International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

A Robust Image Cryptography Scheme using Optimal Band Selection and Dynamic Key Embedding

Ali Baig Mohammad, Tummala Ranga Babu

Abstract*: Secure Image transmission over media like internet has become very important these days. Several techniques for enhancing security during image transmission like cryptography, steganography, etc. evolved over a period of time. In all these techniques, the images are converted to a form that is not detectable by the intermediate user except the sender and the authenticated user. Still these techniques have limitations in ensuring security in the transmission of secret images due to several attacks in the channel through which they are transmitted. In this paper, an approach of embedding secret information in a host image is carried out using a method of selecting the room for embedding in an optimal way to make the model robust against attacks. Further, an optimal way of key embedding is carried out on the selected band. The encrypted image obtained during the above mentioned steps is subjected to several attacks and the effected image is decrypted and the results are compared with the original host image with respect to the metrics like Peak Signal to Noise Ratio (PSNR), Mean Squared Error (MSE) and Normalized Cross Correlation (NCC). This proposed method is applied on several images and the above-mentioned metrics are obtained. The proposed approach proves to outperform the conventional LL band selection and LSB Key embedding methods.

***Keywords*: Cryptography, Discrete Wavelet Transform, PSNR, MSE, NCC.**

I. INTRODUCTION

Security has always remained a prime concern in data exchange. With the growing technology and mode of communication, the need of secure coding and data protection has emerged rapidly. To provide a higher level of secure coding, cryptographic coding was developed. The cryptographic algorithms are categorized based on number of keys as two types: i) Symmetric (Secret Key) cryptography ii) Asymmetric (Public key) cryptography. In symmetric, only one key is used for encryption and decryption and the key should be kept secret. In Public Key Cryptography, two keys are used one is called public key and other is private key. Only private key is secret. The keying based cryptographic approach modulates the original image with an embedding key to provide security coding to the authenticating image data. There are processes where, the image information is embedded with the security information for authentication, such as the watermarking scheme. Even though several methods were proposed, security provisioning still needs to be improved so as to make the transmission robust against attacks. The objective of provisioning security is to preserve the originality of the actual data with providing inherent data towards security, when providing security, it is always that the actual data is encoded, encrypted or embedded. In all these cases, originality of the data is lost due to computing error. The security provisioning efficiency is then measured in terms of the accuracy of the data preserved.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Ali Baig Mohammad, Research Scholar, ECE Dept., ANU College of Engg. & Tech., Acharya Nagarjuna University, Guntur, Assistant Professor, ECE Dept., Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India,
Prof. Tummala. Ranga Babu, Professor & Head, ECE Dept., R.V.R & J.C College of Engineering, Guntur, Andhra Pradesh, India,

II. RELATED WORK

The following works are carried out by different researchers using different means to enhance security in image transmission:

In [1], the Discrete Wavelet Transform on host image is performed and LL band is chosen for embedding the secret data. Also, the LSB positions of selected band are used as rooms for embedding the secret data. A maximum PSNR of 51.6dB is achieved in this method. Towards providing security in image transmission technique, a 2-level Discrete Wavelet Transform is applied on host image and the secret data is embedded in the first two or three or four LSBs of the high frequency components of host image. With this technique, they were able to achieve a maximum PSNR of 49.82dB. Image Hiding method which combines cryptography and steganography is proposed in [3]. An asymmetric cryptographic algorithm which uses public and private key is used. A random LSB embedding is carried out to achieve a maximum PSNR of 56.513dB. A keyless image encryption method is used in [4] which first reserves a room for embedding data by dividing the host image into individual RGB components and then grouped into number of blocks and embedding is carried out. For encryption SDS algorithm is used to obtain a maximum PSNR of 19.19dB. In [5], improvised method of image steganography using Discrete Wavelet Transform, Huffman encoding and RC4 based LSB embedding is proposed. With this technique, a maximum PSNR of 58.7dB is obtained. A stochastic local search method combined with LSB technique for image steganography is proposed in [6].

A maximum PSNR of 74.34dB is obtained in this this proposed method. An image steganography method using QR code and cryptography is proposed in [7]. Embedding of encoded secret message using QR code into high frequency components of host image is carried out.

