International Journal of Security and Its Applications
Vol. 10, No. 7 (2016) pp.51-58
http://dx.doi.org/10.14257/ijsia.2016.10.7.05

A Steganographic Method for Images by 'Skip Position'

P. Anusha[1] and Debnath Bhattacharyya[2*]

[1]*Department of Information Technology,*
Bharati Vidyapeeth Deemed University College of Engineering,
Pune-411043, India
[2]*Department of Computer Science and Engineering,*
Vignan's Institute of Information Technology,
Visakhapatnam-530049, India
anushapammi7@gmail.com, debnathb@gmail.com
[*] *(Corresponding Author)*

Abstract

Data Communication and network have changed the way business and other daily affair works. Now, they rely on computer network and internetwork. Computer network is a telecommunication channel through which we can share our data. It is also called data network. Security for data transmission is one of the important aspects to be considered in modern communication system. In this paper data that is to be transferred is sent in certain pattern which is embedded in the huge amount of data that can be seen by everyone. The effectiveness of the proposed method is described in such a way to increase security of data. To hide data in a binary image, no key is needed here rather this algorithm is based on binary tree traversal through which the bits are plotted in MSB (Most Significant Bit), LSB(Least Significant bit) and MIDDLE bit of a byte. The proposed algorithm assures the data hiding and security.

Keywords*: Data hiding, Steganography, Stego image*

1. Introduction

Security for the important data to be sent is very important. In present generation there are many issues that explore the security risks involved with data transmission, such as eavesdropping and decrypting. In Steganography the data that is to be transmitted is embedded in an image in a certain pattern so that the receivers only could extract the bits in that pattern that is impossible for the third person.

The transformation of hidden data can be achieved through two ways: Encryption and Steganography. By using these two techniques security of hidden data can be increased [1]. This type of sending hidden data in order to make communication secretly is in practice since old days [2]. Encryption is a technique of data hiding in which the data is changed in such a way that no attacker can read it even if they copy the file or message [3]. Steganography is one of the popular techniques in transformation of hidden data. Steganography is not a new practice it was in use from the olden days [4]. Steganography can use some media to encrypt the data, so steganography is considered to be more safe compared to cryptography [5].

There are different techniques used in steganography. They are Linguistic steganography and Technical. Technical steganography uses scientific methods to hide a message, such as the use of invisible ink or microdots and other size-reduction methods. Steganography is achieved by using cover media such as Text, Audio, Video, and Digital Image [6]. The text stegnography is achieved by changing words of the existing text [7].

[*] Corresponding Author

ISSN: 1738-9976 IJSIA

The audio steganography is done through embedding data in the frames of audio file [8]. In video stegnography the data is embedded in the frames of a host video using different techniques [9]. In digital image steganography, information is sent through embedding the data into pixels of the image. The data or information that is to be sent secretly is embedded in the bits of an image and this image is called cover image [10]. This image is known to be stego-image [11]. The information that is to be sent is embedded in the bits of cover media that is not possible to achieve by the attacker. There are two more techniques that are similar to steganography and they are Watermarking and Fingerprinting [12].

There are different types of encrypting methods which differ with security and robustness [13]. There are different ways in which information can be embedded into an image. One of the famous techniques used in embedding message into a colored image was LSB and is considered to be good approach [14]. And there are many more algorithms that give a secured transmission by hiding data in an image [15].

In this paper we proposed a new technique in which bits are embedded into an image in the pattern of binary tree traversal. The binary (0,1) values of the data are considered and embedded in least significant bit, middle bit and most significant bit.

2. Previous Work

Image consists of pixels, each pixel consists of three bytes and each byte consists of eight bits that is total 24 bits. The bits to be sent are embedded in these bits in certain pattern. There are many techniques proposed in order to provide security and robust.

There have been many techniques proposed in the last decade. To hide data in an image the simplest approach is least significant bit insertion. One of the most widely used techniques to hide data is in LSB (Least Significant Bit) [16] in which LSB based steganographic technique was used by considering an Index set(Ω) and partitioned this set into subsets to know steganographic capacity .

Many algorithms were proposed for embedding bits in LSB. One of such embedding algorithm proposed was done through considering optimal pixel adjustment process (OPAP) [17] by enhancing the quality of stego image.

