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

Secret Image Sharing By Diverse Image Media

Dr. Prashant R. Deshmukh [1], Sejal V. Gawande[2]

[2]Student, Computer Science and Engineering, Sipna C.O.E.T., Amravati, Maharashtra, India

[1] pr_deshmukh@yahoo.com; [2]gawandesejal@gmail.com

Abstract - *In this paper, we emphasize on how to improve the capacity of carrier image by hiding secret data in it by using the combination of data hiding and cryptography. To fulfill the requirement, the proposed method highlights an approach of hiding secret data using diverse image media. The proposed system hides the secret data which is first encrypted and then is hidden behind a carrier image and achieves the security by hiding image behind another image. In this way the system achieves its encryption and decryption after going through visual cryptography. The overall effort of the proposed method is the achievement of hiding and extracting secret images. In proposed method, we have tried to increase the capability of the original scheme by improving the capacity of hiding data and increasing security. The main aim of the proposed model is to improve security, efficiency and reliability of the secret image by using the combination of data hiding and cryptography method.*

Key Words: **Data Hiding, Cryptography, Diverse image media, Data Security, Data Extraction**

1. INTRODUCTION

In the modern digital world internet has become a predominant medium through which communication takes place. Secrecy, privacy, confidentiality and authentication are some of the primary entity that every internet user demands. There are two main branches of information security: Cryptology and Data Hiding. Both these branches have fascinated people since centuries and numerous studies have tried to unravel their mysteries. Cryptology is a combination of two areas: Cryptography & Cryptanalysis. Cryptography is the study of schemes used for encryption and Cryptanalysis is the study of techniques used for deciphering a message with no knowledge of enciphering. Data hiding can be defined as the art and science of hiding (or embedding) data into information file so that the existence of data is concealed to the eavesdroppers [1].

Fundamentally both cryptography and data hiding are information securing technique but they differ in their implementation. Cryptography makes secret data unreadable [2] by a third party, whereas data hiding hides secret data from a third party. Both of their notion [3] remain the same. The cover medium suitable for data hiding [4] can be any entity that can be digitally represented such as a text file, image, audio, video and TCP/IP packets.

In case of 24 bit color images, each pixel has three color components: Red, Green and Blue (RGB). Each pixel is represented with 3 bytes to indicate the intensity of three colors (RGB). Data hiding is quite differ from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, data hiding focuses on keeping the existence of a message secret[5]. Its main aim is to present message in unreadable format without secret knowledge, known as the encryption. Data hiding and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. When the presence of hidden information is suspected or even revealed, the purpose of hiding is partly defeated.

Internet is the fastest growing communication medium and essential part of infrastructure, nowadays. To cope with the growth of internet it has become a constant struggle to keep the secrecy of information and when profits are involved, protect the copyright of data. To provide secrecy and copyright of data many of the steganograhic techniques has been developed. But each of the technique has their respective pros and cons. Where one technique lacks in payload capacity, the other lacks in robustness. So, the main motivation of proposed work is to overcome these shortcomings.

When using the color image instead of grayscale image, we get more space to hide the data. Pixel consists of 8 bit of every red, green, blue (RGB) components. If we replace every 5 bit from each component, we can get much more space to hide the data. Various data hiding techniques are used to hide data but the data hiding capacity is less. So we have tried to overcome the existing system and provide high security.

2. LITERATURE REVIEW

The visual cryptography encrypts the secret image into n shares. Security is important issue once we transmit the secret image. Secret image contain the important data therefore to hide such data from hacker we'd like to supply security to the secret image in shares. Here shares are nothing however the significant pictures or noise like pixels however it will increase interception risk throughout the

