International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:10, No:7, 2016

Exploration of Least Significant Bit Based Watermarking and Its Robustness against Salt and Pepper Noise

Kamaldeep Joshi, Rajkumar Yadav, Sachin Allwadhi

***Abstract*—**Image steganography is the best aspect of information hiding. In this, the information is hidden within an image and the image travels openly on the Internet. The Least Significant Bit (LSB) is one of the most popular methods of image steganography. In this method, the information bit is hidden at the LSB of the image pixel. In one bit LSB steganography method, the total numbers of the pixels and the total number of message bits are equal to each other. In this paper, the LSB method of image steganography is used for watermarking. The watermarking is an application of the steganography. The watermark contains 80*88 pixels and each pixel requirs 8 bits for its binary equivalent form so, the total number of bits required to hide the watermark are 80*88*8(56320). The experiment was performed on standard 256*256 and 512*512 size images. After the watermark insertion, histogram analysis was performed. A noise factor (salt and pepper) of 0.02 was added to the stego image in order to evaluate the robustness of the method. The watermark was successfully retrieved after insertion of noise. An experiment was performed in order to know the imperceptibility of stego and the retrieved watermark. It is clear that the LSB watermarking scheme is robust to the salt and pepper noise.

***Keywords*—**LSB, watermarking, salt and pepper, PSNR.

I. Introduction and Litature Review

IN the modern world, advancement in digital communication also demands advancement in security. Security in the digital environment can be achieved either using cryptography or steganography. Using cryptography mechanism of security, an intruder may have some odd felling towards data and may attempt to decrypt it. But the second mechanism of security, i.e. steganography conceals the information in any cover medium such as images, videos, text and audio. This gets any one free from suspicion [1]. The steganography techniques are broadly categorized into two domains either spatial domain or transform domain. The prior one works directly over gray level values, whereas the latter one transforms host image from the spatial domain to transform domain and information is concealed by changing image-coefficient. Popularly known technique in spatial domain, such as PIT (pixel indicator technique) [2], [3], edges based embedding techniques [4] while popularly known techniques in transform domain techniques such as discrete cosine transform technique [5] and Discrete Wavelet Transform [6]. Wang et al. [7] proposed a GA based method on LSB substitution. This scheme requires extra processing moments which were the major disadvantage of this method. Chang et al. [6] proposed an algorithm based on dynamic programming on LSB. Thien and Lin [8] gave an LSB approach using modulus function. Chang and Chen [9] gave a scheme that was based on the pixel tuning approach for getting superior quality. Wu et al. [10] offered a superior system by combining of LSB and pixel differencing scheme. Lou et al. [11] gave another method based on the random addition of +1 and -1 to give pixel if message bit is not same as image bit. Mieleikainen [12] proposed LSB-MR which embeds two secret bits at a time in a pair of pixel. Tsai and Wu [13] projected a high imperceptibility LSB method. It hides message in the edgy area of image or smooth area to increase imperceptibility. Wang et al. [14] projected a way which conceals the data on a moderately significant bit. Jung et al. proposed a semi reversible data hiding technique that uses interpolation and LSB substitution technique. In this technique, before LSB substation, intermediate pixel is generated for hiding the data. The application areas of image steganography include medical imaging, secret communication, and temper proofing watermarking. Watermarking should focus on three characteristics: 1) payload of information 2) Robustness against attacks (Integrity) 3) Quality (imperceptibility) [15] as shown by Figs. 2-4.

II. Watermarking Methods and Experimental Results

The proposed method hides a grayscale watermark image (B) of size (B_R * B_C) in host images (A/A_1) of A_R * A_C (or A_{R1} * A_{C1}) pixels such that $|B_R * B_C| <= |A_R * A_C|$ (or $A_{R1} * A_{C1}$). Here B in experiment taken as 80*88 pixels while, A as 256*256 or 512*512 pixels such that |80*88*8|<=256*256 (or 512*512) i.e. 56320 bits <=65,536 (or 262144) pixels $B = \{b_Z | 0<=z<56320, b_Z \varepsilon \{0,1\}\}$, $A= \{a_{XY}/ a_{XY1} |0<=X<256/512, 0<=Y<256/512, a_{XY}/ a_{XY1} \varepsilon \{0,1,2, \ldots\ldots\ldots\ldots, 255\}\}$. The procedure starts from the very first pixel of host image and continues up to X*Y times (256*256) and in every iteration watermark bit is added to LSB of every selected pixel

K. Joshi is with the Department of Computer Science and Engineering, University Institute of Engineering and Technology, Maharshi Dayanand Uniersity, Rohtak-124001, Haryana, India (Phone: +919416952504; e-mail: kamalmintwal@gmail.com).

