ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

Efficient Image Steganography Using Advanced Pixel Value Differencing

Riddhiman Ghosh[1], Jai Pratap Dixit[2]

Assistant Professor, Dept. of Information Technology, Ambalika Institute of Management & Technology, Lucknow, India [1, 2]

ABSTRACT: Steganography is refer as hiding the information transmitting from sender(s) to receiver(r) and making invisible in the communication process. Now days hiding confidential data in digital images using the pixel-value differencing (PVD) method became very popular and efficient. This technique provides higher embedding capacity without very noticeable changes in the cover image. This paper includes technique, which based on pixel value differencing and also pixel value sum process. This change is so negligible that human eyes can't detect it. The presence of hidden data can be revealed by a number of automatic approaches that can detect differences in statistical properties of the image due to embedding. One of the widely used approaches is histogram analysis. This proposed design is used for embedding large amount of data or data sets by changing the difference between two pixels, by which we also can able to increase the embedding capacity in Steganography. We tried to enhance the embedding capacity in a cover image using PVD in this work.

KEYWORDS: Steganography, Security, Capacity, Image Quality, Pixel-value-differencing, histogram analysis, RGB, PSNR.

I. INTRODUCTION

At present time, the Internet provide a common communication channel in worldwide so Communication media in public system means that there are different problems need to be faced time to time, such as copyright protection, data security etc.

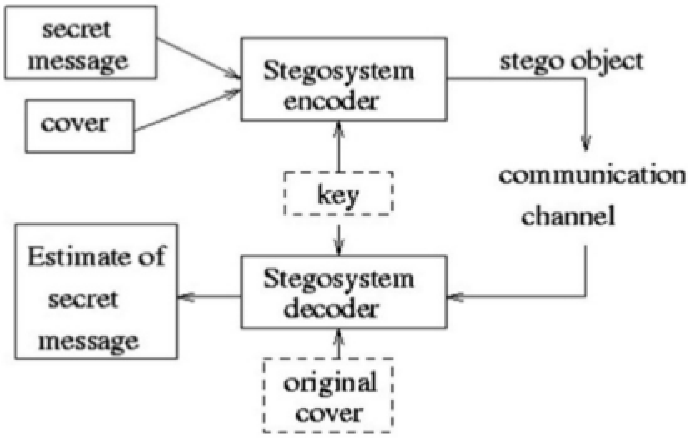


Fig 1: Basic Steganography Model

Data Ciphering is a well known process for security protection but it has the disadvantage of making a data or message unreadable thereby attracting the attention of eavesdroppers. This makes steganography which hides data within data a good choice for secret data communications. Security measurement has become very important and necessary issue in the age of digital transmission of information using Internet. Two schemes are used to protect secret messages from being captured during transmission.

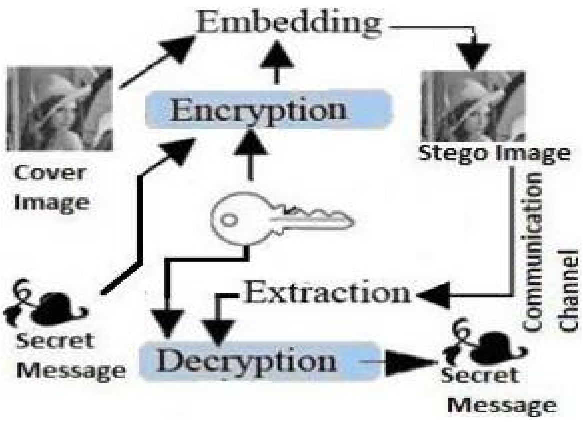


Fig 2: Secret Communication Channel

First one is encryption where the secret information is encrypted in another form by using public key before sending, which can only be decrypted with secret keys. The most used encryption techniques are DES, RSA etc. Other one is steganography which is a technique of hiding secret information into any other media or carrier known as cover media. If the cover media is a digital image, it is called cover image and the cover image with hidden data is called stego-image. Steganography can be used in military, commercial, anti-criminal and so on. There are various steganography techniques available where a digital image is used as a carrier. Wu and Tsai [1] proposed a new scheme to hide more data with outstanding quality of stego-image pixel-value-differencing (PVD) method. Thereafter, based on PVD method various approaches have been proposed [3, 4, 5, 8, and 10]. In this paper, a steganographic approach on colour images, using PVD has been proposed. The colour pixel-components may exceed the range 0~255 in the stego image when applying PVD method. In the proposed method a digital colour image has been used as a cover image. In this method more data can be hidden and also better stego image quality than Wu-Tsai's method.

