Reversible Data Hiding for Security Applications

Baig Firdous Sulthana,
M.Tech Student (DECS),
Gudlavalleru engineering college,
Gudlavalleru, Krishna (District),
Andhra Pradesh (state), PIN-521356

S. Bhavani,
Assistant Professor,
Gudlavalleru engineering college,
Gudlavalleru, Krishna (District),
Andhra Pradesh (state), PIN-521356

ABSTRACT
This paper discuss about RDH technique in encrypted image. In this paper RDH use single-level-2D-DWT and optimal transfer mechanism. Original image is converted into number to string which is having some numeric values. In the RDH technique a host image is taken and is divided into two parts. The pixel values of each part are calculated and estimate the errors using optimal mechanism. Optimal mechanisms find out the errors which are closer to zero and reduce the payload distortion problem. Then data will be embedded. Single-level-2D-DWT is used for filtration of embedded data; it will help in removing the de-noising, compression, expansion of image. The image will be hided and that hided image is send to recipient. The sender will send the two keys. The recipient will successfully take out the embed covert data and recovered the original data using inverse process.

General Terms
Encryption, Data Hiding, decryption and Secret key

Keywords
Optimal transfer mechanism, Reversible data hiding and Single-level-2D-DWT

1. INTRODUCTION
Data hiding is the process where the top secret information is inserted into a delivery service signal by changing the unimportant components for hiding communication, Authentication, fraud detection etc. Now-a-days data hiding has become a well known technique in security applications such as military, defense etc. In some cases data hiding procedure will have distortion in the host signal. Such, distortion signal will not be acceptable at very small condition like medical images and remote Sensing areas. Reversible data hiding is important while adding extra data or message in the reversible style where the original one will be completely restored after taking out the hidden data. Here an image is taken in that image data is inserted which is invisible. After that data embedding process will occur it will decreases the quality of image. In the data hiding process,

Data will be embedded and it is hidden in the digital image so that the third party could not extract the hidden information. The proposed method will use the iterative procedure that is nothing but optimal transfer value mechanism. In optimal transfer mechanism it will estimate the error and payload distortion during the data embedded process. Reversible data hiding technique is used for security applications and it is helpful for reducing the errors and distortion in the image.

This paper scales as different sections, section 1 introduction, section 2 existing work, section 3 proposed scheme. Section 4 experimental results and section 5 conclusions, acknowledgment and section 6 references.

2. EXISTING WORK
2.1 Lossless Compression based method
Lossless compression (LC) method is used for storing purpose. In LC method digital images are taken because image size will be more, so it is necessary to compress the file for easy storage purpose. Example zip files, audio and video images, text etc., in LC method, using exact idleness of the host to perform a LC in order to make additional gap to keep extra top secret data in it. The lossless coding consist of three parameters that are transformation, data to symbol mapping and lossless symbol coding The lossless compression based methods make use of statistical redundancy of the host media by performing lossless compression in order to create a spare space to accommodate extra secret data. Consider a RS method [1], to give a gap in data hiding; the data will be losslessly compressed in the RS status. The pixel value in a system [2], will be embedding the lossless generalized LSB with this there is quantized DCT coefficients in a JPEG image [3] also give the necessary data gap. In the RDH extra space is also provided to keep secret information for longer time when the chosen item is compressed. In Lossless compression based method the capacity will be low, for longer files there is chance of complexity.

2.2 Difference Expansion Method
Difference expansion method is used for restoration of information, message authentication code and the additional data also will be embedded with different values. In the DE method [4], difference among two neighboring pixel are double hence a novel LSB plane can be obtain without moving any information of a original pixel. Therefore, secret message simultaneously will be compressed the location map which will be less important for each pixel couple, it is not important because it is a host information; it will be embedded for obtained LSB plane. In DE the compression rate is high for location map, so that each pixel can take one bit only. In DE method it can embed large amount of data, but the maintenance is poor. There are different techniques in DE method they are pixel value prediction mechanism [5], generalization of location map [6], [7], and [8]along with development of compressibility of location map [9].