R. Yadav is with the Department of Computer Science and Engineering, University Institute of Engineering and Technology, Maharshi Dayanand University, Rohtak-124001, Haryana, India (Phone: +919215997198; e-mail: rajyadav76@rediffmail.com).

S. Allwadhi is with the Department of Computer Science and Engineering, University Institute of Engineering and Technology, Maharshi Dayanand Uniersity, Rohtak-124001, Haryana, India (Phone: +919255384571; e-mail: sachin.allwadhi@gmail.com).

such that the resultant image becomes P = {p_{XY}/ p_{XY1}| p_{XY}/ p_{XY1} = a_{XY}/ a_{XY1}+ b_Z p_{XY}/ p_{XY1} ε {0,1,2, ……., 255}} After this procedure a well-known salt and pepper noise is added by a factor of 0.02 in effect to know stego-image imperceptibility (quality).

MAXERR represents the maximum absolute squared deviation of original and stego image. It represents the maximum difference between the pixels of a cover image and a stego image, i.e. 1 in the case of the Least Significant method of Image steganography. L2RAT shows the ratio of the squared norm of the Original and stego Image. Salt and Pepper: This name arises from the fact of their colors where 0 is black and 255 is white in an 8 bit image. It adds the white and a black pixel in the image.

Fig. 1 Logo for Watermark

Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) are the most usual parameters for measurement of the quality of original and stego image. The PSNR tells the similarity between two images and is inversely proportional to the MSE [16].

The PSNR is evaluated in decibels. It is given by (2).

$$\mathrm{MSE} = \frac{1}{[\mathrm{R}\times\mathrm{C}]^2}\sum_{i=1}^{C}\sum_{j=1}^{R}(X_{ij} - Y_{ij})^2 \quad (1)$$

where R and C are the row and column of the images and X_{ij}, Y_{ij} are the ijth pixels intensity of the Cover and Watermarked image respectively.

$$\mathrm{PSNR} = 10\log_{10}\left[\frac{I^2}{\mathrm{MSE}}\right] \quad (2)$$

where: I is the maximum intensity in an Image i.e. 255.

Figs. 7-11 show the original and corresponding stego images concealing logo as watermark. The size of these images is 256*256 (Image 1 to Image 5) with their respective histograms.

Fig. 2 Relation between robustness and quality

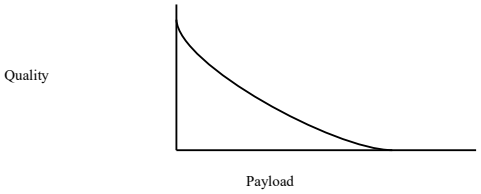


Fig. 3 Relation between quality and payload

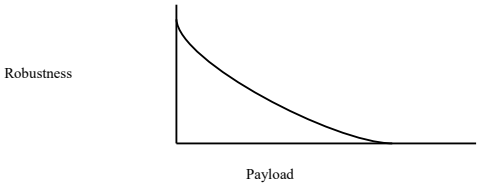
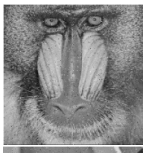
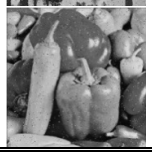


Fig. 4 Relation between robustness and payload

TABLE I
256*256 ORIGINAL IMAGES, WATERMARKED IMAGES AND WATERMARKED IMAGES HAVING NOISE

Image	Host image	Stego-image	Stego-image suffering from noise
1			
2			
3			
4			
5			

TABLE II
512*512 ORIGINAL IMAGES, WATERMARKED IMAGES AND WATERMARKED IMAGES HAVING NOISE

Image	Host image	Stego-image	Stego-image suffering from noise
6			
7			
8			
9			
10			

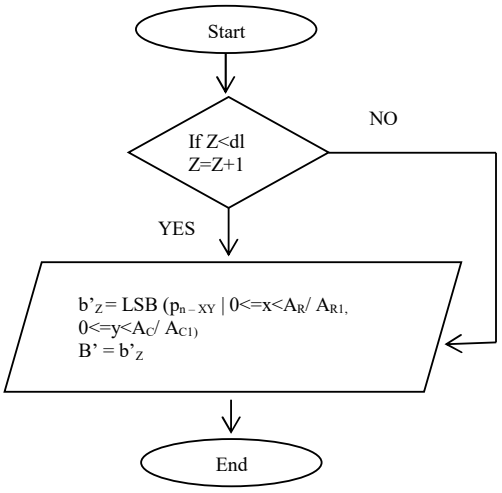


Fig. 5 Retrieval algorithm

Figs. 11-15 show the original and corresponding stego images concealing logo as watermark. The sizes of the images are 512*512 (Image 6 to Image 10) with their respective histograms.

