Volume 6, Issue 2, February 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Performance Evaluation of Universal Steganalysis using Machine Learning Tool

Swagota Bera
Associate Professor, Dept. of E&Tc.
SSIET, Durg, India

Dr. Monisha Sharma
Professor, Dept. of E&Tc.
FET, SSTC, Bhilai, India

Abstract-This paperreprésentés an blindsteganalysisusingtwostepmarkov'sprocessby evaluating transition probability matrix for the JPEG images. The variations in the statistical parameter is enhanced by calculating the features from the difference DWT 2-D arrays.This parameter captures the variations caused by JPEG steganography.The performance parameters are evaluated for the detection method for the well-known JPEG steganographic schemes Jsteg, F5, Outguess with the help of ROC (Receiver Operating Curve).The detection performance isevaluatedusing machine learningtoolWEKA.The support vector machine and bayasianclassifiers are used

Keywords- Steganography, Steganalysis,DWT, SVM, Stego Image, Cover Image

I. INTRODUCTION

The hiding of secret data in another data is known as steganography. The data may be an image, video,audio or text.Using various coding scheme the purpose can be fulfilled. The data can be hidden directly in the image or in the transformed value of image. If the data hiding is done after applying any transformation such as DCT, DWT and quantization to the image pixel, comes under the category of transform domain steganography. The JPEG 2000 accepted DWT along with DCT as transformation algorithm. Since JPEG (Joint Photographic Expert Group) format is the most dominant image format for image storage and exchange at this time, the JPEG steganography is attracting attention of the researcher. FourJPEG steganographic methods, i.e., Outguess [1], F5 [2], Jsteg [11] and DWT [12] is used for generating stego image. Jsteg [11] is JPEG hiding technique in which the zero and one coefficient is not used for hiding. Outguess [1] is a universal steganographic scheme that embeds hidden information into the redundant bits of data sources. It preserves the global histogram of BDCT. It adjust untouched coefficient to preserve the histogram. F5 [2] works on JPEG by modifying the block-DCT coefficients to embed messages. This technique is based on straddling and matrix coding.Straddling scatter the message as uniformly distribution and matrix coding improves embedding efficiency. DWT based steganography [12] hides the secret data bits in the wavelet coefficients such that the global histogram is preserve after hiding.

The reverse process of hiding that is the detection of hidden data is known as steganalysis.Since the startup of the hiding technique was implemented for the antisocial purpose. So, steganalysiswill be a good tool to save our society and country. One approach steganalysis method specific to a particular steganographic algorithm known as embedding algorithm based steganalysis techniques. The other technique is more general class of steganalysistechniques that can be implanted for any hiding algorithm which is known as universal or blind steganalysis techniques.

Blind Steganalysis can be implemented on the image based on the fact that embedding techniques affect different aspects of images. These aspects of the image are mathematically explained by statistical parameters known as image features. Features of typical natural images which can get violated when an image undergoes some embedding process. Hence, designing a feature classification based universal steganalysis technique consists of tackling two independent problems. The first is to find and calculate features which are able to capture statistical changes introduced in the image after the embedding process. The second is coming up with a strong classification algorithm which is able to maximize the distinction captured by the features and achieve high classification accuracy.

The paper is organized as follows. In literature review, the feature generation techniques and its domain are discussed from the various research papers. Then in methodology section, an overview of the proposed technique is discussed and then inimage statistics section, the image feature extraction technique is discussed in detail with mathematical formulae and classification technique is also discussed. In the experiments and results section, the classifier result for the proposed technique is shown along with the comparison performance result with the Ref.[4] , Ref.[7] and Ref.[14] performance result. Finally conclusion is derived.

II. LITERATURE REVIEW

Survey of some latest research papers in the present field is done [25, 28]. The research in this field is started from 1995. A brief introduction is given about the papers .The research paper in which the steganalysis techniquesis related to the work in this paper is only discussed.

