International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol. 2, Issue. 5, Sep.-Oct. 2012 pp-3869-3875 ISSN: 2249-6645

Investigation and Analysis of Vulnerability of Attacks on Watermarked Image and Its Enhancement

G. Srinivas Reddy[1], T.Venkat Narayana Rao[2], Dr.A.Govardhan[3]
[1,] *Assistant Professor, Mahatma Gandhi Institute of Technology [MGIT], Hyderabad, A.P. India*
[2,] *Scholar JNTU-K and Hyderabad Institute of Technology and Management [HITAM], Hyderabad, A.P, India*
[3,] *Director of Evaluation and Professor, C.S.E, Jawaharlal Nehru Technological University, Hyderabad, A.P. India*

ABSTRACT: *This paper demonstrate the attempt to evolve feasible solution to the scenario in which different possible attacks on embedded watermark can be avoided along with the enhancement of the content retrieved from noisy image post watermarking. With the revolution of information technology and wide area networking, data has become less private where in the admittance of media as well as the attempts to change and manipulate the contents of information has become a universal issue. Watermarking techniques have to be used to protect the copyright of the media and for the digital management but without compromising on the visual front. A universal DWT technique is used in this work. The algorithm for embedding watermark into the original image has been developed with novelty for better results than existing mechanisms. The various attacks such as image resizing, image cropping and image filtering are employed on the watermarked image to investigate the reliability of embedding algorithm. It is reported that Peak Signal to Noise Ratio (PSNR) value obtained before and after the attack has been in the ratio of 0.01 to 0.07. The extracted watermark is addressed again to enhance the PSNR value with various de-blurring techniques such as DCT compression, image cropping with noise treatment, Normal and Wiener filtering.*

Keywords: *Attacks, Watermarking, Image Filtering, Extraction, PSNR.*

I. INTRODUCTION

The growth of networked multimedia systems has magnified the need for image copyright protection from any illegal duplication of their data and manuscripts [1]. Some serious work needs to be done in order to maintain the availability of multimedia information but, in the meantime, the industry must come up with the ways to protect intellectual property i.e. the stake of distributors and owners of data [11]. The rapid expansion of Internet in the past years has increased the availability of digital data such as audio, images and videos to the public. The idea of robust watermarking of images is to embed information data within the image with an insensible form for human visual system but in a way that protects from attacks such as common image processing operations [2]. The goal is to produce an image that looks exactly the same to a human eye but still allows its positive identification in comparison with the owner's key if necessary [12]. The fundamental tool of DWT is used in

the present study and is shown in the figure1. The number of vanishing moments describes this property. Scaling function derived from wavelets with higher number of vanishing moments can independently represent polynomials of higher orders [7]. The basic figure 1 depicts the DWT that attracts a universal utility by the researchers in the field of image processing.

II. PROPOSED METHODOLOGY

The Phases In This Proposal Of The Present Investigation Are Mainly Centered At Attacks Possible On Embedded Watermark Image And Developing The Extracted Water Mark Image. Different Attacks May Be Possible On The Information Embedded In The Image. The Investigation Of All Possible Attacks Has Been Addressed By Using Operations Like Image Filtering, Image Resizing And Image Cropping. The Algorithm Used For Watermark Extraction Is Idwt Algorithm And Watermark Retrieved Image Is De-Blurred With Techniques Such As Normal Filtering, Weiner Filtering And Dct Compression. The Psnr Values Have Been Computed At Various Levels For Comparison And Analysis On Output Images [8].

The Haar wavelet transform which is one of the basic tools in embedding mechanism of water mark is one kind of wavelet transform implemented in the investigation as shown in figure 2-3. A digital image I with m x n pixels is transformed to the DWT frequency domain as follows. First, a cover image is decomposed into a low frequency band LL1 and three high frequency bands LH1, HL1 and HH1. Later applying the DWT on the low frequency band LL1 again will generate four lower-resolution sub-bands LL2, LH2, HL2 and HH2. This process is continued an arbitrary number of times, which is usually determined by the application available or a simple algorithm. The approximate image band LL holds the most important information of the original image. The LH, HL and HH bands contain some high-frequency information about the edge components of the signal [4]. In addition, from these DWT coefficients; the original signal can be reconstructed. This reconstruction process is called the inverse DWT (IDWT). An image can be decomposed into a pyramid structure as shown below. Figure 4 shows the image "Lena" and the transformed result after the two-level DWT transformation.

