Mojette (d) Secret Image "SEDIH" in an Encrypted Double Image - A Histo Approach

Padmapriya Praveenkumar, Karuppuswamy Thenmozhi, John Bosco Balaguru Rayappan and Rengarajan Amirtharajan

(Corresponding author: Rengarajan Amirtharajan)

School of Electrical & Electronics Engineering, SASTRA University
Thanjavur-613 401, India
(Email: amir@ece.sastra.edu)

(Received Sept. 29, 2015; revised and accepted Dec. 7, 2015 & Jan. 15, 2016)

Abstract

In this paper, double image encryption technique has been considered to carry secret data using bit plane concept. The Mojette Transformed Huffman Encoded (MOTHE) secret logo image was hidden in the difference image generated by histogram approach formed from the double images. The MOTHE secret logo enhances authentication, security and compression of bits as compared with the traditional embedding algorithms. In this proposed security scheme, transformed secret sequences and reversible data hiding in an encrypted double image were employed to enhance the sternness of the security barrier. The number of bits embedded and it's PSNR (Peak Signal to Noise Ratio) for various images in 512 × 512 and 256 × 256 have been estimated using MATLAB and compared with the available literature.

Keywords: Bit-plane image encryption, histogram modification, Huffman encoding, Mojette transform, reversible data hiding

1 Introduction

Unlike traditional methods, digital era communication habitually consents one to determine one's own level of security. As per one of the many, the means of ensuring that the data is solely available to those who are at liberty to use it, that data can only be altered by those who are meant to do so with the ease of nominal and managerial measures is termed as information security will further classified as cryptography, watermarking, image encryption and steganography. Security attack is a doable concern which is addressed over and over, but even with unswerving endeavors there exist ambiguities in the security system. Of all, crackers and intruders pose a prime threat to secret communication. The information transmitted wireless is exposed to a lot of threats and hence security measures are mandatory.

Reversible data hiding scheme unlike steganography provides reconstruction of the cover and embedded secret data also. Reversible data hiding was introduced and implemented by Ni et al. in 2006 [10] to embed secret data in difference image by improving the PSNR and embedding capacity and they proposed a data hiding technique that's completely reversible and was based on the modification of the histogram. Kuo-Liang Chung et al. [1] introduced a watermark block based complement scheme to decrease the distortion in reversible data hiding. Steganalysis is done to identify the cover and embedded data. Der Chyuan et al. [2] proposed a Steganalysis scheme to identify the hidden data and cover image based on histogram feature coding approach that detects the presence of steganographic data. In recent years the authentication and security of the transformed encrypted images are very efficient when Mojette transform was utilized as it concentrates more on cryptography, watermarking and in compression [2, 3].

The innate relationship between the adjacent pixel information is used to attain the difference between pixels using sub-sampled images to form the resultant histogram are concentrated by Kyung-Su Kim et al. in 2009 [5]. Mohankumar and Shanmuganathan [8] proposes a data embedding technique utilizing high capacity and provides several security levels. Here, the cover image is used to hide and then the stego file is obscured in one more image. Survey on data hiding techniques and principles that uses reversible concept was presented by Masoud Nosrati et al. [12] in which data hiding techniques like Pair-Wise Logical Computation (PWLC) and data hiding by Template ranking with symmetrical Central pixels (DHTC) technique has been considered. Dual image encryption making use of Hill cipher to promote entropy was carried out by Panduranga et al. [14].

Reversible data hiding for encrypted images was carried out to improve security and authentication. An algorithm which includes compression, encryption and embedding and make use of reversible data hiding concept

and improves the PSNR value [15, 16]. Rajendra, Kanphade and Narawade [17] proposed a Forward Modified Histogram Shifting (FMHS) that has reduced the shifting of the pixels and yields high embedding capacity. Most of the factors with PSNR and embedding capacity included have been optimized in this proposed method. In 2012, Ramaswamy and Arumugam [18] projected a Data Hiding scheme that based on the shifting of histogram and completely lossless which accounts for over and under flow problems in pixel values and climbed that colour image embedding provides more embedding capacity as compared to gray scale images.

Raju, David and Rao [19] proposed an algorithm implementing histogram peak and zero points. It is grounded on the binary tree approach for multiple of peak points with histogram shifting for every overflow and underflow. In 2009, data hiding algorithm based on histogram approach utilizing difference of pixels, difference expansion and histogram shifting technique was proposed by Tai et al. [24]. Here, the distribution of pixel differences results not only on large embedding capacity but gives very low deformation. Further, this algorithm also prevents overflow and underflow problem.

Data hiding scheme that uses multi-dimensional and multi-level shifting of histogram has been proposed by Wang et al. [25]. Xinlu and Yang proposes a high capacity and adaptive embedding data hiding based on prediction-error has been considered [4]. A multilevel histogram modification scheme for embedding secret data was proposed by Zhao et al. [26] that modifies the histogram constructed based on the neighbour pixel differences instead of the host images histogram.

Mojette is the well known word of the city of Poitiers, France which means white beans. It was adopted as a standard tool for addition and subtraction computations by the children living there. Initial work on MOT was developed by IRCCyN laboratory, France in 1994. In 1995 the first work on MOT was published. The main aim of MOT is to determine the projections on the image. Radon transform serves as an application of discrete geometry and one best application and replica of it is MOT. It is characterized as specified for rational projection angles [20, 22]. Co generic to radon transform, MOT is also used to embody an image as a set of projections and every finite discrete projection has got its own inverse. It adopts major properties of radon transform and apart from those it has got a noticeable property of redundancy [7].

MOT projections can usefully be modified for the application of compressed sensing. This combination mainly has an outbreak in the reconstruction frame. Hence MOT along with compressed sensing produces effective outcomes of reduced radiation dosages without affecting the image quality. Watermarking the image on the whole only the projections are watermarked [6, 11].

David A. Huffman, in the year 1952, from MIT introduced the finest Huffman entropy coding. The main of his invention is to construct a code to provide minimum redundancy and to provide lossless compression of data. Huffman based text steganography was carried out by Satir and Isik, [21] to provide an increase in compression ratio besides the security features. Steganography methods can be classified as spatial domain [9] or transform domain [23] and few resist statistical steganalysis [13].

