ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 5, November 2012

Invisible Digital Image Watermarking in Spatial Domain with Random Localization

Mustafa Osman Ali(1), Elamir Abu Abaida Ali Osman(2), Rameshwar Row(3)
(1)(3)Electronics & Communication Engineering Dept., (2) Biomedical Engineering Dept.
University College of Engineering, Osmania University, Hyderabad, India.

Abstract*— Authenticating transaction of the digital media becomes an active research field now a day. That is emerging due to the illegal use of data resources and hacking by unauthorized users. In this article, we implemented new algorithms for embedding and extracting watermark. Our algorithm works on spatial domain of digital images where it can embed invisible watermark. A secret key is used to embed and extract watermark. The watermark, according to the secret key, locates in a random manor vertically or horizontally across the base-image. The algorithms are coded and tested by using Matlab.

***Index Terms*— Base-Image, Block, Imperceptibly, Mark-Image, Marked-Image, Robustness, Selected Group, Zero-Image.**

I. INTRODUCTION

Due to the rapid increase in computer and network technology, the need for securing digital information becomes an important target for technology producers; specially researchers. Mainly three approaches for securing digital information are widely used: Encryption, Steganography and Watermarking which is amazing over all!

Steganography and watermarking are slightly similar if we focus on the product after applying each. But watermarking has more than one feature that led it to be better than Steganography especially if we talk about imperceptibility or if the purpose of the use is to authenticate the product. Ingemar J. Cox and his colleagues in their book [1] defined both watermarking and Steganography as in the following:

"We define watermarking as the *practice of imperceptibly altering a Work to embed a message about that Work.*

We define Steganography as the practice of undetectable altering a Work to embed a secret message."

On the other hand, if get compared with watermarking, encryption is the transformation of data into a secret code with the purpose of protecting the secrecy of the data when sent through an insecure channel; whereas watermarking is the process whereby a host media is embedded with data for the purpose of protection and authentication [2].

II. WATERMARKING TECHNIQUE

In general digital watermarking involves two major operations: (i) watermark embedding, and (ii) watermark extraction. For both operations a secret key is needed to secure the watermark. The keys in watermarking algorithms can apply the cryptographic mechanisms to provide more secure services. The secret message embedded as watermark can almost be anything, for example, a bit string, serial number, plain text, image, etc. The most important properties of any digital watermarking technique are: robustness, security, imperceptibility, complexity, and verification. Watermarking techniques can be classified according to the nature of data (text, image, audio or video), or according to the working domain (spatial or frequency), or classified according to the human perception (robust or fragile). In images, the watermarking techniques can broadly be classified into three types: (i) visible watermark, (ii) invisible fragile watermark and (iii) invisible robust watermark, which has wider currency and use [3]-[7].

III. WATERMARKING DOMAINS

Watermark usually embeds into either spatial or frequency domain of the media. Spatial domain embedding is a linear operation which deals directly with the host media bytes one by one consequently. Frequency domain embedding is a nonlinear operation that deals confidently with the frequency components of the host media; therefore a transform method needs to be applied. This makes it more complicated than the spatial operation. But it has better imperceptibility as well as robustness than spatial one [1],[3],[7].

IV. ALGORITHMS

Through this article we are going to propose and test algorithms which are capable to embed and extract a watermark in spatial domain of a digital image. We plan these algorithms in our future work to model into hardware chip, to be capable to embed watermark immediately on the origin time of image captures.

As it is clearly known, watermarking in spatial domain is the most straightforward fundamental schemes for the fields of digital watermarking. This technique has started long time ago by designing the embedding and extracting algorithms to modify the luminance values of the pixels in the spatial domain. Also it allows to modeling as the simplest hardware scheme due to it is direct deal with the bytes of the media in linear technique [4], [8].

