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. 5, May 2016, pg.514 – 523

Data Hiding Security Approached with Position Based Pixel Swapping Standard Method

Rasika P. Ghom[1], Prof. Mahip M. Bartere[2]
[1]P. G. Student, Computer Sci and Engg Dept, G. H. Raisoni College of Engg & Management, Amravati, India
[2]Assistant Professor, Computer Sci and Engg Dept, 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 that must be encrypted using key and hiding secret data in image using Data Hiding Algorithm. Higher group LSB method is applied on image to hide the secret data. 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 cover image which provides double security. The results of the proposed algorithm is increase the data hiding capacity as compare to existing system and provide security to secret data. The result of the proposed system is analyzed and discussed using entropy, mean intensity, data hiding capacity and PSNR.

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

I. INTRODUCTION

Steganography is a technique that enables party to transmit data or message to another without the communication being perceptible to others. The message is embedded in cover media in a manner that only the sender and intended receiver have knowledge of the existence of the message, and the method to retrieve it. Steganography involves hiding the contents inside a file and not scrambling the data, so it is structurally unmodified and intact. Thus, Steganography has an advantage over cryptography as it involves both encryption and obscurity. Image, text, audio can be the cover media. Data in the form of text, image and audio can be embedded in the carrier. The most commonly used carrier is image.

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. 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."

The Steganography algorithms are help to perform secret communication. The most popular data formats used are .bmp, .jpeg, .mp3, .txt, .doc, .gif. Data hiding is the process of hiding a secret message within cover medium such as image, video, text, audio. Hidden image has many applications, especially in today's modern, high-tech world. Privacy and secrecy is a concern for most people on the internet. Hidden image allows for two parties to communicate secretly and covertly. 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 security.

II. LITERATURE SURVEY

In 2001 Giuseppe Atenies, Carlo Blundob, Alfredo De Santisb, Douglas R. Proposed a extended capabilities of visual cryptography [1] to share the secret information but these shares are meaningful shares but this have poor display quality.

In 2004 Tung-Hsiang Liu and Long-Wen Chang, proposed data hiding technique for binary images [2]. 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. We find the best changeable pixels in a block by changing distance matrix dynamically and compute 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 the pseudo random number generator, 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 proposed Novel stenographic method based on LSB Replacement and Pixel Value Differencing (PVD) methods [3] to improve the capacity of the hidden secret data and 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 area in which the secret data 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 2006 Z. Ni, Y. Q. Shi, N. Ansari and W. Su proposed data hiding technique for binary images [4]. 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. We find the best changeable pixels in a block by changing distance matrix dynamically and compute 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.

In 2007 Ching-nung Yang and Tse-shih Chen proposed an Extended Visual Secret Sharing Schemes [5]. Improving the Shadow Image Quality in this paper they present a new EVSS scheme by using gray and white sub pixel to represent a secret pixel and then give a clearer shadow images. But it displays low quality images.

In 2009 Amanpreet Kaur, Renu Dhir, and Geeta Sikka proposed Image Steganography Based on First Component Alteration Technique [6]. In this paper, new steganography scheme introduced spatial domain technique. Using first component alteration technique, hide secret data in cover-image. Techniques used so far focuses only on the two or four bits of a pixel in an image (at most five bits at the edge of 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 proposed a novel steganographic method for hiding information within the spatial domain of the gray scale image [7]. 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 2011 In Koo Kang, Gonzalo R. Arce, Heung-Kyu Lee proposed a color extended visual cryptography using error diffusion [8]. This paper introduces a color visual cryptography encryption method that produces a meaningful color shares via visual information pixel. It is used for color images. But it has poor display quality of the recovered images.

In 2012 Tasnuva Mahjabin, Syed Monowar Hossain and Md. Shariful Haque proposed data hiding method based on pixel value differencing (PVD) and least significant bit (LSB) substitution [9]. 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 but also make secret code breaking a good annoyance for the attacker. This feature of this method provides security of the hidden secret data.

In 2013 Komal B. Bijwe proposed a shifting method with segmentation and efficient higher LSB method for data hiding with encrypted data into guard pixels region of multicarrier image objects [10]. 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 messages.

In 2014 Vinit Agham proposed the novel separable scheme used for encryption [11]. 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 Dipanwita Debnath proposed Hill Cipher & RGB image steganography in which An Advanced Image Encryption Standard Providing Dual Security [12]. Proposed method doesn't directly stores the secret message into a cover image and image quality is low.

