International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-1S3, December 2019

Multi-Layered 'Odd-Even' Reversible Embedding for Encrypted Images

Geetha R, Geetha S

Abstract: ***Reversible Data Hiding (RDH) has been under research for the past two decades. Recently RDH in encrypted images (RDH-EI) draws more attention among the researchers. Since it is used effectively in privacy protection and cloud computing. In this paper, a RDH-EI using LSB based odd-even embedding technique scheme is proposed. Initially the cover image is encrypted using block and pixel scrambling and bit plane mix ordering. Block and pixel scrambling is done through four random walks/Space Filling Curves (SFCs). Each block and pixel is tested for randomness of information source through each random walk. Finally the secret message is embedded in each block of image based on testing the pixel value and position value in the block using LSB embedding. This method avoids overflow/underflow issues that usually happens in RDH/LSB embedding.***

Keywords : encryption, histogram, PSNR, reversible data hiding.

I. INTRODUCTION

Data hiding is a mode of communication secretly between users by modifying the bits in the pixels. Mostly digital images are utilized as cover data in which modification happens. RDH implies that original cover data is recovered after extracting the secret information. Reversible data hiding plays a major role in applications where negligible distortion in the cover image is not acceptable. Selected fields like telemedicine, forensic, military imagery and law enforcement are examples where RDH plays an important role. For the past two decades, various RDH methodologies [1]-[7] have been proposed in order to attain better distortion rate. Now a days, cloud computing and storage development demands privacy protection on data than exposing the original content. This made the researchers to show attention towards RDH-EI.

According to statistics in RDH techniques, it can be broadly classified into three categories. Difference Expansion (DE) methods[12]-[15], Histogram Modification/Shifting (HM/HS) methods[8]-[11] and lossless compression schemes.[3]-[6] In DE techniques, difference between the adjacent pixels is computed and twice the difference is modified to the LSB plane of the pixels to embed the message bit '1'/'0'. In HM/HS techniques, secret bit '1'/'0' is embedded by modifying one or more peak values in the histogram of the cover image. Reversibility is achieved by shifting the remaining pixels peak point and the valley point. In lossless
Compression scheme, data is embedded by creating a sparse space through lossless compression mechanism over cover images. Later, Prediction Error Expansion (PEE)[12,13] [23-26]mechanism was introduced to achieve improved distortion rate performance. Widespread improvement in cloud computing and storing has attracted the content owner by protecting their original content. For this purpose, many researchers started working for RDH in encrypted images. In this approach, three users are involved. The content owner who encrypts the cover image by some encryption algorithm and data hider takes care of the data hiding mechanisms. Data hider uses an effective algorithm suitable for encrypted images to hide the secret information for eg, content owner authentication information, timestamp, etc., Third user is the receiver, based on the authority given to the receiver can either extract the secret information/cover image content.

Manuscript published on 30 December 2019.
* Correspondence Author (s)
Geetha R*, Department of ECE, MVJ College of Engineering, Bangalore India. Email: geetha.r2014phd1168@vit.ac.in
Geetha S, Professor, SCSE, VIT University Chennai, India. Email: geetha.s@vit.ac.in

II. STATE OF ART REVIEW

In general, RDH in encrypted images is broadly differentiated into two categories. Vacating Room After Encryption which is abbreviated as VRAE and Reserving Room Before Encryption (RRBE). In VRAE techniques, the cover image is encrypted directly by the content owner and it is sent to the data hider. Then the data hider, using some RDH mechanism embeds the secret information by altering the encrypted image.. In RRBE methods, the correlation of the pixels in the spatial domain is analyzed throughout the cover image and embedding is done by reserving room before encryption.

A. Encryption Methods

In [14] the proposed VRAE based scheme, initially the content owner does the image encryption by means of bitwise XOR operation using the encryption key. Later the data hider hides the secret information by dividing it into non-overlapping blocks with each block pixels being segmented into two equal halves in accordance to the data hiding key. For embedding one bit of data in each block, with three LSBs flipped and remaining pixels unchanged. At the receiving end unaltered five MSBs are decrypted first and from the remaining flipped LSBs data is extracted and then reformed to original pixel values. In [15] improved smoothness function than [16] was proposed for better accuracy. Still accuracy problem cannot be achieved by these two proposed schemes. Even the embedding rate of the proposed schemes were not satisfactory so far.

