Blind Steganalysis with Modified Markov Features and RBFNN

R.Lakshmi Priya , P.Eswaran, S.L.Ponnambli Kamakshi

PSN College of Engineering & Technology, Tirunelveli, India

Abstract: *In recent years more sophisticated Steganographic tools and techniques have evolved which poses serious challenges to the law enforcement agencies. This is the first and foremost paper which deals with Modified Markov features in feature extraction and Radial Basis Neural Network as neural network classifier. Steganography involves hiding information so it appears that no information is hidden at all. In contrast, Steganalysis technique determines the presence of hidden messages in the image/text/video/audio file. A general steganalysis method that can attack Steganography blindly, detect hidden information irrespective of the embedding algorithm is more useful for real time applications. In this paper, a Steganalysis system was proposed that can detect the hidden information irrespective of the image databases and irrespective of the embedding algorithm using Modified Markov features. Radial Basis Function Neural Network (RBFNN) is utilized to construct a blind classifier. Experimental results show that our method is significantly better than the existing steganalysis system.*

Keywords: *Steganography, Blind steganalysis, Stego image, Cover image, L-GEM, Artificial neural network*

1. Introduction

Steganography [1] is a technique to hide data inside a cover medium in such a way that the existence of any communication itself is undetectable as opposed to cryptography where the existence of secret communication is known but is indecipherable. Steganography includes the concealment of information within computer files. The carrier files used are text, image, audio, video etc. There exist few important requirements for the steganographic systems such as security of the hidden information, size of the payload and robustness against malicious and unintentional attacks. Also for information hiding digital images are widely made use of.

The two major advantages of using digital images for steganography are first, digital images are widely used medium today and second, it takes the advantage of our limited visual perception of colors. The larger the image size, more information can be hidden. However, larger images may require compression to avoid detection. Often there seems to be a misunderstanding between steganography and cryptography, the one difference that can solve this issue is steganography deals with hiding information in the carrier file while cryptography helps to encrypt the hidden information from the carrier file.

Steganalysis [1] is the process of identifying a suspected stego media, inspecting various parameters whether that media contains hidden message, then try to recover the hidden data. In the steganalysis, the suspected media may or may not contain hidden data.

Most of the hidden messages hidden using steganography tools do not leave many (if any) signs that something has been hidden. On the other hand steganalysis is the art and science of detecting secret messages hidden using steganography. In addition, steganalysis also serves as a tool to measure the performance of a steganographic algorithm. Steganographic techniques find its main applications in computer forensics, cyber warfare and tracking the criminal activities etc. With the growing attention given to securing the social public network steganalysis has become a hot research topic. Many steganalysis techniques have been proposed in the literature. Literature reveals that steganalysis can be divided into two classes: target steganalysis and universal steganalysis.

Target steganalysis normally used to detect a specific steganographic method. Also this method will not work for other steganographic techniques. For example, Fridrich et al. broke the F5 algorithm by estimating an approximation of cover image using the stego image [18]. Whereas universal or blind steganalysis is a generic scheme that are capable of detecting the presence of secret message irrespective of the steganographic algorithm being used. Blind steganalysis is more popular for its usefulness in practical applications and also capable of detecting a new steganographic technique for which no targeted steganalysis is available.

The various steganographic tools available today are JSteg[16], F5[14], MB1(Model Based Steganography)[19], MB2(Model Based Steganography with deblocking)[20], Outguess[15], Steghide[21] etc. steganography can be used as a beneficial tool for privacy.

2. Related Works

The first works on blind steganalysis was proposed by Avcibas in [23]. In which the authors have employed image quality metrics as features. They have also used one way ANOVA test to select the metrics that responds consistently and strongly. Based on the features obtained a multivariate regression techniques was used to classify the image as cover image and stego image.

Harmsen et al. in [24] presented a detector based on the Histogram Characteristic Function (HCF) for color images; however its performance is not good for raw images and gray scale images. Later to improve the performance number of works were presented [25,26].

Farid was one of the first to propose the use of higher order statistics to detect hidden messages in a stego medium [10]. He used a wavelet like decomposition to build a higher order statistical model for natural images. Fisher linear discriminant (FLD) pattern classifier is used to train and predict if a given image is cover or stego. The results show an average of 90% detection rate for Outguess and JSteg.

