International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 2, February - 2014

Parametric Evaluation of Images for Classification in View of Steganalysis

J. Anita Christaline[1], R. Ramesh[2], D. Vaishali[3]
Department of ECE[1,2,3], SRM University[1], Saveetha Engineering College[2], SRM University[3].
Chennai, India.

***Abstract* - Image steganography has profound growth owing to the fact that the minor changes in image parameters are perceptually indiscreminable. With the increasing number of image steganographic techniques, the methods to detect them need to be more efficient. Universal steganalysis attempts to detect the presence of embedded information independent of the embedding method used. In such a situation, the analysis of the image in terms of certain parameters becomes essential. This paper intends to identify the image characteristic parameters that ease the steganalysis of images by classifiers. We have implemented the three major types of image steganographic techniques (LSB, Filtering and masking, Transform techniques) that embed an image into another image. The characteristics parameters of an image are calculated between the stego image and the cover image. The analysis shows that, the parametric variations are dependent on the method of steganography. Based on the findings of this research work, it can be seen that these characteristic parameters could be used as a feature set for steganalysis classifier which identifies the presence of steganography. Also, based on the range of values of these characteristic parameters, the probable method of steganography can be identified.**

Keywords – Image steganography, Steganalysis, Classifiers, Image parameters, stego image, cover image.

I. INTRODUCTION

Steganography is the art of hiding information within some media. The word steganography is of Greek origin which means "covered writing". In contrast to cryptography in which the communication is explicit in the form of cipher text, steganography provides invisible communication. In steganography the existence of the secret information is not noticeable by humans. Digital steganography has become more popular due to the fact that digital media like audio, image or video files have data or information that are not easily observed by humans. Minor changes to these digital data like change in colour or change in sound can never be noticed by humans but can be noticed by a person who reads the digital information. This advantage of perceptual invisibility in digital media has led to an increasing number of techniques for hiding or embedding secret information into any digital media [1]. According to the digital medium or carrier chosen for steganography, steganography can be classified as image steganography, audio steganography or video steganography.

The basic components of a Steganographic system are the carrier, message, password and the stego object. The carrier is known as the cover object into which the secret information can be embedded. The message is the confidential information that has to be transmitted from the sender to the receiver. The password is a key that is used by the sender and the receiver to implement the hiding (embedding) and the retrieval (debedding) process. The stego object is the cover object with the embedded or hidden information. The basic model of a Steganographic system is shown in Figure.1.

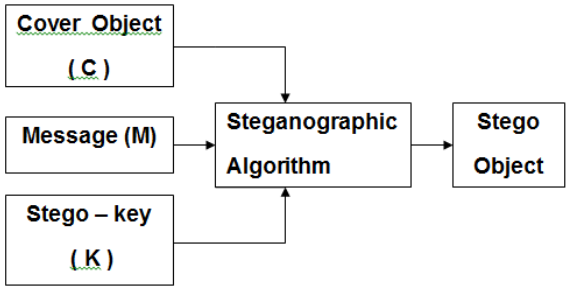

Fig. 1. Basic Model of a Steganographic system.

The process of retrieving the hidden information from the stego object is called as Steganalysis. Current steganalysis methods fall broadly into one of two categories, Embedding specific steganalysis [2] – [8] and Universal steganalysis [9] – [12]. Universal steganalysis attempts to detect the presence of embedded information independent of the embedding method used. In such a situation, the analysis of the image in terms of certain parameters becomes essential.

The concepts related to image steganography are discussed in the next chapter, followed by the characteristic features of the stego images in the third chapter. The fourth chapter presents the experimental data of different image Steganographic methods and their image characteristics. The fifth chapter follows with an analysis of the image characteristics of the stego images obtained by different methods.

II. OVERVIEW OF IMAGE STAGANOGRAPHY

There are various methods of embedding the secret information into the image. According to M. Khan. et al, the most common methods of image steganography are LSB method, Filter method and Transform methods [13].

A. *LSB Method*

The LSB method is the most simple and efficient method for embedding an information into an image. In LSB method, the least significant bits of an image are replaced. Depending on the complexity of the algorithm either one or more LSBs can be replaced by the secret information. An image pixel of a Grayscale image can be represented as an eight bit integer.