Later redundant space transfer RDHEI scheme was proposed in [liu and pun.] In this scheme the redundant space in the cover image is utilized by transferring it to the encrypted image and the same was used in the encrypted image for embedding the secret information. The redundant space present in the encrypted image was used and the data is hidden by means of traditional RDH methods. In this scheme, the entropy of the image also remains unchanged.

B. Non Compressed Domain

In [16], the scheme presented by Zhang, the encrypted image is first partitioned into non-overlapping blocks and half of the pixels are flipped according to the bits to be embedded. The three LSBs of the pixels were flipped and the remaining pixels remain unchanged. Restoration of the original pixels is determined by the blocks that were being flipped and the data was extracted.. This has been achieved by estimating the spatial correlation present in the decrypted image. Hong et al. [17] proposed a method which reduces the error rate in zhang's scheme. This was achieved by introducing a new estimation equation which also involves side matching technique. Later the performance measures in [16,17] was improved in [18] by estimating the complexity present in the pixel distribution in the image blocks. Data hiding scheme considers the neighboring pixels in all directions. In [19], prediction error based scheme was proposed by Wu and Sun. Decryption algorithms aims at estimating the prediction errors present in decrypted image. The above mentioned schemes depends on the spatial correlation of pixels in the cover image. The marked encrypted image needs to be decrypted first before extracting the hidden image.

C. Compressed Domain

In [19], Qian et al. initialized with this kind of compressed domain reversible data hiding scheme for encrypted images for still image bit streams (JPEG). Bit stream of JPEG encrypted image is obtained by encrypting the table that has been quantized and the original bits of JPEG image is appended. The message is encoded using error correcting code before embedding it into the encrypted JPEG bit stream. Finally the encoded bit steam is embedded into the encrypted JPEG bit stream by means of the proposed scheme in [15]. To extract the hidden information from the marked image, first the marked encrypted image is decrypted before extracting the hidden information. Later the hidden data is extracted

III. Proposed Method

In this framework, the cover image is first encrypted using the encryption key. This is done by the content owner, Then the data hider hides the secret information using the data hiding key. The marked encrypted image is transmitted through the channel and at the receiver side, the data is extracted using the data hiding key and the marked image is decrypted using the encryption key. Fig 1 shows the flow chart for the proposed scheme. Two different keys are involved i)Encryption key ii)Data hiding key. Using two keys, more secure the scheme is.

A. Original Image Encryption

During encryption the content owner encrypts the original image using encryption key. Cover image is divided into non-overlapping blocks. Selection of each block and the selection of pixels in each block is performed by means of any one of the scanning mechanisms shown in Fig 2. Different scanning techniques are

- Z Scan SFC
- Hilbert Scan SFC
- Zig – zag Scan SFC
- Moore SFC

B. LSB Embedding

LSB embedding has an upper bound embedding efficiency e_{em} for an embedding rate η is given by equ (1)

$$e_{em}(\eta) \leq \frac{\eta}{H^{-1}(\eta)}, 0 \leq \eta \leq 1 \quad (1)$$

Where $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function. H^{-1} is its inverse.
Upper bound on embedding rate of ±1 LSB embedding having a constrain of R as an average distortion is given by equ (2)

$$E(R) = \begin{cases} G(R), & R \leq 2/3 \\ \log_2 3, & R > 2/3 \end{cases} \quad (2)$$

Where $G(R) = H(R) + R$.

Embedding efficiency e_{em} can be rewritten for an embedding rate η and is given by equ (3)

$$e_{em}(\eta) \leq \frac{\eta}{G^{-1}(\eta)}, 0 \leq \eta \leq \log_2 3 \quad (3)$$

Where G^{-1} is the inverse function of G.

C. Disordering of Bit Planes

The original fray level pixels with values of each pixels and its coordinates is represented as $I(i, j)$ and the each bit in a particular pixel is represented as $b\,i, j, 1, b\,i, j, 2, \ldots, b\,i, j, 8$ for the 8 bits of the pixel value, where $1 \leq i \leq M$ and $1 \leq j \leq N$ This implies that

$$b_{i,j,u} = \left\lfloor \frac{I_{i,j}}{2^{u-1}} \right\rfloor \bmod 2, \quad u = 1, 2, \ldots, 8, \quad (4)$$

$$b_{i,j,u} \Rightarrow b'_{i,j,v}, \quad \begin{cases} v \in [1,\ \lambda], & \text{if } u \in [9-\lambda,\ 8], \\ v \in [\lambda+1,\ 8], & \text{if } u \in [1,\ 8-\lambda], \end{cases} \quad (5)$$

Equation (4) (5) implies the bit plane before disordering and after disordering.