Different approaches are given by the various researchers for feature extraction from images. The authors argue that most of the specific steganalysis techniques concentrate on first order statistics, i.e. histogram of DCT coefficients. Quadratic mirror filters (QMF) are used to decompose the image, after which higher order statistics such as mean, variance, kurtosis, and skewness are calculated for each subband. Also the error obtained from an optimal linear predictor of coefficient magnitudes of each sub band is used as a second set of features. In all the above methods, the calculated features are used to train a classifier, which in turn is used to classify clean and stego images. Different classifiers have been employed by different authors; Ascribes uses a MMSE Linear predictor, whereas Farad uses a Fisher linear discriminate and also a Support Vector Machine (SVM) classifier. SVM classifiers seem to have much better performance in terms of classification accuracy compared to linear classifiers since they are able to classify non-linearly separable features [19, 20, 21].

Steganalysis can also be classified based on the detection parameters .If the detection is done in the basis of the differences in the visual texture of the stego image and cover image then known as visual attacking whereas if the detection is done in the basis of the variation in the statistical parameters of the stego image and cover image the known as the statistical attacking. These attacking technique need the information of cover image and stego image. The universal steganalysis is better technique in which the technique can be implemented to any randomly incoming images and detection can be done. Any portion of the incoming image may alter after applying the detection algorithm. If after removing the noise effect the alteration remains then it is detected that the secret data is hidden in it. If the detection result indicate the presence of hidden information , then the analytic will try to recover the secret data by applying the decoding algorithm in the hit and trial method. Prediction accuracy can be interpreted as the ability of the measure to detect the presence of a hidden message with minimum error on average. The feature should be independent on the type and variety of images supplied to it [22, 23, 24].

The steganography and steganalysis has already discussed in the previous survey report [25]. Few Image Statistical and visual steganalysis techniques are implemented and discussed in previous paper [26, 27].

III. METHODOLOGY

In the proposed technique, using Ref. [7] the two step markov features are used as statistical features and from the same paper calibration technique is also implemented. Using Ref.[6], the prediction technique is implemented which minimize the effect of the noise. So, the proposed technique includes calibration, prediction, and higher order feature extraction using two step markov's process.

All the techniques are implemented in the DCT domain of the image.The image DCT coefficients are divided in the small blocks of size 8 x 8 .The statistical features exploits the correlation between the image pixels within these image blocks which is known as intra block relationship.

The difference matrix between the pixel and its four neighborhoodpixel values for all the blocks are generated and from these difference matrices, the two step transition probability matrix is evaluated known as two step markov'sprocess. The proposed method is implemented to attack the advanced JPEG steganographic methods.

Finally the performance of proposed detectiontechnique is analyzed with support vector machines (SVM) and Naïve Bayes as classifier by conducting experiments over a diverse data set of 4000 JPEG images for each technique. The comparison result is demonstrated and discussed for the proposed scheme. The proposed scheme is represented in Fig 1.

