An interpolation based steganographic technique with leastsignificant-bit and pixel value differencing in a pixel block

Jayeeta Majumder¹, Chittaranjan Pradhan²

¹Department of Computer Science and Engineering, KIIT University, Odissa, India ²School of Computer Engineering, KIIT University, Bhubaneswar, Odissa, India

Article Info

Article history:

Received Nov 13, 2021 Revised May 19, 2022 Accepted Jun 11, 2022

Keywords:

Data hiding Least-significant-bit technique Nearest neighbour interpolation Pixel value differencing scheme Steganography

ABSTRACT

Over the past few years, in order to improve the hiding capacity and the peak signal-to-noise ratio (PSNR) value, several steganographic techniques have been developed. Steganography has become a popular technique to transmit secret data through any medium. In image steganography, the human eye cannot easily identify the hidden data which is embedded into the image. Small changes are also not detected by the human eye. High hidden capacity along with high visual quality is provided by the pixel value differencing (PVD) method. This paper first proposes the method of interpolation between the pixel blocks and then applies the least-significant-bit (LSB) substitution technique with the PVD method. At the starting phase, the original image is fixed to a 2x2 block, then the nearest neighbor interpolation (NNI) technique is implemented. In the next phase, the upper left pixel isembedded by the kbit LSB substitution method along with hidden data. The newly generated neighbouring pixel value is measured. Thus, data is hidden from three directions. Through this paper using two different range tables, the new algorithm is proposed. We observed that in both cases, PSNR and the hiding capacity are improved.

This is an open access article under the <u>CC BY-SA</u> license.



Corresponding Author:

Jayeeta Majumder Department of Computer Science and Engineering, KIIT University Odissa, India Email: jem2003_kolkata@yahoo.co.in

1. INTRODUCTION

Nowadays, the prime and most important issues are to keep the privacy of personal data at the time of broadcast through a common medium. Most commonly, private data is treated before broadcasting over the media. The handling procedure mainly deviates the main text of the data into an indecipherable method. But one and only legally authorized person can accomplish the reversible procedure on the scrambled information to get back the main data. Numerous data protection procedure has been offered to guard the privacy of the original data. When one proposes any data hiding method, the capacity of hidden bit and the un-detectability by human eyepossessions are to be noticed. In contrast, with cryptography, Steganography [1]-[3] is an alternative method to keep the privacy of the data. It does not change the data to throw it away from the trespasser. In this procedure, the hidden and private data are embedded into an unpredictable carrier or covermedia such asaudio, video, and image. To build up expressive data which is identified as stego-data. It is problematic to differentiate the stego-data in comparison with the main cover dataover a medium over an identified cover medium. The security system based on steganographic techniques is applied in numerous applications similar to military applications, commercial initiatives, multimedia applications and the internet of things (IoT) [4]. In the next section describes the previous research in this area. It also gives the idea who has done the most recent and relevant work. After that, in the third section, the proposed work is discussed.

The proposed work has two phases. In the first phase, the nearest neighbor interpolation is implemented in the image pixel block, after that in the second phase, the k-bit least-significant-bit (LSB) technique with pixel value differencing (PVD) is applied. Also, data extraction method has been introduced. In the fourth section, one mathematical explanation is given where we take a randompixel block and mathematically calculate the stego pixel block andfrom the stego pixel block extracts the data. After that, with the help of sample images using MATLAB, we perform work and produce the result through discussion. Calculate also the PSNR value of the image.