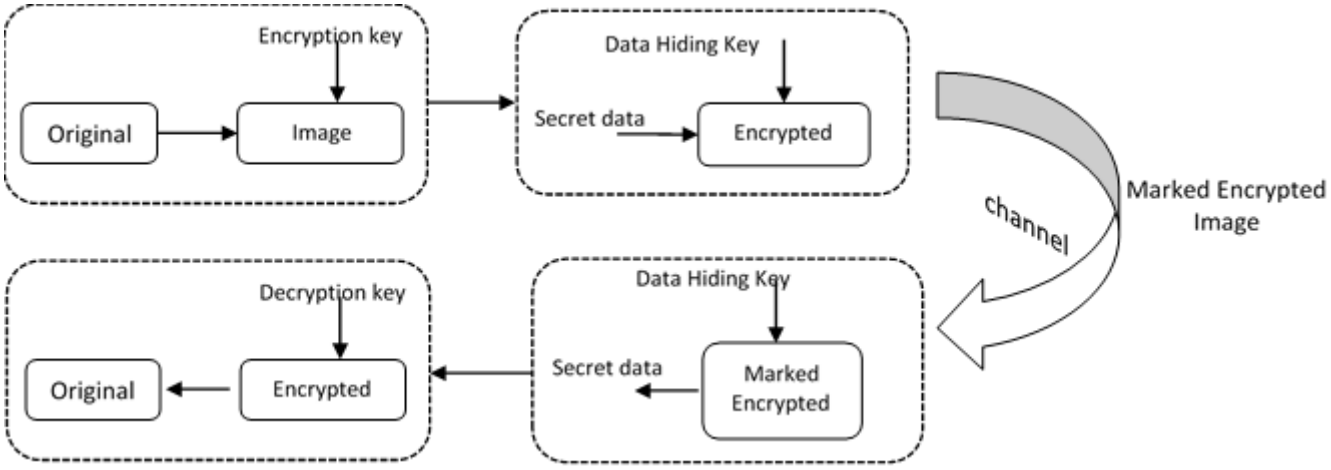


Fig 1 Flow chart of RDHEI

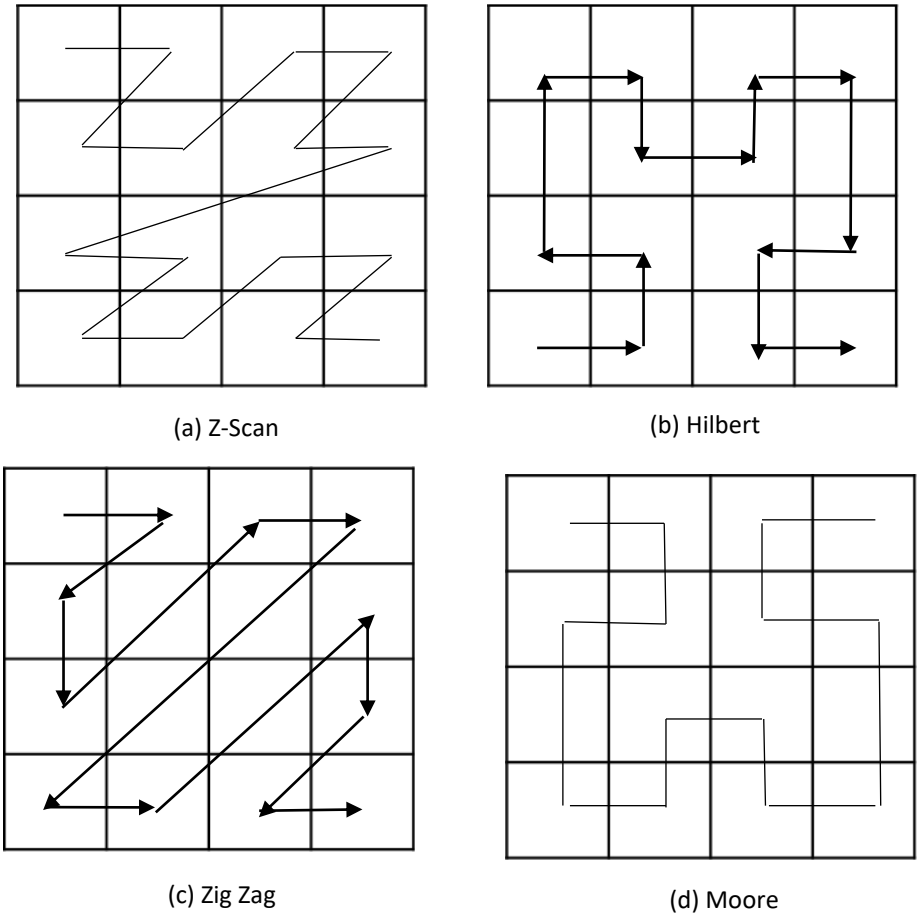


Fig:2 (a) Z scan SFC, (b) Hilbert SFC, (c) Zigzag SFC, and (d) Moore SFC.