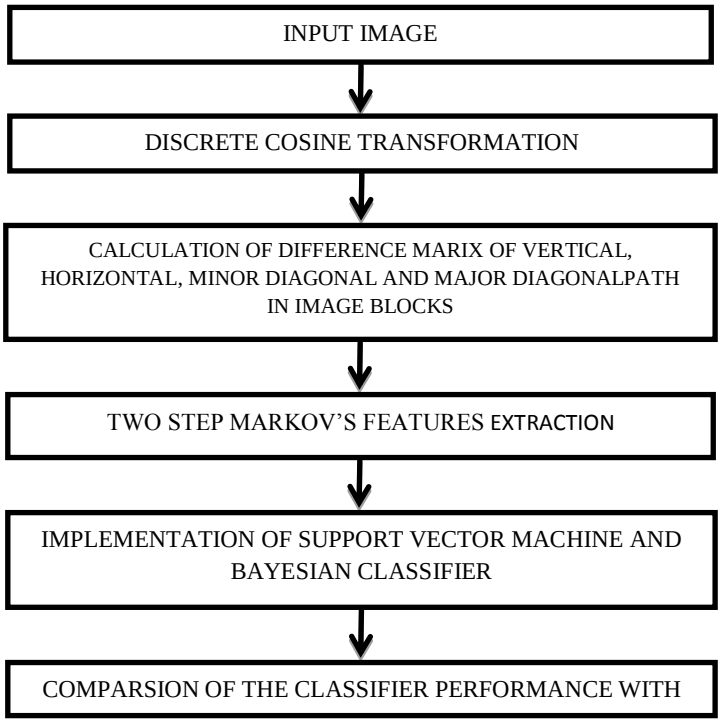


Fig 1.Block Diagram of the Proposed Scheme

IV. IMAGE STATISTICSUSING DISCRETECOSINE TRANSFORM

A. Two Step Markov's Feature

The image matrix is divided into blocks of size 8 X 8 and on these blocks DCT and quantization is applied. There exist relationships between the image coefficients. If these image coefficients get change due to data hiding leads to anomalies in the overall statistical correlation. To find the correlation between the coefficients, the difference between the neighboring coefficients is calculated and then the transition probability matrices is calculated .The transition probability matrices are then calculated from these difference matrices. A two-step transition probability matrix is calculated using equation (3) because it can find a better correlation between the neighboring coefficients. Let Tf, Tr ,Tu , Td are the four transition probability matrices.

$$\mathrm{Tf(I,j,k)} = \frac{\sum_{b=1}^{Bt}\sum_{u=1}^{6}\sum_{v=1}^{8}\delta\left(\mathrm{Ch}(u,v)=i,\mathrm{Ch}(u+1,v)=j,\mathrm{Ch}(u+2,v)=k\right)}{\sum_{b=1}^{Bt}\sum_{u=1}^{7}\sum_{v=1}^{8}\delta\left(\mathrm{Ch}(u,v)=i,\mathrm{Ch}(u+1,v)=j\right)}$$

$$\mathrm{Tr(i,j,k)} = \frac{\sum_{b=1}^{Bt}\sum_{u=1}^{8}\sum_{v=1}^{6}\delta\left(\mathrm{Cv}(u,v)=i,\mathrm{Cv}(u,v+1)=j,\mathrm{Cv}(u,v+2)=k\right)}{\sum_{b=1}^{Bt}\sum_{u=1}^{8}\sum_{v=1}^{7}\delta\left(\mathrm{Cv}(u,v)=i,\mathrm{Cv}(u,v+1)=j\right)}$$

$$\mathrm{Tu\ (i,j,k)} = \frac{\sum_{b=1}^{Bt}\sum_{u=1}^{6}\sum_{v=1}^{6}\delta\left(Cd(u,v)=i,Cd(u+1,v+1)=j,Cd(u+2,v+2)=k\right)}{\sum_{b=1}^{Bt}\sum_{u=1}^{7}\sum_{v=1}^{7}\delta\left(Cd(u,v)=i,Cd(u+1,v+1)=j\right)}$$

$$\mathrm{Td(I,j,k)} = \frac{\sum_{b=1}^{Bt}\sum_{u=1}^{8}\sum_{v=1}^{6}\delta\left(Cm(u,v)=i,Cm(u-1,v+1)=j,Ch(u-2,v+2)=k\right)}{\sum_{b=1}^{Bt}\sum_{u=1}^{8}\sum_{v=1}^{7}\delta\left(Cm(u,v)=i,Cm(u-1,v+1)=j\right)} \qquad (1)$$

Where Bu and Bv denote the number of blocks in horizontal and vertical direction. δ = 1 if the arguments are satisfies. The threshold value taken is -4 to 4. To reduce the dimensionality, the average value is taken.

$$M = \frac{\mathrm{Tf+Tr+Tu+Td}}{4} \qquad (2)$$

The above transition probability matrix M is calculated for all the four discrete wavelet bands. So, in total 324 statistical features are calculated.

