Polynomial Vector Discriminant Back Propagation Algorithm Neural Network for Steganalysis

Sambasiva Rao Baragada

Dept. of Computer Science
Sri Venkateswara University
Tirupati, 517502, India

S. Ramakrishna

Dept. of Computer Science
Sri Venkateswara University Tirupati,
Tirupati, 517502, India

M. S. Rao

Director cum Chief Forensic Scientist
Directorate of Forensic Science
Ministry of Home Affairs
New Delhi, 110003, India

S. Purushothaman

Sun college of Engineering and Technology
Nagerkoil, INDIA

Summary
Machine learning based steganalysis assume no information about stego image, host image, and the secret message. Many techniques have been proposed and new techniques are tried with different combinations to maximize the efficiency of retrieving hidden information. We have proposed a combination of polynomial preprocessed vector discriminant (PVD) with back propagation algorithm (BPA) neural network for steganalysis. Each set of pixel is preprocessed to obtain interpolated pixels to produce patterns using PVD. This is further trained by proposed neural network, adopted to obtain set of final weights. During implementation, the final weights are used to classify the presence of hidden information.
Key words: *Polynomial vector, bitplane, Steganalysis.*

1. Introduction

Steganography is the art of concealing and sending messages; it has been around as long as people have had secret information to relay. This practice has come a long way since the days encrypted Morse code delivered over secret radio frequencies. Computers and the World Wide Web provide a new twist on this covert activity. Today's digital cameras produce high-quality images, and the Internet easily and inexpensively carries enormous volumes of information worldwide. Some illegal uses of steganography could be: Criminal Communications, fraud, hacking, electronic payments, gambling, pornography, and harassment. Steganalysis is the process of detecting the presence of hidden information in a text, image, audio, or video [1,2,3]. It has been noticed that the present literature on steganalysis is broadly categorized as supervised learning model, parametric model [10, 11, 12], blind model [4, 5, 6, 7, 8, 9, 19-25] and hybrid model [29]. A generic steganalysis method that can attack steganography blindly, detect hidden data without knowing embedding methods, will be more useful in practical applications. Farid et al in [13] has been designed a frame work for steganalysis based on supervised learning. The framework was further developed and tested many researchers. Our proposed work belongs to supervised learning based steganalysis, because of two advantages, i) abundant work has been available on supervised learning methodologies ii) supervised learning competes in giving promising results when compared with other models. However the selection of patterns as input to the neural network is the major art to be performed. Significant work has been carried out on supervised steganalysis, using neural networks as a classifier [14, 15, 26-32]. Polynomial processed vector has shown impressive results for steganalysis work in [18]. We tried to present another combination of polynomial vector discriminant with back propagation algorithm neural network.

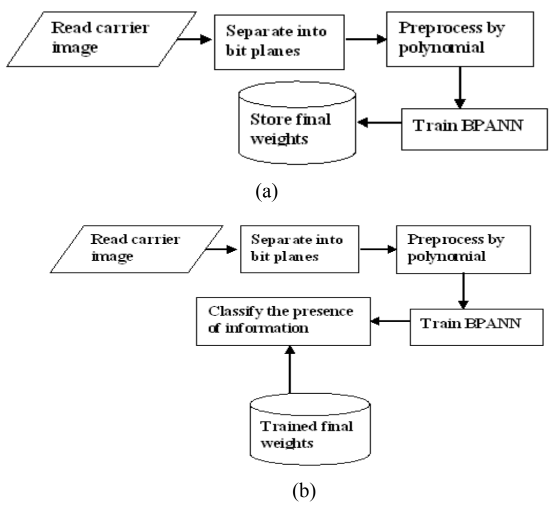

Fig. 1 a) Flowchart for training, b) flowchart for testing

Manuscript received May 5, 2010
Manuscript revised May 20, 2010

2. Methodology

As we have stated earlier, our work falls under the category of supervised learning employing two phase strategies: a) training phase and b) testing phase. In training phase, original carriers are separated by bitplane method and are interpolated by preprocessing into polynomial vectors. This is further trained by back propagation neural classifier to learn the nature of the images. By training the classifier for a specific embedding algorithm a reasonably accurate detection can be achieved. BPA neural classifier in this work learns a model by averaging over the multiple examples which include both stego and non-stego images. In testing phase, unknown images are supplied to the trained classifier to decide whether secret information is present or not. The flowcharts of both the phases are given below in figure 1.

