LSB Based Lossless Digital Image Watermarking using Polynomials in Spatial Domain for DRM

A. Siva Sankar
Dept. of Electronics &
Communication Engg.
Gokula Krishna College of Engg.
Sullurpet, A.P,. India

T. Jayachandra Prasad
Dept. of Electronics &
Communication Engg.
RGMCET, Nandyal, A.P.,India

M.N. Giri Prasad
Dept. of Electronics &
Communication Engg.
JNTU College of Engg.
Pulivendula, A.P., India

ABSTRACT

For many years information hiding has captured the imagination of researchers. Digital watermarking and steganography tools are used to address digital rights management, protect information, and conceal secrets. Digital watermark technology insert the information of copyright to the carrier, thus it aims to protect the carrier. The digital watermark is connecting two groups of data: Hidden data and carrier data. In the most situations, the carrier data will be distortion in the hiding process, and it unable to restore the initial state. That is, after even if the hidden body data already has been extracted, but the carrier data has also encountered the permanent distortion. But in certain applications, does not permit to the data pixel's minimum change. For example military remote sensing image, medicine image, high energy physics image, legal evidence and so on sensitive image. In these applications, any pixel's information thought that is very important. It can affect the image to data any revision the confidence level. These applications request to use the most primitive image data. The authors implemented image watermark based on Least Significant Bit Insertion method using Polynomial. The advantages and disadvantages of this method have also been discussed.

General Terms

Security, Algorithms.

Keywords

DRM, Watermarking, LSB, Polynomial.

1. INTRODUCTION:

Digital Rights Management poses one of the greatest challenges for content communities in the digital age. DRM is a method of controlling access to copyrighted material [1]. A less common DRM method is called Digital Watermark. Digital watermark technology insert the information of copyright to the carrier, thus it aims to protect the carrier[2]. The digital watermark is connecting two groups of data: Hidden data and carrier data. In the most situations, the carrier data will be distortion in the hiding process, and it unable to restore the initial state. That is, after even if the hidden body data already has been extracted, but the carrier data has. also encountered the permanent distortion. But in certain applications, does not permit to the data pixel's minimum change. For example military remote sensing image, medicine image, high energy physics image, legal evidence and so on sensitive image. In these applications, any pixel's information thought that is very important. It can affect the image to data any revision the confidence level. These applications request to use the most primitive image data.

In random LSB insertion methods, a pseudo-random number generator is used to randomly distribute and hide the bits of a secret message into the least significant bits (LSBs) of the pixels within a carrier image, called the cover image. A popular approach to achieve this is the random interval method. Both communication parties share a seed key, K usable as a seed for a random number generator[3]. Random LSB insertions are intended to make it harder for an attacker to detect the embedded secret message with attacks such as the visual attacks and statistical attacks.

Here the authors introduced a new image watermark encoding scheme which separates the colour channels of the windows bitmap images and then randomly hide messages in the LSB of any/all the components of the chosen pixel using polynomial[4]. If polynomial is used, hacker need to predict more than one number i.e all coefficients of polynomial correctly to decode and probability of finding all right coefficients correctly is less compared to predicting single seed as in case random generator.

Using the proposed LSB Embedding and Extract Algorithms with polynomial concepts, one can extract the watermark message exactly as original message without distortion the host image.

2. INFORMATION HIDING IN BITMAP IMAGES

Redundancy is one of the major aspects of creation. A close inspection reveals that redundancy does exist, and exists in abundance. Computer files are not an exception to this fact. For e.g. an image on a computer is represented by tons and tons of pixels, which in turn have many redundant information's. The simplest technique here is to fabricate the redundant bits so as to do the covert communication. For e.g. each pixel of an image consists of a variation of all three primary colors, red, green and blue, in a standard 24-bit bitmap, requiring 8 bits each for these three colors. i.e. there are 256 different variations, ranging from 00000000 to 11111111, for each colour in a pixel. So, to represent the colour white, the code would look like 11111111 11111111 11111111. Keeping in mind that, the human eye cannot distinguish the difference between too many colours, the colour 11111110 11111110 11111110 would look exactly the same as white, which means that the last digit in every bit in every pixel could be changed without much visual degradation of quality. This is the basis of the Least Significant Bit Insertion technique. We require 8 bits to represent an ASCII text and there are three potential slots extra in every pixel of a picture. Therefore, in a conducive environment, with every three pixels, one ASCII text could be concealed. In order to make this practical to the user, a computer program would be needed. After typing in the secret message and determining a suitable host image, the program would go through every pixel to find the potential candidate pixels and will change the least significant bit to represent each bit of the message. The image could then be sent to the recipient who in turn runs his program to take off the least significant bits to form the secret message.

