International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 05 | May-2016 www.irjet.net p-ISSN: 2395-0072

Data hiding in digital image processing using cryptography and steganography.

[1]Shuchi Agarwal,[2]Dr. Jaipal Singh Bhist

[1] *Mtech Student, Department of electronics and communication engineering , RITS, Bhopal, India*
[2]*HOD and guide, Department of electronics and communication engineering, RITS, Bhopal, India*

Abstract - *Digital image processing gained wide popularity all over the world. In this paper we consider review of digital image processing such as steganography and cryptography.*

***Key Words*: steganography, cryptography, LSB, PSNR, MSE etc.**

1. INTRODUCTION

Internet has become more popular and common now-a-days. High risk is involved in sending the important data through the net. To safeguard the data which includes image, audio and video from illegal hindrance is important in this present era. To prevent such illegal attacks from the unintended observer is important. Various techniques are used for image processing such as steganography, cryptography.

1.1 Steganography.

The word "steganography" is basically of greek origin which means hidden writing. The word is classified into two parts steganos which means "secret" and "graphic" which means "writing". However, in hiding information, the meaning of steganography is hiding text or secret messages into another file such as image, text, sound video.

Steganography can be broadly classified into four categories, and these are

a) Text steganography.

b) Image steganography.

c) Audio steganography.

d) Video steganography.

a)Text steganography-A steganography technique that uses text as the cover media is called a text steganography.It is one of the most difficult types of steganography technique. This is because text files have a very small amount of redundant data to hide a secret message.

b) Audio steganography-A steganography technique that uses audio as cover media is called as audio steganography. It is the most challenging task in steganography. It is the most challenging task in steganography. This is because the human auditory system(HAS) has a large dynamic range that it can listen over. Thus, even a minute change in audio quality also can be detected by the human ears.

c) Video steganography-A steganography technique that uses video as the cover media is called video steganography.

d) Image steganography-A steganography technique that uses images as the cover media is called an image steganography. Hiding secret messages in digital images is most widely used method as it can take advantage of the limited power of the human visual system (HVS) and also because images have large amount of redundant information that can be used to hide a secret message.

1.2 Cryptography

Cryptography is a widely used technique that encrypts plain text to generate cipher (encrypted) text. Data that can be read and understood without any special measures is called plaintext or clear text. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called cipher text. Basically cryptography scrambles data for ensuring secrecy and/or authenticity of information and enables to transmit data across insecure networks so that it cannot be read by anyone except the authorized recipient [1, 2]. Cryptology and cryptanalysis are two main branches of cryptography. Cryptology is to keep plaintext secret from eavesdropper or simply the enemy while cryptanalysis deals with the defeating such techniques to recover information or forging information that will be accepted as authentic.

2. STEPS TO HIDE DATA IN COVER IMAGE.

Suppose we have to hide message 'M' into cover image.

Step 1 Convert the data from decimal to binary.

Message 'M'

[ ]

Step 2 Read the cover image

Fig 1: cover image.

The above cover image is read in pixel value as follows.

144	142	146	152	156	147	151	157
160	155	159	162	133	123	133	145
144	141	141	138	61	55	65	78
120	123	131	144	50	61	74	92
170	167	167	166	61	59	56	59
120	125	131	132	61	59	59	59
124	133	139	131	88	76	77	76
138	153	167	154	139	138	133	132

Table -1: pixel value of cover image.

Step 3 Convert the cover image from decimal to binary.

1001 0000	1001 1010	1001 1100	1001 0010	1001 0110	1001 1101	1010 1111	1010 0101
1010 0000	1001 1011	1001 1111	1010 0010	1000 0101	0111 1011	1000 0101	1001 0001
1001 0000	1000 1101	1000 1101	1000 0100	0011 1101	0011 0111	0100 0001	0100 1110
1001 0000	0111 1011	1000 1101	0011 1101	0101 1101	0011 0111	0100 0001	0100 1110
0111 1000	1010 0111	1000 0011	1001 0000	0011 0010	0011 1101	0100 1010	0101 1100
1010 1010	0101 0011	0101 0011	0101 0011	1010 0110	0011 1101	0011 1000	0011 1011
0111 1100	1000 0101	1000 1011	0100 0001	0101 1000	0100 1100	1100 1100	0100 1100
1000 1010	1001 1001	1010 0111	1001 1010	1000 1011	1000 1010	0111 1011	0111 1010

Table -2: binary conversion of pixel values.

Step 4 Break the byte to be hidden into bits.

Thus [10000001] is divided into 8 bits [1 0 0 0 0 0 0 1].

