Efficient RDH Scheme Based on Improved Quality of Retrieved Image and System Performance

S. Pawar and S. Nandusekar

Department of Electronics & Telecommunication, Pillai HOC College of Engineering & Technology, Raigad - 410206. Maharashtra, India
{p.sayu2992@gmail.com; swati.kamthekar@gmail.com}

Abstract: Confidentiality and security of data attracts attention due to fastest growth in communication and internet world. Communities of data privacy and security has attracted considerable attraction towards Reversible Data Hiding (RDH). The methodology proposes a scheme of reversible data hiding in which encryption is performed by data-hider after the selected bits are compressed and is encoded using slepian wolf encoding. Security of image is improved and is made confront towards attack by transforming identical image into un-identical format using digital image scrambling. For enhancement of data security level, encryption is carried out using Logistic chaotic mapping that is most efficient scrambling technique. It is a technique which is based on scrambling of pixel position and scrambling of pixel values. Here the system performance is calculated in the form of robustness, efficiency and capacity. A comparative result of Mean Square Error (MSE), Mean Absolute Difference (MAD), Peak to Signal Noise Ratio (PSNR) and Signal Similarity Index of Image (SSIM) in terms of accuracy is evaluated. Estimated average of parametric values for JPEG, PNG and BMP have been reduced effectively than existing methods.

Keywords: ***Reversible Data Hiding (RDH), Image Scrambling, Logistic chaotic Mapping, Vacating Room After Encryption (VRAE), Vacating Room Before Encryption (VRBE).***

1 Introduction

Hiding or concealing of secret information in digital media that could be in any form is called Data hiding. Data hiding method is connection between two groups of data, one is group of secret data and another group is of original media information. Original media usually may not be related to secret message during secret transmission [1].

Many traditional data hiding techniques undergo lossy compression were the original cover image is not retrieved at the receiver after the extraction of secret message. But there are some military, medical or remote sensing applications where actual original media is to be obtained without any alteration for high accurate data [2, 3]. The technique which satisfies these types of data hiding schemes is called as lossless or reversible data hiding technique.

Reversible data hiding came into existence for data concealing due to its important feature of reversibility. In Reversible data hiding the secret information is hidden into an original media which can be in any form. The secret information is decoded only by a legal receiver and original media can be restored without any alteration. The payload capacity, visual quality, security of image and complexity are the performance parameters of reversible data hiding algorithm. The purpose to design Reversible data hiding scheme is to full this requirements and to restore information without alteration [4].

The remaining paper is organized as section II reviews prior work related to this article. Section III states proposed methodology. Experimental results and Analysis are presented in Section IV. Finally, Section V concludes the paper.

2 Related work

RDH evaluated hiding of secret messages into encrypted images as military and medical fields may not want to share any information with data hider or any other person before data is embedded [5]. Various efficient meth-

B. Iyer, S. Nalbalwar and R. Pawade (Eds.)
ICCASP/ICMMD-2016. Advances in Intelligent Systems Research.
Vol.137, Pp. 617-624.

ods on Reversible data hiding have been proposed in last few years. Based on their compression types this methods are classified into two groups [6]:

- Vacating Room After Encryption (VRAE)
- Vacating Room Before Encryption (VRBE)

Some noticeable research work done in the area of reversible data hiding is as follows:
In [7], X Zhang et.al. encrypted image was separated into small blocks by flipping of three LSB bits and is decrypted to an estimated picture at the receiver. As the hiding rate depends on the block size, the original cover image is retrieved if appropriate block size is chosen.
W. Hong et.al. in [8], states that the drawback of inappropriate block size chosen can be overcome by using side match approach that exploits spatial correlation between neighboring blocks that minimize error rate in image recovery. This method can be used for both reduction of faults in retrieved image as well as calculation of softness of block.
K. Ma et.al. carried out an RDH method in which sparse room for data embedding was created in prior to encryption, making it convenient for data hider to hide message in encrypted image reversely in [9]. Thus the system removed faults on information retrieval and image reconstruction of previous RDH methods and attain genuine reversibility without any fault.
W. Zhang, et.al. in [10] proposed a method related to an evaluation technique, where a great section of pixels is used to evaluate the remaining prior to encryption, and the last edition of encrypted picture is produced by joining the encrypted evaluating faults and a huge section of the encrypted pixels. Extra data can be hidden in the encrypted picture by altering the evaluating faults. But above both methods require an additional RDH process by the sender prior to picture encryption.