Advanced Encryption Standard (AES) is used as encryption method to achieve a maximum PSNR of 71.44dB. In [8], a high-quality image steganography technique using integer Haar Wavelet Transform using modulus function is used. Secret image is embedded in LL band of host image along with the key in LSB position is done to achieve a PSNR of 52.29dB. In the previous developments for security provision, spectral domain was used. this domain gives the process of time/frequency domain coding. in spectral domain wavelet transforms are used for transformation, and almost in all past literature, LL bands is selected for security coding, considering a lower information density in this band as it is derived from a set of low pass filters. However, it is observed that, all the residual information's are concentrated on this band, which could be further filtered to given more finer details. Secondly, in many images, among the 3 details bands (HVD), there would be less density in some band.

III. PROPOSED METHOD

The experimental work is carried out in two steps. As a part of step 1, the host image is preprocessed and Discrete Wavelet Transform (DWT) using biorthogonal filtration is applied on this preprocessed host image. The LL band of the host image is selected as a room for embedding the secret image and the key. Key is used as a security bit in provisioning authentication to a valid user. In the key based security, the key string in binary form is xored with the information bit based on the selected location of the binary bit pattern. In reception, the key is used for unlocking the actual data. The embedding and key security together can be seen in multiple security coding in past. The key based security can be developed both in public and private key based approach. On the received data when the key is applied, the embedded data can be extracted for reference. Key length variation has a direct impact on the processing complexity and security robustness. The key is embedded in the LSB bits of the LL band of the host image. On the resultant image, IDWT is applied and encrypted image is obtained. This encrypted image is subjected to attacks like JPEG compression, Cropping, Salt and Pepper noise, Rotation attacks. The resultant image is applied to the decrypting system and a retrieved image is obtained by performing opposite actions as that of encryption scheme. This retrieved image is compared with original host image and performance metrics like MSE, PSNR and NCC are computed. As a part of second step in experimentation, we took a host image and preprocessed it to get a 110 * 110-pixel sized host image. This host image is decomposed into four spectral bands using Discrete Wavelet Transform (DWT) with biorthogonal filtration. The spectral energy of these bands is computed using Power Spectral Density (PSD). An optimal band is selected which has lowest spectral energy as a room for embedding the secret data. The secret data is embedded in this selected band. For the selected band, key embedding location is derived using RC4 algorithm. This is done by computing spectral distribution of the embedded image. A threshold (th) is obtained using the following equation (1):

$$th = \text{minimum (SD)} * \alpha \quad (1)$$

where SD is Spectral Distortion and α is controlling factor for key embedding. An optimal value of α is taken as 0.75 in this work. The coefficients below the computed value of threshold (th) contribute very less in information, hence those coefficients are selected for key embedding. The key is obtained from the RC4 algorithm as shown in the below steps:

(a) Converting the image into string

(b) Defining the message length and obtaining the information vector (iv) using randint()

(c) Obtain the lengths of iv, key and message.

(d) Obtain the state table consisting of all permutations from 0 to 256.

(e) The required key is generated using the logic shown below:

```
for I = 1: ArrLen
  j = mod (j + S(i) + k(i), ArrLen)
  if j = 0
      j = 1;
  end
 %swap values
  Temp = S(i);
  S(i) = S(j);
  S(j) = Temp;
end
```

For the selected location, key value is transformed to binary and each of the key bit is then xored with LSB bit of the selected pixel. Thus, an encrypted image is obtained by embedding the secret image and key at appropriate locations of host image. This encrypted image is subjected to different attacks like JPEG compression, Cropping, Salt and pepper noise attack, Rotation, etc. The effected image is decrypted where exoring of LSB bit with secret bit is performed. The obtained result is compared with threshold value (th). Each of the value satisfying $V_{ij} <= th$ is upgraded with the value. The results are compared with original host image with respect to Peak Signal to Noise Ratio (PSNR), Mean Squared Error (MSE) and Normalized Cross Correlation (NCC). The algorithmic steps are illustrated in the block diagrams shown below:

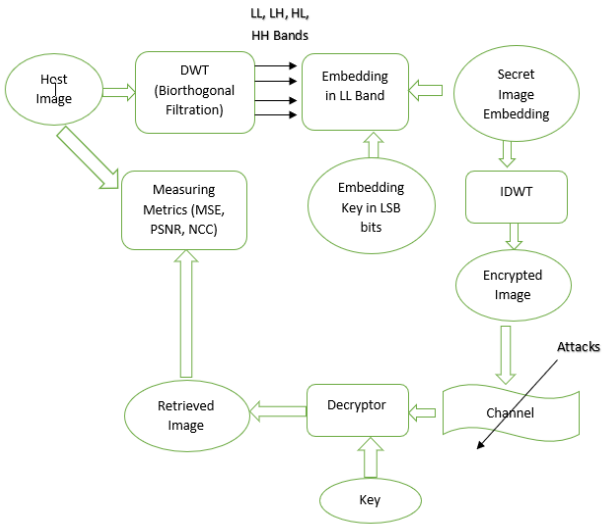

Fig.1: Block Diagram of conventional method

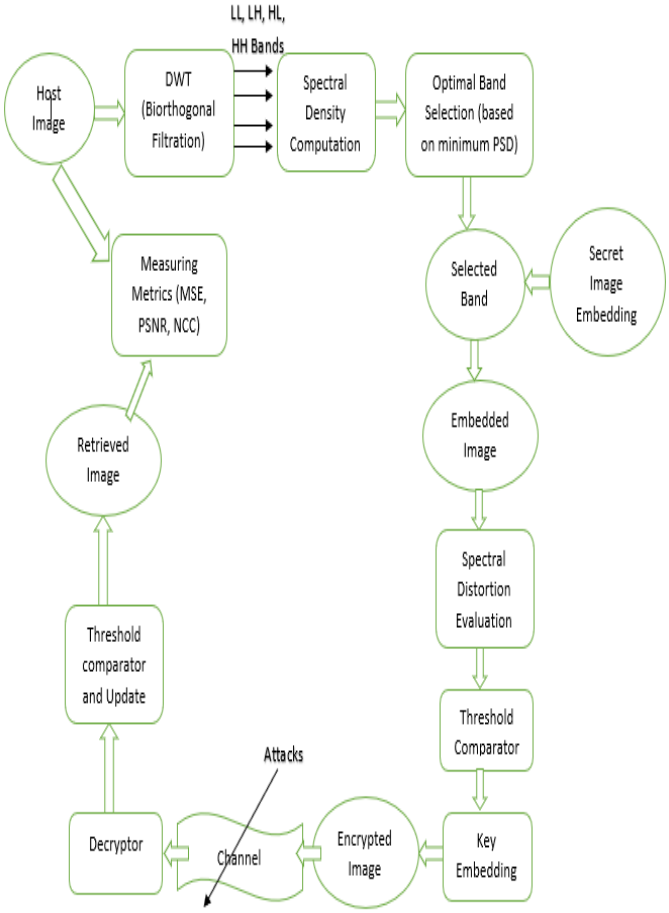

Fig 2: Block Diagram of proposed method

IV. MEASURING METRICS

A. *Mean Squared Error (MSE)*

This parameter is computed between original host image and the retrieved host image using the equation (2) shown below. The security provisioning efficiency is measured in terms of the accuracy of the data preserved. This accuracy is measured in terms of MSE, where it is checked that how much error is introduced due to security coding on the original data. Lower the MSE higher the efficiency of the security-coding algorithm.

$$MSE = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N}\left|A_{ij}-R_{ij}\right|^{2}}{N \times N} \quad (2)$$

where A_{ij} is the original host image, R_{ij} is the retrieved host image and N x N is the size of the original host image after preprocessing.

B. *Peak Signal to Noise Ratio (PSNR)*

This parameter conveys the information about how much the host image got affected due to the embedding of secret image and the key. The higher value of PSNR indicates a better security of the coding algorithm. This is computed using the equation (3) given below:

$$PSNR = 10\log\left(\frac{N^{2}}{MSE}\right) \text{ in dB} \quad (3)$$

where MSE is Mean Squared Error obtained using equation (2) and N is 1 for double precision floating point type images and 255 for unsigned integer type images.

C. *Normalized Cross Correlation (NCC)*

This parameter is computed using the equation (4) shown below:

$$NCC = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N}\left|A_{ij}-R_{ij}\right|}{\sum_{i=1}^{N}\sum_{j=1}^{N}A_{ij}} \quad (4)$$

This parameter reflects the preservation efficiency in terms cross correlation function.