A. Embedding Algorithm

Three tasks are done by our embedding algorithm: generates extraction key, determines the position of the embedding watermark and then embeds watermark. First of all, the algorithm must determine where the watermark should be located; therefore, a base-image is divided into 64 blocks. Each block size is: ($M/8$ × $N/8$) *where*: M and N are the number of the rows and columns of the base-image respectively. So there will be eight groups of rows as well as for columns. The watermark will embed through one of these groups either rows or columns in each base-image but randomly for sequence base-images. In other words, the position of the watermark isn't the same in different sequence base-images. This provides more complexity to secure our watermark. Another thing which is important is that if watermark goes to embed through rows' group, the selection will discard the first and the last group of rows, to avoid losing the watermark if the base-image got cut in its edges later. Also the same will do for first and last group of column if watermark goes to embed through columns' group. In the selected group a LSB (*least significant bit*) over all pixels will extract (*LSB = 0*).

A watermark used in our algorithm is a binary image; its size should be equal to the block size e.g. [*M/8* × *N/8*]. The watermark pixels embed into the base-image pixels – LSB – bit by bit using a binary mask. The binary mask is a byte of Zeros with a unique One. The order of the One through Zeros' byte is the same to the order of the block in the group. This means that the 1st block of the selected group from the base-image will embed only by the 1st bit extracted from the pixels of the mark-image taken pixel by pixel. And the 2nd block will embed only by the 2nd bit, and so on till the last block which will embed by the last bit of the pixels from the mark-image. By the end of the embedding operation, the mark-image bits will be distributed all over the whole pixels of the selected group in the base-image. The described procedure given by looping the following equations in sequence:

$$I_B = \sum_{i=m}^{M}\sum_{j=n}^{N} [\![\left(I_{B_{ij}}]\!] \wedge 254 \right) \quad \dots \ (1)$$

$$Mask_{Emb} = \sum_{p=m'}^{M/8}\sum_{q=n'}^{N/8} \left(\frac{\left(I_{W_{pq}} \wedge 2^{(K-1)} \right)}{\left(2^{(K-1)} \right)} \right) \dots \ (2)$$

$$I_H = \sum_{i=m}^{M}\sum_{j=n}^{N} (I_B \vee Mask_{Emb}) \quad \dots \ (3)$$

Where: I_B, I_W and I_H are represent base-image, mark-image and marked-image respectively. *M* and *N* are the dimensions of the base-image. Parameters *m* and *n* are the values of the first pixel dimensions of the selected group; where *m'* and *n'* indicate the values of the first pixels of certain block in the selected group. *K* is the counter of the block sequence loop counting up to eight. Lastly $Mask_{Emb}$ is a byte value which is used to embed a bit from I_W into I_B to get I_H.

B. Extraction Key Generation

The embedding algorithm generates a secret key which is used later to extract watermark. The initial value of the secret key is collected from the counter of the base-images' capture system – e.g. Camera*. The length of the key depends on the system counter length. The key will encrypted using a simple encryption algorithm to secure it (details omitted for being brief). The generated key should contain three important details: (i) the selected group type (rows' group or columns' group), (ii) the sequence order of the selected group in the base-image, and of course (iii) the sequence number of the base-image. Fig. (1) Illustrates our embedding algorithm main tasks sequence.

C. Extraction Algorithm

To extract the watermark, the algorithm needs to decrypt extraction key to obtain the initial key, through which the algorithm can locate the watermark position in the targeted base-image. An illustrating example: the initial key itself is the sequence number of the base-image. If the initial key value parity equals zero, then, the watermark embedded through rows' group, otherwise it embedded through columns' group. The order of the select group is given by the following Matlab code:

```
group_order = mod (initial key , 8);
if (group_order == 1)
        group_order=4;end
% discards the first group and replaces it with the fourth group.
if (group_order == 0)
         group_order=5;end
% discards the last group and replaces it with the fifth group.
```

Now the required details and the marked-image are available, then the extraction algorithm will initialize a zero-image its size equal to the block size. Again algorithm needs to divide marked-image to 64 blocks, and then determining the watermark location. The extraction operation begins from the 1st block of the determined group by extracting the LSB from each pixel in the group, and then is multiplied by the ordering number of the block before adding it to the corresponding pixel in the zero-image (by this step all pixels' LSB will become valued not default Zero). This will be repeated eight times to revalue the zero-image's pixels with watermark real values obtained from the marked-image LSBs, and the result will be the watermark. This scenario is represented by the following equations:

$$Mask_{Ext} = \sum_{i=m}^{M}\sum_{j=n}^{N} \left(\left(I_{H_{ij}} \wedge 1 \right) \times 2^{(K-1)} \right) \dots \ (4)$$

$$I_{Ext} = \sum_{p=m'}^{M/8}\sum_{q=n'}^{N/8} \left(I_{Zero} + Mask_{Ext} \right) \quad \dots \ \mathbf{(5)}$$

Where: I_{Ext} is the watermark which extracted from marked-image, and I_{Zero} is the empty frame sized [32 32] to store extracted watermark in. The $Mask_{Ext}$ is a byte by which watermark is extracted.