A true color image has three planes of pixels, each of which can be represented by an eight bit integer. A bit plane of a grayscale image can be created by considering only the Bi_s of all the pixels in that image. A bit plane L_0 can be obtained by selecting only the LSB_s of all the pixels, a bit plane L_1 can be created by choosing only the B_{1s} of all the pixels, and so on [14]. With respect to the information content in an image, it could be seen that the LSBs contain less perceptual information about the image and the MSBs contain more perceptual information.

Due to this fact, when the LSB of an eight bit integer is changed, the change in pixel value is less whereas when the MSB of an eight bit integer is changed, the change in pixel value is more. A lesser change in pixel value leads to less perceptual changes, but a larger change in pixel value leads to high perceptual changes that could be noticed by human visual system. In practical situations considering the LSBs from B_0 to B_3, for embedding the secret information shows lesser visible changes in the cover image. Thus LSB method of steganography proves to be very simple but can be easily broken down by common steganalysis methods.

B. *Filter Method*

The Filter method of steganography filters and chooses only certain pixels in the cover image. The selection of the pixels can be random or it can be based on mathematical formulae. This formula is the password or the key for the embedding process in the sender side and the corresponding debedding process in the receiver side. The filtered pixels are then pre-processed based on the requirement of the embedding algorithm. As the embedding logic in filter method is at the discretion of the user, the sender can adopt his own method of embedding and debedding. According to Anita and Vaishali, an implementation of filter method has a pre-processing stage where all chosen pixels are converted to even values [15]. Their embedding algorithm, involves converting the secret information into ASCII bit stream and then incrementing or decrementing the processed pixel values according to the information bit stream. Other methods may involve pixel value differencing or modifying the histograms range to embed the secret information.

C. *Transform Methods*

Transform techniques convert the cover image and the secret information into frequency domain, where they are modulated and then converted back to spatial domain by inverse transform techniques. Popular transform techniques are the DCT, DWT and DFT.

The DCT separates an image into spectral sub bands that differ in visual quality [16]. In steganography, DCT can be applied to the entire image or the image can be segmented into blocks and DCT can be applied to the individual blocks. The secret information can be embedded in the DCT coefficients [17].In wavelet based steganography, information in spatial domain can be converted to frequency domain by wavelet transform. In image steganography, the wavelet is capable of separating the high frequency and the low frequency components. The four bands of DWT are the approximate band coefficients (LL) which represents the low frequency components, horizontal band coefficients (HL), vertical band coefficients (LH) and the diagonal band coefficients (HH). Excluding the LL band, the other bands contain details of the high frequency components and hence are detailed bands. The edge details in the spatial domain are represented by these detailed bands. The four bands of the wavelets can be processed independently without interaction with each other. The inverse wavelet transform of the processed bands, show good similarity with that of the original image [18]. This facilitates image steganography where the secret information can be embedded into the wavelets coefficients.

III. CHARACTERISTIC FEATURES OF STEGO IMAGES

The characteristics of an image can be obtained in terms of parameters like MSE, PSNR, average difference, maximum difference, entropy of normalised cross coefficient, normalized absolute error and structural content of images. These parameters are calculated for a distorted image (stego image) as compared to a clean or cover image. The major disadvantage of MSE is its dependence on the intensity scaling of an image. The Peak Signal to Noise Ratio (PSNR), avoids this scaling problem. The disadvantage with PSNR is that the signal (pixel) strength considered is squared value, rather than the actual signal (pixel) strength. The parameter, average difference (AD) is calculated as the ratio of the sum of error to the size of the image, where error is the difference of the stego image from the cover image.

The maximum difference (MD) is the ratio between maximum values of the error between the two images. MD = error. The normalized absolute error (NAE) is the ratio of the sum of the absolute error to the sum of the pixel values of the cover image. Structural content (SC) between two images is considered as the ratio between their sums of pixel values. Finally, the entropy of normalized cross correlation (ENCC) between two images is the measure of randomness in the normalised cross correlation.

These measures can be used to characterise the difference between two images.

IV. IMPLEMENTATION

In this paper we have implemented four different methods of image steganography in MATLAB and have studied the image characteristics in terms of the above mentioned parameters.

