Hybrid Domain in LSB Steganography

K B Shiva Kumar
Department of TC,
Sri Siddhartha Institute of Technology
Tumkur, Karnataka, India

K B Raja
Department of ECE,
University Visvesvaraya College of Engineering
Bangalore University,
Bangalore, India

Sabyasachi Pattnaik
Department of Computer Science
FM University, Balasore,
Orissa, India

ABSTRACT
The maintenance of privacy and secrecy of information in modern communication is accomplished through steganographic technique. Spatial domain techniques are popular ones in image steganography. In this paper, we propose hybrid steganography (HDLS) which is an integration of both spatial and transform domains. The cover image as well as the payload is divided into two cells each. The RGB components of cover image cell I are separated and then transformed individually from spatial to transform domain using DCT/DWT/FFT and embedded in a special manner, the components of cell II retained in spatial domain itself. The proposed algorithm has better PSNR and security as compared to existing techniques.

Keywords
Steganography, Cover Image, Payload, Stego Image, DCT, FFT, DWT, LSB.

1. INTRODUCTION
Communication of secret information between two entities can be achieved through steganography. The term being derived from Greek words *Steganos* and *graphia* meaning covered writing. Steganography is an information hiding technique where the secret information to be communicated is embedded into a cover media such as image, video, audio and text files such that the hacker looking at the stego image cannot even think of the existence of the secret information and only it can be retrieved at the destination by an authorized person. As the images have redundant insignificant data that can be replaced by the secret data, maintaining the perceptual quality of stego object, the images are used as carriers of secret information in modern steganography.

Modern communication by virtue of its explosive growth through internet with high bandwidth explores the development of steganography for secure communication to protect secrecy of information both steganography and cryptography are used which are closely related and complimentary to each other. In cryptography technique, the secret message is scrambled so that any hacker even if predicts it but unable to read it. Steganography is a technique where the secret image is embedded into cover image to obtain stego image in such a way that no one could imagine about the existence of secret message in it.

The combination of steganography and cryptography certainly provide much better secure communication. Spatial domain steganography and transform domain steganography are the two important techniques of steganography. The spatial domain approach Most Significant Bits (MSBs) of payload pixels replaces the Least Significant Bits (LSBs) of cover image pixels and in transform domain approach, payload and/or cover image are converted into transform domain viz Discrete Cosine Transform (DCT), Discrete wavelet Transform (DWT) and Fast Fourier Transform (FFT) and the LSBs cover image coefficients are replaced by MSBs of payload coefficients.

Steganography finds applications for: information security needed to defend against internal/ external hackers, secure commerce, secure bank accounts/electronic transfers, secure bank accounts/electronic transfers, secure intellectual property, digital rights management, hiding executable multimedia files, covert communications, copy right protection etc.

Contribution: In this paper HDLS is proposed for secure and secret information where cover image and payloads are divided into two cells each and RGB components of cover cell are separated and transformed into frequency domain by retaining the cell II in spatial domain by using DCT and DWT itself. The MSB pixels of payload cell I and cell II are embedded into corresponding cell I and cell II of cover image.

Organization: The paper is organized into following sections. Section 2 is an overview of related work. The steganography model is described in section 3. Section 4 discusses the algorithms used for embedding and extracting process. Performance analysis is discussed in section 5 and Conclusion is given in section 6.

2. LITERATURE SURVEY
Takimoto et al., [1] proposed arrangement and detection method of invisible calibration pattern based on human visual perception characteristics where the calibration pattern is embedded to blue intensity in an original image by adding high frequency component. Zhi-min He Ng et al.,[2] describes steganography detection using localized generalization error model where the discrete cosine transform CDCT features and the markov features are used as inputs of neural networks for detection to provide better performance. Yifeng Sun Fenlin liu[3] proposed a method in selecting cover for image steganography by correlation coefficient to improve the security of steganographic system. The cover data are modeled as Gauss-Markor process where the correlation coefficient of two arbitrary data elements is the exponent of correlation parameter is selected to improve security. Sun et al.,[4] presented a image steganography method based on subband coefficient adjustment in BDCT domain for hiding information. The information file is transformed into a binary sequence and scrambled randomly. Two neighbourong

blocks are selected and transformed by BDCT and Blocks are adjusted to hide information.

