ICIC Express Letters
Volume **15**, Number **8**, August **2021**

 ISSN 1881-803X
pp. **819–827**

HIGH CAPACITY INFORMATION HIDING USING ENHANCED DIFFERENCE EXPANSION TECHNIQUE

Shreela Dash[1], Madhabananda Das[1] and Dayal Kumar Behera[2]

[1]School of Computer Science and Engineering
Kalinga Institute of Industrial Technology, Deemed to be University
Patia, Bhubaneswar, Odisha 751024, India
shreelamamadash@gmail.com; mndas_prof@kiit.ac.in

[2]Department of Computer Science and Engineering
Silicon Institute of Technology
Silicon Hills, Near DLF Cybercity, Patia, Bhubaneswar, Odisha 751024, India

Received November 2020; accepted February 2021

Abstract. *This paper focuses on a robust technique for information hiding based on enhanced differential expansion. To generate more capacity for embedding, the proposed work not only considers the positive difference, but also gives equal importance to the negative difference. In the suggested work, cover image is divided into $n \times n$ block size in raster scan order and the reference pixel is selected as one pixel from the block. The differential value is then determined for each pixel of the block with respect to the reference pixel. The method does not utilize all the pixels in the embedding process. The calculated distances within the range of -3 to $+3$ are used to embed 2 bits of secret data at a time in each pixel. There will be more distortion after direct embedding of the produced stego image. The generated value of each stego pixel is reduced by using logarithmic function to minimize the deformation. The review of the findings reveals a contrast between the proposed method and the various current procedures in the same space in terms of both embedding capability and distortion. The suggested work shows greater capacity with improved peak signal to noise ratio (PSNR).*

Keywords: Information hiding, Enhanced difference expansion, Embedding capacity, PSNR

1. **Introduction.** Information security is a major requirement for transfer of secret information worldwide after the broad use of Internet. During transmission of the secret message unethical users may easily hack, intercept and retrieve the secret information or modify the message. To protect the critical information two most commonly used techniques are cryptography and steganography [1]. The intruder cannot speculate about the covert communication in steganography because the output image is visibly the same as the original image [2]. The digital information hiding can be performed either using spatial domain or transformation domain techniques. Direct interaction and modification occur in the spatial domain and the covert message is hidden in the pixel directly. Several approaches in spatial domain approach have been implemented in [3-6]. The confidential data using frequency components of cover image occurs in transform domain [7-9]. The embedding capability of the spatial domain is increased with elevated PSNR, but more data robustness and security are achieved in the frequency domain [10]. The proposed work is based on spatial domain principle as it gives emphasis to the high payload. The major contributions of the research work are mentioned below.

1) To enhance the embedding capacity with lower distortion more number of secret bits is embedded in each pixel of the block.

DOI: 10.24507/icicel.15.08.819

2) Earlier work focused on smooth region and adjacent two pixels whereas in the proposed work we have used block based embedding and pixels with difference range -3 to $+3$ are chosen for embedding.

3) To minimize the change in cover pixel after embedding, the logarithmic function is used which results in less distortion.

Section 2 addresses similar works in the spatial domain of steganography. The proposed work framework is specified in Section 3. Performance of the proposed work by analyzing and comparing with the existing techniques is specified in Section 4. Section 5 presents the conclusion of the proposed method along with future direction.