2. RELATED WORKS

The most commonly used steganographic method is the LSB substitution method. The pixel value differencing method was primarilyannounced by Wu and Tsai [1] where the edge region of the image is considered to hide more data in comparison with a smoother region. The change of edge region cannot be detected by the human eye. Thus, data hiding in the edge region of an image is the main working principle of PVD technique. Initially, a 2×2 block of image is used for the PVD technique and later the block size is expanded to increase the hiding capacity [2]. In the 2×2 block size of the image there are the total of three diagonal edges that are measured [3]. To identify the differences, Chang and Tseng [4] proposed the differences of the pixel values with the help of multiple adjacent pixels. The position of insertion of data can be randomized and based on the undisclosed messages [5]. Next, the calculation based on the directionally neighboring pixel increases the data hiding capacity for a 2×2 pixel block [6], [7]. By using two different reference range tables by Chen [8] proposed a new PVD based image steganography technique. Liao et al. [9] proposed an adaptive LSB substitution method with the PVD method. A combination of LSB and PVD creates a new hybrid steganography approach implemented in a 1×3 pixel block proposed by Khodaei and Faez [10], Swain [11] and Pradhan et al. [12] established that compared to 2×2 sized block of image, the 2×3 sized block of image gives better performance in the hybrid approach. Swain [13] suggested the adaptive PVD method by taking the horizontal, vertical, and diagonal edges of the pixel. The presentation of the PVD method by taking 6-pixel blocks are appeared in Pradhan et al. [14]. The image edge region complexity can be enhanced by using different adaptive methods. The following Table 1, shows the comparative analysis [1]-[11] of different hiding method using PVD techniques. In this paper, at the starting phase, the original image is fixed to a 2×2 block, then the nearest neighbor interpolation technique is implemented. In the second phase, the steganographic scheme with the 3×3-pixel block uses LSB and PVD techniques. Two variants of range table are used for both peak signal-to-noise ratio (PSNR) and to increase data bit capacity. In a probable encryption technique, it is significant that confidential addresses recognize it when they see the encrypted message [15]-[19]. The data within the cover should not be distorted radically and merge with the embedded data [20], [21]. Embedded data should be kept away from detection to a great extent [22]-[24]. Embedded data has to be directly encoded into the media to keep data consistency [25], [26]. The following Table 1, shows the comparative analysis [1]-[11] of different hiding method using PVD techniques.

| Peference No | Parameters | | | Δ dvantages | | |
|---------------|------------|----------|------------|--|--|--|
| Reference no. | Security | Capacity | Distortion | Advantages | | |
| [1] | moderate | moderate | moderate | PVD method is introduced | | |
| [2] | moderate | low | high | Stego-image quality is better due to change in size of | | |
| | | | | pixel block | | |
| [3] | high | high | high | Tri-way PVD is introduced | | |
| [4] | high | high | moderate | New Direction of PVD | | |
| [5] | high | low | high | Random position is used to hide data | | |
| [6] | high | high | high | Embedding capacity and image quality increased | | |
| [7] | high | high | high | Payload capacity & image quality high | | |
| [8] | high | moderate | high | Range table calculation is different | | |
| [9] | moderate | moderate | high | LSB+PVD used | | |
| [10] | high | moderate | high | LSB+PVD used in 1X3 pixel block | | |
| [11] | high | high | high | Hybrid steganography introduced | | |

Table 1. Comparative study of data hiding method using PVD technique [1]-[11]

3. PROPOSED METHOD

The algorithm of data embedding is separated into two segments. In first, the 2×2 pixel block is installed by using an image interpolation method and in the second phase, the k-bit LSB steganography scheme is applied.the algorithm has two sections; i) interpolation phase and ii) data embedding phase. Interpolation phase uses the nearest neighbor interpolation method. Data embedding phase uses k-bit interpolation method.

3.1. Interpolation phase

The cover image is split into 2×2 non-convergence block by raster scan method. Then, alter the pixel block to 3x3 in size by using nearest neighbor interpolation procedures. Consider all four-neighbor pixel, Px, P (0,1), P (1,0), and P (1,1). First find out the highest pixel value, suppose, it is p_{max} . then, compute p_r as $(p_{max}+(p_x+p(0,1))/2)/2$, measure p_l as $(p_{max}+(p_x+p(1,0))/2)/2$ and finally, determine p_c as $(p_l+p_r)/2$). Also consider p (1,2) and p (2,1). After interpolation the original image block is shown in Figure 1.



