ISSN:0975-9646

Alakrita Aggarwal et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (5) , 2011, 2036-2041

Robust Watermarking of Color Images under Noise and Cropping Attacks in Spatial Domain

Alankrita Aggarwal[1], *Monika Singla*[2]
[1] *Sr .Assistant Professor,* [2]*M.Tech*(C.S.E),*
Department of ComputerScience and Engineering ,
Haryana College of Technology and Management, Kaithal,india

***Abstract*—In this paper a novel spatial domain multiple watermarking scheme for color Images is proposed. The proposed scheme is of type blind and invisible watermarking. A binary watermark image is permutated using a secret key. The host image is divided into five blocks .Blocks size equals on the size of watermark image. The watermark is a binary image, embedded into five blocks of the host image by altering LSB values of the selected region.After performing OR operation on extracted watermarks, Only one watermark will be selected based on highest the NCC value of the extracted watermarks. The proposed scheme is found robust to various image processing operations such as salt and pepper noise, and cropping**

***Keywords*— Color Image, Spatial Domain, Robust Watermarking, Block Based Watermarking.**

I. INTRODUCTION

A digital watermark is a digital signal or a pattern embedded into the host media to be protected, such as an image or audio or video. It contains useful certifiable information for the owner of the host media, such as producer's name, company logo, etc; the watermark can be detected or extracted later to make an assertion about the host media. There are two important properties of a watermark; the first is that the watermark embedding should not alter the quality and visually of the host image and it should be perceptually invisible, the second property is robustness with respect to image distortions. This means that the watermark is difficult for an attacker to remove and it should be also robust to common image processing and geometric operations, such as filtering, resizing, cropping and image compression. Overviews on image watermarking techniques can be found in [2], [5], [7].

The watermarking techniques can be classified into two categories: spatial domain and transform domain techniques. In spatial domain technique [4], [13], [16], [17], [18], [20], the watermark embedding is achieved by directly modifying the pixel values of the host image. The most commonly used method in the spatial domain technique is the least significant bit (LSB). In [4], the least significant bit (LSB) of each pixel in the host image was modified to embed the secret message. In transform domain technique[2],[5]the host image is first converted into frequency domain by transformation method such as the discrete cosine transform (DCT), discrete Fourier transform (DFT) or discreet wavelet transform (DWT) ,etc. then, transform domain coefficients are altered by the watermark. The inverse transform is finally applied in order to obtain the watermarked image. The frequency domain methods allow an image to be broken up into different frequency bands. Embedding the watermark in the low frequency increases the robustness with respect to image distortions. The high frequency band of an image is more prone to dropping due to quantization and it will be lost by compression or scaling attacks. The middle frequencies embedding of the watermark avoid the most visual important parts of the image and it is robust to compression and noise attacks. There are so many ideas have been proposed for placing key inside the binary images or watermark image.[6],[9],[11].

In [13], a watermarking scheme is presented based on embedding the watermark into the original image in spatial domain by dividing the original image into different block size and adjusting brightness of a block according to the watermark. In [16], proposes a spatial domain probability block based watermarking method for color image, which is divided into blocks of size 8*8 and the intensities of all pixels in the block are modified in order to embed a watermark bit. In this method the number of total bits of the watermark must be less or equal to the half of the total number of 8*8 blocks and redundant information is added to the watermark using convolution code. In [17], the proposed method based on chaotic maps in order to encrypt the embedding position and to determine the pixel bit for embedding in host image. In [18], propose a spatial domain-watermarking scheme based on a block probability. The watermark is a binary image, which is permuted using a secret key and Gary code. The permuted watermark is embedded four times in different positions in the blue component of color image. The extraction of the watermark is by comparing the intensities of a block of 8*8 of the watermarked and the original images and calculating the probability of detecting '0' or '1'. The proposed method [16] are quite robust against some common image processing operations, such as median filter, scaling and rotation; however, they are less robust to cropping attack because the watermark bits are embedded into the whole image hence some data must be lost in cropping. The proposed method [18] is quite robust against cropping attack but not the noise attack.

.In this paper, we propose a spatial domain block based watermarking scheme. The watermark is a binary image, which is permuted using a secret key. The permuted watermark is embedded in five positions (top left, top right, bottom left, bottom right, center) in the LSB of color image.
The remaining paper is organized as follows: In Section II, we describe the Proposed Algorithm. In Section III, we describe the experimental results to explain the performance of algorithm. And in Section IV, we conclude our paper.