2. **Related Work.** This section specifies a broad overview of data hiding strategies focused on the expansion of pixel differences. The earliest reference to image steganography based on difference expansion (DE) is found in [11]. Author suggested that it is the most generic approach of reversible data hiding where the payload along with the original values is stored in the cover image. It provides very less embedding capacity and less PSNR. Alattar [12] suggested another calculation to provide greater embedding capacity by expanding Tian's calculation using vector generalized difference expansion (GDE) to construct the method's concealing capacity and calculation skills. However, for each selected pixel, this approach also hides a maximum of 1 bit. Lee et al. described a scheme using centralized difference expansion [13]. Here the cover image of size $p \times q$ is partitioned into blocks with pixels $\{v_0, v_1, v_2, v_3, \ldots, v_{k-1}\}$. Then the median pixel v_m is calculated and the difference between each pixel with median pixel is calculated. The difference is stored in a vector $\{d_0, d_1, d_2, \ldots, d_{k-1}\}$. The blocks are categorized into 4 types depending on the maximum difference value of each block. The classification of each block determines the capacity of embedding. Although the method results in enhancement of capacity, PSNR remains low. Abdullah and Manaf suggested an approach where the secret data is hidden in only smooth region, i.e., the pixel is chosen for embedding if the difference between the adjacent pixels is 1 or 0 and ignores other pixel during embedding process [14].

A block based steganography technique with reduced difference expansion is proposed in [15]. Here the image of size $M \times N$ is divided into blocks of size 2×2 $(u0, u1, u2, u3)$. The last pixel of the block is chosen as the reference pixel. The calculated difference is reduced before embedding as per Equation (1).

$$d'_n = \begin{cases} d_n - \left(2^{\lfloor \log_2 d_n \rfloor}\right) + 2\left(\lfloor \log_2 d_n \rfloor\right) d_n > 1 \\ d_n + \left(2^{\lfloor \log_2 d_n \rfloor}\right) + 2\left(\lfloor \log_2 d_n \rfloor\right) d_n < 1 \end{cases} \tag{1}$$

Using the difference expansion technique to eliminate distortion, this reduced difference is used to conceal the hidden bit. The method considers all the difference except the range -1 to $+1$ for embedding. This method results in more distortion and less PSNR. In [16] another technique in the same domain is proposed which allows the embedding within the difference range -2 to $+2$. It provides more security and high PSNR but the embedding capacity is less as only 1 bit is hidden in the selected pixel. In [17] a numerical model was created using protocol overhead and network. However, the transmission effectiveness is less.

3. **Method.** New steganography approaches are in current progressions and research is still going on for enhancing capacity of payload with more security and less distortion. The proposed algorithm is based on revised differential expansion technique. Here the difference value of the selected pixel is increased or decreased according to the logarithmic function.

3.1. **Embedding algorithm.** The steps for embedding are given below.

Input: Cover image (B) of size $F \times H$ and secret message (S).

Output: Stego image (B')

Step 1: The original image B is partitioned into $n \times n$ size blocks for $n = 2$ to 4. The blocks are scanned for processing in raster scan order. Each block has k pixels where $k = n \times n$. In each block the pixels are represented as $b_1, b_2, b_3, \ldots, b_k$.

Step 2: The center pixel value b_c of each block is calculated using Equation (2) where l and h are the lowest and highest indexes of the block simultaneously. It is used as reference to find the difference values.

$$b_c = \lfloor l + h/2 \rfloor \tag{2}$$

Step 3: The distance values of each pixel from the center pixel b_c in each block are computed. These values are stored in x where each x_i is defined as Equation (3).

$$x_i = b_i - b_c \tag{3}$$

Step 4: The distance array x is scanned according to the condition, i.e., if the distance value x_i is within the range -3 to $+3$, then the corresponding pixel is used for embedding. If the distance is not within the range, then it is ignored.

Step 5: The secret message S is converted to binary and stored in a 1D array. Before concealing the secret bits, each 2 bits is taken and converted to decimal and stored in M.