The current study took windows bit map image file format with loss less compression in to consideration. The proposed algorithm would require secret message (M), a host image (H) and a pseudorandom seed Generated by polynomial (S) as input. In Windows bit map format, every image will have three separate colour channels; a channel dedicated for the red component (rCom), another one for the green component (gCom), and a third one for the blue component (bCom). After separating the colour channels, the program would go through each pixel to find all those pixels where the watermark bits embedded. Spatial details of every such pixel will be stored in an array named Candidate Pixel (CP) and the total numbers of such potential candidate pixels are calculated. If the length of the message (in bits) is more than the length of CP then a message will be displayed prompting the unsuitability of the input image under consideration. If the input image is found to be suitable then a pseudorandom number will be generated from a pre-decided polynomial, by making use of the seed, which was agreed beforehand by both the parties. The pseudorandom number will be mapped to the Target Pixel index (TP) of CP by using the polynomial, with the length of the CP. This will enable us to insert the secret data bit randomly across the wrapper thereby increasing the stealth of the system. Once embedded, all the colour channels will be concatenated to form the Watermarked Image. The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secrete messages. When using a 24-bit image, a bit of each of the red, green and blue color components can be used, since they each represented by a byte. In other words, one can store 3 bits in each pixel.

If compress the secret message(watermark data) before embedding, using any available text compression algorithm, like Run length encoding scheme, may further reduce the message length, thus reducing the entropy and in turn enhancing the robustness of the system. Also the great thing about this insertion technique is that because the secret message is encoded into the color channels, the message is not lost even if the file is compressed.

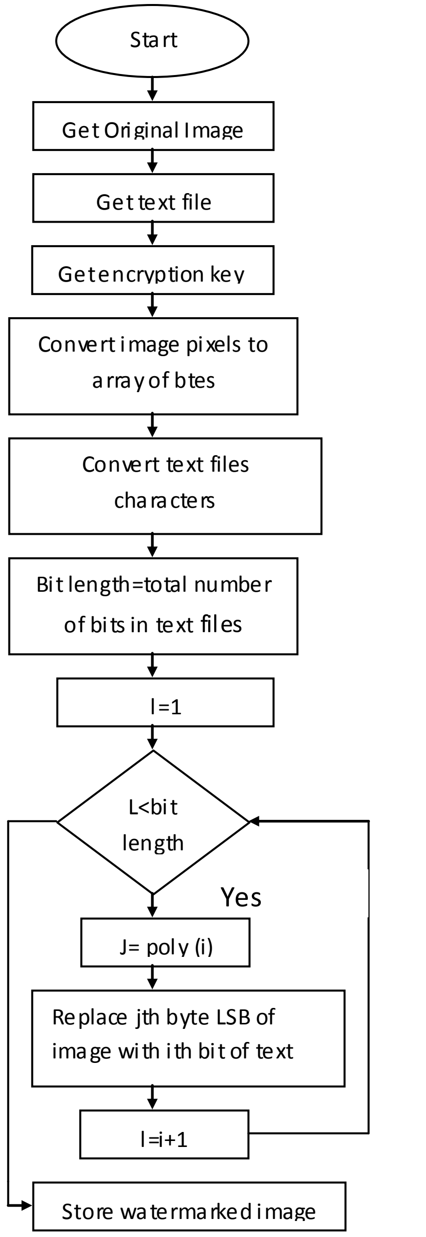
The flow chart of LSB encoding method is shown in next page. First take the original image as shown in the figure.1 and the text file i.e. which have to embedded into original image. Then convert the text data into binary format. Binary conversion is done by taking the ASCII value of the character and converting those ASCII values into binary format and steam of bits are generated. Counter variable is taken which holds the total number of bits of message. Similarly, in cover image, bytes representing the pixels are taken in single array and byte steam is generated. Message bits are taken sequentially and then are placed in LSB bit of image byte. The index number of the image byte where replacement of LSB is to be done is controlled by polynomial equation, which is given in the key. Same procedure is followed till all the message bits are placed in image bytes. The number sequence generated by the polynomial is unique therefore identifying the image bytes where LSB encoding is done is very difficult without polynomial key. Image generated is called watermarked image as shown in the figure 2, is ready for transmission through the internet.