transmission of shares. Hence VSS theme suffers from transmission risk downside.
For hiding secret image varied schemes will be projected. In (2, 2) Visual Cryptography Scheme, original image is split up into 2 shares. In the original image every constituent is described by the non-overlapping block of two or four sub-pixels in each share. Anyone who concerned in the theme for n-1 shares cannot disclosed any secret info. Both the shares area unit superimposed the secret image is appeared [6]. Each share has a try of constituents for each pixel within the original image. In a technique, if the original image pixel is black, the pixel pairs in the image should be complementary. They randomly shared black-white and different white-black. These complementary pairs are overlapped they appeared dark grey. On the other hand they appeared lightweight grey. So once the 2 shares area unit superimposed the first image seems. Each part image has a try of constituents for each pixel within the original image. This scheme is terribly secure and straightforward to implement [6]. Zhi Zhou, Member, Gonzalo R. Arce, Fellow and Giovanni Di Crescenzo proposed Halftone Visual Cryptography. They used blue-noise dithering principles with void and cluster algorithmic program. In Halftone visual cryptography, encoded a binary image into n different halftone shares. Appropriate size of the halftone cells will be used. They obtained the halftone shares. It maintains security and increases quality of the shares [7]. Chang-Chou Lin, Wen-Hsiang Tsai proposed visual cryptography for grey level pictures [8]. A dithering technique is used during this theme. This technique convert gray level image into approximate binary image. In this scheme shares may be created by exploitation acceptable binary pictures. The J Shyu et al [9] proposed a theme for multiple secrets sharing in visual cryptography. At a time two shares will be secured.
K. H. Lee and P. L. Chiu proposed AN extended visual cryptography algorithmic program for general access structures [10]. In this paper, two part secret writing algorithmic program of extended visual cryptography for general access structure will be used. It helps to avoid a possible downside that could arise by noise like shares. The advantage of this scheme is that substantive shares area unit generated and improved the quality of output image. In this scheme take into account one secret image and n-number of natural image. In this scheme cowl image hides a secret image.The pixel enlargement downside will be resolved simply. In this paper cover pictures area unit additional on every share. So it maintains the security. Pei-Ling Chiu and Kai-Hui Lee [11] proposed that a simulated tempering algorithmic program for general threshold visual cryptography schemes. Only binary secret pictures area unit used. The display quality of recovered pictures will be controlled additional exactly. The contrast of the recovered pictures will be improved considerably. Visual secret sharing scheme uses unity carrier for sharing a secret image. It suffers from the transmission risk problem. Because it can awake suspicion and increase interception risk throughout transmission of the shares [11]. Kai-Hui Lee and Pei-Ling Chiu proposed Digital Image Sharing by various Image Media in 2014 [12]. Natural Image Based Visual Secret Sharing theme uses various media for sharing the secret pictures. Diverse media contains hand-printed photos, digital images, printed pictures and therefore on. To reduce transmission risk downside use natural image based mostly visual secret sharing theme. The two participants will distribute the natural image and also the generated share (i.e., cipher text). In decryption method, the secret key are extracted again from the natural image. Then the secret key also because the generated share can recover the first secret image. In the NVSS scheme natural shares may be grey colors of pictures, even flysheet, bookmarks etc. The natural shares can be in digital and written type. Transmission risk problem will be simply resolved [12].

3. PROPOSED METHODOLOGY

In previous work, there are no provision of choosing the key and more encode-decode time consumption. There are lots of data hiding programs available. A few of them are excellent in every respect; unfortunately, most of them lack usable interfaces, or contain too many bugs, or unavailability of a program for other operating systems.

In proposed system is taken into consideration to overcome these limitations by increasing security, reliability and efficiency with the help of combination approach of visual cryptography and data hiding technique. In the implementation, we have combined both the techniques: Cryptography and data hiding. The combination provides more security and confidentiality. To obtain more security we have done two level hiding. There are some objectives behind implementing our technique. These are given below:

3.1 Proposed Objectives

The objectives of this project is to create an easy to use environment in which the user can provide a sample image for hiding the secrete data into it using Higher LSB Data Hiding Algorithm & to extract data from an image using Higher LSB Data Extraction Algorithm.