In 2015 Sneha A. Deshmukh proposed data is hidden in RGB component of pixels with LSB 5 bit Replacement method [13]. 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 ALGORITHM

- Encryption Process

- Steps:

Step 1: Select secret data
Step 2: Convert secret data into binary form.
Step 3: Divide binary form into group of 8 bits and form samples.
Step 4: Select key for encryption
Step 5: Encrypt the secret data
Step 6: Stop

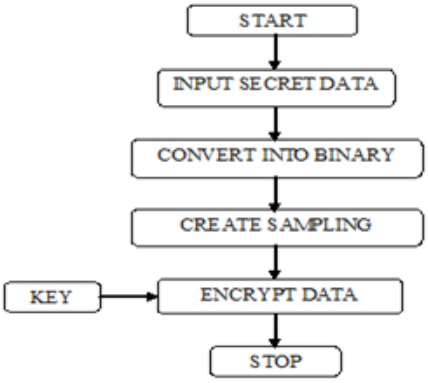

Fig 1: Flow Diagram for Position Based Pixel Swapping Encryption Process

➢ Data Hiding Process

- Steps:

Step 1: Select the carrier image.
Step 2: Convert the carrier image into binary form.
Step 3: Divide the binary form into group of 8 bits.
Step 4: Divide 8 bits of every RGB channel into group of (2, 6) bits.
Step 5: Take given encrypted data.
Step 6: Encrypted image is dividing into group of 6 bits.
Step 7: Generate key to distribute noise.
Step 8: Now replace the 6 bits of secret data with 6 bits from LSB side of carrier image applying higher group LSB data hiding algorithm.
Step 9: Stego image is form
Step 10: Stop

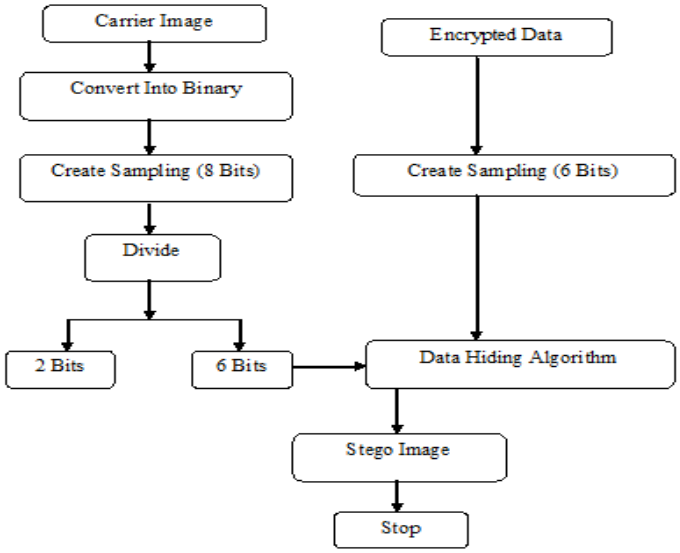

Fig 2: Flow Diagram for Higher Group LSB Data Hiding

The given Figure 5.3 shows the Red, Green, Blue color showing the MSB & LSB side.

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

The given Figure 5.4 shows the Replacement of 6 bits from LSB side.

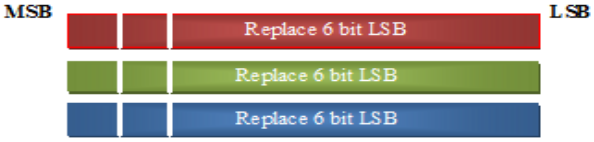

Fig 4: Replacement of 6 bits from LSB side

- Data Extraction Process

- Steps:

Step 1: Start
Step 2: At the receiver side we will get the stego image.
Step 3: This stego image is extracted using the data extraction algorithm.
Step 4: At this stage we will get the encrypted data.
Step 5: stop

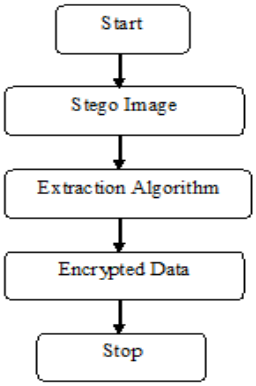

Fig 5: Flow Diagram for Higher Group LSB Data Extraction

- Decryption Process

- Steps:

Step 1: Select encrypted data
Step 2: Converted into binary form
Step 3: Divide binary form into group of 8 bits and form samples.
Step 4: Select key for decryption
Step 5: Decrypt the secret data
Step 6: Secret data
Step 7: Stop

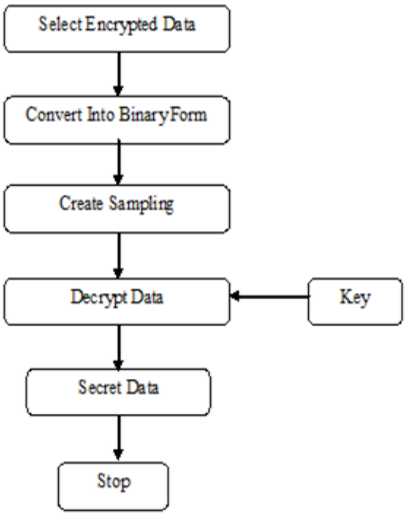

Fig 6: Flow Diagram for Position Based Pixel Swapping Decryption Process

IV. EXPERIMENTAL RESULT

Table I: Comparison between Entropy of Original Image and Stego Image

Sr. No	Image Name	No of bits Encrypted	Entropy of Original Image	Entropy of Stego Image
1	Image 1.jpeg	104 bits	6.78	6.78
2	Image 2.jpeg	160 bits	7.75	7.75
3	Image 3.jpeg	3712 bits	7.72	7.72
4	Image 4.jpeg	4392 bits	6.88	6.89

Above Table I shows entropy of original image and entropy of stego image. From these four images entropy is obtained from original image and stego image.

Fig 7: Graph Shows the Relation between Entropy of Original Image and Stego Image

It is observed from graph in Fig 7 we conclude that entropy of original image is similar to entropy of stego image means quality of image is maintained.

Table II: Comparison between Mean Intensity of Original Image and Stego Image

Sr. No	Image Name	No of bits Encrypted	Mean Intensity of Original Image	Mean intensity of Stego Image
1	Image 1.jpeg	104 bits	190	189
2	Image 2.jpeg	160 bits	90.57	90.57
3	Image 3.jpeg	3712 bits	98.16	98.13
4	Image 4.jpeg	4392 bits	174.15	174.16

Table II shows the mean intensity of original image and mean intensity of stego image. From these four images mean intensity are obtained for original image and stego image.

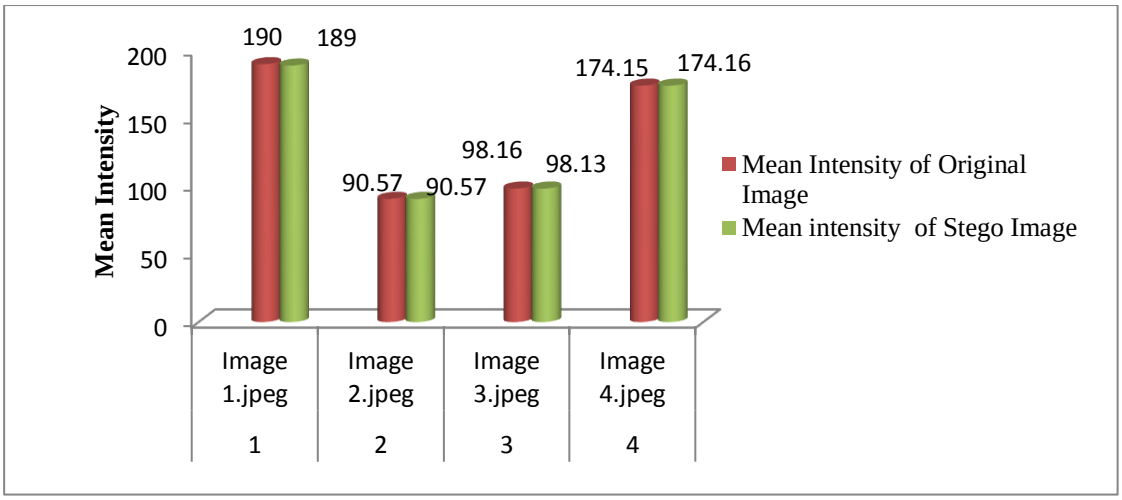

Fig 8: Graph Shows the Relation between Mean Intensity of Original Image and Stego Image

It is observed from graph in Fig 8 that the mean intensity of original image and stego image is almost same so the quality of image is maintained.