The flow chart of LSB Decoding method is shown in the next page. First Watermarked image is taken and single array of bytes is generated as we did at the time of encoding. Total numbers of bits of message and polynomial are taken from the key supplied. Counter is initially set to 1 and is substituted in the polynomial which in turn gives the index number of the pixel byte where message bit is available in LSB. The procedure is repeated till final count of message bits is reached. After this step we have a bit steam of the message. Available bits are framed to form bytes such that each byte represents single ASCII character. Characters are stored in text file which represents the hidden message

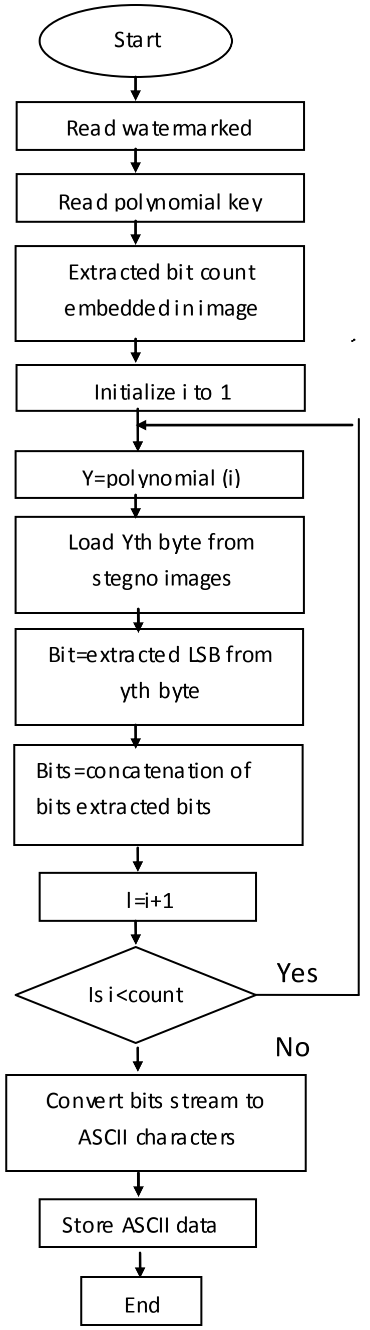
3. RESULTS AND DISCUSSIONS:

Figure 1 and 2 are images with a resolution of 456 X 343 with 24-bit color depth. The sizes of the two windows bitmap images shown are 458 KB (469 224bytes). Fig. 1 is unmodified where as Fig. 2 the modified one and a secrete message is also shown.

It is impossible for the human eye to find a visual difference between two of the below shown images. Since the visual difference test was unable to find any positive results, some statistical tests were exercised with the intention to prove that the image was tampered. If the image happen to be modified then at least some of image's statistical properties may deviate from a norm. Here also no significant difference in the quality of the Original image and Watermarked image were found. We therefore conclude from the basic statistical test that there is no evidence from the current experiment to suggest that the proposed system deteriorate the quality of the image. The different tests conducted and their results are tabulated in table 1


Start
Get Original Image
Get text file
Get encryption key
Convert image pixels to array of btes
Convert text files characters
Bit length=total number of bits in text files
I=1
L<bit length
Yes
J= poly (i)
Replace jth byte LSB of image with ith bit of text
I=i+1
Store watermarked image

