ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

Random Insertion Using Data Parity Steganography Technique

Dipti.G.Dighe, N.D.Kapale
M.E (2nd year) Electronics S.R.E.S college of engineering Kopargaon, Associate prof. Dept. of E&TC college of engineering Kopargaon

Abstract*— Steganography involves transmitting secret messages through seemingly innocuous files. Hiding information by embedding secret data into an innocuous medium is often referred to as Steganography. In this paper message bits are embedded randomly to achieve the higher security. Selected components of pixel are used for embedding. This paper investigates how the parity of data can be used effectively to hide a secret message randomly in the image.

Index Terms— **Random insertion, steganography, Two LSB.**

I. INTRODUCTION

In many situations, transmitting a cryptographic message draws unwanted attention. The use of cryptographic technology may be restricted or forbidden by law. In the computer world, it is very important to keep secret information secret, private information private, and when profits are involved, protect the copyrights of data. To accomplish these difficult tasks, new methods based on the principle of steganography is being developed and used. Steganography is the art and science of communicating in a way which hides the existence of the communication [1]. Steganography is commonly misinterpreted to be cryptography or watermarking. While they are related in many ways, there is a fundamental difference in the way they are defined and the problems to which they are applied. Cryptography hides the content of a secrete message from a malicious people, where as steganography even conceals the existence of the message. Steganography must not be confused with cryptography, where we transform the message so as to make it meaning obscure to malicious people who intercept it. Therefore, the definition of breaking the system is different. In cryptography, the system is broken when the attacker can read the secrete message. Breaking a steganographic system need the attacker to detect that steganography has been used and he is able to read the embedded message. In cryptography, the structure of a message is scrambled to make it meaningless and unintelligible unless the decryption key is available. In other word, steganography prevents an unintended recipient from suspecting that the data exist. A steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion. [2] As an example, it is possible to embed a text inside an image or an audio file.

This technique is based on RGB images. The two least significant bits of the red channel will be used as an indication to the existence of hidden data in green and blue channels. Before embedding the data bits, the parity of the data has been checked [8][16]. Then according to the content of red component data is placed into the pixel. The selection of pixels to embed was crucial since two controlling elements are used for modification of pixel. The technique used random insertion of bits; every pixel doesn't carry the message bits, so it is difficult to detect presence of information in the pixel.

II. PROPOSED SCHEME

RGB image consist of 3 colors red, green & blue. Image component is given by equation (1). Here R(x,y) is used as a controlling element & pair of data bits are embedded into G(x,y) & B(x,y). For any sequence of message bit pairs (m1, m2) (m3, m4). .. .. (m i-1,mi) ,we will compare the message bits with current G(x,y) and B(x,y) and by using table 2 and 3 data bits will get added into pixels. Whether to embed odd or even parity data is decided by performing modulus operation on R(x,y) which is obtained by equation (2).

F(x,y)=R(x,y)+ G(x,y)+ B(x,y) …(1)

(R(x,y) + 2) mod(4) = 0 …(2)

If equation (2) satisfies the condition, difference between message bit pairs & two least significant bits of G(x,y) is calculated using equation (3). If OE is less than ±2, even parity data is embedded into G(x,y).

OE = G(b1,b0) -(mi-1,m i) … (3)

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

Where, b0 and b1 are two least significant bits of pixel. Same technique is used for embedding in B(x,y). OE decides whether to embed or not. If equation (2) does not satisfy the condition, then pair of odd data bits is embedded. OE is used to control embedding data rate. The OE variable affects probability of embedding payload. For maximum efficiency, value of OE must be in between -1 to +1. The following steps are used to embed data in pixels:

Table 1 Embedding scheme

2 LSBs of red	2 LSBs of green	2 LSBs of blue
00	Add data	Add data
01	Add odd parity data	Add odd parity data
10	Add even parity data	Add even parity data
11	Add data	Add data

Table 1 shows the embedding scheme for data bits. If two least significant bits of red color is 10 then embed the even parity bits of the message, otherwise if it is 01 then place the odd parity bits in to the green color and blue color component in pixel as follows

If data bits are 00 then

$$G(x,y) = \begin{cases} G(x,y) & \text{for } g00,g10,g11 \\ G(x,y) - 1 & \text{for } g01 \end{cases} \quad \ldots(4)$$

If data bits are 11then

$$G(x,y) = \begin{cases} G(x,y) & \text{for } g00,g01,g11 \\ G(x,y) + 1 & \text{for } g10 \end{cases} \quad \ldots(5)$$

$$\text{For } R(x,y) \text{ , } mod(2) \; ! = 0 \quad \ldots(6)$$

If data bits are 01 then

$$G(x,y) = \begin{cases} G(x,y) & \text{for } g01,g11 \\ G(x,y) - 1 & \text{for } g10 \\ G(x,y) + 1 & \text{for } g00 \end{cases} \quad \ldots(7)$$

