Journal of Theoretical and Applied Information Technology
20th July 2013. Vol. 53 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

INDEX BASED STEGANOGRAPHY: A NEW SECURE APPROACH FOR IMAGE STEGANOGRAPHY USING TWO IMAGES

[1]B.PERSIS URBANA IVY, [2]P.J.KUMAR , [3]S.SUREKA, [4]G.UMA MAHESWARI

[1]Assistant Professor (SG), SITE, VIT University, Vellore-632 014

[2]Assistant Professor (Sr), SITE, VIT University, Vellore-632 014

[3]Assistant Professor, SITE, VIT University, Vellore-632 014

[4]Assistant Professor (Sr), SITE, VIT University, Vellore-632 014

E-mail: [1]prssivy454@gmail.com, [2]pjkumar@vit.ac.in, [3]ssureka@vit.ac.in, [4]g.umamaheswari@vit.ac.in

ABSTRACT

Steganography is the way of hiding data in such a way that nobody except the intended receiver can detect the presence of data and retrieve it. The most widely used method used for image Steganography is LSB modification method. Although it is a simple technique, but the probability of detecting the hidden data is high since the present Steganalysis algorithms are capable enough to detect not only the alteration in image but also the secret data hidden in image. The linear plain text hidden in an image can easily be detected. In this paper we proposed a new secure method of implementing image Steganography. Instead of using a single image for Steganography, we are using two images. In this method we are hiding the data without altering the image containing the actual data. Thus it provides more security than other methods of hiding data in the image. The proposed method can also efficiently hide large amount of data which was difficult to hide in other Steganographic methods.

Keywords: *STEGNOGRAPHY, INFORMATION HIDING, SECURE STEGNOGRAPHY, INDEX BASED STEGNOGRAPHY*

1. INTRODUCTION

Steganography derived from Greek, literally means “hidden-writing”. It is an art and science of hidden communication i.e. it hides the existence of communication itself. The goal of Steganography is to embed the secret information into other information. Thus it hides the existence of communicated secret information. Steganography is often confused with Cryptography because both are used to protect information. While the goal of Cryptography is to conceal the data to be communicated, the goal of Steganography is to conceal the existence of communication. The basic model of Steganography consists of a cover object, a secret message that is to be transmitted and an algorithm to hide the message in the cover object. In many cases a stego-key is also used to encode the secret message for providing more security. The result of this method is a stego-object which contains the secret message. Now this stego-object can be used in communication. At the receiver’s side, this stego-object is received and is decoded by using a decoding algorithm to obtain the secret message. Figure 1 shows the basic model of Steganography.

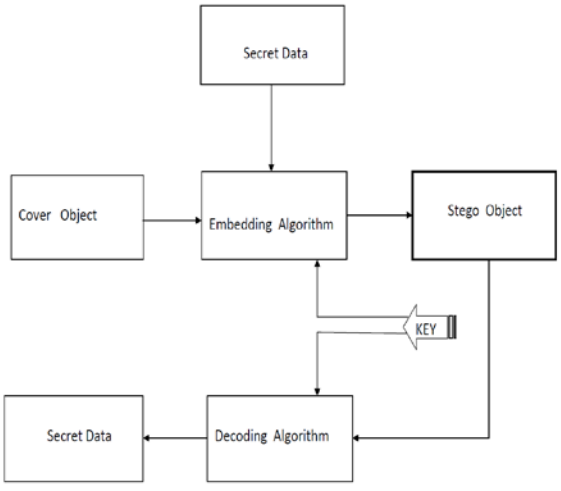

Figure 1: Basic Model Of Steganography

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Different carriers can be used in Steganography such as text, image, audio, video etc, but digital images are the most preferred and widely used because of their availability and also because of the fact that images can easily be spread over the World Wide Web. To hide the data in image, it is altered in such a way that does not draw the attention to the modified image. The most common method to do this alteration to hide data in image is by usage of LSB modification method. This method is preferred because of its easiness of usage. In this paper we propose a new Image Steganography method which can be implemented both in the spatial domain and frequency domain. Our method provides more security than existing methods since our method does not require alteration in the image that contains the secret data. Thus probability of detecting hidden data is reduced using our proposed method. Also the amount of data that can be hidden is increased using our method.