Step 6: The secret bit M_i is concealed in the cover pixels whose distance from the reference pixel is within the range -3 to $+3$. However, to reduce distortion in stego image, the difference values x_i are improved before embedding the secret bit. This modification is done using Equation (4). Ceil function of a number p is defined as the smallest integer that is greater than or equal to the given number p.

$$x_i' = \begin{cases} x_i - [2 \wedge ceil(\log 2(abs(x_i))) + ceil(\sin(x_i))] & x_i > 0 \\ x_i + [2 \wedge ceil(\log 2(abs(x_i))) - ceil(\sin(x_i))] & x_i < 0 \\ x_i & x_i = 0 \end{cases} \tag{4}$$

Step 7: The secret data M_i is then added to the enhanced difference values using Equation (5). The center pixel is not modified as the same pixel is used for extraction.

$$x_i' = x_i' + M_i \tag{5}$$

Step 8: By adding the original cover pixel b_i to the modified difference value, the stego pixel value b_i' is obtained using Equation (6).

$$b_i' = b_i + x_i' \tag{6}$$

3.2. **Recovery algorithm.** The withdrawal of the concealed data is done using the original difference (x) and stego image shared separately by the sender.

In the extraction procedure, we have to follow the steps given below.

Input: Stego image (B') of size $F \times H$

Output: Secret message (S)

Step 1: The stego message (B') is segmented into independent blocks of size $n \times n$. Each sub image ($b_1', b_2', b_3', \ldots, b_k'$) is selected in the same direction as embedding.

Step 2: The central pixel of each block b_c', is chosen as reference pixel.

Step 3: The difference matrix x_i'' for each block is designed by subtracting the reference pixel from the stego pixel.

$$x_i'' = b_i' - b_c' \tag{7}$$

Step 4: The original difference matrix (x) and the calculated difference matrix (x'') for each sub image are compared for finding pixels where secret data is hidden.

Step 5: The hidden data M_i is generated from the stego pixel using the given formula in Equation (8).

$$M_i = \begin{cases} x_i'' - (2 \times x_i - [2 \wedge ceil(\log 2(abs(x_i))) + ceil(\sin(x_i))]) & x_i > 0 \\ x_i'' - (2 \times x_i + [2 \wedge ceil(\log 2(abs(x_i))) - ceil(\sin(x_i))]) & x_i < 0 \\ x_i'' - 2 * x_i & x_i = 0 \end{cases} \tag{8}$$

Step 6: After generating the secret data M_i, it is converted to 2 bits binary and kept in an array.

Step 7: The generated bits are arranged properly to get the original covert message.

Example for embedding and extraction

Different cases giving a clear illumination of how covert message is concealed are shown below. The pictorial representation of embedding procedure is shown in Figure 1. It shows the block of the cover image (B) and the secret message {121312} to be embedded.

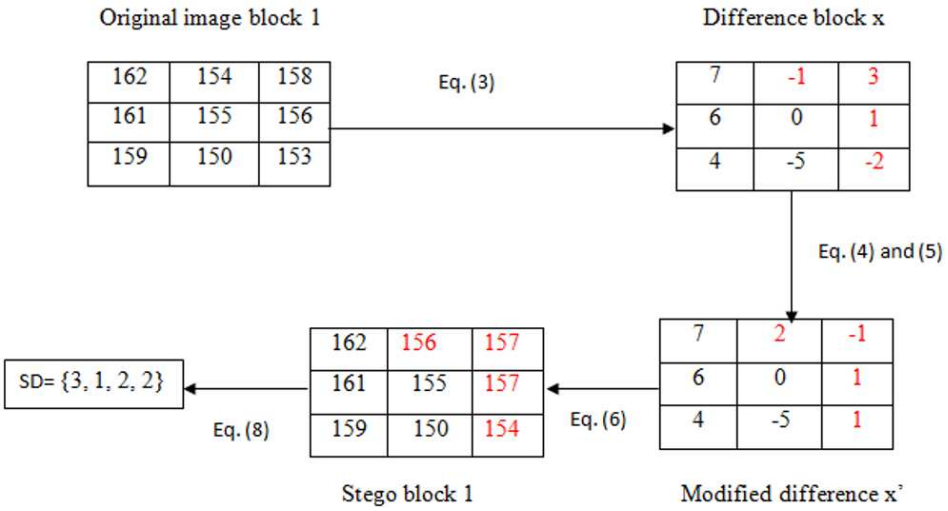


FIGURE 1. Illustration of embedding in a block

The comparison between the existing differential expansion method and modified reduced differential expansion with respect to change in cover pixel is given in Table 1. The distance matrix and stego image are independently sent because combining them may reveal the stego picture.

