

An Additive Watermarking Technique in Gray Scale Images Using Discrete Wavelet Transformation and Its Analysis on Watermark Strength

Kamaldeep Joshi, Rajkumar Yadav, Ashok Kumar Yadav

Abstract—Digital Watermarking is a procedure to prevent the unauthorized access and modification of personal data. It assures that the communication between two parties remains secure and their communication should be undetected. This paper investigates the consequence of the watermark strength of the grayscale image using a Discrete Wavelet Transformation (DWT) additive technique. In this method, the gray scale host image is divided into four sub bands: LL (Low-Low), HL (High-Low), LH (Low-High), HH (High-High) and the watermark is inserted in an LL sub band using DWT technique. As the image is divided into four sub bands, a watermark of equal size of the LL sub band has been inserted and the results are discussed. LL represents the average component of the host image which contains the maximum information of the image. Two kinds of experiments are performed. In the first, the same watermark is embedded in different images and in the later on the strength of the watermark varies by a factor of s i.e. ($s=10, 20, 30, 40, 50$) and it is inserted in the same image.

Keywords—Watermarking, discrete wavelet transform, scaling factor, steganography.

I. INTRODUCTION

TODAY, watermarking is a skill and a discipline of hiding information in multimedia carrier [1]. Watermarking is an application of the steganography. The word steganography is taken from a Greek word which means cover writing [2]. The widespread use of the internet makes the information faster for sharing and exchanging. So, it is necessary to provide security from unauthorized users. Intellectual property, modification and copyright protection are major issues in digital world [3]. Steganography sends message by concealing it so that the intruder cannot detect the presence of the message. Today, transferring the data through the internet in public network is not secure. Watermarking is one of the applications of the steganography. Digital watermarking is one of the best tools to protect the illegal copying and copyright protection [4]. It is an effective tool to prevent a digital document from unauthorized activities [5].

K. Joshi is with the Department of Computer Science and Engineering, University Institute of Engineering and Technology, Maharshi Dayanand University, 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).

AK. Yadav is with the Department of Computer Science and Engineering, Amity University, Noida, India. (Phone: +919911375598; e-mail: ashok_kuk@yahoo.com).

In digital watermarking, the watermark is embedded and extracted using insertion and retrieval algorithm respectively. The main properties of the watermark are: Transparency, Robustness, and Imperceptibility. The watermark can be performed in the spatial or frequency domain [6].

A. Spatial Domain

In the spatial domain, embedding of watermark is done through direct alteration of the pixel values of the cover image. LSB is one of the best techniques in spatial domain.

In 1-bit LSB method the message is hidden at one LSB of a pixel. In 2-bit LSB the message is hidden at two LSBs. Similarly, in three bit LSB method the message is hidden in last three bits of a cover image [7].

B. Frequency Domain

In this technique, watermark is inserted into the host image using various transformations like Discrete Cosine Transformation (DCT), DWT and Discrete Frequency Domain (DFT). It shows better robustness when compared to the spatial domain technique [8].

1) *DCT*: In DCT method, firstly original images divided into 8×8 blocks of pixels to hide the secret data. It divides the watermark into high, low and medium frequency domain. If any changes occur in single coefficient, then it can affect the all 64 blocks pixel [9]. The DCT coefficient is used for image compression. Equations (1) and (2) are used to calculate DCT and its inverse DCT:

$$F(u, v) = \frac{1}{4} C(u)C(v) \sum_{x=0}^7 \sum_{y=0}^7 f(x, y) \cos \left[\frac{\pi(2x+1)u}{16} \right] \cos \left[\frac{\pi(2y+1)v}{16} \right] \quad (1)$$

For $u=0, \dots, 7$ and $v=0, \dots, 7$

$$\text{where } C(k) = \frac{1}{\sqrt{2}} \text{ for } k=0 \\ 1 \text{ otherwise}$$

Inverse DCT

$$F(u, v) = \frac{1}{4} \sum_{x=0}^7 \sum_{y=0}^7 C(u)C(v) f(x, y) \cos \left[\frac{\pi(2x+1)u}{16} \right] \cos \left[\frac{\pi(2y+1)v}{16} \right] \quad (2)$$

For $x=0, \dots, 7$ and $y=0, \dots, 7$

Middle frequency range coefficient is taken from DCT coefficients and changes in the value encode a one or zero in order to embed the bits. For extraction, inverse DCT is

performed [10].