The idea of using Markov random chains was first proposed in [27] to detect the spread spectrum hiding in gray scale images. The Markov chains were used to model the correlation between pixels in an image. The authors have used a supervised learning machine to classify the cover and stego image.

Pevny and Fridich in [8] applied calibration to Markov features and merged the markov feature with DCT features to improve the performance of blind steganalysis.

Shi et al in [7] has presented a Markov feature based approach to attack JPEG stegnography. The author has also got promising results in detecting F5, Outguess and MB1. The advantage with this kind of technique is that it can be used with any existing algorithm without any modification and hence can be categorized as a universal steganalyzer.

Chen and Agaian [6] used RBFNN for steganographic detection through feature preprocessing, feature extraction, data standardization and data classification. The author shows through experimental results that the RBFNN has high classification accuracy.

Patrick and Daniel proposed in [22] a steganalysis method based on markov features and Radial Basis Function Neural Network for data classification. In this paper, the author introduced a steganalysis method to generalize the testing images obtained from different images databases and of different sizes.

This paper is organized as follows. Section 3 starts with the description about the feature construction. Section 4 briefly describes about the classifier construction, which is the training of the RBFNN with L-GEM. Then section 5 presents the experimental results. Finally, conclusion is drawn in Section 6.

3. Feature Extraction

The Markov feature [1] captures the statistics based on the difference JPEG arrays by a Markov process. In this paper, we expand the Markov approach further to a modified Markov approach. First we extract the Markov features based on absolute values of the neighboring DCT coefficients, then on correlation of the neighboring DCT coefficients in the inter-DCT block and finally to DWT approximation subband.

3.1 Modified Markov Feature

Let F denote the matrix of the absolute values of DCT coefficients of the image. Hence, the four difference arrays determined along four directions such as horizontal, vertical, diagonal and minor diagonal are as follows:

$$F_h(u,v) = F(u,v) - F(u,v+1) \tag{1}$$

$$F_v(u,v) = F(u,v) - F(u+1,v) \tag{2}$$

$$F_d(u,v) = F(u,v) - F(u+1,v+1) \tag{3}$$

$$F_m(u,v) = F(u+1,v) - F(u,v+1) \tag{4}$$

The transition probability matrix can be used to characterize the markov random process. In this paper, we make use of 1-step transition probability which gives a balance between the high steganalysis capability and computational complexity.

In this paper, we construct the transition probability matrices only along the vertical and horizontal directions. Hence the transition probability matrices constructed based on $F_h(u,v)$ and $F_v(u,v)$ are as follows

$$\mathbf{M1}_{hh}(i,j) = \frac{\sum_{u=1}^{S_u-2}\sum_{v=1}^{S_v}\delta(F_h(u,v)=i, F_h(u+1,v)=j)}{\sum_{u=1}^{S_u-2}\sum_{v=1}^{S_v}\delta(F_h(u,v)=i)} \tag{5}$$

$$\mathbf{M1}_{hv}(i,j) = \frac{\sum_{u=1}^{S_u-1}\sum_{v=1}^{S_v-1}\delta(F_h(u,v)=i, F_h(u,v+1)=j)}{\sum_{u=1}^{S_u-1}\sum_{v=1}^{S_v-1}\delta(F_h(u,v)=i)} \tag{6}$$

$$\mathbf{M1}_{vh}(i,j) = \frac{\sum_{u=1}^{S_u-1}\sum_{v=1}^{S_v-1}\delta(F_v(u,v)=i, F_v(u+1,v)=j)}{\sum_{u=1}^{S_u-1}\sum_{v=1}^{S_v-1}\delta(F_v(u,v)=i)} \tag{7}$$

$$\mathbf{M1}_{vv}(i,j) = \frac{\sum_{u=1}^{S_u}\sum_{v=1}^{S_v-2}\delta(F_v(u,v)=i, F_v(u,v+1)=j)}{\sum_{u=1}^{S_u}\sum_{v=1}^{S_v-2}\delta(F_v(u,v)=i)} \tag{8}$$