Figs. 5 and 6 give the complete procedure of concealing the watermark in the cover image and the procedure for extraction of the watermark from the watermarked image respectively.

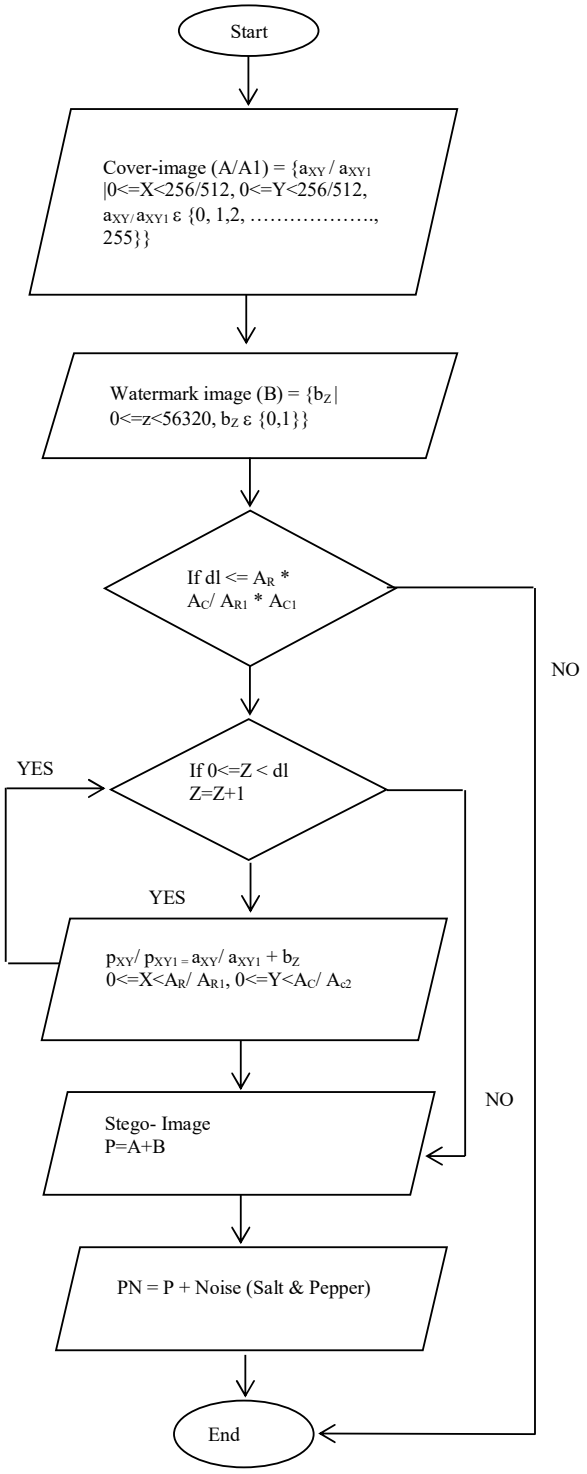


Fig. 6 Insertion Algorithm

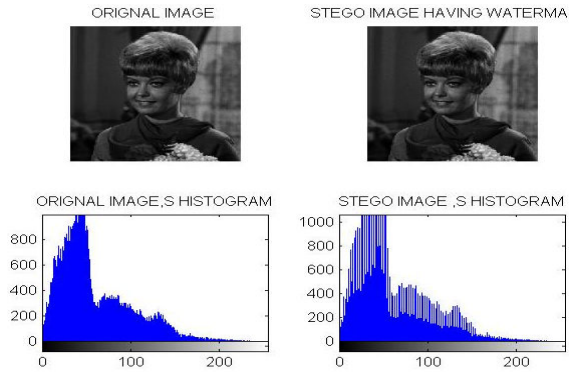


Fig. 7 Original image 1 and its watermarked image with histogram

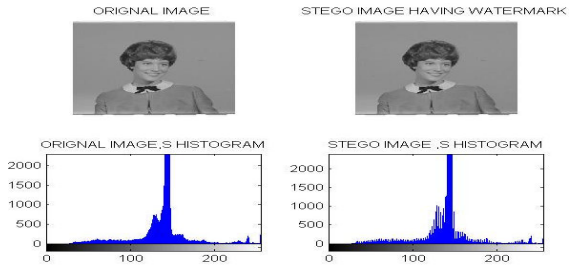


Fig. 8 Original image 2 and its watermarked image with histogram

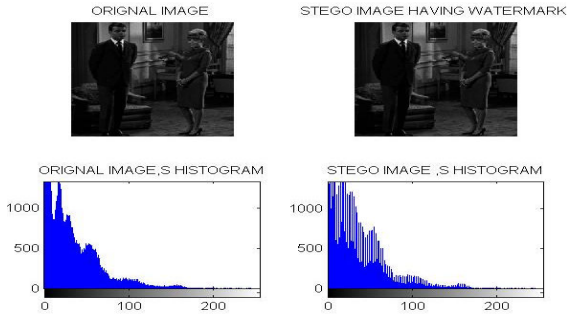


Fig. 9 Original image 3 and its watermarked image with histogram

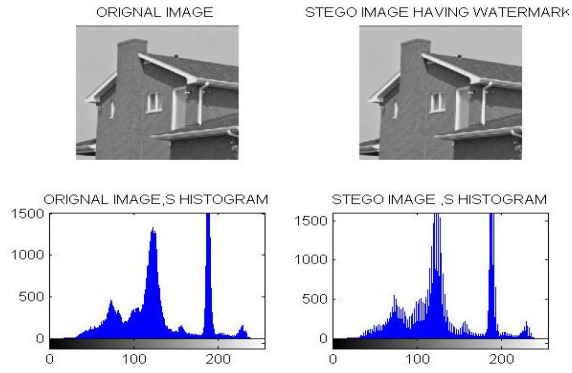


Fig. 10 Original image 4 and its watermarked image with histogram

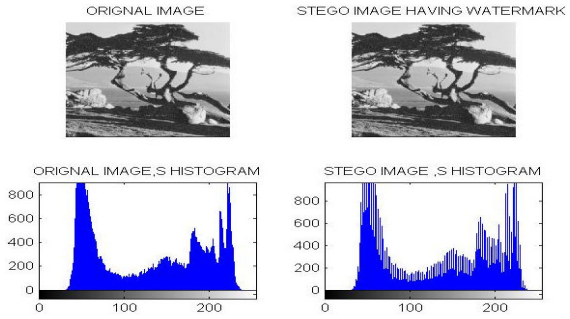


