International Journal of Linguistics and Computational Applications (IJLCA) ISSN 2394-6385(Print)
Volume 1, Issue 1, October - December 2014 ISSN 2394-6393(Online)

Detection of Hidden Information With Bit Plane Analysis

Dr.P.Sujatha

Associate Professor, School of Computing Sciences,Vels University, Chennai, India,

sujinagi@gmail.com

Abstract— Steganalysis is the new research area that is appeared before the late 1990s. It is a technique that is used for detecting the presence of hidden information in some cover media. Normally steganalysis is a challenging task when the pattern of the hidden information is unknown to the steganalysts. To deal with this, bit plane analysis is proposed in this paper. Bit planes of cover and stego images are analyzed by computing the difference of corresponding 8 bit planes so that one can clearly see hidden information with varying densities. Black regions of the image represent the value that is similar for both the images and the white regions represent hidden secret message.

Keywords—*Steganalysis, Cover image, Message image, Stego image, Bit Plane Analysis.*

1. Introduction

Steganography is the process of embedding text information or image into cover image. The "embedding" is otherwise called "hiding information" in a cover image. The cover image appears with no change in the content when looked at the embedded image (stego image). Steganalysis is the way of identifying the presence of hidden information and if possible, recovering the original hidden information for better interpretation.

Covert communication that is implemented using steganography increases much attention in academics and government. Forensics investigation, surveillance systems, criminal investigation, medical imaging, journalism and intelligence services need more reliability while transferring the information in the form of an image. Politicians use steganography communication to express their political thoughts which are more sensitive to the world. The Government can take action on any politician who involve in sensitive issue like decreasing the economical growth of the country. The ease of internet helps in both good and bad usage. Downloading steganography tools easily through internet give challenges for government to trace the people of law breaker. Law enforcement agencies of various nations have started paying much importance in taking preventive measures to defeat the illicit steganography over the Internet. Steganalysis technique can be used for defeating illicit steganography. It is the method of perceiving the hidden message and extracting it. Recent image forensic research has resulted in a number of steganalysis detection techniques utilizing statistical features.

2. Literature Survey

2.1 Rs Steganalysis

Fridrich et al. [3] developed a steganalytic technique for detecting LSB embedding in color and grayscale images. They analyze the capacity for embedding lossless data in LSBs. Randomizing the LSBs decreases this capacity. To examine an image, they define Regular groups (R) and Singular groups (S) of pixels depending upon some properties. Then with the help of relative frequencies of these groups in the given image, in the image obtained from the original image with LSBs flipped and an image obtained by randomizing LSBs of the original image, they try to predict the levels of embedding.

2.2 Dct Domain Steganalysis

Fridrich et al. [5] have shown that this change is proportional to the level of embedding. They also showed that, if an image is cropped by 4 rows and 4 columns, then original DCT histogram can be obtained. The basic assumption here is that the quantized DCT coefficients are robust to small distortions and after cropping the newly calculated DCT coefficients will not exhibit clusters due to quantization. Also, because the cropped stego image is visually similar to the cover image, many macroscopic characteristics of cover image will be approximately preserved. After predicting DCT coefficient's histogram in the original image and comparing with that of a stegoed image, the hidden message length can be calculated.

Many steganalysis researchers such as Neil et al. [9] attempt to categorize steganalysis attacks to recover modify or remove the message, based on information available. The steganalysis technique developed can detect several variants of spread-spectrum data hiding techniques (Marvel et al. [7]). The first steganalysis technique using wavelet decomposition was developed (Farid [2]).

Sullivan et al. [4] use an empirical matrix as the feature set to construct a steganalysis. Chen et al. [11] enhanced and applied the statistical moments on JPEG image steganalysis.

2.3 Feature Extraction For Steganalysis

Yuan Liu et al. [23] proposed three methods for deriving the feature vector such as Robert gradient energy in pixel

domain, variance of Laplacian parameter in DCT domain and higher-order statistics extracted from wavelet coefficients. BPA neural network is applied as the classifier.