II. PROPOSED ALGORITHIM

Let the binary watermark is of size 64*64 be denoted as $W = \{W(i, j), 1 \le i \le 32, 1 \le j \le 32, w(i, j) \ (0,1)\}$. K is the secret binary image which is used as a key. The watermark is encrypted as follows.

$$W=' w \oplus$$

Where $\oplus$. denotes the XOR operation between the original watermark *W* and the a secret key k. Fig. 1,2 and 3 shows the original watermark, image which is used as a key and encrypted image which is uncorrelated to the original watermark and difficult to obtain without knowing the correct secret key.

Fig 1 Original Watermark

Fig 2 Key Image

Fig 3 Encrypted Image

A. Watermark Embedding

This section shows the proposed watermark embedding technique. The watermark image is a binary image where as the host image is an 8 bit color image. The watermark is embedded five times as shown in Fig.4 in non overlapping blocks of color image in order to protect the watermarked image .The five embedded positions are chosen to hide the watermarks in order to be robust against cropping attack from the bottom, the top or the left or the right side of the watermarked image and noise attack and make it difficult for attackers to destroy all of them. Suppose the original color image H with size of 512*512 pixels, which to be protected by the binary watermark W of size pixels 64*64, the original image H is divided into five non overlapping blocks and size of block equals to the size of watermark image i.e.64*64. Embedding the watermark requires the following steps

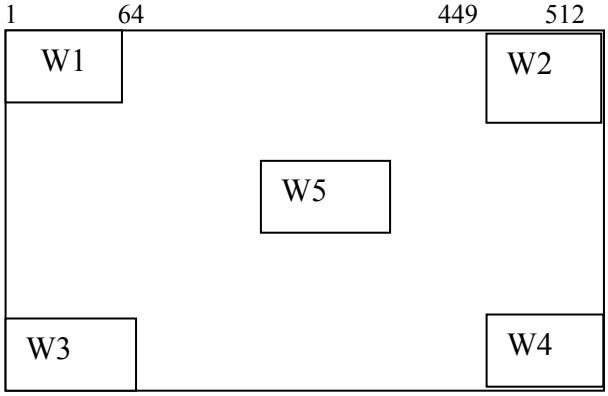

Fig 4. The proposed watermarks embedded positions

Algorithm: Watermark Embedding

Input: Color (Cover) Image (C) and binary Watermark image (W).

Step 1: The watermark W is permuted as described in section II.

Step 2: The original image H is divided into five non-overlapping blocks .Size of each block equals to the size of watermark image i.e. 64*64.

Step 3: Five blocks of image are at five position i.e. upper left, upper right, lower left, lower right and center of cover image.

Step 4: The encrypted watermark w1 is embedded into the first position of cover image .For this purpose the pixel intensities of cover image are converted into binary. Binary watermark is embedded into the LSB of cover image.Bec the watermark is binary it includes either 0 or 1 which is added into binary value of LSB.

Step 5: Other four watermark w2, w3, w4, w5 is embedded into four position of cover image in the same way as first watermark is embedded as describe in 4th step.

B. Watermark Extraction

Watermark extraction required the original host image and the original watermark; therefore, it is a non blind watermarking scheme. The steps of watermark extraction are

Step 1: Five watermarks (w1, w2, w3, w4, w5) are extracted from five positions i.e. upper and lower left and right and center of color image by extracting from LSB of pixel intensities of color image.

Step 2: Read a Binary key k. Key is xor with encrypted watermark as shown in following step.

Step 3: Perform $w1= W' \oplus k$

bec when we will perform xor two times it will perform decryption of encrypted watermark W.Means we will get original watermark.

Step 4: Other four encrypted watermark (w2, w3, w4, w5) are decrypted in the similar way as describe in step 3.

Step 5: After getting original watermark we can perform OR operation b/w

case1: w1 or w2

case2: w3 or w4

case3: w3 or w4 or w5

case4: w1 or w2 or w5

case5: w2 or w3

case 6: w4 or w1

case 7: w1 or w2 or w3 or w4 or w5

case 8: w4or w5

case 9: w2 or w3 or w4

Step 6: With the extraction of visual image watermark, we calculate the normalized cross correlation between the original watermark image W and the extracted watermarks W'1, W'2, W'3, W'4 to make a binary decision on whether a given watermark exists or not.