The other technique used in image stegnography is based on pixel value difference [18] in which bits are embedded by considering the differences of the grey value of the two pixels in the block of a grey color image which is used as a cover image. The other such algorithm which used pixel value difference with long bit stream as the secret data by considering contiguous ranges for embedding data [19].

Other techniques in image stegnography are random insertion in the pixel and one of such algorithm is random insertion by considering data parity [20] in which red, green and blue colors of a pixel are taken as equation.

There are many more techniques that are improved in order to increase security and robustness. Some of them are pixel mapping in order to achieve data hiding [21] in which rules were proposed based on the pixel intensity and its parity, based on this rules the embedding was done.

The other technique used in image steganography is Labeling method. Many algorithms were proposed under this method. One of such algorithm concentrated on sequence of color by using label to the image and embedded message on certain color of image [22] which uses a grey image for steganography.

There are many more techniques proposed in image steganography [23]. Among all the techniques, LSB (Least Significant Bit) is considered to be most advantageous [24] and easy to implement.

EXAMPLE: let us suppose the data to be sent is 100010110

The original image data:-

10010001 00001101 11001001

11001110 00101111 11011010

11110110 01001111 11011010

The bits are embedded as:-

10010101 00001100 11001000

10010110 00001111 11001010

11110111 01001111 11011010

All the bits are embedded in LSB (Least Significant Bit) of the pixel of an image. In the proposed algorithm all the bits are embedded not only in LSB (Least Significant Bit) but also used MSB (Most Significant Bit), MIDDLE BIT of the pixel of an image making use of maximum bits of a pixel.

3. Proposed Work

In this paper a new technique is used that consider least significant bit along with middle bit and most significant bit. The binary representation of data to be sent secretly is embedded in MSB (Most Significant Bit), LSB (Least Significant Bit) and middle bit. The change in MSB and middle bit makes a vast change in image, so we use a matrix called skip position matrix. If the bits of MSB (Most Significant Bit), LSB (Least Significant Bit) and middle bit are to be changed then we skip the bit and that position is saved in the matrix.

10010101 00001101 11001001

10010110 00001111 11001010

Now suppose we want to hide 15 bits of data *i.e.*, 111001101100111110

100**1**010**1** **0**000-[**SKIP POSITION**] 110**1** **1**10**0**100**1**

1001**0**11**0** **1**000**1**111 **1**100**1**01**0**

In this technique the data to be sent is embedded in LSB (Least Significant Bit), MSB (Most Significant Bit) and MIDDLE BIT of each byte. Whenever the bit to be sent does not match with the bit in the image then the position is skipped and embedded the bit in the next position. The skipped position is represented in a matrix and embedded in the LSB's in the bytes in the second half of the image.

The middle bit is to be considered as, if the byte is in even line then fifth bit of byte is taken to embed the data while the line of byte is odd then the bit is embedded in fourth position of a byte.

Line 1[odd] - **1**00**1**010**1** **0**000-[**SKIP POSITION**] 110**1** **1**10**0**100**1**

Line 2[even] - **1**001**0**11**0** **1**000**1**111 **1**100**1**01**0**

$$\begin{bmatrix} 0\,0\,0\,0\,1\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0 \end{bmatrix}$$

Skip matrix

This skip position matrix is represented using LSB algorithm. Let us embed the matrix bits represented above into the data below.

0001011**0** 0000111**0** 1100101**0** ⇨ [represents first three bits of a byte]

1001111**0** 0001000**1** 1100101**0** ⇨ [represents next three bits of a byte]

Here zero represents that the bit at that position is not skipped and secret data is present at that position and one represents the bit is not embedded and skipped the position.

In this technique three bits can be sent in a byte. Number of unused bits can be minimized.

4. Algorithm

There are two algorithms which are used to implement the proposed technique. Embedding algorithm used for hiding the bits in the image in certain pattern and extracting algorithm used to extract the embedded bits in the image.

