Implementation of Radial Basis Function Neural Network for Image Steganalysis

Sambasiva Rao Baragada mrsambasivarao@yahoo.com
Department of Mathematics & Computer Science
Sri Venkateswara University
Tirupati, 517502, India

S. Ramakrishna drsramakrishna@yahoo.com
Department of Mathematics & Computer Science
Sri Venkateswara University
Tirupati, 517502, India

M. S. Rao cfs_dfs@dfs.gov.in
Director cum Chief Forensic Scientist
Directorate of Forensic Science
Ministry of Home Affairs
New Delhi, 110003, India

S. Purushothaman dr.s.purushothaman@gmail.com
Faculty of Engineering
Asia-Pacific Institute of Information Technology
KaulaLumpur, 57000, Malaysia

Abstract

Steganographic tools and techniques are becoming more potential and widespread. Illegal use of steganography poses serious challenges to the law enforcement agencies. Limited work has been carried out on supervised steganalysis using neural network as a classifier. We present a combined method of identifying the presence of covert information in a carrier image using fisher's linear discriminant (FLD) function followed by the radial basis function (RBF). Experiments show promising results when compared to the existing supervised steganalysis methods, but arranging the retrieved information is still a challenging problem.

Keywords: Steganography, carrier image, covert image.

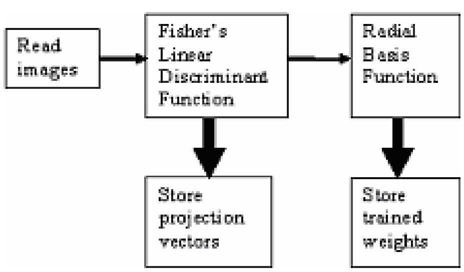
1. INTRODUCTION

Steganography is a type of hidden communication that literally means "covered writing". The message is out in the open, often for all to see, but goes undetected because the very existence of the message is secret [12, 20, 21]. Steganalysis could be described as a method to prevent steganography. There are other attacks on steganography. Attacking the end hosts of the steganography algorithm by searching for security credentials is not steganalysis. Digital forensics encompasses more methods than solely steganalysis to attack steganography. The target for digital forensics is detection of steganography. The objective of steganalysis is "detecting messages hidden using steganography". Steganalysis is about separating cover-messages from stego-messages. In this work, passive steganalysis is focused.

Most of the present literature on steganalysis follows either a parametric model [28, 24, 26] or a blind model [32, 27, 22, 23, 35, 33]. A general steganalysis method that can attack steganography blindly, detect hidden data without knowing embedding methods, will be more useful in practical applications. A framework for steganalysis based on supervised learning has been done in [34]. The framework was further developed and tested. Limited work has been carried out on supervised steganalysis, using neural networks as a classifier [29, 30]. Fishers' linear discriminant function (FLD) as a classifier show impressive results in [31]. The present neural network based steganalytic work is implemented by combining the radial basis function neural network with fishers' linear discriminant function.

2. METHODOLOGY

Machine learning theory based steganalysis assume no statistical information about the stego image, host image and the secret message. This 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 supplied to neural classifier to learn the nature of the images. RBF takes the role of neural classifier in this work. By training the classifier for a specific embedding algorithm a reasonably accurate detection can be achieved. RBF 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:



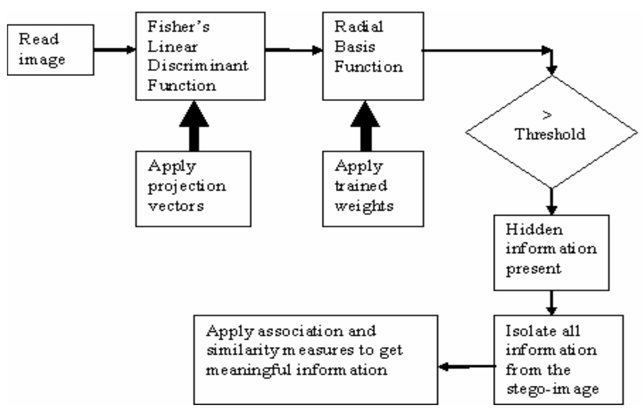


FIGURE 1a: Training Phase **FIGURE 1b:** Testing phase

2.1 Fisher's Linear Discriminant Function

The process of changing the dimensions of a vector is called transformation. The transformation of a set of n-dimensional real vectors onto a plane is called a mapping operation. The result of this operation is a planar display. The main advantage of the planar display is that the distribution of the original patterns of higher dimensions (more than two dimensions) can be seen on a two dimensional graph. The mapping operation can be linear or non-linear. R.A. Fisher developed a linear classification algorithm [1] and a method for constructing a classifier on the optimal discriminant plane, with minimum distance criterion for multi-class classification with small number of patterns [16]. The method of considering the number of patterns and feature size [4], and the relations between discriminant analysis and multilayer perceptrons [17] has been addressed earlier. A linear mapping is used to map an n-dimensional vector space $\Re^n$ onto a two dimensional space. Some of the linear mapping algorithms are principal component mapping [5], generalized declustering mapping [2, 3, 8, 9], least squared error mapping [11] and projection pursuit mapping [6]. In this work, the generalized declustering optimal discriminant plane is used. The mapping of the original pattern 'X' onto a new vector 'Y' on a plane is done by a matrix transformation, which is given by

$$Y=AX \tag{1}$$

where

$$A = \begin{bmatrix} \varphi_1 \\ \varphi_2 \end{bmatrix} \tag{2}$$

and φ1 and φ2 are the discriminant vectors (also called projection vectors).

An overview of different mapping techniques [14, 15] is addressed earlier. The vectors φ1 and φ2 are obtained by optimizing a given criterion. The plane formed by the discriminant vectors is the optimal vectors which are the optimal discriminant planes. This plane gives the highest possible classification for the new patterns.

The steps involved in the linear mappings are:

Step 1: Computation of the discriminant vectors φ1 and φ2: this is specific for a particular linear mapping algorithm.

Step 2: Computation of the planar images of the original data points: this is for all linear mapping algorithms.

1) Computation of discriminant vectors φ_1 and φ_2

The criterion to evaluate the classification performance is given by:

$$J(\varphi) = \frac{\varphi^{T} S_b \varphi}{\varphi^{T} S_W \varphi} \tag{3}$$

Where

S_b the between class matrix, and

S_w the within class matrix which is non-singular.

$$S_b = \sum p(\omega_i)(m_i - m_o)(m_i - m_o)^T \tag{4}$$

$$S_w = \sum p(\omega_i)E\left[X_i - m_o)(X_i - m_i)^T \omega_i\right] \tag{5}$$

where

$P(\omega_i)$ a priori the probability of the i^{th} pattern, generally, p (ω_i) = 1/m

m_i the mean of each feature of the i^{th} class patterns, (i=1.2…,m),

m_o the global mean of a feature of all the patterns in all the classes,

X {xi, I=1, 2,…L} the n-dimensional patterns of each class,

L the total number of patterns.

Eq.(3) states that the distance between the class centers should be maximum. The discriminant vector φ_1 that maximizes 'J' in Eq. (3) is found as a solution of the eigenvalue problem given by:

$$S_b \varphi_1 = \lambda_{ml} S_w \varphi_1 \tag{6}$$

where

λ_{ml} the greatest non-zero eigenvalue of $(S_b S_w^{-1})$

φ_1 eigenvalue corresponding to λ_{ml}

The reason for choosing the eigenvector with maximum eigenvalue is that the Euclidean distance of this vector will be the maximum, when compared with that of the other eigenvectors of Eq.(6). Another discriminant vector φ_2 is obtained, by using the same criterion of Eq.(3). The discriminant vector φ_2 should also satisfy the condition given by:

$$\varphi^T{}_2\,\varphi_1=0 \tag{7}$$

Eq.(7) indicates that the solution obtained is geometrically independent and the vectors φ_1 and φ_2 are perpendicular to each other. Whenever the patterns are perpendicular to each other, it means, that there is absolutely no redundancy, or repetition of a pattern. The discriminant vector φ_2 is found as a solution of the eigenvalue problem, which is given by:

$$Q_p\, S_b\, \varphi_2 = \lambda_{m2}\, S_w\, \varphi_2 \tag{8}$$

where
λ_{m2} the greatest non-zero eigen value of $Q_p\, S_b\, S_w^{-1}$, and
Q_p the projection matrix which is given by

$$Q_p = I - \frac{\varphi_1\, \varphi_1^T\, S_W^{-1}}{\varphi_1^T\, S_W^{-1}\, \varphi_1} \tag{9}$$

where
I an identity matrix

The eigenvector corresponding to the maximum eigenvalue of Eq. (8) is the discriminant vector φ_2. In Eq.(6) and Eq. (8), S_W should be non-singular. The S_W matrix should be non-singular, even for a more general discriminating analysis and multi-orthonormal vectors [7, 18, 19]. If the determinant of S_W is zero, then singular value decomposition (SVD) on S_W has to be done. On using SVD [10, 13], S_W is decomposed into three matrices U, W and V. The matrices U and W are unitary matrices, and V is a diagonal matrix with non-negative diagonal elements arranged in the decreasing order. A small value of 10^{-5} to 10^{-8} is to be added to the diagonal elements of V matrix, whose value is zero. This process is called perturbation. After perturbing the V matrix, the matrix S_w^1 is calculated by:

$$S_w^{\,1} = U * W * V^T \tag{10}$$

where
S_W^1 the non-singular matrix which has to be considered in the place of S_w.
Minimum perturbed value should be considered, which is just sufficient to make S_w^1 non-singular. As per Eq.(7), when the values of φ_1 and φ_2 are innerproducted, the resultant value should be zero. In reality, the innerproducted value will not be zero. This is due to floating point operations.

2) Computation of two-dimensional vector from the original n-dimensional input patterns

The two-dimensional vector set y_i is obtained by:

$$y_i = (u_i , v_i) = (X_i^T\, \varphi_1 , X_i^T\, \varphi_2) \tag{11}$$

The vector set y_i is obtained by projecting the original pattern 'X' onto the space, spanned by φ_1 and φ_2 by using Eq.(11). The values of u_i and v_i can be plotted in a two-dimensional graph, to know the distribution of the original patterns.

2.2 Radial Basis Function

A radial basis function (RBF) is a real-valued function whose value depends only on the distance from the origin. If a function 'h' satisfies the property $h(\mathbf{x})=h(||\mathbf{x}||)$, then it is a radial function. Their characteristic feature is that their response decreases (or increases) monotonically with distance from a central point. The centre, the distance scale, and the precise shape of the radial function are parameters of the model, all fixed if it is linear [25].

A typical radial function is the Gaussian which, in the case of a scalar input, is

$$h(x)=\exp((-(x-c)^2)/(r^2)) \quad (12)$$

Its parameters are its centre *c* and its radius *r*.

A Gaussian RBF monotonically decreases with distance from the centre. In contrast, a multiquadric RBF which, in the case of scalar input, monotonically increases with distance from the centre. Gaussian-like RBFs are local (give a significant response only in a neighbourhood near the centre) and are more commonly used than multiquadric-type RBFs which have a global response. Radial functions are simply a class of functions. In principle, they could be employed in any sort of model (linear or nonlinear) and any sort of network (single-layer or multi-layer). RBF networks have traditionally been associated with radial functions in a single-layer network. In the Figure 2, the input layer carries the outputs of FLD function. The distance between these values and centre values are found and summed to form linear combination before the neurons of the hidden layer. These neurons are said to contain the radial basis function with exponential form. The outputs of the RBF activation function is further processed according to specific requirements.