D. Pixel and Block Scrambling

Once the disordering of bit planes is done, k blocks located in the image and all *k* blocks are scrambled by means of any one of the scanning mechanisms mentioned in figure 2. and the pixels in each block are scanned in any of the order as that of the block scanning mechanism mentioned above. During image encryption stage, the image is encrypted in a block-wise mechanism manner. This gives assurance of confidentiality of the original information and higher security to the hidden information. After bit plane of the pixels are disordered, the original value of the pixels are changed and there is a drastic change in the correlation between the pixels. MSBs being shifted to LSBs and LSB being shifted to MSBs and so on. This will further enhance the security of the data that is being hidden confidentially.

IV. RESULT AND DISCUSSION

The proposed scheme was tested on various gray scale images given in figure 3. Images considered are of 512 x 512 gray scale images. In the proposed scheme standard encryption techniques like DES or AES is not considered for encrypting the cover image. Encryption is carried out in multiple steps. For any RDH methods the performance of the hiding scheme on the images is measured in terms of Mean Square Error(MSE) and Peak Signal to Noise Ratio(PSNR)

The performance analysis of any RDH scheme can be measured by means of Peak Signal to Noise Ratio(PSNR) (dB), embedding capacity in bits per pixel (bpp). Equations (6) (7) governing all the above two measures are given below:

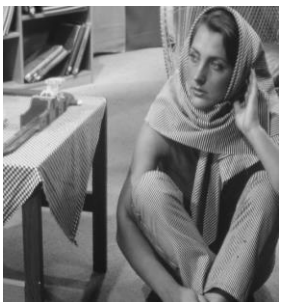
$$PSNR = 10\ log_{10}(255^2/MSE)\ dB \quad (6)$$

Where MSE is the mean square error which can be computed considering the cover image as C and marked image as C' of size $a \times b$.

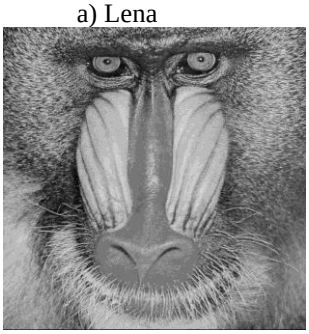
$$MSE = \frac{1}{a \times b} X \sum_{i=1}^{a} \sum_{j=1}^{b} (C(i,j) - C'(i,j))^2 \quad (7)$$

Figure 4 shows the encrypted marked image for the cover images selected for testing. For better visualization of the result for the proposed method with the existing methods, the scheme has been tested on 100 images in the image processing data set. Few images which are familiar are exhibited in this paper for observance and obtained the ER of each image and the PSNR values, and then the results are shown in Table 1.. It can be observed from Table 1 that the PSNR for the proposed method is improved compared to the schemes discussed in [17] and [18]. Irrespective of the nature of the image, this algorithm produces an embedding rate in all images since this algorithm overcomes the problem of overflow and underflow. In the other schemes, the date rate is affected by the smoothness of the image. But this proposed algorithm does not get affected by the smoothness of the images.

a) Lena

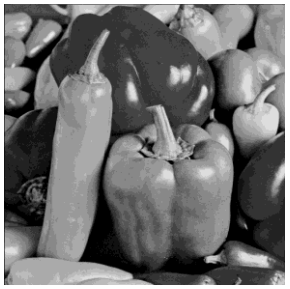


b) Barbara



c) Baboon

d) Airplane



e) Peppers

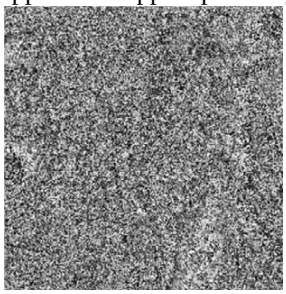
f) Boat

Fig 3. Test images of size 512 x 512

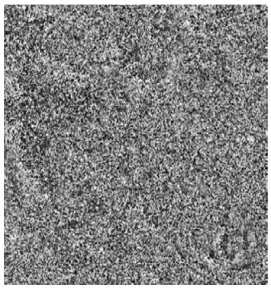
Table I. Comparison of PSNR for ER 1bpp

Test Image	[17]	[18]	Proposed method
Lena	45.12	45.65	46.51
Barbara	46.04	46.91	46.98
Airplane	47.14	47.7	48.25
Baboon	43.22	43.55	44.01
Peppers	46.12	46.65	47.51
Boat	45.12	45.65	46.51
Average	45.12	45.65	46.51