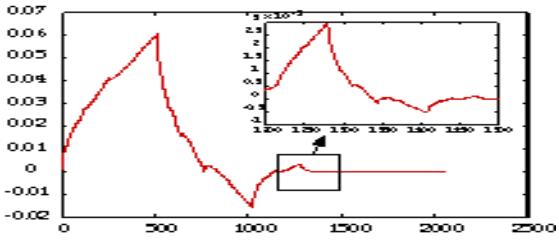


Fig. 1: Discrete Wavelet Transform

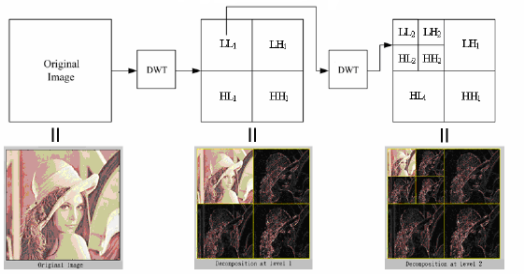


Fig. 2: Three levels Haar Decomposition

The following equations that are universally established in the literature have been employed in the investigation to generate the components of LL_1, $LH_!$, HL_1 and HH_1 values respectively.

$$LL_1(x,y)=\frac{1}{4}\sum_{i=0}^{1}\sum_{j=0}^{1} I(2x+i,2y+j) \quad (1)$$

$$LH_1(x,y)=\frac{1}{4}\sum_{i=0}^{1} I(2x+i,2y)-\frac{1}{4}\sum_{i=0}^{1} I(2x+i,2y+I) \quad (2)$$

$$HL_1(x,y)=\frac{1}{4}\sum_{j=0}^{1} I(2x,2y+j)-\frac{1}{4}\sum_{j=0}^{1} I(2x+1,2y+j) \quad (3)$$

$$HH_1(x,y)=\frac{1}{4}\{I(2x,2y)+I(2x+1,2y+1)- I(2x+1,2y)-I(2x,2y+1)\} \quad (4)$$

Watermarking in the DWT domain includes two parts i.e. Encoding and Decoding. In decoding method we propose hierarchical approach. Post decomposition the received image and the original image is compared. Later the signature is added in the HH_1 band and the difference of the DWT coefficients in HH_1 bands calculated with their cross correlations. In watermarking process, the image is decomposed into frequency bands using three resolutions of Haar wavelets. Figure 2 represents the idea of the octave-band structure of Haar wavelets, which offer pyramid structure [9]. We must focus on, sampling operation after every filtering. It must be understood that the choice of the Haar wavelet in our system is made for simplicity. However, we intend to investigate the influence of the selection of wavelet function in our results but, in order to test the robustness openly, we had to relinquish the idea in support of the addition of extra robustness testing procedures [14].

III. IMPLEMENTATION

3.1 Watermark Generation and Xie's DWT, Quantization, Blind Image Watermarking Algorithm

The mark is a Gaussian sequence of pseudo-random real numbers and will be denoted X = x1, x2,….xn were n is length of watermark. The choice of the watermark length n determines to which degree the watermark is spread out. In most cases the larger the watermark the lesser the embedding strength. There is no one watermark length n that is suitable for all images, therefore it is image specific [3]. This algorithm is the stronger of the two watermarking algorithms used and was first introduced in the paper by Liehua Xie and Gonzalo R. Arce i.e. Joint wavelet compression and authentication watermarking that describes a blind watermarking algorithm for embedding watermark for authentication[13]. The watermark algorithm is implemented in the Discrete Wavelet Transform, DWT. Xie and others also converse about implementation of SPIHT compression algorithms. Since this is a blind algorithm the watermark is extracted without the original image. The median of the sliding window is determined and quantized to obtain a reconstruction point [10]. The bit value is then determined from the associated reconstruction point which is assigned to xi* where X* is extracted watermark. The extracted watermark, X*, is then compared with that of the original watermark X.The basic mechanism for embedding process is followed mathematically as shown in the figure 3.