Figure 1. Nearest neighbour interpolation method

3.2. Data embedding phase with k-bit LSB technique

Step 1: here, the value of k is 3. First secret k bit data isembedded with the earliest pixel value (p_x) and the latest pixel value (p'_x) is formed. Next, calculate the equivalent decimal value of K-bit LSB (L) and also determine the decimal equivalent of K-data bit A. Measure the difference d=L-A. For pixel value adaptation, apply the following n (1).

$$p'_{x} = \begin{cases} p'_{x} + 2^{k}, & \text{if } d > 2^{k-1} \text{ and } 0 \le p'_{x} + 2^{k} \le 255\\ p'_{x} - 2^{k}, & \text{if } d < -2^{k-1} \text{ and } 0 \le p'_{x} - 2^{k} \le 255\\ p'_{x}, & \text{otherwise} \end{cases}$$
(1)

Step 2: calculate the pixel differences between current pixel with the right, left and corner pixel as d_1 , d_2 , d_3 by using (2)-(4).

$$d_1 = |p'_x - p_4|$$
(2)

$$\mathbf{d}_2 = |\mathbf{p}'_{\mathbf{x}} - \mathbf{p}_{\mathbf{c}}| \tag{3}$$

$$d_3 = |p'_x - p_1| \tag{4}$$

Step 3: the quantization range table for type 1 is shown in Table 2 and for type 2 in Table 3.

| Table 2. Range table for type 1 | | | | | | | | | |
|--|---|---|---|---|---|---|--|--|--|
| Range | Range R=[0-7] R=[8-15] R=[16-31] R=[32-63] R=[64-127] R=[128-2: | | | | | | | | |
| Hidden capacity (in bit) | 3 | 3 | 3 | 3 | 4 | 4 | | | |
| Table 3. Range table for type 2 | | | | | | | | | |
| Range $R_i=[0-7]$ $R_i=[8-15]$ $R_i=[16-31]$ $R_i=[32-63]$ $R_i=[64-127]$ $R_i=[128-53]$ | | | | | | | | | |
| Hidden capacity (in bit) | 3 | 3 | 4 | 5 | 6 | 6 | | | |

Step 4: from the tables; find the range R_x , where d_1 , d_2 and d_3 are present. According to the table also determine the no. of bits (t_{x1} , t_{x2} , t_{x3}) that can be hidden and also obtain the lower bounds l_1 , l_2 , l_3 .

Step 5: now, from the secret data bit-stream take t_{x1} , t_{x2} , t_{x3} bits continuously and convert them to equivalent decimal values namely b_1 , b_2 , b_3 respectively. Then calculate the new difference:

$$d_1' = 1_1 + b_1 \tag{5}$$

$$d_2' = 1_2 + b_2 \tag{6}$$

$$d_3' = 1_3 + b_3 \tag{7}$$

Indonesian J Elec Eng & Comp Sci, Vol. 27, No. 2, August 2022: 1074-1082

Step 6: calculate the new stego pixel values p"_r, p"'_rfor p_r . Similarly, p"₁, p"'₁for pl and p"_c, p"'_c for p_c by using the following formula.

$$p''_{r} = p'_{x} - d_{1}'$$

$$p'''_{r} = p'_{x} + d_{1}'$$

$$p''_{c} = p'_{x} - d_{2}'$$

$$p'''_{c} = p'_{x} - d_{2}'$$

$$p'''_{1} = p'_{x} - d_{3}'$$

$$p'''_{1} = p'_{x} + d_{3}'$$

Step 7: now, determine the new values as shown in:

$$p'_{r} = p''_{r}, \text{ if } |p_{r} - p''_{r}| < |p_{r} - p'''_{r}| \text{ and } 0 \le p''_{r} \le 255$$
 (8)

p'''r, otherwise

$$p'_{c} = p''_{c}$$
, if $|p_{c} - p''_{c}| < |p_{c} - p'''_{c}|$ and $0 \le p''_{c} 255$ (9)

p""c, otherwise

$$p'_{1} = p''_{1}$$
, if $|p_{1} - p''_{1}| < |p_{1} - p'''_{1}|$ and $0 \le p''_{1} \le 255$ (10)

 p'''_1 , otherwise:

the pixel block is as shown in Figure 2. Figure 2(a) show initial pixel block and Figure 2(b) stego pixel.