- 2) *DWT*: It performs multi-resolution decomposition of images using a wavelet function. It has its own space frequency property. DWT provides spatial and frequency spread of watermark in cover image [11]. DWT divides the signal into high and low frequency. The high part holds edge element and lower part again divides into two frequencies i.e. low and high. At high frequency, changes in edges are invisible to human [12]. It divides the frequency in four sub bands, as shown in Fig. 1. It decomposes the signal into mutually orthogonal signals. This is the main difference between continuous wavelet transform (CWT) and discrete wavelets transform (DT-CWT). A scaling function is used for constructing wavelet transform because scaling function defines all scaling properties. Some mathematical conditions in DWT are as follows: e.g. Dilation equation.

$$\phi(x) = \sum_{-\infty}^{\infty} ak \phi(s_x - k)z \quad (3)$$

where s is scaling factor and ak is finite set of coefficient which defines the scaling function and the wavelet.

$$\int_{-\infty}^{\infty} \phi(x) \phi(x+l)dx = \delta_0, l \quad (4)$$

DWT is superior transformation because it has two main features: Multi-resolution & the best image localization.

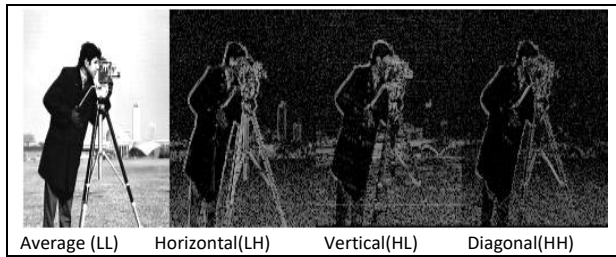


Fig. 1 One level decomposition of Cameraman image

LL	HL
LH	HH

Fig. 2 One level decomposition

LL1	HL1	HL
LH1	HH1	
LH		HH

Fig. 3 Two level decomposition

- 3) *Discrete Frequency Domain (DFT)*: The Discrete frequency domain is used for getting the frequency component for each pixel of the cover image. The DFT of Spatial value $f(u, v)$ for image size $m \times n$ is defined by [14]:

$$F(u, v) = \frac{1}{\sqrt{MN}} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(x, y) e^{-12\pi \frac{ux}{M} + \frac{vy}{M}} \quad (5)$$

In inverse discrete frequency transformation equation, the frequency domain component is converted into the spatial domain. The inverse DFT is given by:

$$F(x, y) = \frac{1}{\sqrt{MN}} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u, v) e^{12\pi \frac{ux}{M} + \frac{vy}{M}} \quad (6)$$

In Fourier transform, the output image is produced in complex number value which could be displayed in two images having two parts i.e. real and imaginary part.

II. RELATED WORK

Singh et al. projected a method to insert multiple watermarks in spatial and frequency domain to make assets secure and dividing the host image into two regions: Region A and region B. In region A, the owner information is inserted with the help of LSB technique and in region B, the watermark is inserted with additive technique DCT-DFT [13]. Singh et al. proposed a method i.e. robust deinterlacing multiple image watermarking technique in DWT. In this method, deinterlacing process was applied to sub band of image according to even and odd row pixel value. Chen et al. also projected a technique which embeds the watermark with the help of frequency domain [15]. Razavi et al. proposed a technique i.e. robust digital image watermarking for protection real property rights using singular value decomposition and DCT [16]. Raval et al. analyzed the performance of multiple watermark image in the low and high frequency sub-band of 2nd level of DWT by inserting 2 different binary watermarks using an additive scaling method by taking strength factor of watermark 0.10 [17]. Ranjan et al. proposed a method which secures non blind based watermark by inserting a binary watermark into last pixel of each block after applying one level of DWT and DCT of block size 8×8 [18]. Sridhar et al. applied multiple watermarking on a single host image. Their proposed method decomposes the host image by using DWT technique. First the image was divided into even and odd number of rows. Then two different images were inserted into these two divided parts. After embedding inverse DWT is applied on sub-bands of the host image and watermarked image is generated [19].