2. PROPOSED METHODOLOGY(INDEX BASED STEGANOGRAPHY)

We are proposing a more secure Steganographic method which is capable enough to survive Steganalysis attack and also reduces the probability of detecting the hidden data in image. It is based on the simple Steganography method of hiding linear plain text in cover image to generate Stego-Image. But we are following a different approach in our method. Traditional approach was to embed the linear plain text with the Cover-Image so as to generate the Stego-Image. And this Stego-Image was used for communication. At the receiver side, Stego-Image is received which is then decoded to get the hidden plain text. The problem with this approach was that the linear plain text hidden in image can easily be detected using any Steganalysis algorithm. Since present Steganalysis algorithms are capable enough not only to detect that the given image is altered but can also detect the exact hidden data in image.

To provide more robustness, we are proposing a method which overcomes this drawback to some extent. Instead of embedding the linear plain text directly with Cover-Image we are using one more Image which will contain our hidden data. We named it as Data-Image. First, the data to be hidden is converted into bits. Then these bits are matched with the Data-Image and the indices of matched bits are stored in an index file. This index file is then embedded with the Cover-Image to generate the Stego-Image and this Stego-Image along with the data-Image is sent to the receiver. And, at the receiver's side the Stego-Image is decoded to get the index file. Now based on the content of index file, the index position of our data bits are known in the Data-Image and thus the hidden data is extracted at the receiver's side.

This approach provides more security in the sense that we are only altering the Cover-Image which is embedded with Index file. Our Image containing the actual data is not altered at all therefore no Steganalysis algorithm will suspect our Data-Image. Stego-Image, containing the index data may be suspected and the embedded data can be obtained using a Steganalysis method but this data will be of no use for the person doing the Steganalysis since our actual hidden data is in the Data-Image which will successfully pass the Steganalysis method.

2.1 Sender's side process

Figure 2 shows the complete Process at the Sender's Side for the proposed method. The steps are described as follows:

Step-1: Choose a Data Image.

Step-2: Get the Secret Data to be communicated.

Step-3: Convert the Secret Data into bits.

Step-4: Match these bits with the bits of Data-image and store the index position of matched bits in a text file (Index File).

Step-5: Choose a Cover Image.

Step-6: Check Whether the Cover-Image is large enough to hold the data of Index File. If "No" then go to Step-5 and choose some other Cover-Image large enough to hold the data. Else go to Step-7.

Step-7: Embed the Index File Data

2.2 Receiver's side process

Figure 3 shows the complete Process at the Receiver's Side for the proposed method. The steps are described as follows:

Step-1: Receive the Data-Image and Stego-Image.

Step-2: Extract the data from the Stego-Image using the decoding algorithm.

Step-3: This data contains numeric data. Store this data in a text file (Index File).

Step-4: Based on the content of this Index File. Move to particular Bit position in the Data-Image

Journal of Theoretical and Applied Information Technology
20th July 2013. Vol. 53 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and store the bits in a Text File (Bit-Data). Perform this step until all the indices are visited.