Step 7: Now we calculate the NCC (normalized cross correlation) of five watermark which are extracted through OR operation as described in step 5. Now the OR operation of watermarks with the highest NCC is considered the final watermark. The normalized cross correlation is defined by

$$NCC = \frac{\sum_i \sum_j W_{ij} W'_{ij}}{\sum_i \sum_j (W_{ij})^2}$$

III EXPERIMENTAL RESULTS

To verify the effectiveness of the proposed method, a series of experiments were conducted. In these experiments, a original image 'full2' is a color image of size 512 × 512, is used as test image, where as the watermark image is a binary image of size 64*64 pixels. Fig 5 and 6 show the original host image and the original watermark respectively, Fig.7 and 8 show the watermarked image and the extracted watermark, respectively .To evaluate perceptual distortion of the proposed technique, Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) are used, which is defined by

$$PSNR = 10 \log_{10} \left(\frac{255^2}{MSE} \right)$$

$$MSE = \frac{1}{3mn} \sum\sum \left[\left(r(i,j) - r^*(i,j) \right)^2 + \left(g(i,j) - g(i,j) \right)^2 + \left(b(i,j) - b^*(i,j) \right)^2 \right]$$

Where r (i, j) , g (i, j) and b (i,j) represents a color pixel in location (i, j) of the original image, r *(i, j) , g*(i, j) and b *(i, j) represents a color pixel of the watermarked image and m , n denote the size pixels of these color images. To test the robustness of the proposed scheme, some typical signal processing attacks, such as, salt and pepper noise, cropping and rotation are performed.

Fig. 5 Original imag

Fig. 6. Original watermark

Fig. 7 Watermarked image

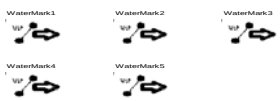

Fig. 8.Extracted watermark.

A. *Effects of Attacks*

The performance of proposed algorithm is analyzed by considering image processing attacks like cropping and noise attacks.

1.) Cropping:- The watermarked image is cropped in terms of percentage of image size. Fig. 9, 10, 11,12,13,14,15 and 16 show the results of cropping attack

Fig. 9 One quarter cropping

It can be seen clearly that the watermark can be extracted correctly under various cropping attack, even when the watermarked image cropped by 50% of the whole image with the cropped portions discarded and then the remaining 50% put in the center area; or when the 25% of the whole image remained from the top; or from the bottom of the watermarked image or when the watermarked cropped on both side by 25%. The experimental results show that our proposed method achieves better performance for cropping attack .In proposed algorithm ,we consider the result of OR operation with maximum NCC.

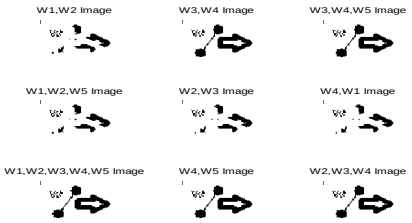

Fig. 10 Cases of OR operation

From Fig 10 its clear in case of One quarter Cropping ,results of (w3 or w4),(w3 or w4 or w5)are better than other.In these cases MSE and PSNR are 0 and Inf .

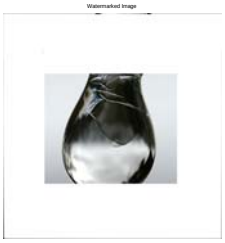

Fig. 11 Cropped watermarked image by 50%

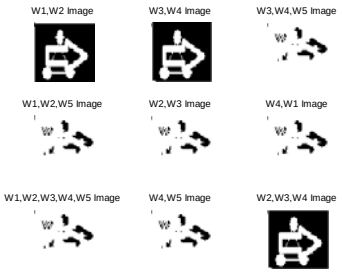

Fig. 12 Cases of OR operation

From Fig 12 its clear When we cropped image 50% then Cropping results of case 8 (W4 OR W5) are similar as of case 3,4,5,6,7 .MSE and PSNR in these cases are 0.0601 and 60.3451. When image is cropped 25% from both side then Cropping result of (W3,W4,W5),(W1,W2,W5),(W2,W3) cases are better than other OR operation.In these cases MSE and PSNR are 0.0601 and 60.3451 . When Image is cropped 75% even then result of MSE and PSNR come close to 0 and infinity of case2 (W3 or W4). NCC in all above cases is to be equivalent 1 which is shown in Table 1.