The Main objectives of this proposed method are:-

1. To hide secret data into carrier image using diverse image media.
2. To implement multiple layers of images for hiding secret data to increase the security.
3. To increase the Payload capacity. It refers to the amount of data that can be inserted into cover media without deteriorating its integrity.
4. 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.
5. To provide security to hidden message from unauthorized accesses.

The proposed scheme consists of two main modules:

i. Higher LSB Data Hiding
ii. Higher LSB Data Extraction

3.1.1 Data Hiding

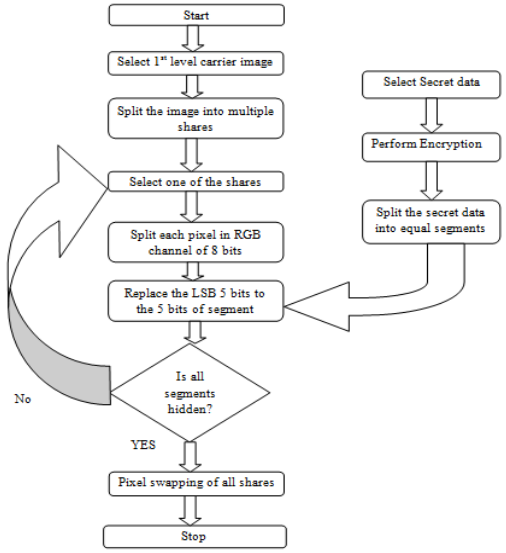

Fig-1: Data Hiding Algorithm (level 1)

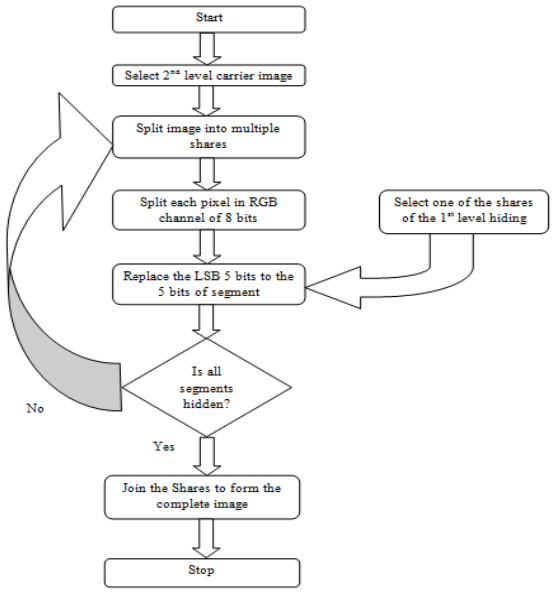

Fig-2: Data Hiding Algorithm (level 2)

In the above proposed system, data hiding to be carried out in the following way:

Step 1: Select level 1 input carrier image.
Step 2: Select level 2 input carrier image.
Step 3: If we want to crop the image then we can perform this operation (optional).
Step 4: An input image gets split into 4 multiple shares. One of the multiple shares is selected from amongst all 4 shares.
Step 5: Select the secret data which we need to encrypt. Encrypt the data using one of encryption algorithm with a key to provide more security. Split the encrypted data into 4 shares of equal length.
Step 6: Every share of an image gets split into RGB channels each of 8 bits. Split each pixel in RGB channel of 8 bits each and separate each of 3 color 8 bit component into 3 bits and 5 bits.
Step 7: Each 5 bits of RGB channel gets replaced with the 5 bits of one of the data segment. In this way we perform data embedding into an image.
Step 8: Pixel swapping of MSB 4 bits with LSB 4 bits is performed on the shares obtained from step 7.
Step 9: Now the 2nd level carrier image is selected and this image gets split into four multiple shares. One of the shares of level 1 image is embedded into one of the shares of 2nd level image. This hiding of image behind another image is performed in the same way as in step 6 & 7.
Step 10: After hiding process, all the shares of level 2 image are joined together to form a complete image which looks similar to the original level 2 image. This image is further transmitted to the receiver end.