II. LITERATURE REVIEW

The LSB is the lowest significant bit in the byte of each pixel in the image. This steganography embeds the secret information in the least significant bits of pixel values of the cover image. [24]This type of embedding procedure is quite simple. It requires eight bytes of the pixels to store 1 byte of the secret data i.e. LSB. Rest of the bits in the pixels remains the same. Suppose the first eight pixels of the original image have the following gray scale values: 11010010 01001010 10001100 00010101 01010111 00100110 01000011. The letter C whose binary value is 1000001. To hide this binary value it can replace the LSBs of these pixels to have the following new gray scale values: 11010011 01001010 10001100 00010100 01010110 00100111 01000011. In this example, the underlined LSB's of the pixel values has been changed. The difference between the cover (i.e. original) image and the stego image is difficult to observe by human eye.

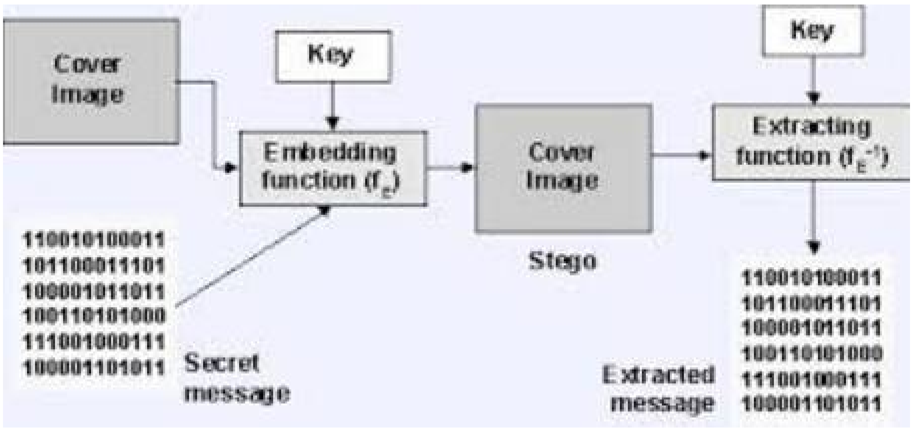


Fig 3: Stego Image with LSB structure

In this method, the secret data is embedding in the cover image. The cover image pixels and secret data is given. To hide the data by PVD, the difference value di is calculated from the two consecutive pixel values pi and pi+1 i.e. i 1 p i p i d . Then the various ranges is defined for 0-255 value such that Ri [li , ui] and li<di
The pixel value pi and pi+1 can be modified as:

$$(p'_i, p'_{i+1}) = \begin{cases} p_i + \left[\frac{m}{2}\right], p_{i+1} - \left[\frac{m}{2}\right], if\ p_i \geq p_{i+1} and\ d'_i > d_i \\ p_i - \left[\frac{m}{2}\right], p_{i+1} + \left[\frac{m}{2}\right], if\ p_i < p_{i+1} and\ d'_i > d_i \\ p_i - \left[\frac{m}{2}\right], p_{i+1} + \left[\frac{m}{2}\right], if\ p_i \geq p_{i+1} and\ d'_i \leq d_i \\ p_i + \left[\frac{m}{2}\right], p_{i+1} - \left[\frac{m}{2}\right], if\ p_i < p_{i+1} and\ d'_i \leq d_i \end{cases}$$

