DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4446

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

STEGANOGRAPHIC METHOD BY MATHEMATICAL ODD-EVEN SEQUENCE

Pammi Anusha
Department of Information Technology
Bharati Vidyapeeth University, College of Engineering
Pune, India

Abstract: Security for data transmission has a great importance in modern communication. Security for information involves defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take. In this paper data in the binary form are transferred by embedding data bits into digital image bits in a pattern so that to enhance the security to data. For secured transmission of data, the data bits are hidden in the image bits using mathematical formula so that the main data cannot be recognized by unauthorized person.

Keywords: Data hiding, Steganography, Cover image, Stego image, pixel.

1. INTRODUCTION

Data transmission through image steganography has increased its importance in secure data communication. Digital image steganography provides a way for the sender to send data as secured as possible that is impossible to extract by the unauthorized person. Image Steganography is used to hide original data bits in the image bits by embedding data bits in a pattern that cannot be extracted by unknown.

In image steganography the original image that is used as media is called as cover image. When the data bits that are to be sent are embedded into bits of this cover image then it is called as stego image. There are many techniques used to embed the data bits in a certain pattern in to the image bits.

There are two ways by which security can be provided for the data. They are Encryption and Steganography. Encryption is considered to be a commonly used technique in order to provide information security [1]. Encryption is a method where message is changed in such a way that unauthorized person cannot understand the original data.

The idea of secret communication is as old as data communication [2]. The main goal of steganography is to hide data using some other media like image, so that the hackers cannot recognize the stego file and the data [3]. Encryption differs from steganography, as encryption does not able to hide the fact that message exists in data communication [4].

In steganography there are two types, they are Linguistic steganography and Technical [5]. Linguistic steganography can be defined as collection of techniques and methods that allow hiding digital information in text [6]. Technical is another type of steganography in which it uses a scientific method to conceal a secret message, such as the use of invisible ink, microdots.

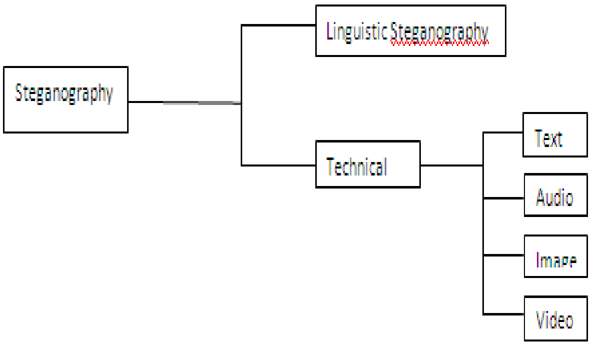

Figure1. Branches of Steganography

Technical steganography is achieved by using some media such as Text, Audio, Image, and Video. Text steganography is implemented by changing the words of text that already existing [7]. In audio steganography the data to be sent is embedded in the frames of audio file [8]. In video steganography the data can be embedded into frames and can be viewed as sequence of still image [9]. There are many techniques involved in image steganography like LSB (least significant bit) method, DCT (Direct cosine transform) method, Wavelet transform method [10].

In digital image steganography the data that is to be sent confidentially is changed to the binary form and embedded into the pixels of the image. The image that is used for data communication is called cover image [11]. The image after embedding the data bits is called stego image [12]. Image steganography is one of the popular methods of data communication in order to provide security for the data.

Steganography is used in many applications such as copyright control of materials, enhancement of robustness of image search engines and smart IDs (identity cards) [13]. Steganalysis is the technique used to attack the steganography methods. There are different types of steganalysis such as attacks can be done to stego only, known carrier et cetera [14].

2. PREVIOUS WORK

A digital image is nothing more than data numbers indicating variations of red, green, and blue at a particular location on a grid of pixels. Most of the time, we view these pixels as miniature rectangles sandwiched together on a computer screen. Each pixel consists of three bytes. These bytes are of length eight bits, it means total 24 bits in a pixel.

The data that is to be sent is first converted into binary form; these binary bits are embedded into the bits of an image. There are many techniques proposed since last decade in order to embed the data bits into image bits and send it in such a way to enhance security that is to protect the data from attackers.