Xiangyang Luo et al. [39] used WPT to decompose image into three scales and obtained 85 coefficient sub bands together. Multi-order absolute characteristic function moments of histogram are extracted from these sub bands as features. Finally these features are normalized and combined to a 255-D feature vector for each image. Back-propagation neural network is used as a classifier.

Yuan-lu Tu et al. [33] proposed a method for feature extraction by calculating the features from the luminance and chrominance components of the images. Features are extracted both in DCT and DWT domains. Wavelet high-order statistics is substituted with the moments of wavelet characteristic function. Non linear SVM classification is implemented.

3. Methodology

Generally, the person involved in retrieving the message will not know the pattern of hidden information that has been used during steganography. Keeping this in view, a method has been proposed to find out the presence of information in the cover image. This is identified by bit plane analysis method. The detailed description of this method is given in the subsequent chapter.

Sample cover images (Group 1) are shown in Figure 1.1 .The total number of cover images considered is 1024. The cover and message images have been taken from the Matlab 7® image library. Message images (Group 2) are shown in Figure 1.2. Stego images (Group 3) are shown in Figure 1.3. Group 3 images have been obtained by embedding Group 2 images into Group 1 images.

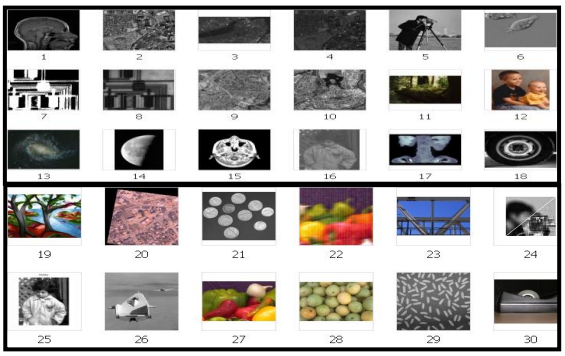

Fig. 1.1 : Cover images (Group 1)

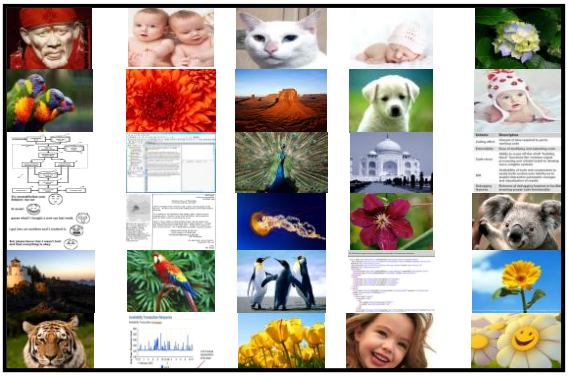

Fig. 1.2 : Message images (Group 2)

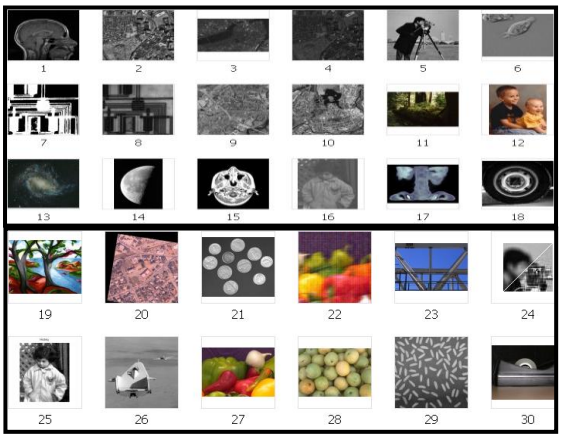

Fig. 1.3 : Stego images (Group 3)

The general procedures followed for embedding information are mentioned below:

- LSB, DCT, DWT, and DFT encoding schemes are considered for the experimental work.
- 256-bit color images (one matrix) and true color images (3 matrices / planes i.e. red, green, blue) - are considered for hiding information.
- Patterns are generated by considering 2 X 2 pixels from cover images, message image and steganographic image. Redundant 2 X 2 pixels are eliminated. Labeling of 2 X 2 pixels is done as 0.1 for cover image, 0.2 for message image and 0.3 for steganographic image.
- The labeling of image types and their target value is shown in Table 1.