Original Image	Stego Image
 Image 1.jpeg	 Image 1.jpeg
 Image 2.jpeg	 Image 2.jpeg
 Image 3.jpeg	 Image 3.jpeg
 Image 4.jpeg	 Image 4.jpeg

The above table is depending on these original images and stego images. Here we hide secret secret data under the carrier image to get stego image.

Table III: Data Hiding Capacity in Percentage

No of Bits	Data Hiding Capacity (In %)
1 Bit	12.5%
2 Bits	25.00%
3 Bits	37.50%
4 Bits	50.00%
5 Bits	62.50%
6 Bits	75.00%

From above table III shows the hiding capacity of different bits. From above table we conclude that, data hiding capacity is more in our paper.

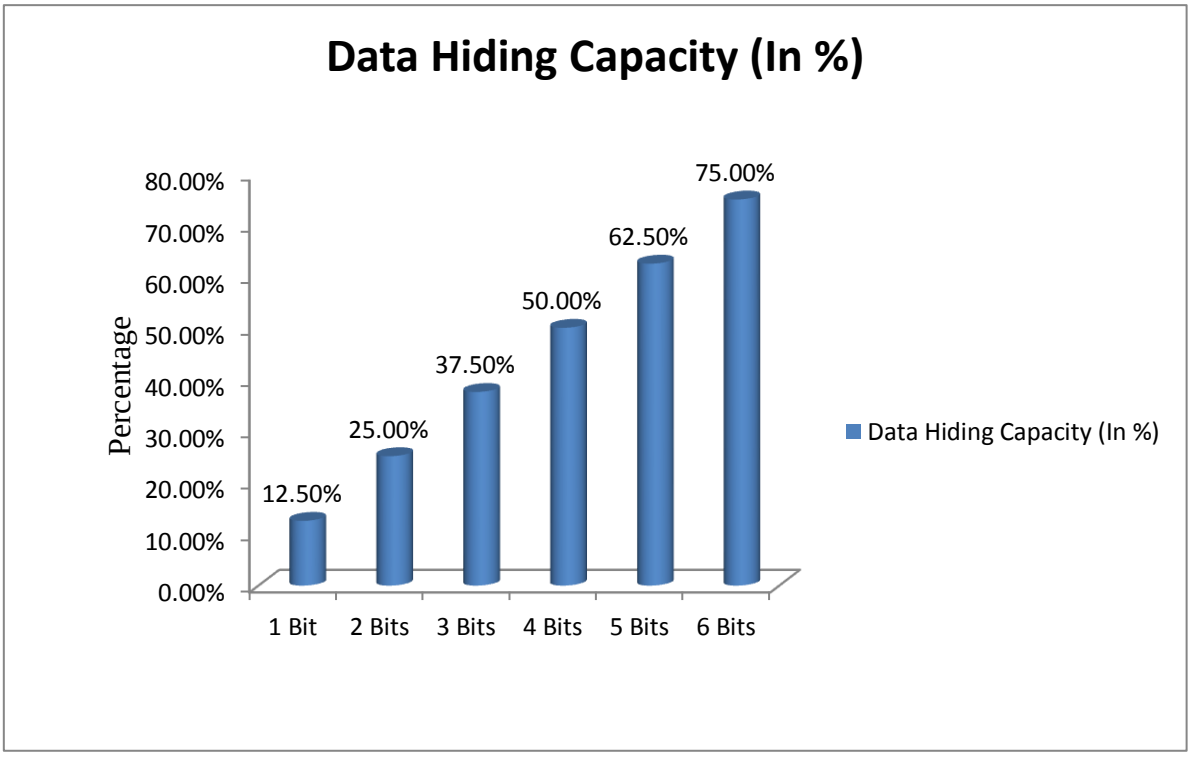

Fig 9: Graph shows Data Hiding Capacity in Percentage

It is observed from graph in Fig 9 that we use six bits so in our project data hiding capacity is more than existing system.

Table IV: Comparison of PSNR values of Existing System and Proposed System

Sr. no	Image	Existing System PSNR	Proposed System PSNR
1		20.32	57.28
2		38.23	58.73
3		30.12	45.11
4		32.54	45.93

Table IV shows the PSNR of existing system and proposed system.