Here S_u and S_v are the dimensions of the image i.e. size of the coefficient matrix along the horizontal direction and vertical direction, the value of δ is equal to 1 iff the arguments are satisified. The range of i and j is [-4,+4]

In order, to reduce the noise, we take the average of vertical and horizontal directions as,

$$F_{avg} = \{ M1_{hh} + M1_{hv} + M1_{vh} + M1_{vv} \}/4 \quad (9)$$

3.2. Markov Feature based on inter-block DCT coefficients:

Here, the markov feature is expanded to the neighbouring DCT coefficients on the inter-blocks as in [8,17].The horizontal and vertical difference arrays on the inter block is determined as follows,

$$D_h(u,v) = F(u,v) - F(u+8,v) \quad (10)$$

$$D_v(u,v) = F(u,v) - F(u,v+8) \quad (11)$$

The transition probability matrices for the difference arrays on the inter-block is calculated as follows,

$$\mathbf{M2}_{hh}(i,j) = \frac{\sum_{u=1}^{S_u-16}\sum_{v=1}^{S_v} \delta(D_h(u,v) = i, D_h(u+8,v)=j)}{\sum_{u=1}^{S_u-16}\sum_{v=1}^{S_v} \delta(D_h(u,v) = i)} \quad (12)$$

$$\mathbf{M2}_{hv}(i, j= \frac{\sum_{u=1}^{S_u-8}\sum_{v=1}^{S_v-8} \delta(D_h(u,v) = i, D_h(u,v+8)=j)}{\sum_{u=1}^{S_u-8}\sum_{v=1}^{S_v-8} \delta(D_h(u,v) = i)} \quad (13)$$

$$\mathbf{M2}_{vh}(i,j) = \frac{\sum_{u=1}^{S_u-8}\sum_{v=1}^{S_v-8} \delta(D_v(u,v)= i, D_v(u+8,v)=j)}{\sum_{u=1}^{S_u-8}\sum_{v=1}^{S_v-8} \delta(D_v(u,v) = i)} \quad (14)$$

$$\mathbf{M2}_{vv}(i,j) = \frac{\sum_{u=1}^{S_u}\sum_{v=1}^{S_v-16} \delta(D_v(u,v)=i, D_v(u,v+8)=j)}{\sum_{u=1}^{S_u}\sum_{v=1}^{S_v-16} \delta(D_v(u,v) = i)} \quad (15)$$

Then the average is taken as,

$$F_{avg} = \{M2_{hh} + M2_{hv} + M2_{vh} + M2_{vv}\}/4 \quad (16)$$

3.3. DWT Approximation Subband

The horizontal and vertical difference arrays along DWT approximation subbands are calculated as follows,

$$WA_h(u,v) = WA(u,v) – WA(u,v-1) \quad (17)$$

$$WA_v(u,v) = WA(u,v) – WA(u+1,v) \quad (18)$$

Let WA denote the Haar DWT approximation sub-band that is multiplied by 2. We prefer Haar transform as it is real and orthogonal than any other wavelet transform.

The transition probability matrices are determined as follows,

$$M3_{hh}(i,j) = \frac{\sum_{u=1}^{SW_u-2}\sum_{v=1}^{SW_v} \delta(WA_h(u,v)=i, WA_h(u+1,v)=j)}{\sum_{u=1}^{SW_u-2}\sum_{v=1}^{SW_v} \delta(WA_h(u,v) = i)} \quad (19)$$

$$M3_{hv}(i,j) = \frac{\sum_{u=1}^{SW_u-1}\sum_{v=1}^{SW_v-1} \delta(WA_h(u,v)= i, WA_h(u,v+1)=j)}{\sum_{u=1}^{SW_u-1}\sum_{v=1}^{SW_v-1} \delta(WA_h(u,v) = i)} \quad (20)$$

$$M3_{vh}(i,j) = \frac{\sum_{u=1}^{SW_u-1}\sum_{v=1}^{SW_v-1} \delta(WA_v(u,v) = i, WA_v(u+1,v)=j)}{\sum_{u=1}^{SW_u-1}\sum_{v=1}^{SW_v-1} \delta(WA_v(u,v) = i)} \quad (21)$$

$$\mathrm{M3}_{vv}(i,j) = \frac{\sum_{u=1}^{SW_u} \sum_{v=1}^{SW_v-2} \delta(\mathrm{WA}_v(u,v) = i, \mathrm{WA}_v(u,v+1) = j)}{\sum_{u=1}^{SW_u} \sum_{v=1}^{SW_v-2} \delta(\mathrm{WA}_v(u,v) = i)} \qquad (22)$$