TABLE 1 : IMAGE TYPES			
Group Name	**Total Images**	**Image type**	**Value**
Group 1	**1024**	**Cover image**	**0.1**
Group 2	**100**	**Message image**	**0.2**
Group 3	**512**	**Steganographic image**	**0.3**

3.1 Bit Plane Analysis

A binary image is a digital image that has only two possible values for each pixel. Binary images are also called bi-level or two-level. The names black-and-white, monochrome or monochromatic are often used, but may also designate any images that have only one sample per pixel, such as gray scale images. Binary images often arise in digital image processing as masks or as the result of certain operations such as segmentation, thresholding and dithering. Every single pixel in an 8-bits gray level digital image consists of 8 bits. Gray-level images are also encoded as a 2D array of pixels, using eight bits per pixel, where a pixel value of 0 usually means "black" and a pixel value of 255 means "white", with intermediate values corresponding to varying shades of gray. An 8-bit monochrome image can also be thought of as a collection of bit-planes, where each plane contains a 1-bit representation of the image at different levels of detail. An image can be represented with maximum intensity value of 255. The value 255 can be represented by binary values "11111111". Each bit is treated as a plane as in Table 2.

TABLE 2 : BIT ASSIGNMENT								
Intensity values of a pixel	**255**							
Bit value	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
Plane	**1st**	**2nd**	**3rd**	**4th**	**5th**	**6th**	**7th**	**8th**
	Upper nibble (Fore ground in an image)				**Lower nibble (back ground in an image)**			

In actual practice, the person involved in retrieving the message will not know the pattern of hiding information that has been used during steganography. Keeping this in view, a method named bit plane analysis has been proposed to find out the presence of information in the cover image. The cover and message images are shown in Figure 1.4 (a) and Figure 1.4 (b) respectively. The stego image is given in 1.4(c).

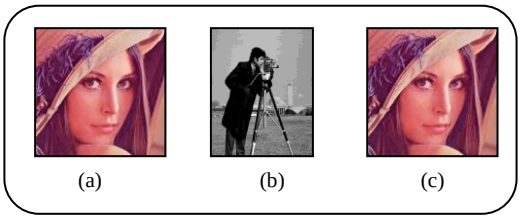

Fig. 1.4 a) Cover image b) Message image c) Stego image

Random least significant bit (LSB) embedding method (Table 3) is used to produce the stego image that is shown in Figure 1.4 (c). Bit planes of cover and stego image which are shown in figure 1.4(a) and Figure 1.4(b) are analyzed. This approach is straight forward and general, so that one can clearly see hidden information with varying densities.

Table 3 LSB Embedding

	Carrier image								Information image							
Category	Upper nibble of carrier image (UN_c)				Lower nibble of carrier image (LN_c)				Upper nibble of information image (UN_I)				Lower nibble of information image (LN_I)			
Original binary value	1	1	1	1	1	0	1	0	1	0	0	1	0	1	0	1
Equivalent decimal value	250								149							
Information embedding																
Method 1									Information embedded in lower 4 bits							
Method 2									Information can be embedded in any of the one or two or three lower bits							
Combined binary value									1	1	1	1	1	0	0	1	Steganographic
Category									UN_c				UN_I			
Decimal value	249															

4. Results And Discussion

Least significant bits are the deserving places in an image to hide the message data, because, their alterations results unnoticeable loss of quality, gives no clue to human eye. The other important nature in LSBs is that, they are completely random in terms of their overall significance to the complete image. The perception of LSBs as a binary image in isolation will appear scattered such that the values make no difference and look very random. Images from the natural scenes mostly include objects which contain color changes because of the varying intensities of visible light subjected on the

objects. Shadows can act as patterns for such type of images. The pixel values of the image decrease by very small amounts as the shadow gets stronger. It can be assumed that the LSBs of an image are more structured posing a huge weakness that can be exploited through visual attacks.