Where $m = |di' - di|$

All the pixel values according to the difference value are set and hence the secret data is embedded. The pixel value differencing method is proposed previously by using different approaches. Wu and Tsai [11] proposed a steganography scheme for gray level images in 2002 to improve the quality of the Stego-image, which utilized the Human Visual System sensitivity to intensity variations from smoothness to high contrast by the selection of the width of the range which the difference value of two neighbor pixels belongs to. [12] Proposed a method which improves the visual quality of the PVD method. It also estimate the falling off problem.PVD issued for secret data embedding for each component(Red, Green and Blue) separately. Variable number of bits are embedded in each pixel for proving the secured transmission. [13] Provide the another steganographic method which is based on the pixel value differencing scheme discussed in [11] and [31]. The data is embedded in this method by embedding the secret message in odd pixel pairs and the additional details were stored in even pixel pair. [25]This method improved the image quality and also the compression ratio. Han ling et al. [14] proposed a method for steganography which uses the largest pixel value between the other three pixels close to target pixel to estimate the no of bits that can be embedded in that target pixel. The method enhances the image quality and increased embedding capacity.

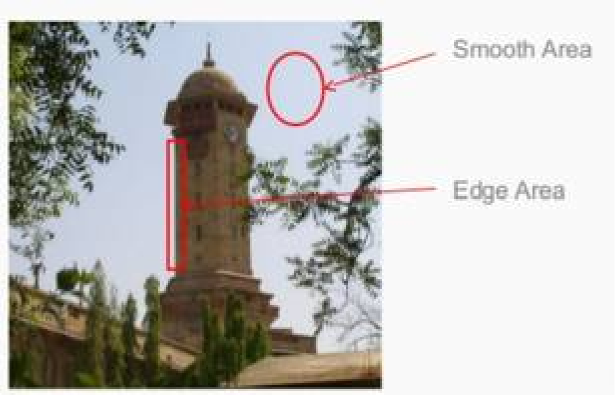
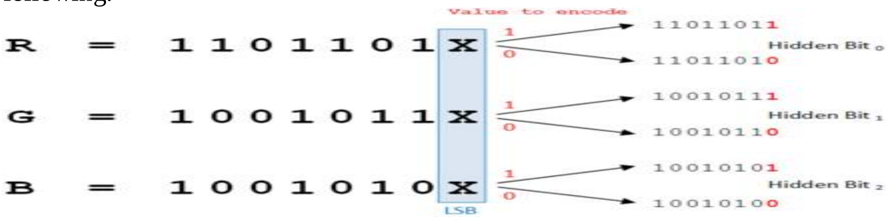


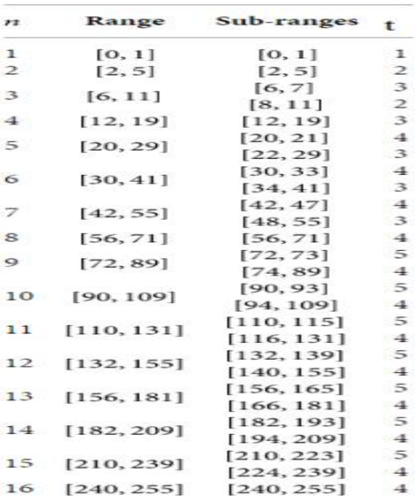
Fig 4: Pixel Value Differencing

In PVD method [1], grey scale image has been taken as a cover image with a long bit-stream as the secret data. At first the cover image is divided into non-overlapping blocks of two consecutive pixels, p_a and p_{a+1}. From each block the ifferencing value d_a is evaluated by subtracting p_a from p_{a+1}. [22]The set of all differencing values may range from -255 to 255. Therefore, $|d_a|$ ranges from 0 to 255. [19] The blocks with lesser differencing value known as smooth area where block with large differencing values are the sharp edged area. According to the capability of vision of human eye, eyes can’t detect changes in sharp-edge area easily than smooth area. So, more data can be embedded into edge area than smooth areas. Therefore, in PVD method a range table has been prepared with n contiguous ranges R_i (where i=1, 2,3… n) where the range can be 0 to 255. The lower and the upper bound are denoted as l_i and u_i respectively, then $R_i \in [l_i, u_i]$. The width of R_i is evaluated as $w_i=u_i-l_i+1$.w_i defines how many bits can be hidden in a pixel block. For more security purpose R_i is kept as a variable, as a result. Original range table is required to extract the embedded data. RGB pixel value as the following.