V. EXPERIMENTAL RESULTS

The conventional and proposed algorithms are implemented on different sets of host images and secret images with different lengths of key using MATLAB 9.5. The experimental results obtained are as shown below:

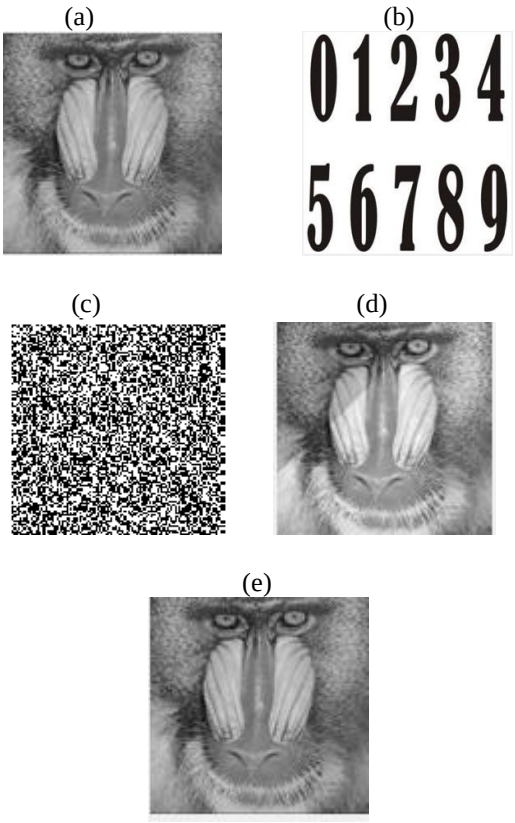

Fig. 3: Baboon – (a) Original Host image, (b) Secret Image, (c) Cipher Image (d) Reconstructed Host image using conventional method (e) Reconstructed Host image using proposed method

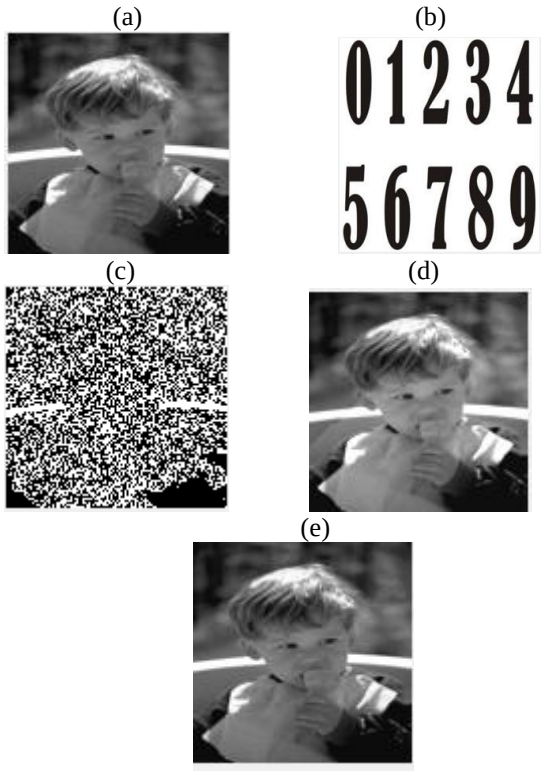

Fig. 4: Kid – (a) Original Host image, (b) Secret Image, (c) Cipher Image (d) Reconstructed Host image using conventional method (e) Reconstructed Host image using proposed method

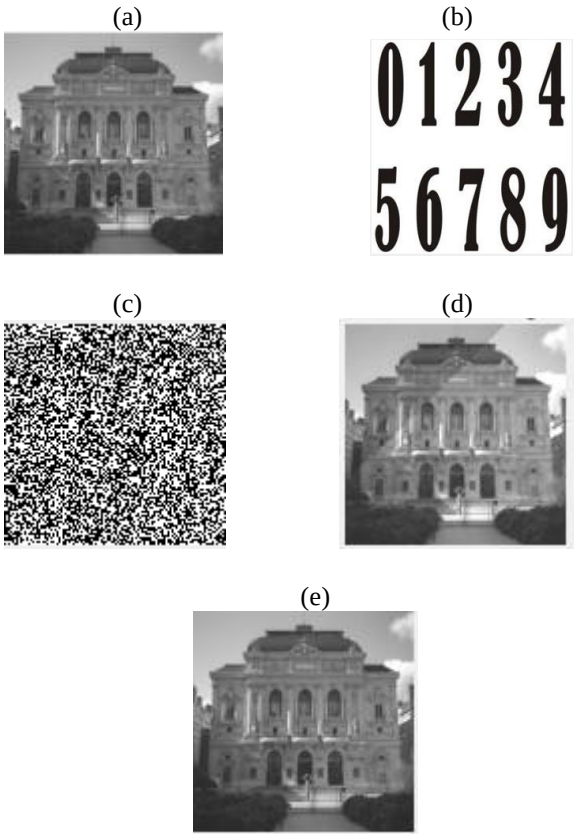

Fig. 5: Opera – (a) Original Host image, (b) Secret Image, (c) Cipher Image (d) Reconstructed Host image using conventional method (e) Reconstructed Host image using proposed method