4. **Experimental Result.** The performance of the proposed algorithm with various existing approaches is measured. The proposed strategy is executed and tried in a PC with windows 7 64 bit operating system, Intel(R) Core(TM) i5-4210U CPU @1.70 GHZ and using MATLAB programming. The measure motivation is to measure the efficiency of the suggested technique with the different existing algorithms difference expansion (DE) [11], generalized difference expansion (GDE) [12], centralized difference expansion (CDE) [13], reduced difference expansion (RDE) [15] and Modulus [16]. In Figure 2, ten standard images having size 512×512 are taken from the image database for the experiment. To analyze the distortion of stego image, PSNR and mean squared error (MSE) are calculated. The PSNR is calculated using Equation (9) and MSE is calculated using Equation (10).

$$PSNR = 10 * \log_{10} \frac{Max^2}{MSE} \tag{9}$$

$$MSE = \left(\frac{1}{p \times q}\right) \sum_{i=1}^{p} \sum_{j=1}^{q} \left[(F_{ij} - H_{ij})^2\right] \tag{10}$$

Here *Max* is used to denote the highest intensity value in the image. The size of cover image (F) and stego image (H) is represented by $p \times q$. F_{ij} and H_{ij} represent the pixel's values at location (i, j). The test images used for result analysis and the resultant stego images are given in Figure 2. We can see no visible difference which can be identified between the input and output images.

TABLE 1. Comparison of modification of the cover pixel without and with reduction

Original difference (x_i)	Secret data to hide (m_i)	Modification to cover pixel without enhancement ($x_i + m_i$)	Modification to cover pixel using Equations (4) and (5)
1	0	1	−1
	1	2	0
	2	3	1
	3	4	2
3	0	3	−2
	1	4	0
	2	5	−3
	3	6	2
−1	0	−1	−1
	1	0	0
	2	1	1
	3	2	2
−2	0	−2	−1
	1	1	0
	2	0	0
	3	1	2

