Implementation of Data Hiding Approach by Diverse Image Media

Miss. Sweeti. A. Parwatkar
Student of Computer Science and Engineering,
ME 2nd Year, P. R. Patil COET, Amravati,
Maharashtra, India.
parwatkarsweety@yahoo.com

Prof. V. B. Bhagat
Assistant Professor, Computer Science and Engineering,
P. R. Patil COET, Amravati,
Maharashtra, India.
matevaishali2@gmail.com

Abstract— The network provides a method of communication to distribute information to the masses. With the growth of data communication over computer network, the security of information has become a major issue. Steganography and cryptography are two different data hiding techniques. Steganography hides messages inside some other digital media. Cryptography, on the other hand obscures the content of the message. In this paper propose a high capacity data approach by the combination of Steganography and cryptography. In the process a message is first encrypted using transposition cipher method and then the encrypted message is embedded inside an image using Higher LSB insertion method. The combination of these two methods will enhance the security of the data embedded. This combinational methodology will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel. In this paper computing Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR).

Keywords— *Cryptography, Data Hiding, PSNR, MSE, Higher LSB*

*****

I. Introduction

The protection of data has becomes an elementary issue. Besides cryptography, stegnography is used to secure data. Stegnography could be a technique of concealing data in digital media. In distinction to cryptography, the message or encrypted message is embedded in a very digital host before passing it through the network, so the existence of the message is unknown.Besides concealing information for confidentially, this approach of data concealing is unknown is extended to copyright protection for digital media: audio, video, and images.[10]

Many different ways are developed to write in code and rewrite knowledge so as to stay the message secret. Sadly, it's typically not sufficient to remain the contents of a message secret. So, it's necessary to stay the survival of the message secret. [4]

VISVAL cryptography (VC) is a technique that encrypts a secret image into *n* shares, with each participant holding one or more shares. Anybody who holds fewer than *n* shares cannot reveal any information about the final secret image. Stacking the *n* shares reveals the secret image and it can be recognized directly by the human eyes. [1]

After encryption the frame and audio will be decompose and distribute final uncompressed video. The planned video encryption scheme operated in the calculation error domain is shown to be able to provide a reasonably high level of security and effectiveness. [10]

1.1 Objective

- To increase the Payload capacity. It refers to the amount of data that can be inserted into cover media without deteriorating its integrity.
- To maintain Image Perceptual quality. It is necessary that to avoid suspicion the embedding should occur without significant degradation or loss of perceptual quality of the cover media.
- To provide security to hidden message from unauthorized accesses.

II. Literature Review

Tung-Hsiang Liu and Long-Wen Chang in 2004 has proposed a simple data hiding technique for binary images in The proposed method embeds secure data at the edge portion of host binary image. Binary images consist of only two colors therefore changing any pixels in this image could be easily detected by human eyes. Therefore, data is stored in the edge portion of binary image; as the modification of edge pixels is more difficult to be recognized by human eyes. The Distance matrix mechanism is used to find the edge pixels of host binary image. Then the Weight mechanism is used to consider the connectivity of the neighborhood around changeable pixels for choosing the most suitable one. For the security and quality consideration, a random number generator is used to distribute the embedding data into the overall image. This method not only embeds large amounts of data into host binary image but also can maintain image quality. [14]

H.-C. Wu, N.-I. Wu, C.-S. Tsai and M.-S. Hwang in 2005 In order to improve the capacity of the hidden secret data and to provide am imperceptible stego image quality. Has proposed a novel stenographic method based on Least Significant Bit (LSB) Replacement and Pixel Value Differencing (PVD) methods. [13]

Hsien-Wen Tseng, Feng-Rong Wu, and Chi-Pin Hsieh 2007 has proposed a novel method for hiding data in binary images. The binary cover image is partitioned into equal-sized, non-overlapping blocks and the watermark will be embedded into blocks by flipping pixels. For security consideration, the watermark data is firstly permuted into a meaningless bit sequence by using a secret key. [12]

Beenish Mehboob and Rashid Aziz Faruqui in 2008 discussed the art and science of Steganography in general and proposed a novel technique to hide data in a colorful image using least significant bit. Least Significant Bit or its variants are used to hide data in digital image. Digital Images are represented in bits. [11]

M.B. Ould Medeniand & El Mamoun Souidi in 2010 has proposed a novel stenographic method for gray level images on four pixel differencing and LSB substitution. The proposed approach works by dividing the cover into blocks of equal sizes and split each pixel into two parts .Then it counts number of one's in most part and embeds the secret message in the least part according to the corresponding number of bits in most part. [9]

RigDas and Themrichon Tuithung in 2012 have proposed novel technique for image stenography based on Huffman Encoding. Huffman Encoding is performed over the secret image/message before embedding and each bit of Huffman code of secret Image/message is embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image. This paper presents a novel technique for image steganography based on Huffman Encoding. [7]