Then the average is taken as,

$$\mathrm{F}_{avg} = \{ \mathrm{M3}_{hh} + \mathrm{M3}_{hv} + \mathrm{M3}_{vh} + \mathrm{M3}_{vv} \}/4 \qquad (23)$$

3.4. Calibrating the images

We adopt calibration method as in [17] in our paper to increase the detection accuracy of the steganalysis system. The calibrated image features do have the same statistical characteristics as that of the original image.

The calibrated features can be obtained as the difference between the test image and the calibrated image. The calibrated features can be determined from the formula

$$\mathrm{F} = |\mathrm{F}_{test} - \mathrm{F}_{cal}| \qquad (24)$$

Where the F_{test} denotes the features extracted from the test image and F_{cal} denotes the features extracted from the original image.

4. Classifier

4.1 Radial Basis Function Neural Network (RBFNN):

RBFNN is a feed forward network. RBFNN is used for pattern recognition, regression and time series prediction applications The architecture of RBFNN is a three layer network in which the input layer is just a fan-out layer (no processing), the hidden layer applies a nonlinear transformation from the input space to the hidden space and the output layer applies a linear transformation from the hidden space to the output space. Also there exists a major problem with RBFNN in selecting the number of hidden neurons. If too many hidden neurons are chosen, then it may lead to over-fitting problem. If very few hidden neurons are chosen then the classifier may not learn well.

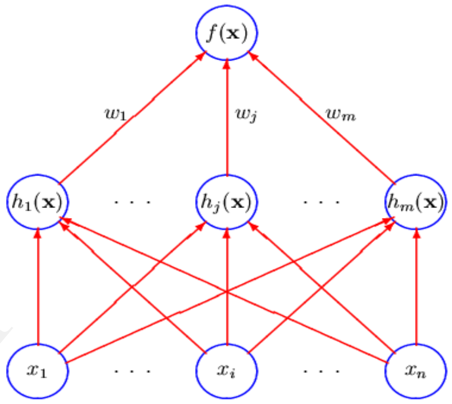


Fig. 2 A Traditional Radial Basis Function Network

4.2 Localized Error Generalization Model (L-GEM)

RBFNN performance is primarily determined by its architecture selection. For this purpose L-GEM is introduced [9] i.e. for architecture selection. The two major concepts in L-GEM are Q-neighbourhood and Stochastic sensitivity measure. The Q-neighbourhood of a training sample [9] is defined as follows

$$\mathrm{S}_Q(x_b) = \{x \mid x = x_b + \Delta x;\ |\Delta x_i| <= Q$$
$$\forall\ i = 1,\ldots..,n\} \qquad (25)$$

Where Q is a real number, Δx be the input perturbation and x_b be the training samples

The localized generalization error of RBFNN [9] is defined as follows

$$R_{SM}(Q) = \int_{S_Q} (f_\theta(x) - F(x))^2 \, p(x)\, dx \qquad (26)$$

Where x, F(x), p(x), S_Q denote the input vector of a sample, the true output, the true unknown probability density function of the input x and the union of all

$S_Q(x_b)$.

Let $\Delta y = f_\theta(x) - f_\theta(x_b)$ & $err_\theta(x_b) = f_\theta(x_b) - F(x_b)$

$$R_{emp} = (1/N)\sum_{b=1}^{N} (err_\theta(x_b))^2 \qquad (27)$$

$$E_{S_Q}((\Delta y)^2) = (1/N)\sum_{b=1}^{N} \int_{S_Q} (\Delta y)^2 / (2Q)^n \, dx \qquad (28)$$