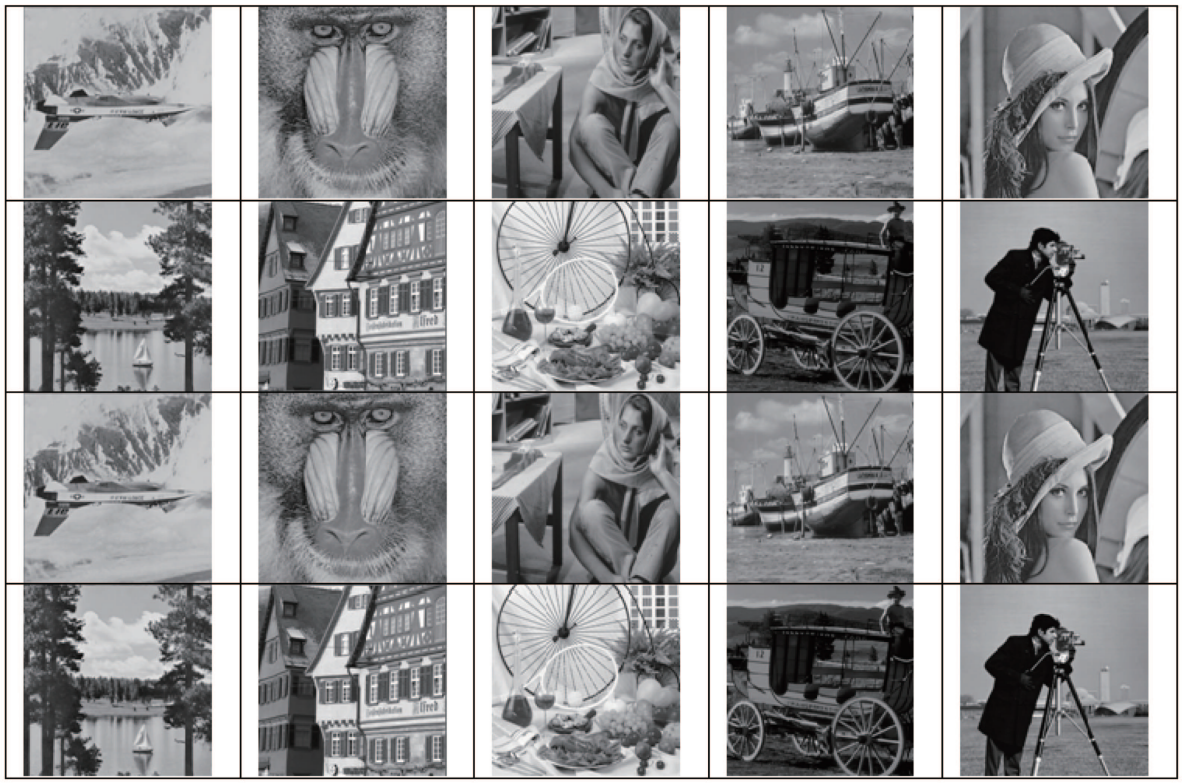


FIGURE 2. Test images and corresponding stego images

Our proposed work is tested in the following cases.

- Same image with different sizes (256×256 and 512×512) with the same size secret message (20000 bit).
- Hiding capability of different images of the same size (512×512). The comparison is done with EC and PSNR.
- Different images with the same size with concealing different amount of secret data, i.e., (3200 bits, 20000 bits, 80000 bits, 160000 bits and 320000 bits).

Case 1: *Capacity versus visual quality with the same image of different sizes*

For this experiment, the standard test image with different sizes is taken. The secret message of 20000 bits generated randomly is chosen for the experiment. The comparison of the proposed technique with the existing techniques is given in Figure 3. The result shows that with hiding capacity the PSNR increases along with the size of the image. Depending on the complexity of the image, the PSNR along with hiding capacity improves. The result shows that the proposed method has better hiding capability with high PSNR.

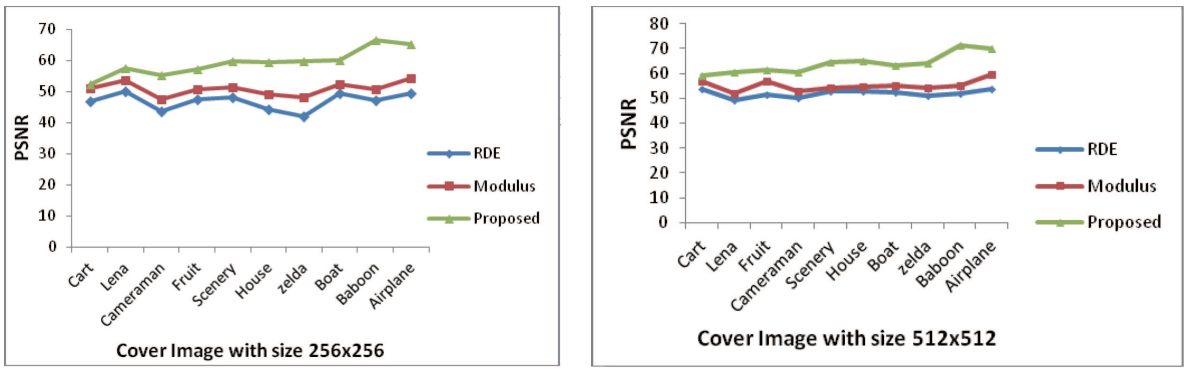


FIGURE 3. Comparison of PSNR with the same size secret bit in 256×256 and 512×512 cover image