Ankit Chaudhary and JaJdeep Vasavada in 2012 has proposed an improved stenography approach for hiding text messages in RGB lossless images The security level is increased by randomly distributing the text message over the entire image instead of clustering within specific image portions. [6]

Tasnuva Mahjabin, Syed Monowar Hossain and Md. Shariful Haque in 2012 has proposed a data hiding method based on PVD and LSB substitution to improve the capacity of the secret data as well as to make stegnalysis a complicated task they made an effort to implement a robust dynamic method of data hiding. [5]

Kai-Hui Lee and Pei-Ling Chiu in 2014 has developed efficient encryption/decryption algorithms for the (*n*, *n*) - NVSS scheme. The proposed algorithms are applicable to digital and printed media. The possible ways to hide the generated share are also discussed. The proposed NVSS scheme not only has a high level of user friendliness and manageability, but also reduces transmission risk and enhances the security of participants and shares. [1]

III. Proposed Method

Proposed Methodology has been divided in 2 Phases:-

1) Data Hiding

2) Data Extraction

1) Data Hiding:-

In this phase, we split the image in different parts. Then intensity of the image gets check to find whether it is closer to darkness or brightness. If it is closer then that image sample will be selected for hiding the data. For hiding the secrete data, firstly data is encrypted with shifting method and then segmented into equal parts. After that each data segment is hiding behind the specific sample of image. At last all the samples are concatenated which will give the stego image.

2) Data Extraction:-

In this phase, whatever the data is hidden in first phase that is being extracted. Following steps will be performed:-

i) First Split the image.
ii) Extract the data segment from image samples.
iii) Decrypt the data segments.
iv) Assemble the data obtain from data segment.

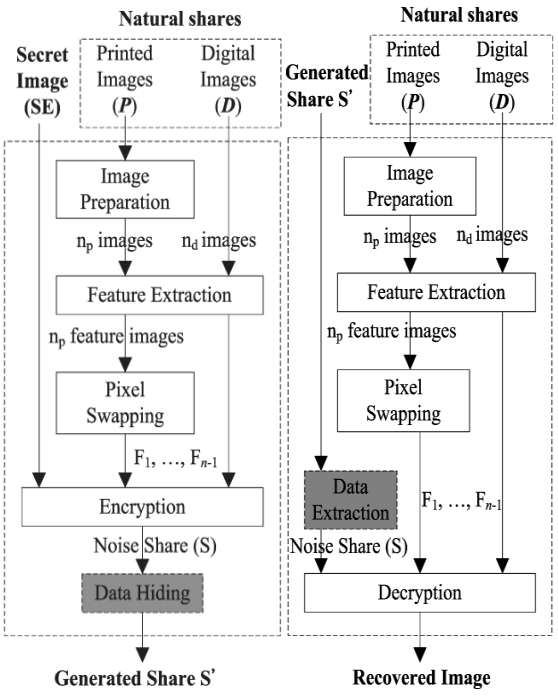


Fig. 1. The encryption/decryption process of the NVSS scheme:
(a) Encryption process, (b) decryption process. [1]

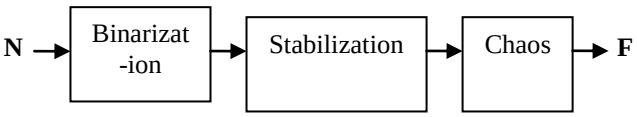
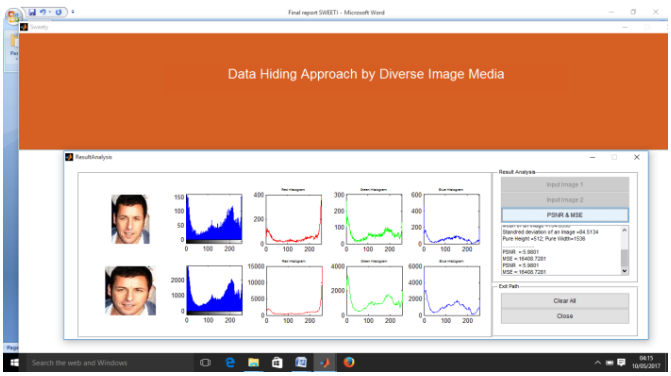


Fig. 2. The block diagram of the feature extraction. [1]

Result Analysis



 ISSN: 2321-8169
183 – 186

Table 1 of Input Carrier Image and Secret Image

Sr No	Carrier Image Name	Secret Image Name	Carrier Image Mean Intensity	Carrier Image Entropy	Secret Image Mean Intensity	Secret Image Entropy	Carrier Image Size	Secret Image Size	Stego Image Size
1	37.bmp	0.814722.bmp	0.4	17.5637	0.48235	17.5637	180×200	20×20	104×137
2	0.55345.bmp	0.814722.bmp	0.45882	17.4214	0.51373	17.5266	109×81	20×20	119×157
3	28.bmp	0.40914.bmp	0.39216	17.7245	0.55294	17.3965	180×100	20×20	84×116
4	0.99632.bmp	0.242. bmp	0.53333	17.8821	0.58824	17.7261	116×124	20×20	84×134
5	6.bmp	0.65155.bmp	0.47059	17.7266	0.41178	17.7896	180×200	20×20	86×119

