International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Image Steganography using Improved Lsb-Mapping Technique with Enhanced Recovery Speed

Shyla.M.K, K.B.Shivakumar, Rajendra Kumar Das

Abstract: ***In recent days, for sending secret messages, we require secure internet. Image steganography is considered as the eminent tool for data hiding which provides better security for the data transmitted over internet. In the proposed work, the payload data is embedded using improved LSB-mapping technique. In this approach, two bits from each pixel of carrier image are considered for mapping and addition. Two bits of payload data can be embedded in one cover image pixel hence enhanced the hiding capacity. A logical function on addition is applied on 1st and 2nd bits of cover image pixel, and a mapping table is constructed which gives solution for data hiding and extraction. Simple addition function on stego pixel is performed to extract payload data hence increases the recovery speed.***
Here the secret data is not directly embedded but instead mapped and added with a number using modulo-4 strategy. Hence the payload data hidden using proposed approach provide more security and it can resist against regular LSB decoding approaches. The proposed work is implemented and tested for several gray scale as well as color images and compared with respect to parameters like peak signal to noise ratio and MSE. The proposed technique gives better results when compared and histogram of cover and stego images are also compared.

Index Terms*: *Addition function, LSB mapping, Mapping table and Recovery speed.

I. INTRODUCTION

Image and its binary data gives more information than a thousand words, hence image data hiding techniques or image steganography has become more popular now a days. Image steganography is the process where one can hide secret/payload data inside a normal image (known as carrier image) and create a new embedded image. The new embedded Stego image visually seems to be same as the original cover image but carries the payload data in it and is send to the intended receiver by means of some transmitting media/channels and hence avoids curious/suspicious activities of the hackers [1].

Image steganographic techniques are broadly divided in to two domains-spatial domains and transform domain. In the first domain, the carrier image pixel levels are altered to hide the payload data. Some of the techniques under spatial domain can be gray-level modification method, encoding method based on edges, pixel indicator techniques, and techniques that consider difference in the pixel values. In second domain, image is converted in to frequency domain and the obtained coefficients are altered to hide payload data. In this technique payload capacity may be less but they are vulnerable to statistical attacks. Some of the transformations are DFT, DCT, DWT, IWT..

While designing any steganographic techniques, it is important to consider payload capacity and security of hidden data. In most of the cases the result of steganography should be undetectable form which means that the stego image should be visually and statistically resemble to the cover image so that an hacker cannot be easily decide the hacked image as a stego image and with random analysis he should not be able to confirm it as stego image. In few applications it is require to give security hence we can make use of cryptographic enciphering algorithm using symmetric or public keys. Few areas where we can use steganographic approaches are in the secret communication of important-secret information, secure online transactions, secure internet banking etc...

Our approach in this paper is considered with high payload capacity, added security while embedding secret data and increased recovery speed. LSB mapping is considered as simple hiding method, which hides the payload data inside a cover image. If we consider two bits of cover image pixel for data hiding then the data hiding capacity can be increased. For example if carrier pixel is 10101011 and suppose if we want to hide payload data 11 in that pixel, then we need to add three to selected two bits of carrier pixel that is the carrier pixel is added with 3 and the resulted stego pixel will be 10101110. Similarly mapping with addition using modulo-4 strategy can be done for all other combinations.

Data retrieving is also based on addition function hence the recovery speed is high.

Manuscript published on November 30, 2019.
* Correspondence Author
Shyla.M.K*, Department of Electronics and communication, SSIT Tumakuru, Karnataka, India.
Dr.K.B.Shivakumar, Department of Tele-communication, SSIT Tumakuru, Karnataka, India.
Dr.Rajendra kumar Das, Principal, DRIEMS, Tangi, Cuuttok, Odisha, India

II. LITERATURE REVIEW

In modulation process, the low frequency message signal is embedded over a high frequency carrier and in the similar manner; the steganographic approaches emdeddes the payload data in to a medium called as cover medium.