III. PROPOSED APPROACH

Surveying the overall previous works on Steganography pixel value differencing method, there are few areas at where some modify can be made to make the procedure more relevant. The modification or some more work can be done on embedding and extracting areas. Here using modified pixel value differencing method, three secret images are hidden in a single cover image in three colour channels sequentially red, green and blue. Just the domain of three colour channels is specifically defined. The image is hidden in cover is extracted in a reversible manner. The locations the stored or remembered to extract the secret data and the amount of bits of that data is also calculated in reversible manner. The output after extraction is primarily received in binary form, and then it is changed in decimal form to get original hidden data. We here followed and taken the Wu-Tsai’s Calculation part for completing our work.Here we are using Data Embedding and Data extraction as per specified images
For embedding the hide data, we are using color in different image. The embedding procedure is as the following.



n	Range	Sub-ranges	t
1	[0, 1]	[0, 1]	1
2	[2, 5]	[2, 5]	2
3	[6, 11]	[6, 7]	3
		[8, 11]	2
4	[12, 19]	[12, 19]	3
5	[20, 29]	[20, 21]	4
		[22, 29]	3
6	[30, 41]	[30, 33]	4
		[34, 41]	3
7	[42, 55]	[42, 47]	4
		[48, 55]	3
8	[56, 71]	[56, 71]	4
9	[72, 89]	[72, 73]	5
		[74, 89]	4
10	[90, 109]	[90, 93]	5
		[94, 109]	4
11	[110, 131]	[110, 115]	5
		[116, 131]	4
12	[132, 155]	[132, 139]	5
		[140, 155]	4
13	[156, 181]	[156, 165]	5
		[166, 181]	4
14	[182, 209]	[182, 193]	5
		[194, 209]	4
15	[210, 239]	[210, 223]	5
		[224, 239]	4
16	[240, 255]	[240, 255]	4

Table I: The quantized range table based on perfect square number

Here we are using Data Embedding and Data extraction as per specified images

A. Data Embedding: There are the following steps

- Read the cover image and partition it into non overlapping blocks of two consecutive pixels.
- Insert the secret key by XORing the LSB with the 7th bit in each pixel.
- Determine the capacity of pixels in the image.
- If there is a match i.e. the XOR value is 0. Embed the n bits of secret message directly using Pixel value sum and Differencing.
- Otherwise data is inverted before embedding.
- Repeat the procedure until all the secret data bits is embedded.
- Data is written in the form of image file to obtain a Stego-image.

B. Data Extraction : There are the following Steps as

- Open the Stego-image and again partition it into non-overlapping blocks of two consecutive pixels. 2. Apply the secret key.
- XOR the LSB with 7th bit of each pixel.
- If the XOR value is 0. Extract the n bits of the secret data directly.
- Otherwise the data is first extracted and the reverse of the string is done in order get the correct data. 6. Repeat the procedure until all the bits of the secret data are extracted.

IV. MODIFIED PVD ALGORITHM

A. EMBEDDING ALGORITHM:

- The cover image is taken and the domain of its three colour components red, green and blue is defined. Then a single hiding image is taken for every colour component. Then the particular colour component of the cover image is selected for embedding.
- Now the length of the secret or hiding image is converted from decimal to binary form and the first 20 bits of the original bit stream is taken as input and 7 bits from that stream is used from embedding at a single time.
- Before embedding some calculations have to be performed to make it simpler and efficient manner, such as- difference between two consecutive pixels(d_i), lower and upper bound of every colour component, the range

DOI: 10.15680/IJIRCCE.2016. 0412059

table, and new difference value to calculate the new pixel values in case of overflow and underflow situation occurrence.