Table 2 of Data Hiding

Sr. No	Carrier Image Name	Carrier Image Mean Intensity	Carrier Image Entropy	Stego Image Mean Intensity	Stego Image Entropy	PSNR	MSE
1	0.72316	0.4	17.5637	0.48235	17.753	5.9808	16406.0488
2	0.81472	0.66667	17.1027	0.62353	17.3097	7.5329	11476.0079
3	0.40914	0.55294	17.3965	0.55294	17.5378	6.6254	14142.9309
4	0.242	0.58824	17.7261	0.58431	17.739	7.7591	10893.6937
5	0.65155	0.41176	17.7896	0.41176	17.8125	9.314	7615.1963

Table 3 of Data Extraction

Sr.No	Actual Image Hided	Extracted Image Mean Intensity	Extracted Image Entropy
1	37.bmp	134.6664	17.7531
2	0.55345.bmp	127.2047	7.4214
3	28.bmp	98.1687	7.7245
4	0.99632.bmp	131.1547	7.8821
5	6.bmp	107.3832	7.7266

Table 4 of Hiding Capacity

SN	Reposed Method	Hiding Capacity	Quantization Error
1	Proposed	6/8	64
2	1st LSB	1/8	1
3	2 LSB	1/8	2
4	3	1/8	4
5	4	1/8	8
6	5	1/8	16
7	6	1/8	32
8	Group of 2	2/8	3
9	Group of 3	3/8	8
10	Group of 4	4/8	16
11	Group of 5	5/8	32

Conclusion

Although just some of the most steganographic techniques were mentioned here, one will see that there exists an oversized choice of approaches to activity data in digital media. All the most important image file formats have totally different ways of activity messages, with totally different robust and weak points severally. Wherever one technique lacks in payload capability, the opposite lacks in lustiness. So, our future study and analysis includes developing the information activity ways with high embedding capability & lustiness.

References

[1] Kai-Hui Lee and Pei-Ling Chiu," Digital Image Sharing by Diverse Image Media ", IEEE transactions on information forensics and security, January 2014.

[2] Minal Nerkar, Kshitij Naik, Taniya Rohmetra, Sayali Sate, Tejan Irl*a," ***Encrypting Digital Images and Using Diverse Image Media for Sharing Digital Images*",*** International Journal of Emerging Engineering Research and Technology, (IJERT) October 2014.

[3] Ming Li, Michel K. Kulhandjian, Dimitris A. Pados, Stella N. Batalama, and Michael J. Medley,*"* Extracting Spread-Spectrum Hidden Data From Digital Media", IEEE transactions on information forensics and security, July 2013.

[4] Mrs.K.Rajasri, Mrs.D.Gayathri, Ms.T.Indhumathi," Image Steganography and Steganalysis Using Pixel Mapping Method", International Journal of Engineering Research & Technology, (IJERT) November 2013.

[5] Tasnuva Mahjabin, Syed Monowar Hossain, Md. Shariful Haque*,"* A Block Based Data Hiding Method in Images Using Pixel Value Differencing and LSB Substitution Method", IEEE 2012.

[6] Ankit Chaudhary, JaJdeep Vasavada,"A Hash Based Approach for Secure Keyless Image Steganography in Lossless RGB Images*", IEEE 2012*.

[7] RigDas, Themrichon Tuithung," A Novel Steganography Method for Image Based on Huffman Encoding", IEEE 2012.

[8] Babloo Saha and Shuchi Sharma, "Steganographic Techniques of Data Hiding using Digital Images", Defence Science Journal, (DSJ) January 2012.

[9] M.B. Ould Medeni, El Mamoun Souidi,"A Novel Steganographic Method for Gray-Level Images With four-pixel Differencing and LSB Substitution *",* IEEE 2010.

10] Hamdan.O.Alanazi, A.A.Zaidan, B.B.Zaidan, Hamid A.Jalab and Zaidoon Kh. AL-Ani," New Classification Methods for Hiding Information into Two-part: Multimedia Files and Non Multimedia Files*"*, journal of computing, (ISSN) march 2010.

[11] Beenish Mehboob and Rashid Aziz Faruqui," A Stegnography Implementation", IEEE 2008.

[12] Hsien-Wen Tseng, Feng-Rong Wu, and Chi-Pin Hsieh," Data Hiding for Binary Images Using Weight Mechanism", IEEE 2007.

[13] H.-C. Wu, N.-I. Wu, C.-S. Tsai and M.-S. Hwang," Image steganographic scheme based on pixel-value differencing and LSB replacement methods", IEE Proc.-Vis. Image Signal Process, October 2005.

[14] Tung-Hsiang Liu and Long-Wen Chang, *"*An Adaptive Data Hiding Technique for Binary Images", Proc.IEEE 17th Int.Conf. On Pattern Recognition (ICPR'04) 2004.