Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 4, April 2016, pg.159 – 163

DATA HIDING SECURITY APPROACHED WITH POSITION BASED PIXEL SWAPPING STANDARD METHOD

Rasika P. Ghom[1], Prof. Mahip M. Bartere[2]

[1]Master of Engineering Student, Computer Science and Engg Department,
G. H. Raisoni College of Engg & Management, Amravati, India
[2]Guide, Computer Science and Engg Department
G. H. Raisoni College of Engg & Management, Amravati, India
[1] rasika11ghom@rediffmail.com, [2] mahip.bartere@raisoni.net

Abstract— ***In this paper, Position Based Pixel Swapping Standard Method has been proposed, which includes the secret data must be encrypted using key and hiding secret data in image using Data Hiding Algorithm. Applied higher group LSB method to it and finally hides the data into red, green and blue images of a selected data or information. Therefore, the proposed algorithm is a combination of encryption of any form of data or information first then hiding the any form of data or information into the carrier image which provides double layer security.***

Keywords— ***Steganography, least significant bit, RGB images, MSE, PSNR, Data Hiding, Data Extraction.***

I. INTRODUCTION

In the world of technology, data security is really a big issue such that the data or information cannot be mistreat for an illegal purpose. [11] Data Hiding is one of the techniques that have been receiving much attention now days. The main motive for this is encryption and decryption. Using this data or information is imperceptibly hidden. This art of hiding data or information is known as Steganography.

Steganography is one of the security in which data is secretly embedded in a cover image, where the actual message want to be sent is completely changed to another form, hidden data under a cover image and sent to the destination.[12] Only the person who knows the technique can easily decrypt the message. The performance of Steganography methods can be rated by three Parameters: capacity, security and imperceptibility. So "Steganography means hiding one piece of data within another."

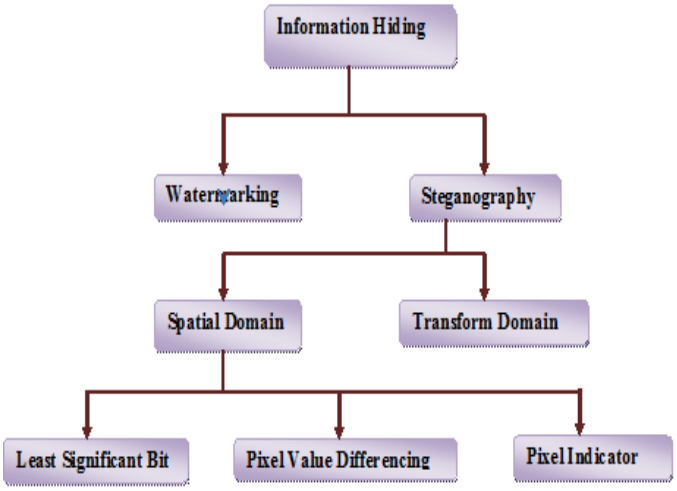

Fig1: Information Hiding Technique

The Steganography algorithms are help to perform secret communication. The most popular data formats used are .bmp, .jpeg, .mp3, .txt, .doc, .gif.

Cryptography concentrates on keeping the message content secret whereas data hiding focus on keeping the existence of the message secret. [6] Data hiding is another most important technique for secured communication. The hidden data must be secure during transformation can be obtained by two ways: Encryption and Data Hiding. A combination of the two techniques can be used to increase the data hiding security.

II. LITERATURE REVIEW

In 2004 Tung-Hsiang Liu and Long-Wen Chang,[1] proposed data hiding technique for binary images. Embeds secure data at the edge portion of host binary image is the propose method. A binary image consists of only two colors therefore in image, changing any pixels could be easily detected by human eyes. By changing distance matrix dynamically and compute we find the best changeable pixels in a block its changeable score by weighting mechanism. The proposed method uses the pseudo random number generator based on Rabin Public Key Cryptography System to embed secret data into a binary image. According to this, we can distribute secret data into the binary image to make binary image quality better and get high security.

In 2005 H.-C. Wu, N.-I. Wu, C.-S.Tsai and M.-S. Hwang [2] proposed Novel stenographic method based on LSB Replacement and to improve the capacity of the hidden secret data used Pixel Value Differencing (PVD) methods to provide an imperceptible stego-image quality. First, a different value from two consecutive pixels by utilizing the PVD method is obtained. A large difference value can be located on an edged area smooth area and the small one can located on smooth areas. Because the range width is variable, and the secret data area is concealed by LSB or PVD method are hard to guess, the security level is the same as that of a single using the PVD method of the proposed method. From the experimental results, compared with the PVD method being used alone, the proposed method can hide much larger information and maintains a good visual quality of stego-image.