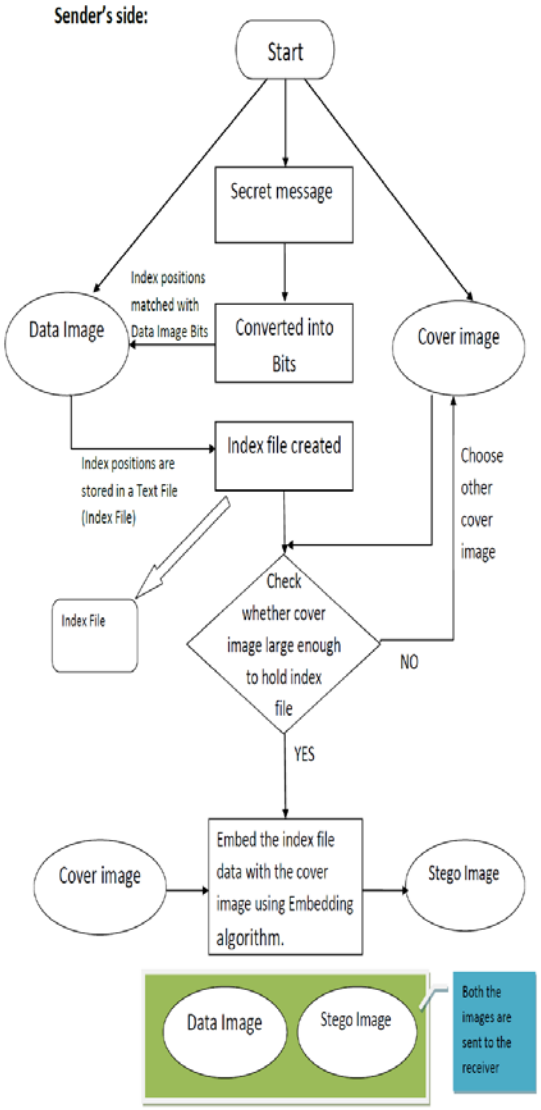

Figure 2: Sender's Side Process

2.3 Embedding Algorithm

We are using this algorithm based on simple LSB modification method to embed the Index File data with the Cover Image so as to generate the Stego Image. Using the same algorithm, before the index file data, first the length of the index file data is embedded in the first eight bytes of the cover Image. Embedding the length in first eight bytes will be helpful for decoding the data using Decoding algorithm.

Step-1: Read the Cover Image and Index File.

Step-2: Convert the Cover Image and Data in Byte Array.

Step-3: Get each byte from the Data Byte Array and convert it into bits.

Step-4: For each Bit, go through each Image Byte and replace the LSB of the Image Byte with the bit.

Step-5: Repeat the process until each byte of Data Byte Array is traversed.

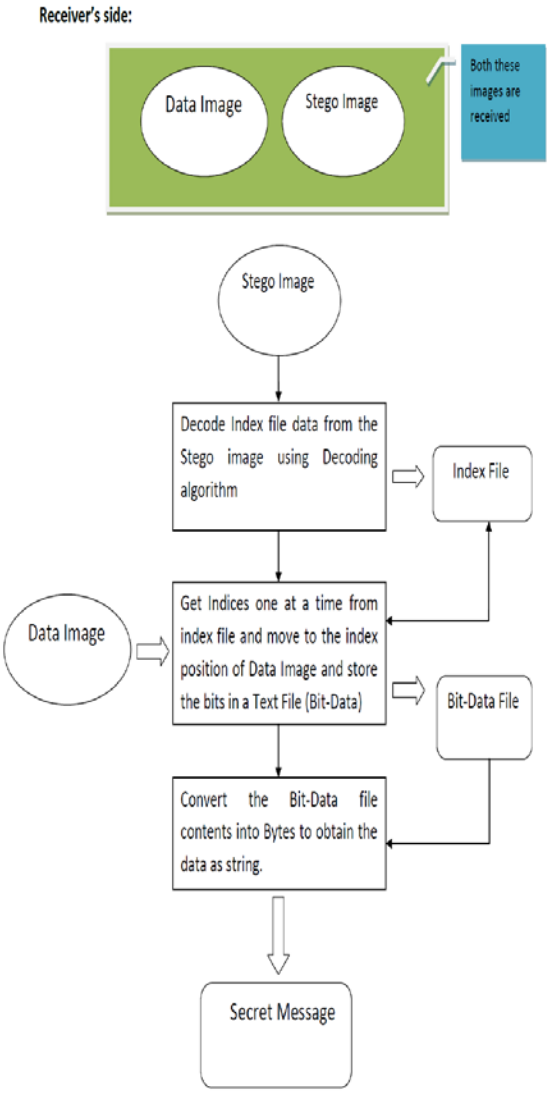

Figure 3: Receiver's Side Process

Journal of Theoretical and Applied Information Technology
20th July 2013. Vol. 53 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2.4 Decoding Algorithm

This algorithm is used to decode the data from the Stego Image. The decoding process is described as follows:

Step-1: Read the Stego Image.

Step-2: Convert the Stego Image in Byte Array.

Step-3: Go through the First eight bytes of this array and get the LSB of each byte.

Step-4: This will give us eight bits. Club the bits to obtain a value. This value is the length of the data to be decoded.

Step-5: Create a new Byte Array of the length obtained in the Step-4. This array will store the resultant data decoded from the Stego Image.

Step-6: Now traverse through the Image Byte Array after the first eight bytes and repeat the Step-7 and Step-8 until the resultant byte array is full.

Step-7: Traverse each Byte and get the LSB from it.

Step-8: Club the set of eight LSB's to create a Byte value and store this byte in Resultant Byte Array created in Step-Step-9: The data is obtained from the Resultant Byte Array.