Watermark Embedding Algorithm


Start
Read watermarked
Read polynomial key
Extracted bit count embedded in image
Initialize i to 1
Y=polynomial (i)
Load Yth byte from stegno images
Bit=extracted LSB from yth byte
Bits=concatenation of bits extracted bits
I=i+1
Is i<count
Yes
No
Convert bits stream to ASCII characters
Store ASCII data
End

Watermark Extraction Algorithm

Since the statistical tests were not able to decide whether the image contains a hidden message or not, histogram analysis was performed. Westfeld and Pfitzmann observed that embedding encrypted data into a GIF image changed the histogram of the respective color frequencies [5]. When using the least-significant bit method to embed watermark data into an image that contains the color one more often than the color two, the color one is changed more often to the color two than the other way around. As a result, the difference in color frequency between one and two has been reduced by the embedding. Figure 3 shows two histograms: the above row is that of the unmodified images' and the below one that of the modified ones'. Both the histograms look exactly the same and show little noticeable differences, thus proving no loss in watermark data as well as host image.

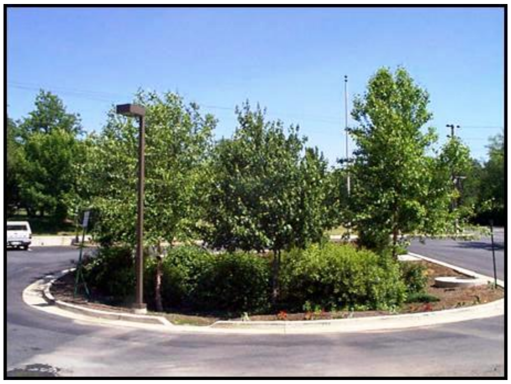


Fig 1: Original Image

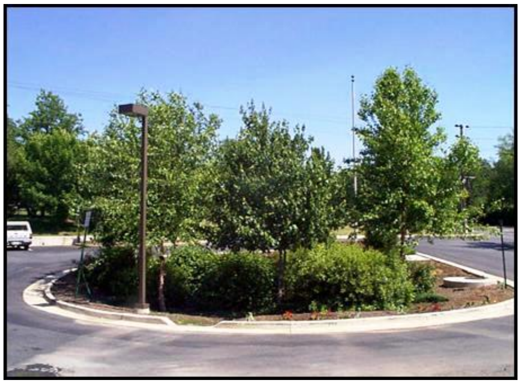
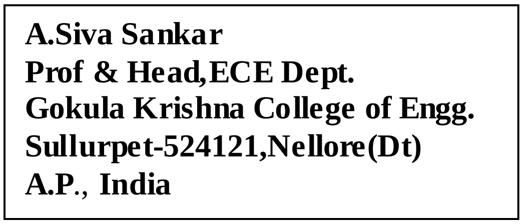


Fig 2: Watermarked Image



A.Siva Sankar
Prof & Head,ECE Dept.
Gokula Krishna College of Engg.
Sullurpet-524121,Nellore(Dt)
A.P., India