Image Steganographic techniques are used for secret communication where the carrier image is used to hide payload image such that its existence should not be noticeable. While designing any steganographic algorithms, one should take care of two important things, first one is based on perception of stego image, it should be almost similar to cover image and the second one is data hiding capacity which gives the amount of payload data embedded in the cover image [2]. In the beginning, the types of media used to carry payload data are text, image, audio and video files. The most recently used cover mediums are digital images because of the availability and usage over the internet [3]. The techniques and algorithms proposed in the last decade for data hiding are based on two techniques, in the first technique, the gray scale or RGB levels of the image on which data is embedded is modified in order to hide that data and in the second technique, the payload data is embedded in the frequency domain parameters of cover image. The different frequency transformations can be in intra block and inter block correlations [4], Discrete form of Cosine functions [5], and data hiding using discreetly sampled wavelet functions [6]. In substitution techniques, lower bits are considered as random noise which will not respond quickly to any small changes in their levels and hence modification can be done on these bits to hide data [7]. In few LSB modification methods pixels of the cover image are changed in random manner and others do modification in some selected regions of cover image, few others change the value of pixel by increasing or decreasing the original pixel value [8]. LSB matching (LSB-M) is another improved version of the LSB approach where the cover image pixel is added by one if the message bit is similar to cover image pixel and similarly subtracted by one if the payload data bit is not same as that of the cover image pixel [9]. Another technique where only few carrier image pixels are changed and few stego image pixels are selected to get lossless recovery of payload information [10]. An algorithm designed [11] to improve the visual quality of embedded stego image, where the substitution of LSB bits using three modulo strategies.

Cover image is encrypted and divided in to non overlapping blocks and data hiding can be done based on pixel value differences and another method in which histogram modification in multilevel was used to embed payload data [12-14]. Other than changing or matching least significant bits of cover image pixels, one more technique which uses two adjacent pixels to hide two adjacent pixels of payload data and it is given name as LSB matching revisited[15]. But the overall embedding rate for both techniques LSB matching and revisited becomes one bit per pixel only, again gives less embedding capacity.

In order to increase the security of previous techniques LSB matching and re visited, a new technique based on payload data adaptive method was introduced in [16]. This method check whether the payload data matches with the corresponding cover image pixel or not, if it doesn't matches then correction can be done on neighboring pixels of cover image instead of searching for pixel which matches in random manner[17]. Another method on adaptive data hiding which make use of complexity region that uses 8 adjacent pixels to determine suitable region for data hiding [18].

Another steganographic approach [19], uses concept of interpolation to increase data hiding capacity with more visual clarity, histogram shifting and LSB substitution are used for data hiding. The payload data is compressed so that only few cover image pixels can be modified using bit inversion approach which alters LSBs only if they appear in certain pattern [20].

III. PROPOSED WORK

In the proposed LSB-addition technique, the cover image pixels are denoted as CI_i, Payload pixel is represented as PL_i and the corresponding stego image after embedding as SI_i, where i denotes i^{th} pixel respectively.

In this method, we are hiding 2 bits of payload data in one pixel of cover image, and modifying only one bit of cover image. In order to understand the method used in this technique, we will consider an example. Let the payload (PLi) pixel to be hidden be 11010010, carrier image pixel is CIi=10101000, then the corresponding stego pixels (SI_i) will be $SI_1 = CI_1+1$ i.e., 10101001. Table I gives the LSB-addition for few values of cover image pixels and payload data.

