International Journal of Scientific Research and Engineering Development-– Volume 6 Issue 5, Sep- Oct 2023

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Data Transmission Using Steganography

Mr. Deepak U. Chaudhari
M.E. (E&Tc),
MVPS's Rajarshi Shahu Maharaj Polytechnic, Nashik, Maharashtra, India
deepak.chaudhari@rsmpoly.org

Mrs. Ashwini H. Kale
M.E. (E&Tc),
MVPS's Rajarshi Shahu Maharaj Polytechnic, Nashik, Maharashtra, India
ashvini.kale@rsmpoly.org

Mrs. Gayatri B. Ghangale
M.E. (E&Tc),
MVPS's Rajarshi Shahu Maharaj Polytechnic, Nashik, Maharashtra, India
gayatri.ghangale@rsmpoly.org

Abstract:

In this paper data bits are embedded randomly to achieve the highest securityby combiningsteganography& cryptography. To protect the contents of a messageCryptography is used &to protect both messages andcommunicating partiessteganography is used. To improve data capacity in an image2LSB technique is used.The study of invisible communication is called Steganography. In Steganography usually hide the existence of the communicated data in such a way that it remains confidential & it maintains secrecy between two communicating parties. How the parity of data can be used effectively to hide a secret message randomly in the image is explain in this paper. To hides the content of a private message from a unwanted people used Cryptography, whereas steganography even conceals the real message. Steganography & cryptography are commonly different concepts. The relation between them is related in many ways, the fundamental difference between them in the way they are defined and application of them for the different problems to which they are applied. Steganography & cryptography are different & where we transform the message so as to make it meaning obscure to unwanted people who intercept it. So, the definition of breaking the system is different.The structure of a message is jumbled in cryptography to make it meaningless and unintelligible unless the decryption key is detected.

Keywords: Steganography, Cryptography, Random insertion, 2 LSB.

I. INTRODUCTION

In todays computer world, it is very important to keep secret information secret, private information private, and when profits are involved, protect the copyrights of data. Thenew methods based on the principle of steganography is being developed and used to accomplish these difficult tasks,.Many times, a cryptographic message transmition gives unwanted attention [3]. The cryptographic concept may be restricted for use. The combination ofart and science of communication in a way which hides the existence of the communication is called Steganography.

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.[9]. The parity of the data has been checked, before embedding the data bits [5]. Then data is placed into the pixel according to the content of red component. The selection of pixels to embed was crucial since two controlling elements are used for modification of pixel. Every pixel doesn't carry the message bits in the technique used random insertion of bits, so it is difficult to detect & correct presence of information in the pixel [7].In other word, steganography prevents a unwanted recipient from suspecting that the data exist. A steganography system when embeds hidden content in unexceptional cover media so as not to produce an eavesdropper's suspicion. [1]. It is possible to embed a text inside an image or another file.

II. PROCESS PROPOSED SCHEME

The system is broken in cryptography when the hacker can read the secrete message. To break a steganographic system attacker have to detect that steganography has been used and he is detect to read the embedded message[8]..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 the sequence of message bit pairsdata bits will get added into pixels for (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. 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 above equations satisfies the condition, difference between two least significant bits&message bit pairs 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,mi)...(3)

Where, b0 and b1 are two least significant bits of pixel. For embedding in B(x,y) same technique is used. OE decides whether to embed or not. The pair of odd data bits is embedded if equation (2) does not satisfy the condition, 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. To embed data in pixels the following steps are used:

Table 1. Embedding scheme

2 LSBs of Red	2 LSBs of Green	2 LSBs of Blue
00	Add evenparity	Add evenparity
01	Add oddparity	Add oddparity
10	Add evenparity	Add evenparity
11	Add oddparity	Add oddparity

Table 1 shows the embedding scheme for message bits if two least significant bits of red color is divisible by 2 then and only then embed the even parity bits of the message Otherwise place the odd parity bits in to the green color and blue color component of that particular pixel. According to the following steps.

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

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

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

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

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

Equations (4) to (8) are used to embed the message bits into green color. To embedding in blue color same equations

can be used. We have performing the operations on G(x,y) and placed the message bits in B(x,y).

If R=00 or R=10 and data bits are 00 or 11 then

Table 2. Embedding scheme when R = 00orR=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 R=11 and data bits are 00 or 10 then

Table 3. Embedding scheme when R = 01 R=11

	D01	D10
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 data bits are having even parityand equation (6) satisfies the condition &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 degrade the quality of 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 R=00 or R=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 target is to providehigher embedding rate and higher security.

III. EXPERIMENTAL RESULTS

Take differentsame size imagesfor inserting the same message and then different messages of equal size have been taken to insert in one image. Other experiments are also performed ondifferent size of messages and different size of images.As embedding of data is depends on the parity of message bits all pixels will not participate in embedding of message; the algorithm is tested by two different ways. Experimental results show that 66 to 75% 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.

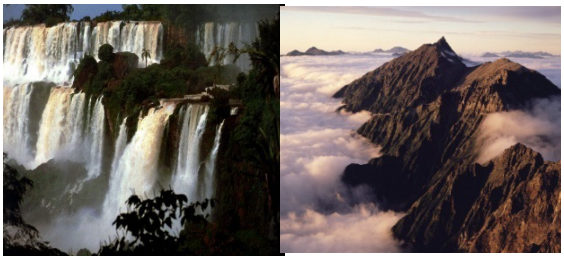

Image 1 Image 2

Image 3 Image 4

Fig 1. Cover images

Image 1 Image 2

Image 3

Image 4

Fig 2.Stego images

IV. CALCULATION OF PSNR

To avoid the stego-image from the suspected of hiding secret information the quality of the stego-image should not be down significantly. The mean squared error between thestego-image and thecover image (embedding distortion) can be used as one of the measures to assess the relative perceptibility of the embedded text. [4]. Therefore, the Peak SignaltoNoise Ratiois used to evaluate the distortion between thepost-processing image and thepre-processing image.