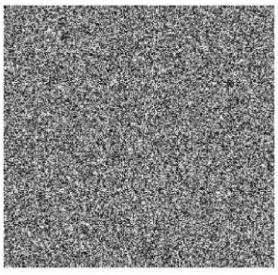
Table I and II shows the result of PSNR for embedding rate of 1bpp and 1.5bpp respectively



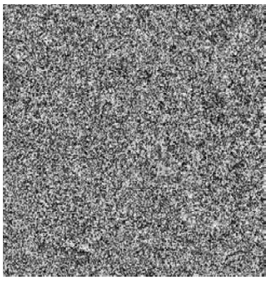
a) Lena



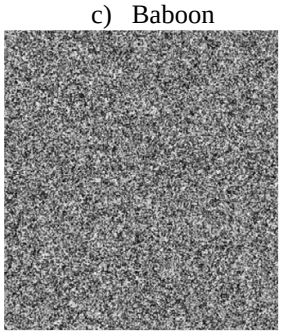
b) Barbara



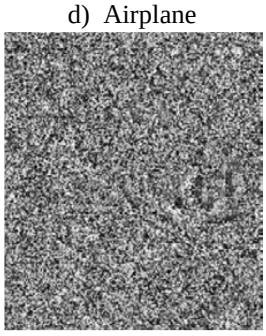
c) Baboon



d) Airplane



e) Pepper



f)Boat

Fig 4: Marked Encrypted images for the given test images

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Table II. Comparison of PSNR for ER 1.5bpp

Test Image	[17]	Gui[18]	Proposed method
Lena	42	42.5	43.36
Barbara	43	43.12	43.38
Airplane	44	44.	44.39
Baboon	40	40.23	41.33
Peppers	42	43	43.35
Boat	42.5	42.65	43.37
Average	**42**	**42.5**	**43.36**

V. CONCLUSION

In this paper, we proposed a LSB embedding based on the pixel bit plane being ODD or EVEN. Embedding can be done multiple times preserving the nature of the pixel pair which is being recorded as an auxiliary information which is required for extraction of the data and for reversibility. This scheme can also be applied on medical images. The proposed method does not suffer from underflow or overflow problem which prevails in other embedding techniques. That's why this scheme is best suited for medical images since medical images has more chance of overflow or underflow problems.