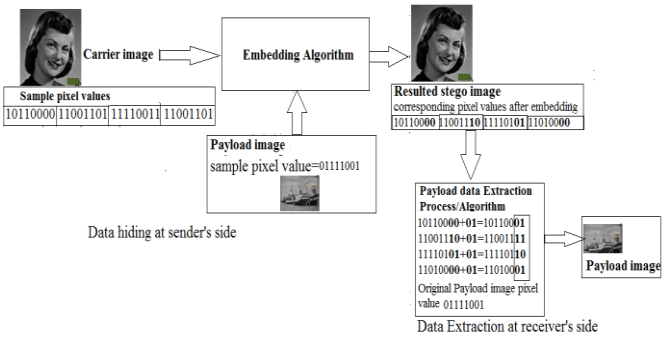

Fig1. Proposed model

The proposed model shown in fig1 consists of a carrier image and payload image as inputs to embedded algorithm/technique. Few sample pixel values for the selected portions of carrier and payload images are considered as inputs and the corresponding stego image pixel values are shown as output. The hiding technique is based on LSB-mapping with simple addition function. LSB two bits of carrier pixel are considered for addition function and the corresponding value to be added is based on the payload bits.At the receiver side, the recovery process is as shown in fig2. The stego image pixel is added with one to extract payload/secret image and results obtained for few stego pixels are tabulated in tableII.

III.a) ADDITION TECHNIQUE USED FOR DATA HIDING

Table I: LSB-Addition used for data hiding

CI_i(cover-image pixel value)	PL_i(2-bit-Payload data to hide)	SI_i(Stego-image-pixel value)	Change in cover image pixels
CI_1=10110**00**	**01**	SI_1=CI_1 (10110**00**)	No change
CI_2=11001**01**	**11**	SI_2=CI_2+1 (11001**1**0)	one bit change
CI_3=11110**11**	**10**	SI_3=CI_3+2 (11110**0**1)	one bit change
CI_4=11001**01**	**01**	SI_4=CI_4+3 (1101000**0**)	one bit change
CI_5=10101**10**	**00**	SI_5=CI_5+1 (1010101**1**)	one bit change

III.b) MAPPING TECHNIQUE USED FOR DATA EXTRACTION

Here the simple addition function is used for data recovery. TableII gives the mapping or logic used for the values of stego pixels given in the fourth column of table I. Table II shows that recovery process of stego pixel values, where we need to add one to SI_i then we can extract least significant two bit values of stego pixels and those values are equal to that of payload pixel values given in tableI.

Table II: Simple addition function used for data extraction

Sl.No.	SI_i (Stego-image-pixel value)	Addition function	Recovered payload pixel value
1	SI_1=10110**00**	SI_1+1	01
2	SI_2=11001**1**0	SI_2+1	11
3	SI_3=11110**0**1	SI_3+1	10
4	SI_4=1101000**0**	SI_4+1	01
5	SI_5=1010101**1**	SI_5+1	00

The proposed work is implemented in matlab R2017a version for many gray scale as well as color images and the histogram of those cover images and stego images are compared with existing methods.

PROPOSED ALGORITHM

At sender's side

1. Select a cover image of size C(i, j)
2. Consider a payload or secret data of size PL(i, j)
3. Select the cover image pixel for data hiding according to the improved mapping table as shown in table1
4. Embedding algorithm make changes in cover image pixels according to the payload data bits
5. Pay load data bits are considered as two bits per cover image pixel
6. Steps from 3- 5 are repeated till all the payload bits are embedded in the cover image
7. The stego image resulted with visually distortion less can be send to the receiver

At receiver's side

1. The received stego image is decoded using simple addition function as shown in tableII
2. Decoded image is exactly same as the original payload for few images with less image size and for few with good PSNR more than 75db

IV. RESULT ANALYSIS AND COMPARISIONS

The proposed work is implemented in matlab R2017a version. Many gray scale images as cover and payload images of different sizes are considered. The proposed work is also implemented on color images and the histogram of those cover images and stego images are compared with already existed methods. Results obtained for gray scale images for the proposed method are compared with previous work [21] and are tabulated in tableIII.

TableIII. Comparison between the proposed method and the existing method [21] in terms of PSNR and MSE.

Carrier image of size 256*256	Payload data size	Results from Existing method [21]		Results of the Proposed method	
		PSNR	MSE	PSNR	MSE
Lena	2KB	55.405	0187	67.973	0.0144
Baboon	4KB	52.396	0.374	67.668	0.011
Home	6KB	50.626	0.562	64.576	0.0227
Girl	8KB	49.296	0.764	63.800	0.0272
Cameraman	16KB	--	--	62.594	0.0358

The performance analysis of this work is done by visual comparison of the histograms of original images and their stego images as shown in bellow figures2-9.