Gallegue et al.,[5] proposed a steganographic method based on wavelets and center weighted median filter making use of iterative center weighted median(ICWM) algorithm to estimate the noisy areas of an RGB image and information is hidden in these noisy areas. Weiqui Luo et al.,[6] described an edge adaptive image steganography based on LSB matching revisited which can select the embedding regions according to the difference between two consecutive pixels in the cover image. Shejul and Kulkarni[7] proposed a DWT based approach for steganography using Biometrics in skin tone regions of image that provides secure location for hiding secret data is hidden in one of the high frequency subband of DWT by tracing skin pixels in that sub band. Qinhua Huang and Weimin Ouyang[8] described a steganographic method for making region selection on images to find suitable area for embedding by counting on each pixel whether it could be protected. Ba noci et al.,[9] presented an information hiding method using pseudo-random number sequences with error correction based on code division multiple access(CDMA) approach. Jing-ming Guo and Thanh-Nam Le [10] proposed a method of secret communication using JPEG double compression where the quality factor in a JPEG image is embedding space to hide secret information. Shirali and Shirali et al.,[11] proposed a steganography method in speech signals which is real time and MPEG-1 layer III compression resistant where the silence intervals of speech are found and the length of these interval is changed to hide information.

Djebbar et al.,[12] described dynamic energy based text-in-speech spectrum fast fourier transform method using speech masking properties. It exploits high energetic magnitude frequency components of speech spectrum to hide secret text by evaluating the energy level of each magnitude component and considered only if it is high enough to embed secret data. Yargi et al.,[13] proposed a data hiding method that embed secret data during mixed excitation linear prediction(MELP) coding of the speech signal. The secret data bits are hidden by using quantization index modulation (QIM) which is carried out in the multistage vector quantization(MSVQ) of the spectral frequencies(LSF) parameters. Al-Nabhani et al.,[14] presented an information hiding system to hide the information(data file) after end of header within execution file(EXE file) to make sure changes made to the file will not be detected by universe and the functioning after hiding process and also the execution file is used as a cover file. Zhao et al.,[15] suggested a steganographic to covertly transmit data in multimedia streaming over networks via normal or delayed B frame packets without changing the original traffic pattern and still maintaining relatively high bandwidth and high video quality. Hong mei wang et al.,[16] proposed a triangular algorithm of image hiding which is of higher security and lower distortion y exploring the differences between the blocks of cover image and secret image. Elshoura and Megharbi[17] presented an information can be hidden in gray level images with high transparency using tchebichef moments. A water mark image for hidden data authentication and tampering localization purpose. Jinsuk Back kim et al.,[18] proposed (N,1) secret sharing approach based on steganography with gray digital images by utilizing some simple observed relationships between the binary representation and the utilization of a simple ex-or operation based on N images available to the sender and the receiver. Al Mohammed and Ghinea[19] investicated the pros and cons of images when used as steganography covers and concludes that use of colour images is better for data hiding. Also a research study is made to examine the capability and impact of using chrominance components for data hiding and suggested that in order to increase the hiding capacity. Chrominance components can be used for data hiding at the cost of quality of stego images. Chi-Shiang et al.,[20] proposed a hybrid data hiding method to embed three secret bits to four cover pixels. In the proposed method a Hamming code word consists of the parity check bits whose values are identical to three secret bits and four data bits whose values are derived by performing xor function on four cover pixels. At most one cover pixel would be modified by adopting xor function satisfying the condition of (7,4) Hamming code.

3. MODEL

In this section evaluation parameters, proposed embedding and retrieval models are discussed.

3.1 Evaluation Parameters

3.1.1 Mean Square Error (MSE):

It is defined as the square of error between cover image and stegoimage. The distortion in the image can be measured using MSE and is calculated using Equation 1.

$$\boldsymbol{MSE= [\frac{1}{N*N}]^2 \sum_{i=1}^{N} \sum_{j=1}^{N} (x_{ij}- x_{ij}')^2} \quad (1)$$

Where:

X_{ij} : The intensity value of the pixel in the cover image.

$\bar{X}_{ij}$: The intensity value of the pixel in the stego image.

N: Size of an Image.

3.1.2 Peak Signal to Noise Ratio (PSNR): It is the measure of quality of the image by comparing the cover image with the stegoimage, i.e., it measures the statistical difference between the cover and stegoimage is calculated using Equation 2.

$$PSNR = 10log_{10} 255^2/MSE \ db \qquad - (2)$$

***3.1.3. Capacity*:** It is the size of the data in a cover image that can be modified without deteriorating the integrity of the cover image. The steganographic embedding operation needs to preserve the statistical properties of the cover image in addition to its perceptual quality. Capacity is represented by bits per pixel (bpp) and the Hiding Capacity (HC) in terms of percentage.