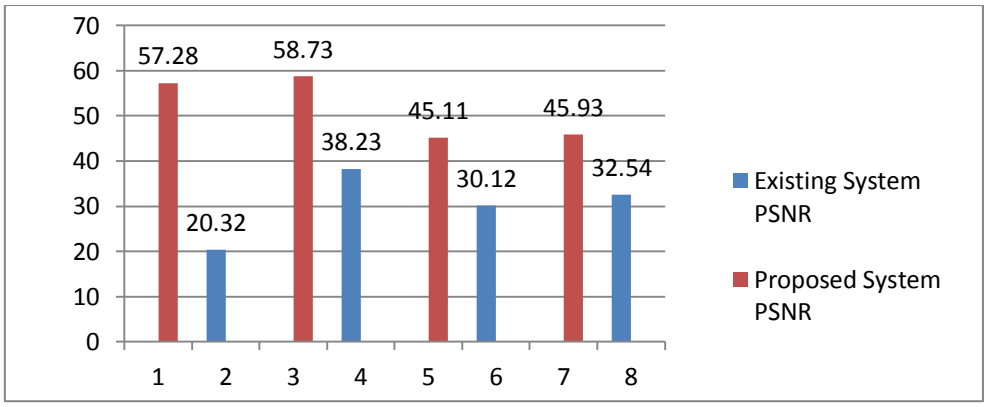

Fig 10: Graph Shows PSNR of Existing System and Proposed System

It is observed from graph in fig 10 that the PSNR value of proposed system is greater than existing system, so quality of image in proposed system is better than existing one.

V. CONCLUSION

We presented a reduced distortion algorithm for LSB image steganography. The key idea of the algorithm is data hiding bit embedding that causes minimal embedding distortion of the host image. Visualization tests showed that described algorithm succeeds in increasing the depth of the embedding group of 6 bits LSB layer without affecting the perceptual transparency of the hidden data.

REFERENCES

[1] G. ATENIESE, C. BLUNDO, A. D. SANTIS, AND D. R. STINSON, "EXTENDED CAPABILITIES FOR VISUAL CRYPTOGRAPHY," THEORETICAL COMPUTER SCIENCE, VOLUME 250, ISSUE. 1–2, PP. 143–161, JANUARY 2001.

[2] Tung-Hsiang Liu and Long-Wen Chang, "An Adaptive Data Hiding Technique for Binary Images," Processing IEEE 17th International Conference on Pattern Recognition (ICPR 04), volume 4, pp. 831-833, 2004.

[3] 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," IEEE Processing-Visual Image Signal Process, volume 152, No. 5, October 2005.

[4] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Transaction Circuits System Video Technology volume 16, No. 3, pp. 354-362, March 2006.

[5] C. N. Yang and T. S. Chen, "Extended visual secret sharing schemes: Improving the shadow image quality," International image Pattern Recognition. volume 21, No. 5, pp. 879-898, August 2007.

[6] Beenish Mehboob and Rashid Aziz Faruqui, "A Stegnography Implementation," IEEE Transaction on Biometrics and security technologies, pp.1-5, 2008.

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

[8] In Koo Kang, G. R. Arce, and H. K. Lee, "Color extended visual cryptography error diffusion," IEEE Transaction Image Process., volume 20, No. 1, pp.132–145, January 2011.

[9] Tasnuva Mahjabin, "A Block Based Data Hiding Method in Images Using Pixel Value Differencing and LSB Substitution Method," Computer And Information Technology (ICCIT), pp. 168-172, IEEE 2012.

[10] 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, pp. 423-426, December 2013

[11] Vinit Agham, "Data Hiding Technique by Using RGB LSB Mechanism," ICICES, S. A. Engineering college, Tamil Nadu, India, 2014.

[12] Dipanwita Debnath, "An Advanced Image Encryption Standard Providing Dual Security: encryption using Hill Cipher & RGB image Steganography," International Conference on Computational Intelligence & Networks, India, pp. 178-183, 2015.

[13] Sneha A. Deshmukh, "An Authentication of Secretely Encrypted Message Using Half-Tone Pixel Swapping From Carrier Stego Image," International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 6 (3) , pp. 2409-2014, 2015.

