A MODIFIED DATA STENOGRAPHY APPROACH BASED ON ROBUST LSB TECHNIQUE FOR LARGE SIZE INFORMATION HIDING CAPABILITY

[1] **K Saraswati ,** [2] **Sumit Sharma** [3]**Jitendra Agrawal**
M.Tech Scholar CSE[1], Head of Department CSE[2] , Professor IT[3]
Vashnavi Institute of Technology (VIT)[12,], School of Information Technology RGPV[3]
Bhopal [M.P.]

Abstract : In today world digital Image processing is used in many fields like computer vision, remote sensing, medical imaging, robotics, satellite images and aerial photography etc. There are different Data hiding scheme and techniques are available for shield creation. We know hackers are also updated day to day. Steganography is the fine art for encryption of the confidential data in cover media to protect such data that are hack by hacker. The main purpose of steganography is, hiding the existence of the actual communication. In steganography, data can be hidden in carriers such as image, audio files, text files and video files. Three level security is the prime objective of this Dissertation, First is provided by hiding secret message in cover image pixels that are selected on small 3x3 windows and left the pure white and black window when hide the data in cover image, second by shuffling the original message when embedding with cover image and third by using LSB method as Steganography techniques that overcome to chance of eavesdrop the secret information compare then Complemented Random Invert LSB and another LSB techniques.MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio) are two common quality measurements to measure the difference between the cover-image and the stego-image.Image-based data hiding techniques are secure but day to day size of secret data is increasing day by day.

***Index Terms* - Data Hiding, steganography Random Invert LSB and LSB.**

I. INTRODUCTION

With advancements in digital communication technology and thus the extension of PC power and storage, the complications in ensuring persons' privacy become more and harder. The degrees to that people appreciate privacy dissent from one person to another. Numerous strategies are investigated and developed to shield personal privacy. Encoding is perhaps the most obvious one, and then comes steganography. This position is kind of different from the perspective taken with cryptography as an example. Governments invested with vast money and resources to create an unbreakable encoding algorithmic program. Many of the existing approached assumes that flexibility to noise, double compression, and different image processing manipulations aren't required in the steganography context. As such, within the warden passive attack scenario their hide information will be destroyed or won't be recoverable. Adjustive steganography aimed toward distinguishing textural or quasi-textural areas for embedding the secret information runs into a few problems at the decoder aspect since its classification algorithms aren't salient. During this thesis, skin-tone areas are the preferred selection for texture detection since the detection algorithmic rule is robust and distinctive. Furthermore, skin-tone regions continuously show chrominance standards exist in on a middle range, hence, the issue of underflow or overflow is overwhelmed automatically. Within the methodology of finding out a good skin-tone detection algorithmic rule, the various accessible techniques are established to either be slow in execution and/or accompany intolerable false alarms. Often, these algorithms neglect the fact that luminance can facilitate improve their performance.

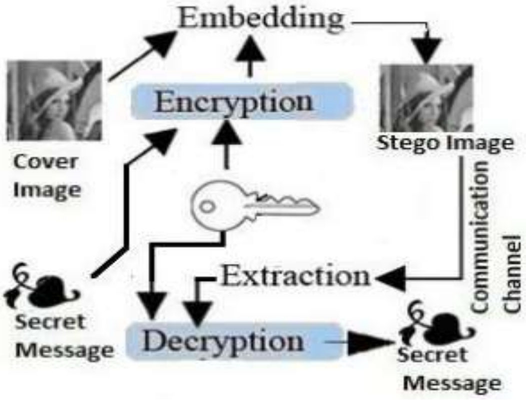

Figure. 1 Block Diagram of Steganography

This Steganography procedure is more mainstream in a late year than other Steganography conceivably on account of the surge of electronic picture data accessible with the coming of computerized cameras and fast web dispersion. It can include concealing data in the normally happened clamour inside the picture. Most sorts of data contain some sort of commotion. Clamour alludes to the defects innate during the time spent rendering a simple picture as an advanced picture. In image steganography we hide the data behind the cover image pixel .image steganography is one type of steganography for data security, where the data is hidden or embedded with the cover image using some encryption /decryption algorithm. The Attacker uses the different type of decoding method or algorithm to decode the original message from the cover image. In steganography, the original image is called a cover image, and embedded image with the message is called a stego-image. In a Data Hiding Method: a username and password are required to use the system for hiding the Data. Once the client has been login into the framework, the client can utilize the data (information) together with the mystery key to conceal the information inside the picked picture. This technique is accustomed to concealing the presence of a message by concealing data into different bearers. This keeps the identification of concealed data. Steganography is a Technical steganography utilizes exceptional devices, gadgets or logical strategies to conceal a message. In this type, one can use invisible ink, microdots, computer-based various hiding method places to keep message secret.