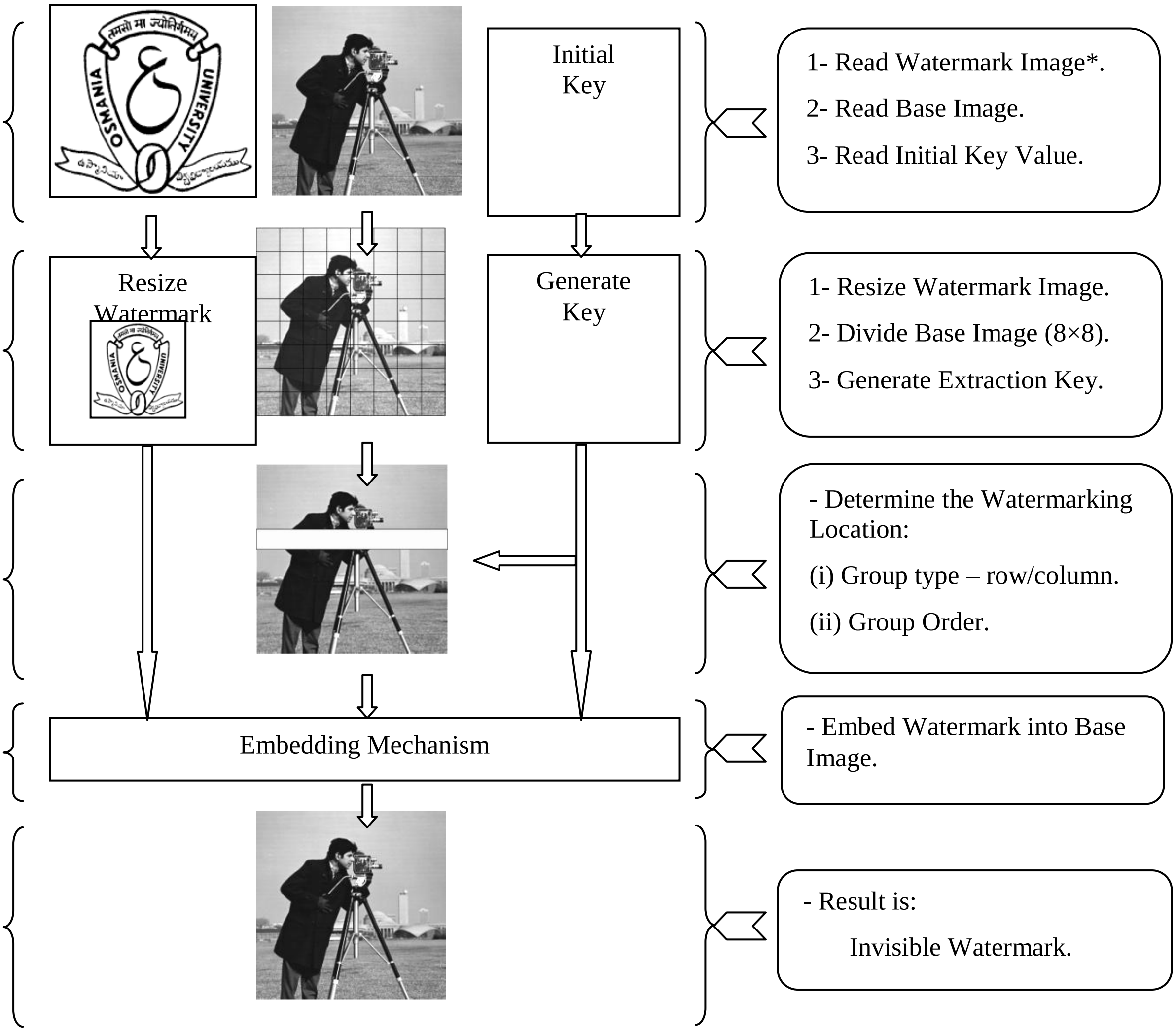
Initial Key
1- Read Watermark Image*.
2- Read Base Image.
3- Read Initial Key Value.
Resize Watermark
Generate Key
1- Resize Watermark Image.
2- Divide Base Image (8×8).
3- Generate Extraction Key.
- Determine the Watermarking Location:
(i) Group type – row/column.
(ii) Group Order.
Embedding Mechanism
- Embed Watermark into Base Image.
- Result is:
Invisible Watermark.