The first method embeds an image into another image by replacing four LSB bit planes of the cover image. The cover image used is mask and we have chosen the secret images as woman, bust, rice and circles. The logic for this LSB method is as follows,

A. *Embedding logic for LSB replacement method*

1. Load the cover image.

2. Mask the LSBs from B_0 to B_3.
3. Load the secret image.
4. Mask the LSBs from B_0 to B_3.
5. Set the LSB bits of cover as the MSB bits of the secret image.
6. Display the cover and the stego images.

The second method is a filter method that selects certain pixels from the cover image based on a chosen mathematical formula. These chosen pixels are used to embed another image. The cover image used is mask and we have chosen the secret images as woman, bust, rice and circles.

B. Embedding logic for Filter method

1. Load the cover image.
2. Select pixels for embedding.
3. Load the secret image.
4. Embed the secret image into cover image by incrementing the cover image, if the secret image pixel value is greater than a chosen threshold.
5. Display the cover and stego images.

The third and fourth methods are the DCT and DWT methods of steganography. The cover image used is mask and we have chosen the secret images as woman, bust, rice and circles. Here the cover image and the secret image are converted into DCT and DWT coefficients and then the coefficients are added in frequency domain to embed the information.

C. Embedding logic for Transform methods.

1. Load the cover and secret images.
2. Obtain the DCT or DWT transforms of both the images.
3. Generate a stego image from the transform coefficients.
4. Display the cover and stego images.

V. ANALYSIS OF IMAGE DATA

We have implemented the above four steganographic methods for four different secret images namely woman, bust, rice and circles. The cover image chosen is mask. For the sixteen different combinations we have analysed all the above mentioned seven image characteristics. As the MSE is the mean squared error between the images, a higher value of MSE indicates that the cover image is corrupted to a larger extent by steganography. Thus MSE is a good image characteristic parameter for transform method of steganalysis. Similarly a high value of PSNR indicates that there is less possibility of corruption of the cover image. If PSNR is low, then it indicates that steganography has corrupted the cover image. Also a higher value of absolute error and maximum error denote occurrence of steganography, while lower value indicates less chances of steganography.

The tables showing the characteristic parameter variations are shown below.

TABLE I
LSB METHOD

COVER IMAGE IS mask				
Image parameter	Secret image is woman.	Secret image is bust.	Secret image is rice.png	Secret image is circles.png
MSE	26.5731	34.1093	23.3000	73.3562
PSNR	33.8864	32.8021	34.4572	29.4764
AD	0.5780	0.4662	1.1262	7.6131
MD	15	14	13	15
NAE	0.0223	0.0266	0.0213	0.0409
SC	1.0046	0.9979	1.0105	1.0791
ENCC	4.1544	4.1420	4.1559	4.1525

TABLE II
FILTER METHOD

COVER IMAGE IS mask				
Image parameter	Secret image is woman.	Secret image is bust.	Secret image is rice.png	Secret image is circles.png
MSE	0.8046	0.6810	0.8326	1
PSNR	49.0749	49.7994	48.9265	48.1308
AD	-0.8046	-0.6810	-0.8326	-1
MD	0	0	0	-1
NAE	0.0043	0.0037	0.0045	0.0054
SC	0.9921	0.9939	0.9918	0.9902
ENCC	4.1556	4.1571	4.1560	4.1560

TABLE III
TRANSFORM MEETHOD – DCT

COVER IMAGE IS mask				
Image parameter	Secret image is woman.	Secret image is bust.	Secret image is rice.png	Secret image is circles.png
MSE	1.665e+004	2.0038e+004	1.4182e+004	0.2157
PSNR	5.9180	5.1123	6.6136	54.7930
AD	-118.815	-121.8587	-111.2468	-0.2157
MD	1.7053e-013	-18.0000	-40.0000	1.7053e-013
NAE	0.6386	0.6550	0.5979	0.0012
SC	0.3812	0.3532	0.4034	0.9981
ENCC	4.1633	4.0710	4.2141	4.1560

TABLE IV
TRANSFORM MEETHOD – DWT

COVER IMAGE IS mask				
Image parameter	Secret image is woman.	Secret image is bust.	Secret image is rice.png	Secret image is circles.pn
MSE	1.6645e+004	2.0038e+004	1.4182e+004	0.2157
PSNR	5.9180	5.1123	6.6136	54.7930
AD	-118.81	-121.8587	-111.246	-0.2157
MD	-1.2487e-010	-18.0000	-40.0000	2.1714e-010
NAE	0.6386	0.6550	0.5979	0.0012
SC	0.3812	0.3532	0.4034	0.9981
ENCC	4.1633	4.0710	4.2141	4.1560