Fig. 13 Cropped watermarked image on both side by 25%

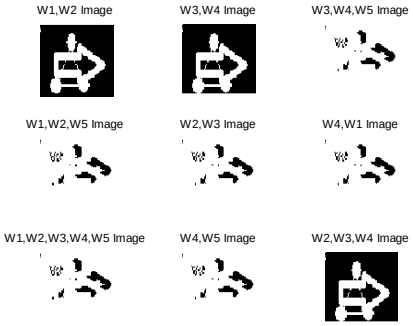

Fig 14 Cases of OR operation

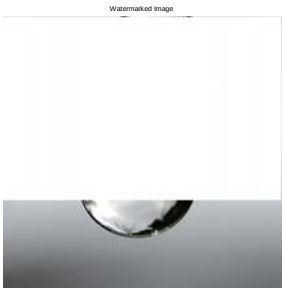

Fig. 15. Cropped watermarked by 75%

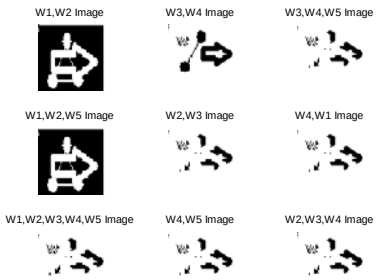

Fig.16. Cases of OR operation

TABLE I

MSE, PSNR and NCC RESULT of DIFFERENT CROPPING %

% Cropping	MSE	PSNR	NCC
One quarter cropping	0	INF	1.0
50% Cropping	0.06	60.34	1.0
25% cropping from both side	0.06	60.34	1.0
75% cropping	0	INF	1.0

2SALT and PEPPER NOISE:- The salt and pepper noise is added to the watermarked image I. The performance of extraction algorithm is analysed by increasing density of the noise starting from 0.01 up to 0.07. The extracted watermark and original watermark are compared in terms of NCC. Fig. 17,18,19 shows the effect of salt and pepper noise With density .001,.004,.007.We considered the OR case with highest NCC

Fig.17 Watermarked image under salt and pepper noise attack (intensity=0.1)

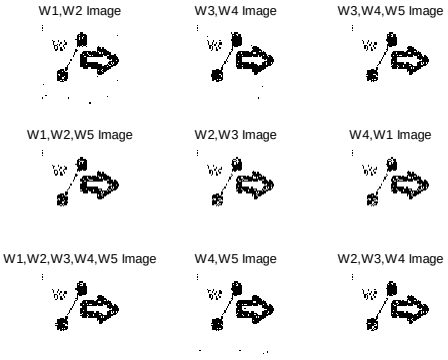

Fig. 18 Cases of OR operation (Best case is 7)

TABLE III

NINE CASES OF OR OPERATION UNDER NOISE INTENSITY 0.01

CASE	MSE	PSNR	NCC
Case1 (W1or W2)	0.0173	65.7418	.9973
Case 2 (W3 or W4)	0.0144	66.5459	0.9981
Case3 (W3 or W4 or W5)	0.0222	64.6640	0.9998
Case 4 (W1 or W2 or W5)	0.0234	64.4317	1.0000
Case 5 (W2 or W3)	0.0327	62.9834	1.0000
Case 6 (W4 or W1)	0.0293	63.4626	1.0000
Case7(W1orW2orW3orW 4or W5)	0.0193	65.2781	1.0000
Case 8 (W4 or W5)	0.0178	65.6212	0.9966
Case 9	0.0176	66.3305	.9975

In table 2, all case s with noise density 0.1 are shown. From table, it is clear 4 cases i.e. (W1 or W2 or W5), (W2 or W3), (W4 or W1), (W1orW2orW3orW4or W5) are having value of NCC parameter 1.The case is considered best if value of NCC is 1 ,MSE value is close to 0 and PSNR is close to infinity. but in case 4,5,6 value of MSE is more than as compare to case 7 but PSNR value is less than as compared to case 7. So Case7 (W1orW2orW3orW4or W5) is considered the best case.