If data bits are 10 then

$$G(x,y) = \begin{cases} G(x,y) & \text{for } g10,g00 \\ G(x,y) - 1 & \text{for } g11 \\ G(x,y) + 1 & \text{for } g01 \end{cases} \quad \ldots(8)$$

Equation (4), (5), (7) and (8) are used to embed the message bits in to green color. Same equations can be used to embedding in blue color. We have placed the message bits in B(x,y) after performing the operations on G(x,y) If the contents of R= 10 and at the same time if data bit s are 00 or 11

Table 2 Embedding scheme when R = 10

	d00	d11
For G=00	G=G	DON'T ADD
For G=01	G=G-1	DON'T ADD
For G=10	DON'T ADD	G=G+1
For G=11	DON'T ADD	G=G

If the contents of R=01 and at the same time if data bits are 00 or 10

Table 3 Embedding scheme when R = 01

	d01	d10

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

For G=00	G=G + 1	DON'T ADD
For G=01	G=G	G=G+1
For G=10	G=G -1	G=G
For G=11	DON'T ADD	G=G - 1

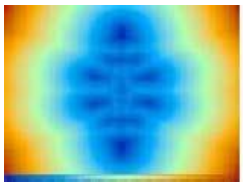
If equation (6) satisfies the condition & data bits are having even parity. Then equation (9) can be used to embed the data. In this case pixel value will be changed without embedding data bits. This is undesired operation which helps to degrade the image. But embedding capacity is increases. Since some of the pixel doesn't carry any information, it is difficult to detect the pixel which carries the information. When contents of R are 00 or 11 then add the message bits without checking any condition. It has been observed that if we use parity check for R= 00 or 11, around 35 to 40% pixels get wasted, which doesn't carry the message bits. Our aim is to provide higher security with higher embedding rate.

III. EXPERIMENTAL RESULTS

All pixels will not participate in embedding of message, as embedding of data is depends on the parity of message bits; the algorithm is tested by two ways. First, different images of same size have been taken for inserting the same message. And then different messages of same size have been taken to insert in one image. Some experiments are also performed on different size of images and different size of messages. Experimental result shows that 65 to 74 percent of pixels contained data. For embedding data bits in to image OE must be less than ±2, it is observed that equation (2) limits the embedding rate. This is because of random insertion. These Images are taken from www.google.com


Img_1


Img_2


Img_3


Img_4

Fig 1. Cover images.

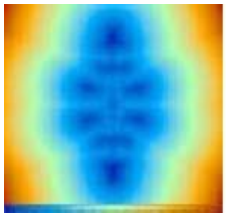


Fig 2.stego images

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

IV. CALCULATION OF PSNR

The mean squared error between the cover image and the stego-image (embedding distortion) can be used as one of the measures to assess the relative perceptibility of the embedded text. [3][6]. In order to avoid the stego-image from being suspected of hiding secret information in, the quality of the stego-image should not be degraded significantly. Usually, the PSNR (Peak Signal-to-Noise Ratio) formula is used to evaluate the distortion between the pre-processing image and the post-processing image.

$$MSE = \left[\frac{1}{X * Y}\right] \sum_{I}^{X} \sum_{J}^{Y} \left[X_{IJ} - X'_{IJ}\right]^2$$

$$PSNR = 10 \log_{10} [(2^{n} - 1) / MSE]$$

The **x** and y stand for image's height and width, respectively. The Xij and X'_{ij} represent the preprocessing image pixel value in position (i,j) and the post-processing image pixel value in position (i,j), respectively. Theoretically, if the distortion between the preprocessing image and the post processing image is small, the value of PSNR comes out larger. Therefore, a larger value of PSNR means that the processed image has better quality. Usually, if the PSNR value is greater than or equal to **30** db, the distortion between the original image and the processed image is not suspicious to the human eye The experiment is performed on different images to calculate PSNR. The figure 1 shows the cover images and figure 2 shows the respective stego images. Cover images are taken from google.com. Table 4 illustrates the PSNR values and mean square error.

Table 4 PSNR Values of the images

IMAGE	MSE	PSNR
Img_1	0.7292	148.1678
Img_2	0.7932	147.5643
Img_3	0.7900	147.5928
Img_4	0.6449	152.8843

V. CONCLUSION

Since two LSB's are used for embedding. Present method is having high embedding rate. The capacity of the algorithm is better. Experimental result shows that PSNR ratios of images are founds to be much more than 30dB. Thus processed images are not suspicious to the human eye, along with this advantage the random insertion method is used. And thus the transmission of data is highly secured.