II. LITERATURE SURVEY

Kumar Singh at.al [2020], In this paper, Presented an , a eminent data hiding technique is developed using super pixels to ease the hiding of data at the corresponding blocks of the Cb and Cr colour components through DCT and CA. The labelled image of super pixel is taken into consideration to classify a block as heterogeneous or homogeneous. The proposed method of implementation was found to be more optimal than the four possible methods after making a trade-off between visual quality (PSNR) and embedding bits (capacity). The selected method achieved an average PSNR of 49 dB with a relatively high embedding bit on a standard database image. Moreover, the scheme performed significantly better than all state-of-the-art schemes on common images. Further, various experiments and analysis are conducted to show the efficacy of the proposed method. The stated method is tested to determine the robustness and visual quality of the stego image under different geometric and non-geometric attacks. The secret image is recovered within an acceptable condition even after the tampering of the stego images. Security of the proposed scheme is enhanced by employing Arnold transform which utilizes sharable keys to determine the sequence of order of selection of blocks for data hiding. A user will not be able to obtain the secret image with invalid keys even if it knows the algorithm. Thus, the proposed scheme will serve the need for secret data communication and ownership authorization in different institutions and organizations such as health care, courts of law, and in securing of intellectual property. Nevertheless, the proposed scheme needs to be enhanced in the future course of work for high embedding capacity, robustness against JPEG compression, and vector quantization along with self-recovery properties.[01] S. Arunkumar at.al.,[2019], In this paper, Presented an A robust image steganographic scheme based on RIWT, DCT and SVD has been proposed in our paper. This scheme has combined the technology of RIWT, DCT, the SVD decomposition technique and the logistic chaotic map. As RIWT is a shift invariant, reversibility and robustness are achieved in our proposed scheme. Better imperceptibility is achieved by using SVD and DCT, as embedding is completed on singular values. Usage of the logistic chaotic map to encrypt secret medical images provides extra security and also improved robustness to our scheme. As decomposition is done using SVD and embedding is done on a specific sub band of decomposed block, steganalysis has become a tough task. Moreover, modification of the SVs of SVD efficiently resists geometric attacks and attacks by image manipulation. The experimental results, as well as the analysis and comparison with similar schemes in the literature, show that our scheme is superior to other schemes in terms of imperceptibility, reversibility and robustness. Confidentiality is a key requirement in healthcare areas such as Telemedicine. The medical image needs to be secured during transmission. Authentic images and their integrity are prime requirements in healthcare. This proposed method can provide authenticity and integrity of the medical images in the transmission process, and cryptography can ensure the confidentiality of these medical images. The method can be used for Military applications too, where secrecy is a must. In the future, we plan to enhance the steganography framework by embedding secret medical image blocks only in few cover image blocks based on statistical measure like contrast and correlation.[02] Aniruddha Kanhe at.al.[2018], In this paper Presented an a novel audio watermarking technique based on DCT and SVD transform. The proposed technique embeds the watermark bits adaptively in selected frames having low frequency and high energy. The watermark bits are embedded in DCT coefficients of selected frames by performing SVD operation. The watermark bits are embedded in non-diagonal elements of SVD matrix. Experiments are conducted to evaluate the performance of the proposed audio watermarking technique and compared with recent frequency-domain audio watermarking techniques. The high-SNR values confirm that the proposed technique is highly imperceptible. The robustness of proposed audio watermarking technique is evaluated by computing BER and AIL for re-sampling, re-quantization, AWGN, and MP3 compression attacks with high data payload. The proposed watermarking scheme achieves comparable, if not better, results compared with other recently developed techniques for various attacks considered in this work. Future research work may include the enhancement of proposed technique to withstand with random cropping attack, pitch shifting attack, and time-scale modification attack. The proposed technique can be made robust against these attacks by embedding synchronization codes with watermark bits.[03] Rupali Bharadwaj ,at.al. ,[2016], In this paper, Presented an three stage complementing the secret message in First stage, then using pseudo random number generator data are selected randomly and hiding complemented secret message in cover image pixels in second stage and in third stage inverted bit LSB use as steganography rather than simple LSB used, thus, it provide maximum security and less chance to eavesdrop or detect the error. Experimental study proofs the proposed system is better than basic LSB in term of higher PSNR value of hiding secrete message in the cover image thus it overcome the chance of attack on the communication and attacker cannot easily detect the original message..