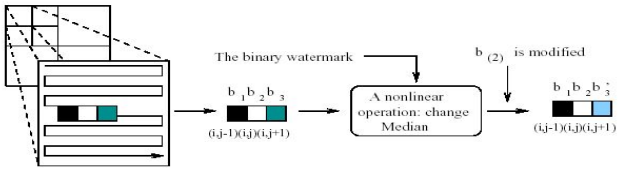


Fig. 3: Xie Embedding Watermark Method

Scheme of the proposed approach is showcased in figure.4

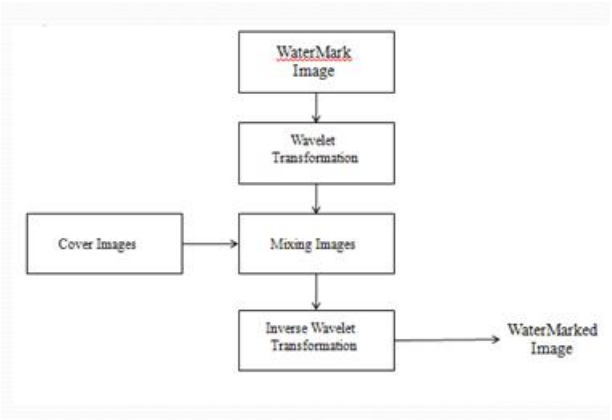


Fig. 4 Embedding Watermarking in image

3.2 The Watermark Embedding Phase

Basic DWT is implemented to embed the water mark in the image. Following are the steps in Embedding Algorithm:

Input: The color image H(N x N) and watermark W_p (2M x 2M)
Output: The embedded image (watermarked image)
Step 1: Applying one level DWT on the image H. to get the blocks
Step 2: Applying three level on watermark W_p to obtain four blocks. W_p^1 (LL band), W_p^2 (LH band), W_p^3 (HL band), W_p^4 (HH band)
Step 3: Select the blocks W_p^1, W_p^2, W_p^3, W_p^4 of watermark and transform to binary streams. $WR^n(K)$, $WG^n(K)$ and $WB^n(K)$ respectively where K = 1, 2, …… N/8 x N/8
Step 4: For n = 1 to 4, do steps 1 to 3. Transform the blocks of original image to binary bit streams. For K = 1 to M x M, do step as follows. If K is odd, embed watermark into original image according to the logic rules
Step 5: Applying one level IDWT to obtain watermarked image.

3.3 Attacks possible on embedded image

This section demonstrates the potentiality of embedding algorithm implemented in the work and focus on robustness and reliability.The figure 5 shows the possible assumed attacks in the present study.

i. **Active attacks**: Here, the hacker tries deliberately to eradicate the watermark or simply make it undetectable. This is a big issue in copyright protection, fingerprinting or copy control.

ii. Pa**ssive attacks**: In this case, the attacker would try to remove the watermark but simply attempting to determine if a given mark is present or not. As the reader should understand, protection against passive attacks is of the utmost importance in covert communications where the simple knowledge of the presence of watermark itself poses immense vulnerability in the future.

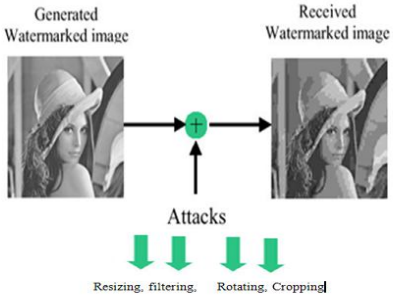


Fig. 5 shows the various attcks possible on the embedded water image

3.4 Image operations used in the Implementation: Image resizing, Image cropping and Image filtering.

i. Image resizing: Aim of this attack on watermarked image is either to remove or to identify the watermark. Averaging every pixel in certain number leads to reduction dimensionality of image [15]. In this section it is to attempt the technique for removing or tracing the watermark of original image. The attack would be performed with the following steps.

