Computational Complexity Evaluation of ANN Algorithms for Image Steganalysis

Dr.P.Sujatha
Assistant Professor, Department of Computer Science
Vels University, Chennai, India.

Dr.S.Purushothaman
Professor, PET Engineering college, Vallioor – 627 117
Tirunelveli Dt., India,

P.Rajeswari
Research Scholar, Mother Therasa University
Kodaikanal, India,

Abstract - The major growth of information technology is based on the way how the security measures are implemented. Steganography is a technique that implements high level security by hiding a message in a multimedia object such as image. Steganalysis is the way of detecting such hidden messages. In order to detect the presence of hidden message, artificial neural network algorithms such as Back Propagation and Radial Basis Function are used. This paper performs the computational complexity evaluation of these two algorithms.

Keywords - Covert communication, Steganography, Steganalysis, ANN, Back Propagation, Radial Basis Function

I. INTRODUCTION

In today's digital age, there are more chances for altering the information represented by an image without leaving any traces of tampering. Many areas such as forensics investigation, surveillance systems, criminal investigation, medical imaging, journalism and intelligence services need reliability while transferring the information in the form of an image. Planning is the crucial part and the information planning is passed to others through covert communication in order to hide from government and other people. The effective medium of hidden communication is achieved by steganography. An article (Jack [11]) ensured that terrorists used steganography for secret communication during 11th September 2001 attack.

Politicians use steganography communication to express their political thoughts that are more sensitive to the world. The Government can take action on any politician who involves in sensitive issue like decreasing the economical growth of the country. The ease of Internet helps in both good and bad usage. Downloading various tools for steganography becomes a challenging task for government to trace the law breakers. The majorities of documents used in publishing industry were digital documents with foreground (black) and background (White) binary values. Multiple documents are manipulated everyday with binary values. Those documents are scanned and used as a medium of steganography. Variety of data embedding algorithms and variety of images that makes the steganography a toughest mission for researchers to develop a powerful technique for steganalysis.

II. IMAGE STEGANALYSIS

The counter-technique of image steganography is known as image steganalysis. Steganalysis begins by identifying the artifacts that exist in the suspectable file which is a result of message embedding. The goal is not to advocate the removal or disabling of valid hidden information such as copyrights, but to point out approaches that are vulnerable and may be exploited to investigate illicit hidden information (Anderson et al. [1]; Johnson et al. [2]; Neil et al. [7]; Rajarathnam et al. [9]). Attacks and analysis on hidden information may take several forms like detecting, extracting, and disabling or destroying hidden information (Westfeld et al. [3]). An attacker may also embed counter-information over the existing hidden information. These approaches vary depending upon the methods used to embed the information into the cover media.

A. Steganalysis Methods

Based on the way of detecting the presence of hidden message, steganalysis methods are divided as follows.

i) Statistical steganalysis
   a) Spatial domain
   b) Transform domain
ii) Feature based steganalysis

Statistical Steganalysis:

Existence of the hidden message is detected using statistical analysis that is done with the pixels. It is further classified as spatial domain steganalysis and transform domain steganalysis. In spatial domain, the pair of pixels is considered and the difference between them is calculated. In transform domain, frequency counts of coefficients are calculated and then histogram analysis is performed.

Feature based steganalysis:

The features of the image are used to detect hidden message in an image. They can also be used to train classifiers.

III. RELATED WORKS

Fridrich [5] developed a steganalytic technique that detects 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. With the help of relative frequencies of these groups in the given image along with an image obtained from the original image with LSBs flipped and with an image obtained by randomizing LSBs of the original image, they try to predict the levels of embedding.

Fridrich [8] proposed Pairs analysis method. This approach is well suited for the embedding archetype that randomly embeds messages in LSBs of indices to palette colors of palette image.

Westfeld [4] used visual attacks to detect the steganography by making use of the ability of human eyes to inspect the images for the corruption caused by the embedding.

Martin [6] attempts to directly use the notion of the naturalness of images to detect hidden data. Though they found that data hidden certainly caused shifts from the natural set, knowledge of the specific data hiding scheme provides far better detection performance.