The proposed technique is also implemented for color images and their results in terms of PSNR and MSE using equations 1 and 2 are tabulated in table4 and compared with other technique [22]. The color cover image of size 256*256 and payload data of 1KB is considered to hide and the corresponding images are shown in bellow figures.

$PSNR=10\log_{10}[(I^2)/MSE]$ (1)

Where I=255

$MSE=1/(mn)[x(i,j)-x^1(i,j)]^2$, for all i=1 to n and j=1 to m (2)

The work presented in this paper is also implemented for few color images their performance analysis are tabulated in terms of PSNR and MSE. Results are compared with other method [22] and values are given in table4. Original cover images of various sizes are considered with different payload capacities. Data is successfully embedded and extracted with good results.

TableIV. PSNR and MSE values for color images.

Color Cover image	Other method[22]		Proposed work		
	PSNR	MSE	PSNR	MSE	Time elapsed in sec
Lena.bmp	64.23	0.02	68.971	0.0082	4.102
Baboon.bmp	63.33	0.03	69.420	0.0074	3.875

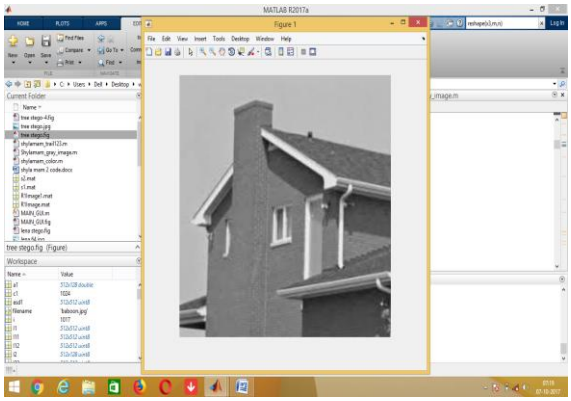

Fig.2.Carrier Home image

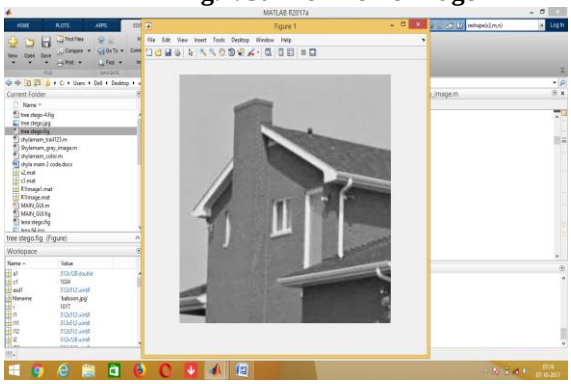

Fig.3.Stego Home image

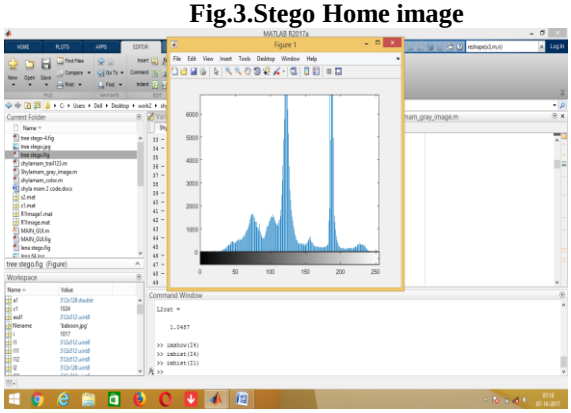

Fig.4.Histogram of Original cover Home image

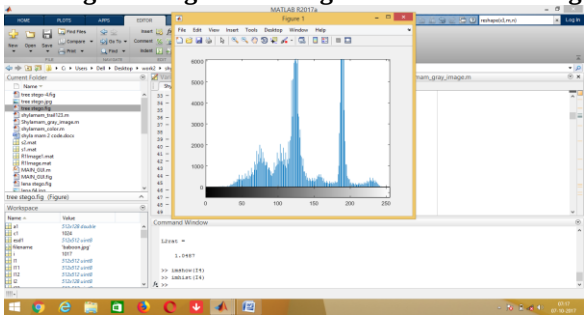

Fig.5. Histogram of stego Home image

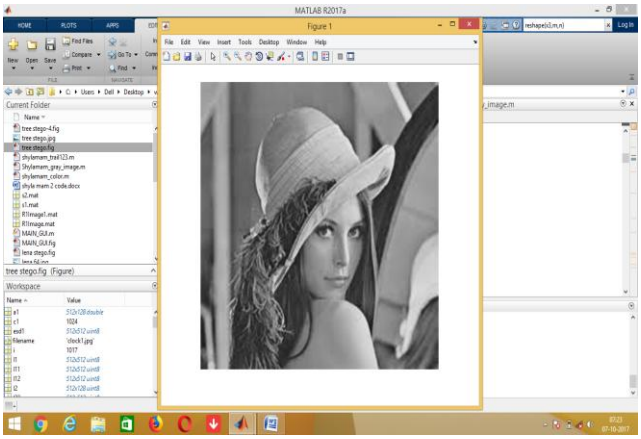

Fig.6.Carrier Lena image

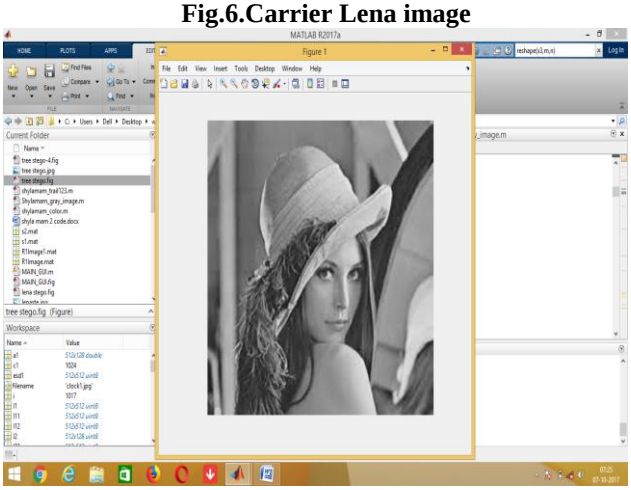

Fig.7.Stego lena image

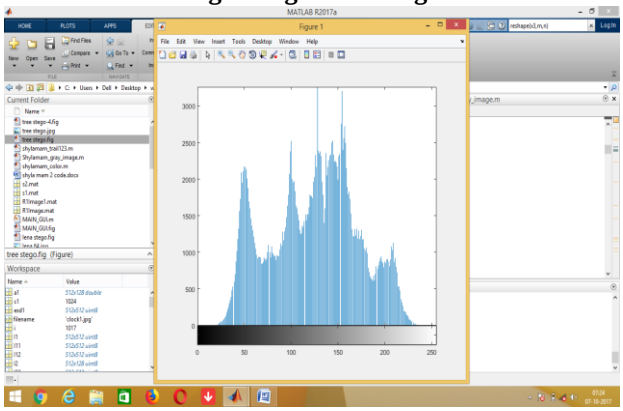

Fig.8. Histogram of carrier Lena image

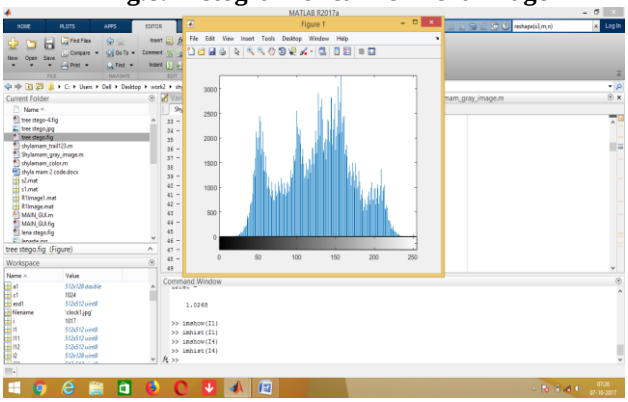

Fig.9.Histogram of stego Lena image

Retrieval Number: B3701078219/2019©BEIESP
DOI:10.35940/ijrte.B3701.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Fig.10.Baboon cover imge

