ISSN: 2454-4248
439 – 445

Study of Pixel Indicator Technique on SSIM and PSNR Based Parameters

Sachin
Research Scholar, Department of CSE,
U.I.E.T, M.D.U, Rohak,
Haryana, India

Abstract:-Information hiding and its security is the most challenging task in this digital environment. In this paper, an approach named P.I.T (Pixel Indicator Technique) is used to obtain the solutions of such challenges. In P.I.T, a pixel of covered image is divided into 3-channels named as R, G and B, wherein R component used as indicator and G and B as data channels. Images of dimension 512*512 are taken into experiment to hide data of different sizes 4KB, 8KB and 16KB. Further the results are analyzed in terms of PSNR and SSIM based parameters.
Keywords: *Steganography; LSB; P.I.T; PSNR; SSIM*

*****

1 INTRODUCTION AND LITERATURE SURVEY

In modern world of digital communication security of data is an utmost concern. To achieve the security of data either we can use cryptography or steganography. The prior one scrambles the data which makes an attacker to decrypt it while the latter one conceals the message in any of carrier mediums like images, videos, audios and so on. So it provides a better option without getting know the concealed message in any of the above medium [1, 2, 17, 18 ,19]. Many techniques are present in history to hide the data. The simplest one is LSB approach wherein data is hidden at LSB of every pixel. So this technique not only easy to implement but also provides better PSNR [3, 20, 21, 22, 23]. Joshi et. al [4] implemented a steganography algorithm using LSB approach and investigated the results over different images concealing varying amount of data . Lou et. al [5] presented an approach to check whether the message bit is same as image bit or not based on addition or subtraction of 1. Wang et. al [6] provided a technique to hide data on a bit that is moderately significant. Joshi and Allwadhi [7] gave a GLM based technique over medical image system wherein data is hidden in various medical images like X-Rays, CT-scans, and MRIs and so on. Muhammad et. al [8] gave a spatial domain technique wherein an image is converted into HSI color space and the I plane is subdivided into four regions in which data is stored based on some secret key. Joshi et. al [9] provided a technique over spatial domain for the robustness of watermark when the stego image is suffered from salt and pepper noise. Chang and Chen [10] provided an approach based on adjustment of pixel for obtaining a better quality image. Rao and Kumari [11] provided an authentication algorithm using watermarking technique in medical images. Avci et. al [12] projected a stegaongraphic algorithm in transform domain based on probabilistic XOR method.

2 P.I.T METHOD AND EXPERIMENTAL RESULTS

This technique best suites for RGB images wherein capacity of payloads and security of data is increased by dividing the RGB image into two channels named as Indicator and data channels. Every pixel has one indicator and two data channles corresponding to three components i.e R, G and B. Two LSBs of Indicator chann el indicates that on which data channel (either G or B) data bits are to be stored. Here it is assumed only two bits are stored as LSB data bits for every data channel. **S**o it not only increases the payload capacity but also security by dividing the RGB-image into channels unlike simple LSB approach. PIT can be demonstrated by the following example if both the bits of indicator channel (say R) = 00 then both the data channel**s** (G and B) store nothing In the experiment a cover media as a Host colored image i.e $H = \{ h_{rc} \mid 0<=r< R_H , 0<=c<C_H \}$ and $h_{rc} = \{R_{rc}, G_{rc}, B_{rc}\}$, where each of the pixel's component i.e R_{rc} , G_{rc} and B_{rc} ε {0, 1 , 2, ……………, 255} and data to be concealed in this image H is

ISSN: 2454-4248
439 – 445

$D=\{d_i \mid 0<=k<l , d_i \varepsilon \{0,1\}\}$ where l is length of message. Insertion procedure starts from very first colored pixel (h_{00}) of which R-channel 2 LSB's are checked, if these 2-bits are 00, then nothing is stored on data channels i.e G and B components. If it is 01 and 10, then 2 message bits are stored on B channel and G channel respectively. To store data bits over both the components i.e G and B, R component's 2 LSB will be 11 as shown in following Table 1. This procedure continues until message of length 'l' is over and finally we obtain our stego image (S) i.e $S= \{ s_{rc} \mid 0<=r< R_S , 0<=c<C_S \}$ and $s_{rc} = \{Rs_{rc}, Gs_{rc} , Bs_{rc}\}$, where each of the pixel's component i.e Rs_{rc} , Gs_{rc} and Bs_{rc} ε {0, 1 , 2, ……………, 255}. Now at the receiving end message is obtained from Stego image (S) by looking the R-component's 2 LSBs starting from its very first pixel (S_{00}) when 2 LSB's are 00, we do not extract anything from any of its channel. If it is 01 or 10, we extract 2 message bits from B and G component respectively. Now if it is 11, then we retrieve 4 message bits from both the components i.e B and G as shown in following Table 2. The insertion and retrieving procedures of data are shown in figure 3 and 4 respectively. After inserting data in different host images, we retrieve the corresponding stego images as shown in Table 3 while Table 4 represents the results obtained in terms of PSNR and SSIM.