III. PROPOSED WORK

In this paper, the analysis performance of watermark in low frequency sub band of 1st level of DWT by inserting different watermarks using scaling factor i.e. s is performed. DWT decomposes the image into four part which are named as horizontal, vertical, diagonal and average. The result is given in the form of four tables i.e. Table I-IV.

The watermark is added at the low sub band of DWT transformation. We have taken grayscale images of the experimental setup. In our proposed work, the watermark is inserted in the LL sub band using a scaling factor by taking strength factor of watermark equal to 10.

Let I represent a gray level host image having $R_x * C_y$ pixels and represented as

$$I = \{i_{xy} \mid 0 \leq x < R, 0 \leq y < C, i_{xy} \in \{0, 1, \dots, 255\}\}$$

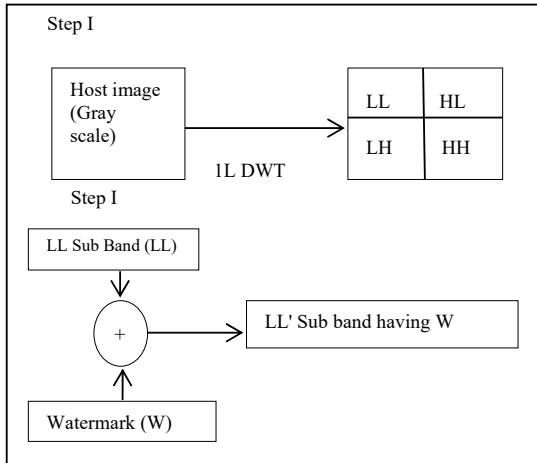


Fig. 4 Wavelet decomposition of host image and Watermarking Process

Let W be a binary watermark image having $R * C$ pixels

$$W = \{w_{xy} \mid 0 \leq x < R, 0 \leq y < C, w_{xy} \in \{0, 1\}\}$$

where $W(x, y) = LL(x, y)$. Let I' be the watermarked-image such that $I' = I + W$ and represented as

$$I' = \{i'_{ij} \mid i'_{ij} = I(LL)_{ij} + w_n, s_{ij} \in \{0, 1, \dots, 255\}\}$$

A. An Algorithm for Embedding the Watermark

1. Input the Gray scale image $I(x, y)$
2. Apply 1-level DWT on host image $I(x, y)$ and we got four sub band of host image: LL, HL, LH and HH.
3. Select watermark image W such that $W(x, y) = LL(x, y)$; Otherwise resize watermark.
4. Insert watermark in LL sub band using additive approach i.e. $LL' = LL + W(x, y)$.
5. Apply inverse DWT on LL' sub band and its respective sub bands i.e. HL, LH and HH.
6. Calculate and find PSNR, MSE, MAXERR and L2RAT, $LL' = LL + W(x, y) * S$, S is scaling factor which is multiplied by W to increase the strength of W

B. Algorithm for Extraction the Watermark:

1. Get the watermarked image $I'(x, y)$.
2. Apply DWT transformation on $I'(x, y)$.
3. Read the host image $I(x, y)$.
4. Apply DWT Transformation on $I(x, y)$ and $I'(x, y)$.
5. Find $W(x, y) = LL(x, y)$ of $I' - LL(x, y)$ of I .

IV. EXPERIMENTAL RESULT

In this section, the experimental result of the DWT watermarking is presented with illustration. The sample images having sizes $256 * 256$ were taken from USC-SIPI database. For our experimental work, we used MATLAB software.