Input: Watermarked Image
Output: Attacked watermarked image
Step 1: Select the watermarked image I_w (N x N)
Step 2: Changing the pixel format
Step 3: Transform to the data type of the pixels to double and converting to single row of matrix.
Step 4: Calculating the average of certain number of pixels in overlapped manner
Step 5: Displaying the attacked output image.

ii. Image Cropping Attack: Using the crop tool of image editing program which would draw a box around a selected portion of your digital image. When you execute the crop tool the remaining picture contains only what was inside the drawn box. A standard crop tool allows you to draw a rectangle of any height and width ratio. Most image editing programs would allow to crop to a constrained ratio or proportion like 8 by 10 or 5 by 7[14]. Some image editing programs will allow you to crop with a constrained ratio to resize and scale the image to a required print resolution in one operation.

Input : Watermarked Image
Output: Cropped Watermarked Image
Step 1: Selecting the watermarked image I_w (N x N)
Step 2: Change the pixel format of the image into double.
Step 3: Transforming the pixels to single row of matrix.
Step 4: Applying the Cropping Operation on certain selected portion of image *"Crop (I_w)"*
Step 5: Displaying the output attacked image.

iii. Image Filtering Attack

Input: Watermarked Image
Output:Attacked watermarked image
Step 1: Select the watermarked image I_w (N x N)
Step 2: Changing the pixel format
Step 3: Transform to the data type of the pixels to double and converting to single row of matrix
Step 4:Appying the Filter operation function on both transformed pixel format and pixel in double format
Step 5:Displaying the attacked output image on filtering operation.

3.5 Watermark Extraction Algorithm

Input:Colour embedded image (Watermarked Image) Im^n (N x N) Output:The retrieved watermark image Ri (2M x 2M)

Step1: Apply three level DWT on R,G and B planes of embedded image Im^n

Step 2: Select the blocks of I_m^1 , I_m^2 , I_m^3 , I_m^4 and transform each block to binary streams

Step 3: Select original image and applying DWT on original image & transform the blocks to binary streams

Step 4: Subtract the bit streams of watermarked and original image

Step 5: Apply IDWT on difference to obtain the coefficients

Step 6: Displaying the extracted watermark.

3.6 De-blurring with Cropping with Normal, Wiener filter and DCT compression Technique

The most important technique for removal of blur in images due to linear motion or unfocussed optics is the Wiener filter. From a signal processing, blurring due to linear motion in a photograph is the result of poor sampling [16]. Each pixel in a digital representation of the photograph should signify the intensity of a single stationary point in front of the camera [6]. Unfortunately, if the shutter speed is too sluggish and the camera is in motion, a given pixel will be a mix of intensities from points along the line of the camera's motion. I = imcrop creates an interactive crop image and the image displayed in the current figure is called the target image. The crop image tool is a moveable, resizable rectangle that we can position interactively using the mouse. When the crop image tool is active, the pointer changes to cross hairs when you budge it over the target image [17]. Using the mouse, we can specify the crop rectangle by clicking and dragging the mouse.

IV. RESULTS OF THE EXPERIMENT

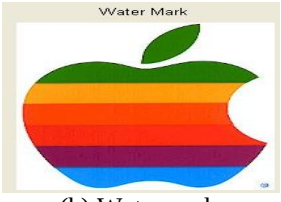
To measure the feasibility of the proposed scheme, we have conducted a series of experiments. The color host images include "Academy building" and "Logo". The watermark is a visually recognizable binary image with the size of 88 X 88 pixels. The watermark size is 88 X 88, which is calculated according to the selected embedded locations and the PSNR value. The blocks size of the I^3, I^4 ,I^7 and I^8 (refer to figure 6 - 15.) from the R and B bands for embedding are 32768. Because the secret sharing scheme will cause the size of the watermark four times larger. The watermark is decided to 88 x 88.

The image processing operations that have been applied are cropping, blurring, sharpening, scaling, JPEG compression, brightness adjustment and contrast adjustment[5]. The experimental results are listed one by one in the following sections. In the analysis of various images PSNR is calculated $PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)$

4.1 Embedding Watermark

The output of embedded watermark is shown in the following image which shows seperately original, watermark and embedded image.