The analysis of these tables shows that, the MSE is very large for transform methods compared to LSB and filter methods. The MSE is very small for circles.png in transform methods. The PSNR is large for the filter method and is very small for transform methods. The average difference and maximum difference are least for transform methods and is large for LSB method. The normalised absolute error is high for transform methods and is less for filter method. The value of structural content is large for LSB method and is least for transform method. The entropy of normalised cross correlation is almost in the same range for all the methods. Thus based on the image characteristic parameters, the presence of steganography can be identified and based on the range of their values, we can guess the method of steganography that was probably used.

VI. CONCLUSION

This paper has implemented the three major types of steganographic techniques (LSB method, Filter method and Transform method) for four different secret images. The parametric variations between the stego and the clean cover image have been analysed in terms of MSE, PSNR, average difference, maximum difference, entropy of normalised cross coefficient, normalized absolute error and structural content of images. From the data analysis, it can be inferred that MSE, PSNR, maximum difference, normalised absolute error and the structural content parameters show good variations than other parameters. As the current steganalysis methods depend on classifiers, these characteristic parameters of the images can be used as a feature set for a classifier that identifies or classifies stego images from the clean cover images. Another inference from this research work is that based on the range of values of the characteristic parameters, the probable method of steganography could be identified. Thus this paper intends to identify the image characteristic parameters that ease the steganalysis of images by classifiers.

A future work of this paper could be the implementation of the various steganographic techniques to embed text information into images and study the variations in the characteristic parameters. Also few additional parameters may be added to the feature set so as to enhance the classification of stego images.

REFERENCES

1. V. Potdar, E. Chang. , "Visibly Invisible: Ciphertext as a Steganographic Carrier.", *Proceedings of the 4th International Network Conference (INC2004)*, page(s):385–391, Plymouth, U.K., July 6–9, 2004.
2. N. Johnson and S. Jajodia, "Steganalysis of images created using current steganography software," in *Lecture Notes in Computer Science*, vol. 1525, 1998, pp. 273–289.
3. A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in *Proc. Information Hiding, Third Int. Workshop*, Dresden, Germany, 1999.
4. N. Provos and P. Honeyman, "Detecting Steganographic Content on the Internet*," Univ. Michigan, Ann Arbor, Tech. Rep. CITI 01-1a*, 2001.
5. J. Fridrich, M. Goljan, and D. Hogea, "Steganalysis of JPEG images: Breaking the F5 algorithm," presented at *the 5th Int. Workshop on Information Hiding*, Noordwijkerhout, The Netherlands, 2002.
6. A. Westfeld, "Detecting low embedding rates," presented at *the 5th Int. Workshop on Information Hiding*, Noordwijkerhout, The Netherlands, 2002.
7. X. Wu, S. Dumitrescu, and Z. Wang, "Detection of LSB steganography via sample pair analysis," presented at the *5th Int. Workshop on Information Hiding*, Noordwijkerhout, The Netherlands, 2002.
8. S. Lyu and H. Farid, "Detecting hidden messages using higher-order statistics and support vector machines," presented at the *5th Int.Workshop on Information Hiding*, Noordwijkerhout, The Netherlands, 2002.
9. I. Avcibas, N. Memon, and B. Sankur, "Steganalysis using image qualitymetrics," *IEEE Trans. Image Processing*, vol. 12, no. 2, pp. 221–229, Feb. 2002.
10. J. Fridrich, M. Goljan, and D. Hogea, "New methodology for breaking steganographic techniques for JPEGs," in *Proc. SPIE, Symp. Electronic Imaging*, Santa Clara, CA, 2003.
11. J. Harmsen andW. Pearlman, "Steganalysis of additive noise modelable information hiding," in *Proc. SPIE Symp. Electronic Imaging*, 2003.
12. J. Fridrich, "Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes," presented at the *6th International Workshop on Information Hiding*, Toronto, ON, Canada,2004.
13. M. Khan, V. Potdar, E. Chang, "A prototype implementation of Grey Level Modification Steganography,", *Proceedings of the 30 th Annual Conference of the IEEE Industrial Electronics Society (IECON2004), vol.1 page(s):463–471*, Busan, Korea, Nov. 2–6, 2004
14. Hideki Noda, Jeremiah Spaulding, Mahdad N. Shirazi, and Eijiawaguchi,, "Application of Bit-Plane Decomposition Steganography to JPEG2000 Encoded Images", *IEEE SIGNAL PROCESSING LETTERS, VOL. 9, NO. 12*, DECEMBER 2002
15. J. Anita Christaline, Vaishali. D, "IMAGE STEGANOGRAPHIC TECHNIQUES WITH IMPROVED EMBEDDING CAPACITY AND ROBUSTNESS" , *IEEE International Conference of Recent Trends in Information Technology*, Chennai, India. June 3-5, 2011.
16. Hardik Patel, Preeti Dave , Steganography Technique Based on DCT Coefficients , International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 (2012), www.ijera.com Vol. 2, Issue 1,Jan-Feb 2012, pp.713-717 713
17. Dr. Ekta Walia, Payal Jain, Navdeep, Analysis of LSB & DCT based Steganography . GJCST Computing Classification F.2.1 & G.2.m (2010), P a g e | 4 Vol. 10 Issue 1 (Ver 1.0), April 2010 Global Journal of Computer Science and Technology
18. Jianyun Xu, Andrew H. Sung, Peipei Shi, Qingzhong Liu, "JPEG Compression Immune Steganography Using Wavelet Transform", *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04)* 0-7695-2108-8/04 $ 20.00 © 2004 IEEE.