Step 5 Now hide the data according to the LSB algorithm.

3.STEPS TO INSERT DATA IN IMAGE.

a. Take an input image.

b. Find out the pixel values.

c. Select the pixel on which we want to insert data.

This process of selection of pixel is done as user's choice he may choose pixel continuous or alternate or at a fixed distance.

i) Insert the data values in pixels.

For example a grid for 3 pixels of a 24-bit image can be as follows:

00101101 00011101 11011100

10100110 11000101 00001101

11010010 10101100 01100011

When the number **200**, which binary representation is **11001000**, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

00101101 00011101 11011100

10100110 11000101 00001101

11010010 10101100 01100011

4. CONCLUSIONS

The main goal of this paper is to review different data hiding techniques which includes cryptography and steganography. The main focus is on text steganography which is one of the most difficult types of steganography technique. Text steganography includes how secret image can be embedded and how it can be sent through the internet by fooling grabbers. Many problems are encountered when transferring important data over the network. A safe and secure procedure is needed to transfer them easily. For this purpose simple image hiding techniques are used and the quality of stego images is also improved by using different mechanisms. So the hackers may not the stego image and will know nothing about the embedded secret image in it. The experimental results show that the stego image and the cover image remain more or less identical which is the main focus of this paper. This means that a secret message can be sent to the destination without any glitch and this can be used for image integrity protection and in places where important, undisclosed secrets should be sent to the recipient. Research is going on in privacy protection and intellectual property rights protection. In the future, it is expected to find an even better technique and procedure to hide more data in a cover image. The future focus should be made on even more less modification in the cover image and the differences between the cover image and the stego image should be null when statistically analyzed.

ACKNOWLEDGEMENT

Apart from my efforts, I wish to express our deep sense of gratitude to my guide Dr. Jaipal Singh Bhist, HOD, RITS, Bhopal and special thanks to our Mtech coordinator Professor Aman Sarraf.

REFERENCES

[1]Zhang and Wang, "Binary power data hiding scheme"1434-8411/@2015 Elsevier.

[2]R.Rathna Krupa, "An overview of image hiding techniques in image processing"ISSN:2321-2381@2014 Published by the standard international journals(The SIJ).

[3]Vipul Sharma and Sunny Kumar, "A new approach to hide text in images using steganography"ISSN:2277 128X @2013,IJARCSSE.

[4]W-C Kuo and C-C Wang, "Data hiding based on generalized exploiting modification direction method" The Imaging Science Journal Vol 61 IMAG 324 @ RPS 2013.

[5]Aarti Mehndiratta, "Data hiding system using cryptography and steganography:A comprehensive modern investigation."e-ISSN:2395-0056,p-ISSN:2395-0072@2015,IRJET.NET.

[6]B.Subramanan "Image encryption based on aes key expansion" in IEEE applied second international conference on emerging applicaton of information technology,978-0-7695-4329-1/11,2011.

[7]Vipul Madhukar Wajgade,Dr. Suresh Kumar,Stegocrypto – A Review of Steganography techniques using Cryptography",International Journal of Computer Science and engineering Technology,ISSN:22229-3345,vol. 4,2013,pp. 423-426.

[8] T. Sharp, An implementation of key-based digital signal steganography, Proc. of the 4th Information Hiding Workshop, vol. 2137, pp. 13-26, Springer, 2001.

[9] J. Mielikainen, LSB matching revisited, IEEE Signal Processing Letters, vol. 13, no. 5, pp. 285-287,2006.

[10] X. Li, B. Yang, D. Cheng, and T. Zeng, A generalization of LSB matching, IEEE Signal Processing Letters, vol. 16, no. 2, pp. 69-72, 2009.

[11] Dipti Kapoor Sarmah, Neha bajpai, " Proposed System for Data Hhiding Using Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887), Volume 8 – No. 9, October 2010.

[12] Eiji Kawaguchi and Richard O. Eason, "Principle and applications of BPCS-Steganography", Kyushu Institute of

Technology, Kitakyushu, Japan, University of Maine, Orono, Maine 04469-5708.
[13]Sashikala Channalli and Ajay Jadhav, "Steganography An Art of Hiding Data", International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141.

BIOGRAPHIES

Shuchi Agarwal has completed her degree in electronics and engineering form Lakshmi Narain college of technology Bhopal affiliated from R.G.P.V .She is now pursuing degree in digital communication from Radharaman institute of technology and science Bhopal affiliated from R.G.P.V.She has special interests on research fields like image processing, data hiding with special focus on steganography and cryptography.