| p _x (0,0) | pr | | p' _x (0,0) | p'r | |
|----------------------|----|--|--------------------------|--------|--|
| p_1 | Рc | | p′1 | p'c | |
| (a) | | | (t |)) | |

Figure 2. 2×2 pixel block using nearest neighbour interpolation (a) initial pixel block and (b) stego pixel block

3.3. Data extracting process

Cover image split into 2x2 non- convergence block by raster scan method. Suppose, we take the pixel block then follow the steps.

Step 1: Calculate the pixel difference values:

$$\begin{array}{l} d_1' = \; |\; p_r' \; - \; p_{\;x} \; | \\ d_2' = \; |\; p_c' - \; p_x' \; | \\ d_3' = \; |\; p_1' \; - \; p_x' \; | \end{array}$$

Step 2: Find the range R_x , where d'₁, d'₂and d'₃belongs. According to the table also determine the no. of bits (t_{x1} , t_{x2} , t_{x3}) that can be hidden and also obtain the lower bounds l_1 , l_2 , l_3 from the range table.

Step 3: Determine the Secret data bit stream by using the following formulas.

$$S_1 = d'_1 - 1_1 \tag{11}$$

$$S_2 = d'_2 - 1_2 \tag{12}$$

$$S_3 = d'_3 - 1_3 \tag{13}$$

Now convert the values of S_1 , S_2 and S_3 into t_{x1} , t_{x2} and t_{x3} binary bits respectively.

4. MATHEMATICAL EXPLANATIONS

Consider the cover image pixel block of 2×2 . Now, applying nearest neighbour interpolation (NNI) method. Now, $p_{max}=140$ and $p_x=90$.

 $\begin{array}{l} p_r =& (140 + (90 + 140)/2)/2 = 138 \\ p_l =& (140 + (90 + 110)/2)/2 = 120 \\ p(1,2) =& (140 + (140 + 80)/2)/2 = 125 \\ p_c =& (128 + 120)/2 = 124 \\ p(2,1) =& (140 + (110 + 80)/2)/2 = 118 \end{array}$

| 90 | 140 | 90 | 128 | 140 |
|-----|-----|---------|-----|-----|
| | | 120 | 124 | 125 |
| 110 | 80 | 110 | 118 | 80 |

After that start he procedure of data embedding. Take 2×2 Pixel block, i.e,

| 90 | 128 |
|-----|-----|
| 120 | 124 |

Here k value=3 and consider data bit stream 111001110011 as secret data.

px=90=(01011010)2

Now, after 3 bit LSB substitution we get $p'_x=(01011101)_2=(93)_{10}$. After adjustment, $p'_x=93 - 2^3 = 93 - 8 = 85$. Now, the pixel differences are,

d1=|85-128|=43

 $d_2 = |85 - 124| = 39$

d₃=|85-120|=35

Determine the total no. of hidden bits and also the lower range from the range table. From the bit stream, 111001110011 we calculate b_1 , b_2 , b_3 value,

b1=(111)2=7, b2 = (001)2=1, b3=(110)2=6

 $\begin{array}{l} d_1 \ensuremath{'=l_1+b_1=32+7=39}\\ d_2 \ensuremath{'=l_2+b_2=32+1=33}\\ d_3 \ensuremath{'=l_3+b_3=32+6=38} \end{array}$

The hidden data bit are (111001110)2.