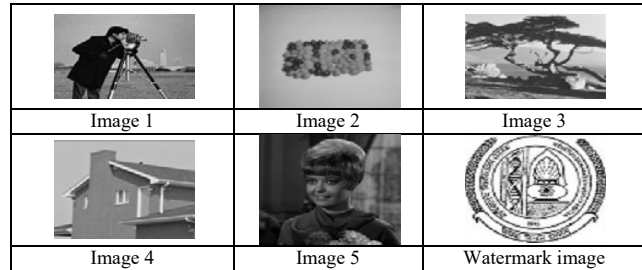


Fig. 5 Five cover (gray scale) images and one watermark image

PSNR determines the quality of original and stego image. Larger PSNR shows the goodness of the watermarking technique [20]. MSE is the average square error of original and stego image it can be estimated more than one way to define the difference between the estimated value and true quality of the image. It is the risk function to calculate expected value of squared error [20].

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad (7)$$

$$MSE = \frac{1}{N \times M} \sum_{i=1}^N \sum_{j=1}^M (a_{ij} - b_{ij})^2 \quad (8)$$

where a_{ij} , and b_{ij} are the pixels of stego and original image respectively. M and N are the rows and column of the image.

A. Result Analysis

Table I represents the watermark strengths i.e. i.e. after multiplying the watermark by a factor of 10. The strength of watermark is increased step by step and the histogram analysis is done on the original and watermarked image. For Table I, the image is kept same and the intensity of watermarked is varied gradually till the intensity reaches 15, the watermarked image does not show any change. After 15 the watermark is visible in the host image. Table I also contains the histogram analysis of the watermarked and host image i.e. cameraman. Table II demonstrates the watermarked image and the watermark which has been inserted in the host image. It also includes the histogram analysis of watermarked and different host image.

TABLE I
FIXED WATERMARKED IMAGE AND FIXED WATERMARK INTENSITY AND HISTOGRAMS OF ORIGINAL AND WATERMARKED IMAGE



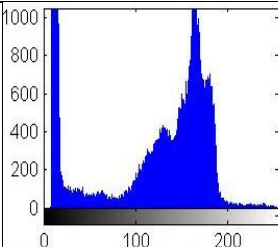
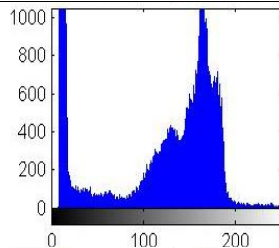


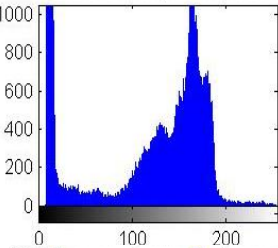
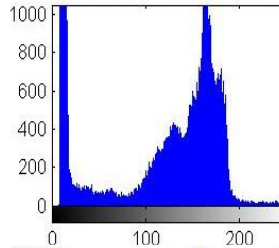


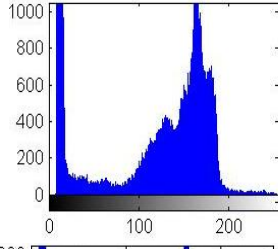
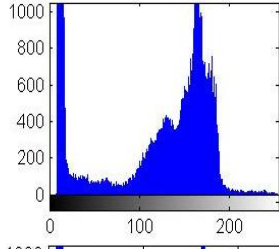


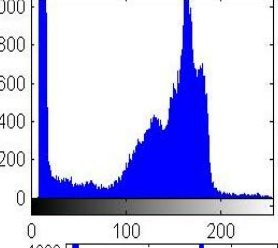
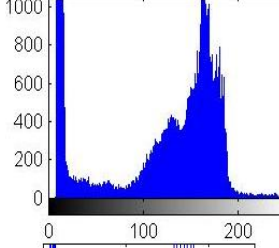


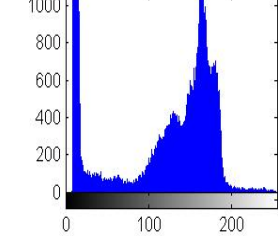
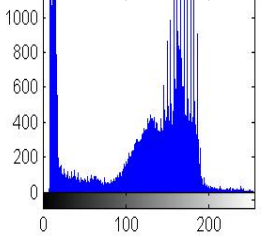
Watermark Strength	Watermarked image	Watermark	Original image histogram	Stego image histogram
10				
20				
30				
40				
50				