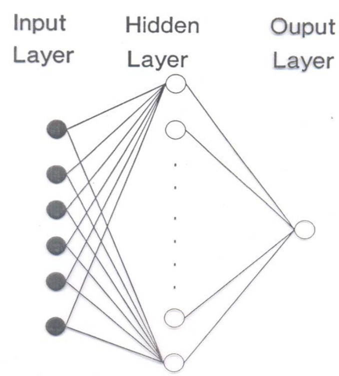


FIGURE 2: Radial Basis Function Network

3. IMPLEMENTATION

a) Training

1. Decide number of cover images.
2. Read each Image.
3. Calculate the principal component vector by

$$Z=Z * Z^T$$

where

Z denotes the intensities of image

4. Find eigenvector of the Z matrix by applying eigen process.
5. Calculate the φ_1 and φ_2 vectors.

φ_1 **=** eigenvector ($S_b * S_w^{-1}$)

$S_b = \sum (PCV_i - M_0) (PCV_i - M_0)^T / N$

where:

PCV_i (i = 1,2,3)

PCV_1, Principal component vector1
PCV_2, Principal component vector2
PCV_3, Principal component vector3
M_0 = Average of ($PCV_1 + PCV_2 + PCV_3$)
$S_w = (\sum (PCV_i - M_i) (PCV_i - M_i)^T) / N$

where:

M_i (i = 1, 2, 3)
M_1, average of PCV_1
M_2, average of PCV_2
M_3, average of PCV_3

6. Calculate φ_2 vector.
   φ_2 **=** eigenvector ($Q\, S_b\, S_w^{-1}$)
   $Q = I - ((\varphi_1 * \varphi_1^{-1} * S_w^{-1}) / (\varphi_1^t * S_w^{-1} * Phi\_\varphi_1))$
7. Transfer for N dimensional vector into 2 dimensional vector.
   U **=** $\varphi_1 * PCV_{i\ (1,2,3)}$
   V **=** $\varphi_2 * PCV_{i\ (1,2,3)}$
8. Apply RBF.
   No. of Input = 2
   No. of Patterns = 15
   No. of Centre = 2
   Calculate RBF as
   RBF = exp (-X)
   Calculate Matrix as
   G = RBF
   $A = G^T * G$
   Calculate
   $B = A^{-1}$
   Calculate
   $E = B * G^T$
9. Calculate the final weight.
   F = E * D
10. Store the final weights in a File.

b) Testing

1. Read steganographed image.
2. Calculate the principal component vector.
   $Z=Z * Z^T$
3. Find eigenvector of the Z matrix by applying eigen process.
4. Calculate RBF as.
   RBF = exp (-X)
   G = RBF
   $A = G^T * G$
   $B = A^{-1}$
   $E = B * G^T$
5. Calculate.
   F = E * D
6. Classify the pixel as containing information or not.

4. RESULTS AND DISCUSSION

The simulation of steganalysis has been implemented using MATLAB 7®. Sample sets of images considered are gray and true color images. The different sets of cover images considered in the simulation are given in Figure 3. The information image is given in Figure 4. Encryption technique has not been considered during the simulation. The different ways the secret information scattered in the cover images are given in Figure 5.