2.1 Bitplane processing

In this research work 256-color or 8-bit images are considered. Each image is split into 8 planes, each plane contains one bit of all the pixels.

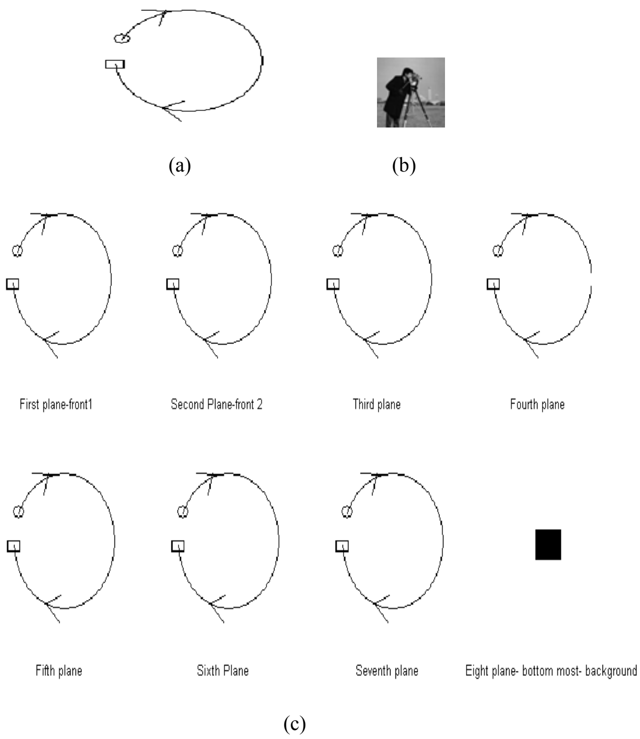

Fig. 2 a)Carrier Image b) Message Image c) The mixed image

2.2 Normalization of patterns

The patterns are normalized 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:

$$x_i = x_i / x_{max} \tag{1}$$

where,

x_i is the value of a feature, and

x_{max} is the maximum value of the feature.

2.3 Selection of patterns for training

The number of classes, which are based on the classification range of the outputs, are decided. If only one output is considered, the range of classification is simple. If more than one output is considered, a combination criterion has to be considered. The total number of patterns is decided for each class. Out of these patterns, the number of patterns to be used for training the network is decided. The remaining patterns are used for testing the classification performance of the network. The patterns selected for training the network should be such that they

$$E_i^2 = \frac{\sum_{j=1}^{nf} (x_{ij} - \bar{x}_j)^2}{\sigma_i^2}$$

represent the entire population of the data. The selection of patterns is done by:

(2)

where,

$$\sigma_i^2 = \frac{\sum_{j=1}^{nf} (x_{ij} - \bar{x}_j)^2}{L}$$

E_i^2 is the maximum variance of a pattern,
nf is the number of features, and

(3)

where the value of E_i^2 is found for each pattern. Patterns with maximum E_i^2 are chosen from each class for training the network. For each pattern target outputs are defined, so that during training, supervised algorithms can be used and during testing, the required output can be obtained by giving inputs. The total variance found by using equation

(2) is categorized to know whether the patterns are similar to eliminate redundant patterns. Redundancy is identified if patterns total variance is less than particular range when any one of the pattern alone is considered.

$\bar{x}_j$ is the mean for each feature, and

L is the number of patterns

2.2 Polynomial Interpretation

Polynomial interpolation is the interpolation of a given pattern set by a polynomial set obtained by outer producting the given pattern. It can also be described as, given some points, the aim is to find a polynomial which goes exactly through these points [16, 17]. Polynomial Interpolation forms the basis for computing information between two points.

Let X present the normalized input vector, where $X = \{X_i\}$; i=1,…nf,

X_i is the feature of the input vector, and
nf is the number of features

An outer product matrix X_{OP} of the original input vector is formed, and it is given by:

$$Xop.. = .. \begin{bmatrix} X1X1 & X1X2 & X1X3 \\ X2X1 & X2X2 & X2X3 \\ X3X1 & X3X2 & X3X3 \end{bmatrix}$$

Using the X_{OP} matrix, the following polynomials are generated:

i) Product of inputs (NL1)
it is denoted by:

$\Sigma w_{ij} x_i$ $(i \neq j)$ = Off-diagonal elements of the outer product matrix. (4)
The pre-processed input vector is a 3-dimensional vector.

ii) Quadratic terms (NL2)
It is denoted by:

$\Sigma w_{ij} x_i^2$ = Diagonal elements of the outer product matrix. (5)
The pre-processed input vector is a 3-dimensional vector.

iii) A combination of product of inputs and quadratic terms (NL3)

It is denoted by:

$\Sigma w_{ij} x^i (i \neq j) + \Sigma w_{ij} x_i^2$ = Diagonal elements and Off-diagonal elements of the outer product matrix. (6)

The pre-processed input vector is a 6 dimensional vector.

iv) Linear plus NL1 (NL4)
The pre-processed input vector is a 6-dimensional vector. (7)

v) Linear plus NL2 (NL5)
The pre-processed input vector is a 6-dimensional vector. (8)

vi) Linear plus NL3 (NL6) (9)
The pre-processed input vector is a 9-dimensional vector.

In Eq. (4) through Eq. (9), the term 'linear' represents the normalized input pattern without pre-processing. While training the BPA, anyone of the 6 polynomial vectors can be used as input depending upon the requirements. The abbreviation 'NL' represents the non-linearity. The number next to 'NL' is used to identify the type of polynomial generated. The combination of different polynomials with BPA is given. in table 1.

NL1+BPA	NL2+BPA
NL3+BPA	NL4+BPA
NL5+BPA	NL6+BPA

Table 1: Combination of PVDBPA

2.4 Back Propagation Algorithm Neural Network

The Back Propagation Algorithm Neural Network uses the steepest-descent method to reach a global minimum. The number of layers and number of nodes in the hidden layers are decided. The connections between nodes are initialized with random weights. Preprocessed vectors are presented in the input layer of the network and the error at the output layer is calculated. The error is propagated backwards towards the input layer and the weights are updated. This procedure is repeated for all the training patterns. This forms one-iteration. At the end of each iteration, test patterns are presented to neural network, and the prediction performance of network is evaluated. Further training of ANN is continued till the desired prediction performance is reached. The flowchart for PVDBPA is given in figure 3.

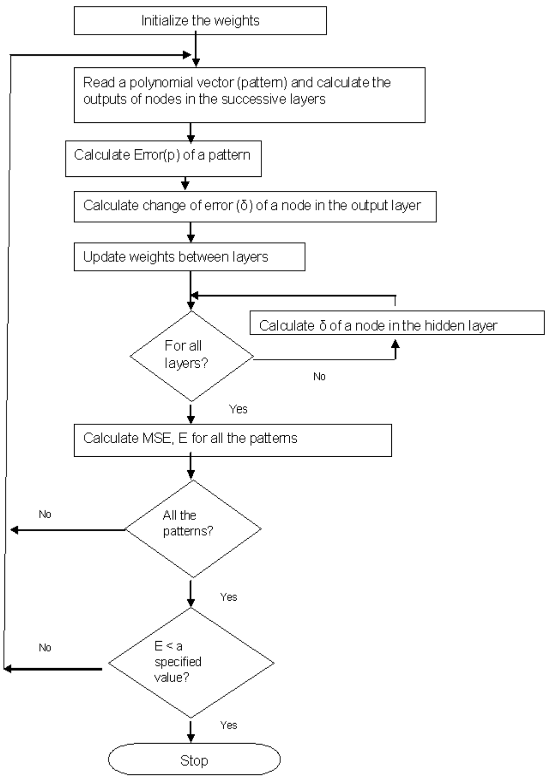

Fig.3 Flowchart of PVDBPA

Fig.4 Three cover images under consideration

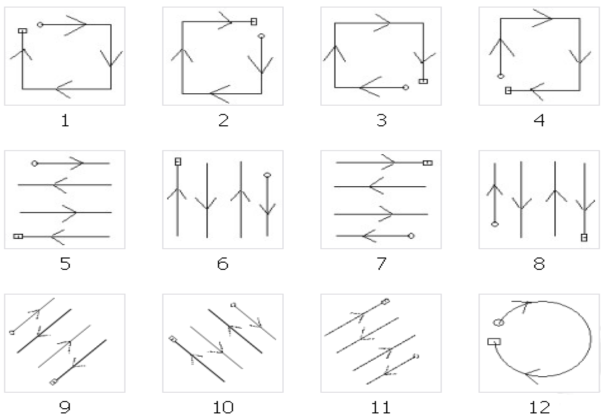

Fig.5 Distribution of information image in cover image

Size of the image	256 * 256
Number of bits in each pixel of the cover image considered	4 bits (background)
Number of bits preferred in each message image	4bits (foreground)
Method of embedding	replacing all the background four bits of cover image by four information bits (foreground) of message image or replacing any one bit or any two bits or any three bits of cover image with equal number of bits of message image

