Study of Effect of DCT Domain Steganography Techniques in Spatial Domain for JPEG Images Steganalysis

G.R. Suryawanshi
Research Scholar
DYPITE Pune

S.N. Mali, PhD
SITS Pune

ABSTRACT

Steganography is a technique of hiding secret data into digital images in different domain like frequency, spatial or wavelet. Data hiding in image change its statistical properties which leaves vulnerability for Steganalysis. In this paper a effective study is carried out for frequency domain Steganography and It's effects in spatial domain. Study shows that secret data embedding in frequency domain reflects significant changes in spatial domain w.r.t embedding algorithm. A set of feature is identified for the analysis of covert communication through the image.

Keywords

Steganalysis, Feature Extraction, Image Quality Measures (IQM).

1. INTRODUCTION

One of the most important challenges in information Forensic is to improve the performance of Steganalysis techniques and prevention of secrete information from outside world. It is also important to exchange secret information through internet without any interpretation by any Steganography techniques. Several Steganography techniques are available in literature which embeds the message in different domain like frequency, Spatial. Computer security, law enforcement, and intelligence professionals need the capability to both detect the use of digital Steganography applications to hide information and then extract the hidden information. The counter measures for malicious activity is Steganalysis whose ultimate aim is to detect the presence of secret communication. There are many approaches to differential Steganography techniques. The classification could be depends upon use of cover media or according to modification of cover while applied during embedding of messages. In this paper second approach is followed. fig 1 shows the classification of Steganography.

Detail classification of Steganalysis done by Arooj Nissar and A H Mir [1]. Generally the Steganalysis can be carried out by two different approaches Blind [2,3,4,5,6] and Targeted [7,8,9,10,11] Steganalysis. The goal of Steganalysis is to collect sufficient evidence about the presence of embedded message and to break the security of its carrier.

The recent attacks on Information System, Cyber Security and Cyber Forensics have become a primary concern for both governments and commercial industries. Attacker of information systems can potentially use sophisticated means to hide messages in cover media like images for covert communication. Identifying such communication must be automated in order to be able to effectively and partially monitor such behaviour. Our proposed work will give a right direction for the analysis of images for covert communication through statistical properties of digital image

1.1 Image Format

A digital image is produced through a process called digitization. Digitizing an image involves converting analogue information into digital information; thus, a digital image is the representation of an original image by discrete sets of points. Each of these points is called a picture element or pixel. Pixels are normally arranged in a two-dimensional grid corresponding to the spatial coordinates in the original image. The number of distinct colors in a digital image depends on the number of bits per pixel (bpp). Hence, the types of digital image can be classified according to the number of bits per pixel. There are three common types of digital image.

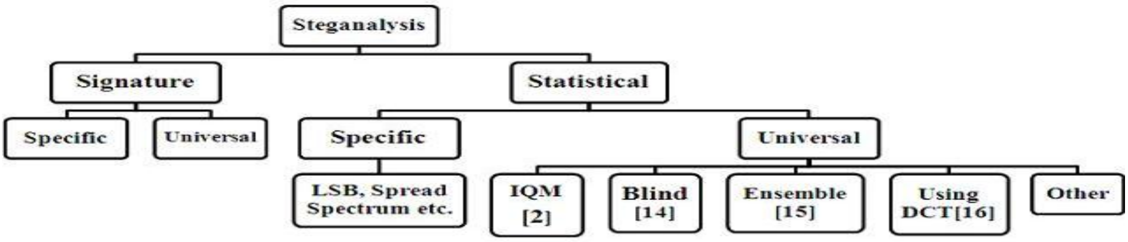


Fig 1 Classification of Steganography

- *Binary image*. In a binary image, only one bpp is allocated for each pixel. Since a bit has only two possible states (on or off), each pixel in a binary image must represent one of two colors. Usually, the two colors used are black and white. A binary image is also called a bi-level image.
- *Gray scale image*. A gray scale image is a digital image in which the only colors are shades of grey. The darkest possible shade is black, whereas the lightest possible shade is white. Normally, there are eight bits per pixel assigned for a gray scale image. This creates 256 possible different shades of grey.
- *Color image*. In general, a pixel in a color image consists of several primary colors. Red, green and blue are the most commonly used primary colors. Each primary color forms a single component called a channel, with eight

bits usually allocated for each channel, producing 24 bits per pixel. This corresponds to roughly 16.7 million possible distinct colors.