2.3 Histogram Modification
In histogram modification (HM) method [10],[11], data hider can also occupy HM method to grab reversible data hiding. Here each blocks will divided in two parts after pseudo-randomly segmenting process, alterations of histograms of two parts of a loop is used to insert one bit is present in each block. In HM it implemented the prediction error of host [12].[13] and several good prediction approaches have been introduced to improve the performance of RDH [14].In the

recipient side, the original image recovered by back procedure. Therefore the payload will be low in each block and each block will carry one bit in it. In HM method the contrast of background noise will increase, while decreasing the usable signal.

3. PROPOSED WORK

The proposed scheme of RDH technique is achieved for gray scale image as it improves the capacity of hidden data. Originally for more privacy protection content holder encrypt the original image by using encrypted key and data hiding key is used for hiding the information in the image. Both the keys are used in the destination side to recover the hidden data. Proposed work is explained with the help of flowchart consist of three modules encryption, reversible data hiding and decryption. The content holder encrypt the original image by using encryption key and it is embedding the hidden data in an encrypt image. Then by using data hiding key the secret data and image is hided. During the data embedding process a host image is taken in that pixel value is divided is two parts and pixel value of each part is calculated. After that pixel estimation takes place. It will estimate the errors during the pixel estimation. Optimal value mechanism is used for estimation of errors. The optimal transfer mechanism is formed to maximize the quantity of secret data, i.e., the pure payload. Optimal mechanism is used to modify the error and the data embedding is orderly performed, and if there is additional information are present and that information also embedded. If there is problem distortion it will be solved by using optimal mechanism as it happens during the embedding process. After embedding process then filtration occur for that single-level-2D-DWT is used as it help for removing de-noising, compression, expansion problem. The recipient will get the two keys send by sender and recipient can successfully take out the embedded top secret data and recovered the original data in inverse process. Using the proposed method the errors and make the image distortion free and it is used for high security purpose also.

3.1 Module Encryption

In an encrypted image mainly it is having three drawbacks that are data integrity and when a homogenous zones i.e., when the blocks are using the same color at that time the blocks will be encrypted in the same manner and third one is, it cannot robust to noise because as there will be large number of blocks will be present in it. It will be in size of 128bits. It means it use 128 cipher key in it. So, to overcome the problem AES algorithm is used. In the AES algorithm it is having number of rounds in it and in this iteration process also occur in it. In a AES algorithm number of rounds depends on size of the key and size of the block in it. As AES algorithm calculate more then128, 192,256 bits in it. AES algorithm is good for security purpose.

3.2 Module Reversible Data Hiding

In reversible data hiding process, consider how the data hiding process will occur in the encrypted image. Let us take an original image to that image apply encrypted key and then the encrypted image will be hidden with some data and again there will be data hiding key will be applied to hiding data and image. It recovers the original content, as the sender will send the key to the recipient side so that no one can stole the key. Reversible data hiding is the process where the data is extracted in the inverse manner but there will be no loss of data. Errors are not allowed in the reverse manner. The optimal transfer value mechanism is used in the size of the additional information that does not affect the optimal transfer value matrix. In a data embedding procedure host image is taken and pixel divided into two parts and calculates the each pixel value. In RDH technique optimal mechanism is used which is helpful in estimating the errors and payload distortion. By optimal mechanism, estimate the error in each pixel and neighboring pixel also and then data embedding process will take place. Then the two data embedded parts A and part B will be combined to give the new data hided image. For that optimal mechanism is used. For that new image filtration is done. For that single-level-2D-DWT is used. This transform is using daubechisD4 wavelet transform. It is helpful for removing noise, compression and expansion from an embedded image.