Fig. 11 Original image 5 and its watermarked image with histogram

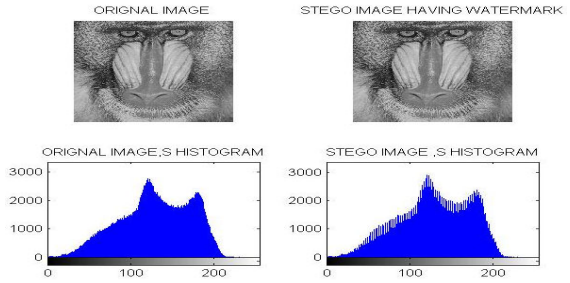


Fig. 12 Original image 6 and its watermarked image with histogram

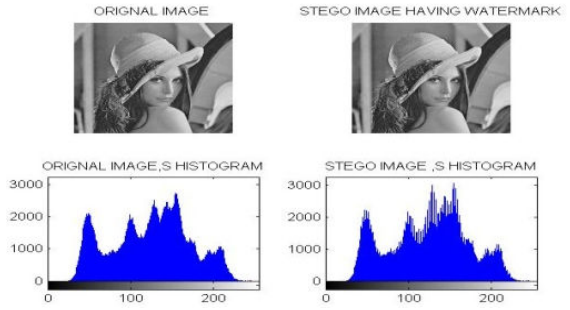


Fig. 13 Original image 7 and its watermarked image with histogram

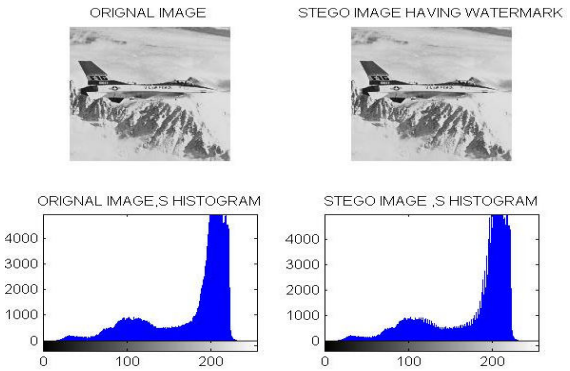


Fig. 14 Original image 8 and its watermarked image with histogram

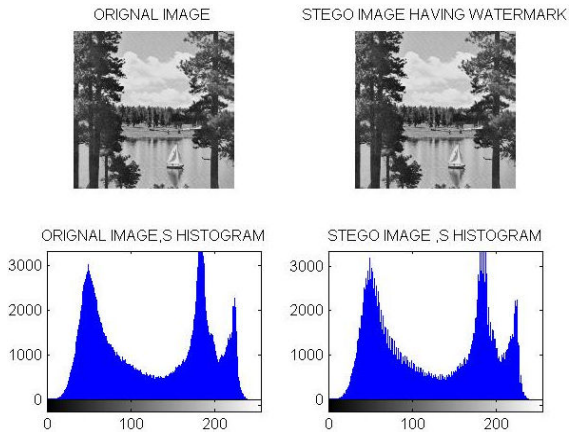


Fig. 15 Original image 9 and its watermarked image with histogram

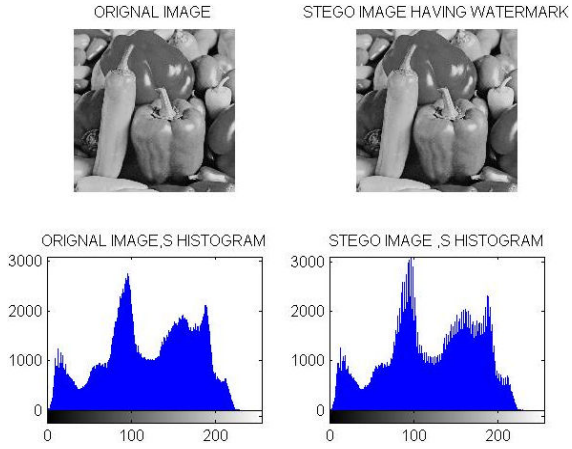


Fig. 16 Original image 10 and its watermarked image with histogram

Figs. 17-21 show original and retrieved watermark after inserting the noise (.02) in image of size 256*256 while 22 to 26 show the same in image of size 512*512.