3 System Model

The main drawbacks of existing system are insecurity in the algorithm used for encryption and inefficient system performance. Therefore its essential to develop and implement an algorithm that have enhanced security with less computational time obtaining good quality image at the receiver. An approach to retrieve good quality image with extraction of secret message without alteration with a strategy of first applying an original image by the content owner to a data hider and then to a receiver is proposed. Fig.1 depicts architecture of reversible data hiding. The proposed scheme is elaborated, which contains of three stages: content owner, data hiding, and Receiver. In phase I, the sender sends the actual image to the Data hider. In phase II, the data-hider chooses and contracts few MSB of the image to generate an unused room, and hides secret data into the image using an embedding key then encrypts the image by scrambling algorithm i.e. Logistic Chaotic Scrambling Algorithm. In phase III, the receiver retrieves the hidden information using the private key and decrypts the image.
1. Content Owner: It is sender or an owner of the original image which sends original image to the data hider for further processing.
2. Data Hider: Data Hider is a service provider who embeds secret message in to the image using embedding key. Before embedding additional secret bits data hider undergoes decomposition of image. Here the original image P is decomposed into four sub-images P1, P2, P3, P4 each having size I/2×J/2. From the decomposed sub-images P2, P3, P4 MSB bits are selected and shuffled and slepian wolf is performed to compress the selected bits [11, 12]. Then the selected bits are used to embed additional data into it by the data hider using embedding key. After the secret message is embedded into an image by using an embedding key, the original image is further encrypted by image scrambling [13].

3.1 Image Encryption

The most realized technique for image encryption is image scrambling. Here the Logistic Chaotic scrambling technique is carried out for encryption as the emphasis of these system to meet basic security necessities and effectiveness by developing highly robust and feasible algorithm [14]. Logistic Mapping is a dynamic system and is stated using expression,