If original cover is available then a forensic expert obtaining the LSB planes of both the original and the suspect image can conclude the cleanness of the suspect image by computing the difference between the two obtained LSB planes one from the other. They will then be left with an image similar to that in which the black regions of the image represent the values that do not change between both images, and the white regions represent secret message detection. The 8 bit planes of both the original and stego image are shown in Figure 1.5 and Figure 1.6 respectively. The difference of corresponding 8 bit planes of original and suspect image is computed and shown in Figure 1.7. White regions are observed within the bit plane images in the Figure 1.7. It can also be observed that the lower bit plane holds much secret information compared to its next higher plane. It is clear that the suspect file is embedded with secret information.

The steganalyst can therefore conclude that the suspect image has been secretly embedded, and they can even identify the locations of the modified pixels. But in practical, the original cover will not be available during steganalysis in most of the cases. To produce a more guaranteed analysis, it is needed to combine several steganalysis methods to fix a suspect image.

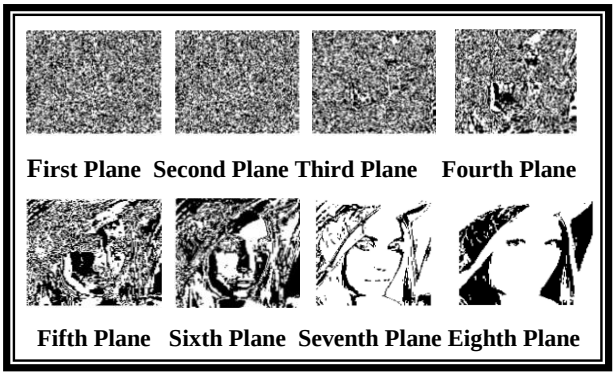

Fig 1.5 Bit Plane Analysis of Cover File

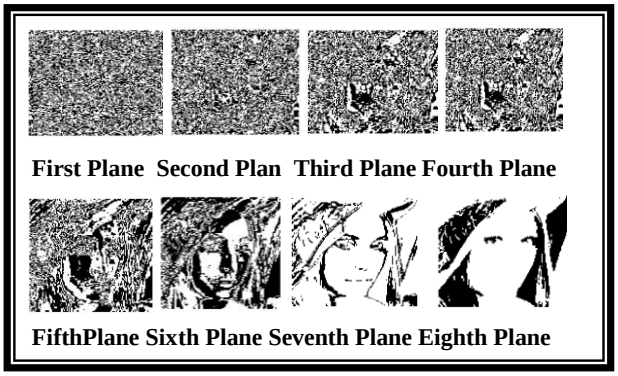

Fig 1.6 Bit Plane Analysis of Stego File

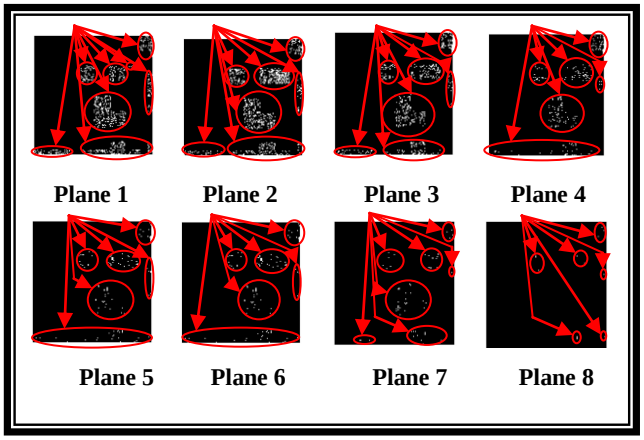

Fig 1.7 Differences of Cover and Stego File

5. Comparison Of Proposed Method With Existing Methods

The proposed method is compared with few more methods which are given in Table 4. The proposed method uses normalized gray scale value as a feature so that the values of the features from the cover images are in the range of 0 to 1, and the computational complexity is reduced. The normalization of the patterns is done by