There are many techniques in image steganography. These techniques are divided into four domains [15] they are spatial domain methods, transform domain technique, distortion Techniques, masking and filtering.

To hide data in an image, the mostly frequently used technique is embedding data in LSB (least significant bit) [16]. In this technique it is difficult to differentiate the cover image and stego image. When changing the bits in LSB there will not be vast change in magnitude of the pixel which results in no change in the image after embedding the bits. So it is considered to be most preferred algorithm. This is one of the methods in spatial domain technique.

In spatial domain there is another method called Pixel value differencing technique (PVD). It is considered to be one of the reliable algorithm in which all the colors of the pixel are separated [17] and formed as separate matrix M*N, and data is embedded in these matrix in sequence manner.

Transform domain technique in image steganography is more complex way of hiding data uses various algorithms and transformations to hide the data in image. Discrete Wavelet transformation technique (DWT) is one of the techniques of transform domain [18] which uses sines and cosines in fourier analysis. Some other techniques of transform domain are Discrete Fourier transformation technique (DFT), Discrete cosine transformation technique (DCT), Lossless or reversible method (DCT), Embedding in coefficient bits [15].

Distortion technique (DT) is a domain of image steganography in which decoding process requires the original cover [19], and a sequence of modification are done to the message in order to communicate secretly. Masking and filtering techniques are similar to watermarking [20]. These techniques use more significant area to embed the message which is used to hide into noise level [21].

In this paper, a new technique is used by which bits are embedded in LSB (Least significant bit) in certain pattern. Let us consider normal LSB algorithm with an example.

EXAMPLE: Let us suppose the data to be sent is 100101001

The original image data:-

10010011 11001101 00100101
10101010 00110011 01011101
00010111 11011011 10100011

The data bits are embedded as follows:

1001001**1** 1100110**0** 0010010**0**
1010101**1** 0011001**0** 0101110**1**
0001011**0** 1101101**0** 1010001**1**

There are many techniques implemented inorder to embed bits in LSB (Least significant bit). One such technique is to embed bits in one to four bits of LSB (least significant bit) of image bits [22]. LSB (Least significant bit) algorithm is easiest method that can be easily decoded, so the message in encrypted initially and then embedded into the bits using LSB algorithm [23].

3. PROPOSED WORK

In this paper a new technique is used in which LSB algorithm is used. The bits are embedded into the least significant bits of the byte in the selective pixels. These pixels are selected by considering a key that is choosen by the sender. The same key is communicated to the receiver by which extraction of bits are done. The key value is substituted in the formula, which gives an integer as a result and this number is choosen to embed the data bits.

Method:

Initially sender had to select a number (n).

- ❖ If n is odd, then sender substitutes the n value in below formula:

  $((n-1)*k)/2$

  Here $k=1, 2\ldots, n>3$.

- ❖ If n is even ,then sender has to follow the formula:

  $(((n-1)*k) + \lambda)/3$

  Where $\lambda=0$ or 1 or -1, according to the situation

  Here $k=1, 2\ldots., n>2$.

Here n is number selected by the sender and communicated to receiver, k is a set of natural numbers, and λ value is implemented as per the requirement.

Let us consider an example:

- Let us take n value as 25

  As n is an odd number , we substitute in $((n-1)*k)/2$.

  $((25-1)*1)/2= 12$
  $((25-1)*2)/2= 24$
  $((25-1)*3)/2= 36$

  The data that is to be transmitted is embedded in the pixel line numbers 12, 24, 36……..

- Let us consider n value to be 54

  As n is even number, we substitute in $(((n-1)*k) + \lambda)/3$
  $(((54-1)*1) +1)/3= 18$ [here λ is taken as 1 as the 53 is not divisible by 3]
  $(((54-1)*2) +1)/3= 36$
  $(((54-1)*3) +1)/3= 54$

The data that is to be transmitted is embedded in the pixel line numbers 18, 36, 54…

When the number minus one divisible by 3 then the λ value is considered to be 0, if the number minus one is not divisible by 3 then λ value is taken as +1 or -1 as per the satisfying condition.

After calculating the line numbers, the data that is to be sent is embedded in the line number using LSB algorithm. The n value must be communicated through some media to the receiver in order to extract the bits from the image.