Case 2: *Hiding capacity of different cover images of the same size*

From the experiment it was observed that the payload capability of each test image is different due to texture, sensitivity and features. According to the complexity of the test image the embedding capability and PSNR vary. If the complexity of cover image is higher, then the payload capacity is less. Baboon image has rich edges and is more complex, so it leads to less embedding rate, and the capability of hiding is less, i.e.,

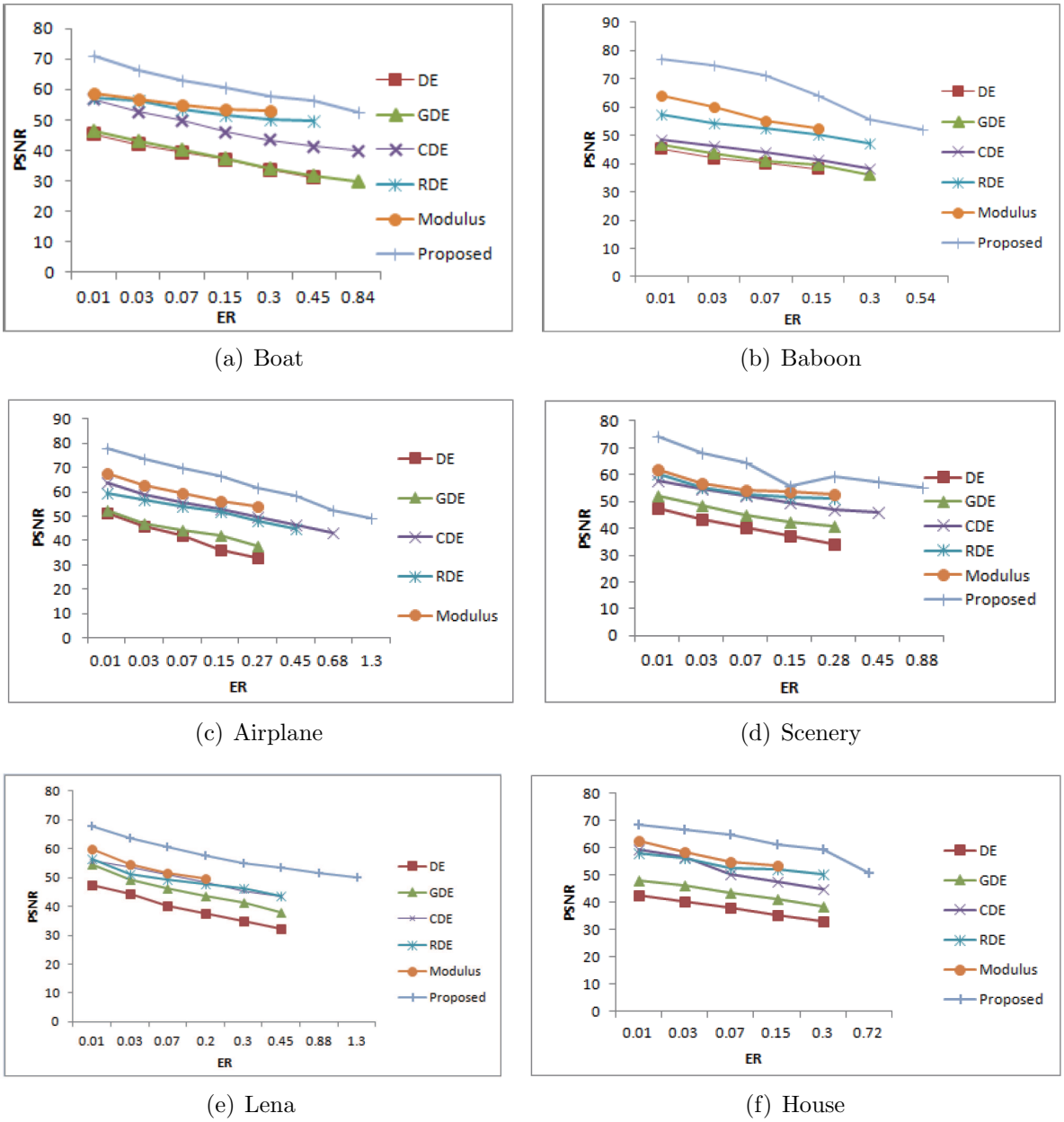
TABLE 2. ER and PSNR of different test images with the same size