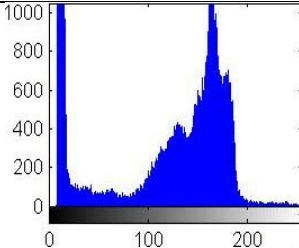
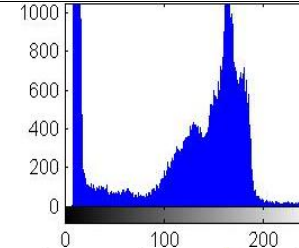


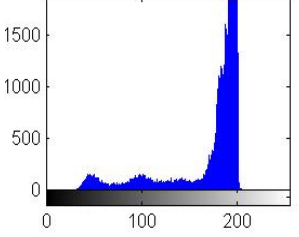
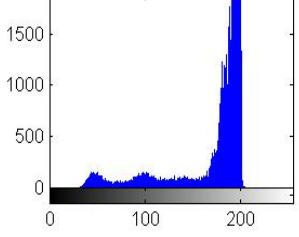


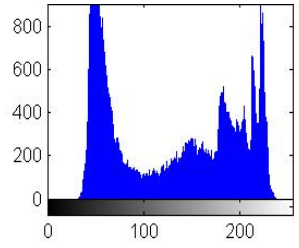
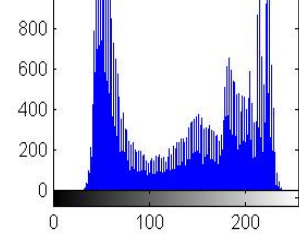


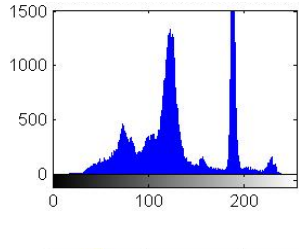
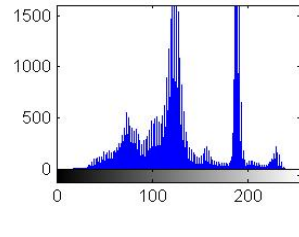


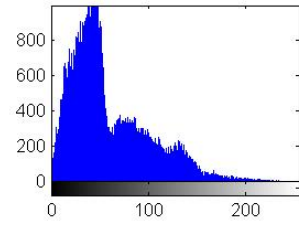
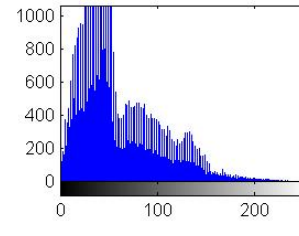
TABLE II
PSNR, MSE, MAXERR AND L2RAT OF FIXED IMAGE (CAMERAMAN: 256*256) AND VARIABLE WATERMARK INTENSITY

Image name	Watermark strength	PSNR	MSE	MAXERR	L2RAT
1	10	34.7897	21.5832	7.1651	1.0583
2	20	28.7691	86.3326	14.3301	1.0966
3	30	26.8309	134.8947	17.9127	1.1370
4	40	25.2472	194.2484	21.4952	1.1776
5	50	22.7485	345.3305	28.6603	1.4731

TABLE III
VARIABLE IMAGES AND FIXED WATERMARK INTENSITY AND HISTOGRAMS OF ORIGINAL AND WATERMARKED IMAGE

Image name	PSNR	MSE	MAXERR	L2RAT
1	54.7897	0.2158	0.7165	1.0047
2	52.7897	0.2389	0.7165	1.0052
3	56.7897	0.2002	0.7165	1.0102
4	57.7897	0.1989	0.7165	1.0056
5	54.0098	0.2199	0.7165	1.0057
Average of 50 images	50.7897	0.2500	0.7165	1.0057

TABLE IV
PSNR, MSE, MAXERR AND L2RAT 256*256 FIXED IMAGE AND VARIABLE WATERMARK INTENSITY

Image name	Watermarked Image	Watermark	Original image histogram	Stego image histogram
1				
2				
3				
4				
5				