Table 2: Simulation environment

Method	Polynomial vector length
NL1	36
NL2	9
NL3	45
NL4	45
NL5	18
NL6	54

Table 3: Polynomial vector

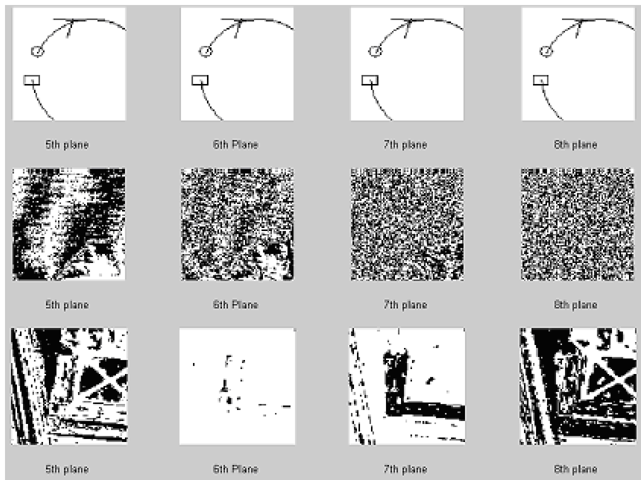

Fig 6. Each row corresponds to one image – background bits are shown

3. Results and Discussion

The numerical values in the patterns play important role in proper classification. This is possible only if the patterns are orthonormal. Either the patterns can be converted into orthonormal or the patterns can be converted into a polynomial surface. This is achieved, by forming a matrix for each pattern and considering diagonal values, or off-diagonal values or combination of diagonal and off diagonal values. By this way, the dimension of each pattern increases to form a polynomial surface. Due to conversion of patterns into polynomial surface, convergence is achieved in 2 to 3 iterations with higher percentage of identification.

Training of the network with different learning factor has been tried and finally a value learning factor with 1 has been chosen. This indicates a standard convergence. If any other values are chosen then convergence is faster, however, the convergence gets stuck up into local minima. If the data is not normalized properly, then it takes huge iterations to converge. Identifying the correct way of normalizing the data itself was a challenging task. In fact, two types of normalizing have been tried. One method involves in finding the maximum values for each feature and dividing the remaining values with the maximum value. By this process, the values lie in the range of 0 to 1. There is another method that has been tried. In this method, 4 features of a pattern have been considered at a time, each summation of square of all features is found. Each feature is then divided by the square root of the summed value. This process shows the link among the features, however, the former way of normalizing is considered. The convergence time taken in each method is totally different. In this work finally, normalizing with maximum value has been considered.

In this simulation, Least Significant Bit (LSB), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transformation (DFT) encoding schemes are considered for the experimental work. Some of cover images considered in the simulation is presented in figure 4. The information image is shown in figure 2 (b). Encryption technique has not been considered during the simulation. Some possible ways the secret information scattered in the cover images are given in figure 5. Bits corresponding to background are shown in figure 6. The simulation environment is given in table-2. The number of iterations taken for training is shown in figure 7. Randomly selected one untrained image is tested with the network. The detection of the message for the same image is shown in figure 8. Table 3 gives the lengths of polynomial vectors developed during preprocess. The computational effort taken by the proposed method has been shown in table 4. The proposed combinations are able to identify the hidden information.