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

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

The **x** and y stand for image's height and width, respectively. The Xij and Xiij 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,processed image has better qualityif larger value of PSNR is calculated. Usually, if the value of the PSNR is greater than or equal to **30** db, the distortion between the processed image andoriginal image is not suspicious to the human eye.Different types of images are used to calculate the PSNR. The figure 1 shows the cover images and figure 2 shows the respective stego images. Cover images are taken from google.com. Following table illustrates themean square error andPeak SignaltoNoise Ratio values.

Table 4. PSNR Values of the images

Image	MSE	PSNR
Image 1	0.7316	37.2678
Image 2	0.7814	35.4343
Image 3	0.7336	36.5528
Image 4	0.7218	40.7283

V. CONCLUSION

As per the above method, the two LSB of pixel will used to embed the data bits therefore the capacity of the algorithm is increase. Encryption and steganography can achieve separate goals. Encryption encodes data such that an unintentional recipient cannot determine thedata. 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 more than 30dB. The main advantage of this process is that the processed images are not suspicious to the human eye because random insertion is used therefore the transmission of data is highly secured.

REFERENCES:

[1].LiuFenlin, Yang, Chunfang, Luo, Xiangyang., Zeng Ying, "Pixel Group Trace Model-Based Quantitative Steganalysis in Multiple Least Steganography", IEEE Transactions for Information Forensics and Security, Vol. 8, No. 1, January 2013.

[2]Jarno Milikainen, "LSB Matching Revisited", Signal Processing Letter, IEEE, Publication :May 2006Volume : 13, Issue : 5, pp. 285- 287.

[3] J.Milikainen, "LSB Matching Revisited" Signal Processing Letters, IEEE, Publication :May 2006Volume : 13, Issue : 5, pp. 265- 287.

[4] J.Kaur and Sanjeev Kumar, " Study and Analysis of various image forsteganographytechniques" IJST Vol.3 Issue 2, September 2012.

[5]LeeChen,L.H. "High capacity image Steganographic model", Visual Image Signal Processing, 147:03,June 2008

[6] Sharp T., "An implementation of key-based digital signal Steganography" in Pro. Information Hiding Workshop, Springer LNCS 2137, pp. 13–26, 2001.

[7] G. Manikandan, M. Kamarasan and N. Sairam "A Hybrid Approach for Security Enhancement by Compressed Crypto-Stagno Scheme ", Research Journal of Applied Sciences, Engineering and Technology 4(6): 608-614, 2012

[8] Bailey, K., and Curran, K., "An Evaluation of Image Based Steganography Methods", Journal of Multimedia Tools and Applications, Vol. 30, No. 1, pp. 55-88, 2006.

[9] Dumitrescu, S. W. Xiaolin and Z. Wang, 2003. Detection of LSB steganography via sample pair analysis. In: LNCS, Vol. 2578, Springer-Verlag, New York, pp: 355 -372.

[10] Sanjeev Kumar&Jagvinder Kaur, " Study and Analysis of Various Image Steganography Techniques" IJCST Vol.2, Issue 3, September 2011

[11] Ahn, L.V. and N.J. Hopper, 2004. Secret-key steganography. In Lecture Notes in Computer Science.Vol. 3027 /2005 of Advances in Cryptology - EUROCRYPT 2004, pp: 323–341. Springer-Verlag Heidelberg.

[12]Ishwarjot Singh andJ.P Raina,"Advance Scheme for Secret Data Hiding System using Hop field & LSB" International Journal of Computer Trends and Technology (IJCT) – volume 4 Issue 7–July 2013

[13]N.FJohnson,Jajodia, S., "Exploring Steganography:Seeing the Unseen", Computer Science Journal, February 2008.

[14] Shabir A. Parah, G.M. Bhat, Javaid A. Sheikh, "Data Hiding in Intermediate Significant Bit Planes, A High Capacity Blind Steganographic Technique", Intenational Conference on Emerging Trends in Science, Engineering and Technology , pp.192-197, July 2012.

[15]Adnan Gutub, Abdulaziz Tabakh,Ayed Al-Qahtani "Triple-A: Secure RGB Image Steganography Based on Randomzation", International Confernce on Computer Systems and Applicatons (AICCSA-2009), pp: 400-403, 10-13 May 2009

[16] Chang, Iuan-Chang ,Chin-Chen., Lin, and Yaun-Hui YU., " A new Steganographic method for color and gray scale image hiding", Computer Vision and Image Understanding, ELSVIER, Vol. 107, No. 3, pp. 183-194,2007.

[17] Malik Swati, Ajit "Securing Data by Using Cryptography with Steganography" Intenational Journal of Advanced Research in Computer Science and Software Enginering, Volume 3, Issue 5, May 2013.

[18] K. M. Singh, L.S. Singh, Singh A. B. and K.S. Devi,"Hiding Secret Message in Edges of the Images", Information and Communication Technology, 2007. ICICT '07, pp. 238-241.

[19] Michel K. Kulhandjian, Dimitris A. Pados, Ming Li, Stella N. Batalama, and Michael J. Medley, "Extracting spread-spectrum hidden data from digital media ", IEEE transactions on information forensics and security, vol. 8, no. 7, july 2013.

[20]Nagaraj V., Dr. Vijayalakshmi V. and Dr. Zayaraz G., "Modulo based Image Steganography Technique against Statistical and Histogram Analysis", IJCGA Special Issue on"Network Security and Cryptography" NSC, 2011.