III. PROPOSED METHOD

This presented work The structure of proposed method is broadly divided into the two parts. Encoder end and decoder end. The encoder end is described first. This end generates the information and also creates the stego image (CI) and stego data (SD)

Encoder Part

In the encoder part is important part of the proposed method. The transmitter end is also known as an encoder part of the proposed method. In this part we create the stego image. Stego text is the summation of secret data. This stego image hides into a cover image with the help of proposed method. In this part there are four important terms used here.

Secret Data (SD)
Stego Image (SI)
Cover image (CI)

Secret Data (SD) Secret data is the data which we want to hide. The quality of proposed work is based on the secret data. Secret data is generated at the user end and embedded into Cover Image (CI). Similarly that secret data is obtained at the receiver end by stego image (SI).. In general secret data is in binary form, images and also ASCII based data available.

Stego Image (SI) For embedding of secret data first apply image steganography and add secret data or secret image different size small image.

Cover image (CI) Cover image is the image in which Crypto Image is hiding. The proposed work focuses on spatial domain. It means that secret data (SD) is hidden only in pixels. There are different type of cover image data sets that are available in the field of image processing. The proposed method uses a standard data set images. In this part of proposed method, the steps of implementation of proposed work are shown.

First step In the first step, we will enter the information which we want to hide into the cover image or any small image from the database which is used to hide secret data.

Second Step After selecting the small image, small image is used for further processing of the proposed task of the image. Select a window size 3X3 which is changed according to the pixel level.

Case 1 If 3X3 window contain all zeros and all ones, escape the window.

$$\text{Matrix} = \begin{matrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{matrix}$$

$$\text{Matrix} = \begin{matrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{matrix}$$

Case 2 - If all pixel contain different values then all binary data embed into these pixels.

$$\text{Matrix} = \begin{matrix} 212 & 73 & 145 \\ 149 & 193 & 19 \\ 140 & 192 & 13 \end{matrix}$$

Fourth Step –After embedding the stego image in the cover image we get embedded image (EI). This is sent to the communication channel. After completing the “Embedded image”, transmitter end process is completed.

Decoder part

First Step - First collect the stego image from the encoder end. Select the collected “Stego” image.

Second Step – After selecting the stego image, processing of the proposed task of the image. Select a window size 3X3 which is changed according to the pixel level.

Case 1 If 3X3 window contain all zeros and all ones, escape the window.

$$\text{Matrix} = \begin{matrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{matrix}$$

$$\text{Matrix} = \begin{matrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{matrix}$$

Case 2 - If all pixel contain different values then all binary data embed into these pixels.

$$\text{Matrix} = \begin{matrix} 212 & 73 & 145 \\ 149 & 193 & 19 \\ 140 & 192 & 13 \end{matrix}$$

In stego image decoding process is applied. Check the pixel and select the LSB bit if satisfy the above condition for data extraction from the stego image.

Third Step – Convert this binary information into the “String from or data from”. Separate both the secret data and image and cover Image.

Fifth Step – After obtaining the secret data match the secret data of encoder end. For quality measurement of the proposed work, different parameters are used. They are PSNR, MSE, SSIM and payload capacity of the image. These are some quality check parameter. After satisfaction of the quality check parameter, the visual result of proposed work is seen.

IV. SIMULATION RESULTS AND DISCUSSION

Mean Square Error (MSE): The MSE measures the standard amendment between the actual image (X) and the noised image (Y) and is given by:

$$\mathrm{MSE} = \frac{1}{N}\sum_{j=0}^{N-1}(X_j - Y_j)^2 \qquad 1$$

X_j Shows the cover image

Y_j Shows the stego image

The MSE has been extensively used to quantify image quality and once used alone; it doesn't correlate powerfully enough with sensory activity quality. It ought to be used, therefore in conjunction with alternative quality metrics and perception.