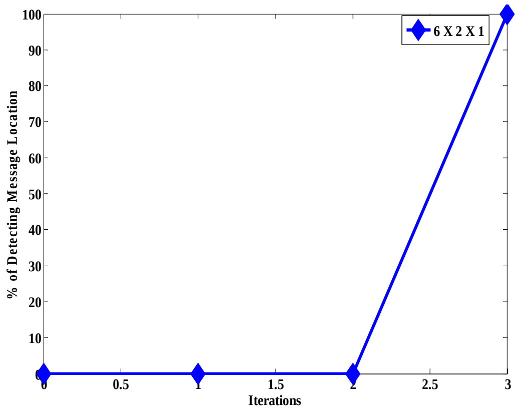

Fig 7a. Iterations vs %detection, BPA+NL1

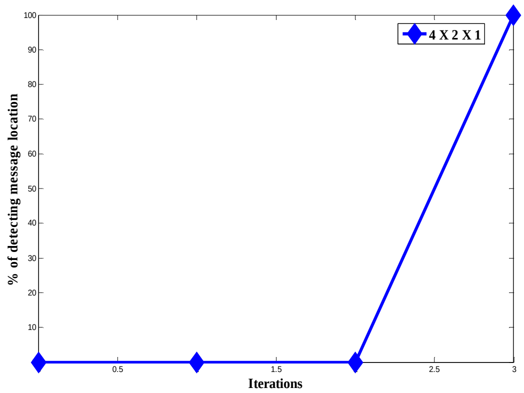

Fig 7b. Iterations vs %detection, BPA+NL2

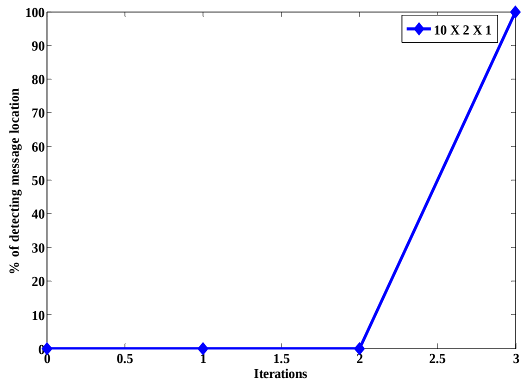

Fig 7c. Iterations vs %detection, BPA+NL3

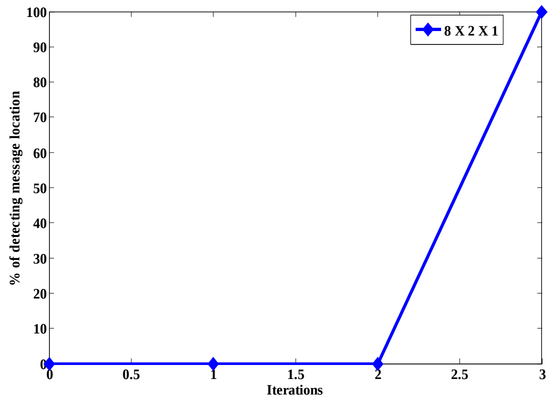

Fig 7d. Iterations vs %detection, BPA+NL4

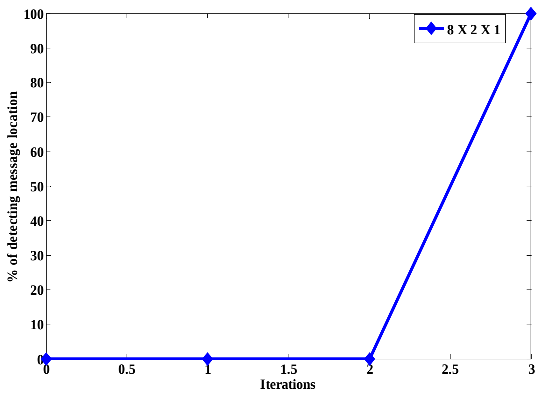

Fig 7e. Iterations vs %detection, BPA+NL5

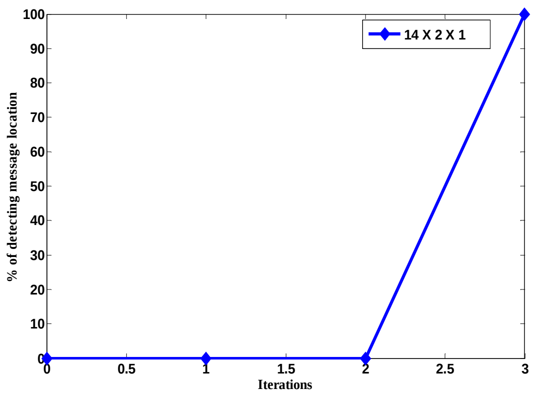

Fig 7f. Iterations vs %detection, BPA+NL6

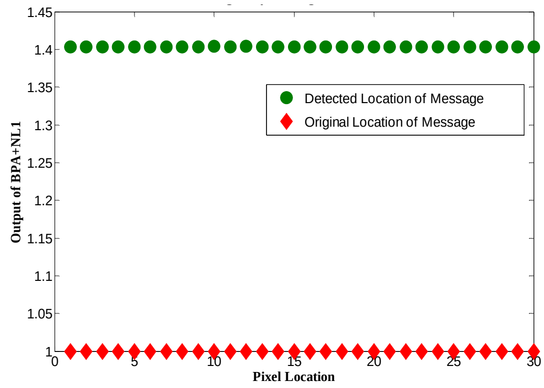

Fig 8a. Message detection, BPA+NL1

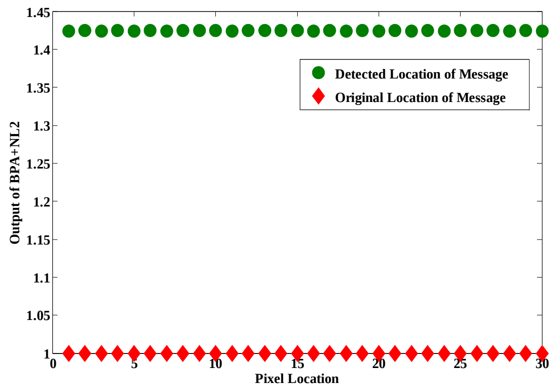

Fig 8b. Message detection, BPA+NL2

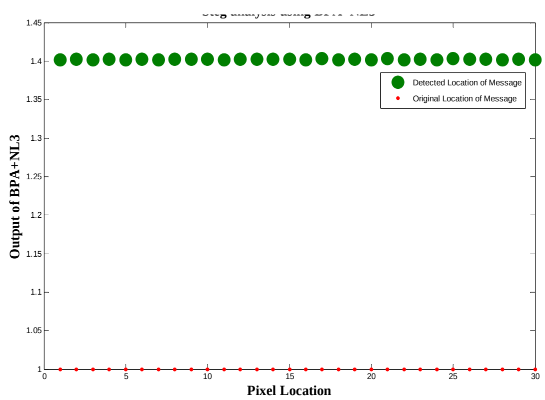

Fig 8c. Message detection, BPA+NL3

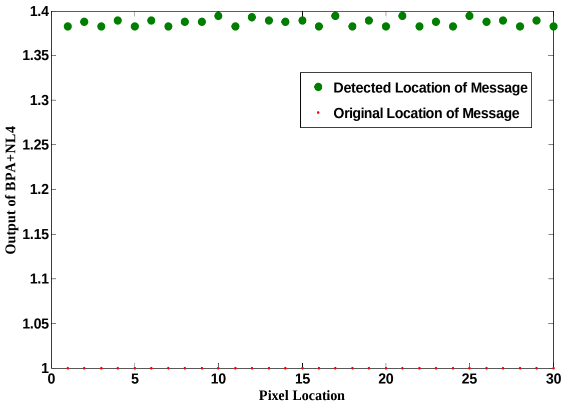

Fig 8d. Message detection, BPA+NL4

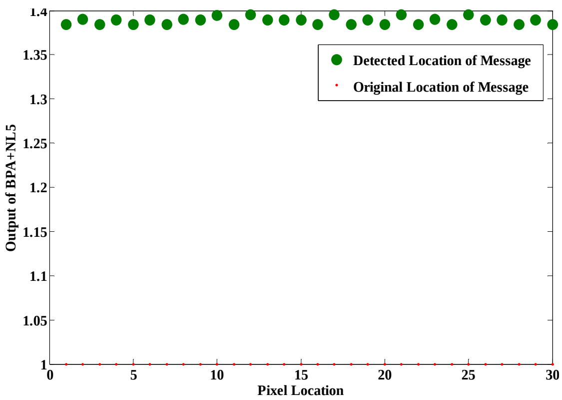

Fig 8e. Message detection, BPA+NL5

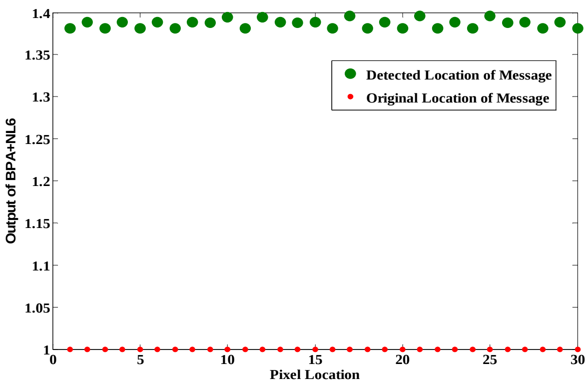

Fig 8f. Message detection, BPA+NL6

4. Conclusion

Steganalysis has been implemented using preprocessed vector with BPA. The outputs of the algorithms for one steganographed image have been presented. Secret information is getting retrieved by the proposed algorithms with various degrees of accuracies. It can be noticed that the combined method PVDBPA is giving a newer direction to detecting the presence of hidden information. The cover images chosen for the simulation are standard images taken from Matlab7.1. BPA was trained on 1024 images of group 1 (no hidden message), and 512 images of group 2 (hidden message). Then, patterns from 256 untrained images were computed and given as input to BPA for testing. The work produced a positive classification of 95% and 5% of misclassification. As there are numerous algorithms that have been developed for steganalysis, few more algorithms based on requirements can be verified with the collected images.