(a) Image



(b) Watermark

(c) Embedded Watermarked Image

Fig. 6: (a,b,c)

The Embedding Algorithm Simulation is carried out in the MATLAB environment and the output images are shown in the figures.

4.2 Attacks

The selection reveals robustness and reliability of embedding algorithm used in this project. The various attacks on watermarked image are attempted and PSNR value calculated corresponding to the all mechanisms of attacks.

i. **Attack of watermarked image with filtering**

This attack involves both normal and Weiner filtering techniques. The simulation of this technique gives the output image as follows.

Fig. 7: Filtered Image

The PSNR value above attacked image is found to be equal to 0.041538.

ii. **Attack of watermarked image resizing**

The image resizing algorithm as discussed in the preceding section and produces the output image as follows.

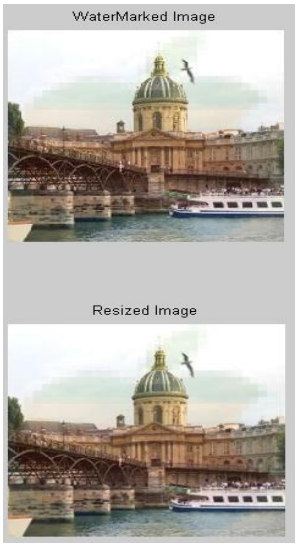


Fig. 8: Resized Image

The PNSR value for above image is equal to 0.09238.

iii. **The attack of watermarked image cropping**

The cropping image algorithm is implemented that simulates the following images as output.

Fig. 9: cropped Image

The PSNR value is 0.0374

4.3 Watermark Extraction and De-Blurring

The watermark has been extracted as discussed in earlier section. The extracted watermark is noisy and blurred. The PSNR value of this image is calculated and is found to be equal to 25.5203. The simulation of watermark detection algorithm produces the following output.

Fig. 10: Extracted watermark

The noisy extracted watermark is developed with various de-blurring techniques. And therefore PSNR can be enhanced that leads to clarity of the image. In this paper various de-blurring algorithms are attempted for filtering the redundant information. The foregoing analysis shows the simulation of filtering techniques to de-blur the noisy extracted watermark. The detailed description and functionality of the de-blurring algorithms implemented in the paper are already given in the preceding chapter. The de-blurring techniques play a vital role in watermarking task.

i. Normal and Wiener Filer

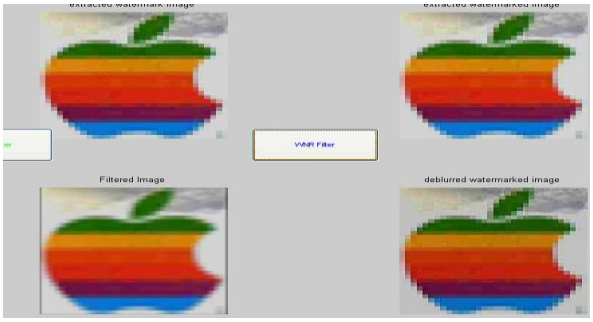


Fig. 11: Normal and Wiener Filtered Watermark

PSNR for normal filter 29.59 and Wiener filter 31.92

ii. De-Blurring with DCT Compression

Fig. 12: DCT Compressed image

PSNR value is 38.7791

iii. De-blurring with Cropping technique

Cropping removes some parts of an image. The experiment crops the three host images with different areas. According to the experiment, when the remaining cropped areas is 448 x 448, the accuracy rate of the watermark with the correction is nearly 90%, which can be identified by human eyes.

Fig. 13: Image cropped

iv. Cropping with Noise treatment

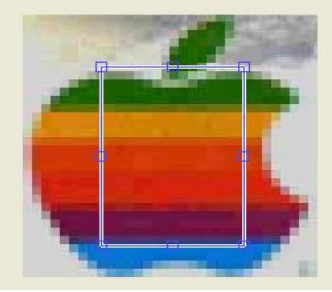


Fig. 14: Image cropped with noise treatment

In this paper, a copyright protection scheme for color images using discrete wavelet transform (DWT) is demonstrated. The implementation verifies robustness and reliability against various attacks on the embedded watermarked image. This scheme is suitable for color images. And it is also noted that PSNR in the de-blurred images enhances successively with implementation of normal, Wiener filtering, DCT and JPEG Compression techniques.