B. Data Classification Technique

Data classification comes under the machine learning. SVM is the robust classifier for two class classification. Support Vector Machine is a classification and regression prediction tool that uses machine learning theory to maximize predictive accuracy while automatically avoiding over fit to the data. Naive Bayes classifiers are a family of simple probabilistic classifiers based on applying Bayes' theorem with strong (naive) independence assumptions between the features.In Fig 2. The block diagram represents the classification model.

Cross validation is used while selecting the training and testing dataset. Implementing this technique each image of the dataset is used as training data and testing data. From the information of the confusion matrix the classifications parameters can be calculated using TN (True Negative), FP (False Positive),FN (False Negative), TN (True Negative) value. The parameters discussed here are:

$$\text{Sensitivity} = \frac{TP}{TP+FN}$$

$$\text{Accuracy} = \frac{\mathrm{TP+TN}}{\mathrm{TP+FP+FN+TN}}$$

$$\text{Precision} = \frac{TP}{FP+TP} \qquad (3)$$

The performance of a steganalysis classifier can also be visualized by ROC(Receiver Operating Characteristic) curve [13].

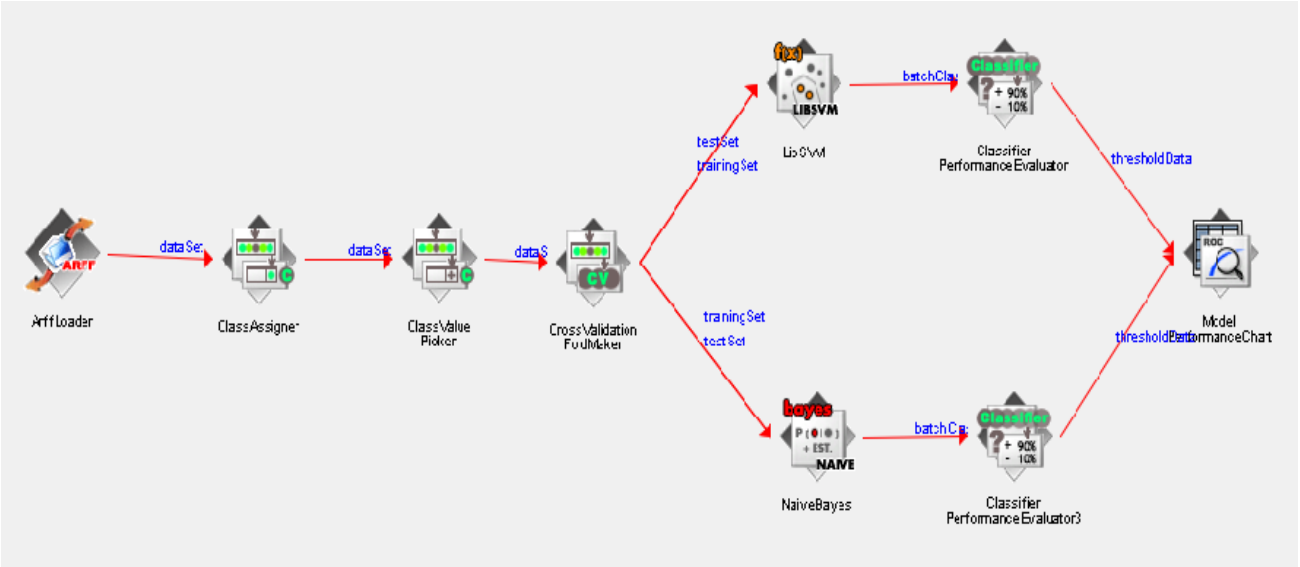


Fig 2. Block Diagram of Classification Model

V. EXPERIMENTS AND RESULTS

A. Image set

An image set consisting of 4000 JPEG images with quality factors ranging of 90 is used in our experimental work. Each image was cropped (central portion) to the dimension of either 640 X 480. Some sample images are given in Fig 3.