No	Algorithm	No. of nodes IL (HL)	No. of iterations	MSE	Effort pattern / iteration
1	BPA	2(2)	6	0.00081121604667	111
2	BPA + NL1	6(2)	3	0.33415400093	295
3	BPA + NL2	4(2)	3	0.347946724346	203
4	BPA + NL3	10(2)	3	0.333474113642	479
5	BPA + NL4	8(2)	3	0.325764541307	387
6	BPA + NL5	8(2)	3	0.326399266719	387
7	BPA + NL6	14(2)	3	0.325624200935	663

Table 4: Computational effort required for per pattern/iteration

5. Acknowledgements

We express our sincere thanks to Shri Mohinder Singh, GEQD, Hyderabad, for his valuable encouragement in our research work. We also express our heartful thanks to Mr. P. Krishna Sastry and Mr. M. Krishna, for their outstanding technical support in doing experiments at Computer Forensic Division, GEQD, Directorate of Forensic Science, Ministry of Home Affairs, Govt. of India, Hyderabad.

6. References

[1] Simmons, G. J., “The Prisoners’ Problem and the Subliminal Channel,” CRYPTO83, Advances in Cryptology, August 22-24, pp. 51 – 67, 1984.
[2] R. J. Anderson and F.A.P Petitcolas, “On the limits of steganography,” IEEE Journal on Selected Areas in Communications, vol. 16 no. 4, pp. 474 -484, 1998.
[3] N.Johnson and J. Sklansky, “Exploring steganography: seeing the unseen,” IEEE Computer, pp. 26 – 34, 1998.
[4] Shalin Trivedi and R. Chandramouli, “Secret Key Estimation in Sequential Steganography,” IEEE Trans. on

Signal Proc., vol. 53, no. 2, pp. 746 - 757, February 2005.

[5] J. Harmsen and W. Pearlman, "Steganalysis of additive noise modelable information hiding," Proc. SPIE Electronic Imaging, 2003.

[6] N. Provos and P. Honeyman, "Detecting steganographic content on the internet," CITI Technical Report 01-11, August, 2001.

[7] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," Third Information Hiding Workshop, September. 1999.

[8] Zugen Liu, Xuezeng Pan, Lie Shi, Jimin Wang, Lingdi Ping, "Effective steganalysis based on statistical moments of differential characteristic function," International Conference on Computational Intelligence and Security, vol. 2, pp. 1195 – 1198, November 2006.

[9] Liang Sun, Chong-Zhao Han, Ning Dai, Jian-Jing Shen, "Feature Selection Based on Bhattacharyya Distance: A Generalized Rough Set Method," Sixth World Congress on Intelligent Control and Automation, WCICA, vol. 2, pp. 101-105, June, 2006.

[10] S. Lyu and H. Farid, "Steganalysis Using Color Wavelet Statistics and One-Class Support Vector Machines," SPIE Symposium on Electronic Imaging, San Jose, CA, 2004.

[11] J. Fridrich, R. Du, and M. Long, "Steganalysis of lsb encoding in color images," IEEE ICME, vol. 3, pp. 1279 – 1282, March 2000.

[12] R. Chandramouli, "A mathematical framework for active steganalysis," ACM Multimedia Systems, vol, 9, no.3, pp.303 – 311, September 2003.

[13] H. Farid, "Detecting hidden messages using higher-order statistical models," Proc. IEEE Int. Conf. Image Processing, New York, pp.905- 908, Sep. 2002.

[14] Shi, Y.Q, Guorong Xuan, Zou, D, Jianjiong Gao, Chengyun Yang, Zhenping Zhang, Peiqi Chai, Chen, W, 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 , July 2005.

[15] 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, pp. 105 – 109, June 2005.

[16] Kendell A. Atkinson (1988). An Introduction to Numerical Analysis (2nd ed.), Chapter 3. John Wiley and Sons.