Evaluation work:

a. Calculate the difference values d_a of two consecutive pixels p_a and p_{a+1} for each block of the cover image. This is denoted by

$$d_a=|p_{a+1}-p_a|.$$

b. Calculate the optimal range where the difference lies in the range table by using d_a. This is calculated as

$R_i = \min(u_i - d_a)$, where $u_i \geq d_a$ for all $1 \leq i \leq n$

c. Calculate the number of bits "t" can be hidden in a pixel block can be defined as $t= \lfloor \log2\ wi \rfloor$.
Where w_i is the width of the range in which the pixel value difference (d_a) is belonging to $[w_i=u_i-l_i+1]$

d. Take "t" bits from binary secret data and convert it into its corresponding decimal value b.
For instance if t=0101, then b=5

e. Calculate the new difference value d_a' which is given by $d_a'=l_i+b$

f . Modify the values of p_a and p_{a+1} by the following formula:

$$(p_a,p_{a+1}) = (p_a+m/2,p_{a+1}-m/2), \text{if } p_a \geq p_{a+1} \text{ and } d_a'>d_a$$
$$(P_a,p_{a+1})=(p_a-m/2,p_{a+1}+m/2), \text{if } p_a<p_{a+1} \text{ and } d_a > d_a'$$
$$(P_a,p_{a+1})=(p_a-m/2),p_{a+1}+m/2), \text{ if } p_a \geq p_{a+1} \text{ and } d_a' \leq d_a$$
$$(P_a,p_{a+1})= (p_a+m/2, p_{a+1}-m/2), \text{ if } p_a<p_{a+1} \text{ and } d_a' \leq d_a$$
$$\text{Where } m=|d_a'-d_a|$$

Now we get the pixel pair (p_a',p_{a+1}') after embedding the secret data into pixel pair (p_a,p_{a+1}). Repeat steps (4.a - 4.f) until all secret data are embedded into the cover image. After embedding all the secret data we get the stego-image. When extracting the hidden information from the stego-image, original range table is needed. At first divide the stego-image into pixel blocks, having two consecutive non-overlapping pixels each. Calculate the difference value for each block as $d_a'=|p_a'-p_{a+1}'|$. Then find the optimum range R_i of d_i'. Then b' is obtained by subtracting l_i from d_i'. Convert b' into its corresponding binary of "t" bits, where $t= \lfloor \log2\ w_i \rfloor$. These t bits are the hidden secret data obtained from the pixel block(p_a',p_{a+1}').

B EXTRACTION ALGORITHM :

- The stego-image is taken and the colour component in which embedding was done is selected and domain is defined again.
- Using the same previous calculations done in embedding and the conditions used in embedding, the consecutive pixel values between which the embedding is done is calculated. If overflow or underflow conditions aroused in case of embedding then these conditions are also checked.
- After getting the pixel values, now the pixel value difference can be calculated. With this value and the width of range table calculated previously along with the other calculations the amount of data or the number of bits embedded is calculated.
- Now the bits are converted into decimal and reshaped to get the original hidden message or secret message which was embedded.

V. RESULTS

The PSNR calculates the peak signal-to-noise ratio, among two images, in unit of decibels. This ratio is often used for measurement of quality between the original and a duplicate image. The better the quality of the reconstructed image as the PSNR value lies in higher side. The **Mean Square Error (MSE)** and the **Peak Signal to Noise Ratio (PSNR)** are the two error metrics used to evaluate image compression quality. The MSE defines the cumulative squared error between the duplicate and the original image, whereas PSNR value defines a measure of the peak error. The rate of error becomes lower as the MSE value becomes lower.

To evaluate the PSNR, the block first calculates the mean-squared error using the equation below:

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M * N}$$

In the equation, *M* and *N* are the number of rows and columns in the input images, respectively. Then the PSNR is evaluated using the following equation:

$$PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right)$$

In the previous equation, *R* is the maximum deviation in the input image data type. For example, if the input image has a double-precision floating-point data type, then *R* is 1. If it has an 8-bit unsigned integer data type, *R* is 255, etc.