Fig. (1) The Embedding Algorithm Flowchart.

V. EXPERIMENTAL RESULTS

Both the embedding and extracting algorithms were coded and tested successfully by using Matlab 7.9.0 (R2009b). The test has done over different several images, some of them are available in the tool box of Matlab and the others are private ones; the results are acceptable and have well imperceptibly. Fig. (2) shows the result obtained when applying [32 32] watermark to the base-image [256 256] cameraman.tif, coins.png and football.jpg images respectively in different positions. The result clearly proves that the watermark embedded as invisible watermark with higher imperceptibly. And lastly, the watermark is extracted safely as a full meaning image as shown in fig. (3).

Many factors are available to measure marked-image quality such as peak-signal to noise ratio (PSNR) and bit correct ratio (BCR) [3], [4], [9]. PSNR used to evaluate the imperceptibility of the watermarked-image. PSNR can be found by equation (6) and the robustness of the watermarking measured by BCR using equation (8).

$$PSNR = 10 \times log_{10}\left(\frac{255^2}{MSE}\right)(dB) \quad \dots \quad (6)$$

$$MSE = \frac{1}{M \times N}\sum_{i=0}^{M}\sum_{j=0}^{N}(I_B(i,j) - I_H(i,j))^2 \dots (7)$$

$$BCR = \left(1 - \frac{\sum_{i=0}^{M}\sum_{j=0}^{N} I_B(i,j) \oplus I_H(i,j)}{M \times N}\right) \times 100\% \dots (8)$$

Where I_H and I_B stand for the marked-image and the base-image, respectively, M and N represent dimensions of I_H and I_B images, and MSE is the Mean Square Error. For imperceptible watermarking, the marked-image should look as similar as the base-image, thus the MSE between the two images in equation (7) should be as small as possible. From equation (6), the higher value of the PSNR leads to less imperceptibility of the marked-image [3],[4],[7].