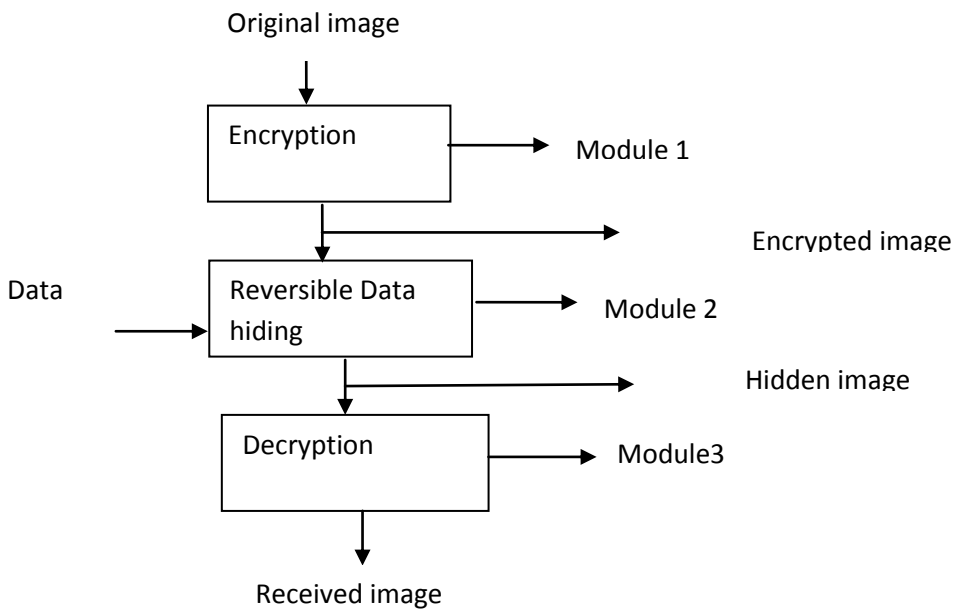


Fig 1: Flowchart of proposed work

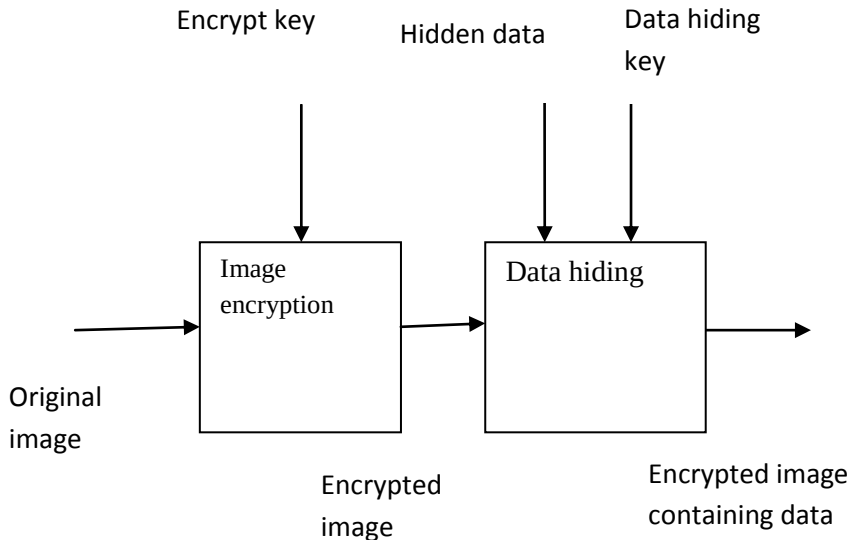


Fig 2: Data hiding in encrypted image

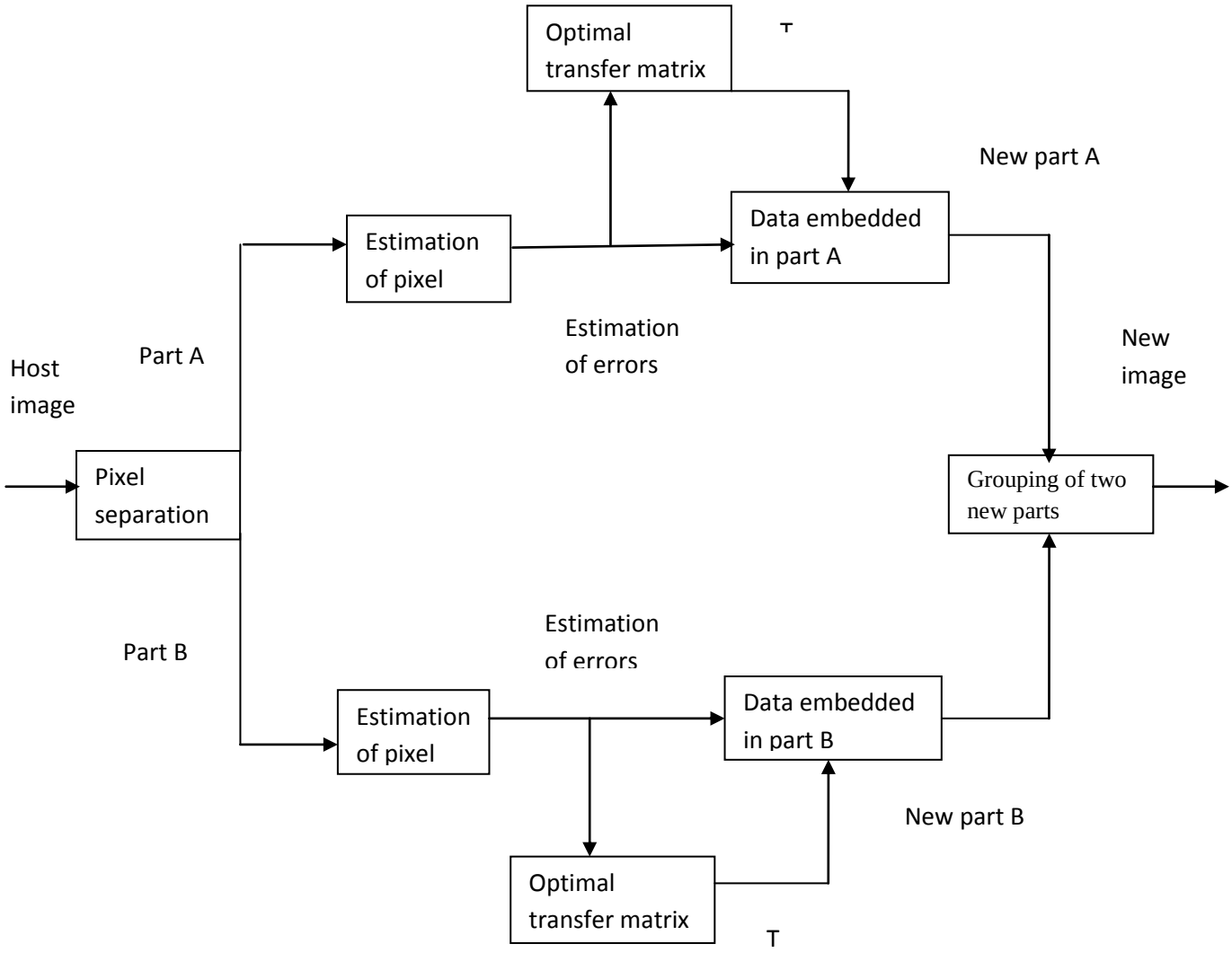


Fig 3: Data embedding procedure

3.2.1 Optimal Transfer Mechanism

In the RDH, using the optimal value transfer mechanism, it is a iterative procedure that is nothing but mathematical expression only. It will be in matrix format only; it will modify the cover values in RDH. In RDH optimal transfer matrix model is used. To denote a histogram data

$H=\{\ldots,h_{-3},h_{-2},h_{-1},h_0,h_1,h_2,h_3,\ldots..\}$ where h_k= The amount of obtainable data with a value k.
To denote the amount of available data possessing of original value i and new value j for data hiding as $p_{i,j}$, and the transfer matrix is $T=\begin{bmatrix} Px1,x2 & \cdots & Px1,x2 \\ \vdots & \ddots & \vdots \\ Px1,x2 & \cdots & Px1,x2 \end{bmatrix}$

Where x1 and x2 are a minimum and maximum available cover data. In a optimal mechanism the difference Between two neighboring pixel are doubled and the secret bit present in it is embedded. In the LSB the new difference value is $q'=2.q+b$ here q ,q' and b are the original pixel-difference, new reference value and the secret bit ,here difference in the original value q will changed as 2q/(2q+1) where the secret bit b as 0/1.

3.2.2 Single-level-2D-DWT

In a single-level-2D-DWT, daubechisD4 transform is used; it is used for special cases applications, because it is used in finite data sets. It is a matrix technique in linear algebra in this scaling function and wavelet function is calculated. The daubechisD4 scaling and wavelet function coefficient can shift from right to left by two places in each iteration. There will be no overlapping occur .The scaling functions coefficients and wavelet transform are

DaubechiesD4 scaling functions:

$a_i = f_0s_{2i}+f_is_{2i+1}+f_2s_{2i+2}+f_3s_{2i+3}$

$a[i] = f_0s[2i]+f_1s[2i+1]+f_2s[2i+2]+f_3s[2i+3]$

DaubechiesD4 wavelet function:

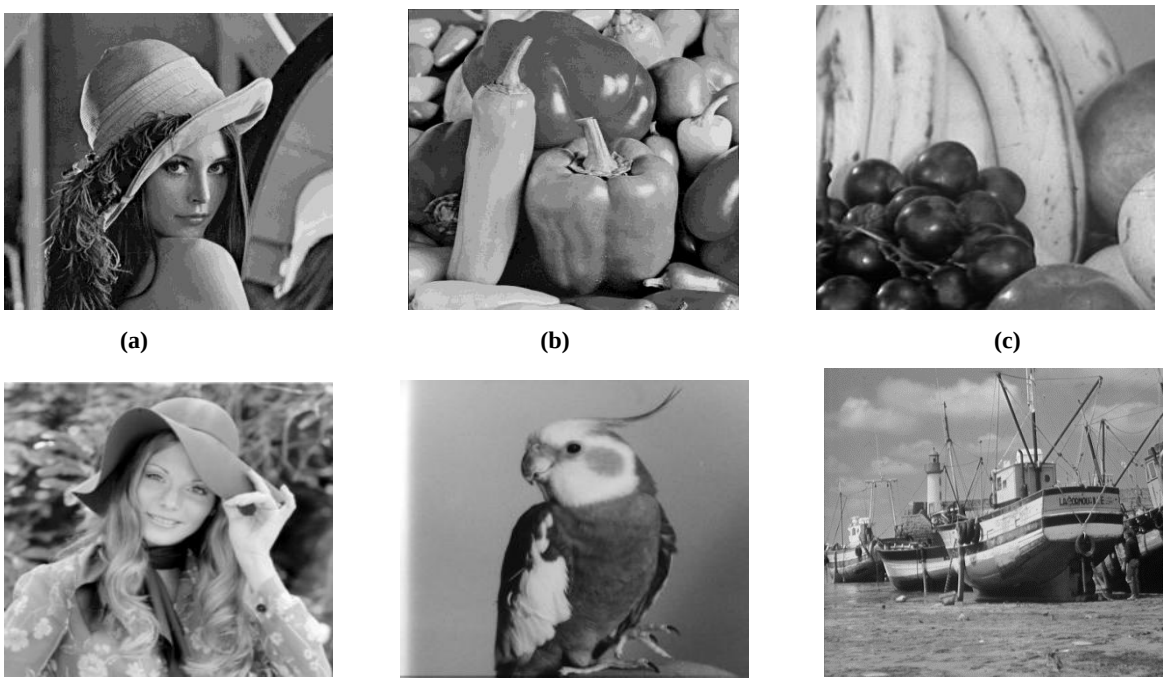
$w = b_0s_{2i}+b_1s_{2i+1}+b_2s_{2i+2}+g_3s_{2i+3}$

$w[i] = b_0s[2i]+b_1s[2i+1]+b_2s[2i+2]+b_3s[2i+3]$

3.3 Module Decryption

In the decrypted image data is extract and the required data that is embedded secret information and it recovered the original data in inverse manner. In a decryption side the exact data what have sent in the source side is achieved. Therefore, in the recipient side distortion free image and required data is achieved.

4. EXPERIMENTAL RESULTS



(a) **(b)** **(c)**

(d) **(e)** **(f)**

Fig 4: Host images sized 512x512 (a) Lena (b) peppers (c) fruit (d) hat (e) bird (f) boat

In a host images which is sized as 512x512, show in a below Fig 4. As these host images is divided in the two parts i.e., Part A and Part B and each parts having the pixel and each pixel value is calculated. The Part A and Part B is divided as odd pixel and even pixel and it is taken as white pixels and black pixels. Then pixel value is estimated, during the estimation process errors may occur. For that optimal mechanism is used, it will modify the error and payload distortion problem. Then image is encrypted by using the AES algorithm. There will be encrypted key is applied. In RDH process the embedding process will take place at that time there is chance of error to estimate that error is removed by using the optimal transfer mechanism in it. Single-level-2D-DWT is used for compression and noise and for filtration purpose. Finally decryption takes place in it. In recipient side, successfully take out the embedded secret data and recover - ed the original information in the inverse manner. On the other side when there is additional information is present at that time the data is inserted in the image. At that time the data will be small and it will not affect the baboon image as there will be no distortion problem in it. Final result is good payload-distortion presentation and error free image.