But majority of these schemes make use of histogram approach with either gray scale or colour images to improve the hiding capacity and PSNR. In this work, two grey scale images were formed by using bit plane concept using double image encryption. Here the histogram of the second image has been constructed based on the pixel difference from the first image. Then in the resultant image, MOTH secret logo has been embedded in the peak point to improve the embedding capacity and PSNR of the proposed scheme. This improves compression of secret data as compared with the traditional schemes. The PSNR and the number of bits embedded of the proposed algorithm were compared with the available literature and found to be better. In total, this study highlights the following;

1) Reversible data hiding;
2) Double image technique involving bit plane concept;
3) The Mojette Transformed Huffman Encoded (MOTHE) secret logo were hidden;
4) It provides high PSNR, embedding capacity and compression of bits as compared with the available literature;
5) Histogram approach formed from double images.

2 Preliminaries

2.1 Reversible Data Hiding

It is a technique, where secret data bits were embedded into a cover as traditional secret communication and includes the extraction of the secret data and the cover medium. The performance metrics can be analyzed using the complexity of the key involved, visual quality and the payload capacity.

2.2 Histogram Shifting

This method embeds the secret data in the cover media considering and analyzing the histogram of the image by shifting process.

2.3 Peak Point Embedding

This method finds either the peak or zero points in the histogram. Secret data hiding is carried out by shifting these peak or zero points resulting in maximum payload capacity with minimal distortion. It avoids overflow (pixel value going beyond 255) and underflow (Pixel value below 0) problems.

3 Proposed Methodology

In the proposed scheme, double image encryption has been concentrated, in which two 512 × 512 grey scale images were used to form a single image using bit plane concept. Then based on the pixel difference from the first image, the histogram of the second image was formed. To the resulting image, MOTH secret logo has been embedded in the peak point to improve the embedding capacity and PSNR. The proposed reversible data hiding encryption and decryption schemes are given in Figures 1 and 2 respectively.

3.1 Encryption Algorithm

1) Get the input cover images C1 & C2.
2) Separate C1 & C2 into its corresponding bit planes.
3) Replace the LSB bit planes of C2 with LSB bit planes of C1 and store it as A1.
4) Replace the LSB bit planes of C1 with LSB bit planes of C2.
5) Read the image matrix A1 and A2.
6) Resize A1 & A2 to 512 × 512 (P × Q), where P, Q represents the size of A1 & A2.
7) Convert A1 & A2 to double values.
8) Compute histogram to image matrix A1 & A2.
9) Divide the image into 4 × 4 blocks.
10) Compute the difference between adjacent columns.

$$\begin{aligned} A1(i,j) &= |A(i,j) - A(i,j+1)|; \\ &\quad 0 \leqslant i \leqslant P, 0 \leqslant j \leqslant Q-2. \\ A2(i,j) &= |B(i,j) - B(i,j+1)|; \\ &\quad 0 \leqslant i \leqslant P, 0 \leqslant j \leqslant Q-2, \end{aligned}$$

where A1 & A2 are the difference block of size $P \times Q - 1(4 \times 3)$. A, B are the 4 × 4 image block of A1 & A2. i, j are the rows and columns of Z.

11) Compute the difference between resultant image A1 & A2.

$$Z(i,j) = A1 - A2;$$

12) Compute the histogram of Z (i, j).
13) Record the peak point p in the histogram of Z (i,j), where V represents the peak point that has larger no of pixel values.
14) If Z(i, j) greater than peak point then Z'(i, j)= Z(i, j)+1.

$$Z'(i,j) = \begin{Bmatrix} Z(i,j)+1) & if\ Z(i,j) > V \\ Z(i,j) & otherwise \end{Bmatrix}$$

For $0 \leqslant i \leqslant P$, $0 \leqslant j \leqslant Q-2$, where Z'(i, j) = difference image.

15) The principle Z'(i, j) is applied for each image blocks.
16) If the pixel value is equal to V can be modified to hide U, where U represents the secret data bits.
17) Then the condition for hiding message in each block is given by,

$$Z''(i,j) = \begin{Bmatrix} Z'(i,j)+U) & if\ Z'(i,j) = V \\ Z'(i,j) & otherwise \end{Bmatrix}$$

For 0 ⩽ i⩽ P, 0⩽ j⩽ Q-2, where Z"(i, j) is the modified hidden difference image, U represents the secret data bits.

18) Performing inverse transformation J^{-1} to each 4×3 block of difference image and construct marked image.

$$W(i,1) = \begin{Bmatrix} A(i,2) + Z''(i,2) & if\ A(i,1) > A(i,2) \\ A(i,1) & otherwise \end{Bmatrix}$$

For 0 ⩽ i⩽ P, 0⩽ j⩽ Q-2.

$$W(i,2) = \begin{Bmatrix} A(i,1) + Z''(i,1) & if\ A(i,1) \leqslant A(i,2) \\ A(i,2) & otherwise \end{Bmatrix}$$

For 0 ⩽ i⩽ P, 0⩽ j⩽ Q-2.

3.2 Mojette Transform (MOT)

The main property of MOT is only additions, subtractions and apparently the initial discrete information can be distributed into multiple projections. Reconstruction of initial information can also be performed when ample projections are available. The main objective is to derive certain inconsistent set of information from projections to avoid rotation attacks. This serves to be a useful cryptographic scheme. The linearity property of the transform is much helpful in decoding the cryptic image where it takes modulus addition of pixels.

The MOT projects the original image block as,

$$A = A(b,c); \quad b = 1...D; \quad c = 1...E$$

On a set of projections

$$E = \{E_g(h) \quad g = 1, ...g \quad h = h...h_g\}$$

It's a version DRT for a group

$$E_g(h) = projection \quad (J_f, K_f, l_f)$$

where J_f and KJ_f are the projection lines.

$$E_g(h) = \sum^{b,c\sum H} A(b,c) \quad \partial(b_l - iq_k - jp_k)$$

where,

$$\partial(a) = \begin{Bmatrix} 1 & if \quad a = 0 \\ 0 & otherwise \end{Bmatrix}$$