3. EXPERIMENTAL RESULTS AND DISCUSSIONS

Figure 4: Data Image

Figure 5: Cover Image

Figure 6: Stego Image

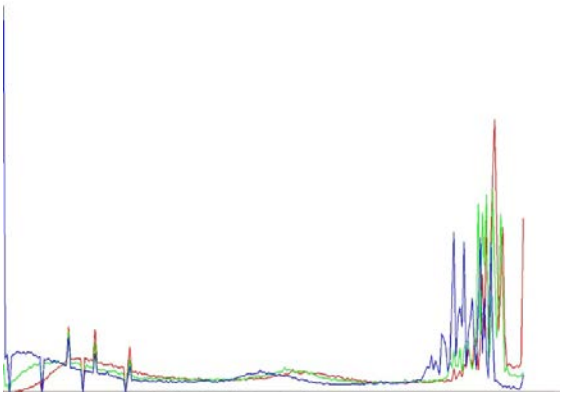

Figure 7: Histogram Of Data Image Used In Experiment

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

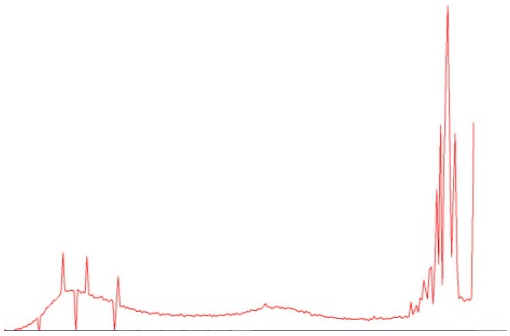

Figure 8: R Component Of Data Image

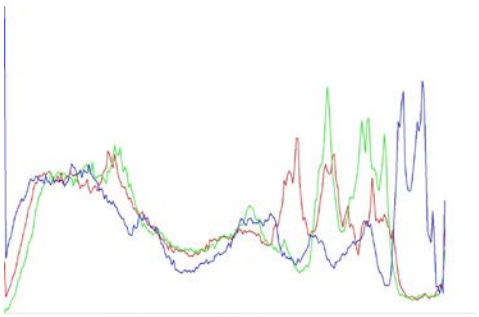

Figure 9: Histogram Of Cover Image

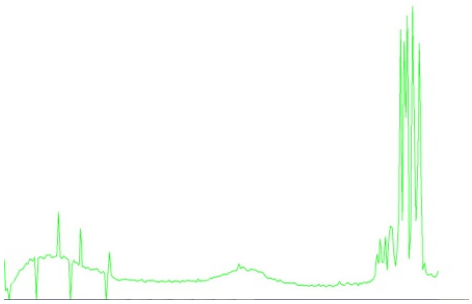

Figure 10: G Component Of Data Image

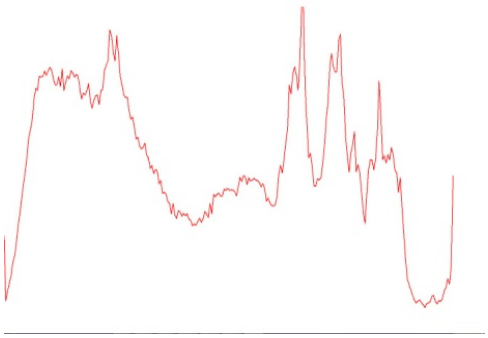

Figure 11: R Component Of Cover Image

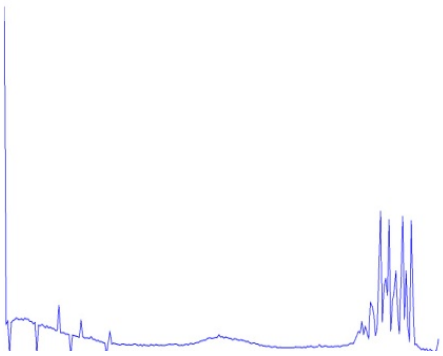

Figure 12: B Component Of Cover Image

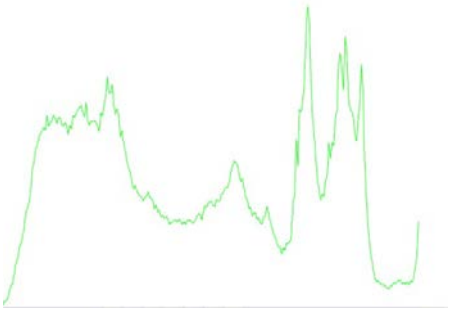

Figure 13: G Component Of Stego Image

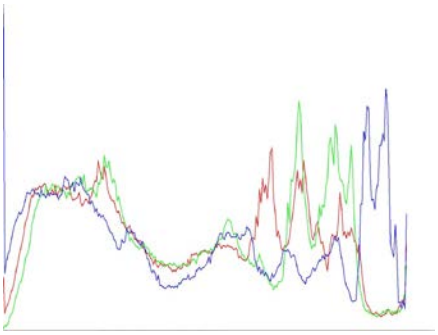

Figure 14: Histogram Of Stego Image

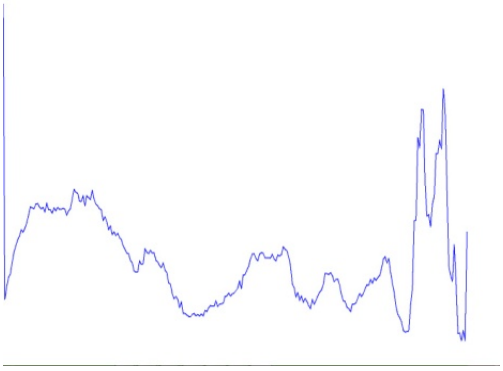

Figure 15: B Component Of Stego Image

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

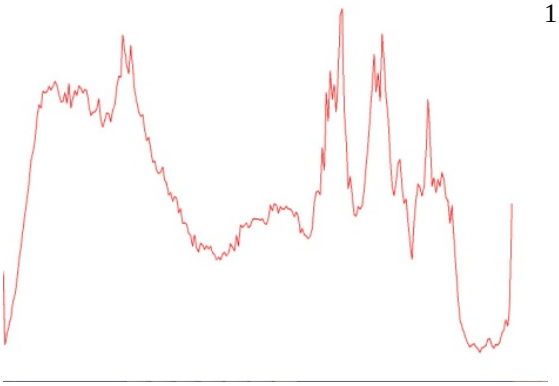

Figure 16: R Component Of Stego Image

From the above experimental results it is clear that our proposed method provides better security than existing Steganographic methodologies. The probability of detecting the hidden data is reduced effectively since we are not altering our Data Image. When using the traditional approach of Steganography the secret data in the image can be detected once the person doing the Steganalysis knows that the image is altered to hold the data. But this is not possible in our proposed method and thus the security is improved making the detection of data impossible. Also the amount of data that can be hidden in image is increased using our method. Even a small data image can hold large data since we are not hiding the data in LSB in our Data Image. We can use all the bits of Data Image in our method, hence large data could be hidden efficiently. To hold the large data we just need a cover image which is large enough to hold the indices of the bit positions of secret data in Data image.

