This method provides better security for information than the traditional methods. 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. By this method the storage capacity will reduce and the transmission rate will increase. 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.

REFERENCES

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

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

[3] Moerland, T., “Steganography and Steganalysis”, *Leiden Institute of Advanced Computing Science*,www.liacs.nl/home/tmoerl/privtech.pdf.

[4] Silman, J., “Steganography and Steganalysis: An Overview”, *SANS Institute*, 2001.

[5]Jamil, T., “Steganography: The art of hiding information is plain sight”, *IEEE Potentials*, 18:01, 1999.

[6] M. M. Amin, M. Salleh, S. Ibrahim, M.R.Katmin, M.Z.I. Shamsuddin, “Information Hiding using Steganography” Proceedings of 4th National Conference on Telecommunication Technology, Shah Alam, Malaysia, 2003.

[7] N.F. Johnson &S. Jajodia, “Steganalysis of Images Created Using Current Steganography Software”, in Proceeding for the Second Information Hiding Workshop, Portland 0 region, USA, April 1998, pp. 273-289.

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

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

[10] D. Artz, "Digital Steganography: Hiding Data within Data", IEEE Internet Computing, pp. 75-80, May-June 2001.

[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.

ACKNOWLEGDEMENT

The authors acknowledge for the support of excellent facilities provided by the Director Dr.L S S Reddy .They furthermore thanks to Staff and Students of Lakireddy Bali Reddy College of Engineering who provided helpful comments and discussions throughout my work.

ABOUT THE AUTHORS

Maidam Pavani received her B. Tech degree in Information Technology at Nova College of Engineering and Technology for women, Jupudi. Pursuing M.Tech in Software Engineering at Lakireddy Bali Reddy College Of Engineering, Mylavaram.

Mr.S. Naganjaneyulu received his MCA degree from Acharya Nagarjuna University, Guntur, in 1999. M. Tech degree in Computer Science from Dr. M.G.R. University, Chennai in 2007 and pursuing his Ph.D in Digital Image Processing from Nagarjuna University, Guntur. Currently, he is working as an Associate Professor of IT in Lakireddy Bali Reddy College of Engineering, Mylavaram, India. He has got 10 years of teaching experience.