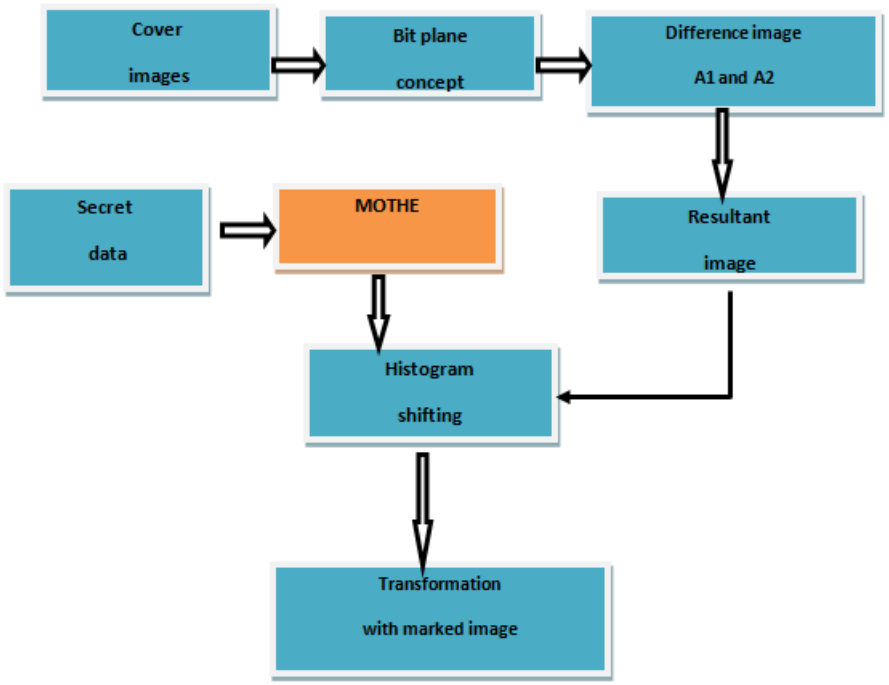

Figure 1: Encryption scheme

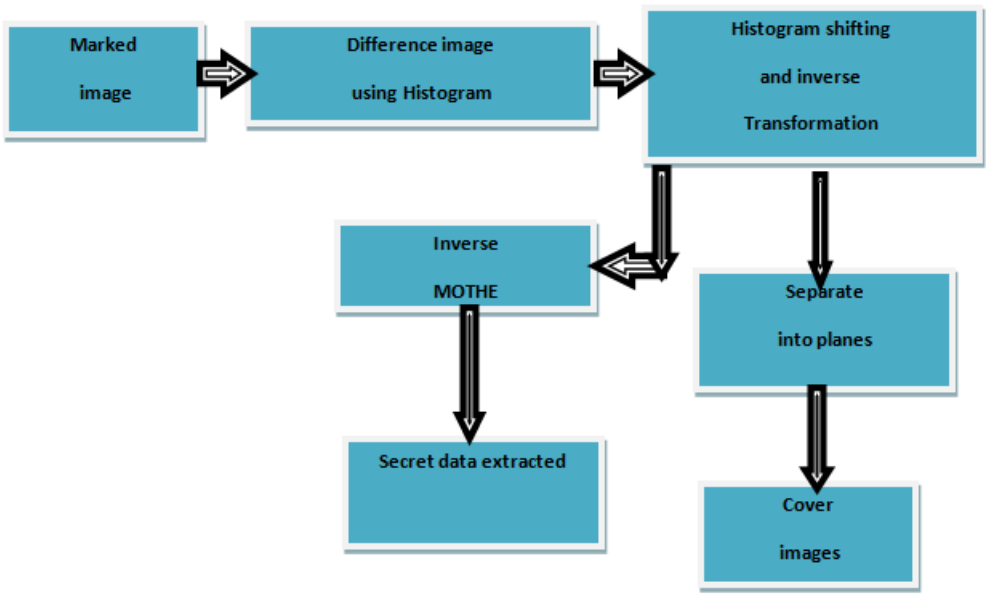

Figure 2: Decryption scheme

$$H = (b, c; \quad l_h - bk_f - cj_f = 0)$$

H represents the digital bin in ϕ_f direction and on l_h Then the total number of bins will be calculated by

$$y_b = (D-1)\,|J_f| + (E-1)\,|K_f| + 1$$

The projection angles are given by θ_i=$\tan^{-1}(j_a/i_a)$, where the set of vectors (j_a/i_a) should be co-prime and ia should always be positive except for a single case of (1,0). The transformed image will have a set of projections of which every element is termed as bins. These bins are obtained by addition of pixels along the line of projection. In order to recover the image an iterative process of search and update of one-one pixel-bin is performed. Back-projection of this bin value onto the pixel and consequent subtraction in other respective projections will be done. Then the pixel values from the projection bins are chosen and the unwanted bins are discarded during reconstruction. This reduces redundancy of the projection bins.

3.3 Secret Logo Embedding

1) Read the image matrix S.
2) LSB bit-planes of S are combined as N (512 × 512 image).
3) Difference between the adjacent pixel values was taken.
4) Read the difference image as M.
5) M is subjected to Mojette Transform, followed by Huffman encoding.
6) As an example, consider a 3×3 matrix from the secret data to be embedded as in Table 1.

Table 1: 3 × 3 Secret data

4	6	1
2	2	0
3	5	8

7) Calculate the bin values as in Figure 3.
8) For retrieval of the original data at the receiver end, bins 1, 5, 6,7, 8, 9, 10, 11 and 13 are required.
9) Among 13 bin values estimated, only 9 bins are used neglecting the 4 bin values.
10) For the 9 bin values (3, 1, 4, 8, 6, 5, 8, 9, 9), calculate the mean value and the mean value is found to be 6.
11) Then from the calculated mean value, find the difference between the mean and the bin values, calculated value= mean value − bin value.
12) The calculated values are -3, -5, -2, 2, 0, -1, 2, 3, 3.

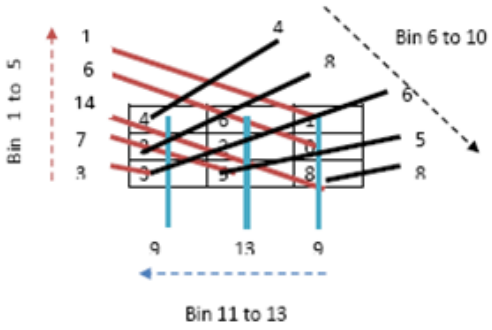

Figure 3: Bin values calculation

Table 2: Bin values and their estimated probability values

Calculated bin values	Probability
-3	0.5
-5	0.05
-2	0.05
2	0.125
0	0.05
-1	0.05
2	0.125
3	0.25
3	0.25

13) To provide compression, Huffman encoding was applied to the calculated values.
14) Distribute the probability for the calculated values as in Table 2.
15) The Calculated bin values are encoded using Huffman encoding procedure as shown in Figure 4.
16) The encoded bits are 11100001000011011111111100011001.
17) Totally 32 bits are encoded.
18) For a 3 × 3 matrix, normally 9 × 8=72 bits will be transmitted; instead it has been reduced to 32 bits by applying MOHTE.