Table 1 – Example Showing Insertion Using P.I.T

R-Component (As indicator Channel)	**G-Component (As data Channel)**	**B-Component (As data Channel)**
10101000 **(00 Indicates Nothing to be Stored)**	10101111	10001011
10111101 **(01 Indicates data Stored on B Component)**	10111101	10111110
10111110 **(10 Indicates data Stored on G Component)**	10111101	10111110
10111111 **(11 Indicates data Stored on both G and B Components)**	10111101	10111100

Table 2 - Example Showing Retrieval of data Using P.I.T

R-Component (As indicator Channel)	**G-Component (As data Channel)**	**B-Component (As data Channel)**
10101000 **(00 Indicates Nothing to be Stored)**	10101111	10001011
10111101 **(01 Indicates data Stored on B Component)**	10111101	10111110
10111110 **(10 Indicates data Stored on G Component)**	10111101	10111110
10111111 **(11 Indicates data Stored on both G and B Components)**	10111101	10111100

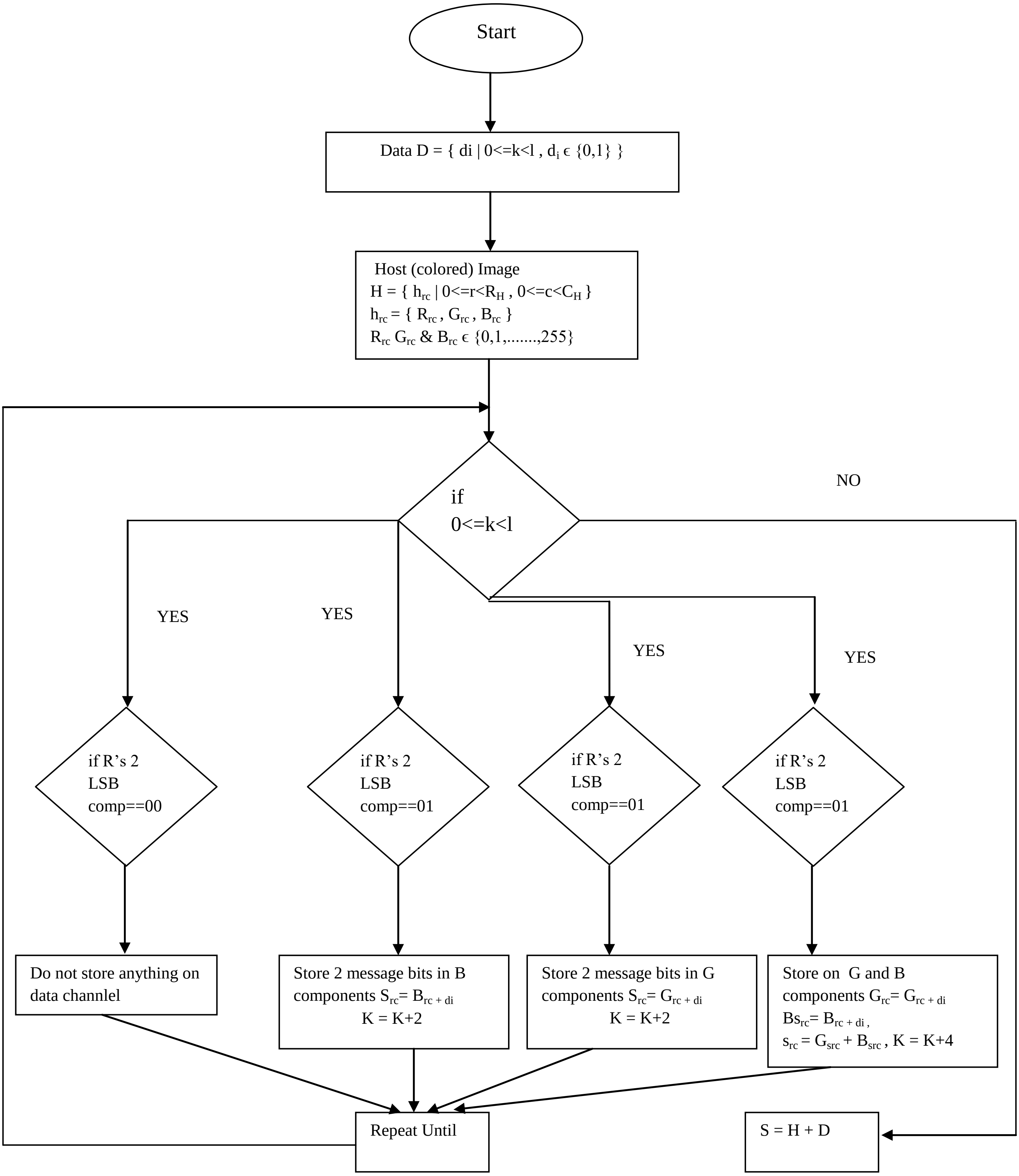

Fig. 1

Insertion Flowchart

ISSN: 2454-4248
439 – 445

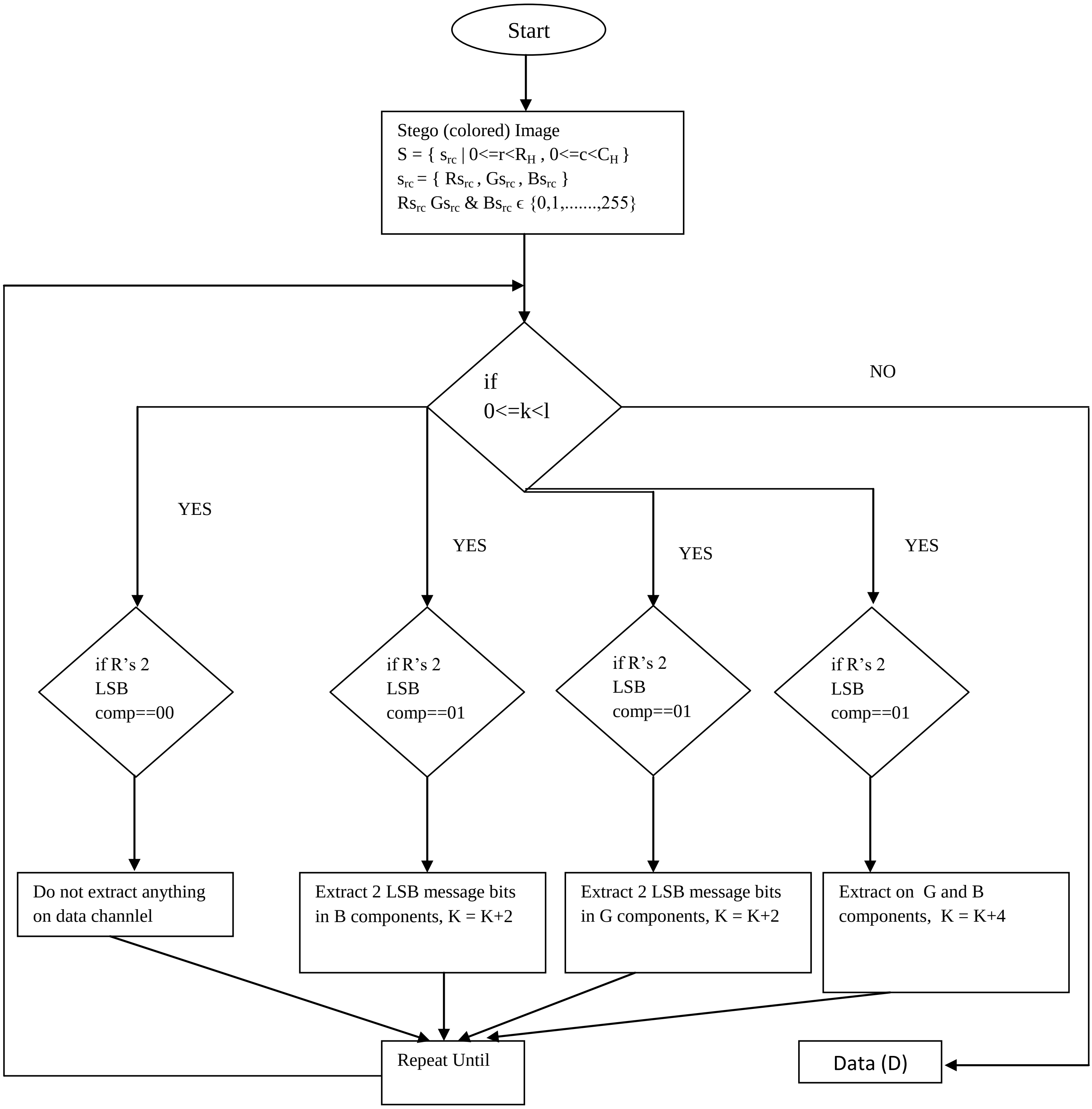

Fig.2 Retrieval Flowchart

ISSN: 2454-4248
439 – 445

3 PSNR AND SSIM

Peak Signal to Noise Ratio (PSNR) used as the similarity index between host and stego image and is given as:

$$\text{PSNR} = \mathbf{10\log_{10}}\left[\frac{I^2}{MSE}\right] \tag{1}$$

Structure SIMilarity Index (SSIM) is a method for measuring the similarity between two images. The SSIM index can be viewed as a quality measure of one of the images being compared provided the other image is regarded as of perfect quality [14]. σx, σy, σxy, μy, and μx refer to some local parameters that are related to statistics[15, 16].

$$SSIM(C,S) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^{\ 2} + \mu_y^{\ 2} + C_1)(\sigma_x^{\ 2} + \sigma_y^{\ 2} + C_2)} \tag{2}$$

Table 3 – PSNR and SSIM of 512*512 Stego Images

Image No.	Data Size = 8KB		Data Size = 16KB		Data Size = 32KB	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Image 1	48.98	0.9848	50.10	0.9696	47.15	0.9581
Image 2	52.58	0.9799	46.97	0.9795	46.01	0.9595
Image 3	52.55	0.9993	45.51	0.9794	44.35	0.9693
Image 4	53.88	0.9754	47.31	0.9898	45.93	0.9794
Image 5	49.65	0.9692	46.56	0.9693	44.23	0.9496
Image 6	50.92	0.9869	48.37	0.9791	45.28	0.9497
Image 7	51.85	0.9823	49.92	0.9692	46.61	0.9398
Image 8	50.45	0.9689	48.37	0.9695	46.39	0.9394
Average of 100 images	**51.35**	**0.9808**	**47.88**	**0.9756**	**45.74**	**0.9556**

Table 4 - 512*512 Host and Stego images

Sr. No	Host Images	Stego-images		