1.2 Spatial And Frequency Domain Images

In a general sense, an image (I) can be considered a result of the projection of a scene (S). The spatial domain image is said to have a normal image space, which means that each image element at location ℓ in image I is a projection at the same location in scene S. The distance in spatial domain corresponds to the real distance. A common example of the spatial domain image is BMP image. The frequency domain image has a space where each elements value at location ℓ in image I represents the rate of change over a specific distance related to the location ℓ. A popular frequency domain image is the JPEG image.

2 LITERATURE SURVEY

Following collection of statistical features can be found in literature from different domain. There are 26 image quality measures described by Avcibas [13] which are categorized in following group

1. Co-occurrence Matrix
2. Statistical Moments
3. Wavelet Sub bands
4. Pixel Difference

Co-occurrence Matrix, Sullivan et al. use an empirical matrix as the feature set to construct a Steganalysis [14]. The Steganalysis technique developed can detect several variants of spread-spectrum data hiding techniques [15,16] and perturbed quantization Steganography [13]. This empirical matrix is also known as a co-occurrence matrix. The feature set is stochastic and may not effectively capture the modification done by Steganography. Xuan et al. [17] constructed a better feature set from the co-occurrence matrices. Chen et al. developed a blind Steganalysis based on a co-occurrence matrix [18]. It is well known that direct use of a co-occurrence matrix as the feature will create an expansion of the matrix dimension. There is relationship between the discrete cosine transform (DCT) coefficients in intra- and inter-blocks of JPEG images. Intra-block correlation is the correlation between neighboring coefficients within a block; inter-block correlation measures the correlation between a DCT coefficient in one block and the coefficient of the same position in another block. Arrangement of the DCT coefficients should be in zigzag order in a block into a one-dimensional vector. For each block, only AC coefficients are considered while the DC coefficient is discarded. This is because normally DC coefficients are not changed in JPEG Steganography. Some coefficients with a high frequency of occurrence will be discarded. (i.e. coefficients with a value of zero). All the blocks in a JPEG image are scanned in a fixed pattern to form a new re-ordered block called a 2-D array. Only the magnitudes of the coefficients are used. *Statistical Moments,* In a different work [19], Xuan et al. developed an enhanced version, based on statistical moments. Enhancement is achieved with an additional level of wavelet decomposition. The authors of [18] raised the concern of precision degradation in the first-order statistic when a wavelet is used (i.e., the wavelet coefficients are floating points). Hence, the co-occurrence matrix (discrete integers) was used instead of wavelet decomposition. Inspired by the work in [20], Chen et al. enhanced and applied the statistical moments on JPEG image Steganalysis [21].

Wavelet sub bands, It is well known that natural images exhibit strong higher-order statistical regularities and consistencies. Thus, wavelet decomposition is often used to represent these characteristics for various image processing purposes. It is also well known that Steganography embedding significantly disturbs the characteristics of statistics. Hence, it is very natural to employ wavelet decomposition to detect disturbances. The first Steganalysis technique using wavelet decomposition was developed by Farid [22, 23]. In his work, quadrature mirror filters (QMFs) are used to decompose a given image into multiple scales and orientations of wavelet sub bands, obtaining nine wavelet sub bands. Lyu and Farid [23] extended their work to include phase statistics (in addition to their prior work with magnitude statistics). In their work, phase statistics are modeled using the local angular harmonic decomposition (LAHD). The LAHD can be regarded as a local decomposition of image structure by projecting onto a set of angular Fourier basis kernels.

Pixel Difference, Liu et al. consider the differential operation as high-pass filtering process when applied to images [24]. This is desirable as it can capture the small distortion caused by the embedding operation. In [24] the differential operation is defined as the pixel-wise difference between two neighboring pixels in the horizontal direction (similarly in the vertical direction). a transition probability matrix is computed. Thresholding is also utilized to achieve a balance between detection accuracy and computational complexity.