3.4 Decoding of the Secret Data Bits

1) From the transmitted sequence, the calculated values are obtained using Huffman tree.
2) The calculated values are -3, -5, -2, 2, 0, -1, 2, 3, 3.
3) Then to the calculated value mean will be added to determine the original bin values. Calculated value + Mean value = Original bin value.
4) Then the original bin values are recovered as 3, 1, 4, 8, 6, 5, 8, 9, 9.

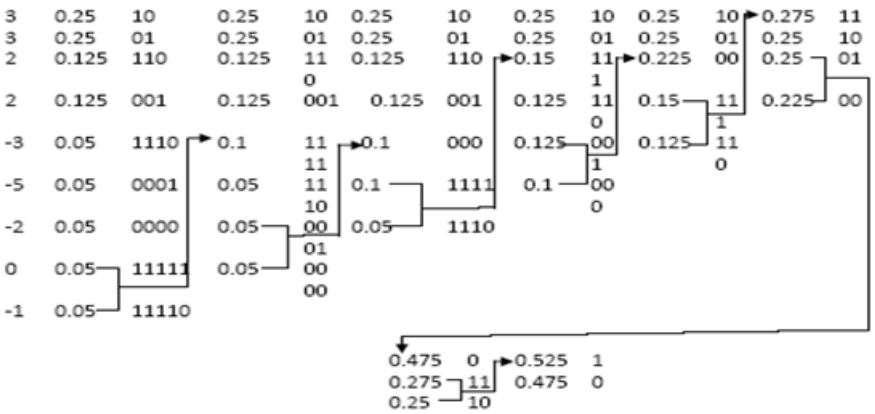

Figure 4: Bin value calculation using Huffman encoding procedure

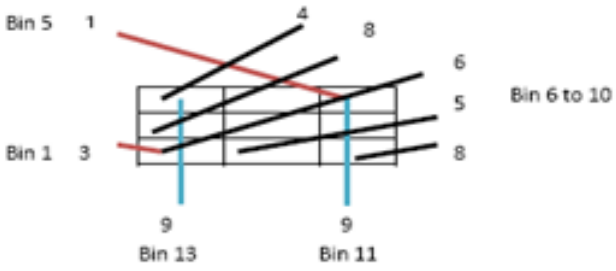

Figure 5: Arrangement of bin values

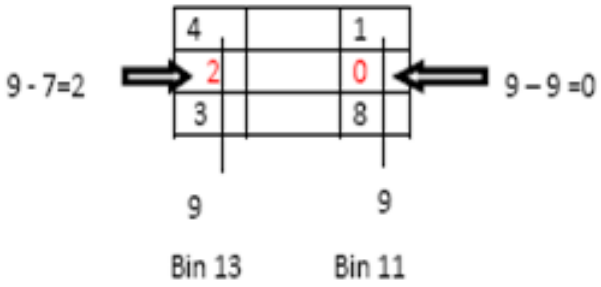

Figure 6: Bin values estimation

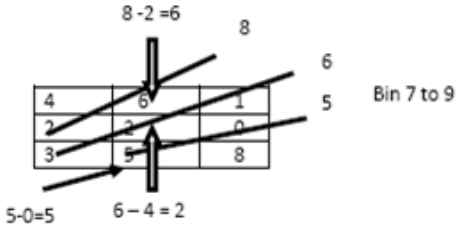

Figure 7: Secret matrix formation

5) Then arrange the original bin values in respective positions to extract the matrix values as shown in Figure 5.

6) Using the bin values 1, 5, 6 and 10 the corner value of the matrix was obtained.

7) Then using the bin values 13, 11 and using Step 19, next two matrix elements are calculated as shown in Figure 6.

8) By using the bin values, 7, 8 and 9 the remaining matrix elements was obtained as shown in Figure 7.

9) Thus the original secret 3 *times* 3 matrix was reconstructed.

3.5 Decryption

Perform the inverse operation of encryption to extract the cover images 1 and 2 and the secret data bits.

3.6 Secret Logo Image to be Embedded

Secret logo image to be embedded is given in Figure 8. From Table 4 it is clear that, for a 256 × 256, the original data to be embedded will be 65, 536 bits and after applying Mojette Transform (MOT) it will be reduced to 10, 752 and still reduced to 3392 bits after applying

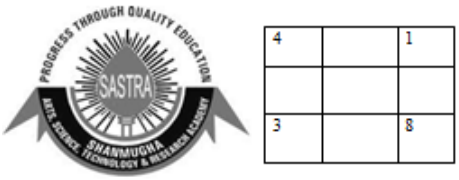

Figure 8: Secret logo to be embedded after applying MOTH

Mojette Transform Huffman encoding (MOTH). Then for 512×512 image, the original data to be embedded will be 262144 bits and after applying Mojette Transform (MOT) it will be reduced to 21, 504 and still reduced to 6784 bits after applying MOTH.

Table 3: Comparison of Mojette transform with traditional embedding

Secret logo	Bits to be embedded		
	Without MOHTE	With MOT	With MOTHE
256× 256	65,536	10,752	3392
512×512	2,62,144	21,504	6784

4 Results and Discussion

The proposed algorithm was based on the bit plane based reversible data hiding on double images. Figure 8 shows the secret logo to be embedded after applying MOTH. Here two cover images of camera man and moon are taken as input as shown in Figure 9a and Figure 9b. Difference images of 9(a) and 9(b) are given in Figure 10a and b respectively. Then the difference image between 10a and b was computed and the resultant image and its histogram were shown in Figure 11a & Figure 11b respectively. Figure 12a represents the secret data bits embedded in 11(a) and its corresponding histogram in Figure 12b.The marked image was given in Figure 13a and its histogram in Figure 13b using inverse transformation and then Gaussian noise with zero mean and 0.02 variance is added to the marked image and was given in Figure 14a and its histogram in Figure 14b.The decrypted image was found to be robust even after adding noise.

Figure 15a provides the decrypted image after adding Gaussian noise and its histogram in Figure 15b.