3.1.2 Data Extraction

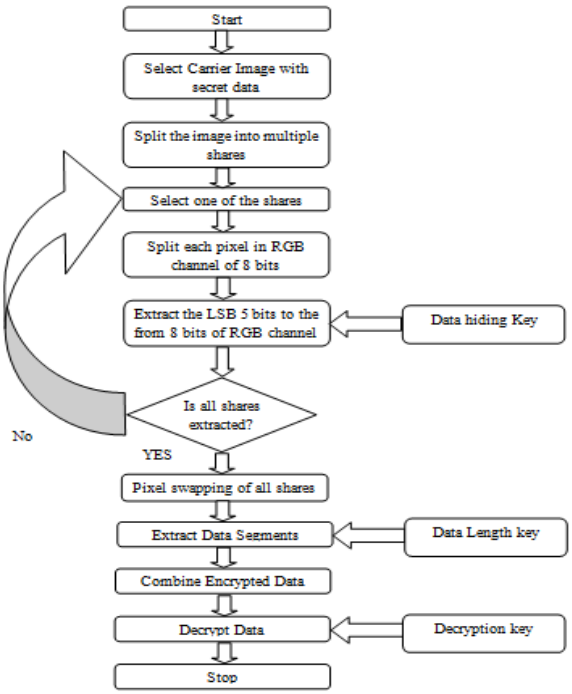

Fig-3: Data Extraction Algorithm

In the above proposed system, data extraction to be carried out in the following way:

Step 1: Select the received carrier image containing secret encrypted data.
Step 2: Split the selected image into four multiple shares. One of the shares is selected amongst all 4 shares.
Step 3: Every share of an image gets split into RGB channels each of 8 bits. Split each pixel in RGB channel of 8 bits each

and separate each of 3 color 8 bit component into 3 bits and 5 bits.

Step 4: Each 5 bits of RGB channel gets extracted to obtain the shares of stego image. On the obtained shares of stego image, perform the pixel swapping of MSB 4 bits with LSB 4 bits.

Step 5: Extract the encrypted data segments from the shares using data length key. Combine the segments obtained to produce the complete encrypted secret data.

Step 6: Perform the decryption of the secret data using the decryption key to obtain the original data.

4. EXPERIMENTAL RESULTS

4.1 Mean Intensity and Entropy

Experimental results show that the values of entropy, mean intensity of the image before the encryption and hiding are closely similar to the values after the encryption and hiding. Since the image parameters have not changed much, the method offers a good concealment of data and reduces the chance of the secret data being detected. Thus, it indicates a perfectly secure steganographic system. Furthermore, the secret information can be retrieved without encountering any loss of data.

Before Encryption and Hiding			After Encryption and Hiding		
Cover Image	Mean Intensity	Entropy	Stego Image	Mean Intensity	Entropy
Lena	0.55294	17.7551	StegoLena	0.55294	17.7585
Baboon	0.51765	17.7555	StegoBaboon	0.51765	17.7565
Peppers	0.45882	17.3785	StegoPeppers	0.45882	17.4103
Tree	0.60784	15.3018	StegoTree	0.61961	15.4027

Table-1: Comparison of Entropy & Mean Intensity of Cover Image and Stego Image

Input Image	Existing Method [13]				Proposed Method	
	Hiding Capacity	Jpeg-Jsteg (Huffman) 1-bit embedding	Jpeg-Jsteg (T-code) 1-bit embedding	4-bit XOR operation embedding	Hiding Capacity	Higher LSB Method
Lena	4215	37.77	37.57	30.79	9600	49.3792
Baboon	5946	36.49	36.52	30.58	9600	56.5096
Peppers	4215	37.77	37.87	30.83	9600	46.2109
Tree	5412	36.78	36.54	30.66	9600	47.7500

Table-2: Comparison of Existing Techniques with Proposed technique

In this table, we take reading from different author schemes. We calculated data hiding capacity and PSNR and compare our implemented methods with the existing system. As per the calculation of table implemented method has high embedding capacity.