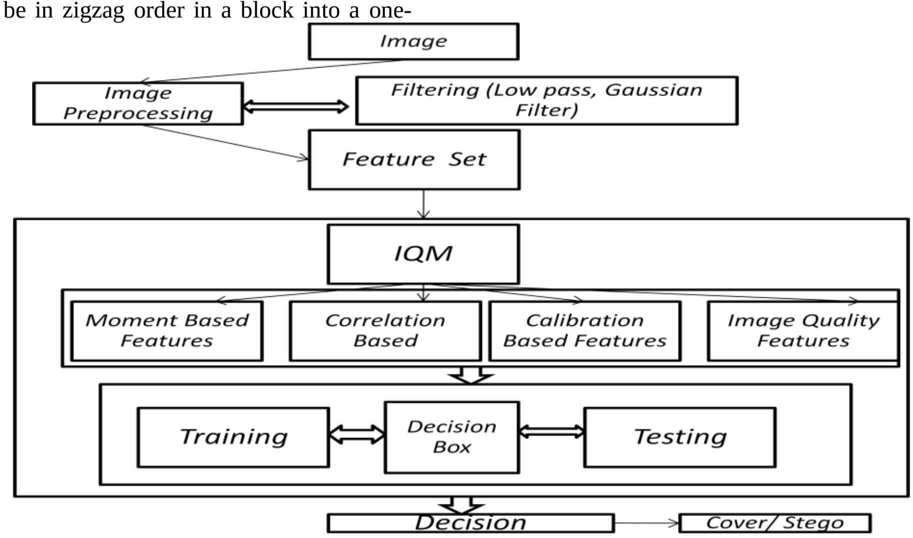


Fig 2 Proposed Frame work

3 PROPOSED FRAME WORK

Fig 2 shows architecture of proposed model which is pre-processing of images, Features extraction, Domain Classifier, Decision Box. Whereas Pre-processing, removes unwanted signals from cover images so that the high accuracy of classifier will be achieved. In pre-processing use of different filters are assumed i.e. low pass filter which remove high frequency and gives as good as original image. Also use of Gaussian filter is assumed in this pre-processing. Features extraction is the processes of constructing a set of discriminative statistical attributes from an image. In this part the prominent features extracted from given input. The set of that features used to classify the category of input image. Domain classifier classify the category of image to which is belongs to. There are different classifiers are available which has their own advantages like FLD, SVM, NN, Multivariate Regression. SVM is not scalable with respect to dimensionality of feature set. FLD is used for linear date set. Extended version of FLD is Exponential linear discriminator which is useful for high dimensional data set.

Feature extraction is a process of identifying the statistical features of digital images from different domain like spatial, frequency etc. The features are classified into different classes like pixel difference, correlation measures, content based measures, HVS based measures. Fig 3 shows the feature extraction process of digital image. Feature generation has been divided into two parts. First part generates the features and standardizes it with assigning rank to it. Whereas second part process on generated features for classification of it. It is required to identify the class of features

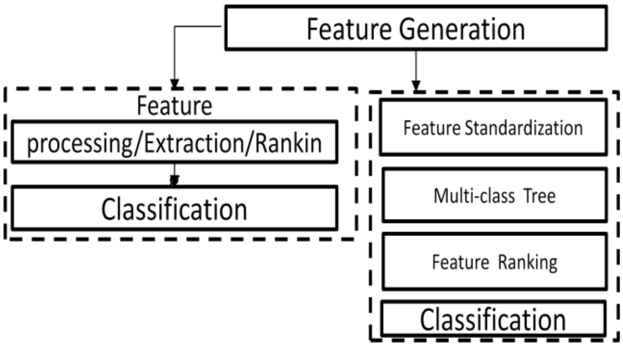


Fig 3 Feature Extraction

3.1 Pseudo code

```
X-> Read Image (I)
Y->Preprocessing on X
Divide Image into Blocks of Same Size 8x8
B= {b1, b2, b3,….}
Extract  Features from B
F= { Set of features w. r. t  B}
F= { Fspatial, Fedge,Fcorelation,Fspectral, ……….}
Fspatial->Pixel difference features D1-D7
Fedge -> E1-E3
Fcorelation -> C1-C3
Fspectral -> S1-S3
Fstatistical -> {SPAM,CC,CCPEV,Chan,SRM}
Fset= fusion of {fspatial,Fedge, Fcorelation, Fspectral}
All Feature vectors will be calculate and stored for training phase
FSet= {D1-D7,E1-E3,C1-C3,S1-S3, SPAM, CC, CCPE, Chan, SRM}
Frank-> Ranking of features
```