From Figure 15a it is revealed that even after adding noise decryption is possible. Figure 16a, b, c, d and e provides the difference image, marked image, marked image with Gaussian noise, final decrypted cover image 1 and the final decrypted cover image 2 respectively. Figure 17 a, b, c, d and e provides the Lena image formed from bit-planes of double image, its difference image, marked image, marked image with Gaussian noise, final decrypted

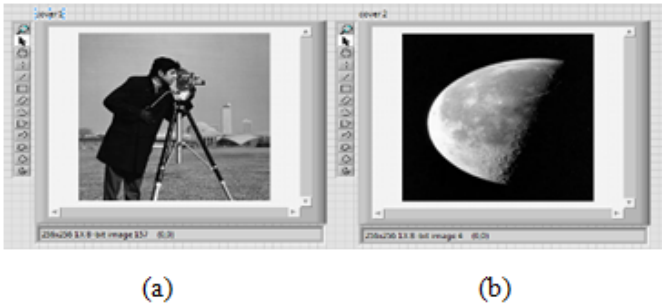

Figure 9: a) Cover image C1; b) Cover image C2

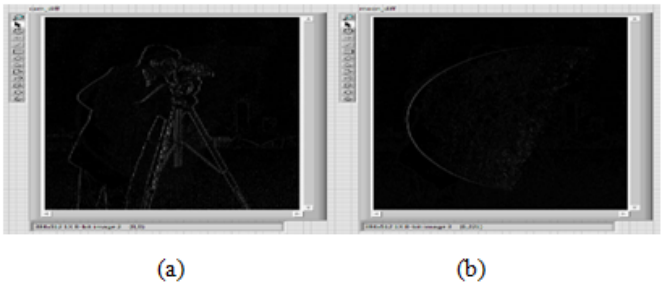

Figure 10: a) Difference image of 9(a); b) Difference image of 9(b)

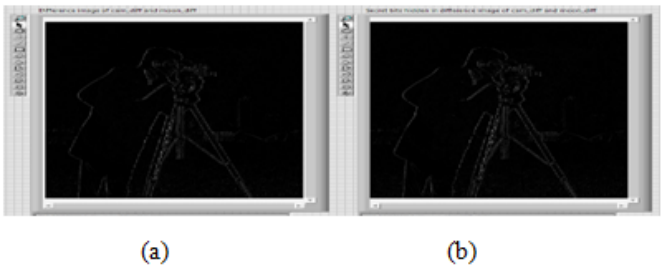

Figure 11: a) Difference image of 10(a & b); b) Secret data bits hidden in 11(a)

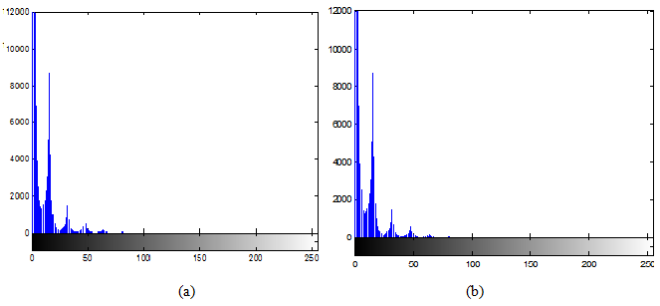

Figure 12: a) Histogram of 11(a); b) Histogram of 11(b)

Table 4: Performance metrics for various images of size 512 × 512

Images (512 × 512)	Number of pixels embedded	PSNR
Boat	49297	48,816
Barbara	36919	48.8380
Jet	51233	48.7596
Pout	57514	49.5636
Lena	50580	48.8000
Cell	60141	49.7397
Cameraman	51801	48.9513
Baboon	38091	48.4060
Average PSNR		49.06 dB

Table 5: Comparative analysis of PSNR in dB

Host image	Xinlu, Li and Yang.(2013)	Ratna Raju et al., (2010)	Ramaswamy et al., (2012)	Proposed
Lena	42.71	44.28	37.79	48.8
Jet	46.03	44.02	36.24	48.75
Boat	37.81	44.01	39.67	48.8
Baboon	2.01	44.19	36.24	48.4

Table 6: Comparison of payload characteristics I

Host image	Payload (bpp) (Ni et al., 2006)	Proposed	Increased payload (in percentage)
Lena	5460	50580	826
Boat	7301	51233	601
Baboon	5421	38091	603
Average	6060	46634	669

Table 7: Comparison of payload characteristics I

Host image	Payload (bpp) (Ratna Raju, David and Prasada Rao, 2010.)	Proposed	Increased payload (in %)
Lena	22390	50580	125.90
Baboon	25530	38091	49.200
Average	23960	44335	85.03

Figure 13: a) Marked image; b) Marked image with Gaussian noise of zero mean and 0.02 variance

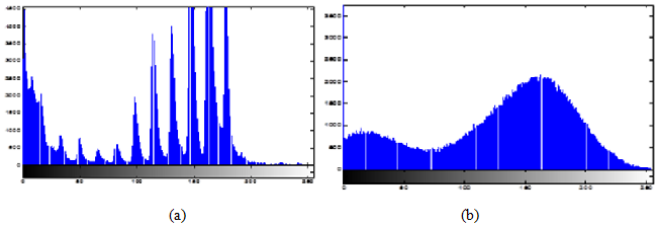

Figure 14: a) Histogram of 13(a); b) Histogram of 13(b)

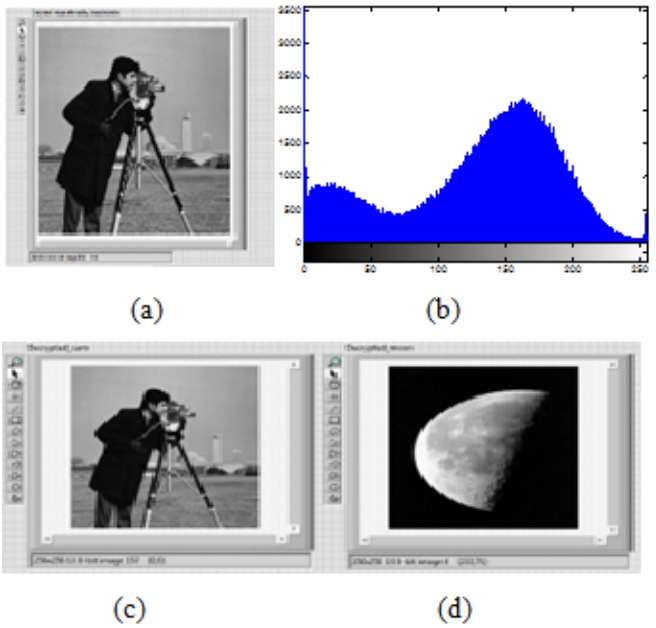

Figure 15: a) Decrypted cover image 1 affected by Gaussian noise; b) Histogram of 15(a); c), d) Decrypted cover images 1 and 2