Furthermore, the advantages of the previously proposed scheme are still preserved in the improved proposed algorithm.

(1) It does not modify the host image, and therefore is suitable for unchangeable images,

(2) It is secure because of the employment of watermark.

(3) It is robust according to the experimental results with the calculated parameter of PSNR.

V. CONCLUSION

The investigation has shown that proposed technique is of an immense potentiality in secure transmission of data in the networks. The processes of embedding, extracting and de-blurring have been successfully simulated to reveal mechanism of avoiding the theft of secret watermark for sustained authenticity of the owner. The noisy retrieved image is de-blurred by employing various algorithms given in the paper and corresponding SNR is also estimated. An interesting point noted in the attempt is that performance of all proposed algorithms is well appreciated. Reliability and robustness of embedding algorithm have been examined carefully in the way to the analyze in case of image information embedded is being retrieved by any third party as a opponent.

References

[1] Abdelwahab, A.A. & Hassan, L.A., 2008. A discrete Wavelet transform based technique for image data hiding. In *Proceedings of 25th National Radio Science Conference, NRSC 2008*. Egypt, 2008. March 18-20.pp.1-9.

[2] Areepongsa, S., Kaewkamnerd, N., Syed, Y.F. & Rao, K.R., 2000. Exploring on steganography for low bit rate wavelet based coder in image retrieval system. In *Proceedings of IEEE TENCON*. Kuala Lumpur, Malaysia, 2000.

[3] Ashtiyani, M., Birgani, P.M. & Hosseini, H.M., 2008. Chaos-based medical image encryption using symmetric cryptography. In *Proceedings of IEEE 3rd International Conference on Information and Communication Technologies: From Theory to Applications (ICTTA 2008).*, 2008. 7-11 April. pp.1-5.

[4] Cancelli, G., Doërr, G.J., Barni, M. & Cox, I.J., 2008. A comparative study of +/-1 steganalyzers. In *Proceedings of IEEE 10th Workshop on Multimedia Signal Processing*. Queensland, Australia, 2008. 8-10 Oct. pp.791-796.

[5] Chang, C.C., Chen, T.S. & Chung, L.Z., 2002. A steganographic method based upon JPEG and quantization table modification. *Information Sciences*, 141(1-2), pp.123-38.

[6] Deguillaume, F., Voloshynovskiy, S. & Pun, T., 2003. Secure hybrid robust watermarking resistant against tampering and copy attack. *Signal Processing*, 83(10), pp.2133-70.

[7] Delahaye, J.P., 1996. Information noyée, information cache. *Pour la Science*, 229, pp.142-46. www.apprendre-en-ligne.net/crypto/stegano/229_142_146.pdf.

[8] Denis, T.S., 2006. Cryptography for Developers. In *Syngress*., 2006.

[9] Jarvis, J.F., Judice, C.N. & Ninke, W.H., 1976. A Survey of Techniques for the Display of Continuous-tone Pictures on Bilevel Displays. *Computer Graphics and Image Processing*, 5(1), pp.13-40.

[10] Nirinjan, U.C. & Anand, D., 1998. Watermarking medical images with patient information. In *Proceedings of the 20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. Hong Kong, China, 1998. 29 Oct-1 Nov. pp.703-706.

[11] Saenz, M., Oktem, R., Egiazarian, K. & Delp, E., 2000. Color image wavelet compression using vector morphology. In *Proceedings of the European Signal Processing Conference*. Tampere, Finland, 2000. 5-8 September. pp.5-8.

[12] Van Der Weken, D., Nachtegael, M. & Kerre, E., 2004. Using similarity measures and homogeneity for the comparison of images. *Image and Vision Computing*, 22(9), pp.695-702.