Table I: Comparison of conventional and proposed methods in terms of PSNR

Host image/Secret image	Conventional method	Proposed method		
		Key Length (no. of bits)		
		2	32	128
Baboon//E3	41.69	67.06	66.74	62.91
Kid/E3	41.47	81.69	81.63	81.42
Flower/E3	46.67	82.95	82.91	82.61
Opera /E3	41.65	85.67	77.87	67.79
E5/E3	40.22	83.16	83.16	77.86

Table II: Comparison of conventional and proposed methods in terms of MSE

Host image/Secret image	Conventional method	Proposed method		
		Key Length (no. of bits)		
		2	32	128
Baboon//E3	4.3998	0.0128	0.0138	0.0332
Kid/E3	4.6334	0.0043	0.0046	0.0047
Flower/E3	5.5656	0.0329	0.0322	0.0356
Opera /E3	4.4503	0.0017	0.0011	0.0108
E5/E3	6.1805	0.0034	0.0036	0.0042

Table III: Comparison of conventional and proposed methods in terms of NCC

Host image/Secret image	Conventional method	Proposed method
Baboon//E3	0.1565	1.1266
Kid/E3	0.1457	1.1108
Flower/E3	0.3632	1.2280
Opera /E3	0.1345	0.8585
E5/E3	0.4682	5.3388