4. EXPERIMENTAL SETUP

BOSS base image dataset which contains 300 JPEG,PGM and BMP images each of 481x381, 512x512, 256x256 resolution respectively, with sizes varying from 23 KB to 111 KB, was used for experiment for preparing the training datasets. Out of the 300 images, 300 were used for preparing training as well as testing dataset used for preparing testing dataset. Out of the 300 training images, 33 images were used as clean images and the rest images were used for embedding text messages using the well known Steganography algorithms. Similarly from the test images, out of 100 images, 33 images were used as clean. The well known Steganography algorithms used for embedding text in training images were F5, Quickstego, StegHide, Four statistical features are calculated from 33 stego and cover images of different type. Calculated features are skweness, kurtosis, mean and standard deviation. Table 1 shows the details of dataset used

Table 1 Details of Dataset

SN	Type	Resolution	Size	Quantity	PSNR
1	Gray	512x512	256k	100	75
2	Color	481x321	603K	100	75
3	Color	256x256	256k	100	75

5. RESULTS

Calculated features in different embedding domain for different Steganography algorithms show the effect of change of Mean, Skewness, kurtosis and Standard Deviation. Fig 4 shows the relationship between mean and standard deviation. Value of mean of pixel is must be less than the standard deviation of any image for different embedding algorithms

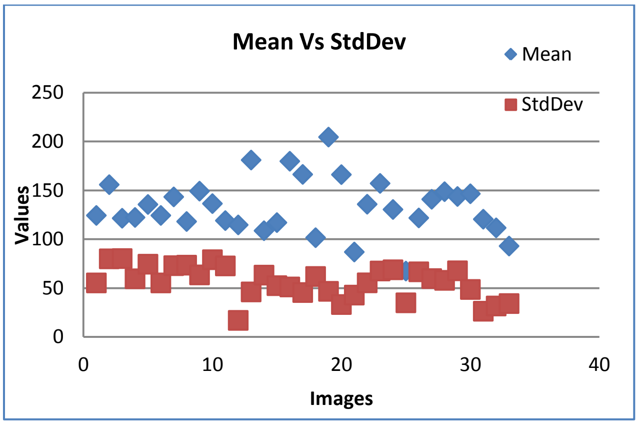
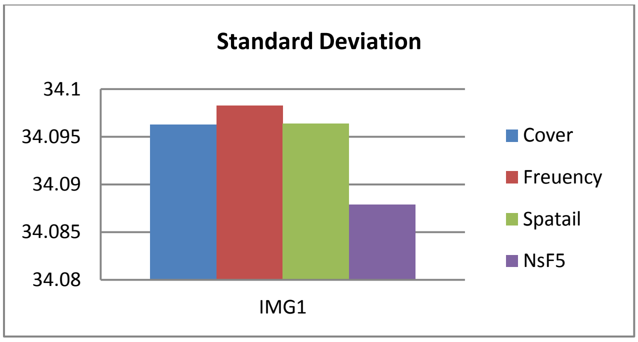