4. CONCLUSION AND FUTURE WORKS

A new method for secure Steganography is proposed in this paper. It modifies the existing Steganographic techniques to provide better security. Using two images it escapes the attention of the person doing the Steganalysis. The image containing the actual data is not suspected at all. The experimental results demonstrate the practicability of this method and also prove that large amount of data can be hidden efficiently using this method.

Our Index Based Steganography method can be improved in several ways:

Using the different embedding algorithms based on our approach.

1. Using Frequency Domain techniques for embedding the Index File Data in Cover Image.

ACKNOWLEDGEMENT

We would like to thank Tarun Pratap Singh, Shailendra Jain, Chetan Singh Umath for their wonderful cooperation.

REFRENCES:

[1] S. K. Moon and R.S. Kawitkar, “Data Security using Data hiding”, IEEE International Conference on computational intelligence and multimedia applications, vol. 4, pp. 247-251, Dec. 2007.

[2] Adnan Gutub, Ayed Al-Qahtani, Abdulaziz Tabakh, “Triple - A: Secure RGB Image Steganography Based on Randomization”, IEEE/ACM international conference on computer systems and applications, pp. 400 - 403, 2009.

[3] W. N. Lie and L. C. Chang, ”Data Hiding in images with adaptive numbers of least significant bits based on human visual system”, IEEE international conference on image processing, vol. 1, pp. 286-290, 1999.

[4] Eric Cole,"Hiding in Plain Sight: Steganography and the Art of Covert Communication", Wiley Publishing, 2003.

[5] Neil F. Johnson and Sushil Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE, pp. 26-34, 1998.

[6] Donovan Artz, Los Alamos National Laboratory, “Digital Steganography: Hiding Data within Data”, IEEE Internet Computing: vol. 5, no.03, pp. 75-80, 2001

[7] Neil F. Johnson and Stefan C. Katzenbeisser, “A survey of Steganographic techniques”, In Information Hiding: Techniques for Steganography and Digital Watermarking, Boston, Artech House pp. 43-78, 2000.