Peak Signal to Noise Ratio (PSNR): The PSNR is computed as:

$$\mathrm{PSNR} = 10\log_{10}\frac{s^2}{\mathrm{MSE}} \qquad 2$$

The PSNR is higher for an excellent worth image and lower for a poor quality image. It measures image fidelity, that is, however closely the distorted image resembles the actual image. In our research work on the basis of our image size 255x255.

Table .1 Comparison of proposed method different methods

Cover image	Message Image	Simple LSB [ref. no. 10]		Random LSB [ref. no.10]		Inverted LSB [ref . no 10]		CILSB [ref. No.10]		Proposed Method	
Lena	Cameraman	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE
512x512	4225 bits	59.657	0.064	59.695	0.064	59.713	0.249	59.727	0.064	59.885	0.066
512x512	16384 bits	53.798	0.249	53.805	0.380	53.814	0.248	53.817	0.249	54.144	0.250
512x512	24964 bits	51.977	0.380	51.978	0.380	51.984	0.380	51.997	0.380	52.331	0.380

The table 1 shows the result of proposed method shown in above. The compression of different previous methods shown in above table they are simple LSB, random LSB, inverted LSB, Complemented Inverted LSB (CILSB) and proposed. In the above table 1 compare the different methods on the basics of peak signal to noise ratio (PSNR) and mean square error (MSE). So the proposed method shows better result as compare to other previous methods. PSNR and MSE of the proposed method 59.885 and 0.066.

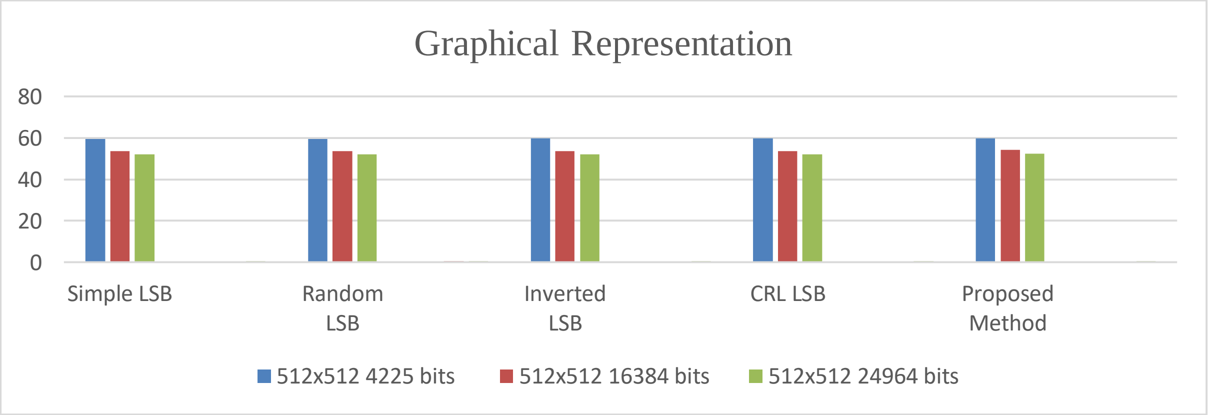

Fig. 1 shows the graphical comparison of proposed method with different methods

The above figur.1 shows the graphical representation of proposed method. In the graphical representation clearly see that proposed method shows better result as compare to other previous methods.

In the above figure 1 compare the result on "Lena" image. Now calculate the result on different standard test image shown in below. In the table.2 shows the comparison of proposed method like "Lena", "Pepper" and "baboon" images. In the table shows the result of proposed method on different images with different data size. Same cover image size512X512, but different data size that is 4225, 16384 and 24964. The values of standard parameters like PSNR and MSE calculate, avg. value of PSNR at 4225 bits is 59.8dB, similar that on other different size is 54.15 and final is 52.32. The overall performance of proposed method good as compare to other methods.

V. CONCLUSION

Digital Steganography is an engrossing scientific area which comes under the security system. In this paper, Steganography use based pixel identification and embed the secret data using proposed methodology. At the last but not least compare the spatial domain based different image steganography techniques on the basis of peak signal noise ratio performance in table of chapter 5.