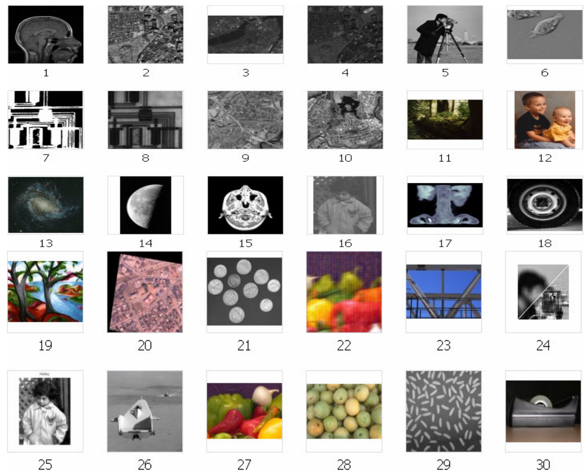


FIGURE 3: Cover images

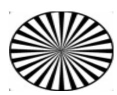


FIGURE 4: Information Image

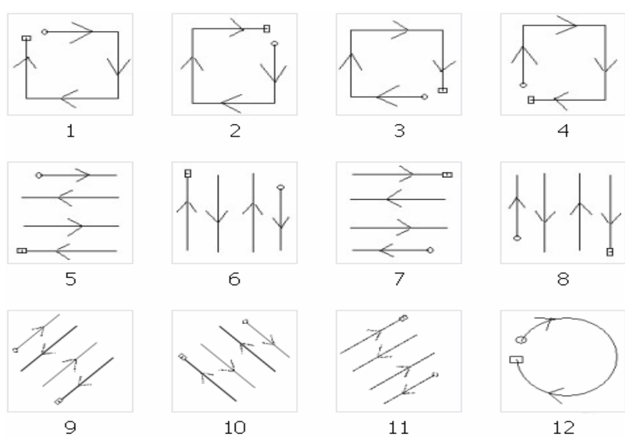


FIGURE 5: Distribution of information image in cover image

In this simulation, the information is embedded using least significant bit (LSB), discrete cosine transformation (DCT) separately. In certain cases, 50% of the information image is embedded using LSB and remaining 50% of the information is embedded using DCT. In the entire simulation, the size of the information image is considered to 1/8 size of the original image (Table I). The outputs of the FLD (Figure 6), RBF (Figure 7), and combined method FLD with RBF (Figure 8) are shown. The projection vectors are given in Table II.

Embedding methods used	LSB, DCT, LSB and DCT
Size of the cover image	512 X 512
Size of the secret image	128 X 128 = 1/16th (512 X 512)
Method of embedding	Specific sequences formed (Fig. 4)
Processing the true color image (RGB)	Red , green , blue planes are embedded separately in the lower nibble

Table I: SIMULATION ENVIRONMENT USED

φ_1	φ_2
0.8243	0.6975
0.5662	0.7166

Table II: PROJECTION VECTORS

These vectors obtained after finding out the S_w and S_b matrices considering 30 steganographed images using the images given in Figure 3 and Figure 4. Figure 7 and figure 8 are obtained by setting a detection threshold value of 2. Any output greater than a threshold is considered as the pixel containing the information. The threshold value is different for different method.