IV. PROPOSED ALGORITHM

Apart from all modern sciences and technologies, Artificial Neural Network (ANN) plays a vital role in capturing and representing both linear and non-linear relationships. ANN is an intelligent system which helps to enable machines to solve problems like human by extracting and storing the knowledge. To incorporate intelligent method for steganalysis, this paper focuses ANN to overcome the drawbacks of the conventional steganalysis methods. The proposed methods are,

- Back Propagation Algorithm (BPA)
- Radial Basis Function (RBF)

A. Implementation of BPA:

The BPA 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. A pattern from the training set is presented in the input layer of the network and the error at the output layer is calculated. The error is propagated backward towards the input layer and the weights are updated. At the end of each iteration, test patterns are presented to ANN, and the prediction performance of ANN is evaluated. Further training of ANN is continued till the desired prediction performance is reached.

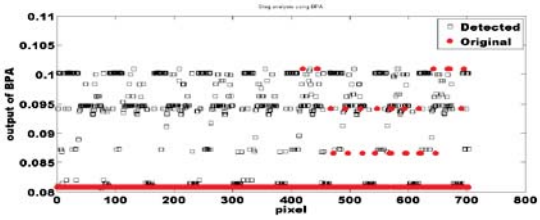


Figure 1. Detection of location of message by BPA

In Figure 1, "● Original" refers to the actual information of the image. "□ Detected" information indicates that the suspect image is a stegnographic image.

B. Implementation of RBF:

Every function can be uniquely identified by its inherent properties, and this makes a form of Φ suitable in approximation to one problem or a particular class of problems. The selection of position and the number of centers is similar to problems choosing the number and initial values of the weights in a multilayer perceptron (MLP). A best approximation can be produced when optimal number of centers is identified. Neither very few nor many centers should be chosen, since this may lead to poor approximation. It is very important to maintain equilibrium between the number of centers and the amount of training data.

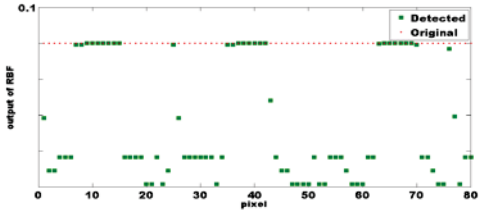


Figure 2. Detection of Message location using RBF

In the above figure, the detected information is represented by '■'. The pixels in cover image are represented by '●'.

IV. COMPARISON OF PERFORMANCES

A. Computational Complexity

The computational complexity of an algorithm is defined as the number of arithmetic operations required for training the proposed algorithm. The performance comparison of modified ANN algorithm (Vu et al. [10]) is studied for. Empirical formulae for computational effort are presented for BPA and RBF in Table 1.

Table 1. Computational Complexity Evaluation

Algorithm	**Formula for evaluating the number of arthmetic computation**
BPA	Forward computational effort in BPA for one pattern is given by $2\sum_{i=1}^{L-1} n_{i+1}(n_i+1)$ **(1.1)** Reverse computational effort in BPA for one pattern is given by $9n_L + 7\sum_{i=1}^{L-1} n_i n_{i-1} + \sum_{i=L-1}^{2}(4n_i+5)n_{i-1}$ **(1.2)** TCE for BPA= $\{(ite)\, a_o\}\, n_p$ **(1.3)**

RBF	TCE for RBF = $\{2n_c^2 + inv(n_c^2)\, n_c^2\}\ n_p$ **(1.4)**
	where: TCE Total computational effort, n_c is number of centers+1(bias) , n_p is number of training patterns, inv is inbuilt function inverse of a matrix, ite is the number of iteration a_o is {Forward computation in BPA + Reverse computation in BPA} L is the total number of layers including the input layer, 'i' is the layer number, and (n_i) is the number of nodes in the i^{th} layer

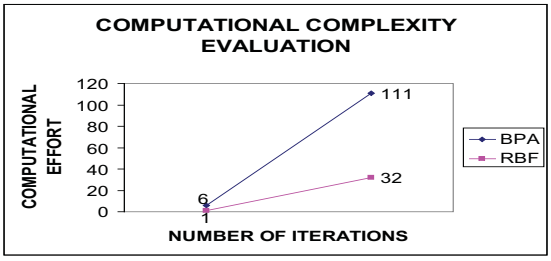
B. Computational effort comparison:

Results of the computational effort comparison of proposed algorithms are given in Table 2. By using equations given in Table 1, the computational effort for each algorithm has been calculated and presented, in order to compare them with regard to the total number of computational effort required by each algorithm.

Table 2. Computational effort comparison for proposed algorithms.