Method	DE [11]		GDE [12]		CDE [13]		RDE [15]		Modulus [16]		Proposed	
Standard test image	ER	PSNR	ER	PSNR	ER	PSNR	ER	PSNR	ER	PSNR	ER	PSNR
Scenery	0.28	34.2	0.34	39.1	0.55	42.3	0.31	50.9	0.28	52.5	0.88	55.3
Airplane	0.31	32.7	0.41	34.2	0.65	35.16	0.45	45.1	0.27	54.2	1.3	49.8
Baboon	0.2	35.9	0.32	38.6	0.4	37.9	0.39	46.6	0.21	46.8	0.54	52.1
Lena	0.3	32.1	0.56	36.6	0.65	39.4	0.45	43.8	0.23	49.7	1.3	49.9
Boat	0.41	31.4	0.65	29.8	0.72	39.1	0.45	49.8	0.3	52.8	0.84	52.5
House	0.3	33.1	0.41	35.1	0.65	40.5	0.31	50.4	0.18	53.1	0.72	50.7
Cart	0.2	36.1	0.56	37	0.61	40.2	0.4	46	0.15	54.5	0.98	47.9
Zelda	0.3	35.9	0.4	38.2	0.5	41.5	0.37	47.1	0.17	53.2	0.88	50.4
Fruit	0.3	35.7	0.6	39	0.62	39.8	0.41	50.1	0.16	54.8	0.96	46.8
Cameraman	0.2	37.8	0.7	36	0.8	41.1	0.7	44.3	0.15	52.3	1.4	47.6

0.54 with PSNR 52.1. The cover image with less complexity like Lena, Airplane and Cameraman has high capacity to embed, i.e., up to 1.3. Table 2 shows the embedding rate (ER) of each cover image with the PSNR.

Case 3: *Different test images with the same size for hiding different amount of secret bits*

For this experiment the different test images of the same size, i.e., 512×512 is chosen and different amount of random secret bits are hidden to calculate the amount of distortion. The result analysis of each image is given in Figure 4.



(a) Boat (b) Baboon

(c) Airplane (d) Scenery

(e) Lena (f) House

FIGURE 4. ER vs. PSNR for different cover images

We observed from the outcome that Baboon has a payload capacity of 145,000 with PSNR above 50. We observed that the images Scenery and Baboon result in the highest PSNR above 70 with less amount of secret bit. Lena, House and Cameraman have PSNR value less than 70 with the same amount of secret bits. We also found that Lena and Airplane and Cameraman can embed up to 345,000 bits with PSNR value nearly 50. Finally, the suggested technique is compared with many existing approaches in the same domain. The analysis in Table 2 also shows that CDE approach also results in higher

embedding capacity in Cameraman up to 160,000 with PSNR over 40. For other images also CDE method results in higher embedding rate but with less PSNR. The modulus approach gives less embedding rate than CDE, but PSNR is high. The figure shows that the proposed method gives better result with respect to other existing techniques.

5. **Conclusion.** The methodology described in the paper suggests a novel approach of information hiding by making the stego image perceptually imperceptible. The resulting PSNR is more than 50 for payload size 320,000 bits which show any visible distortion in the stego image cannot be identified through naked eye. The proposed method results in high embedding capacity by embedding 2 bits of secret data in each pixel which falls in the difference range using the difference expansion method. The technique also uses both the positive and negative differences for hiding secret data. The original difference is revised to reduce the misrepresentation in stego image. The result analysis is done on different standard images available from the image database. The comparison with existing techniques shows that our proposed work gives high embedding capacity and more PSNR with less distortion. The secret message is also successfully retrieved from the stego image. Here the block based embedding is utilized for information hiding with each block hiding different amount of secret bits. The proposed work can be improved further by considering the features of each block and predicting the embedding capacity of each block. This new technique may give future direction to the research work in the image steganography domain.