3.2 Proposed HDLS Embedding Model:

The payload is embedded into the cover image by segmentation, DCT/DWT to generate the stego image for secret information to be transported to the destination over communication channel confidentially using HDLS is shown in the Figure1.

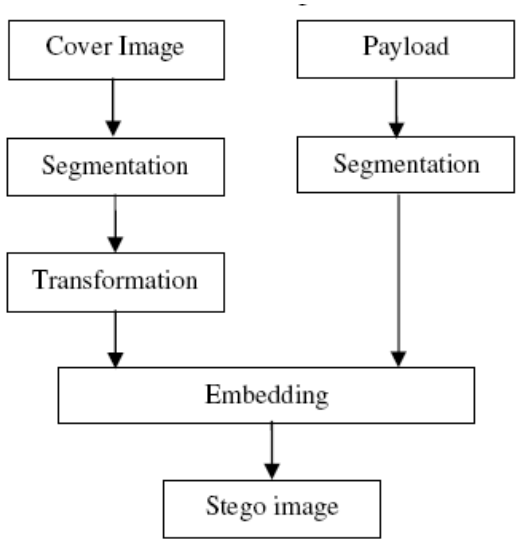

Fig 1: HDLS Embedding Model

3.2.1 Cover Image (CI): The color image of any size and format is considered as a cover image to carry the secret information to the destination through the communication channel.

3.2.2 Payload (PL): The color image of suitable size with different format to be transmitted in covert way embedded into the CI without affecting the statistical properties of CI can be considered as payload.

3.2.3 Segmentation: Cover image and payload are divided into two cells of desired dimensions as shown in figure 2.

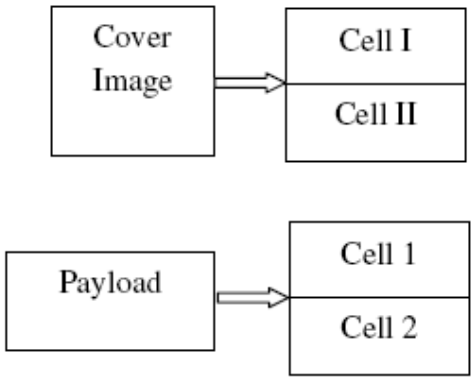

Fig 2: Cell Division

Let the two cells of cover image be cell I and cell II and that of the payload be cell 1 and cell 2

The RGB components are separated in the cover image and payload cells in order to preserve the statistical characteristics of the color image after manipulating CI and PL.

3.2.4 Transformation: The RGB components of cover image cell I are individually transformed from spatial domain to frequency domain using DCT and DWT whereas the components of cell II of cover image are being retained in spatial domain itself as shown in Figure 3.

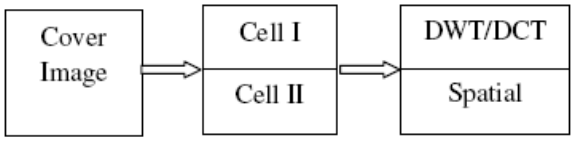

Fig 3: CI Transformation

3.2.5 Embedding Process: The four MSB bits of each pixel in the payload cell 1 and cell 2 are embedded in the second and fourth LSB positions of cover image cell I and cell II respectively to increase the security of the payload and generate stego image in transform domain.

3.2.6 Stego Image: The stego image in the transform domain after embedding payload into the cover image is converted into spatial domain by changing cell I from transform domain into spatial domain. The final stego image in spatial domain is obtained by combining cell I and cell II

3.3 HDLS Retrieval Model:

The retrieval process for the HDLS is described in Figure 4. The payload is extracted by performing the inverse operation of the embedding process.

3.3.1. Stego Image: The payload is embedded into the cover image using HDLS technique with DCT and DWT to obtain stego image

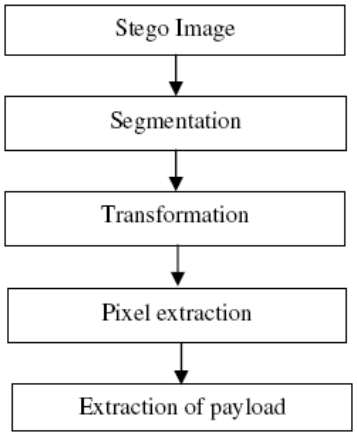

Fig 4: HDLS Retrieval Model

3.3.2. Segmentation: The stego image matrix is divided into two cells of same dimensions as done in embedding process. Let the two cells of stego image be cell 1 and cell 2. The RGB components of stego image are separated.