$$xp + 1 = \mu xp(1 - xp) \qquad (1)$$

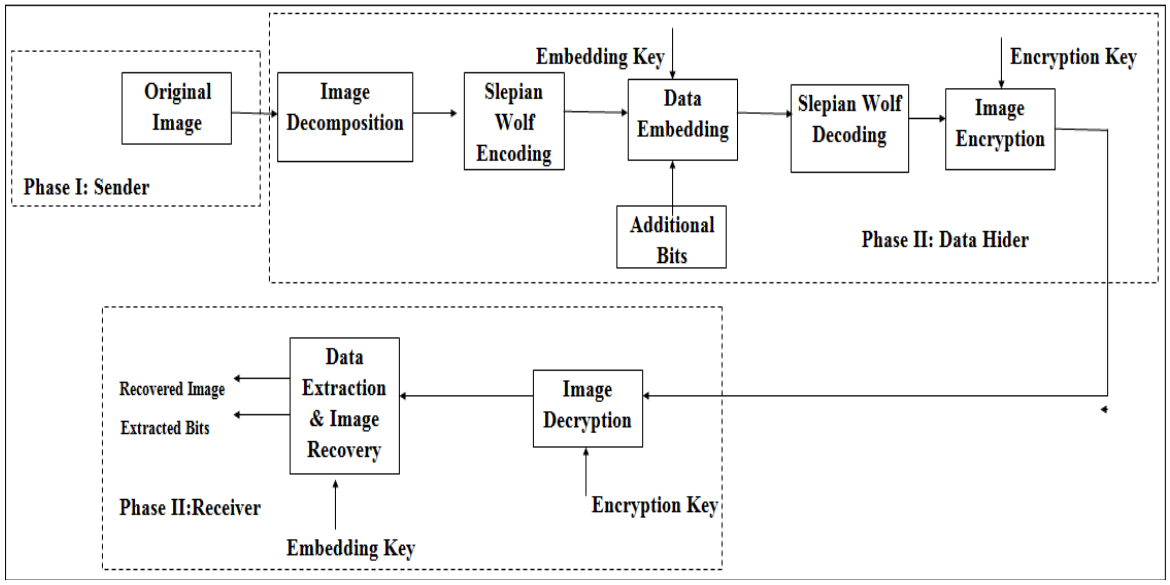

Fig. 1: Block Schematic of Proposed Methodology

Where u is constant, $\chi\rho \in (0,1)$, $p \in N$. It reaches to Chaos state when $3.569945 < u \leq 64$.Compactness, sensitivity and noise like characteristics of chaotic sequence make them advantageous to use for scrambling of digital images. Consider an original image P_{AB} where A and B denotes height and width of the image and P (m, n) indicates pixel gray level value in which coordinates are located as (m, n)= (m=0,1,2,3...A-1; n=0,1,2,3....B-1). The size of encrypted image Q will still remain the same A*B. The steps carried out for scrambling are as follows:

1. Formation of two dimensional random sequence S using keys 1 and 2 is further multiplied with 255 in order to give one dimensional sequence S(m, n)(m=0,1,2,3....A-1;n=0,1,2,3...B-1).

2. From original image P, P1 can be obtained by changing its gray level of pixel's. This operation is carried out as P1 (m, n) = P (m, n)$\oplus$ S (m, n).

3. By changing pixel position of the image P1 encrypted image Q is obtained. Thus scrambled image Q is obtained.

4 Receiver

4.1 Image Retrieval Process

Decryption is counter process that of the image scrambling process. Here the original image is retrieved when encryption key is present with the user.

4.2 Data Extraction Process

In this process the unaltered secret message can be extracted from the stego image by the user, if the embedding key it with him [15].

5 Experimental Results

The comparative analysis of data security and retrieve image quality is drawn by considering three basic parameters i.e. transparency, capacity and robustness. The parameters required for evaluation are:

1. Peak Signal To Noise Ratio : It is the ratio of maximum power of a signal to the noise;

$$PSNR = 10log_{10}\frac{MAXi^2}{\text{MSE}} \quad (2)$$

2. Structural Similarity Index: The amount of similarity between original and scrambled image is SSIM and can be obtained as;

$$\text{SSIM} = \frac{(2\mu_x\mu_y+c1)(2\sigma_{xy}+c2)}{(\mu_x 2+\mu_y 2+c1)(\sigma_x 2+\sigma_y 2+c2)} \tag{3}$$

3. Mean Square Error : MSE is defined as the square of error between original and stego image. Distortion in images is measured using MSE and is expressed as,

$$MSE = \frac{1}{mn}\sum_{i=0}^{n-1}\sum_{j=0}^{m-1}((\text{I}(\text{i},\text{j}) - \text{R}(\text{i},\text{j}))^2 \tag{4}$$

4. Mean Absolute Difference : It is the difference between original image and stego image and can be expressed as;

$$MAD = \frac{1}{mn}\sum_{i=0}^{n-1}\sum_{j=0}^{m-1}|((\text{I}(\text{i},\text{j}) - \text{R}(\text{i},\text{j}))|^2 \tag{5}$$

Table 1. Average Parametric Values

Type of Image	Number of Image	PSNR	MAD	MSE	SSIM
JPEG	50	45.5861	0.048	0.002	0.004
PNG	50	45.53	0.06	0.003	0.007
BMP	50	45.58	0.06	0.002	0.006