REFERENCES

1. I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*. San Mateo, CA, USA: Morgan Kaufmann,2007.
2. Y. Q. Shi, Z. Ni, D. Zou, C. Liang, and G. Xuan, ``Lossless data hiding:Fundamentals, algorithms and applications," in *Proc. IEEE Int. Symp.Circuits Syst.*, vol. 2. May 2004, pp. 33_36.
3. R. Caldelli, F. Filippini, and R. Becarelli, ``Reversible watermarkingtechniques: An overview and a classi_cation," *EURASIP J. Inf. Secur.*,vol. 2010, 2010, Art. no. 134546.
4. Y. Q. Shi, ``Reversible data hiding," in *Proc. Int. Workshop Digit.Watermarking*, 2004, pp. 1_12.
5. F. Bao, R.-H. Deng, B.-C. Ooi, and Y. Yang, ``Tailored reversible watermarking schemes for authentication of electronic clinical atlas,"*IEEE Trans. Inf. Technol. Biomed.*, vol. 9, no. 4, pp. 554_563, Dec. 2005.
6. W.Zhang, B.Chen, N.Yu, Improving various reversible data hiding schemes via optimal codes for binarycover, IEEE Trans.Image Process.21(6) (2012) 2991 – 3003.
7. J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and applications*. Cambridge, U.K.: Cambridge Univ. Press, 2009.
8. Tian J (2003) Reversible data embedding using a difference expansion. IEEE Trans. Circuits Syst., 13(8):890–896.
9. Z. Ni, Y.-Q. Shi, N. Ansari, andW. Su, ``Reversible data hiding," in *Proc .IEEE Int. Symp. Circuits Syst.*, May 2003, pp. II-912_II-915.
10. 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
11. D. Coltuc and J. M.Chassery, ``Very fast watermarking by reversible contrast mapping," *IEEE Signal Process. Lett.*, vol. 14, no. 4, pp. 255_258, Apr. 2007.
12. S. Weng, Y. Zhao, J.-S. Pan, and R. Ni, ``Reversible watermarking based on invariability and adjustment on pixel pairs," *IEEE Signal Process. Lett.*, vol. 15, pp. 721_724, 2008.
13. L. Kamstra and H. J. A. M. Heijmans, ``Reversible data embedding into images using wavelet techniques and sorting," *IEEE Trans. Image Process.*, vol. 14, no. 12, pp. 2082_2090, Dec. 2005.
14. K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, ``Reversible data hidingin encrypted images by reserving room before encryption," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 3, pp. 553_562, Mar. 2013.
15. W. Zhang, K. Ma, and N. Yu, ``Reversibility improved data hidingin encrypted images," *Signal Process.*, vol. 94, no. 1, pp. 118_127, Jan. 2014.
16. X. Zhang, ``Reversible data hiding in encrypted image," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255_258, Apr. 2011.
17. S. Lian, Z. Liu, Z. Ren, and H. Wang, ``Commutative encryption and watermarking in video compression," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 17, no. 6, pp. 774_778, Jun. 2007.
18. M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. De Natale, and A. Neri, ``A commutative digital image watermarking and encryption method in the tree structured Haar transform domain," *Signal Process., Image Commun.*, vol. 26, no. 1, pp. 1_12, 2011.
19. R. Schmitz, S. Li, C. Grecos, and X. Zhang, ``A new approach to commutative watermarking-encryption," in *Proc. 13th Joint IFIP TC6/TC11Conf. Commun. Multimedia Secur.*, 2012, pp. 117_130.
20. Jung K, Yoo K (2009) Data hiding method using image interpolation. Comput. Stand. Interfaces, vol: 31 PP: 465–470
21. Luo L, Chen Z, Chen M, Zeng X, Xiong Z (2010) Reversible image watermarking using interpolation technique. IEEE Trans. Inf. Forensics Secur., 5 (1): 187–193.
22. Abadi MAM, Danyali H, Helfroush MS (2010) Reversible watermarking based on interpolation error histogram shifting. 5th International Symposium on Telecommunications (IST), Kish Island, Iran, pp. 840– 845
23. Lee CF, Huang YL (2012) An efficient image interpolation increasing payload in reversible data hiding. Expert Systems with Applications, Elsevier, vol: 39, pp: 6712-6719.
24. Geetha R, Geetha S (2018) Improved Reversible Data Embedding In Medical Images Using I-IWT and Pairwise Pixel Difference Expansion. Smart and Innovative Trends in NGCT 2017, CCIS 828, Springer Nature.pp 601-611
25. R. Geetha and S. Geetha, "Multilevel RDH scheme using image interpolation," *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Jaipur, 2016, pp. 1952-1956.
26. R. Geetha and S. Geetha, "Embedding Electronic Patient Information in Clinical Images: An Improved and Efficient Reversible Data Hiding Technique" Multimedia Tools and Applications -Springer Nature (Accepted for publication) DOI: 10.1007/s11042-019-08484-2

AUTHORS PROFILE

R. Geetha is an Assistant Professor in the Department of ECE, MVJ College of Engineering, Bangalore. India. She has received B.E. in Instrumentation and Engineering, and M.E. in Electronics from Madurai Kamaraj University, and Madras Institute of Technology, Chennai in 2000 and 2002 respectively. She is pursuing Ph.D. Degree from VIT university Chennai. She has more than 13 years of teaching and research experience. She has published 10 papers in reputed International Conferences and refereed Journals. Her research interests include multimedia security, intrusion detection systems, machine learning.

Dr. S. Geetha is a Professor and Associate Dean in School of Computing Science and Engineering, VIT University, Chennai campus, India. She has received the B.E., and M.E., degrees in computer Science and Engineering from Madurai Kamaraj University, India in 2000 and Anna University of Chennai, India in 2004, Ph.D. Degree from Anna University in 2011, respectively. She has more than 18 years of rich teaching and research experience. She has published more than 80 papers in reputed International Conferences and refereed Journals. Her research interests include steganography, steganalysis, multimedia security, intrusion detection systems, machine learning paradigms, and information forensics. She serves as a Life Member in HKCBEES, ISCA, IACSIT, and IAENG.