3.3.3 Transformation: The RGB components of the cell I are individually transformed from spatial domain to frequency domain using DCT/DWT. The cell II components are retained in the spatial domain.

3.3.5. Extraction of payload: The extracted payload bits are arranged in proper way to generate payload image.

4. ALGORITHM

The embedding and retrieval of payload using HDLS algorithm is discussed in this section.

Problem definition: Given cover image and the payload, the objectives are:

1. To embed the payload into the cover image to derive stego image.
2. High robustness with reasonable PSNR to be achieved.

4.1 HDLS Embedding Algorithm: The payload is embedded in the cover image using LSB technique. The cover image matrix and payload are divided into two cells each and the algorithm is given in Table 1.

4.2 HDLS Extraction Algorithm: The retrieval process for HDLS Embedded stego image to extract the payload by performing exactly the inverse operation of the embedding process and the algorithm is given in Table 2.

- Input: Cover image , Payload
- Output: Stego image

(i) Read the cover image and payload images
(ii) Divide the cover image and payload images into two cells each of desired dimension
(iii) RGB components are separated from both cover image and payload image
(iv) The cover image RGB components of cell I are transformed from spatial domain to transform domain, where as the cell II components are retained in spatial domain itself.
(v) Four MSB bits of payload cell 1 and cell 2 are embedded in the second and fourth LSB positions of cover image cell I and cell II respectively to improve security.
(vi) Components in cover image cell I are transformed back to spatial domain and added with cell II components to generate stego image.

Table 1. HDLS Embedding Algorithm

Table 2. HDLS Extraction Algorithm

- Input: Stego Image
- Output :Payload

(i) Divide the Stego image matrix into 2 cells
(ii) RGB components of stego image are separated and transformed from spatial domain to frequency domain
(iii) Extracting the payload MSB bits from segmented cells
(iv) The extracted payload bits are properly arranged to get back the payload image.

Table 3. PSNR comparison for different Techniques with HDLS (DCT)

Image CL(512x512) PL(128x128)	**PSNR**			
	FFT	**DCT**	**DWT**	**HDLS (DCT)**
CL: peppers PL: old image	**39.30**	**34.30**	**35.87**	**41.21**
CL: peppers PL: araras	**38.25**	**34.45**	**35.07**	**41.58**
CL: peppers PL: audrey	**37.0**	**34.31**	**35.22**	**41.3**

Table 4 . PSNR comparison for different Techniques with HDLS (DWT)

Image CL(512x512) PL(128x128)	**PSNR**			
	FFT	**DCT**	**DWT**	**HDLS (DCT)**
CL: peppers PL: old image	**39.30**	**34.30**	**35.87**	**41.21**
CL: peppers PL: araras	**38.25**	**34.45**	**35.07**	**41.58**
CL: peppers PL: audrey	**37.0**	**34.31**	**35.22**	**41.3**

5. PERFORMANCE ANALYSIS

The evaluation parameter PSNR is used as performance analysis factor to verify the image quality between cover image and stego image. The algorithm is tested for over one hundred different kinds of cover images and payloads with different sizes and formats. A cover image and few payloads are shown in Figure 5 for the demonstration purpose. The PSNR values between cover image and stego image for different transform domains such as FFT, DCT, DWT, HDLS with DCT, and HDLS with DWT are compared in the Table 3 and table 4.

in the spatial domain itself. The HDLS with DWT has better PSNR compared to HDLS with DCT as well as individual transform domain techniques. The security to the payload is better in HDLS because it is the combination of spatial and transform domain steganographic techniques.

6. CONCLUSIONS

In modern communication using public channel steganographic method is adopted for maintaining privacy and secrecy of data. In this paper HDLS algorithm is proposed. The cover image and payload are divided into two cells each and RGB components of cover image cell I are transformed using DWT/DCT by retaining the components of cell II in spatial domain itself. The four MSB bits of payload cell I and cell II are embedded into the second and fourth LSB positions of cover image cell I frequency coefficients and cell 2 spatial pixel values respectively. The cell I coefficients are transformed back to spatial domain and then combined with cell II components to derive stego image in spatial domain.The Proposed model is observed to have better PSNR compared to the existing transform domain techniques with improved security.