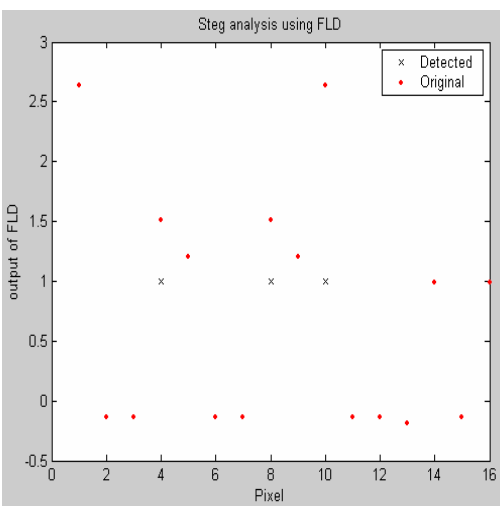


FIGURE 6: Steganalysis using FLD

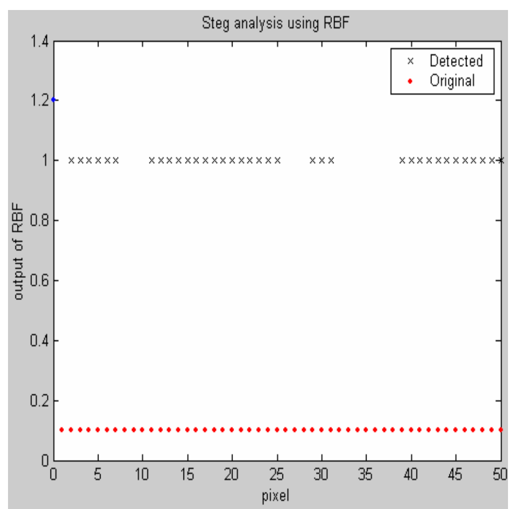


FIGURE 7: Steganalysis using RBF

5. CONCLUSION

Steganalysis has been implemented using FLD, RBF and combination of FLD and RBF algorithms. 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 FLDRBF is much promising in detecting the presence of hidden information. The cover images chosen for the simulation are standard images. The percentage of identifying the hidden information is more than 95%, but arranging the retrieved information is still a challenging problem. The information can be well arranged in a meaningful way by using a set of association rules.

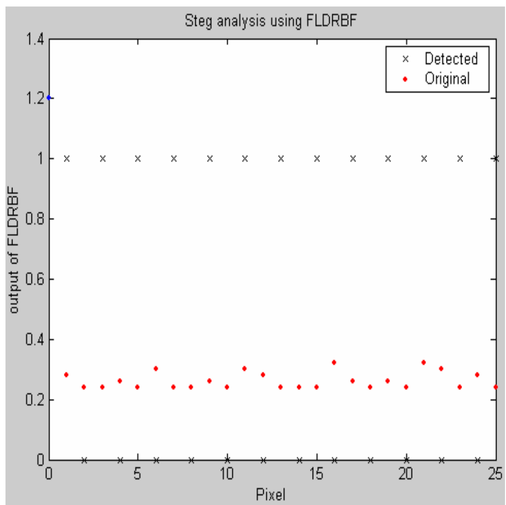


FIGURE 8: Steganalysis using FLDRBF

6. ACNOWLEDGEMENT

We express our sincere thanks to Mr. Ch Gandhi, GEQD, Hyderabad for his valuable support in improving the quality of the paper. We also express our heartful thanks to Mr. P. Krishna Sastry and Mr. M. Krishna for their technical support in doing experiments at computer forensic division, Hyderabad. Appreciation also goes to Ms. S. Rajeswari, Ms. G. Sarada, Ms. Uma Devi, and Ms. Chennamma and for their help in literature survey

7. REFERENCES

1. R.A.Fisher, "*The Use of Multiple Measurements in Taxonomic Problems*," Ann. of Eugenics, vol. 7, pp. 178 – 188, 1936.
2. J.W.Sammon, "*An Optimal Discriminant Plane*," IEEE Trans. On Comp, vol. 19, no. 9, pp. 826 – 829, 1970.
3. J.W Sammon., "*Interactive Pattern Analysis and Classification"*, *IEEE* Trans. on Comp., vol. 19, no. 7, pp. 594–616, 1970.
4. D.H.Foley, "*Consideration of Sample and Feature Size*," IEEE Trans., on Info. Theory, vol.18, no. 5, pp. 626 – 681, September 1972.
5. J.Kittler, P.C.Young P.C, "*Approach to Feature Selection Based on the Karhunen-Loeve Expansion*," Pattern Recognition, Vol. 5, No 5, pp. 335 – 352, 1973.
6. H.Friedman, J.W Turkey, "*A Projection Pursuit Algorithm for Exploratory Data Analysis*," IEEE Trans. on Comp., vol. 23, no. 9, pp. 881–890, 1974.