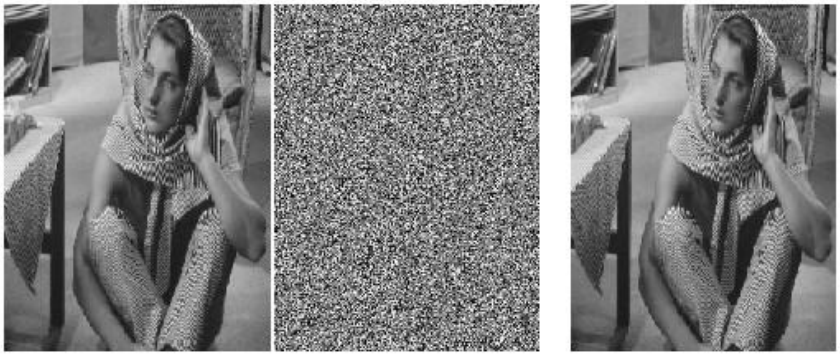

Fig. 2: Scrambling Using Logistic Transform

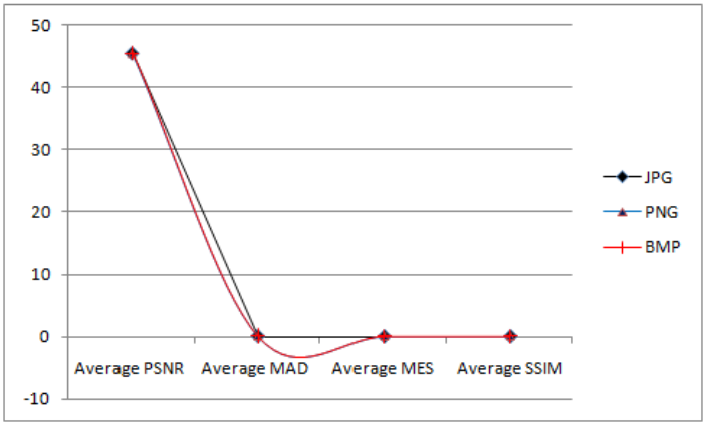

Fig. 3: Average Parametric Values

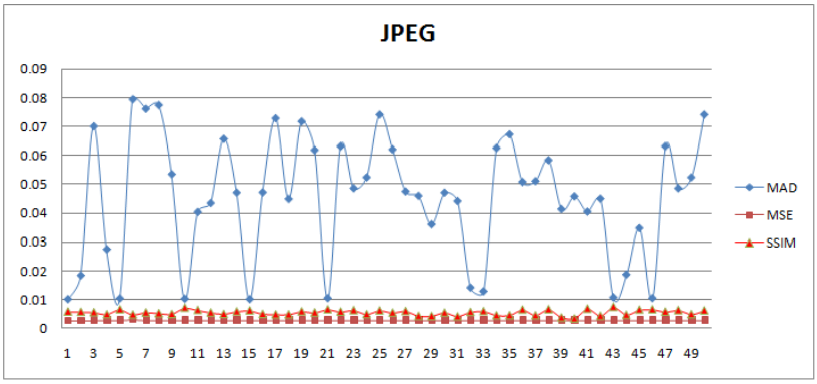

Fig. 4a: JPEG Parameters

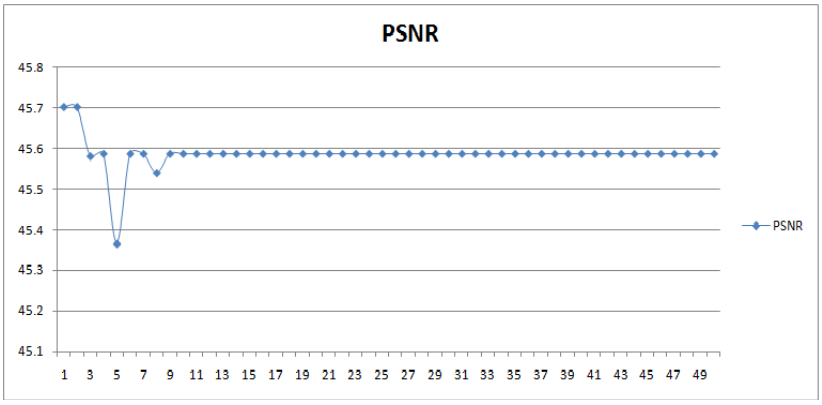

Fig. 4b: JPEG PSNR

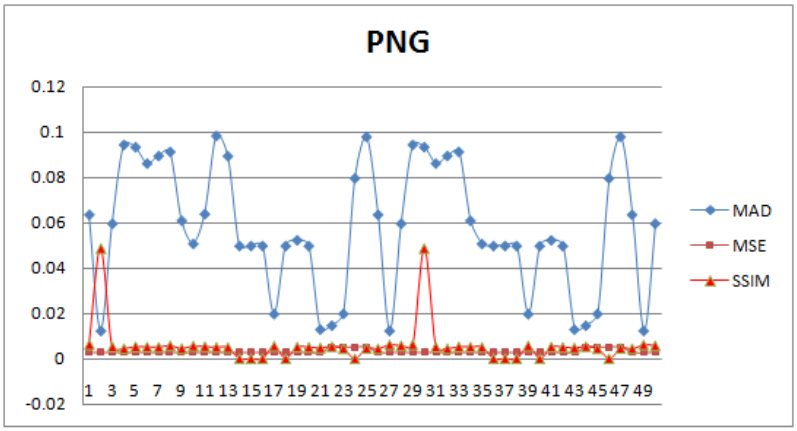

Fig. 5a: PNG Parameters

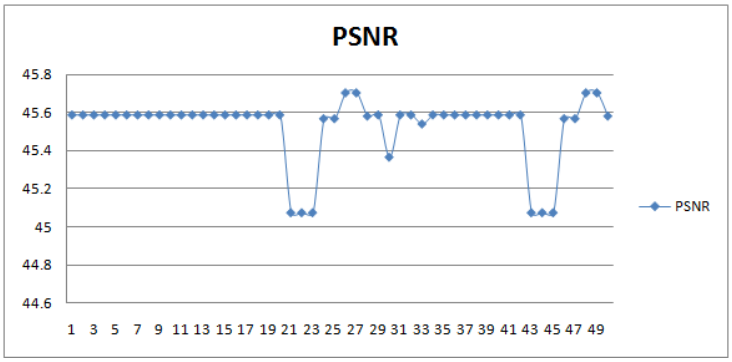

Fig. 5b: PNG PSNR

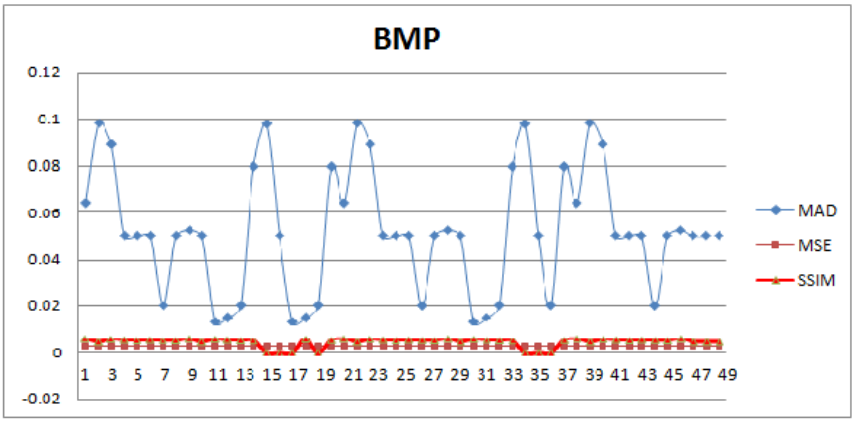

Fig. 6a: BMP Parameters

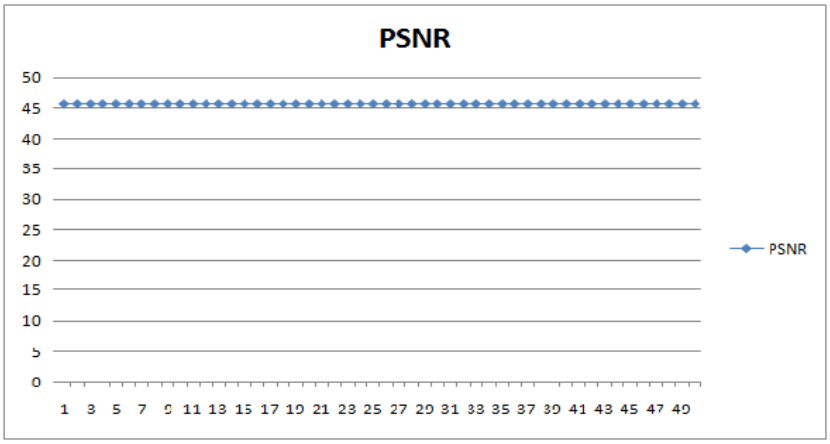