Fig 4 Mean vs Standard Deviation



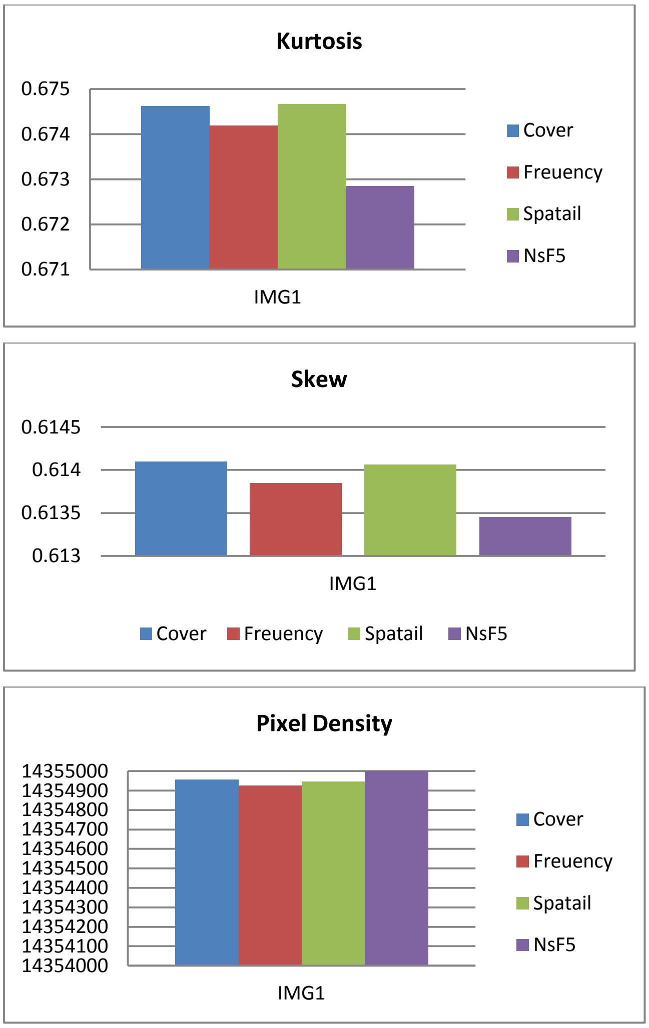


Fig 5 Effect of Steganography algorithms on Features

Effect of Frequency domain algorithm on statistical features of image is seen in this experiment. The prominent feature set is a vital key for analysis of image. In this experiment standard deviation, Mean, kurtosis, skewness and histogram analysis are selected for monitoring the effect of embedding algorithm on spatial domain of image. Fig 6 show the probability of changes with respect to DCT value of images and number of changes in DCT coefficient with respect to DCT value of image.

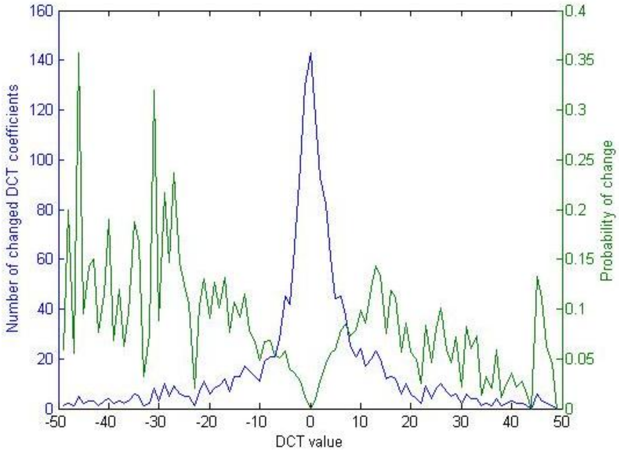


Fig 6 Probability of changes w.r.t. DCT value

6. CONCLUSION

Different domain Steganography algorithms leave the artifact in Stego images which will be used by analyzer for discrimination between cover and Stego images. Proposed work gives the direction not only in finding the relationship between features of different domain but also helps to identify prominent features with respect to domain. Experimental results show that the significant effect of DCT domain Steganography in Spatial domain by means of statistical properties of image. If image has zero DCT coefficients then the probability of changes will be high or vice versa. For further work, the selection of prominent features will be a challenging task. Feature set must be combination of different domains statistical properties which will be useful to identify different domain Steganography algorithms.

7. REFERENCES

[1] Arooj Nissar , A.H. Mir, "Classification of steganalysis techniques: A study," Digital Signal Processing 20 (2010) Elsevier, pp.1758–1770 ,2010.

[2] M.Chapman, G. Davida, and M. Rennhard, "A Practical and Effective Approach to Large-Scale Automated Linguistic Steganography," Proceedings of the Information Security Conference,, pp. 156-165, October 2001

[3] Udit Budhia, Deepa Kundur, and Takis Zourntos, "Digital Video Steganalysis Exploiting Statistical Visibility in the Temporal Domain", IEEE Transactions On Information Forensics And Security, Vol. 1, No. 4.,2006

[4] Jessica Fridrich, Member, IEEE, And Jan Kodovský, "Rich Models For Steganalysis Of Digital Images," IEEE Transactions On Information Forensics And Security, Vol. 7, No. 3, pp no. 868-882, 2012

[5] Min Wu, Member, IEEE, and Bede Liu, Fellow, IEEE ,"Data Hiding in Image and Video:Part I—Fundamental Issues and Solutions," IEEE Transactions on Image Processing, Vol. 12, No. 6, June 2003"