PSNR (Peak Signal-to-Noise Ratio) is a standard measurement used in order to test the quality of the resultant images. PSNR defines the ratio between the maximum power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR is usually expressed as decibel scale. The PSNR is then calculated as follows:

$$PSNR = 10 \log 10 \frac{MAX^2}{MSE} (db)$$

MSE is a risk function corresponding to the expected value of squared error. The MSE is the second moment of error and thus incorporates both the variance of the estimate and its bias. Mean square error is computed by averaging the squared intensity of the original (input) image and the resultant (output) image pixels.

$$\text{MSE} = \frac{1}{NM} \sum_{m=0}^{m-1} \sum_{n=0}^{N-1} \mathbf{e}(\mathbf{m},\mathbf{n})^2$$

Where e (m, n), error is the difference between the original and the distorted image.

5. CONCLUSION

The proposed technique has been utilized for applications that need high volume embedding with robustness against sure statistical attacks. The present technique is an effort to spot the necessities of a decent information concealing algorithmic rule. It is not intended to interchange steganography or cryptography however rather to supplement it. Steganography is not a decent solution to secrecy, but neither is coding. But if these strategies area unit combined, we can have 2 layers of protection. If a message is encrypted and hidden with higher LSB method the embedding capability will increase and therefore we tend to will hide high volume of information. The method satisfies the necessities like capability, security and robustness that area unit meant for information concealing. The resulting stego-image will be transmitted while not revealing the key data being changed.

REFERENCES

[1] Mohan A. K., Anusudha K, "Hybrid Algorithm for Improved RDH using Dual Imaging & Histogram Shifting" M. Tech in Electronics, Pondicherry University, Kalapet, Puducherry-14, 2015

[2] Ying Wang and Pierre Moulin, "Perfectly Secure Steganography: Capacity, Error Exponents and Code Constructions", IEEE Transactions of Information Theory, Vol. 54, No. 6, pp. 2706-2722, 2008

[3] Mao, J.F., Ru, Z., Niu, X.X.,Yang, Y.X. and Zhou, L. N, "Research of Spatial Domain Image Digital Watermarking

Payload", Eurasip Journal on Information Security, pp.1-12 , 2011

[4] Tayana Morkel, Jan H P Eloff And Martin Olivier, S. " An Overview of Image Steganography", Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA), Sandton, South Africa, 2005.

[5] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004.

[6] Moni Naor and Adi Shamir ,"Visual cryptography", In Proceedings of Advances in Cryptology, EUROCRYPT 94, Lecture Notes in Computer Science, 1995, (950):pp. 1-12.

[7] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography," IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453,Aug. 2006.

[8] Chang-Chou Lin, Wen-Hsiang Tsai, "Visual cryptography for graylevel images by dithering techniques", Pattern Recognition Letters, V.24 n.1-3.

[9] S. J. Shyu, S. Y. Huanga,Y. K. Lee, R. Z. Wang, and K. Chen, "Sharing multiple secrets in visual cryptography", Pattern Recognition, Vol. 40, Issue 12, pp. 3633 - 3651, 2007.

[10]K. H. Lee and P. L. Chiu, "An extended visual cryptography algorithm for general accessstructures," IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 219–229, Feb. 2012.

[11] P. L. Chiu and K. H. Lee, "A simulated annealing algorithm for general threshold visual cryptography schemes," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 992–1001, Sep. 2011.

[12] Kai-Hui Lee and Pei-Ling Chiu, "Digital Image Sharing by Diverse Image Media", IEEE Transactions On Information Forensics And Security, VOL. 9, NO. 1, pp. 88-98, January 2014

[13] Sushil Kumar, "Data Hiding in Digital Image using Steganography", Ph. D. Thesis, Dept. of Computer Science, Faculty of Mathematical Sciences, Univ. of Delhi, India, 2013