PSNR values and Data hiding capacity both parameters are inversely proposal. Peak signal to noise ratio based comparison is important for pixel value based method. Proposed method also compare with different images and different data sets. In this paper compare seven different pixels based method and its PSNR values. The proposed method shows better result as compare to other previous methods like LSB, Inverted LSB, and Random LSB. That On the basis of this comparative analysis in future proposed a new method for image-based data hiding which contains the high value of PSNR and low value of MSE. Also, shows the better data hiding capacity.

- Steganography includes a sort of application which will be without doubt be investigated within the approaching future. However, the following predictions square measure given as an affordable set of prospects.
- Steganography techniques will become a lot of common and more and more refined.
- Stego-analysis tools will become a lot of difficult but can usually be behind their steganography counterparts.

References

[1] AliSingh, Prabhash Kumar, Biswapati Jana, and Kakali Datta. "Superpixel based robust reversible data hiding scheme exploiting Arnold transform with DCT and CA." *Journal of King Saud University-Computer and Information Sciences* **(2020).**

[2] Arunkumar, S., V. Subramaniyaswamy, V. Vijayakumar, Naveen Chilamkurti, and R. Logesh. "SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images." *Measurement* 139 **(2019):** 426-437.

[3] Kanhe, Aniruddha, and Aghila Gnanasekaran. "Robust image-in-audio watermarking technique based on DCT-SVD transform." *EURASIP Journal on Audio, Speech, and Music Processing* 2018, no. 1 **(2018):** 1-12.

[4] Shete, Kalpana Sanjay, Mangal Patil, and J. S. Chitode. "Least significant bit and discrete wavelet transform algorithm realization for image steganography employing FPGA." *International Journal of Image, Graphics and Signal Processing* 8, no. 6 **(2016):** 48.

[5] S. Channalli and A. Jadhav, "Steganography an Art of Hiding Data", International Journal o Computer Science and Engineering, IJCSE, vol. 1, no. 3, **(2009)**.

[6] C.-H. Yang, C.-Y. Weng, S.-J. Wang, Member, IEEE and H.-M. Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems", IEEE Transactions on Information Forensics and Security, vol. 3, no. **(2008)** September 3, pp. 488-497.

[7] K.-H. Jung, K.-J. Ha and K.-Y. Yoo, "Image data hiding method based on multi-pixel differencing and LSB substitution methods", Proc. 2008 International Conference on Convergence and Hybrid Information Technology (ICHIT '08), Daejeon (Korea), **(2008)** August 28-30, pp. 355-358.

[8] H. Zhang, G. Geng and C. Xiong, "Image Steganography Using Pixel-Value Differencing", Electronic Commerce and Security, ISECS '09. Second International Symposium on **(2009)** May.

[9] Wu D, Tsai W. A stenographic method for images by pixel value differencing. Pattern Recognit. Lett. **(2003)**; 24:1613–1626.

[10] Zhang X, Wang S. Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. Pattern Recognit. Lett. **(2004);** 25: 331–339.

[11] Ker A. Improved detection of LSB steganography in grayscale images. In Proc. Information Hiding Workshop Springer LNCS**(2014)**; 3200: 97–115.

[12] Yang HC, Weng CY, Wang SJ, Sun HM. Adaptive data hiding in edge areas of images with spatial LSB domain systems. IEEE Trans. Inf. Forensics Security **(2008)**; 3: 488–497.

[13] Akhtar N, Khan S, Johri P. An improved inverted LSB image steganography. In Issues and Challenges in Intelligent Computing Techniques (ICICT), International Conference on. IEEE,**(2014)**; p. 749-755.

[14] Rupali Bhardwaj, Vaishali Sharma, "Image Steganography Based on Complemented Message and Inverted bit LSB Substitution" Elsevier, **(2016).**

[15] Chetan, K., Nirmala, S., 2015. An efficient and secure robust watermarking scheme for document images using integer wavelets and block coding of binary watermarks. J. Inf. Secur. Appl. **(2015)** 24, 13–24.