The L-GEM provides an upper bound for the of RBFNN with a probability 1-η, we have,[9]

$$R_{SM}(Q) \leq (\sqrt{R_{SM}(Q)} + \sqrt{E_{S_Q}((\Delta y)^2)} + A)^2 + \varepsilon$$

$$\text{i.e.,} R_{SM}(Q) = R^*_{SM}(Q) \qquad (29)$$

Where $\varepsilon = B(\sqrt{\ln \eta / (-2N)})$, E_{S_Q}, A, Δy, N and B denotes the stochastic sensitivity measure of RBFNN, difference between the maximum and minimum values of target outputs, output perturbation, the number of training samples and maximum possible value of the MSE. Here MSE is the mean square error i.e. the measure of the difference between the classifier f_θ and the mapping function F. Stochastic sensitivity measure can be calculated as follow [9].

$$E\, S_Q((\Delta y)^2) = 1/3Q^2 \sum_{j=1}^{M} \upsilon_j + 0.2/9\, Q^4\, n \sum_{j=1}^{M} \zeta_j \qquad (30)$$

Where M denotes the number of hidden neurons. Here $s_j = \| x - u_j \|^2$, then we have,

$$\upsilon_j = \varphi_j \left(\sum_{i=1}^{n} (\sigma^2_{x_i} + (\mu_{xi} - \mu_{ji})^2) / \upsilon_j^4 \right. \qquad (31)$$

$$\zeta_j = \varphi_j / \upsilon_j^4 \qquad (32)$$

$$\varphi_j = (w_j)^2 \exp((\operatorname{var}(s_j)/2\upsilon_j^4) - (E(s_j)/\upsilon_j^2)) \qquad (33)$$

$$\operatorname{var}(s_j) = \sum_{i=1}^{n} \begin{pmatrix} E_D\left[(x_i - \mu_{x_i})^4\right] - (\sigma^2_{x_i})^2 + \\ 4\sigma^n_{x_i}(\mu_{x_i} - u_{ji})^2 \\ + 4E_D\left[(x_i - \mu_{x_i})^3\right](\mu_{x_i} - u_{ji}) \end{pmatrix} \qquad (34)$$

$$E(s_j) = \sum_{i=1}^{n} \left(\sigma^n_{x_i} + (\mu_{x_i} - u_{ji})^2 \right) \qquad (35)$$

Where u_j and v_j denote the center and width of the j^{th} RBFNN hidden neuron, w_j be the weights between the j^{th} hidden neuron and its corresponding output neuron, μ_{x_i} and $\sigma^2_{x_i}$ be the expectation and variance, u_{ji} denotes the ith input feature of the jth center of the hidden neuron and D the training data set.

Also the other architecture selection methods such as cross validation, sequential learning and ad-hoc methods [9] yields best classification accuracy but only with fewer hidden neurons and less training time. This paves way for the usage of the Localized Generalization Error Model (L-GEM).

5. Results and Discussion

5.1 Image set

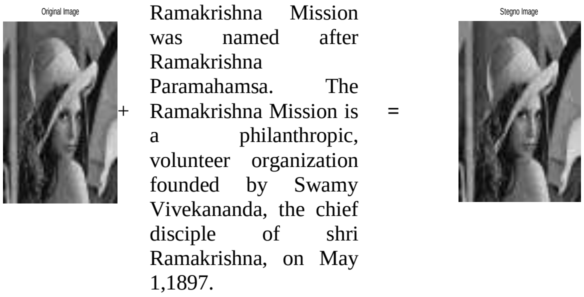
In our experiment, 1000 images were downloaded from http://www.freefoto.com ,1000 images from BROWS 2 image database and 1000 images from ucid database. All these 3000 images were joint to form a new image database. All these images were resized to 256 ×256 from the center of the original images.

About 80% of the images were used for training and 20% images were used for testing. Though all the images were color images we have converted them into gray scale images in our experiment. Figure 2 shows some of the sample images used in this experiment.

Fig. 2 Sample Images used in this Experiment

5.2 Stego Image Generation

Stego images were generated by using four embedding algorithms namely, MB1[19], MB2[20], F5[14] and JSteg[16]embedding algorithm at four different embedding rates:5%, 10%, 15%, and 20% bits per non zero AC coefficients. Figure 3 shows the stego image generated using JSteg Embeding Algorithm. The emdedded message used in this experiment is text and images.