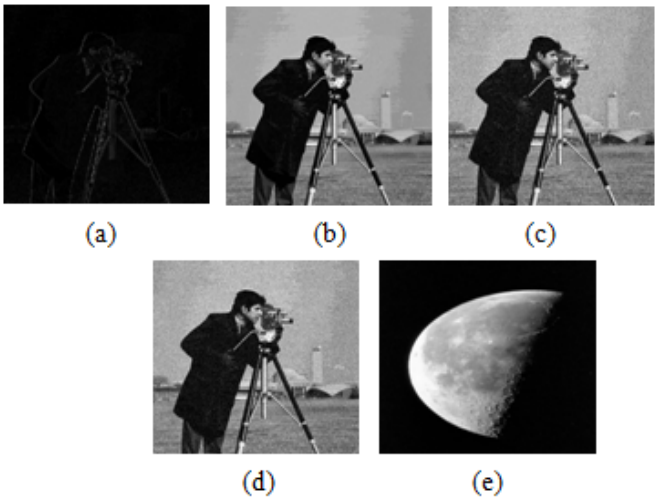

Figure 16: a) Difference image; b) Marked image; c) Marked image with Gaussian noise; d) Decrypted cover image 1; e) Decrypted cover image

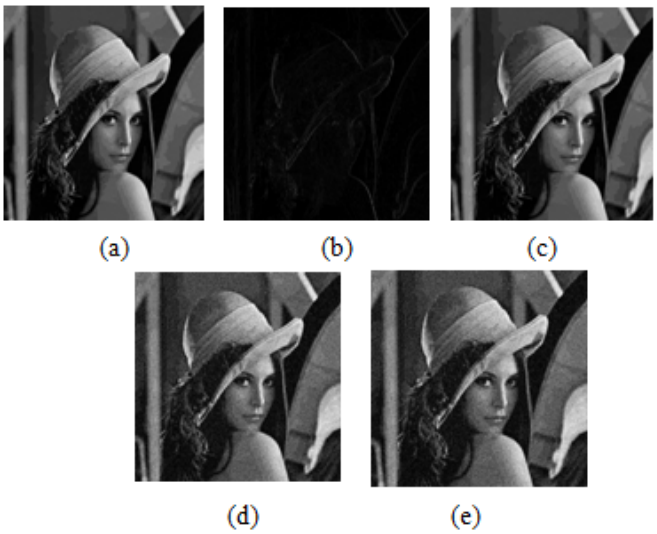

Figure 17: a) Original biplane hidden image; b) Secret bits embedded in 17 (a); c) Marked image; d) Marked image with Gaussian noise; e) Decrypted cover image 1

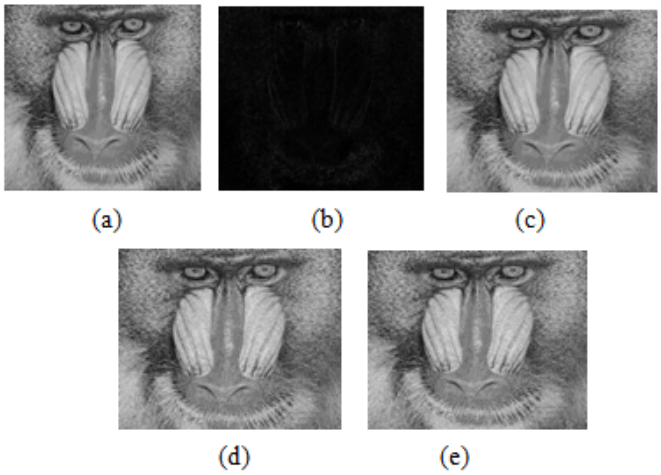

Figure 18: a) Original biplane hidden image; b) Secret bits embedded in 18(a); c) Marked image; d) Marked image with Gaussian noise; e) Decrypted cover image 1

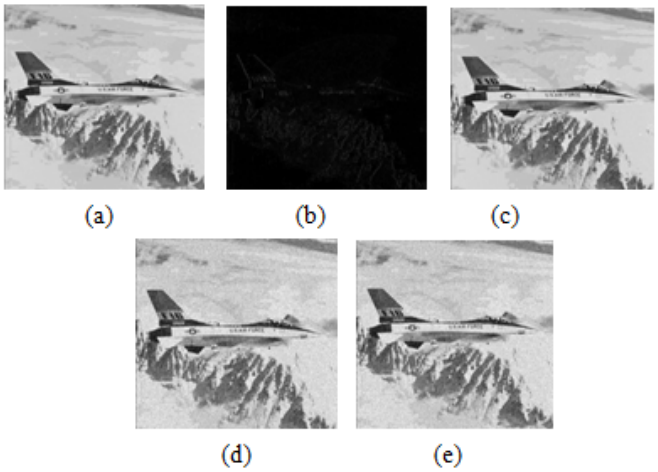

Figure 19: a) Original biplane hidden image; b) Secret bits embedded in 19(a); c) Marked image; d) Marked image with Gaussian noise; e) Decrypted cover image 1

cover image 1 respectively.

Figure 18 a, b, c, d and e provides the Baboon image formed from bit-planes of double image, its difference image, marked image, marked image with Gaussian noise, final decrypted cover image 1 respectively. Figure 19 a, b, c, d and e provides the plain image formed from bit-planes of double image, its difference image, marked image, marked image with Gaussian noise, final decrypted cover image 1 respectively. For all the test images considered, moon image was considered to be the second cover image. Figure 20 a, b and c represents the decrypted image after applying gaussian, pepper-Salt and median noise attacks respectively. Figure 21 a and b represents decrypted image after cropping and rotation attacks respectively Table 5 provides the information about the number of bits embedded and its PSNR for various images in 512 × 512 format. Table 6 estimates the PSNR

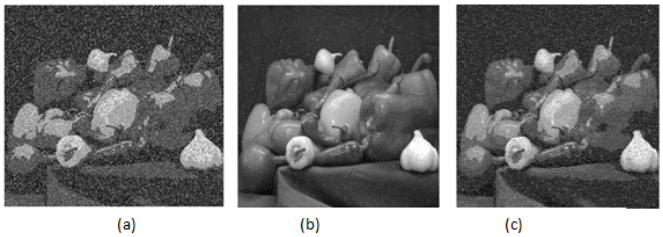

Figure 20: Decrypted image after a) Gaussian filtering attack; b) pepper-salt noise attack; c) median filtering