Fig.11.Baboon stego imge

Fig.12.Lena cover imge

Fig.13.Lena stego imge

V. CONCLUSION

In this improved LSB mapping technique, the cover image pixels are mapped with four combinations hence uses only two bits of a cover image pixel to hide two bits payload data, hence increasing embedding capacity. For a cover image of size 256*256, we can hide 16KB data and for 512*512 cover, we can hide 64KB of payload data. Experiment is done on both color as well gray scale images. The best part of this paper is recovery speed, since we are using very simple addition function to recover payload data, and a simple four values mapping table for data hiding, time required is very less and it is approximately around 3.5 sec on an average of 150 images. For gray scale images histogram of cover and stego images are compared.

The obtained stego image is visually very less distorted image hence it is difficult to predict as stego image, since this is one of the important goal of steganographic approach, our work in this paper achieved good results both for grayscale as well as color images.

REFERENCES

1. Afrakhteh, M., & Ibrahim, S. (2010, 25-27 June 2010). Adaptive steganography scheme using more surrounding pixels. Paper presented at the Computer Design and Applications (ICCDA), 2010 International Conference on.
2. X. Zhang and S. Wang, "Steganography using multiplebase notational system and human vision sensitivity," IEEE Signal Processing Letters, vol. 12, pp. 67-70, Jan. 2005.
3. Alturki, F., & Mersereau, R. (2001, Apr 2001). A novel approach for increasing security and data embedding capacity in images for data hiding applications. Paper presented at the Information Technology: Coding and Computing, 2001. Proceedings. International Conference on.
4. C. Chen and Y. Q. Shi, "JPEG image steganalysis utilizing both intrablock and interblock correlations," in Circuits and Systems, 2008. ISCAS 2008. IEEE International Symposium on, 2008, pp. 3029-3032.
5. K. S. Kumar, K. Raja, R. Chhotaray, and S. Pattanaik, "Bit length replacement steganography based on dct coefficients," International Journal of Engineering Science and Technology, vol. 2, pp. 3561-3570, 2010.
6. S. Bhattacharyya and G. Sanyal, "A robust image steganography using dwt difference modulation (DWTDM)," International Journal of Computer Network and Information Security, vol. 4, p. 27, 2012.
7. C.-K. Chan and L.-M. Cheng, "Hiding data in images by simple LSB substitution," Pattern recognition, vol. 37, pp. 469-474, 2004.
8. Cheddad, A., 2009. Steganoflage: A new image steganography algorithm. Doctor of Philosophy Thesis, University of Ulster, Northern Ireland, UK.
9. B. Li, J. He, J. Huang, and Y. Shi, “A survey on image steganography and steganalysis”, Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, pp. 142–172, 2011
10. Chang, C.-C., Chen, W.-J., & Le, T. H. N. (2010). High payload steganography mechanism using hybrid edge detector. [Report]. Expert Systems With Applications, 37(4), 3292+.
11. Xu W-L, Chang C-C, Chen T-S, Wang L-M. 2016 An improved least-significant-bit substitution method using the modulo three strategy. Displays 42, 36–42. doi:10.106/j.displa.2016.03.002)
12. P. Jagtap, A. Joshi, and S. Vyas, “Reversible Data Hiding in Encrypted Images,” IARJSET, pp. 35–38, 2015.
13. X. P. Zhang, “Separable reversible data hiding in encrypted image,” IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 826–832, 2012.
14. Z.Pan, S.Hu, X.Ma, andL.Wang, “Reversible data hiding based on local histogram shifting with multilayer embedding,” Journal of Visual Communication and Image Representation, vol. 31, pp. 64–74, 2015.