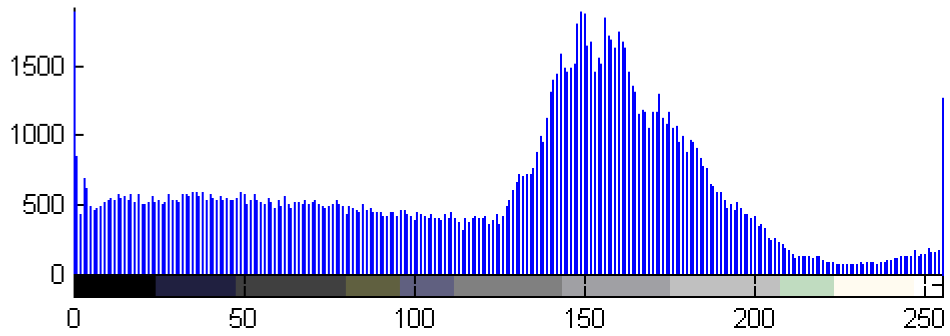
Watermark Data

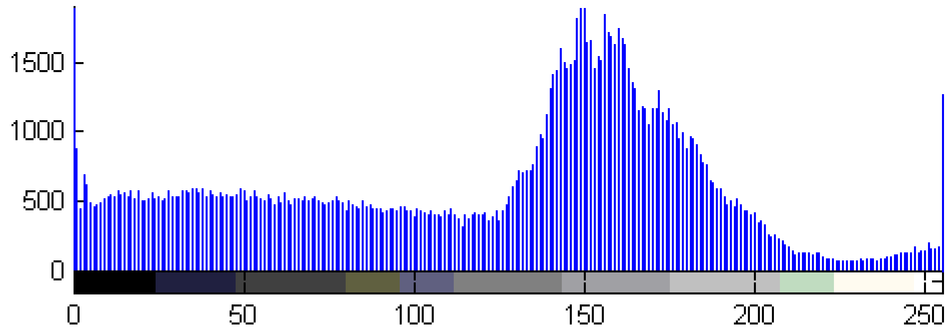
TABLE 1: STATISTICAL RESULTS

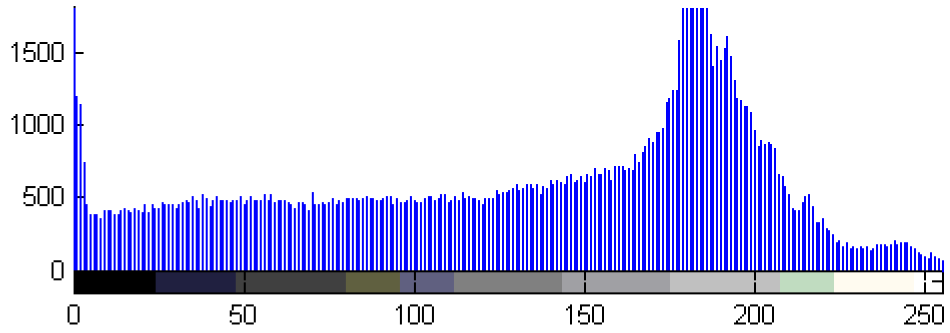
Test Name	Original Image (Fig.1)	watermarked Image (Fig. 2)
Mean	128.316803	128.316833
Standard deviation	75.100266	75.100166
Median	143.00	143.00
Size	469224.00	469224.00