Now, to get the new pixel value after boundary condition checking:

p'r=124, p'c=118, p'l=123

after data embedding the generated stego-pixel block,

| 85 | 124 |
|-----|-----|
| 123 | 118 |

Now, start the procedure of data extraction.

d'₁=|124-85|=39 d'₂=|118-85|=33 d'₃=|123-85|=38

Again, determine the total no. of hidden bits and also the lower range from the range table,

D 1079

```
\begin{array}{l} S_1 = 39 - 32 = 7 = (111)2 \\ S_2 = 33 - 32 = 1 = (001)2 \\ S_3 = 38 - 32 = 6 = (110)2 \end{array}
```

After data extraction we get $(111001110)_2$.

5. RESULT AND DISCUSSION

Here, we take 3 sample cover images, like Lena, Boat and Baboon, and 756,035 data bits are hidden. The proposed algorithm is verified by MATLAB.As a result, the stego-image is detected. Following are the details of the cover images and stego images. The gray scale images are considered as cover image in Figure 3. The results for the proposed techniques as shown in Figure 4 and Figure 5. The proposed technique and the existing techniques such as Khodaei and Faez (2012) [10] and Swain *et al.* (2016) [11] have been showed in table 4 using Type 1 and Table 5 using Type 2.

RS analysis of Lena image using type 1 and Type 2 shows in Figure 6. RS analysis of Baboon image using type 1 and Type 2 shows in Figure 7, PDH analysis of Lena image using type 1 and Type 2 shows in Figure 8 and PDH analysis of Baboon image using type 1 and Type 2 shows in Figure 7 respectively.



Figure 3. Cover image



Figure 4. Stego-image (using type 1)

Figure 5. Stego-image (using type 2)



Figure 6. RS analysis curve for Lena image (a) using Type 1 (b) using Type 2

An interpolation based steganographic technique with least-significant-bit and ... (Jayeeta Majumder)



Figure 7. RS analysis curve for baboon image (a) using type 1 and (b) using type 2



Figure 8. PDH analysis (a) Lena image using type 1, (b) Lena image using type 2, (c) boat image using type 1, and (d) boat image using type 2

Table 4. Comparison the proposed technique with the other techniques for type 1, k=3

| Imagas 512×512 Gray imaga | Khodaei and Faez [10] | | Swain [11] | | Proposed | |
|---------------------------|-----------------------|----------|------------|----------|----------|----------|
| mages 512×512 Gray mage | PSNR | Capacity | PSNR | Capacity | PSNR | Capacity |
| Lena | 42.34 | 2375278 | 42.83 | 2361875 | 42.86 | 2365795 |
| Boat | 39.75 | 2391994 | 38.38 | 2370147 | 39.38 | 2370158 |
| Baboon | 37.59 | 2443361 | 34.98 | 2393475 | 35.56 | 2427365 |

Table 5. Comparison the proposed technique with the other techniques for type 2, k=3

| Imagas 512,512 Cross imaga | Khodaei and Faez [10] | | Swain [11] | | Proposed | |
|----------------------------|-----------------------|----------|------------|----------|----------|----------|
| Images 512×512 Gray Image | PSNR | Capacity | PSNR | Capacity | PSNR | Capacity |
| Lena | 41.58 | 2345786 | 42.14 | 2312546 | 42.78 | 2356174 |
| Boat | 37.84 | 2312748 | 38.24 | 2298716 | 38.84 | 2313146 |
| Baboon | 35.52 | 2398674 | 35.16 | 2385186 | 35.64 | 2398762 |

CONCLUSION 6.

The principle of image interpolation with LSB substitution and PVD steganography process is measured by i) RS analysis and ii) pixel difference histogram (PDH) analysis. In this paper, both the LSB and PVD are used along with nearest neighbor interpolation. The interpolation is operated on a 2x2 pixel block and a 3x3 pixel block is then generated. Next, LSB and PVD are applied. After interpolation, the new pixel value is used for the difference calculation with its consecutive neighbour. Using the difference, with the help of a range table, the PVD is implemented. Here multiple edge directionsare applied, so, PDH analysis makes no difference. So, the data hiding capacity and PSNR value give satisfactory results. The secret data can also be in compressed form. One data compression technique was also added with the data hiding technique. To transmit the information to a user authentication method will be present in the proposed algorithm. Besides, there must be no chances of distortion within the generated stego-image.