REFERENCES

[1] H. S. El-Sayed, S. F. El-Zoghdy and O. S. Faragallah, Adaptive difference expansion-based reversible data hiding scheme for digital images, *Arabian Journal for Science and Engineering*, vol.41, no.3, pp.1091-1107, 2016.

[2] A. K. Gulve and M. S. Joshi, A high capacity secured image steganography method with five pixel pair differencing and LSB substitution, *International Journal of Image, Graphics and Signal Processing*, vol.7, no.5, pp.66-74, 2015.

[3] Y. Y. Tsai, D. S. Tsai and C. L. Liu, Reversible data hiding scheme based on neighboring pixel differences, *Digital Signal Processing: A Review Journal*, vol.23, no.3, pp.919-927, 2013.

[4] J. Mandal, Colour image steganography based on pixel value differencing in spatial domain, *International Journal of Information Sciences and Techniques*, vol.2, no.4, pp.83-93, 2012.

[5] W. Wang, J. Ye, T. Wang and W. Wang, A high capacity reversible data hiding scheme based on right-left shift, *Signal Processing*, vol.150, pp.102-115, 2018.

[6] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. Ho and K. H. Jung, Image steganography in spatial domain: A survey, *Signal Processing: Image Communication*, vol.65, pp.46-66, 2018.

[7] Z. Xiang, J. Sang, Q. Zhang, B. Cai, X. Xia and W. Wu, A new convolutional neural network-based steganalysis method for content-adaptive image steganography in the spatial domain, *IEEE Access*, vol.8, pp.47013-47020, 2020.

[8] V. Holub, J. Fridrich and T. Denemark, Universal distortion function for steganography in an arbitrary domain, *EURASIP Journal on Information Security*, 2014.

[9] A. Al-Ataby and F. Al-Naima, A modified high capacity image steganography technique based on wavelet transform, *International Arab Journal of Information Technology*, vol.7, no.4, pp.358-364, 2010.

[10] M. S. Subhedar and V. H. Mankar, Secure image steganography using framelet transform and bidiagonal SVD, *Multimedia Tools and Applications*, vol.79, pp.1865-1886, 2020.

[11] J. Tian, Reversible data embedding using a difference expansion, *IEEE Trans. Circuits and Systems for Video Technology*, vol.13, no.8, pp.890-896, 2003.

[12] A. M. Alattar, Reversible watermark using the difference expansion of a generalized integer transform, *IEEE Trans. Image Processing*, vol.13, no.8, pp.1147-1156, 2004.

[13] C. C. Lee, H. C. Wu, C. S. Tsai and Y. P. Chu, Adaptive lossless steganographic scheme with centralized difference expansion, *Pattern Recognition*, vol.41, no.6, pp.2097-2106, 2008.

[14] S. M. Abdullah and A. A. Manaf, Multiple layer reversible images watermarking using enhancement of difference expansion techniques, *Communications in Computer and Information Science*, 2010.

[15] P. Maniriho and T. Ahmad, Enhancing the capability of data hiding method based on reduced difference expansion, *Engineering Letters*, vol.26, no.1, pp.45-55, 2018.

[16] P. Maniriho and T. Ahmad, Information hiding scheme for digital images using difference expansion and modulus function, *Journal of King Saud University – Computer and Information Sciences*, vol.31, no.3, pp.335-347, 2019.

[17] Y. Song, H. Ni and X. Zhu, Analytical modeling of optimal chunk size for efficient transmission in information-centric networking, *International Journal of Innovative Computing, Information and Control*, vol.16, no.5, pp.1511-1525, 2020.