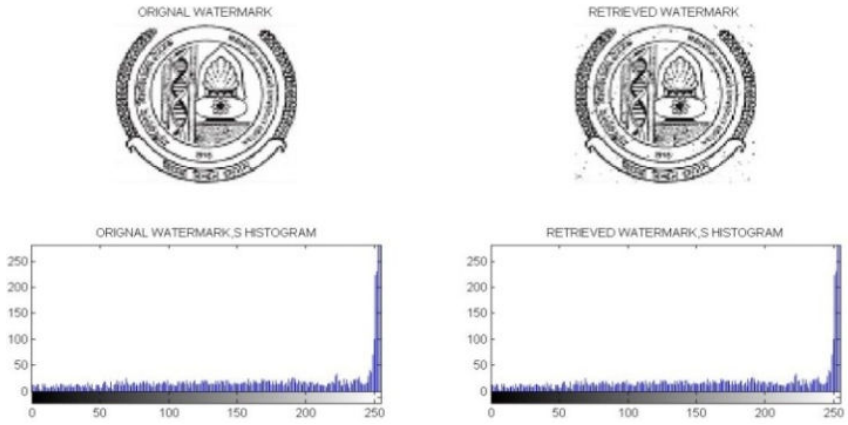


Fig. 17 Retrieved watermark from image 1

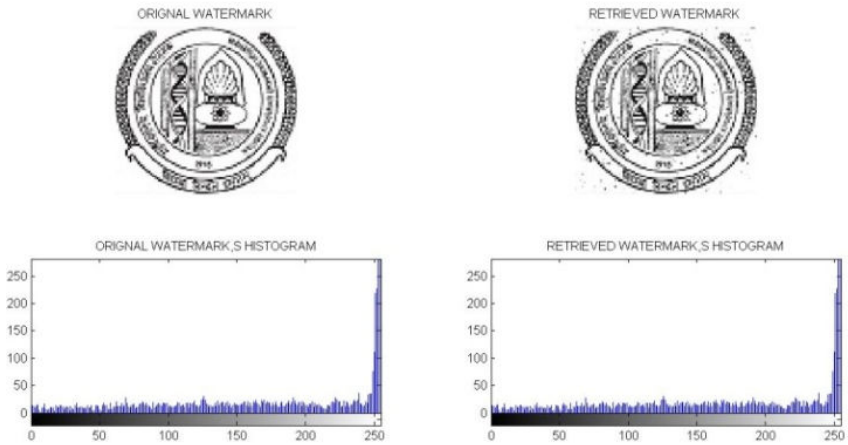


Fig. 18 Retrieved watermark from image 2

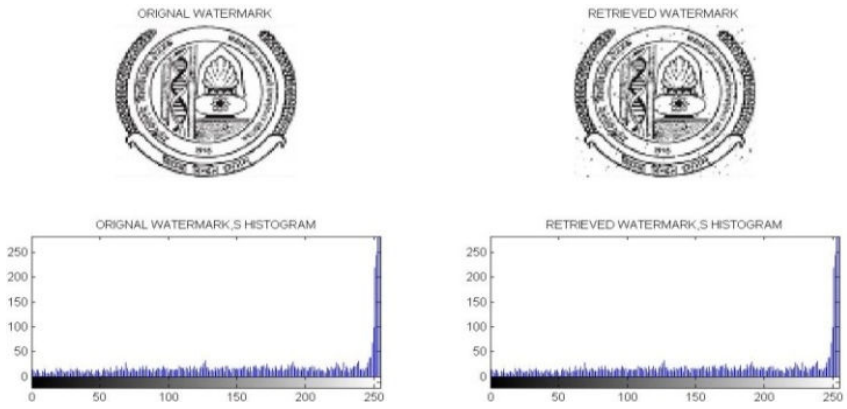


Fig. 19 Retrieved watermark from image 3

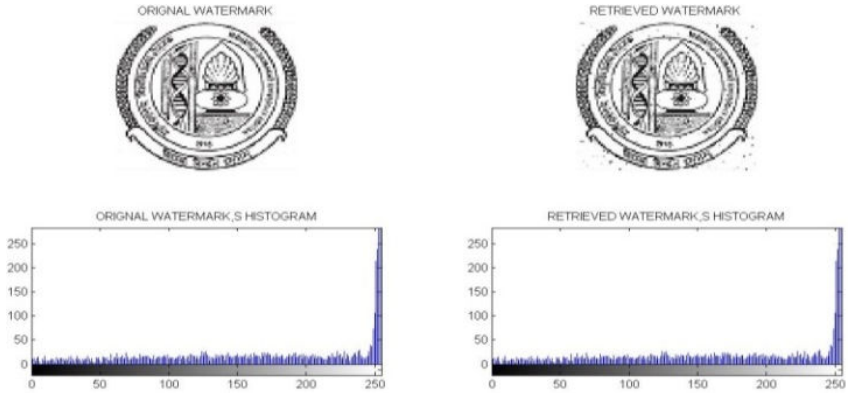


Fig. 20 Retrieved watermark from image 4

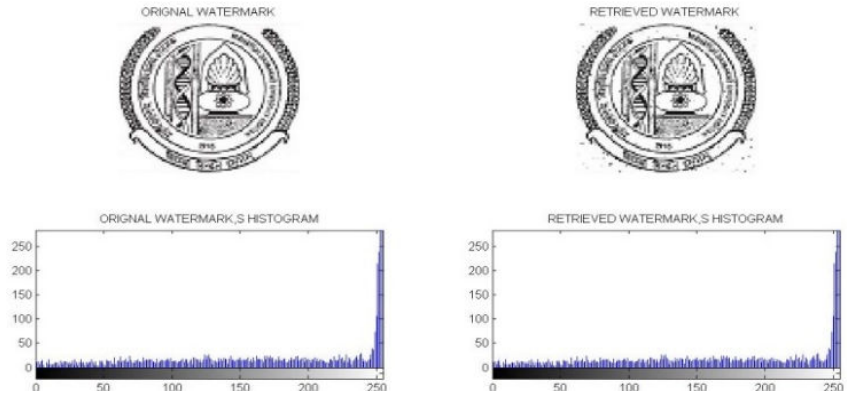