Three different size images are taken for embedding and extraction for different colour components using our method. The value of MSE is low in case of lower size files and PSNR value is high at the same time.

	Value of MSE	PSNR
Red	0.0817	59.0450
Blue	0.0320	63.1091
Green	0.0024	74.2748

Table 2: Differencing MSE and PSNR value of RBG

Fig:5 Differencing RGB and Gray Scale Cove Images

VI. DISCUSSION AND CONCLUSION

Here we divided the cover image into 3 components region (red, blue, and green) spatially and three different hiding data (image) or secret data (image) are hidden in the cover image. A single secret data is hidden in every colour component of cover image. Thus the amount of data to be stored in a cover image is increased and number of data to be hidden is also increased which tends to our main goal which is to increase the total capacity of secret data to be hidden. In future we are trying to enhance the capacity of hiding secret data (image) and multiple images to be hidden in each colour component of a single cover image.

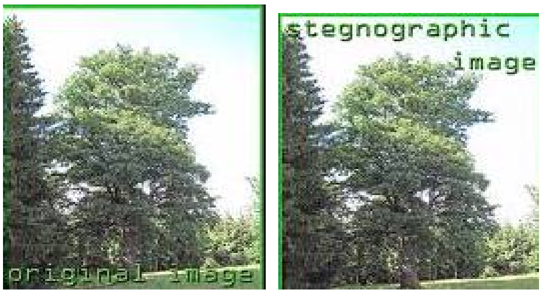


Fig 6: Original and Steganographic Images

In this paper, we have discussed a Steganographic method for data hiding by using quantized tange table and local area pixel differencing. Experimental results show the proposed scheme has a much better performance than Tseng‟s scheme in terms of stego-image quality. The Steganographic capacity and imperceptibility represent the most important aspects of any steganography technique. Thus, this paper addresses and improves these two fundamental aspects of digital steganography methods: Steganographic capacity and stego image quality. This research proposed novel steganography methods in order to increase the Steganographic capacity and enhance the imperceptibility (i.e. stego image quality).