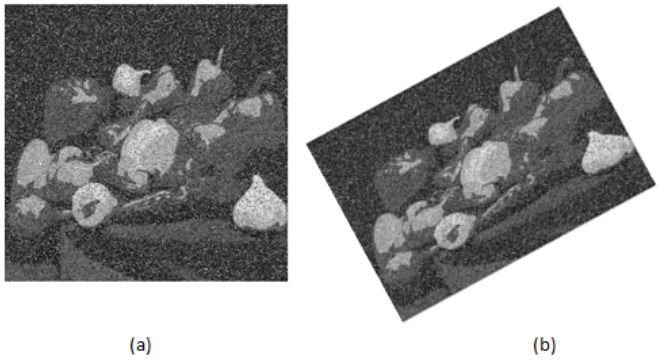

Figure 21: Decrypted image after a) cropping and b) rotation

of the proposed scheme with the available literature and found to be better. Table 7 and 8 provides the comparison of payload characteristics considering various images like Lena, Boat and Baboon in comparison with (Ni et al., 2006 and Ratna Raju, David and Prasada Rao. 2010) respectively.

5 Performance Analysis

5.1 PSNR & MSE

PSNR is a measure to validate the image quality after embedding. It is given by

$$PSNR = 10 \times log_{10} \frac{I^2}{MSE}$$

$$MSE = \frac{1}{MN} \sum_{i=1}^{M-1} \sum_{j=1}^{N-1} [I()i,j) - K(i,j))]^2$$

where M and N represents the row and column of the image matrix and I take the value 255.The average PSNR value of proposed method is found to be 49.06dB which is superior when compared to (Ramaswamy and Arumugam. 2012; David and Prasada Rao. 2010 and Xinlu, Li and Yang. 2013).

5.2 Embedding Capacity

Embedding capacity provides the hiding capacity of the algorithm. The embedding capacity depends on the pixel

values at the peak point Embedding capacity = number of pixels at peak point of difference image. The estimated values of the proposed method are found to be better with the previous work in payload (Ni et al., 2006 and Ratna Raju, David and Prasada Rao. 2010).

6 Compression Achieved through MOHT

The secret logo to embed was passed through MOHTE. For a 4×4 image, the number of bins will be 21 by applying MOT. Then each bit will be represented by 8 bits, so totally 21×8=168 bits are required for embedding. But out of the 21 bins, 16 bins are sufficient to retrieve the original 4×4 image. So it will be reduced to 16×8=128 bits results in the removal of 40 redundant bits.

Then to this 16 bin values, Huffman encoding has been applied to remove redundant bits. The resultant bits after MOTH will be 53 bits. Thus an increase in the compression of 31 percentage will be provided.

So, for a 256×256 image, there will be hardly 64 numbers of 4×4 blocks will be there. So the required bits are 64×53 bits = 3392 bits. Similarly for a 512×512 image, there will be hardly 128 numbers of 4×4 blocks will be there. So the required bits are 128×53 bits = 6784 bits.

7 Conclusions

In this paper, bit planes of the double images have been formed, and then difference image was computed based on histogram approach from the double images. Then MOHT secret logo image was hidden in the difference image to improve the hiding capacity in spatial domain. This embedding provides compression, authentication and security as compared with the traditional embedding schemes. The proposed methodology employs grey scale images and implemented using MATLAB. The results demonstrate that embedding capacity of 60141 bits and PSNR of 49 dB and 48dB has been achieved considering 512×512 and 256×256 images respectively. It can be further improved by adding Quantum based QR codes for authentication purposes.

References

[1] K. L. Chung, Y. H. Huang, W. M. Yan and W. C. Teng, "Distortion reduction for histogram modification-based reversible data hiding," *Applied Mathematics and Computation,* vol. 218, no. 9, pp. 5819–5826, 2012.

[2] D. Chyuan, C. H. Hu and C. C. Chiu, "Steganalysis of histogram modification reversible data hiding scheme by histogram feature coding," *International Journal of Innovative Computing Information and Control,* vol. 7, pp. 6571–6583, 2011.

[3] J. P. Guedon and N. Normand, "Mojette transform: Applications for image analysis and coding," *Visual Communications and Image Processing,* vol. 3024, pp. 873–884, 2007.

[4] X. Gui, X. Li and B. Yang, "A high capacity reversible data hiding scheme based on generalized prediction-error expansion and adaptive embedding," *Signal Processing,* vol. 98, pp. 370–380, 2013.

[5] K. S. Kim, M. J. Lee, H. Y. Lee and H. K. Lee, "Reversible data hiding exploiting spatial correlation between sub-sampled images," *Pattern Recognition,* vol. 42, no. 11, pp. 3083–3096, 2009.

[6] A. Kingston and F. Autrusseau, "Lossless image compression via predictive coding of discrete Radon projections" *Signal Processing: Image Communication,* vol. 23, pp. 313–324, 2008.

[7] C. Liu and J. Guédon, "Finding all solutions of three-material image reconstruction problem," *Journal of South China University of Technology*, vol. 41, no. 7, pp. 114–119, 2013.

[8] P. Mohan Kumar and K. L. Shunmuganathan, "A reversible high embedding capacity data hiding technique for hiding secret data in images," *International Journal of Computer Science and Information Security,* vol. 7, pp. 109–115, 2010.

[9] S. Maria Celestin Vigila and K. Muneeswaran, "Hiding of confidential data in spatial domain images using image interpolation," *International Journal of Network Security,* vol. 17, pp. 722–727, 2015.

[10] Z. Ni, Y. Q. Shi, N. Ansari and W. Su, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 16, no. 3, pp. 354–362, 2006.

[11] N. Normand, A. Kingston and P. Évenou, "A geometry driven reconstruction algorithm for the mojette transform," in *Discrete Geometry for Computer Imagery,* LNCS 4245, pp. 122–133, Springer, 2006.

[12] M. Nosrati, R. Karimi and M. Hariri, "Reversible data hiding: Principles, techniques, and recent studies," *World Applied Programming,* vol. 2, no. 5, pp. 349–353, 2012.

[13] A. Nag, S. Biswas, D. Sarkar and P. P. Sarkar, "Semi random position based steganography for resisting statistical steganalysis," *International Journal of Network Security,* vol. 17 pp. 57–65, 2015.