		Hiding 8KB data	Hiding 16KB data	Hiding 32KB data
Image 1				
Image 2				

ISSN: 2454-4248
439 – 445

Image 3				
Image 4				
Image 5				
Image 6				
Image 7				
Image 8				

4 CONCLUSION

Data can be hidden using steganography for different purposes and using different techniques. Out of these techniques P.I.T is one of the basic techniques. Here in this paper, data of sizes 8KB, 16KB and 32KB are embedded into colored images of dimension 512*512 and experimental results are analyzed in terms of PSNR and SSIM based factors. Further it is found that average PSNR over 8KB, 16KB and 32KB data is 51.35, 47.88 and 45.74 respectively and overall SSIM nearly approached to 1, which tells recovered data is almost correct.

REFERENCE

[1] N.F Johnson and S. Jajodia, "Exploring steganography seeing the unseen" Computer (Long, Beach, Calif) vol. 31 no. 2 1998

[2] Amirtharajan R, Archana P, Rajesh V, Devipriya G, Rayappan J (2013) Standard deviation converges for random image stegaongraphy. In: Information & Communication Technologies (ICT), 2013 I.E Conference on. Pp 1064-1069

[3] R. Yadav, "Study of Information Hiding Techniques and their Counterattacks: A Review Article", International Journal of Computer Science & Communication Networks, Vol. 1, (2011), pp. 142-164.