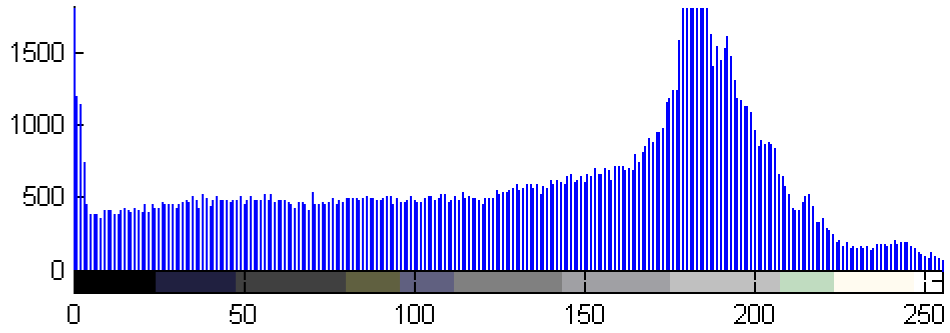
TABLE2: Quality Metrics Analysis

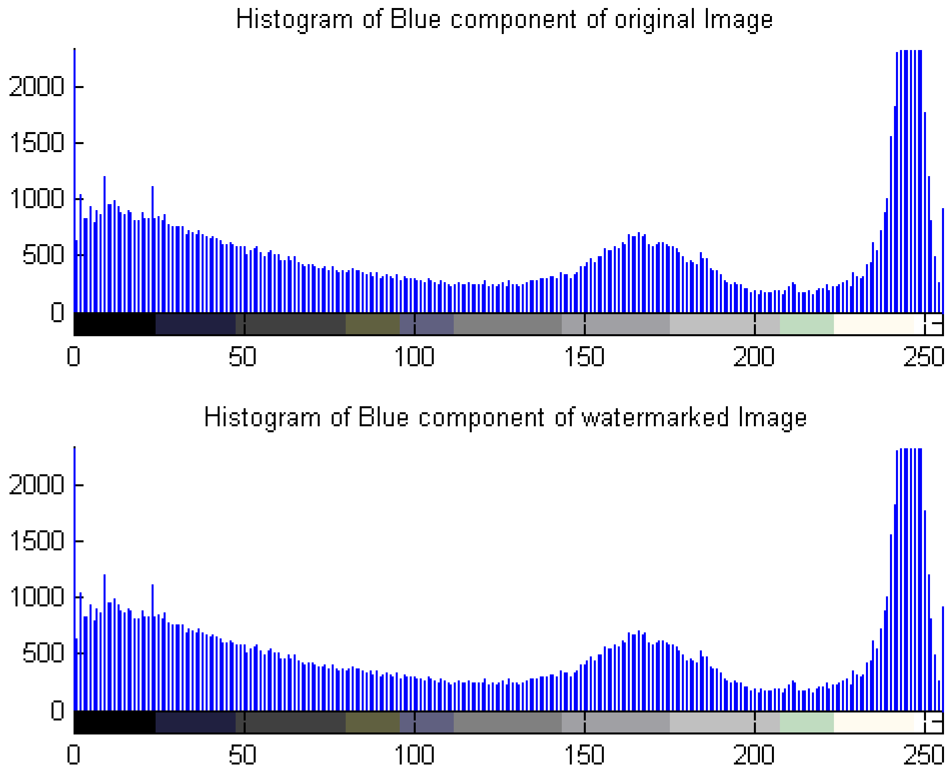
Test Name	Original Image Vs Original Image	Original Image Vs Watermarked Image
PSNR	infinite	Infinite(appr.)
Absolute average difference	0.000000	0.000002
Normalized Absolute Error	0.000000	0.000000
Normalized Cross corr.	1.000000	1.000000
Mean Square Error	0.000000	0.000049
Structural Content	1.000000	1.000000


Histogram of Red component of original Image


Histogram of Red component of watermarked Image


Histogram of Green component of original Image


Histogram of Green component of watermarked Image



X-axis: r_k- Kth Gray Level.
Y-axis: P (r_k) – Probability of occurrence of K^{th} Gray Level

Fig 3

Quality Metrics:

Quality of the Watermarked Image is analyzed, by executing various quality metrics. In order to estimate the quality, the watermarked image is compared with the original image. In addition, original image is compared with itself to estimate the deviation of watermarked image from original image. The value obtained for different quality metrics are shown in Table.2.

4. CONCLUSION

In this paper, the authors have introduced a new embedding scheme, randomly hide messages in the LSB of any/all component of the chosen pixel using polynomial. If polynomial is used, hacker need to predict more than one number i.e all coefficients of polynomial correctly to decode and probability of finding all right coefficients correctly is less compared to predicting single seed as in case random generator.

Using the proposed LSB Embedding and Extract Algorithms with polynomial concept, one can extract the watermark message exactly as original message without distortion the host image. Hence it is a lossless image watermarking scheme.

5. REFERENCES:

[1]. Chengjun Xu et al, “Digital Rights Management Solutions based on IPTV DRM”, International Conference on Networking and Digital Society, pp.43-46, IEEE 2010.

[2]. Ge Xiuhui et al, “Research on Applications of Reversible Digital Watermarking Algorithm”, CSSE’08, pp.810-813, IEEE 2008.

[3]. Jiju A.Matthew et al, “Steganography and Covert Communication in Open System Environment”, ART Communication’09, pp.847-849, IEEE 2009.

[4]. A. Siva Sankar, Dr.T.Jayachandra Prasad, Dr.M.N.Giri Prasad, “Image Steganography Using Polynomial Equation”, International Journal of Scientific Computing, Vol.4, No.1, pp.25-31, Jan-June 2010.