[14] H. T. Panduranga, H. S. Sharath Kumar and S. K. Naveen Kumar, "Hybrid approach for dual image encryption using nibble exchange and Hill-cipher," in *IEEE International Conference on Machine Vision and Image Processing,* pp. 101–104, 2012.

[15] L. Y. Por, D. Beh, T. F. Ang and S. Y. Ong, "An enhanced mechanism for image steganography using sequential colour cycle Algorithm," *International Arab Journal of Information Technology,* vol. 10, pp. 51–60, 2013.

[16] W. Puech, M. Chaumont and O. Strauss, "A reversible data hiding method for encrypted images," in *Processing of SPIE, Electronic Imaging, Security,*

Forensics, Steganography, and Watermarking of Multimedia, pp. 1–9, 2008.

[17] D. Rajendra, D. Kanphade and N. S. Narawade, "Forward modified histogram shifting based reversible watermarking with reduced pixel shifting and high embedding capacity," *International Journal of Electronics and Communication Engineering,* vol. 5, pp. 185–191, 2012.

[18] R. Ramaswamy and V. Arumugam, "Lossless data hiding based on histogram modification," *International Arab Journal of Information Technology,* vol. 9, no. 5, pp. 445–451, 2012.

[19] P. D. Ratna Raju, B. A. David and K. Prasada Rao, "Binary tree approach for data hiding based on histogram modification," *International Journal of Computer Applications,* vol. 5, pp. 21–24, 2010.

[20] B. Recur, H. Der Sarkissian, M. Servires, N. Normand and J. Guédon, "Validation of Mojette reconstruction from Radon acquisitions," in *IEEE International Conference on Image Processing,* pp. 1041–1045, 2013.

[21] E. Satir and H. A. Isik, "Huffman compression based text steganography method," *Multimedia Tools and Applications,* vol. 70, no. 3, pp. 2085–2110, 2014.

[22] I. Svalbe, A. Kingston, J. Guédon, N. Normand and S. Chandra, "Direct inversion of Mojette projections," in *IEEE International Conference on Image Processing,* pp. 1036–1040, 2013.

[23] S. A. Seyyedi, V. Sadau and N. Ivanov, "A secure steganography method based on integer lifting wavelet transform," *International Journal of Network Security,* vol. 18, pp. 124–132, 2016.

[24] W. L. Tai, C. M. Yeh and C. C. Chang, "Reversible data hiding based on histogram modification of pixel differences," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 19, pp. 906–910, 2009.

[25] Z. H. Wang, C. C. Chang, M. L. Li and Y. S. Cui, "Multi-dimensional and multi-level histogram-shifting-imitated reversible data hiding scheme," *Advances in Intelligent Systems and Applications,* vol. 21, pp. 149–158, 2013.

[26] Z. Zhao, H. Luo, Z. M. Lu and J. S Pan, "Reversible data hiding based on multilevel histogram modification and sequential recovery," *AEU-International Journal of Electronics and Communications,* vol. 65, no. 10, pp. 814–826, 2011.

Padmapriya Praveenkumar received her B.E (ECE) from Angala Amman college of Engineering and Technology and M.E (Communication system) from Jayaram college of Engineering and Technology. Currently she is working as an Assistant Professor III in the Department of ECE in SASTRA University, Thanjavur. She has a teaching experience of 13 years and she has published 26 Research articles in National & International journals. She is currently working towards her Ph.D. Degree in SASTRA University. Her research area includes Wireless communication and Steganography

K. Thenmozhi received her B.E (ECE) and M.E (Communication system) degrees from Regional Engineering college (NIT) Tiruchirappalli and Ph.D. from SASTRA University, Thanjavur. Currently she is working as an Associate Dean in the Department of ECE in SASTRA University, Thanjavur. She has a teaching experience of 20 years. Her current research area includes Wireless communication, Steganography and Information Theory and Coding. She has supervised more than 100 UG projects, 10 Master Students and Supervising 4 Ph.D. Scholars. So far she has published 53 Research articles in National & International journals@conferences. She received EDI award from broadcast Engineering Society for the year 2007.

John Bosco Balaguru Rayappan was born in Trichy, Tamil Nadu province, India in 1974. He received the B.Sc., M.Sc. and M.Phil. Degree in Physics from St. Joseph College, Bharathidasan University, Trichy and Ph.D. in Physics from Bharathidasan University, Trichy, Tamil Nadu India in 1994, 1996, 1998 and 2003, respectively. He joined the faculty of SASTRA University, Thanjavur, India in Dec 2003 and is now working as Professor & Associate Dean Research School of Electrical and Electronics Engineering at SASTRA University, Thanjavur, Tamil Nadu, India. His research interests include Lattice Dynamics, Nanosensors, Embedded System and Steganography. So far he has published 161+ Research articles in National and International journals and 14 conference papers. He has Supervised 25 Master Students and Supervising 5 Ph.D. Scholars. Currently he is working on four funded projects in the fields of Nanosensors and Steganography supported by DST and DRDO, Government of India, New Delhi. Indo-Swedish collaboration work.

R. Amirtharajan was born in Thanjavur, Tamil Nadu province India, in 1975. He received B.E. degree in Electronics and Communication Engineering from P.S.G. College of Technology, Bharathiyar University, Coimbatore, India in 1997. M.Tech. and Ph. D. from SASTRA University Thanjavur, India in 2007 and 2012 respectively. He joined SASTRA University, Thanjavur, Tamil Nadu, India (Previously Shanmugha College of Engineering) as a Lecturer in the Department of Electronics and Communication Engineering since 1997 and is now Associate Professor, His research interests include Image Processing, Information Hiding, Computer Communication and Network Security. So far, he filed one international patent; he has published more than 116+ research articles in national and international journals and 22 IEEE conference papers with 4 Best Paper Awards. He also holds the Certificate of Appreciation from IBM in 2009 for Great Mind Challenge, Mentor IBM Academic Initiative Program. Recently, he received the Founder Chancellor Award for the best Ph.D. thesis for 2013 from SASTRA University and he received the

SASTRA Anukul Puraskar for Higher Involvement in Research and Education Award for 2011-2012 and 2013-2014. He serves as a Life Member in CRSI, SSI, IAENG, and IACSIT. He also served as the TPC Member and Review Member for more than 30+ IEEE and Springer supported international conferences apart from more than 10 peer reviewed journals. He had been working on funded project in the field of steganography supported by DRDO, Government of India, New Delhi, India.