[14] Wang, K.W., 2009. Image encryption using chaotic maps. In Kocarev, L., Galias, Z. & Lian, S. *Intelligent computing based on chaos*. Springer. p.345.

[15] Wang, Y. et al., 2007. image encryption method based on chaotic map. In *Proceedings of IEEE 2nd Conference on Industrial Electronics and Applications (ICIEA)*. harbin, China, 2007. 23-25 May. pp.2558-2560.

[16] Yu, Y.H., Chang, C.C. & Lin, I.C., 2007. A new steganographic method for color and grayscale image hiding. *Computer Vision and Image Understanding*, 107(3), pp.183-94.

[17] Zeghid, M. et al., 2006. A modified AES based algorithm for image encryption. *International Journal of Computer Science and Engineering*, 1(1), pp.70-75

BIOGRAPHIES

G. Srinivas Reddy, received M.Sc. in Applied Electronics from Osmania University, Hyderabad, India, holds an M.Tech in Computer Science and Engineering from Jawaharlal Nehru Technological University, Hyderabad, A.P., India. He has 9 years of experience in teaching at various Engineering Colleges. He is presently Assistant Professor at Mahatma Gandhi Institute of Technology [MGIT], Hyderabad, A.P, INDIA. His areas of research include Evolutionary algorithms, Artificial Neural Networks, Computational physics, Digital Image Processing, Network Security and other Emerging areas of computing sciences. He is pursuing Ph.D. He can be reached at

T.Venkat Narayana Rao, received B.E in Computer Technology and Engineering from Nagpur University, Nagpur, India, M.B.A (Systems), holds a M.Tech in Computer Science from Jawaharlal Nehru Technological University, Hyderabad, A.P., India and a Research Scholar in JNTU, Kakinada. He has 21 years of vast experience in Computer Science and Engineering areas pertaining to academics and industry related I.T issues. He is presently working at , Department of Computer Science and Engineering, Hyderabad Institute of Technology and Management [HITAM], Gowdavally, R.R.Dist., A.P, INDIA. He is currently working on research areas which include Digital Image Processing, Digital Watermarking, and other Emerging areas of Information Technology. He can be reached at

Dr.A.Govardhan, BE in computer Science and Engineering from Osmania University College of Engineering, Hyderabad, M.Tech from Jawaharlal Nehru University, Delhi and Ph.D from Jawaharlal Nehru Technological University, Hyderabad. Worked as Principal and Professor, C.S.E, College of Engineering, Jawaharlal Nehru Technological University-Hyderabad, Nachupally Karimnagar**,** A P, India. Presently working as Director of Evaluation JNTU, Hyderabad. A member of Standing Committee for Academic Senate, JNT University Hyderabad and Academic Advisory Committee (AAC), UGC-Academic Staff College, JNT University Hyderabad. He is the Chairman for Post Graduate Board of Studies (BOS) in Computer Applications, Yogi Vemana University, and Kadapa. A member, BOS for CSE and IT (UG and PG), JNT University Hyderabad and VR Siddhartha Engineering College, Vijayawada. He was the Chairman for Board of Studies (Computer Science and Engineering) during 2008-2009 for UG and PG at Dept. of CSE, JNTUH College of Engineering Hyderabad and Member BOS at School of Information Technology, JNTU Hyderabad. He was the Co-convener for EAMCET 2009. He has been a committee member for various International and National conferences including PAKDD2010, IKE10, ICETCSE-2010 ICACT-2008, NCAI06. He is a Coordinator for the ongoing Research Project on Telugu in IT. Government of A.P. He is also a member in various professional bodies including CSI, ISTE, IAENG, FSF and WASET. He has been listed as one among the Top Three Faculty in JNTU Hyderabad made by Outlook Survey for the year 2008. He has 135 research publications at International/National Journals and Conferences. He is Member, Editorial Board of many reputed International Journals of Emerging Technologies and Applications in Engineering Technologies. He has been a program committee member for various International and National conferences. He has delivered number of Keynote addresses and invited lectures. His areas of interest include Databases, Data Warehousing & Mining, Information Retrieval, Computer Networks, Image Processing and Object Oriented Technologies.