Fig. 6b: BMP PSNR

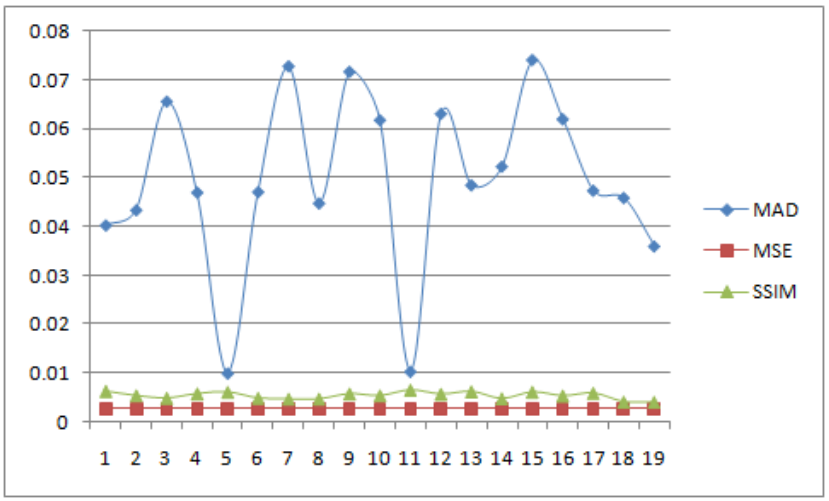

Fig. 7a: High Frequency Parameters

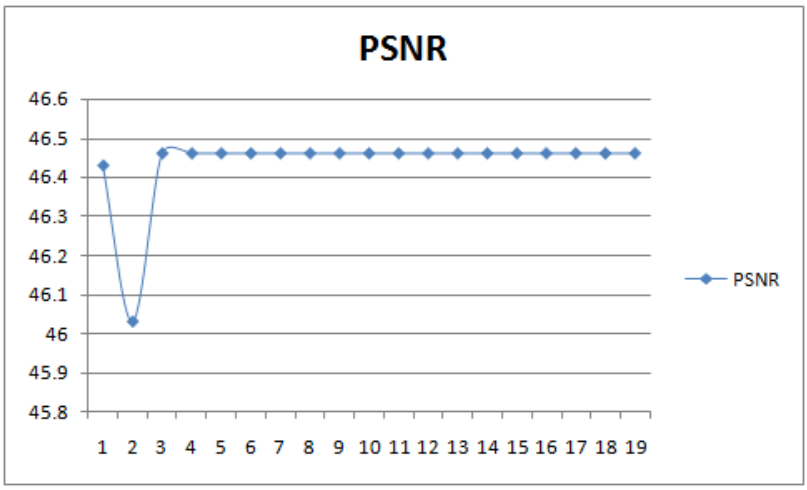

Fig. 7b: High Frequency PSNR

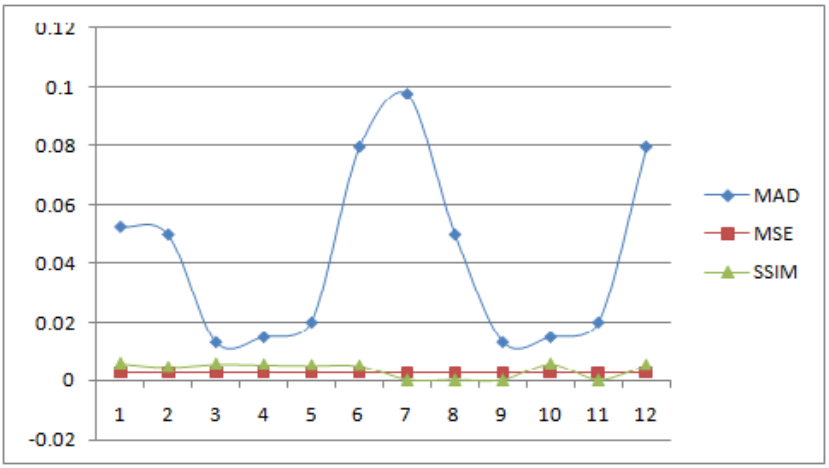

Fig. 8a: Low Frequency Parameters

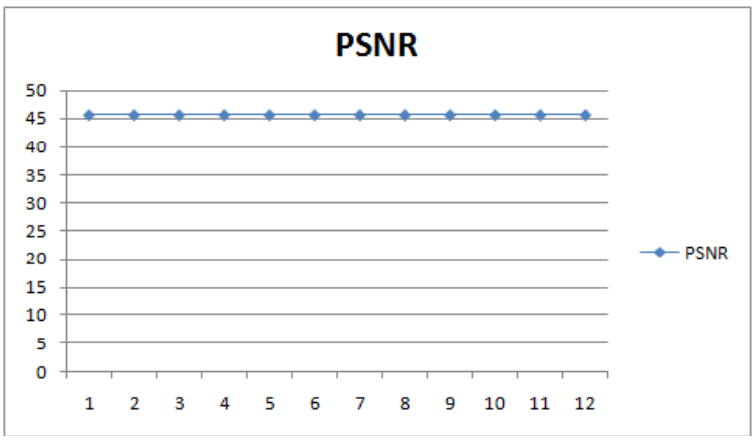

Fig. 8b: Low Frequency PSNR

Logistic mapping technique carried for scrambling of image retrieves non- square image at the receiver without alteration is shown in Fig. 2. The variation in histogram gray levels of original and scrambled images maintain security of image from third party user. For result and experimentation test images are taken randomly from UCID (Uncompressed Image database) and HOLIDAYS datasets. Table.1 gives the average of parametric values for 150 images of different types that show values obtained for MAD, MES, and SSIM are less and

brought down from 0.5 to 0.04 till 0.004 (encrypted image is completely unidentical from the original image) and also data security is further enhanced with increase in PSNR from 16dB to 45.5dB by the proposed system than other LSB methods which is graphically represented in Fig. 3. The experimental results also demonstrate that the proposed system is more efficient for JPEG images as compared to other type and are shown in Fig. 4a, 4b, 5a, 5b, 6a and 6b respectively. In addition, similar experiments are carried out for low and high frequency images which gives PSNR greater than 45dB and image similarity values less than 0.1, depicted in Fig. 7a, 7b and Fig. 8a, 8b respectively. This outperforms the other existing systems by providing more security and efficiency.