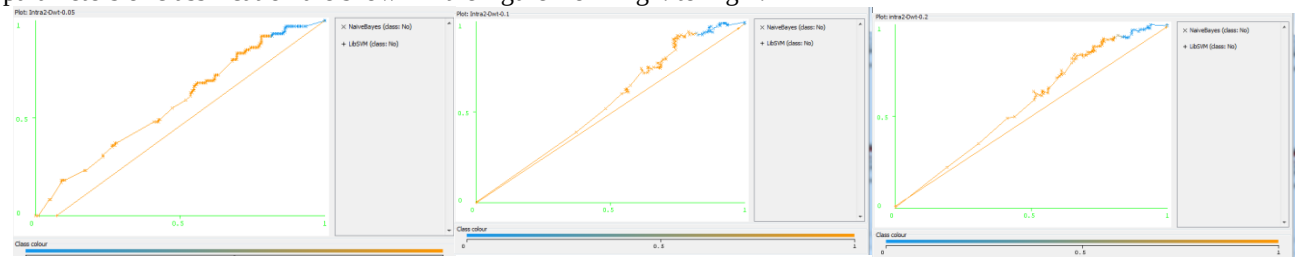
Fig 3. Some Sample Images used in this Experimental Work

B. Stego images generation

The images from the database are gone through various well known JPEG hiding techniques. They are Outguess, F5, Jsteg and DWT based of different capacities 0.05, 0.1, 0.2 bpnc. The texts and images are hidden in the image dataset using the above algorithm [1, 2, 11, 12].

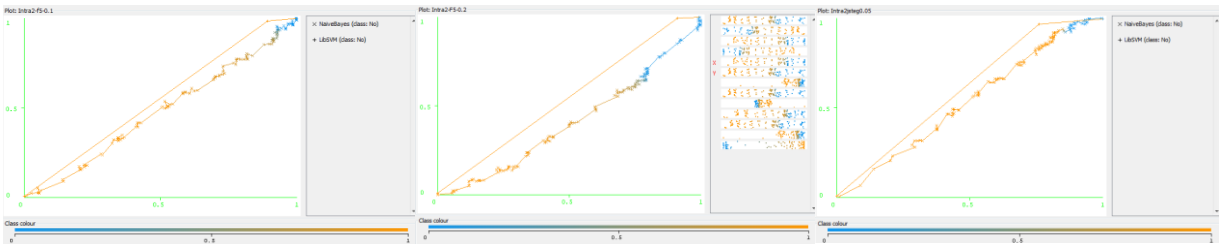
C. Steganalysis on the stego image database

Matlabcode is generated for implementing the proposed scheme.The obtained features are used for the SVM classification with the help of WEKA data mining software. The cross-validation is selected for the better result [18].
The images from the database have been used for both training and testing of the SVM classifier. The performance parameters of classification are shown in the figure from Fig4. to Fig 7.