Result of case 7 are MSE = 0.0151 PSNR =66.3305 NC = 0.9975

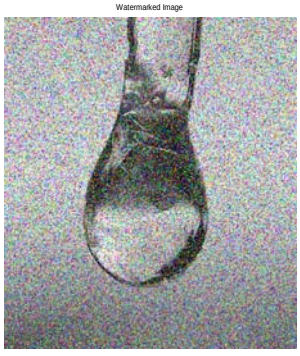

Fig.19 Watermarked image under salt and pepper noise attack (intensity=0.4)

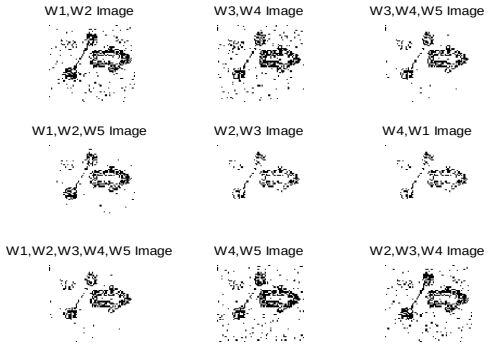

Fig. 20 Cases of OR operation(Best case 5)

From fig 20,its clear that when salt and pepper noise with intensity 0.4 is placed on image, then NCC of case 5(W4 OR W5) comes 1.0 than other cases.MSE and PSNR in this case are 0.0952 and 58.3438.

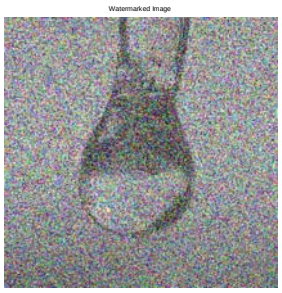

Fig .21 Watermarked image under salt and pepper noise attack (intensity=0.7).

From fig 22 ,its clear that when salt and pepper noise with intensity 0.7 is placed on image, then NCC of case 5(W4 OR W5) comes 1.0 than other cases.MSE and PSNR in this case are 0.1301 and 56.9871 .

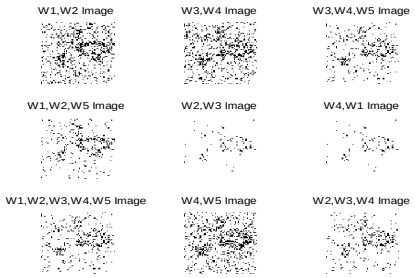

Fig. 22 Cases of OR operation (Best case is 5) NCC in all above cases is 0.1.

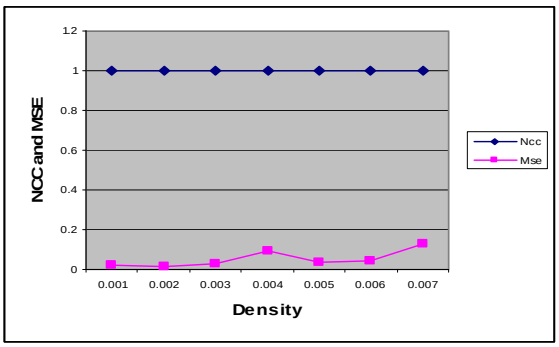

Fig. 23 Effect of salt and Pepper Noise

From Fig. 23 ,it is clear we have got approximately NCC =1 in all cases and MSE is close to 0 which shows best result as compared to other algorithims . In paper[18],as increase in the noise density reduces the performance of extraction algorithm. But in our proposed algorithm,as noise density is increased,proposed algorithm performance is not so decreased as shown in fig. 23

IV. CONCLUSIONS

A robust watermark scheme based on a block base for color image is presented, which operates in spatial domain by embedding the watermark image five times in different positions in order to be robust for cropping attack. The original image is not needed in the detection process, so it is a non-blind watermarking scheme. The experimental results show that our scheme is highly robust against various of image processing operations such as cropping with different % and salt and paper noise from .0001 to .007. It is also secure scheme. The proposed algorithm is weak to geometrical transformation attack such as rotation, translation, scaling. Thus the future work is to design a geometrical transform-invariant watermarking algorithm.

REFERENCES

[1] W. Bender,D.Gruhl,N.Mormoto, and A.Lu,*Techniques for data hiding*, IBM Systems Journal, vol. 35, no 3 pp 313-336, 1996.

[2] F. Hartung and M. Kutter, "*Multimedia watermarking techniques*," Proceedings of the IEEE, vol. 87, pp. 1079-1107, 1999.