4.1. Embedding Algorithm

a. Read characters from data files and convert the ASCII value into its equivalent binary value.

b. Repeat step ‘a’ until the terminating character is found.

c. From the image file, read the RGB bits of a pixel.

d. Read the total number of pixels of the image, as to use the first half for embedding the data to be sent and the second half is to represent the skip positions of the bits in pixel.

e. Consider each LSB, MIDDLE BIT and MSB of RGB of an image.

f. Compare the bits of the character of data file with the MSB, LSB, and MIDDLE BIT of RGB of the image.

g. If the bit that is to be embedded into the image bit is same to the bit at that position then the bit is not skipped and considered that the secret bit is present.

h. If the bit to be embedded into the image bit is not same to the bit at that position then the position of the bit are skipped and the position is saved into a matrix.

i. Repeat step ‘f’ to step ‘g’ until the terminating character is found.

j. This termination character is explicitly chosen by the sender and it may be dot (.) or any special character.

k. The skipped positions matrix is now arranged in the second half bits of an image.

l. Each successful and unsuccessful embedding of the bits is represented as 0, 1 and presented in LSB of the pixel.

m. Repeat step ‘l’ until all positions are represented in the second half of the image pixel.

In this method we used the pixel’s MSB, LSB and MIDDLE BIT in order to stuff the information to be sent by the sender. And also the pixel count is also taken in order to make it as two parts to represent the main data in the first part using MSB, LSB and MIDDLE BIT and the second half consists of skipped position where the matrix is embedded in LSB.

4.2. Extraction Algorithm

a. Open the Stego Image file in read mode.

b. Consider the number of pixel of the image in which first half pixels contain main Message and second half pixels contain skipped position representation.

c. Initially the LSB bits of second half of the image are taken which gives the receiver about the skip positions of the stuffed bits.

d. If the LSB of the pixel is 1, it means that the position is skipped and if the bit is 0, it means the position is not skipped.

e. Now the first half part of the image is taken in which the bits of LSB, MSB and MIDDLE BIT is taken by considering the skip bits in second half of the image.

f. Repeat the step ‘c’ to step ‘e’ until the termination symbol is found.

g. The process is done and printed the values until the termination symbol is found.

In the process of extraction, pixel count is taken. Through which the second half bits are extracted and skip positions are known followed by main bits extraction in the first half of the image bits.

5. Result

As per observations done using the proposed algorithm there is increased encoding strength providing a reliable data and enhanced security.

Table 1. Comparison of Algorithms

Algorithm	Encoding strength	Security	Reliability
LSB	Medium	Medium	High
PROPOSED ALGORITHM	High	High	High

In Table 1, we have a comparison among LSB and the proposed algorithm on encoding strength, security and reliability parameters. The proposed algorithm provides about 95% of secured data transmission through image Steganography.

In Figure 1, we have original image in which the bits are extracted and the proposed algorithm is applied. Figure 2 is stego image which is formed after implementing proposed algorithm on the bits of Figure 1 and this Figure is sent in order to send data secretly.

Figure 1. Original Image

Figure 2. Stego Image

6. Conclusion

This proposed algorithm has following advantages:

a. Minimal changes are done in the pixels of image which a human eye cannot recognize.

b. Provides a high security for the data sent.

c. A separate key is not required in this algorithm.

We conclude that this algorithm have been proposed using steganography as a tool to send data with high security and providing high safety. And can be used to send data to anybody throughout the world. Proposed algorithm provides a high security and the information is quite invisible. Provide the reliable data after decryption.

A modification to this algorithm provides further security for the data.