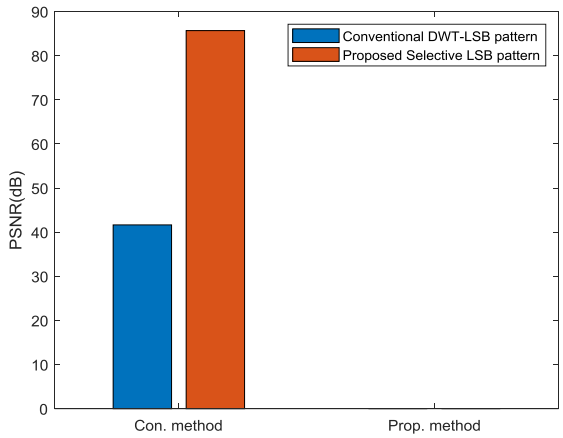

Fig. 6: PSNR Plot for Opera image

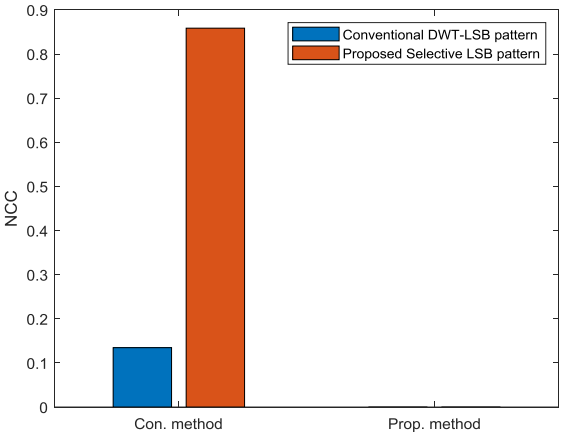

Fig. 7: NCC Plot for Opera image

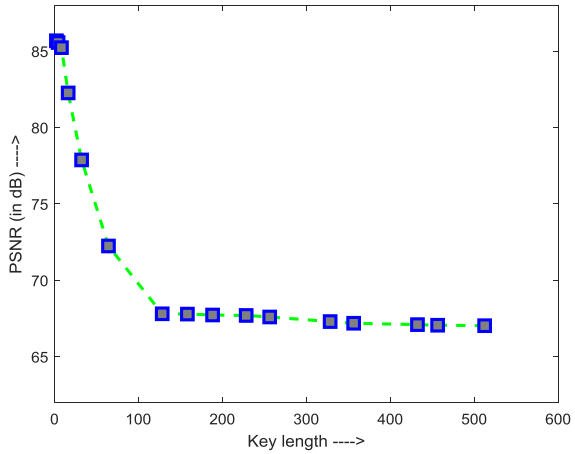

Fig. 8: PSNR variation with key length

VI. CONCLUSION

In conventional method, secret image is embedded in LL band of the host image considering lower information density in LL band. However, the information in LL band is aggregated low-pass output which further contains details that can be detected at the next level. Hence choosing of LL band resulted in retrieval error. For key embedding, this LL band pixels are converted to binary values and LSB position is used to perform exoring operation. This embedding is however maintained in a specific linear manner which is detectable. In the proposed method, instead of fixing to LL band, we go for deciding an optimal band to embed based on its lowest content energy. In this proposed approach, the location of embedding key is derived dynamically based on the pixel content. This dynamic selection is based on spectral distortion and its coefficient selection. Dynamical selection gives two advantages. One is robustness to attacks due to dynamically changing the location for each host image. And the other advantage is that we get less distortion because of selecting low energy region for embedding the secret message. We conclude from the obtained simulation results that the proposed approach is better than conventional method in terms of PSNR values. From this approach, it is also evident that the PSNR values decreases with the increase in key length.

REFERENCES

1. Essam H. Houssein, Mona A. S. Ali and Aboul Ella Hassanien, "An Image Steganography Algorithm using Haar Discrete Wavelet Transform with Advanced Encryption System", *Proceedings of the Federated Conference on Computer Science and Information Systems*, vol. 8., pp. 641-644, 2016
2. Punam Bedi, Veenu Bhasin and Tarun Yadav, "2L-DWTS – Steganography technique based on second level DWT", *Intl. Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Sept. 21-24, 2016, pp. 1533-1538
3. Xinyi Zhou, Wei Gong, WenLong Fu and LianJing Jin, "An Improved Method for LSB Based Color Image Steganography Combined with Cryptography", 15th International Conference on Computer and Information Science (ICIS), pp. 1-4, 2016
4. Miss. Nuzhat Ansari and Prof. Rahila Shaikh, "A Keyless Approach for RDH in Encrypted Images using Visual Cryptography", *Procedia Computer Science (2016)*, vol. 78, Dec 2015, pp. 125-131.
5. Janki Jasani, Sarita Visavalia "A secure and high capacity image hiding scheme using DWT and arithmetic coding", *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, October 2016, pp, 492-496.
6. Dalila Boughaci, Abdelhafid Kemouche ,Hocine Lachibi, "Stochastic Local Search Combined with LSB Technique for Image Steganography", 2016 13th Learning and Technology Conference (L&T), September 2016, pp. 36-44.
7. Vladimír Hajduk, Martin Broda, Ondrej Ková, Dušan Levický, "Image steganography with using QR code and cryptography", *26th Conference Radioelektronika 2016, Košice, Slovak Republic*, April 19-20, 2016.
8. Prajanto Wahyu Adi, Farah Zakiyah Rahmanti , Nur Azman Abu "High Quality Image Steganography on Integer Haar Wavelet Transform using Modulus Function", 2015 International Conference on Science in Information Technology (ICSITech), pp. 79-84.

AUTHORS PROFILE

Ali Baig Mohammad obtained his M.E. in Electronics & Communication Engineering (Systems & Signal Processing) from Osmania University, Hyderabad, B.Tech. from Bapatla Engineering College, Bapatla (affiliated to Acharya Nagarjuna University). He is currently pursuing his Ph.D in Electronics and Communication Engineering at Acharya Nagarjuna University and working as an Assistant Professor in ECE Dept., KLEF deemed to be University. He is a member in various professional bodies like IETE, IAENG. His research interests are Signal processing, Image processing and Machine Learning.

Tummala Ranga Babu obtained his Ph.D. in Electronics and Communication Engineering from JNTUH, Hyderabad, M.Tech in Electronics & Communication Engineering (Digital Electronics & Communication Systems) from JNTUA, Anantapur, M.S.(Electronics & Control Engineering) from BITS, Pilani. He obtained his B.E. (ECE) from University of Madras. He is currently holding the position of Professor & Head of the Department of Electronics & Communication Engineering., RVR & JC College of Engineering, Guntur. He is a member in various professional bodies like IEEE, IETE, ISTE, CSI, IACSIT. His research interests include Image Processing, Pattern Recognition, Embedded Systems, Digital Communication.