ACKNOWLEDGMENT

I express my gratitude to our guide **Prof. N. D. Kapale** for providing me adequate facilities, way and means by which we are able to complete this paper. I am also thankful to my departmental staff for sharing their knowledge with me.

REFERENCES

[1] Chen Ming Zhang Ru Niu Xinxin Yang Yixian "Analysis of Current Steganography Tools: Classifications & Features" Proceedings of the 2006 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH- MSP'06) 0-7695-2745-0/06 © 2006 IEEE.

[2] Elvin M. Pastorfide and Giovanni A. Flores "An Image Steganography Algorithm for 24-bit Color Images Using Edge-Detection Filter" Cmsc 190 Special Problem, Institute of Computer Science 2006 ICS University of the Philippines Los Banos.

[3] Venkatraman.S, AjithAbraham, Marcin Paprzycki, "Significance of Steganography on Data Security" IEEE Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04) 0-7695-2108-8/04 © 2004 IEEE.

[4] Neil F. Johnson Sushil Jajodia George Mason University "Exploring Steganography Seeing the Unseen" Computer0018-9162/98© 1998 IEEE February 1998 pg. 26 to 34.

[5] Abdul-Rahman Shaheen, Mahmoud Ankeer, Muhammed Abu Ghalioun "Using Pixel Indicator Technique in Images for Better Steganography".

[6] Chin-Chen Chang Iuon-Chang Lin "A New (t, n) Threshold Image Hiding Scheme for Sharing a Secret Color Image" Department of Computer Science and Information Engineering, Proceedings of ICCT.2003 pg.196 to 201.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

[7] Andrew D. Ker, "Steganalysis of Embedding in Two Least-Significant Bits" IEEE Transactions On Information Forensics And Security, Vol. 2, No. 1, March 2007. pg. 46 to 54.

[8] Rajkumar , Rahul Rishi, Sudhir Batra, "A New Steganography Method for Gray Level Images using Parity Checker", International Journal of Computer Applications (0975 – 8887) Volume 11– No.11,December 2010.

[9] N. Johnson and S. Jajodia, "Exploring steganography: seeing the unseen," IEEE Computer, pp. 26-34, February 1998.

[10] Mehdi Kharrazi1, Husrev T. Sencar2, and Nasir Memon2 "Image Steganography: oncepts and active" WSPC/Lecture Notes Series: 9in x 6in April 22, 2004.

[11] Jarno Mielikainen, Member, IEEE "LSB Matching Revisited" IEEE Signal Processing Letters, Vol. 13, No.5, May 2006 Pg.285 To 287.

[12] Jun Zhang Ingemar J. Cox and Gwena¨el Do¨err. "Steganalysis for LSB Matching in Images with High- frequency Noise" MMSP 2007 1-42441274- 9/07©2007 IEEE pg. 385 to 388.

[13] Andrew D. Ker "Steganalysis of LSB Matching in Grayscale Images" IEEE Signal Processing Letters, Vol. 12, No. 6, June 2005 Pg. 441 To 444.

[14] Joyshree Nath, Asoke Nath "Advanced Steganography Algorithm using Encrypted secret message"(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011.

[15] Weiming Zhang, Xinpeng Zhang, and Shuozhong Wang, A Double Layered "Plus-Minus One", Data Embedding Scheme, IEEE SIGNAL PROCESSING LETTERS, VOL. 14, NO. 11, NOVEMBER 2007.

[16] Sampath Kumar Dara, Harshavardhan Awari, "Tree Based Parity Check Scheme for Data Hiding", International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5, September 2012.

[17] Joyshree Nath, Sankar Das, Shalabh Agarwal, Asoke Nath," Advanced Steganographic Approach for Hiding Encrypted Secret Message in LSB, LSB+1,LSB+2 and LSB+3 Bits in Non standard Cover Files", International Journal of Computer Applications (0975 – 8887) Volume 14– No.7, February 2011.

AUTHOR BIOGRAPHY

Miss. Dipti G. Dighe. Pursuing M.E (Electronics) from S.R.E.S college of engineering Kopargaon. Completed B.E (E&TC) from M.A.E Alandi in 2011 with first class.

Prof. N. D. Kapale, Associate prof. Dept. of E&TC College of engineering Kopargaon. Pursuing PHD from COE pune. Completed M.E (Electronics) from Walchand College of engineering, Sangali in 2007. Completed B.E (Industrial Electronic) from SSGN College of engineering Shegaon in 1994.