[16] Chowdhuri, P., Jana, B., Giri, D., 2018. Secured steganographic scheme for highly compressed color image using weighted matrix through dct. Int. J. Comput. Appl., 1–12,**(2018)**

[17] Chowdhuri, P., Pal, P., Jana, B., 2019. Improved data hiding capacity through repeated embedding using modified weighted matrix for color image. Int. J. Comput. Appl. 41, 218–232.**(2019)**

[18] Codella, N.C., Gutman, D., Celebi, M.E., Helba, B., Marchetti, M.A., Dusza, S.W., Kalloo, A., Liopyris, K., Mishra, N., Kittler, H., et al., 2018. Skin lesion analysis toward melanoma detection: a challenge at the 2017 international symposium on biomedical imaging (isbi), hosted by the international skin imaging collaboration (isic). In: 2018 IEEE 15th International Symposium on Biomedical Imaging **(ISBI 2018),** IEEE. pp. 168–172..

[19] Das, C., Panigrahi, S., Sharma, V.K., Mahapatra, K., 2014. A novel blind robust image watermarking in dct domain using inter-block coefficient correlation. AEU Int. J.Electron. Commun. 68, 244–253.**(2014.)**

[20] Dey, N., Das, P., Roy, A.B., Das, A., Chaudhuri, S.S., 2012. Dwt-dct-svd based intravascular ultrasound video watermarking. In: 2012 World Congress on Information and Communication Technologies, IEEE. pp. 224–229**.(2012)**.

[21] Dey, N., Maji, P., Das, P., Biswas, S., Das, A., Chaudhuri, S.S., 2013a. An edge based blind watermarking technique of medical images without devalorizing diagnostic parameters. In: 2013 International Conference on Advances in Technology and Engineering (ICATE), IEEE. pp. 1–5.. **(2013)**

[22] Dey, N., Samanta, S., Yang, X.S., Das, A., Chaudhuri, S.S., 2013. Optimisation of scaling factors in electrocardiogram signal watermarking using cuckoo search. Int. J. Bio-Inspired Comput. 5, 315–326.**(2013)**

[23] Ekodeck, S.G.R., Ndoundam, R., 2016. Pdf steganography based on chinese remainder theorem. J. Inf. Secur. Appl. 29, 1–15. Fridrich, J., Goljan, M., Du, R., 2001. Invertible authentication. In: Security andWatermarking of Multimedia contents III, International Society for Optics and Photonics. pp. 197–208**(2016)**.

[24] Gupta, A.K., Raval, M.S., 2012. A robust and secure watermarking scheme based on singular values replacement. Sadhana 37, 425–440.Hamza, R., Hassan, A., Huang, T., Ke, L., Yan, H., 2019.

[25] Pranay Yadav – "Color Image Noise Removal by Modified Adaptive Threshold Median Filter for RVIN" in National Institution of Technology (NIT - Shilog) Confrence date 28 – 29 Jan. 2015. (Scopus http://ieeexplore.ieee.org/document/7060562/

[26] Pranay Yadav and Parool Singh – "Color Impulse Noise Removal by Modified Unsymmetric Trimmed Median Mean Filter for FVIN" in PARK College of Engineering and Tekhnology, Coimbatore-641659, Tamilnadu, India. IEEE International Conference on Computational Intelligence and Computing. 17 – 19 Dec. 2014 (Scopus) http://ieeexplore.ieee.org/document/7238369/

[27] Shachi Sharma and Pranay Yadav "Removal of Fixed Valued Impulse Noise by Improved Trimmed Mean Median Filter" in PARK College of Engineering and Tekhnology, Coimbatore-641659, Tamilnadu, India. International Conference on Computational Intelligence and Computing.17-19 Dec 2014. (Scopus) http://ieeexplore.ieee.org/document/7238368/ \

[28] Pranay Yadav and Vivek Kumar– "Image De-noising for Salt and Pepper Noise by Robust Mean Filter " fourth international conference on Advances in Engineering and Technology –AET -2013 AET2013AEE547RE. http://searchdl.org/index.php/book_series/view/1521

[29] Kumar V, Yadav P, Samadhiya A, Jain A, Tiwari P, Comparative Performance Analysis of Image De-noisingTechniques, International Conference On Innovation in Engineering And Technology(ICIET)Bangkok,Thailand2013,http://dx.doi.org/10.15242/IIE.E1213576