[17] L. Brutman (1997), Lebesgue functions for polynomial interpolation — a survey, Ann. Numer. Math. 4, 111–127.

[18] Sambasiva Rao. Baragada, S. Ramakrishna, M.S. Rao, S. Purushothaman, "Polynomial Discriminant Radial Basis Function for Steganalysis", International Journal of Computer Science and Network Security, Vol. 9, Issue 2, pp. 209 – 218, February 2009.

[19] Gul G, Kurugollu F,"SVD Based Universal Spatial Domain Image Steganalysis", IEEE Transactions on Information Forensics and Security, Vol. 5, No.1, February 2010.

[20] Zhuo Li; Kuijun Lu; Xianting Zeng; Xuezeng Pan, "Feature-Based Steganalysis for JPEG Images", International Conference on Digital Image Processing, pp. 76–80, Thailand, 2009.

[21] Xiao Yi Yu, Aiming Wang, "An Investigation of Genetic Algorithm on Steganalysis Techniques", 5th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 1118–1121, Kyoto, September 2009.

[22] Xue Zhang, Shang-Ping Zhong, "Blind steganalysis method for BMP images based on statistical MWCF and F-score method", International Conference on Wavelet Analysis and Pattern Recognition", pp. 442–447, Baoding, July 2009.

[23] Xiao Yi Yu, Aiming Wang, "Steganalysis Based on Bayesion Network and Genetic Algorithm", International Conference on Image and Signal Processing", pp. 1–4, Tianjin, October 2009.

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

[25] Xiongfei He, Fenlin Liu, Xiangyang Luo, Chunfang Yang, "Classification between PS and Stego Images Based on Noise Model", 3rd International Conference on Multimedia and Ubiquitous Engineering, pp. 31–36, June 2009.

[26] Ziwen Sun, Hui Li, Zhijian Wu, Zhiping Zhou, "An Image Steganalysis Method Based on Characteristic Function Moments of Wavelet Subbands", International Conference on Artificial Intelligence and Computational Intelligence, Vol. 1, pp. 291–295, November 2009.

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

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

[29] Yuan Liu, Li Huang, Ping Wang, Guodong Wang, "A blind image steganalysis based on features from three domains", Proc. of Control and Decision Conference (CCDC), pp. 613–615, China, July 2008.

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

[31] Ferreira, R. Ribeiro, B. Silva, C. Qingzhong Liu Sung, A.H, "Building resilient classifiers for LSB matching steganography", IEEE International Joint Conference on Neural Networks (IJCNN), pp. 1562–1567, Hong Kong, June 2008.

[32] Sambasiva Rao. Baragada, S. Ramakrishna, M.S. Rao, S. Purushothaman, "Implementation of Radial Basis Function Neural Network for Image Steganalysis", International Journal of Computer Science and Security, Vol. 2, Issue 1, pp. 12 – 22, February 2008.

Sambasiva Rao Baragada received his B.Sc and M.Sc degrees in Computer Science from Acharya Nagarjuna University in 1999 and 2001 respectively. He completed his M.Phil in Computer Science from Alagappa University in 2006. He has published two research papers in International Journals. Currently he is pursuing his Ph.D degree in Computer Science under the guidance of Prof. S. Ramakrishna, Sri Venkateswara University, Tirupati. His area of research includes Artificial Intelligence, Neural Networks, Computer Forensics, Steganography and Steganalysis.

Dr S. Ramakrishna is working as Professor in the Department of Computer Science at Sri Venkateswara University, Tirupati, India. He received his M.Tech. from Punjabi University, and Ph.D. from Sri Venkateswara University, Tirupati. He published more than 30 research papers in national and international journals. His area of research includes Artificial Intelligence, Neural Networks, Computer Forensics, Steganography and Steganalysis.

Dr. M S Rao, Former Chief Forensic Scientist to Govt. of India is a well known forensic scientist of the country and started his career in Forensic Science in the year 1975 from Orissa Forensic Science Laboratory. Dr. Rao is steering the Ph.D work of research scholars in the areas of computer forensics and forensic ballistics. He published more than 40 research papers in national and international journals.

Dr. S. Purushothaman is working as professor in Sun College of Engineering, Nagerkoil, India. He received his Ph.D from IIT Madras. His area of research includes Artificial Neural Networks, Image Processing and signal processing. He published more than 20 research papers in national and international journals.