REFERENCES

- D. C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value differencing," Pattern Recognition Letters, vol. 24, [1] no. 9-10, pp. 1613-1626, Jun. 2003, doi: 10.1016/S0167-8655(02)00402-6.
- K. C. Chang, C. P. Chang, P. S. Huang, and T. M. Tu, "A novel image steganographic method using tri-way pixel-value differencing," *Journal of Multimedia*, vol. 3, no. 2, pp. 37–44, Jun. 2008, doi: 10.4304/jmm.3.2.37-44. [2]
- Y. P. Lee, J. C. Lee, W. K. Chen, K. C. Chang, I. J. Su, and C. P. Chang, "High-payload image hiding with quality recovery using [3] tri-way pixel-value differencing," *Information Sciences*, vol. 191, pp. 214–225, May 2012, doi: 10.1016/j.ins.2012.01.002. C. C. Chang and H. W. Tseng, "A steganographic method for digital images using side match," *Pattern Recognition Letters*, vol.
- [4] 25, no. 12, pp. 1431-1437, Sep. 2004, doi: 10.1016/j.patrec.2004.05.006.
- C. H. Yang, C. Y. Weng, H. K. Tso, and S. J. Wang, "A data hiding scheme using the varieties of pixel-value differencing in [5] multimedia images," Journal of Systems and Software, vol. 84, no. 4, pp. 669–678, Apr. 2011, doi: 10.1016/j.jss.2010.11.889.
- H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB [6] replacement methods," IEE Proceedings: Vision, Image and Signal Processing, vol. 152, no. 5, pp. 611-615, 2005, doi: 10.1049/ipvis:20059022.
- C. H. Yang, C. Y. Weng, S. J. Wang, and H. M. Sun, "Varied PVD + LSB evading detection programs to spatial domain in data [7] embedding systems," Journal of Systems and Software, vol. 83, no. 10, pp. 1635–1643, Oct. 2010, doi: 10.1016/j.jss.2010.03.081.
- J. Chen, "A PVD-based data hiding method with histogram preserving using pixel pair matching," Signal Processing: Image [8] Communication, vol. 29, no. 3, pp. 375-384, Mar. 2014, doi: 10.1016/j.image.2014.01.003.
- X. Liao, Q. Y. Wen, and J. Zhang, "A steganographic method for digital images with four-pixel differencing and modified LSB [9] substitution," Journal of Visual Communication and Image Representation, vol. 22, no. 1, pp. 1-8, Jan. 2011, doi: 10.1016/j.jvcir.2010.08.007.
- M. Khodaei and K. Faez, "New adaptive steganographic method using least-significant-bit substitution and pixel-value [10] differencing," IET Image Processing, vol. 6, no. 6, pp. 677-686, Aug. 2012, doi: 10.1049/iet-ipr.2011.0059.
- G. Swain, "A steganographic method combining LSB substitution and PVD in a block," Procedia Computer Science, vol. 85, pp. [11] 39-44, 2016, doi: 10.1016/j.procs.2016.05.174.
- A. Pradhan, K. R. Sekhar, and G. Swain, "Digital image steganography using LSB substitution, PVD, and EMD," Mathematical [12] Problems in Engineering, vol. 2018, pp. 1-11, Sep. 2018, doi: 10.1155/2018/1804953.
- [13] G. Swain, "Adaptive pixel value differencing steganography using both vertical and horizontal edges," Multimedia Tools and Applications, vol. 75, no. 21, pp. 13541-13556, Nov. 2016, doi: 10.1007/s11042-015-2937-2.
- A. Pradhan, K. R. Sekhar, and G. Swain, "Adaptive PVD steganography using horizontal, vertical, and diagonal edges in six-pixel [14] blocks," Security and Communication Networks, vol. 2017, pp. 1–13, 2017, doi: 10.1155/2017/1924618.
- [15] T. C. Lu, "An interpolation-based lossless hiding scheme based on message recoding mechanism," Optik, vol. 130, pp. 1377-1396, Feb. 2017, doi: 10.1016/j.ijleo.2016.11.176.
- [16] B. G. Kodge, "Information Security: A review on steganography with cryptography for secured data transaction," International Journal of Scientific Research in Network Security and Communication, vol. 5, no. 6, pp. 1-4, Dec. 2017, doi: 10.26438/ijsrnsc/v5i6.14.
- H. Yao, C. Qin, Z. Tang, and Y. Tian, "Improved dual-image reversible data hiding method using the selection strategy of shiftable [17] pixels' coordinates with minimum distortion," Signal Processing, vol. 135, pp. 26–35, Jun. 2017, doi: 10.1016/j.sigpro.2016.12.029.
- M. Hussain, A. W. A. Wahab, N. Javed, and K. H. Jung, "Hybrid data hiding scheme using right-most digit replacement and adaptive [18] least significant bit for digital images," Symmetry, vol. 8, no. 6, p. 41, May 2016, doi: 10.3390/sym8060041.