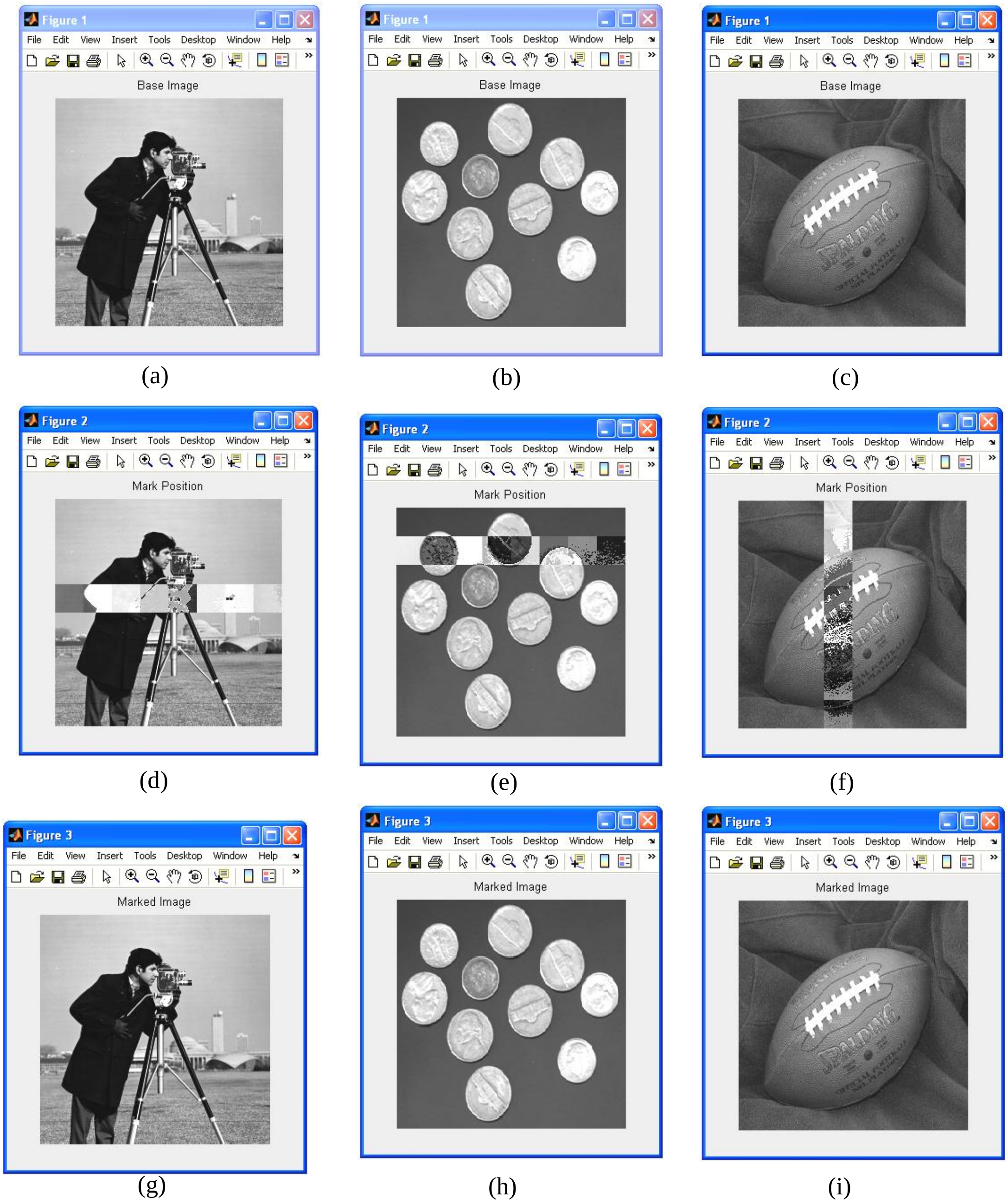

Fig. (2) The Algorithm Results, First Row Images (A, B And C) Show The Base-Images: Cameraman.Tif, Coins.Png and Football.Jpg Respectively. The Second Row Images (D, E And F) Show The Random Locations Of The Watermark. and The Third Row Images (G, H And I) Show The Corresponding Marked Images Generated

Excellent results are obtained from testing the images which gained by our algorithm when applying PSNR and BCR equations. The results show that both imperceptibility and robustness verifying high quality.

VI. Applications

We believe that our algorithms are useful with high level of reliability to secure transaction of digital images over WEB. Media correspondents and journalists, for example, can use it safely to send their images, and the editors can verify and authenticate their resources as well. Also they can be useful for authenticating short clips of video media.

VII. Conclusion

In this paper we implemented a simplest model of watermark technique. It has the ability to insert an invisible watermark into a spatial domain of a base-image. This technique yields marked-images with high imperceptibility and robustness quality. The algorithm provides high level of security by generating encryption key which is used to extract the watermark later; also, the algorithm is able to randomize the location of the watermark in different base-images. On the other hand, an extraction algorithm is prepared and tested successfully. Both algorithms are coded in Matlab 7.9.0

(R2009b). We are interested in the spatial domain watermarking due to its easiest modeling into hardware and for its economical features. Therefore we are planning to implement our proposed algorithm as a hardware chip as soon as possible in the nearest future.

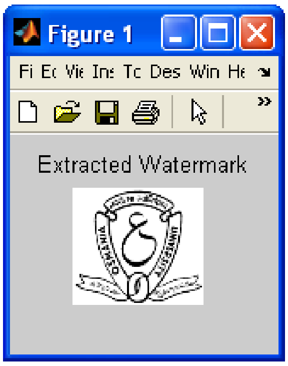

Fig. (3) Extracted Watermark {Osmania University Logo}

REFERENCES

[1] Ingemar J. Cox, MatthewL. Miller, Jeffrey A. Bloom, Jessica Fridrich, and Ton Kalker, "Digital Watermarking and Steganography," 2nd edition, Elsevier, 2008.