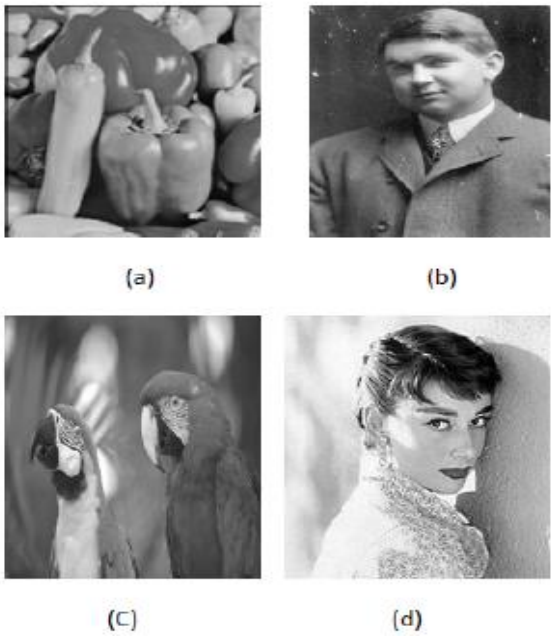

Fig 5: (a) Pepper (b) Old Image (c) Araras (d) Audrey

7. REFERENCES

[1] Takimoto, H Yoshimori, S Mitsukura, Y Fukumi and M Okayama, "Invisible Calibration Pattern Based on Human Visual Perception Characteristics," International Conference on Pattern Recognition(ICPR), pp.4210-4213, 2010

[2] Zhi-Min He Ng, Wing W Y Chan, Patrick P K Yeung and Daniel S "Steganography Detection using Localized Generation Error Model," International Conference on System Man and Cybernetics(SMS), pp.1544-1549, 2010

[3] Yifeng Sun Fenlin Liu, "Selecting Cover for Image Steganography by Correlation Coefficient," International Workshop on Education Technology and Computer Science(ETCS), pp.159-162, vol 2 ,2010

[4] Sun, Qiudong Qiu, Yongping Ma, Wenxin Yan, Wenying Dai, Hong "Image Steganography Based on Sub-Band Coefficient Adjustment in BDCT Domain," International conference on Multimedia Technology(ICMT), pp.1-4,2010

[5] Gallegos-Funes, F J Carvajal-Gamez, B E Lopez-Bonilla, J L Ponomaryov,, "SteganograpHic Method Based on Wavelets and Center Weighted Median Filter," International Kharkov Symposium on Physics and Engineering of Microwaves, Millimeter and Submillimeter Waves(MSMW),pp.1-3,2010

[6] Weiqi Luo Fangjun Huang Jiwu Huang Guangdong, Sun Yat-Sen., Guangzhou, China "Edge Adaptive Image Steganography Based on LSB Matching Revisited," IEEE Transactions on Information Forensics and Security, pp. 201 – 214, vol 5, 2010

[7] Shejul, A.A. Kulkarni," A DWT Based Approach for Steganography Using Biometrics." International Conference on Data Storage and Data Engineering (DSDE), pp.39 – 43,201

[8] Qinhua Huang Weimin Ouyang , Shanghai "Protect fragile regions in steganography LSB embedding," 3rd International Symposium on Knowledge Acquisition and Modeling (KAM), pp.175 – 178,2010

[9] Ba noci, V Buga r, G Levicky , "Information hiding using pseudo-random number sequences with error correction," 20th International Conference Radio elektronika ,pp. 1 – 4, 2010

[10] Jing-Ming Guo Thanh-Nam Le, Taipei "Secret communication Using JPEG Double Compression," Signal Processing Letters, pp. 879 – 882, 2010

[11] Shirali-Shahreza, M.H. Shirali-Shahreza, S. Amirkabir, "Real-time and MPEG-1 layer III compression Resistant Steganography in Speech," *Information Security,IET*, vol.4, pp. 1-7, January 2010

[12] Djebbar, Fatiha Abed-Meraim, Karim Guerchi, Driss Hamam and Habib, "Dynamic Energy Based Text-in-Speech Spectrum Hiding Using Speech Masking,"

International conference on Industrial Mechatronics and Automation(ICIMA), vol.2, pp. 422-426, May 2010

[13] Yargi c og lu and A U I lk, "Hidden Data transmission in mixed excitation Linear Prediction Coded Speech using Quantisation Index Modulation," *Information Security IET*, vol.4, pp. 158-166, September 2010

[14] Al-Nabhani, Y Zaidan B B , "A New System for Hidden Data Within Header space for EXE-File using Object Oriented Technique," *International Conference on Computer Science and Information Technology(ICCSIT)*, vol.7, pp. 9-13, 2010