Fig. 21 Retrieved watermark from image 5

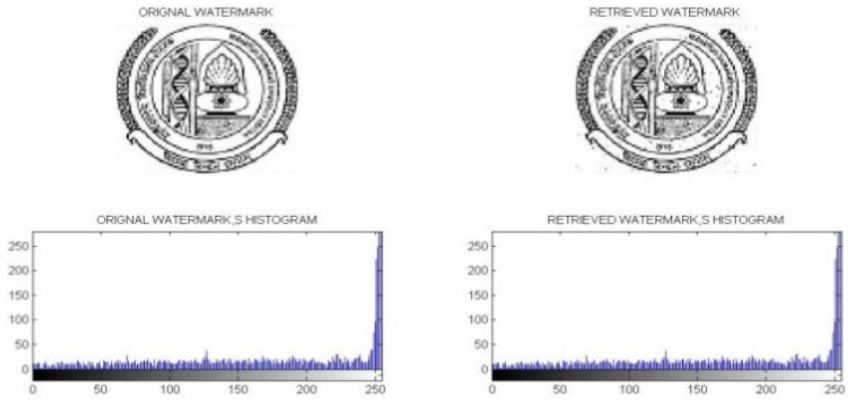


Fig. 22 Retrieved watermark from image 6

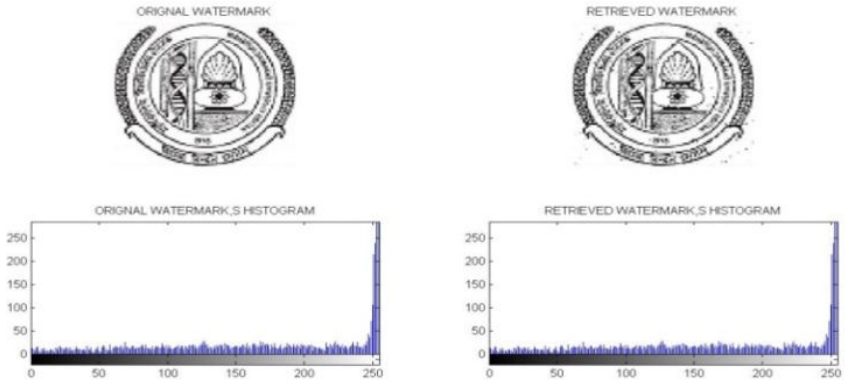


Fig. 23 Retrieved watermark from image 7

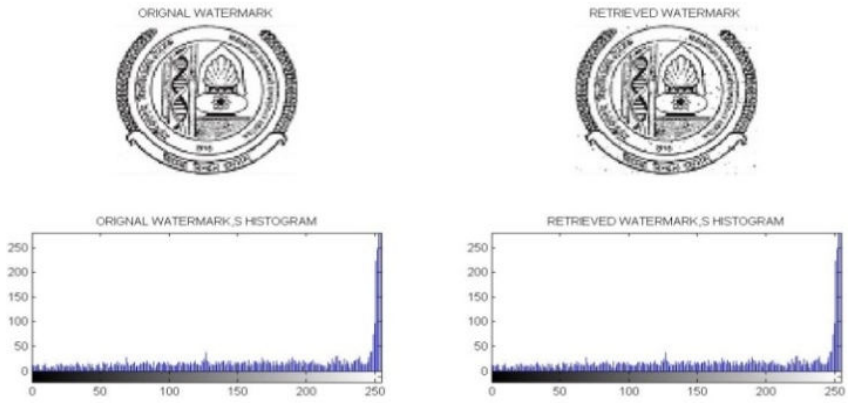


Fig. 24 Retrieved watermark from image 8

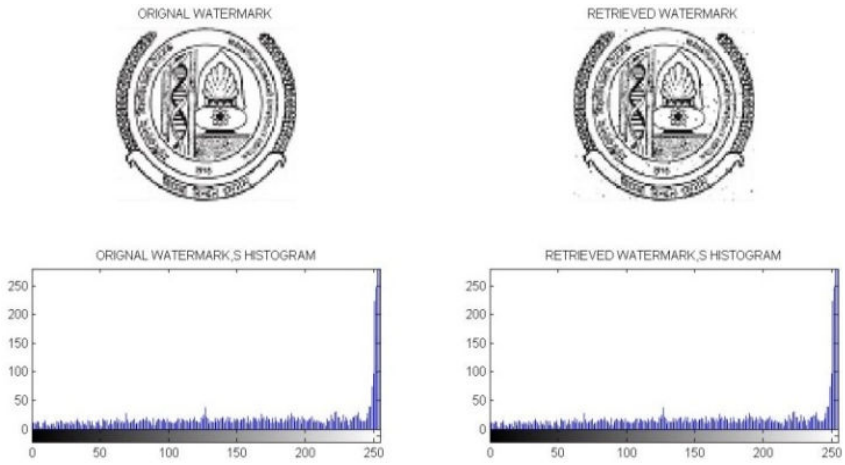