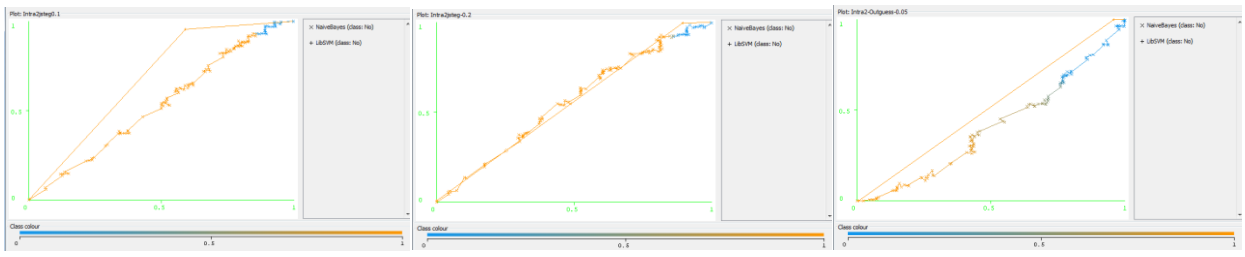
0.05 0.1 0.2

Fig 4. ROC curve for DWT Based Stego Images for 0.05 bpnc, 0.1 bpnc and 0.2 bpnc



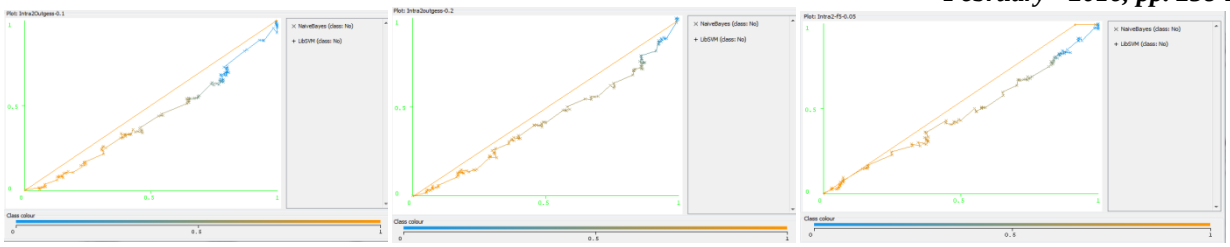
0.05 0.1 0.2

Fig 5. ROC curve for F5 Based Stego Images for 0.05 bpnc, 0.1 bpnc and 0.2 bpnc



0.05 0.1 0.2

Fig 6. ROC curve for JstegStego Images for 0.05 bpnc, 0.1 bpnc and 0.2 bpnc



0.05 0.1 0.2

Fig 7. ROC curve for Outguess Stego Images for 0.05 bpnc, 0.1 bpnc and 0.2 bpnc

In all the figures ROC (Receiver Operating curve) for both Bayes Classifier and Support Vector Machine Classifier are represented.

VI. DISCUSSION AND CONCLUSIONS

For developing Jsteg [11] stego image set, the optimized quantization table is used on the Block DCT coefficient. For DWT based, F5, Jsteg and Outguess hiding technique, the detection accuracy is higher than [4] and [7] but slightly higher than [14].It is observed that the area of ROC curve is more in all the case of bayesclassifier for the DWT Based Stego image. But for the rest Support Vector machine performance is better. As per the literature survey, it is observed that the use of Support Vector Machine is very common classification technique adopted for blind steganalysis in transform domain.

ACKNOWLEDGMENT

Appreciation goes to Dr. AyushSinghal Postdoctoral ResearchFellow, NCBI, National Institute of Health, Maryland, PhD, M.Sc (University of Minnesota, Twin Cities, MN, USA) andB.Tech (IIT Roorkee, India) for giving me the information about weka data mining tool.