15. C. Sumathi, T. Santanam, and G. Umamaheswari, "A study of various steganographic techniques used for information hiding", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013
16. X. Li, B. Yang, D. Cheng, and T. Zeng, "A generalization of LSB matching", IEEE Signal Processing Letters, vol. 16, no. 2, pp. 69–72, 2009.
17. C. Wang, X. Li, B. Yang, X. and Lu, C. Liu, "A content-adaptive approach for reducing embedding impact in steganography". Proc. IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP), Dallas, TX, USA, 2010, pp. 1762–1765.
18. W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on LSB matching revisited", IEEE Transactions on Information Forensics and Security, vol. 5, no. 2, pp. 201–214, 2010
19. Y. Tsai, Y. Huang, R. Lin, and C. Chan, "An Adjustable Interpolationbased Data Hiding Algorithm Based on LSB Substitution and Histogram Shifting", International Journal of Digital Crime and Forensics, vol. 8, no. 2, pp. 48–61, 2016.
20. N. Akhtar, "An LSB Substitution with Bit Inversion Steganography Method", Smart Innovation, Systems and Technologies, Springer India, vol. 43, pp 515–521, 2015.
21. Kamaldeep Joshi , Swati Gill, and Rajkumar Yadav (2018) Hindawi /Journal of Computer Networks and Communications Research Article A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image Volume 2018, Article ID 9475142, 10 pages https://doi.org/10.1155/2018/9475142
22. Mohammad Obaidur Rahman†, Muhammad Kamal Hossen (2018) JCSNS International Journal of Computer Science and Network SecurityAn Approach for Enhancing Security of Cloud Data using Cryptography and Steganography with E-LSB Encoding Technique, , VOL.18 No.9, September 2018

AUTHORS PROFILE

Mrs. SHYLA.M.K has obtained her Bachelor's degree in Electronics and communication and Master's degree in Digital Electronics from Visveswaraya technological university, Belgaum. She is a permanent member of Indian Society of Technical Education. She has three publications in national conferences and one in international conference. One of her paper is published as Lecture notes in Electrical Engineering, VOL545. Springer. Singapore.

Her field of interest includes cryptography and network security, analog communication, Steganography, Image and video processing etc..she is serving as Assistant Professor in the department of Electronics and communication, Sri Siddharthe Institue of Technology, Tumakuru .

Dr. K.B. Shiva Kumar received the BE degree in Electronics & Communication Engineering, ME degree in Electronics, MBA Degree from Bangalore University, Bangalore and M Phil Degree from Dravidian University Kuppam. He obtained Ph.D. in Information and Communication Technology from Fakir Mohan University, Balasore, He has got 35 years of teaching experience and has over 82 research publications in National and International conferences and journals. Currently he is working as Professor and Head, Dept. of Telecommunication Engineering, Sri Siddhartha Institute of Technology, Tumakuru. He is permanent member of Indian Society of

Technical Education His research interests include Signal processing, image processing, Multi rate systems and filter banks, and Steganography.

Dr. Rajendra kumar das received the BE degree in Electronics Engineering from Bangalore university, ME degree in communication system engineering from Sambalpur University, UCE,Burla, LLB from Ulkal University, MLC Baripada.He obtained Ph.D in Information and communication, Tecnology from Fakir Mohan University, Balasore and also CMI level 5 in Management & Leadership from Charted Management Institute, Dudley College, UK& AICTE, New-Delhi. He has got 22 years of teaching experience and has over 26 research publications in National and International conferences and journals. He has received 10 awards/Honours. **One of the Remarkable Achievements** is An write up on **Road map on Reformation in Quality Technical Education** has been sent to Hon'ble Prime Minister on 7.12.16 & 10.05.17 with a copy to **Hon'ble Minister, MHRD, Govt. of India**, **Chairman AICTE, New Delhi**