Fig. 25 Retrieved watermark from image 9

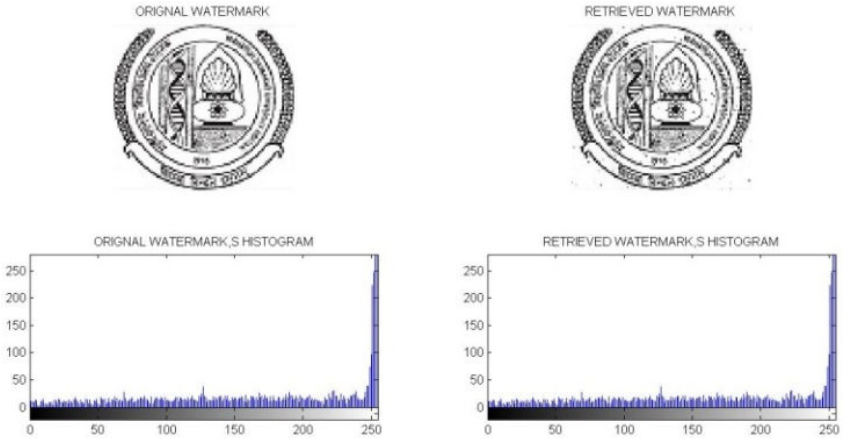


Fig. 26 Retrieved watermark from image 10

TABLE III
PSNR AND MSE 256*256 ORIGINAL AND STEGO-IMAGES

Sr. No. of Images	PSNR	MSE	MAXERR	L2RAT
Image 1	51.7930	0.4303	1	1.0041
Image 2	51.7583	0.4338	1	1.0025
Image 3	51.7780	0.4318	1	1.0059
Image 4	51.8034	0.4293	1	1.0024
Image5	51.8164	0.4280	1	1.0022