REFERENCES

[1] (2010) The googlewebsite.[Online].Available :http:// www. outguess.org.
[2] (2010) The google website.[Online].Available:http://www.rn.inf.tu-dresden.de/ ~westfeld/f5.html.
[3] S. Lyu and H. Farid, Detecting Hidden Messages using Higher-Order Statistics and Support Vector Machines, Information Hiding, Springer, pp. 340-354, 2003.
[4] J. Fridrich, Feature BasedSteganalysisfor JPEG Images and its implications for Future DesignofSteganographicSchemes,InformationHiding, Springer, pp. 67-81,2005.
[5] H.Farid and S. Lyu, Steganalysisusing Higher- OrderImage Statistics, IEEE Transactions on Information Forensics and Security, Vol.1,Issue.1, pp. 111– 119,2006.
[6] ChenChunhua, Y. Q. Shi,Chen Wen and XuanGuorong, StatisticalMomentsBasedUniversalSteganalysisusingJPEG 2-D Array and 2-D Characteristic Function ,IEEE international conference on Image Processing, pp. 105-108, 2006.
[7] Y.Q .Shi, C.Chen. and W. Chen, A Markov Process Based Approach to Effective Attacking JPEG Steganography, LectureNotes in Computer Science, Information Hiding, Springer, pp. 249–264, 2007.
[8] D.Fu, Y.Shi , DekunZou and GuorongXuan , JPEG Steganalysis using Empirical Transition Matrix in Block DCT Domain,IEEEWorkshop on Multimedia Signal Processing, pp. 310-313,2007.
[9] C. Chen and Y. Shi,"JPEG Image Steganalysis Utilizing both Intrablockand InterblockCorrelations",IEEE InternationalSymposium on in Circuits and Systems, 2008, Page No. 3029- 3032.
[10] M. Kumar , Steganography andSteganalysis of Joint Picture Expert Group (JPEG) Images, Ph.D.Thesis, University of Florida, 2011.
[11] S. Bera. and M. Sharma, Frequency Domain Steganography System using Modified Quantization Table, International Journal of Advanced and Innovative Research, Vol.1, Issue.7, pp. 193-196, 2012.
[12] S. Bera. and M. Sharma, Development and Analysis of Stego Imageusing Discrete Wavelet Transform, International Journal of Science &Research, Vol. 2, Issue .1, pp. 142-148, 2013.
[13] F.G. Mohammadi and M.S.Abadeh, Recent Advances in teganography:ASurvey of Data Mining Techniques in Steganalysis, InTechPublication, Croatia, Europe, ISBN-978-953-51-0840-5, Chapter.1, 2012.
[14] G.T. Kumar, R. Jithin and D. Shankar, Feature Based Steganalysis using Wavelet Decomposition and Magnitude Statistics, IEEEConference on Advances in Computer Engineering, pp. 298-300, 2010.
[15] S. Bera. and M. Sharma, Steganalysis of Real Time Imageby Statistical Attacks, International Journal ofEngineering Science and Technology, Vol. 2, Issue. 9, pp. 4397-4406, 2010.
[16] S. Bera. and M. Sharma, Steganalysis of theImage by Visual and Statistical Attack , i- manager'sJournalof Electronics Engineering,Vol.1, Issue .2, pp. 49-55, 2010.
[17] S. Bera. and M. Sharma, (2012), A Review on Blind Still ImageSteganalysis Techniques usingFeatures Extraction and Pattern Classification Method, International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol. 2,Issue. 3, pp.117-135, 2012.
[18] (2015) Thegoogle website.[Online].Available:http://www.cs.waikato.ac.nz/ml/weka.

[19] Anonymus "*What is Steganography*?" www.tech-faq.com/steganography.html.

[20] ApostolMaile,LasunZhanna,SardinasAna,YigitYasemin ," *Image Encryption Using LSB/MSB* ", Term Project, CpE-462, 04/30/02,April 2002.

[21] Anonymus "*Miscellaneous Steganographic*" ,scien.stanford.edu/class/ psyh221/project /05/vvikram/stegomisc.htm.

[22] Jahne,Bernd,Digital Image Processing, "*Concepts,Algorithms ,an Scientific Applications*" II nd ed., Springer-Verlag,1993.

[23] R. B. Wolfgang, E. J. Delp ,"*A watermark for digital Images*", in International Conference on Images Processing,Lausanne,Switzerland, , IEEE, pp. 219–222, 16–19 Sept. 1996.

[24] Mehdi Kharrazi1, Husrev T. Sencar, and NasirMemon,"*Image Steganography:Concepts and Practices*" Department of Electrical and Computer Engineering, Department of Computer and Information Science Polytechnic University, Brooklyn, NY 11201,USA fmehditaha, memong@isis.poly.edu,www.ims.nus edu.sg preprints/2004-5.pdf.

[25] SwagotaBera andMonishaSharma,"*Survey on Steganographic Techniques &Steganalysis*", National Conference in Advances in electronics & Telecommunication Technologia,vision- 2020,IIM,28-29, Pune, India, Oct 2007.

[26] Monisha Sharma, SwagotaBera , "Steganalysis of Real Time Image by Statistical Attacks", International Journal of Engineering Science and Technology ,Vol. 2(9), 4397- 4406, 2010.

[27] Monisha Sharma, SwagotaBera , "Steganalysis of the Image by Visual and Statistical attack", in i-Manager's Journal of Electronics Engineering,ISSN-2229- 7286,Vol.1,No.2,Dec -2010,Feb-2011,P-49-55.