APPENDICES

A. Appendix A

1). Output for LSB method

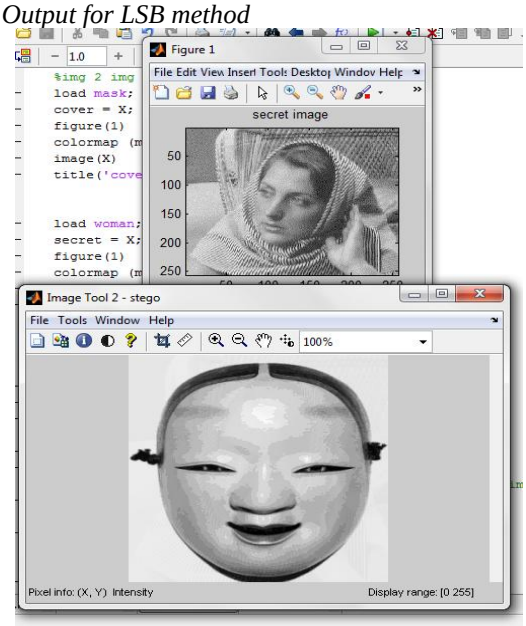

Figure 2. LSB method – cover image is mask and secret image is woman.

2). Output for Filter method

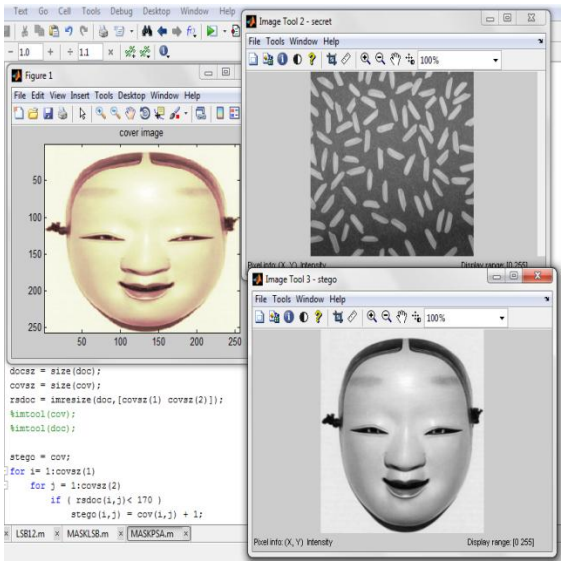

Figure 3. Filter method – cover image is mask and secret image is rice

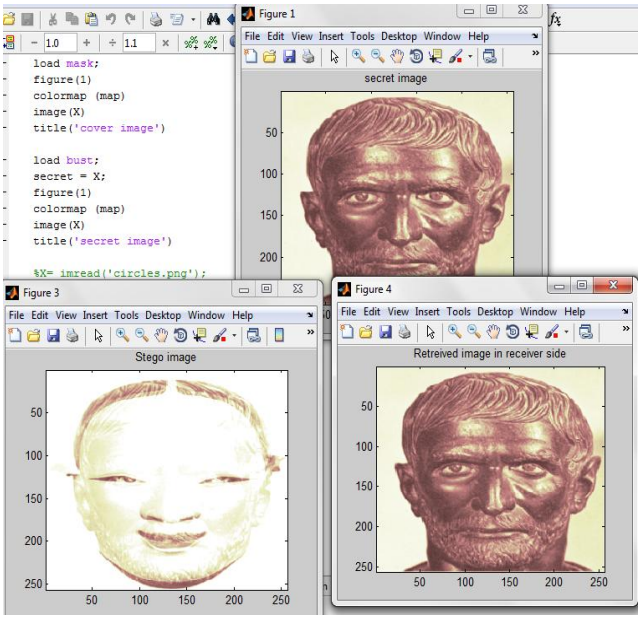

Figure 5. DWT method – cover image is mask and secret image is bust.

3). Output for DCT method

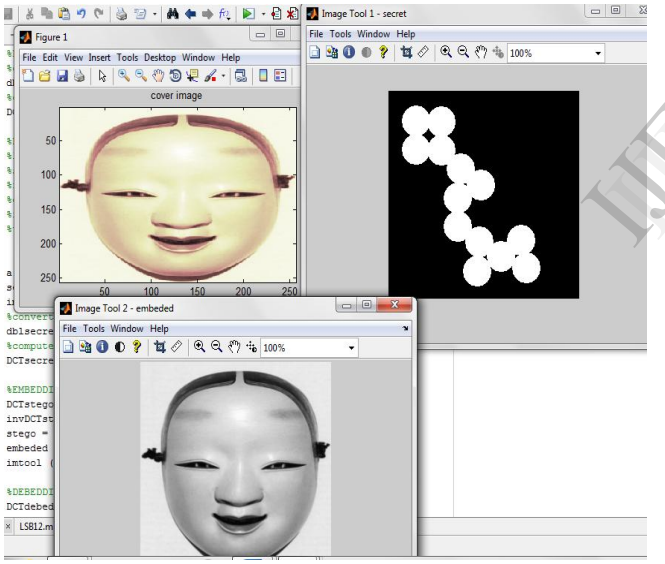

Figure 4. DCT method - cover image is mask and secret image is circles.

4). Output for DWT method

AUTHOR DETAILS

1. J. Anita Christaline was born in Dindigul, India in 1974. She completed her B.E. Degree in Electronics and Communication Engineering in 1996 from Bharathidasan University, Trichy. She is recipient of GATE score during 2003. She received her M.E.Degree in Applied Electronics in the year 2006 from Anna University, Chennai. She is currently working as Assistant Professor in SRM University, Chennai where she is pursuing her Doctoral Degree. Her area of interest is Steganography and Steganalysis by computational intelligence.
Member IEEE , IEEE Id: 92890927

2 R.Ramesh was born in Kanyakumari, India, 1976. He received theB.E.Degree in Electronics and Communication Engineering in 1998 and theM.E. degree in Communication Systems in 2000, both from MaduraiKamaraj University, India. He has been awarded Doctoral degree in theSRM University in the year 2009 for his research work on Testing theStability of two dimensional recursive filters. He is currently working as aProfessor in the Department of Electronics and CommunicationEngineering at Saveetha Engineering College, Chennai. India. His currentresearch interests concern digital signal processing particularly to find thestability of two dimensional recursive digital filters.

ss

3.D.Vaishali was born in Pune, India, 1969.She received B.E .Degree in Electronics and Telecommunication Engineering in 1994 and the M.E. degree in Communication Systems in 2002, both from Pune University, India. She is a research scholar in the SRM University and her research work is progressing in the field of Image Processing with wavelet Transforms. She is currently working as a Asst .Professor in the Department of Electronics and Communication Engineering at SRM University, Chennai. India.
Member IEEE , IEEE Id: 92890908