TABLE IV
PSNR AND MSE 512*512 ORIGINAL AND STEGO-IMAGES

Sr. No. of Images	PSNR	MSE	MAXERR	L2RAT
Image 3	57.8333	0.1071	1	1.0006
Image 4	57.8364	0.1070	1	1.0006
Image 5	57.7939	0.1081	1	1.0005
Image 6	57.8429	0.1069	1	1.0006
Image 7	57.8054	0.1078	1	1.0007

III. CONCLUSION

In this paper, the effects of noise (Salt and Pepper) were analyzed on the LSB method of image steganography. A watermark i.e. logo of 80*88 was taken to embed in the gray image. The experiment shows that the LSB has high rate of imperceptibility as the maximum change in a pixel is +1 or -1. A noise factor of .02 was added on different sizes images (256*256, 512*512). The watermark was successfully removed by the retrieval algorithm as shown in Figs. 17-26. The retrieved watermark is also having some black and white spots but can be easily recognized as shown in Figs. 17-26. Following by this, the PSNR, MSE, MAXERR and L2RAT of stego image and original image were calculated. A histogram analysis was performed on the original and stego image. It shows that the changes made by the insertion process of watermark in the original image. These values show that the imperceptibility of LSB method is very good.

REFERENCES

[1] Emad T. Khalaf, Norrozila Sulaiman (2011) "A Robust Data Hiding Technique based on LSB Matching," International Journal of Computer, Electrical, Automation, Control and Information Engineering, World Academy of Science, Engineering and Technology, Vol:5, No:10
[2] Gutub, A. A. A. (2010). Pixel indicator technique for RGB image steganography. Journal of Emerging Technologies in Web Intelligence, 2(1), 56–64. http://doi.org/10.4304/jetwi.2.1.56-64
[3] Gutub A, Ankeer M, Abu-Ghalioun M, Shaheen A, Alvi A (2008) Pixel indicator high capacity technique for RGB image based Steganography.

In: WoSPA 2008–5th IEEE International Workshop on Signal Processing and its Applications. pp 1–3
[4] Pal, A., & Pramanik, T. (2013). Design of an Edge Detection Based Image Steganography with High Embedding Capacity. Quality, Reliability, Security and Robustness in …, 794–800. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-37949-9_69
[5] Jia-Fa, M., Xin-Xin, N., Gang, X., Wei-Guo, S., & Na-Na, Z. (2015). A steganalysis method in the DCT domain. Multimedia Tools and Applications, (180). http://doi.org/10.1007/s11042-015-2708-0
[6] Chang C-C, Hsiao J-Y, Chan C-S (2003) "Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy". Pattern Recogn 36:1583–1595,
[7] Wang R-Z, Lin C-F, Lin J-C (2001) Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recogn 34:671–683
[8] Thien C-C, Lin J-C, (2003) "A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function". Pattern Recogn 36:2875–2881
[9] Chan C-K, Cheng L-M (2004)"Hiding data in images by simple LSB substitution". Pattern Recogn 37:469–474
[10] Wu H-C, Wu N-I,"Tsai C-S, Hwang M-S (2005)"Image steganographic scheme based on pixel-value differencing and LSB replacement methods". IEE Proc Vis Image Signal Process 152:611–615
[11] Luo W, Huang F, Huang J (2010) Edge adaptive image steganography based on LSB matching revisited. Inform Forensic Secur IEEE Trans 5:201–21, 2010
[12] Mielikainen J (2006) LSB matching revisited. Signal Proc Lett IEEE 13:285–287
[13] Dumitrescu S, Wu X, Wang Z, (2003)" Detection of LSB steganography via sample pair analysis." Signal Process IEEE Trans 51:1995–2007,
[14] Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin (2000), "Hiding data in images by optimal moderately significant-bit replacement", IEE Electron. Lett. 36 (25) 2069–2070.
[15] Rao, N. V., & Kumari, V. M. (2011). Watermarking in Medical Imaging for Security and Authentication. Information Security Journal: A Global Perspective, 20(3), 148–155.
[16] Joshi K, Yadav R, Allwadhi S., "PSNR and MSE based investigation of LSB" IEEE Proceeding on International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), 280 - 285, 2016.

Kamaldeep Joshi received his M.Tech degree in Computer Science and Engineering from Maharishi Dayanand University, Rohtak, Haryana (INDIA). He is currently working as assistant professor in Computer Science and Engineering Department at University Institute of Engineering & Technology (Maharshi Dayanand University Rohtak, Haryana) India. His research interest includes Steganography, Watermarking, and Neural Network.