Ramakrishna Mission was named after Ramakrishna Paramahamsa. The Ramakrishna Mission is a philanthropic, volunteer organization founded by Swamy Vivekananda, the chief disciple of shri Ramakrishna, on May 1,1897.

Fig.3 Stego Image generated using JSteg Embeding Algm

5.3 Experimental Results

In our experiment we have evaluated the detection accuracy by varying the feature set. We have employed markov features proposed in [22] and modified markov features proposed in this paper. The classifier used is RBFNN with Localized Error Generalization Model. In the proposed method the threshold value is set to 4. Experimental results show that the detection accuracy of the proposed method is better than the markov features proposed in [22]. The proposed method is tested with MB1, MB2, F5 and JSteg algorithm. The table 1 shows the results obtained in our experiment. The detection accuracy of the method that employed modified markov feature is dominant than the features proposed in [22].

6. Conclusion

In this paper, we improve the steganalysis performance by expanding the Markov process to both DCT and DWT domains and applying the L-GEM. based RBFNN. The neural network RBFNN is trained with several training images in online. The percentage of identifying hidden information is more than 98% when compared with the previous work. The high performance of this algorithm shows that it can be used as an important tool in the world of steganalysis for the detection of stego images. Future work may improve the feature extraction by investigating third order markov chain and also merge some more statistics of DCT coefficient to improve the detection accuracy of the blind steganalysis.

Embedding Algorithm	Embedding Rate	Modified markov features (This Paper)	Markov features in [22]
MB1	5%	98.9%	98.5%
	10%	99.1%	98.8%
	15%	99.4%	99.1%
	20%	99.9%	99.2%
MB2	5%	96.2%	92.6%
	10%	98.1%	94.8%
	15%	98.9%	96.1%
	20%	99.5%	98.8%
JSTEG	5%	95.4%	94.71%
	10%	97.9%	96.77%
	15%	98.89%	98.23%
	20%	99.88%	99.46%
F5	5%	98.4%	96.2%
	10%	98.2%	97.4%
	15%	98.8%	98.1%
	20%	99.4%	98.6%

Table 1. Comparison of Detection Accuracy of Modified markov features and Original markov features

References

[1] R. Chandramouli , M. Kharrazi and N. menon, “Image Steganography and Steganalysis: Concepts and Practice”, Springer-Verlag, Lecture Notes in Computer Science, Digital Watermarking, Vol. 2939, pp. 204-211, 2004.

[2] Kang Leng Chiew, Josef Pieprzyk "Blind Steganalysis : A Countermeasure for Binary Image Steganography". International Conference on Availability, Reliability and Security, 2010

[3] Alondra Gabriela Hernandez Chamorro and Mariko Nakano Miyatake "A New Methodology Of Image Steganalysis including for JPEG Steganography", Electronics and Automotive Mechanics Conference, 2010

[4] Wenqiong Yu, Zhuo Li, Lingdi Ping "Blind Detection for JPEG Steganpgraphy" International Conference on Networking and Information Technology, 2010

[5] Qingzhong Liu, Andrew H.Sung, mengyu Qiao, Zhongxue Chen, Bernardete Ribeiro "An Improved Approach To Steganalysis of JPEG Images", Information Sciences, Vol. 180, pp 1643-1655, 2010

[6] Mei-Ching Chen, Sos S. Agaian, C. L. Philip Chen, Benjamin M. RodRiguez "Steganography Detection Using RBFNN",International Conference on Machine Learning and Cybernetics, pp. 3720-3725, 2008

[7] Yun Q. Shi, Chunhua Chen, Wen Chen "A Markov Process Based Approach to Effective Attacking JPEG Steganography", Information Science, Vol. 180, pp. 1643-1655, 2010

[8] Tomas Pevny, Jessica Fridrich "Merging Markov and DCT Features for Multi-Class JPEG Steganalysis", In Proceedings of SPIE : Security, Steganography and Watermarking of Multimedia Contents IX, San Jose, CA, USA, 2007