In 2008 BeenishMehboob and Rashid Aziz Faruqui [3]. This paper discusses the art and science of Steganography in general proposed to hide data in a colorful image used Novel technique using LSB. Many techniques are used to hide data in various formats in steganography. Least Significant Bit or its variants are normally used to hide data in a digital image. The idea of playing with 0's and 1's seem very simple but a little bit change in value may transform an image completely. The other bits may be used but it is highly likely that image would be distorted.

In 2009 Amanpreet Kaur, Renu Dhir, and Geeta Sikka [4] proposed Image Steganography Based on First Component Alteration Technique. In this paper, new steganography scheme introduced spatial domain technique. Using first component alteration technique, hide secret data in cover-image. Techniques used to focuses only on the two or four bits of a pixel in an image which results less peak to signal noise ratio and high root mean square error. The future work is to modify given scheme to improve image quality by increasing PSNR value and lowering MSE value.

In 2010.M.B. Ould MEDENI [5] for hiding information within the spatial domain of the gray scale image used a novel steganographic method. The proposed approach works by dividing the cover into blocks of equal sizes and then embeds the message in the edge of the block depending on the number of ones in left four bits of the pixel. The experimental results have shown that the proposed method not only has an acceptable image quality but also provides a large embedding capacity. The results are compared with the PVD method, and the values obtained are better than the PVD method.

In 2012 Tasnuva Mahjabin, Syed Monowar Hossain and Md. Shariful Haque [7] proposed data hiding method based on pixel value differencing and least significant bit substitution. Using PVD & LSB methods achieved an increased embedding capacity and lower image degradation also improved security. An efficient and dynamic embedding algorithm was proposed here that not only hides secret data with an imperceptible visual quality and increased capacity. This feature of this method provides security of the hidden secret data.

In 2013 Komal B. Bijwe [9] proposed a shifting method with segmentation and efficient higher LSB method for data hiding with encrypted data into guard pixels region of a multicarrier image objects. We know that steganography is the science which involves secret data communicating in an appropriate multimedia carrier, e.g. data, image, audio and video files. Using this method, it is useful to hide data secretly but for the different image file formats have different methods of hiding data.

In 2014 Vinit Agham [10] proposed the novel separable scheme used for encryption. With the help of encryption it also include key. Using this scheme hide large amount of data without compressing and quality of image also maintain. But according to this paper, scheme is not work if data or information is in the form of sound and video.

In 2015 Sneha A. Deshmukh [12] proposed data is hidden in RGB component of pixels with LSB 5 bit Replacement method. In this an Authentication of Secretly Encrypted Message Using Half-Tone Pixel Swapping from Carrier Stego Image. This paper used a secured LSB (5 bit) for image steganography has been presented. In this the proposed method not only has an acceptable image quality but also can provide a large embedded secrete data capacity.

III. PROPOSED WORK

A. Encryption Process

- The encryption is nothing but the conversion of data or information into another form.
- Only authorized user understood the secret data.

1. Encryption Algorithm:

Step1: Input the secret data.
Step2: Encrypt that secret data using Position Based Pixel Swapping Encryption Algorithm.
Step3: Take image as a cover image for hiding secret data.
Step4: Apply data hiding algorithm on cover image.
Step5: Finally we will get the stego image.

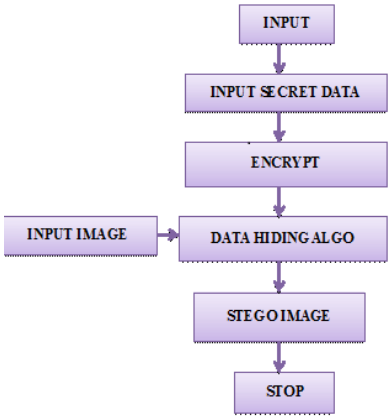

Fig 2: Position Based Pixel Swapping Encryption Algorithm

B. Data Hiding

- In the data hiding phase we can hide the secret data into cover image using higher group LSB data hiding algorithm.
- It can provide more security to secret data or information.