TABLE 4 COMPARISON OF PROPOSED METHOD WITH EXISTING METHODS

Proposed Method	Pattern Needed / Not Needed	Features	No.Of Images Used	Steganalysis Type	Data Hiding Methods	Reference
Bit Plane Analysis	Pattern not needed	Normalized Gray Scale Value	1024 Cover Images 512 Stego Images	Passive	Random LSB, DCT, DWT, DFT	Current Paper by Dr.P.Sujatha
Neural Network with Local Binary Pattern	Pattern Needed	Local Binary Pattern	1000 Cover Images 1000 Stego Images	Passive	Blindside	Patricia Lafferty et al. [36]
BPA	Pattern Needed	Skewness, Variance, Kurtosis, Mean	44 images for training and 81 images for testing	Passive	Quantization	Liu Shaohui et al. [38]
Feedforward Network With BPA	Pattern Needed	Statistical Moments of Characteristic Function, Wavelet Sub bands	1096 Images	Passive	Generic QIM, Generic LSB, SS, Block SS, Blind SS	Shi, Y.Q. et al. [37]
ANN	Pattern Needed	IQM, Mean, Variance, Skewnes , Kurtosis	1300 images	Passive	Not Mentioned	Jennifer Davidson et al. [39]

$$xi = xi / xmax \quad \text{---------- ---------- (4.1)}$$

Where xi is the value of a feature, and xmax is the maximum value of the feature.Also, bit plane analysis

method is preferable for the steganalysts when the pattern of the hidden information is not known.

6. Conclusion

Hidden information is detected with different densities by analyzing the bit planes of cover and stego image. The amount and density of information present in each plane is also represented in this paper. The hidden information is clearly depicted using white dots. The significance of Bit plane analysis is that it is very much useful when the pattern of the hidden information is unknown for the steganalysts. Also it uses the normalized gray scale values as a feature and hence the computational complexity is reduced. However in most of the cases the original cover image will not be available for the steganalysts. In such case, several steganalysis methods should be combined to produce a more guaranteed analysis.

References

[1] Fridrich, J., and Goljan, M., Digital image steganalysis using stochastic modulation, Proceedings of IST/SPIE's 15th Annual Symposium on Electronic Imaging Science and Technology, San Jose, CA, 2003.

[2] Farid H., Detecting steganographic Messages in Digital images, TR2001-412, Department of Computer Science, Dartmouth College, 2001.

[3] Fridrich, J., Goljan, M., and Du R., Reliable Detection of LSB steganalysis in Color and Gray-Scale Images, Magazine of IEEE Multimedia Special Issue on Security, 2001, pp. 22-28.

[4] Kenneth Sullivan , Onkar Dabeer, , Upamanyu Madhow, Shivakumar Chandrasekaran, and Manjunath, B.S., Detection of Hiding in the Least Significant Bit, IEEE Transactions on Signal Processing, 2004, Vol. 52, No. 10, pp. 3046-3058.

[5] Fridrich, J., and Miroslav Goljan., Practical steganalysis-state of the art, Proceedings of SPIE Photonics West, 2002, Vol.4675, pp 1–13.

[6] Liu Shaohu, I., Yao Hongxun., and Gao Wen., Neural Network Based steganalysis in Still Images, IEEE International Conference on Multimedia and Expo, (ICME), 2003, Vol. 2, pp. 509 - 512.

[7] Marvel, L., Boncelet Jr, C.G., and Retter, C.T., Spread spectrum image steganalysis, IEEE Transaction on Image Processing, 1999, Vol. 8, No. 8, pp. 1075-1083.

[8] Mohsenzadeh, Y., Mohajeri, J., and Ghaemmaghami, S., Histogram shift steganography: A technique to thwart histogram based steganalysis, Proceedings of 2nd International Workshop on Computer Science and Engineering, 2009, Vol. 2, pp. 166-170.

[9] Neil Johnson, F., and Sushil Jajodia., steganalysis: the investigation of hidden information, IEEE Information Technology Conference, Syracuse, New York, USA, 1998, pp. 113-116.