REFERENCES

1. H.C. Wu, N.I. Wu, C.S. Tsai and M.S. Hwang, "Image steganographic scheme based on pixel value differencing and LSB replacement method", IEEE Proceedings on Vision, Image and Signal processing, Vol. 152, No. 5,pp. 611-615, 2005.
2. Schneier B.'Applied cryptography'(John Wiley & Sons, New York, 1996, 2nd Edn.)
3. W. bender, D. gruhl, N. Morimoto, A.Lu, "Techniques for data hiding", IBM Systems Journal Vol. 35(3-4),pp. -336, 1996.
4. F.A.P peticolas, R.J Anderson and M.G. Kuhn, "Information Hiding – a Survey" proceedings of the IEEE,VOL. 87,PP. 1062-1078, 1999.
5. Y.K. Lee, L.H. Chen, "High capacity image steganographic model", IEEE Proceedings on Vision, Image and Signal processing, Vol. 147, No.3,pp. 288-294, 2000.
6. R.Z. Wang, C.F. Lin, J.C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm", Pattern Recognition Vol. 34, pp. 671-683, 2001.
7. Tseng, Y.C Chen Y.Y. Pan H.K.:'A secure data hiding scheme for binary images', IEEE Trans. Commune. , 2002, 50,pp. 1227-1231
8. C.C. Chang, J.Y. Hsiao, C.S. Chan, "Finding optimal least-significant -bit substitution in image hiding by dynamic programming strategy", Pattern Recognition Vol. 36, Issue 7,pp. 1583-1595, 2003.
9. D.C. Wu, and W.H. Tsai, "A Steganographic method for images by pixel-value differencing", Pattern Recognition Letters, Vol. 24, pp. 1613-1626, 2003.
10. C.K. Chan, L.M. Cheng," Hiding data in images by simple LSB substitution" ,pattern recognition vol. 37, Issue 3,pp. 469-474, 2004.
11. C.M. Wang, Nan-I Wu, C.S. Tsai, M.S. Hwang, "A high quality Steganographic method with pixel value differencing and modulus function", The journal of Systems and software, 2007.
12. Sukhjinder Singh, Kulbhushan Singla, Dr. Rahul Malhotra "A Robust Image Steganography Technique Using Quantized Range Table And Local Area Pixel Value Differencing"in (IJARECE) Volume 5, Issue 2, February 2016
13. J. K. Mandal and Debashis Das, "Steganography Using Adaptive Pixel Value Differencing (APVD) of Gray Images Through Exclusion of Overflow/Underflow." CCSEA, SEA, CLOUD, DKMP, CS & IT 05, pp. 93–102, 2012.
14. C. Cachin, "An Information-Theoretic Model for Steganography",in proceeding 2nd Information Hiding Workshop, vol. 1525, pp. 306-318, 1998.
15. Ker, A.D., 2007. Steganalysis of embedding in two least-significant bits. IEEE Transactions on Information Forensics and Security 2 (1), 46–54.
16. Lee, Y.K., Chen, L.H., 2000. High capacity image steganography. IEE Proceedings on Vision Image and Signal Processing 147 (3), 288–294.
17. Li, X., Yang, B., Cheng, D.F., Zeng, T.Y., 2009. A generalization of LSB matching. IEEE Signal Processing Letter 16 (2), 69–72.
18. Liu, J.C., Shih, M.H., 2008. Generalizations of pixel value differencing steganography for data hiding in images. Fundamenta Informaticae 83 (3), 319–335.
19. Wang, C.M., Wu, N.I., Tsai, C.S., Hwang, M.S., 2008. A high quality Steganography method with pixel-value differencing and modulus function. Journal of Systems and Software 81 (1), 150–158.
20. S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain, "A New Approach for LSB Based Image Steganography Using Secret Key", Proceedings of 14th International Conference on Computer and InformationTechnology, Bangladesh, 2011.
21. Da-Chun Wu , Wen-Hsiang Tsai, "A steganographic method for images by pixel-value " Pattern Recognition Society, Published by Elsevier Science,pp. 1613-26, 2003.
22. J . K. Mandal and Debashis Das "Colour Image Steganography Based On Pixel Value Differencing In Spatial Domain" IJIST Vol.2, No.4, July 2012.
23. Himakshi, Verma,H.K., Singh, R.K., Singh,C.K., " Bi Directional pixel-value differencing approach for RGB Color Image.",Proceeding of IEEE, 2013.
24. Han-ling Zhang , Guang-zhi Geng and Cai-qiong Xiong " Image Steganography using Pixel-Value Differencing" Second International Symposium on Electronic Commerce and Security ,IEEE, 2009.
25. Champakamala, B.S, Padmini.K and Radhika DK "Least Significant Bit algorithm for image steganography" IJACT Vol 3, No. 4, pp. 34-38, 2011.
26. V. S. Shirguppi, "A Novel Approach for hiding data in Image Steganography by using Three Pixel Pair Differencing Method", International Journal of Advanced Research in Electronics and Communication Engineering , Vol. 4(12), pp. 2886-89, 2015.
27. A. Tyagi, R. Roy, S. Changder, "High Capacity Image Steganography based on Pixel Value Differencing and Pixel Value Sum," Proceeding of IEEE, 2015.
30. Ankita Sancheti "Pixel Value Differencing Image Steganography Using Secret Key" IJITEE, Vol. 2(1), Dec. 2012.

BIOGRAPHY

Riddhiman Ghosh working as Assistant professor in Ambalika Institute of Management & Technology Lucknow. He received M.Tech (Software Engineering) from JIS college of Engineering, Kalyani under WBTU in year 2013. His Research Interest field are Image processing and Software Engineering.

Jai Pratap Dixit working as Assistant professor in Ambalika Institute of Management & Technology Lucknow. He received M.Tech (IT) from IIIT Allahabad 2010. His Research Interest field are data security, Image processing and Software Engineering.