References

[1] W. Bender, D. Gruhl, N. Morimoto and A. Lu, "Techniques for data hiding", IBM System Journal, vol. 35, Issue 3- 4, **(1996)**, pp. 313-336.
[2] S. P. Mohanty, "Digital Watermarketing: A tutorial review", http://citeseer.ist.psu.edu/mohanty99digital.html, visited 15, **(2005)** June, pp. 1-24.
[3] F. Petitcolas, R. Anderson and M. Kuhn, "Information Hiding-A Survey", Proceedings of the IEEE, special issue on protection of multimedia content, vol. 87, Issue 7, **(1999)** July, pp. 1062-1078.
[4] K. Rabah, "Steganography – The Art of Hiding Data", Information Technology Journal, vol. 3, no. 3, Asian network for Scientific Information, **(2004)**, pp. 245-269.
[5] S. Bansod and G. Bhure, "Data Encryption by Image Steganography", International Journal of Information and Computation Technology, vol. 4, no. 5, **(2014)**, pp. 453-458.
[6] C. P. Sumathi, T. Santanam and G. Umamaheswari, "A Study of Various Steganographic Technique Used for Information Hiding", International Journal of Computer Science & Engineering Survey (IJCSES), vol. 4, no. 6, **(2013)** December, pp. 9-25.
[7] A. Koluguri, S. Gouse and Dr. P. B. Reddy , "Text Steganography Methods and its Tools", International Journal of Advanced Scientific and Technical Research, Issue 4, vol. 2, **(2014)** March-April, pp. 888-902.
[8] M. Nosrati, R. Karimi and M. Hariri, "Audio Steganography: A Survey on Recent Approaches", World Applied Programming, vol. 2, no. 3, **(2012)** March, pp. 202-205.
[9] K. N. Choudry and A. Wanjari, "A Survey Paper on Video Steganography", Kedar Nath Choudr, / (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 6, no. 3, **(2015)**, pp. 2335-2338.
[10] K. Stefan and A. Fabien, "Information hiding techniques for steganography and digital Watermarking", Artech House Books, **(1999)** December.
[11] D. Bhattacharyya, A. Roy, P. Roy and T.-h. Kim, "Receiver Compatible Data Hiding in Color Image", International Journal of Advanced Science and Technology, vol. 6, **(2009)** May, pp. 15-23.

[12] R. Poornima and R. J. Iswarya, "AN OVERVIEW OF DIGITAL IMAGE STEGANOGRAPHY", International Journal of Computer Science & Engineering Survey (IJCSES), vol. 4, no. 1, **(2013)** February, pp. 23-31.
[13] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, "Handbook of Applied Cryptography", CRC Press, **(1996)**.
[14] R. Begum R. D. and S. Pradeep, "Best Approach for LSB Based Steganography Using Genetic Algorithm and Visual Cryptography for Secured Data Hiding and Transmission over Networks", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, Issue 6, **(2014)** June, pp. 114-119.
[15] M. Wu, E. Tang and B. Liu, "Data Hiding in Digital Binary Image", 2000 IEEE International Conference on Multimedia and Expo, New York City, NY, USA, vol. 1, **(2000)** July 30-August 2, pp. 393-396.
[16] R. Chandramouli and N. Memon, "Analysis of LSB Based Image Steganography Techniques", International Conference on Image Processing, Thessaloniki, Greece, vol. 3, **(2001)** October 7-10, pp. 1019-1022.
[17] C.-K. Chan and L.M. Cheng, "Hiding data in images by simple LSB substitution", The Journal of pattern recognition Society, City University of Hong Kong, Hong Kong, **(2004)**, pp. 469 – 474
[18] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value Differencing", Pattern Recognition Letters, vol. 24, **(2003)**, pp. 1613–1626.
J. K. Mandal and D. Das, "Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain", International Journal of Information Sciences and Techniques (IJIST), vol. 2, no. 4, **(2012)** July, pp. 83-93.
[19] D. G. Dighe and N. D. Kapale, "Random Insertion Using Data Parity Steganography Technique", International Journal of Engineering Science and Innovative Technology (IJESIT), vol. 2, Issue 2, **(2013)** March, pp. 364-368.
[20] P. K. Panjabi and P. Singh, "An Enhanced Data Hiding Approach using Pixel Mapping Method with Optimal Substitution Approach", International Journal of Computer Applications, vol. 74– no.10, **(2013)** July, pp. 36-43.
[21] H. Motameni, M. Norouzi, M. Jahandar and A. Hatami, "Labeling Method in Steganography", International Journal of Computer, Electrical, Automation, Control and Information Engineering, vol. 1, no. 6, **(2007)**, pp. 1600-1605.
[22] M. Hussain and M. Hussain, "A Survey of Image Steganography Techniques", International Journal of Advanced Science and Technology , Shaheed Zulfiqar Ali Bhutto Institute of Science & Technology, (SZABIST), Islamabad, Pakistan, vol. 54, **(2013)** May, pp. 113-124.
[23] S. S. Jaber, H. A. Fadhil, Z. I. Abdul Khalib and R. A. Kadhim, "Survey on recent digital image steganography techniques", Journal of Theoretical and Applied Information Technology, vol. 66, no. 3, **(2014)** August 31st, pp. 654-660.