S.No.	Algorithm	No. of nodes in input layer (Hidden layer)	Number of iterations	MSE	Computational effort
1	BPA	2(2)	6	0.000811216	111
2	RBF	2(2)	1	NA	32

The network trained with transformed vector requires the least computational effort. RBF algorithm needs less computational effort than BPA.



V. CONCLUSION

This paper proposed the most popular supervised artificial neural network algorithms such as BPA and RBF for detecting the presence of the hidden message. The computational effort is also compared for the proposed algorithms. The comparison shows that RBF needs less computational effort than BPA.

REFERENCES

[1] Anderson, R.J., and Petitcolas, F.A.P., 1998, "On the limits of steganography", IEEE Journal on Selected Areas in Communications, Vol. 16, No. 4, pp. 474-484.
[2] Johnson, N., and Sklansky, J., 1998, "Exploring steganography: seeing the unseen", IEEE Computer, pp. 26-34.
[3] Westfeld, A., and Pfitzmann, A., 1999, "Attacks on steganographic systems", Lecture notes in computer science, proceedings of the 3rd International Workshop on Information Hiding, Vol. 1768, pp. 61-76.
[4] Westfeld, A., and Pfitzmann, A., 2000, "Attacks on Steganographic Systems", Lecture Notes in Computer Science, Springer-Verlag, Berlin, Vol. 1768, pp. 61-75.

[5] Fridrich, J., Goljan, M., and Du R., 2001, "Reliable Detection of LSB Steganography in Color and Gray-Scale Images", Magazine of IEEE Multimedia Special Issue on Security, pp. 22-28.
[6] Martin, A., Sapiro G., and Seroussi G., 2004, "Is image steganography natural?", Information Theory Research Group, HP Laboratories Palo Alto, HPL-39(R.1).
[7] Neil Provos, and Peter Honeyman, 2003, "Hide and Seek: An Introduction to Steganography", IEEE Security & Privacy, Vol. 1, No. 3, pp. 32-44.
[8] Fridrich, J., and Goljan, M., 2003, "Digital image steganography using stochastic modulation", Proceedings of IST/SPIE's 15th Annual Symposium on Electronic Imaging Science and Technology, San Jose, CA.
[9] Rajarathnam, Chandramouli, Mehdi Kharrazi, and Nasir Memon, 2004, "Image Steganography and Steganalysis: Concepts and Practice", Lecture Notes in Computer Science, International Workshop on Digital Watermarking, Korea, Vol. 2939, pp. 35-49.
[10] Vu Dao, N.P., and Rao Vemuri, 2002, "A Performance Comparison of Different Back Propagation Neural Networks Methods in Computer Network Intrusion Detection", Differential Equations and Dynamical Systems, Vol. 10, No. 1, pp. 201-214.
[11] Jack Kelley., 2001, "Terror Groups Hide Behind Web Encryption", USA Today.
[12] Natarajan, V., and Anitha, R., 2012, "Blind Image steganalysis Based on Contourlet Transform", International journal on Cryptography & Information Security, Vol. 2, No. 3, pp. 77-87.
[13] Chin-Chen Chang, Lin, CY., and Fan, YH., 2008, "Lossless data hiding for color images based on block truncation coding", Pattern Recognition, Vol. 41, No. 7, pp. 2347–2357.
[14] Yun Shi, Q., Guorong Xuan, Chengyun Yang, Jianjiong Gao, Zhenping Zhang, Peiqi Chai, Dekun Zou, Chunhua Chen, and Wen Chen, 2005, "Effective steganalysis Based on Statistical Moments of Wavelet Characteristic Function", IEEE International Conference on Information Technology: Coding and Computing, Vol. 1, pp. 768-773.
[15] Yong Wang, JiuFen Liu, and WeiMing Zhang, 2009, "Blind JPEG steganalysis Based on Correlations of DCT Coefficients in Multi-directions and Calibrations", International Conference on Multimedia Information Networking and Security, MINES'09, Vol. 1, pp. 495-499.
[16] Xiao Yi Yu, and Aiming Wang, 2009, "Steganalysis Based on Bayesion Network and Genetic Algorithm", 2nd International Congress on Image and Signal Processing, CISP'09, pp. 1-4.
[17] Declan Mc Cullah., 2001, "Secret Messages Come in Wavs", Wired News.
[18] Daniel Lerch-Hostalot, and David Meg´ıas, 2012, "Steganalytic Methods for the Detection of Histogram Shifting Data Hiding Schemes", Proceedings of Reunión Española Cryptology and Information Security (RECSI).