[3] Francesc Sebe, Josep Domingo-Ferrer, and Jordi Herrera, Spatial-Domain *Image Watermarking Robust against Compression, Filtering, Cropping, and Scalin*g Universitate Rovira i Virgili, Department of Computer Science and Mathematics, Springer-Verlag Berlin Heidelberg , LNCS 1975, pp. 44–53, 2000.

[4]Y. K. Lee and L. H. Chen, "*High capacity image steganographic model*," Vision, Image and Signal Processing, IEEE Proceedings -, vol. 147, pp. 288-294, 2000

[5] Hsiang-Kuang Pan, Yu-Yuan Chen, and Yu-Chee Tseng, "*A Secure Data Hiding Scheme for Two-Color Images*", in Fifth IEEE Symposium on Computers and Communications, pp. 750 – 755, July 2000.

[6] M. Wu, E. Tang, and B. Liu, "*Data hiding in digital binary image*," Electrical Engineering Dept., Princeton Univ., Princeton, NJ 08544,Electrical & Computer Engineering Dept., John Hopkins Univ., Baltimore, MD 21218 in Proc. Of IEEE Int. Conf. on Multimedia and Expo, New York City, pp. 393-396, July 31 to August 2, 2000

[7] F. A. P. Petitcolas, "*Watermarking schemes evaluation*," I.E.E.E. Signal Processing, vol. 17, no. 5, pp. 58–64, September 2000

[8] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk,*"Watermarking digital image and video data. A state of the-art overview,*" Signal Processing Magazine,IEEE, vol. 17, pp. 20-46, 2000.

[9] Ping Wah Wong and Nasir Memon, "*Secret and public key image watermarking schemes for image Authentication and ownership verification"* IEEE transactions on image processing, vol. 10 no. 10, pp 1593-1600, October 2001

[10] H.Ren-Junn, K. Chuan-Ho, and C. Rong-Chi, "*Watermark in color image,"* Proceedings of the first International Symposium on Cyber Worlds, pp. 225-229, 2002.

[11] C.De Vleeschouwer, J.F.Delaigle, and B.Macq,*"Invisibility and application functionalities in perceptual watermarking an overview," Proceedings of the IEEE*, vol. 90, pp.64-77, 2002.

[12] P.Bas, J. M. Chassery and B.Macq, *"Geometrically Invariant Watermarking Using Feature Points"*, IEEE Trans. On Image Processing, vol. 11, No. 9, pp 1014- 1028, 2002

[13] S. Kimpan, A. Lasakul, and S. Chitwong,"*Variable block size based adaptive watermarking in spatial domain*," presented at Communications and Information Technology, ISCIT 2004. IEEE International Symposium on, vol. 1, pp. 374-377, 2004.

[14] Feng-Hsing Wang, Lakhmi C. Jain, Jeng-Shyang Pan, *"Hiding Watermark in Watermark*", in IEEE International Symposium in Circuits and Systems (ISCAS) ,Vol. 4, pp. 4018 – 4021, May 2005

[15] Juan Jose Roque, Jesus Maria Minguet *SLSB: Improving the Steganographic Algorithm LSB* Universidad Nacional de Educación a Distancia, 2006.

[16] B. Verma, S. Jain, D. P. Agarwal, and A.Phadikar, *"A New color image watermarking scheme,"* Info comp, Journal of computer science , vol. 5,No.2, pp. 37-42, 2006.

[17] X. Wu and Z.-H. Guan, *"A novel digital watermark algorithm based on chaotic maps*," Department of Control Science and Engineering, Huazhong University of Science and Technology, Wuhan, Hubei 430074, PR Chinab School of Electronics and information, Yangtze University, Jingzhou, Hubei 434023, PR China, Science Direct, Physics Letters A, vol. 365, pp. 403-406, 2007.

[18] Ibrahim Nasir, Ying Weng, Jianmin Jiang, *"A New Robust Watermarking Scheme for Color Image in Spatial Domain",* School of Informatics, University of Bradford, UK 2008.

[19] Nagaraj V. Dharwadkar and B. B. Amberker ,*Secure Watermarking Scheme for Color Image Using Intensity of Pixel and LSB Substitution*, journal of computing, volume 1, issue 1, ISSN: 2151-9617, December 2009 .

[20] V.Madhu Viswanatham, Jeswanth Manikonda, *Novel Technique for Embedding Data in Spatial Domain* ,School of Computing Science and Engineering, VIT University, Vellore, India, International Journal on Computer Science and Engineering Vol. 02, pp.233-236,2010.