[4] K. Joshi, R. Yadav, S.Allwadhi, " PSNR and MSE based Investigation of LSB" in the proceedings of IEEE, International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), pp. no. 178 -183 on March 11-13, 2016

[5] Luo W. Huang F. Huang J (2010) Edge adaptive image steganography based on LSB matching revisited. Inform Forensic security IEEE Trans 5:201-221, 2010.

[6] Wang R-Z, Lin C-F, Lin J-C, "Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recogn", 34:671-683, 2001.

[7] K. Joshi and S. Allwadhi, "Image Steganography Model for Medical Images Using GLM" in Journal of COMPUSOFT, An International journal of advanced computer technology, pp. 2120 – 2124 5(5), May – 2016 (Volume –V, Issue-V) ISSN:2320-0790

[8] K. Muhammad, M.Sajjad, I.Mehmood, S.Rho, S.Baik, "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image" Springer Science and Business Media, DOI 10.1007/s11042-015-2671-9, 2015

[9] K. Joshi, R. Yadav, S.Allwadhi, “Exploration of Least Significant Bit Based Watermarking and its Robustness against Salt and Pepper Noise” in Journal of World Academy of Science Engineering and Technology (WASET), Vol 10, No 7, Paper No. 213, 2016.

[10] Chan C-K, Cheng L-M, “Hiding data in images by simple LSB substitution”. PatternRecogn 37:469-474

[11] N.V Rao and V.Kumari, “Watermarking in Medical Imaging for security and Authentication” Taylor & Francis DOI 10.1080/19393555.2011.561154, vol 20 pp 148-155, 2011

[12] E. Avci, T.Tuncer, D.Avci, “A Novel Reversible Data Hiding Algorithm Based on Probabilistic XOR Secret Sharing in Wavelet Transform Domain” Springer. DOI 10.1007/s 13369-016-2124-4, 2016.

[13] M. Aziz, M.H Tayarani-N and M. Afsar, “A cycling chaos-based crptic-free algorithm for image steganography” Nonlinear Dyn. Vol 80. No. 3. pp 1271-1290, 2015.

[14] Z.Wang, A.C.Bovik,H.R. Sheikh,E.P.Simoncelli, “Image Quality Assessment: From Error Visibility to Structural Similarity”, IEEE Transaction on Image Processing Vol 13, No 4, pp 600-612, 2004.

[15] M. Sajjad, N. Ejaz, and S. W. Baik, "Multi-kernel based adaptive interpolation for image super-resolution," Multimedia Tools and Applications, pp. 1-23, 2012.

[16] M. Sajjad, N. Ejaz, I. Mehmood, and S. W. Baik, "Digital image super-resolution using adaptive interpolation based on Gaussian function," Multimedia Tools and Applications, pp. 1-17, 2013.

[17] S. Allawadhi, S.Dhingra, “Steganography Techniques: A Survey” International Journal of Latest Trends in Engineering and Technology, pp 258-263, Vol. 8, 2017.

[18] K. Joshi, R. Yadav, "A new LSB-S image steganography method blend with Cryptography for secret communication", 2015 Third International Conference on Image Information Processing (ICIIP), pp. 86-90, 2015.

[19] K. Joshi, P Dhankhar, R. Yadav, “A new image steganography method in spatial domain using XOR”, 2015 Annual IEEE India Conference (INDICON), pp1 – 6, 2015.

[20] Joshi, Kamaldeep, Rajkumar Yadav, and Gaurav Chawla. "An Enhanced Method for Data Hiding Using 2-Bit XOR in Image Steganography." International Journal of Engineering and Technology 8.6 (2016).

[21] Saini, Anamika, Kamaldeep Joshi, and Sachin Allawadhi. "A Review on Video Steganography Techniques." International Journal of Advanced Research in Computer Science 8.3 (2017).

[22] Joshi, Kamaldeep, Rajkumar Yadav, and Ashok Kumar Yadav. "An Additive Watermarking Technique in Gray Scale Images Using Discrete Wavelet Transformation and Its Analysis on Watermark Strength." World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering 10.7 (2016): 1428-1433.

[23] Joshi, Kamaldeep, and Rajkumar Yadav. "A LL Sub Band Based Digital Watermarking in DWT." IJ Engineering and Manufacturing volume 7, Issue 2, pp 50-63 (2017).