Table 1: comparison table for proposed method and existing method

Techniques		**Lena**	**Peppers**	**Fruit**	**Hat**	**Bird**	**Boat**
Reversible Data Hiding (RDH)	PSNR	51.41	49.91	48.97	48.82	48.65	47.89
	Payload	2.11	2.37	0.68	0.53	0.76	1.74
watermarking by Difference Expansion	PSNR	33.59	34.00	34.67	29.52	35.18	33.51
	Payload	0.40	0.50	0.67	0.52	0.761307	0.32

Comparison table shows the difference between proposed method (reversible data hiding) and existing method (watermarking by difference expansion) under PSNR and Payload values. The Payload value is measured in bpp (bits per pixel).In RDH technique it is noted that 8-bits images are used. When comparing to watermarking by difference expansion method the PSNR and Payload values are more in RDH method. For example take Lena image which is 8-bit image, in RDH method Lena image the PSNR value is 51.41dB where as in watermarking by difference expansion method the PSNR value for Lena is 33.59dB. In RDH method the Payload value for Lena is 2.11bpp where as in watermarking by difference expansion method the Payload for Lena is 0.40bpp. Comparing both methods the PSNR value and Payload value will be decreases. In a comparison table the remaining images PSNR and Payload values will be decreases when comparing with watermarking by difference expansion method RDH method is good.