[10] Guorong Xuan, Jianjiong Gao, Shi, Y.Q., and Zou, D., Image steganalysis Based on Statistical Image Moments of Wavelet Sub band Histograms in DFT Domain, IEEE 7th International Workshop on Multimedia Signal Processing, Shanghai, China, 2005, pp.1-4.

[11] Chen, C., Shi, Y. Q., Chen, W., and Xuan, G., Statistical Moments Based Universal steganalysis using JPEG 2-D Array and 2-D Characteristic Function, IEEE International Conference on Image Processing, 2006, pp. 105–108.

[12] Ryan Benton, and Henry Chu, Soft Computing Approach to steganalysis of LSB Embedding in Digital Images, Third International Conference on Information Technology: Research and Education, ITRE, 2005, pp. 105-109.

[13] Mei-Ching Chen, Agaian, S.S., Chen, C.L.P., and Rodriguez, B.M., steganalysis detection using RBFNN, International Conference on Machine Learning and Cybernetics, 2008, Vol. 7, pp. 3720-3725.

[14] Qingzhong Liu, Andrew Sung, H., Jianyun Xu, and Bernardete Ribeiro, M., Image Complexity and Feature Extraction for steganalysis of LSB Matching steganalysis, 18th International Conference on Pattern Recognition, 2006, Vol. 2, pp. 267-270.

[15] Yuan Liu, Li Huang, Ping Wang, and Guodong Wang, A blind image steganalysis based on features from three domains, Proceedings of Control and Decision Conference (CCDC), 2008, pp. 2933-2936.

[16] Muhanna, M., Turabieh, H., Aljarrah, O., and Elsayad., A steganalysis of LSB Encoding in Digital Images Using GLCM and Neural Networks, Proceedings of the 3rd International Conference on Informatics and Systems (INFOS2005), Cairo, Egypt, 2005, Vol. 14, pp. 31-37.

[17] Ying Wang, and Pierre Moulin, Optimized Feature Extraction for Learning-Based Image steganalysis, IEEE Transactions on Information Forensics and Security, 2007, Vol. 2, No. 1, pp. 31-45.

[18] Ferreira, R., Ribeiro, B., Silva, C., and Qingzhong Liu Sung, A.H., Building resilient classifiers for LSB matching steganalysis, IEEE International Joint Conference on Neural Networks (IJCNN), 2008, pp. 1562-1567.

[19] Xiongfei He, Fenlin Liu, Xiangyang Luo, and Chunfang Yang, Classification between PS and stego images Based on Noise Model, 3rd International Conference on Multimedia and Ubiquitous Engineering, 2009, pp. 31-36.

[20] Malekmohamadi, H., and Ghaemmaghami, S., Reduced complexity enhancement of steganalysis of LSB-matching image steganalysis, IEEE/ACS International Conference on Computer Systems and Applications, 2009, pp. 1013-1017.

[21] Lingna Hu, Lingge Jiang, and Chen He, A novel steganalysis of LSB matching based on kernel FDA in grayscale images, International Conference on Neural Networks and Signal Processing, 2008, pp. 556-559.

[22] Martin, A., Sapiro, G., and Seroussi, G., Is image steganalysis natural? , IEEE Transactions on Image Processing, 2005, Vol. 14, No. 12, pp. 2040-2050.

[23] Yuan Liu, Li Huang, Ping Wang, and Guodong Wang, A blind image steganalysis based on features from three domains, Proceedings of Control and Decision Conference (CCDC), 2008, pp. 2933-2936.

[24] Ziwen Sun, Hui Li, Zhijian Wu, and Zhiping Zhou, An Image steganalysis Method Based on Characteristic Function Moments of Wavelet Sub bands, International Conference on Artificial Intelligence and Computational Intelligence, 2009, Vol. 1, pp. 291-295.