[15] Zhao, Hong Shi, Yun Q Ansari and Nirwan, "Hiding Data in Multimedia Streaming Over Network," *Communication Networks and Services Research Conference (CNSR)*, pp. 50-55, 2010

[16] Hongmei Wang Limin Qu Fengru Wang, "A Triangular Algorithm of Image-Hiding," *World Congress on Intelligent Control and Automation (WCICA)*, pp. 1012-1016, July 2010

[17] Elshoura and Megherbi, "High Capacity Blind Information Hiding Scheme s Using Tchebichef Moments," *International Conference on Future Computer and Communication (ICFCC)*, vol 1, pp. 649-653, May 2010

[18] Jinsuk Baek Kim, Cheonshik Fisher and Paul S Hongyag Chao, "(N,1) Secret Sharing Approach Based on Steganography With Gray Digital Images," *International Conference on Wireless Communications, Networking and Information Security(WCNIS)*, pp. 325-329, June 2010

[19] Almohammad and A Ghinea, "Image Steganography and Chrominance Components," *International Conference on Computer and Information Technology(CIT)*, pp. 996-1001, July 2010

[20] Chi-Shiang Chan Ching-Yun Chang, "Hiding Secret in Parity Check Bits by Applying XOR Function," *International Conference on Cognitive Informatics (ICCI))*, pp. 835-839, July 2010

AUTHORS PROFILE

ShivaKumar K B received the BE degree in Electronics & Communication Engineering, ME degree in Electronics, MBA from Bangalore University, Bangalore and MPhil from Dravidian University Kuppam. He is pursuing his Ph.D. in Information and Communication Technology of Fakir Mohan University, Balasore, Orissa under the guidance of Dr. K. B. Raja, Assistant Professor, Department of Electronics and Communication Engineering, University Visvesvaraya College of Engineering, Dr.Sabyasachi Pattanaik Reader & HOD, Department of Information and Communication Technology F M University, Balasore, Orissa R K Chhotaray, Principal, Seemantha Engineering College, Orissa. He has got 27 years of teaching experience and has over 25 research publications in National and International conferences and journals. Currently he is working as Professor, Dept. of Telecommunication Engineering, Sri Siddhartha Institute of Technology, Tumkur. His research interests include Signal processing, Multi rate systems and filter bags, and Steganography.

Dr. K B Raja is an Assistant Professor, Dept. of Electronics and Communication Engineering, University Visvesvaraya college of Engineering, Bangalore University, Bangalore. He obtained his BE and ME in Electronics and Communication Engineering from University Visvesvaraya College of Engineering, Bangalore. He has been awarded Ph.D. in Computer Science and Engineering from Bangalore University. He has got 25 years of teaching experience and he has over 60 research publications in refereed International Journals and Conference Proceedings. Currently he is guiding 10 Ph D scholars in the field of image processing. He has received Best Paper Award for the contributed paper in Fourteenth IEEE-ADCOM 2006. His research interests include Image Processing, Biometrics, VLSI Signal Processing and computer networks.

Dr. Sabyasachi Pattnaik has done his B.E in Computer Science, M Tech., from IIT Delhi. He has received his Ph D degree in Computer Science in the year 2003 & now working as Reader in the Department of Information and Communication Technology, in Fakir Mohan University, Vyasavihar, Balasore, and Orissa, India. He has got 20 years of teaching and research experience in the field of neural networks, soft computing techniques. He has got 50 publications in National & International journals and conferences. He has published three books in office automation, object oriented programming using C++ and artificial intelligence. At present he is involved in guiding 8 Ph D scholars in the field of neural networks, cluster analysis, bio-informatics, computer vision & stock market applications. He has received the best paper award & gold medal from Orissa Engineering congress in 1992 and institution of Engineers in 2009.

Dr. R K Chhotaray received B.Sc Engineering in Electrical Engineering and M.Sc Engineering in Electrical Engineering with specialization in Control Systems from Banaras Hindu University, and Ph D in Control Systems from Sambalpur University. He was Professor and Head of Department of Computer Science and Engineering, Regional Engineering College, Rourkela, from which he retired in 2003. Currently he is working as Principal of Seemanta Engineering College, Orissa. He has been associated with many Universities of India in the capacity of Chairman and member of various Boards of Studies, syllabus committee, and Regulation committee. He has about hundred publications in International and National journals of repute, and has received Best Technical Paper award in many occasions. His special fields of interest include Control of Infinite dimensional Hereditary Systems, Modeling and Simulation, Theoretical Computer science, signal and Image processing, and optimization.