V. CONCLUSION

In this paper, an additive scaling factor technique using DWT is being presented. The aim of watermarking algorithms is to make watermark secure and invisible to the human eye. We analyzed scaling factor technique using DWT with different scaling factor and grayscale images. We get the result in a form of PSNR, MSE, MAXERR and L2RAT. Table IV shows result with variable images and fixed watermark. If we increase the scaling factor of the watermark, then the size of PSNR is decreased and MSE, MAXERR is increased. The imperceptibility is inversely proportional to the intensity of the

watermarked image. And the watermark is visible if the value of the scaling factor is greater than 15. Table II shows the results. If the scaling factor is below 15 then the watermark will not be visible to the human eye. Table I shows the results.

REFERENCES

- [1] Rama Kishore, Sunesh (2015). Digital Watermarking Based on Visual Cryptography and Histogram International Journal of Computer, Electrical, Automation, Control and Information Engineering, World Academy of Science, Engineering and Technology, Vol:10, No:7,
- [2] Hussain, M., & Hussain, M. (2013). A Survey of Image Steganography Techniques, 54, 113–124.

- [3] Rao, S. S. (2003). Copyright: its implications for electronic information. *Online Information Review*, 27(4), 264–275. <http://doi.org/10.1108/14684520310489050>
- [4] Nyeem, H., Boles, W., & Boyd, C. (2014). Digital image watermarking: its formal model, fundamental properties and possible attacks.
- [5] Singh, S. (2016). A Robust Deinterlacing Multiple Image Watermarking Technique in DWT, 261–266.
- [6] Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing*, 90(3), 727–752. <http://doi.org/10.1016/j.sigpro.2009.08.010>
- [7] Muhammad, K., Sajjad, M., Mehmood, I., Rho, S., & Baik, S. W. (2015). A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image. *Multimedia Tools and Applications*. <http://doi.org/10.1007/s11042-015-2671-9>
- [8] Malekmohamadi, H., & Ghaemmaghami, S. (2009). Steganalysis of LSB based image steganography using spatial and frequency domain features. 2009 IEEE International Conference on Multimedia and Expo, 1744–1747. <http://doi.org/10.1109/ICME.2009.5202858>
- [9] 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>
- [10] Karri, S., & Sur, A. (2014). Steganographic algorithm based on randomization of DCT kernel. *Multimedia Tools and Applications*, 74(21), 9207–9230. <http://doi.org/10.1007/s11042-014-2077-0>
- [11] Chen, P., & Lin, H. (2006). A DWT Based Approach for Image Steganography, (4), 275–290.
- [12] Atawneh, S., & Sumari, P. (2013). Hybrid and blind steganographic method for digital images based on DWT and chaotic map. *Journal of Communications*, 8(11), 690–699. <http://doi.org/10.12720/jcm.8.11.690-699>
- [13] Singh, S. (2016). Region Based Undetectable Multiple Image Watermarking Technique in DWT, 267–270.
- [14] 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>
- [15] Chen, P., & Lin, H. (2006). A DWT Based Approach for Image Steganography, (4), 275–290.
- [16] Babakalak, S. R., Balafar, M. A., & Farzan, A. (n.d.). A new DWT-SVD based robust watermarking scheme for real property rights, 4274, 69–78.
- [17] MS raval and PP Rege. "Discrete wavelet transform based multiple watermarking scheme", in the proceeding of IEEE conference on convergent technologies for the Asia-Pacific Region. In *tencon*. vol.3, pp.935-938, 2003
- [18] Ranjan Kumar Arya, Shalu singh. and Ravi Saharan, "A secure Non-blind block based digital Image Watermarking technique using DWT and DCT" In the Proceeding of IEEE. *Advances in computing communication and informatics (ICACCI)*, pp. 2042-2048. 2015
- [19] B.Sridhar, DR. C. Arun, "On secure multiple image watermarking technique using DWT", IEEE Third national conference on computing Communication & networking technologies (ICCNET), 2012
- [20] Joshi, K. (2016). PSNR and MSE Based Investigation of LSB, IEEE Third national conference on computing Communication & networking technologies (ICCNET), 2012 178–183.

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.