1. Data Hiding Algorithm:

Step1: Given encrypted image consist of pixel
Step2: Pixel consists of RGB channel
Step3: Suppose R is 8 bits, G is 8 bits and B is 8 bits
Step4: Divide 8 bits of every RGB channel into group of (2, 6)
Step5: Suppose there is secret data, now secret data is converted into binary form
Step6: Sample the binary data into 6 group
Step7: Replace 6 group of secret data to given RGB
Step8: At this stage we get new RGB value
Step9: From this new RGB value, make pixel
Step10: This way we hide secret data

The given diagram shows the Red, Green, Blue color showing the MSB & LSB side.

Fig 3(a): Showing Red, Green, Blue color with MSB & LSB side

In the proposed method we are going to replace 6-bit of LSB with secrete data as given in the below.

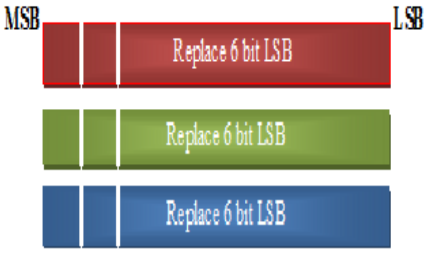

Fig 3 (b): Replacement of 6 bit from LSB side

C. Decryption Process

- Decryption is process of converting encrypted data back into its original form.
- Person who knows the technique to decrypt the message can decrypt it easily.

1. *Decryption Algorithm:*

Step1: At the receiver side we will get the stego image.
Step2: This stego image is extracted using the data extraction algorithm.
Step3: At the stage we will get the encrypted data.
Step4: Now encrypted data is decrypted using position based pixel swapping decryption algorithm.
Step5: Finally we will get the secret data which hidden under the image.

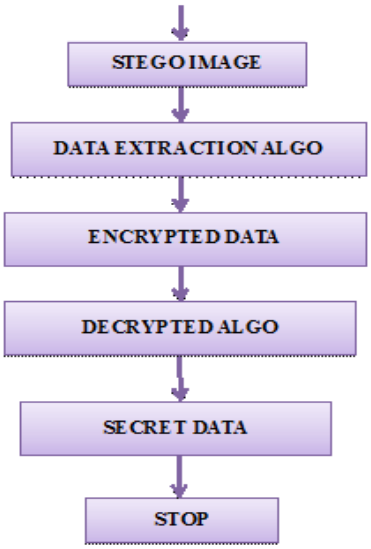

Fig 4: Position Based Pixel Swapping Decryption Algorithm

REFERENCES

[1] 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.

[2] 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., Vol. 152, No. 5, October 2005.

[3] BeenishMehboob and Rashid Aziz Faruqui*," A Stegnography Implementation*", IEEE 2008

[4] AmanpreetKaur, *"A New Image Steganography Based On First Component Alteration Technique*", (IJCSIS) International Journal of Computer Science and Information Security, Vol 6, No. 3,pp, 53-56 ,2009

[5] M.B. Ould MEDENI, *"A Novel Steganographic Method for Gray-Level Images With four-pixel Differencing and LSB Substitution* "IEEE2010

[6] Arvind Kumar, Km. Pooja, *"Steganography- A Data Hiding Technique"* International Journal of Computer Applications, Vol. 9– No.7, pp,19-23,November 2010

[7] TasnuvaMahjabin," *A Block Based Data Hiding Method in Images Using Pixel Value Differencing and LSB Substitution Method*", IEEE2012.

[8] Narendra K Pareek, *"Design and analysis of a novel digital image encryption scheme*", IJNSA, Vol.4, No.2, March 2012, pp.95-108.

[9] Komal B. Bijwe, "*An Efficient Higher LSB Method for Hiding Encrypted Data into Guard Pixels Region of a Multicarrier Image Objects*", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Volume 2 Issue 12, December 2013

[10] Vinit Agham, "*DATA HIDING TECHNIQUE BY USING RGBLSB MECHANISM*", ICICES2014

[11] Dipanwita Debnath," *An Advanced Image Encryption Standard Providing Dual Security: encryption using Hill Cipher & RGB image steganography*", 2375-5822/15 2015 IEEE DOI 10.1109/CINE.2015.41 176 178

[12] Sneha A. Deshmukh, "An *Authentication of Secretely Encrypted Message Using Half-Tone Pixel Swapping From Carrier Stego Image*", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 2409-2414