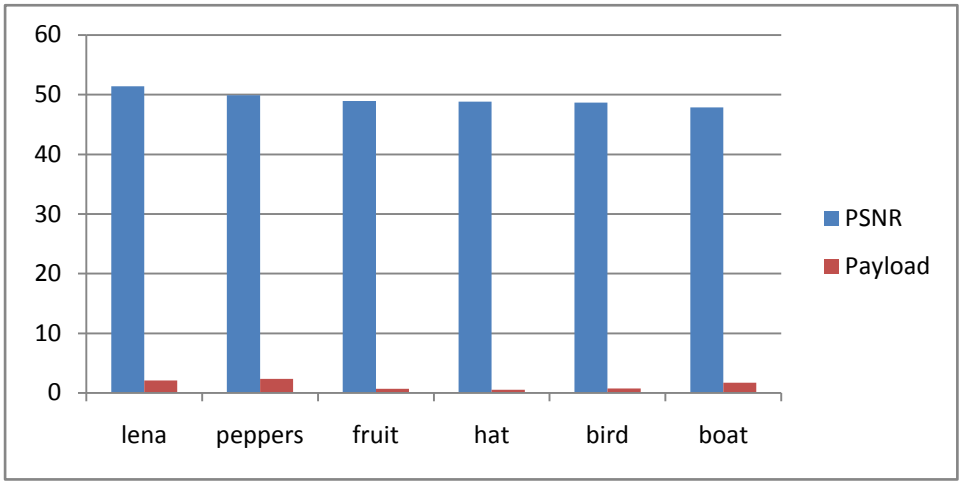


Fig 5: PSNR and Payload for proposed method

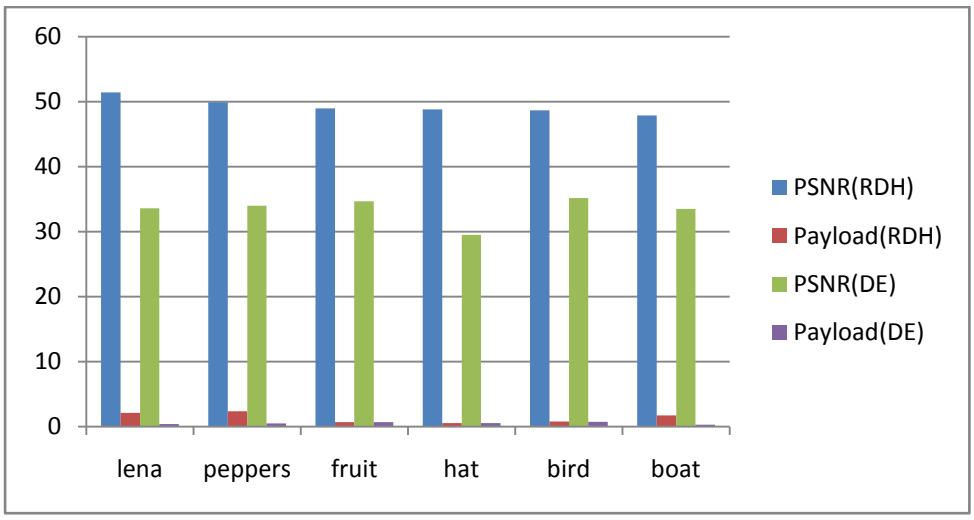


Fig 6: comparison graph between proposed method and existing method

5. CONCLUSION

Transmission of hidden data with good payload- distortion and less errors is done by optimal transfer value mechanism. The optimal transfer mechanism is used to estimate the errors which are closer to zero, so that a good performance can be achieved. The payload size depends on image complexity. For smooth host images, the proposed method significantly outperforms the previous reversible data hiding methods. The noise during compression and expansion is removed using sigle-level-2D-DWT. RDH technique provides better encryption and successful secret data transmission compared to existed techniques. It is mainly used for security applications like defense, military, banking sectors etc. If smarter prediction method is exploited to make the estimation errors closer to zero, a better performance can be achieved, but the computation complexity due to the prediction will be higher. The combination of optimal transfer mechanism and other kinds of available cover data deserves further investigation in the future.

6. ACKNOWLEDGMENTS

Our thanks to the experts who have contributed towards development of the template.

7. REFERENCES

[1] M.Goljan, J.Fridrich, & R.Du, "Distortion-free in data embedding," In proc. 4th Int. Workshop is on Information Hiding, Lecture Notes in Computer Science, vol. 2137, pp. 27-41 , 2001.

[2] M.U.Celik, G.Sharma, A.M.Tekalp, & E.Saber, "lossless generalized LSB data on embedding," IEEE trans. Image process. vol. 14, no.2, pp. 253-266, Feb 2005.

[3] J.Fridrich, M.Goljan, & R. Du,"Lossless data embedding for all image formats,'' in proc.4th SPIE. Security and Watermarking of Multimedia Contents, vol. 4675, pp. 572-583, 2002.

[4] J.Tia, " Reversible data embedding using the difference expansion, " IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890-896, Aug 2003.

[5] H.-C. Wu, C.-C. Lee, C.-S. Tsai, Y.-P. Chu & H.-R. Chen, "In a high capacity reversible data hiding scheme with an edge prediction & difference expansion," J. Syst. Softw., vol. 82, pp. 1966-1973, 2009.

[6] L.Kamstra & H.J.A.M. Heijmans,"Reversible data embedding keen on images using wavelet techniques and sorting," IEEE Trans. Image Proces., vol. 14, no. 12, pp. 2082-2090, Dec 2005.

[7] H.J.Kim, V.Sachnev, Y.Q.Shi, J.Nam, & H.-G.Choo,"A novel difference expansion transform used for reversible data embedding," IEEE Trans. Inf. Forensics.

[8] S.Weng, Y. Zhao, J.-S. Pan, & R.Ni," Reversible watermarking based on invariability and adjustment on pixel pairs," IEEE Signal Process. Lett, vol. 15, pp. 721-724, 2008.

[9] Y.Hu, H.-K .Lee, & J.Li," DE-based reversible data hiding by improving overflow location map," IEEE Trans.Circuits Syst, Video Techol., vol. 19, no. 2, pp. 250-260, Feb 2009.

[10] Z.- Ni, Y.Q. Shi, N. Ansari, & W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354-362, Mar 2006.

[11] W.-L. Tai, C.-C. Chang, "Reversible data hiding based on histogram modification of pixel differences," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 6, pp. 906-910, Jun 2009.

[12] C.-C. Chang, C.-C. Lin, Y.-H. Chen," Reversible data-embedding scheme using differences between original & predicted pixel values," IET Inf. Security, vol. 2, no. 2, pp. 35-46, 2008.

[13] P.Tsai, Y.-C.Hu, H.-L. Yeh, "Reversible image hiding scheme using predictive coding & histogram shifting," Signal Process. vol. 89, pp. 1129-1143, 2009.

[14] W. Hong, T.-S.Chen, Y.-p. Chang, a C.-W.Shiu, "In a high capacity reversible data hiding scheme using of orthogonal projection and prediction error modification," Signal Process., vol .90, pp. 2911-2922, 2010.