[2] O. B. Adamo, Saraju P. Mohanty, E. Kougianos, and M. Varanasi, "VLSI Architecture for Encryption and Watermarking Units Towards the Making of a Secure Camera," Proc. In IEEE International Conference SOC, pp. 141-144, 2006.

[3] S Jayaraman, S Esakkirajan, and T Veerakumar: Digital Image Processing. McGraw-Hill, 2009.

[4] Mustafa Osman Ali, and Rameshwar Rao. Fundamentals of Digital Image Watermarking: an Overview. International Conference on Information and Communication Technology.. pp. 64–67, Oct. 2011.

[5] Nidhi S Kulkarni, IndraGupta, and S. N. Kulkarni, "A Robust Image Encryption Technique based on Random Vector," Proc. of IEEE 1st International conference on Emerging Trends in Engineering and Technology, pp.15-19, 2008.

[6] D. Samanta, A. Basu, T. S. Das, V. H. Mankar, Ankush Ghosh, Manish Das and Subir K Sarkar, " SET Based Logic Realization of a Robust Spatial Domain Image Watermarking," Proc. in 5th International Conference on Electrical and Computer Engineering-ICECE 2008, Dhaka, Bangladesh, pp. 986-993, Dec. 2008.

[7] Jeng-Shyang Pan, H. C. Huang, and L. C. Jain: Intelligent Watermarking Techniques. World Scientific, 2004.

[8] Mustafa Osman Ali and Rameshwar Rao. "An Overview of Hardware Implementation for Digital Image Watermarking," Proc. of International Conference on Signal, Image Processing and Applications (SIA 2011), Chennai, India, pp. 19-24, Dec. 2011.

[9] Saraju P. Mohanty, "A Secure Digital Camera Architecture for Integrated Real-Time Digital Rights Management," Elsevier, 2009.

AUTHOR BIOGRAPHY

Mr. Mustafa Osman Ali has received his B.Sc. and M.Sc. degrees in Electronics - Computer Engineering at Sudan University for Science and Technology (SUST), Khartoum, Sudan in 2006. Currently, he is working towards the Ph.D. degree in Digital Systems at Osmania University, Hyderabad, India. His research interests include Image Processing, Computer Interfacing, and Digital Communications. He is a Lecturer in Nile Valley University, Eng. College, Atbara, Sudan since March 2003 – he was a head of Electrical & Electronic Eng. Dept. for three years (2007 – 2010).He is also assistant professor in SUST University, Elshikh Abdallah Elbadri Technical College, and open education in his country. Also he is a member in Sudanese Engineering Sociaty, And Sudanese Engineering Concil, Khartoum, Sudan. Mr. Mustafa has published five intrnational papers.

Elamir Abu Abaida Ali Osman has received his B.Sc. and M.Sc. degrees in Bio-medical Electronics at Kharkov State Technical University of Radio Electronic - UKRAINE in 2000. Currently, he is working towards the Ph.D. degree in Biomedical Engineering at Osmania University, Hyderabad, India. His research interests include Fields in Magnetic Stereotactic System, Stereotactic Surgery. He is a Lecturer in Salman Ben Abdul Aziz University from 2010 to date, and he was a Lecturer in King Saud University (Aflaj community college) from 2004 to 2010.

Prof. Rameshwar Rao, has obtained his Bachelor of Engineering in Electronics and Communication Engineering from University College of Engineering, Osmania University, Hyderabad. He obtained both his M.Tech in Communication Engineering and Ph.d from IIT, Bombay. His interests' areas are: Digital communication, Digital Design using VHDL, Computer Networks, VLSI Design, and Mobile Cellular Communication. Prof. Rameshwar Rao, has charged many academic chairs in ECE dept. and Engineering College. Right now he is the vice chancellor of JNTU, Hyderabad. He has guided more than 25 PhD students, and he has more than 70 published papers.