[5]. A. Westfeld and A. Pfitzmann, "Attacks on Steganographic System", Proc. Information Hiding-3 Int'l Workshop in Information Hiding, Springer- Verlag, 1999, pp. 61-76.

[6]. Kefeng Fan, Qingqi Pei et al, “A Novel Authentication Mechanism for Improving the Creditability of DRM System”, IEEE 2009.

[7]. K.Sukumar et al, “Multi Image-Watermarking scheme based on Framelet and SVD”, International Conference on Advances in Recent Technologies in Communication and Computing, IEEE Computer Society, IEEE 2009.

[8]. Rakhi C.Motwani et al, “A Proposed Digital Rights Management System for 3D Graphics using Biometric Watermarks”,IEEE CCNC 2010 Proceedings, IEEE 2010.

[9]. Yequing Liao et al, “Applying Dual Digital Watermarking Technology In Digital Rights Management”, pp.616-619, IEEE 2010.

[10]. Mehmet Utku Celik et al, “ Lossless Watermarking for image Authentication: A New Framework and an Implementation”, IEEE Transactions on image processing, Vol. 15, No. 4, IEEE 2006.

[11]. Tianyu Ye et al, “A Robust Zero-watermark Algorithm based on Singular Value Decomposition for Digital Right Management”, IEEE 2009.

ABOUT AUTHORS:

Prof. A. Siva Sankar obtained his Diploma in Electronics and communication Engineering at Governament Polytechnic, Tirupati and obtained his AMIE in Electronics and Communication Engg., from The Institution of Engineers (India), Kolkata 700 020 , and Master of Technology degree in Digital Electronics and Advanced Communication from Manipal Institute of Technology(MIT), Manipal – 576104, Karnataka state, India. He is pursuing his Ph.D. Degree (Digital Rights Management) in ECE from JNTUCE, ATP, India.

He worked in Hindustan College of Engineering, Chennai from Jun, 1997 to April, 2002 as a lecturer. Also he worked as a Lecturer in ECE Dept. in Anand Institute of Higher Technology, Chennai, from Sep, 2003 to June, 2004. Now he is working in Gokula Krishna College of Engineering, sullurpet from July, 2004 to till date in various positions such as Assistant Professor and HOD, Associate Professor and HOD and Professor and HOD. Present working as a Professor and HOD in ECE Dept. in Gokula Krishna College of Engineering, Sullurpet, A.P., India to till date. He is having more than 14 years of teaching experience and has more than 6 technical publications in International journals. He is a life member of ISTE (India), Associate of Institution of Engineers (India).

Dr.T.Jayachandra Prasad obtained his B.Tech in Electronics and Communication Engg.,from JNTU College of Engineering, Anantapur 515002, and Master of Engineering degree in Applied Electronics from Coimbatore Institute of Technology, Coimbatore. He earned his Ph.D. Degree (Complex Signal Processing) in ECE from JNTUCE, ATP. He worked in K.S.R.M, Kadapa from august 1984 to May 2006 in various positions such as assistant professor, associate professor and Professor and HOD .He worked as Head of ECE Dept. for 09 years at K.S.R.M.C.E., Kadapa. He was instrument for the establishment of various laboratories at K.S.R.M.C.E. Later he joined in RGMCET, Nandyal. Presently he is the Principal of RGMCET; Nandyal-518502.He is having more than 22 years of experience and has more than 32 technical publications in National /International journals and conferences. He is a life member of ISTE (India), Fellow of Institution of Engineers (Kolkata), Fellow of IETE, Life member of NAFEN, MIEEE. He is acting as member on the board of studies ECE dept, Yogivemana University, Kadapa, India.

Dr. M. N. Giriprasad is working as Principal at Jawaharlal Nehru Technological University college of Engineering, Pulivendula, Kadapa, India. Previously, he worked as a professor & HOD in the Department of ECE in the same college. His research work done in the Bio medical signal processing. . He has 20 years of teaching experience. He has more than 30 publications in standard international/National technical journals. He is guiding more than 12 Ph.D research scholars.