4. ALGORITHMS

In this paper two algorithms are given in which first algorithm is used to embed the data bits into image bits. The second algorithm is to extract the data bits from the image.

4.1 Embedding algorithm

a. Read characters from data file, convert the ASCII values equivalent to its binary value.
b. Read the bits from the image.
c. Select ‘n’ value that should be communicated to the receiver.
d. If ‘n’ value is even, then use $(((n-1)*k) + \lambda)/3$ formula to calculate lines in which the data bits are embedded.
e. If ‘n’ value is odd, then use $((n-1)*k)/2$ formula to calculate line in which the data bits are embedded.
f. Embed the bits in LSB (least significant bit) of the line which are calculated using the above‘d’ and ‘f’ steps.
g. Repeat the step ‘f’ till the end of the data.
h. Represent a termination character at the end of data which is explicitly chosen by sender.

In the above algorithm, the bits that are to be transmitted are embedded in certain pixels using specified formula. When the line numbers are calculated the bits can be embedded in that selected pixels using LSB algorithm.

4.2 Extraction algorithm

a. Open the stego image.
b. By using the ‘n’ value that is used by sender to calculate the line number, find the line numbers by using the same formula.
c. Extract the least significant bits of the specified pixels that are calculated using the formula.
d. Repeat the process and print the values, until a termination symbol is found.

At the receiver side the extraction of bits is done by using ‘n’ value. By substituting this n value into the formula the line at which data is embedded is found. The LSB values of the selective pixels that are taken from the formula is the data.

5. RESULT

As per observations, it is found that the proposed algorithm enhances the security of data and increases the encoding strength.

Table 1. Comparison of algorithms

Algorithms	Security	reliability	Encoding strength
Simple LSB Algorithm	Medium	high	medium
Proposed algorithm	High	high	high

In the above table, comparison has been done between the simple LSB and the proposed algorithm. According to the observations it is found that the proposed algorithm has a good encoding strength and communication of data can be more secure. The proposed algorithm can provide 90% of secure data communication.

In Figure 1, we have a original image which is used for the data communication using image steganography. This image is used to hide the data that should be communicated secretly. The RGB pixels of this original image are used in order to embed the original data bits.

Figure 2. Original Image

This original image is used and the data bits are embedded into the LSB of selective pixels, which are calculated by using the algorithm proposed in this paper. The image that is formed by embedding the bits is called stego image. There will be slight change in the image which cannot be recognized by human eye.

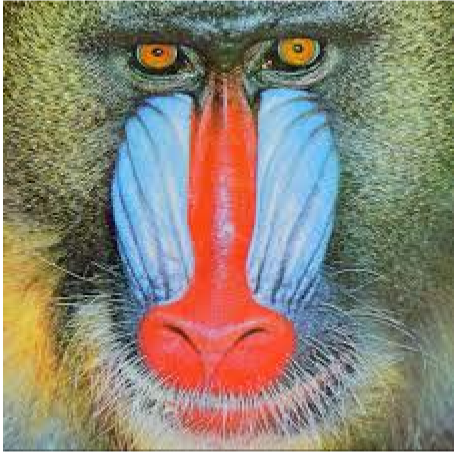

Figure 3. Stego image

6. CONCLUSION

The proposed algorithm has the following advantages:

a. Small changes are done in the pixels, so there is only a slight change in image that cannot be recognized by human eye.
b. Provides security and reliability of data.

We conclude that the proposed algorithm is developed using image steganography. This algorithm can be used when a data must be transmitted secretly and should posses’ reliability. Modifications to the proposed algorithm may provide further security for the data.

REFERENCES

[1] E. Thambiraja, G. Ramesh, Dr. R. Umarani, “A Survey on Various Most Common Encryption Techniques” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July **2012**, pp. 226-233.

[2] Saraju. P. Mohanty, ”Digital Watermarketing: A tutorial review” http://citeseer.ist.psu.edu/mohanty99digital.html , visited 15 June **2005**, pp.1-24.

[3] Bowsiya Begum M, Selvamary D, “Color Image Steganography with Double Encryption” International Conference on Electrical, Information and Communication Technology, February **2015**, pp. 69-71.