7. D.H Foley, J.E.Sammon, “*An Optimal Set of Discriminant Vectors*,” IEEE Trans. on Comp., vol. 24, no. 3, pp. 281 – 289, 1975.
8. J. Fehlauer., B.A Eisenstein., “*A Declustering Criterion for Feature Extraction in Pattern Recognition*, IEEE Trans. on Comp., vol. 27, no. 3, pp. 261 – 266, 1978.
9. E.Gelsema, R.Eden, “*Mapping Algorithms in ISPAHAN*,” pattern Recognition, vol. 12, no. 3, pp.127 – 136, 1980.
10. V.C.Klema, A.J.Laub, “*The Singular Value Decomposition: Its Computation and Some Applications*,” IEEE Trans. on Automatic Control, vol. 25, no.2, pp. 164 – 176, 1980.
11. D.F.Mix, R.A.Jones, “*A Dimensionality Reduction Techniques Based on a Least Squared Error Criterion*, IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 4, no. 1, pp. 537 – 544, 1982.
12. Simmons, G. J., “*The Prisoners’ Problem and the Subliminal Channel*,” CRYPTO83, Advances in Cryptology, August 22-24, pp. 51 – 67, 1984.
13. B.J.Sullivan, B.Liu, “*On the Use of Singular Value Decomposition and Decimation in Discrete-Time Band-Limited Signal Extrapolation*,” IEEE Trans. on Acoustics, Speech and Signal Processing, vol. 32, no. 6, pp. 1201 – 1212, 1984.
14. W.Siedlecki, K.Siedlecka, J. Skalansky, “*An Overview of Mapping Techniques for Exploratory Data Analysis*,” Pattern Recognition, vol. 21, no. 5, pp. 411 – 429, 1988.
15. W.Siedlecki, K.Siedlecka., J.Skalancky, “*Experiments on Mapping Techniques for Exploratory Pattern Analysis*,” Pattern Recognition, vol. 21, no.5, pp. 431 – 438, 1988.
16. Z.Q.Hong, Y.J.Yang, *“Optimal Discriminate Plane for a Small Number of Samples and Design Method of Classifier on the Plane*,” pattern recognition, vol. 24, pp. 317 – 324, 1991.
17. P.Gallinari, S. Thiria., F.Badran., F Fogelman-Soulie F., “*On The Relations Between Discriminant Analysis and Multilayer Perceptrons*,” Neural Networks, vol. 4, no.3, pp.349 – 360, 1991.
18. K.Liu, Y.Q.Cheng, J.Y.Yang J.Y., “*A Generalized Optimal Set of Discriminant Vectors*,” Pattern Recognition, vol. 25, no. 7, pp. 731 – 739, 1992.
19. Y.Q.Cheng, Y.M.Zhuang, J.Y.Yang, “*Optimal Fisher Discriminant Analysis Using the Rank Decomposition*,” Pattern Recognition, vol. 25, no. 1, pp. 101 – 111, 1992.
20. 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.
21. N.Johnson and J. Sklansky, “*Exploring steganography: seeing the unseen*,” IEEE Computer, pp. 26 – 34, 1998.
22. N. Provos and P. Honeyman, “*Detecting steganographic content on the internet*,” CITI Technical Report 01-11, August, 2001.
23. A. Westfeld and A. Pfitzmann, “*Attacks on steganographic systems*,” Third Information Hiding Workshop, September. 1999.
24. J. Fridrich, R. Du, and M. Long, “*Steganalysis of lsb encoding in color images*,” IEEE ICME, vol. 3, pp. 1279 – 1282, March 2000.
25. Meng Joo Er,.Shiqian Wu, Juwei Lu and Hock Lye Toh, “*Face Recognition with Radial Basis Function(RBF) Neural Networks*,” IEEE Trans. on Neural Networks, vol. 13, no.3, pp. 697 – 910, May 2002.
26. R. Chandramouli, “*A mathematical framework for active steganalysis*,” ACM Multimedia Systems, vol, 9, no.3, pp.303 – 311, September 2003.
27. J. Harmsen and W. Pearlman, “*Steganalysis of additive noise modelable information hiding*,” Proc. SPIE Electronic Imaging, 2003.
28. 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.
29. 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.
30. 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.
31. Ming Jiang, Wong, E.K. Memon, N. Xiaolin Wu, "*Steganalysis of halftone images*," Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing, ICASSP, vol. 2, pp. 793 – 796, March 2005.
32. 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.
33. 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.
34. H. Farid, "*Detecting hidden messages using higher-order statistical models,*" Proc. IEEE Int. Conf. Image Processing, New York, pp.905- 908, Sep. 2002.
35. 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.