[9] Daniel S. Yeung, Wing W. Y. Ng, Defeng Wang, Eric C. C. Tsang, Xi-Zhao Wang,"Localized Generalization Error Model and Its Application to Architecture Selection for Radial Basis Function Neural Network", IEEE Trans. On Neural Networks, Vol.18, 1294-1305, 2007

[10] Siewi Lyu, Hany Farid "Steganalysis Using Higher-Order Image Statistics", IEEETrans. On Information Forensics and Security, Vol. 1, pp. 111-119, 2006"

[11] Jennifer Davidson, Clifford Bergman and Eric Barlett, "An Artificial Neural Network for Wavelet Steganalysis" Proc. of SPIE : the International Society for Optical Engineering , Vol 5916, Mathematical Methods in Pattern and Image Analysis, pp. 1-10, 2005

[12] Siewi Lyu, Hany Farid "Steganalysis Using Color Wavelet Statistics and One-Class Support Vector Machines", In Proc. SPIE Symp. Electronic Imaging, 2004

[13] Ismail Avcibas, Nasir Memon, Bulent Sankur "Image Steganalysis With Binary Similarity Measures", In Proc. of 2002 IEEE International Conference on Image Processing, Vol. 3, pp.645-648, 2002

[14] Andreas Westfeld"F5: A Steganographic Algorithm, High Capapcity Despite Better Steganalysis" I.S. Moskowitz (Ed.) : IH 2001, LNCS 2137, pp. 289-302, 2001

[15] N. Provos, "Defending against Statistical Steganalysis", 10th USENIX Security Symposium, Washington DC, USA, 2001.

[16] D. Upham, Jsteg. Available from: ftp://ftp. funet.fi/ pub/crypt/steganography/, 2002.

[17] J. Fridrich, "Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes," in Information Hiding. Springer, 2005, pp. 67–81.

[18] J. Fridrich, M. Goljan, and D. Hogea, "Steganalysis of JPEG images: Breaking the F5 algorithm," Lecture Notes in Computer Science, pp. 310–323, 2003.

[19] P. Sallee, "Model-based steganography," Digital Watermarking, pp. 254–260, 2004.

[20] P.Sallee, " Model Based methods for Steganography and Steganalysis", International Journal of Image and Graphics, Vol. 5, No. 1, 167-189,2005

[21] S.Hetzl, "Steghide" http:// Steghide. sourceforge.net/, 2003.

[22] Wing W.Y. Ng, Zhi-Min He, Patrick P.K. Chan, Daniel S. Yeung, " Blind Steganalysis With High-Generalization Capability for Different Image Databases Using L-GEM", In Proc of the 2011 International Conference on Machine Learning and Cybernetics, Gullin, 10-13 July, 2011

[23] I. Avcibas, N. Memon, and B. Sankur. Steganalysis using image quality metrics. In E. Delp and P. W. Wong, editors, In Proc. of SPIE Electronic Imaging, Security and Watermarking of Multimedia Contents III, volume 4314, pages 523–531, 2001.

[24] Harmsen, J. and Pearlman, W., "Higher-order statistical steganalysis of palette images," In Security and Watermarking of Multimedia Contents V, Proc. SPIE 5020, 131–142 (2003).

[25] Ker, A., "Steganalysis of LSB matching in grayscale images," IEEE Signal Processing Letters 12(6), 441–444, (2005).

[26] Xuan, G., Shi, Y., Gao, J., Zou, D., Yang, C., Zhang, Z., Chai, P., Chen, C., and Chen, W., "Steganalysis based on multiple features formed by statistical moments of wavelet characteristic functions," In Proc. 7th Information Hiding Workshop, Springer LNCS 3727, 262–277 (2005).

[27] K. Sullivan, U. Madhow, S. Chandrasekaran, and B.S. Manjunath. Steganalysis of spread spectrum data hiding exploiting cover memory. In E. J. Delp and P. W. Wong, editors, Proc. SPIE, Electronic Imaging, Security, steganography, and Watermarking of Multimedia, Contents VII, volume 5681, pages 38{46, San Jose, CA, January 16{20, 2005.

[28] http://bows2.gipsa-lab.inpg.fr/

[29] http://www- staff.lboro. ac.uk /~cogs/ datasets /UCID

[30] http://www.freefoto.com