[4] Shikha Mohan, Satnam Singh, “Image Steganography: Classification, Application and Algorithms”, International Journal of Core Engineering & Management (IJCEM), Volume 1, Issue 10 January **2015,** pp. 93-96.

[5] C.P.Sumathi, T. Santanam, G.Umamaheswari, “A Study of Various Steganographic Techniques used for Information Hiding”, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December **2013**, pp. 9-25.

[6] M. K. Kaleem, “AN OVERVIEW OF VARIOUS FORMS OF LINGUISTIC STEGANOGRAPHY AND THEIR APPLICATIONS IN PROTECTING DATA”, Journal of Global Research in Computer Science , Volume 3, No. 5, May **2012**, pp. 33-37.

[7] Abhishek Koluguri , Sheikh Gouse , Dr. P. Bhaskara Reddy ,” Text Steganography Methods and its Tools”, International Journal of Advanced Scientific and Technical Research Issue 4 volume 2, March-April **2014**, pp. 888-902.

[8] Masoud Nosrati, Ronak Karimi, Mehdi Hariri, “Audio Steganography: A Survey on Recent Approaches”, World Applied Programming, Vol (2), No (3), March **2012**, pp. 202-205.

[9] Sherly A P and Amritha P, “A Compressed Video Steganography using TPVD”, International Journal of Database Management Systems (IJDMS) Vol.2, No.3, August **2010**, pp. 67-80.

[10] Shashikala Channalli, Ajay Jadhav, “Steganography an Art of Hiding Data”, International Journal on Computer Science and Engineering Vol.1 (3), **2009**, pp. 137-141.

[11] K. Stefan and A. Fabien, “Information hiding techniques for steganography and digital watermarking”, Artech House Books, December **1999**.

[12] Debnath Bhattacharyya, Arpita Roy, Pranab Roy, and Tai-hoon Kim, “ Receiver Compatible Data Hiding in Color Image”, International Journal of Advanced Science and Technology, Volume 6, May, **2009**, pp. 15-23.

[13] A.Cheddad, J.Condell, K.Curran and P. Mc Kevitt, “Digital Image Steganography: Survey and Analysis of Current Methods”, volume 90, Issue 3, March **2010**, pp.727-752.

[14] R.Poornima and R.J.Iswarya ,”AN OVERVIEW OF DIGITAL IMAGE STEGANOGRAPHY” International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.1, February **2013**, pp. 23-31.

[15] Mehdi Hussain and Mureed Hussain, “A Survey of Image Steganography Techniques”, International Journal of Advanced Science and Technology, Vol. 54, May, **2013,** pp. 113-124.

[16] R. Chandramouli and Nasir Memon, "Analysis of LSB Based Image Steganography Techniques", International Conference on Image Processing, October 7-10, **2001**, Thessaloniki, Greece, Vol. 3, pp. 1019-1022.

[17] J. K. Mandal and Debashis Das, “Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain”, International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July **2012**, pp. 83-93.

[18] Gurmeet Kaur and Aarti Kochhar, “Transform Domain Analysis of Image Steganography”, International Journal for Science and Emerging Technologies with Latest Trends, **2013**, pp. 29-37.

[19] Hamid.A.Jalab, A.A.Zaidan, B.B.Zaidan, “ New Design for Information Hiding with in Steganography Using Distortion Techniques”, IACSIT International Journal of Engineering and Technology Vol. 2, No.1, February **2010**, pp.72-77.

[20] Masoud Nosrati, Ronak Karimi, Mehdi Hariri, “An introduction to steganography methods”, World Applied Programming, Vol. 1, No. 3, August **2011**, pp. 191-195.

[21] Rashi Singh, Gaurav Chawla, “A Review on Image Steganography”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 5, May **2014**, pp.686-689.

[22] Namita Tiwari, Dr.Madhu Shandilya, “Evaluation of Various LSB based Methods of Image Steganography on GIF File Format”, International Journal of Computer Applications, Volume 6, No.2, September **2010**, pp.1-4.

[23] Shailender Gupta, Ankur Goyal, Bharat Bhushan, “Information Hiding Using Least Significant Bit Steganography and Cryptography”, I.J.Modern Education and Computer Science, vol. 6, **2012**, pp. 27-34.