[25] Chandramouli, R., and Subbalakshmi, K.P., Active steganalysis of Spread Spectrum image steganalysis, Proceedings of International Symposium on Circuits and Systems, ISCAS, 2003, Vol. 3, pp. 830-833.

[26] Shaohui Liu, Lin Ma, Hongxun Yao, and Debin Zhao, Universal steganalysis Based on Statistical Models Using Reorganization of Block-based DCT Coefficients, 5th International Conference on Information Assurance and Security, 2009, Vol. 1, pp. 778-781.

[27] Daniel Lerch-Hostalot, and David Meg´ıas, Steganalytic Methods for the Detection of Histogram Shifting Data Hiding Schemes, Proceedings of Reunión Española Cryptology and Information Security (RECSI), 2012.

[28] Chandramouli, R., A mathematical framework for active steganalysis, ACM Multimedia Systems, 2003, Vol. 9, No. 3, pp. 303-311.

[29] Ming Jiang, Edward Wong, Nasir Memon, and Xiaolin Wu, A simple Technique for Estimating Message Lengths for Additive Noise steganalysis, 8th International Conference on Control, Automation, Robotics and Vision (ICARCV), Kunming, China, 2004, pp. 983-986.

[30] Xiangyang Luo, Fenlin Liu, and Han Zong, A wavelet-based blind JPEG image steganalysis using co-occurrence matrix, 11th International Conference on Advanced Communication Technology (ICACT), 2009, Vol. 3, pp. 1933-1936.

[31] Sambasiva Rao Baragada, Ramakrishna S., Rao M.S., and Purushothaman S., Polynomial Discriminant Radial Basis Function for Steganalysis, International Journal of Computer Science and Network Security, IJCSNS, 2009, Vol. 9, No. 2, pp. 209-218.

[32] Han Zong, Fenlin Liu, and Xiangyang Luo, A wavelet-based blind JPEG image steganalysis using co-occurrence matrix, 11th International Conference on Advanced Communication Technology (ICACT), 2009, Vol. 3, pp. 1933-1936.

[33] Yuan-lu Tu, and Sheng- rong Gong, Universal steganalysis Using Color Correlation and Feature Fusion, International Symposium on Information Science and Engineering, ISISE'08, 2008, Vol. 1, pp. 107 - 111.

[34] Jennifer Davidson, Clifford Bergman, and Eric Bartlett, An Artificial Neural Network for wavelet steganalysis, Proceedings of SPIE, 2005, Vol. 5916, pp. 1-10.

[35] Jacob Jackson, T., Gregg Gunsch, H., Roger Claypoole, L., Jr, and Gary Lamont, B., Blind steganalysis Detection Using a Computational Immune System: A Work in Progress, International Journal of Digital Evidence, 2003, Vol. 4, No. 1, pp. 1-19.

[36] Patricia Lafferty, and Farid Ahmed, Texture based steganalysis: results for color images, Proceedings of SPIE, 2004, Vol. 5561, pp. 145-151.

[37] Shi, Y.Q., Guorong Xuan, Zou, D., Jianjiong Gao, Chengyun Yang, Zhenping Zhang, Peiqi Chai, Chen, W., and Chen, C., Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network, IEEE International Conference on Multimedia and Expo, ICME, 2005, pp.1-4.

[38] Liu Shaohui, Yao Hongxun, and Gao Wen, Neural Network Based steganalysis in Still Images, Proceedings of International Conference on Multimedia and EXPO, 2003, Vol. 2, pp. 509-512.

[39] Xiangyang Luo, Fenlin Liu, Jianming Chen, and Yining Zhang, Image universal steganalysis based on wavelet packet transform, IEEE 10th Workshop on Multimedia Signal Processing, 2008, pp. 780 - 784.

Dr.P. Sujatha completed Ph.D from Vels University in 2013. Her specialization is Image Processing and Artificial Neural Network. Presently 5 research scholars are with her. She has Published 6 International Journals. She has presented papers in 5 International Conferences and 10 National Conferences. She has 15 years of teaching experience. Currently she is working as Associate Professor, School of Computing sciences, Vels University, Chennai.