- [19] R. Kumar, D. S. Kim, and K. H. Jung, "Enhanced AMBTC based data hiding method using hamming distance and pixel value differencing," *Journal of Information Security and Applications*, vol. 47, pp. 94–103, Aug. 2019, doi: 10.1016/j.jisa.2019.04.007.
- [20] A. Pradhan, K. R. Sekhar, and G. Swain, "Digital image steganography based on seven way pixel value differencing," *Indian Journal of Science and Technology*, vol. 9, no. 37, Oct. 2016, doi: 10.17485/ijst/2016/v9i37/88557.
- [21] M. J. Thenmozhi and T. Menakadevi, "A new secure image steganography using LSB and spiht based compression method," *International Journal of Engineering Research & Science (IJOER)*, vol. 16, p. 17, 2016.
- [22] K. Shabnam and S. Hemachandran, "LSB based Steganography using Bit masking method on RGB planes," *International Journal of Computer Science and Information Technologies*, vol. 7, no. 3, pp. 1169–1173, 2016.
- [23] A. S. Pandit and S. R. Khope, "Review on image steganography," International Journal of Engineering Science, p. 6115, 2016.
- [24] R. Bhuvanya, K. Vijayalakshmi, S. Uma, and A. Suresh, "Secret data sharing using steganography and image processing," *International Journal of Engineering and Technology (UAE)*, vol. 7, no. 1.7, pp. 100–104, Feb. 2018, doi: 10.14419/ijet.v7i1.7.9584.
- [25] M. M., A. A., and F. A., "An improved image steganography method based on LSB technique with random pixel selection," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 3, 2016, doi: 10.14569/ijacsa.2016.070350.
- [26] B. Datta, U. Mukherjee, and S. K. Bandyopadhyay, "LSB layer independent robust steganography using binary addition," *Procedia Computer Science*, vol. 85, pp. 425–432, 2016, doi: 10.1016/j.procs.2016.05.188.

BIOGRAPHIES OF AUTHORS



Jayeeta Majumder D SI SE D is an Assistant Professor of department of CSE of Haldia Institute of Technology. She has achieved M. Tech in Computer Science in 2009 from WBUT; West Bengal.Her research area is information Security. At present, she is pursuing PhD from KIIT University on image steganography. She is an author of more than 15 research papers in journal and conferences. She can be contacted at email: jem2003_kolkata@yahoo.co.id.

Dr. Chittaranjan Pradhan D S S P is an Associate professor of KIIT University, Odissa. He has been awarded PhD degree from the KIIT university. Digital watermarking is his research interest. At present he is the member of various professional bodies. He has more than 30 communications in journal and conference and book chapter. He reviewed many research papers. He can be contacted at email: chitaprakash@gmail.com.