5 Conclusion

This method presents an efficient RDH scheme which is based on scrambling of pixel values and position in order to obtain an encrypted image. The original image from content owner is sent to data hider for further processing. Here before embedding secret data, image is decomposed and vacant space is created by compressing redundant bits because of which the approximate capacity of data embedding for an system is known. Then the encrypted or stego image is given to receiver along with both encryption and private key in order to extract secret message ones the original image is retrieved. By correlating results with the current methodologies, it is concluded that reversible data hiding with scrambling of pixel values and position leads to more accurate and upgraded results compared to that of existing methods. The algorithm is of great use as it can prove beneficial for efficient data secrecy.

References

[1] X. Zhang , Reversible data hiding with distributed source encoding, IEEE Signal Trans. circuits and system for video Technology, Vol. 16, no. 4, pp. 636-646, (Apr. 2015).
[2] Z. Ni, Y. Shi, N. Ansari and S. Wei Reversible data hiding, IEEE Trans. Circuits Syst. Video Technol., Vol. 16, no. 3, pp. 354-362, Mar. (2006).
[3] Zhenxing Qian, Xinpeng Zhang, Reversible Data Hiding in Encrypted Image With Distributed Source Coding. IEEE Transactions on Circuits and Systems for Video Technology, 2418611,(Aug 2015).
[4] Zhenxing Qian, Xinpeng Zhang, and Shuozhong Wang, Reversible Data Hiding in Encrypted JPEG Bitstream, IEEE Transactions on Multimedia, Vol. 16, No. 5,Aug.2014.
[5] W. Puech, M. Chaumont and O. Strauss , A reversible data hiding method for encrypted images," Proc. SPIE 6819, Security, Forensics, Stenography, and Watermarking of Multimedia Contents, Vol. 6819, pp.430-438, (Feb 2008).
[6] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, lossless generalized-LSB data embedding, IEEE Transactions on Image Processing,14(2), pp. 253-266 (Feb. 2005).
[7] X. Zhang , Reversible data hiding in encrypted images, IEEE Signal Process. Lett., Vol.18, no. 4, pp. 255-258, (Apr. 2011).
[8] W. Hong, T. Chen, and H. Wu, An improved reversible data hiding in encrypted images using side match, IEEE Signal Process. Lett., Vol. 19, no. 4, pp. 199-202, (Apr. 2012).
[9] K. Ma, W. Zhang, K. Ma and N. Yu, Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption, IEEE Trans. Inf. Forensics Security, Vol.8,no.3, pp. 553-562, (Apr.2013).
[10] W. Zhang, K. Ma and N. Yu, Reversibility improved data hiding in encrypted images, Signal Processing, Vol. 94, pp. 118-127, (June 2014).
[11] D. Slepian and J. K.Wolf, Noiseless coding of correlated information sources, IEEE Trans. Inform. Theory, vol. IT-19, pp. 471480, (July 1973).
[12] D.M. Thodi and J. J. Rodriguez, Expansion embedding techniques for reversible watermarking, IEEE Trans. Image Process., vol. 16, no. 3, pp. 721-730, (Mar.2007)
[13] A. D. Liveris, Z. Xiong and C. N. Georghiades. Compression of binary sources withside information at the decoder using LDPC codes, IEEE Communications Letters, vol. 6, no. 10, pp. 440-442 (2002).
[14] W. Yanling. Image scrambling method based on chaotic sequences and mapping. In Education Technology and Computer Science, ETCS 09. First International Workshop on, volume 3, pages 453457, (March 2009).
[15] C. Honsinger, P. Jones, M. Rabbani, and J. Stoel, Lossless recovery of an original image containing embedded data ", U. S. Patent 6 278 791, (2001).
[16] M. Patil, B.Iyer and R.Arya, “Performance analysis of PCA and ICA for facial expression recognition”, Advances in Intelligent Systems and Computing, Vol. 436, pp. 965-976, Mar.2016.