[6] Chunfang Yang, Fenlin Liu, Xiangyang Luo, and Bin Liu, "Steganalysis Frameworks of Embedding in Multiple Least-Significant Bits," IEEE Transactions on Information Forensics and Security, Vol. 3, No. 4, December 2008

[7] Yun Cao, Xianfeng Zhao, and Dengguo Feng, " Video Steganalysis Exploiting Motion Vector Reversion Based Features," IEEE Signal Processing Letters, Vol 19, No. 1, pp no 35-38, 2012

[8] Mengyu Qiao, Andrew H. Sung , Qingzhong Liu, "MP3 audio steganalysis," Information Sciences 231 Elsevier 123–134, 2013

[9] R. Sridevi, A. Damodaram and S.V.L. Narasimham, "Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key with Enhanced Security," Journal of Theoretical and Applied Information Technology, Vol. 5, No. 6, pp. no 768 – 771, June 2009.

[10] D. Kirovski and H. Malvar, "Spread spectrum Watermarking of Audio Signals," IEEE Transactions on Signal Processing, vol. 51, no. 4, pp. 1020 – 1033, April 2003.

[11] Tomáš Pevný, Jessica Fridrich, And Andrew D. Ker, "From Blind To Quantitative Steganalysis," IEEE Transactions On Information Forensics And Security, Vol. 7, No. 2, pp. no 445-454, 2012

[12] Jan Kodovský, Jessica Fridrich, "Ensemble Classifiers For Steganalysis Of Digital Media," IEEE Transactions On Information Forensics And Security, Vol. 7, No. 2, pp no. 432-444, 2012

[13] I. Avcibas, M. Nasir, and B. Sankur., "Steganalysis Based on Image Quality Metrics," IEEE 4th Workshop on Multimedia Signal Processing, pages 517–522, 2001

[14] K. Sullivan, U. Madhow, S. Chandrasekaran, and B. Manjunath, "Steganalysis for Markov Cover Data With Applications to Images," IEEE Transactions on Information Forensics and Security, 1(2):275–287, 2006

[15] R. J. Anderson, "Stretching the Limits of Steganography," 1st International Workshop on Information Hiding, 1174:39–48, 1996.

[16] R. J. Anderson and F. A. P. Petitcolas, "On the limits of Steganography," IEEE Journal of Selected Areas in Communications, 16(4):474–481, 1998

[17] S. Badura and S. Rymaszewski, "Transform Domain Steganography in DVD Video and Audio Content," IEEE International Workshop on Imaging Systems and Techniques, pages 1–5, 2007

[18] X.Chen, Y. Wang, T. Tan, and L. Guo, "Blind Image Steganalysis Based on Statistical Analysis of Empirical Matrix," International Conference on Pattern Recognition, 3:1107–1110, 2006

[19] G. Xuan, Y. Q. Shi, J. Gao, D. Zou, C. Yang, Z. Zhang, P. Chai, C. Chen, and W. Chen,"Steganalysis Based onMultiple Features Formed by Statistical Moments of Wavelet Characteristic Functions," 7th International Workshop on Information Hiding, 3727:262–277, 2005

[20] Y. Q. Shi, G. Xuan, D. Zou, J. Gao, C. Yang, Z. Zhang, P. Chai, W. Chen, and C. Chen, "Image Steganalysis Based on Moments of Characteristic Functions Using Wavelet Decomposition, Prediction-Error Image, and Neural," Network. IEEE International Conference on Multimedia and Expo, pages 269–272, 2005

[21] C. Chen, Y. Q. Shi, W. Chen, and G. Xuan, " Statistical Moments Based Universal Steganalysis using JPEG 2-D Array and 2-D Characteristic Function," IEEE International Conference on Image Processing, pages 105–108, 2006

[22] H. Farid, "Detecting Steganographic Messages in Digital Images," TR2001-412, Department of Computer Science, Dartmouth College, 2001

[23] S. Lyu and H. Farid, "Steganalysis Using Higher-Order Image Statistics," IEEE Transactions on Information Forensics and Security, 1(1):111–119, 2006.

[24] Z. Liu, L. Ping, J. Chen, J. Wang, and X. Pan, " Steganalysis Based on Differential Statistics," 5th International Conference on Cryptology and Network Security, 4301:224–240, 2006

[25] J. Harmsen and W. Pearlman, "Steganalysis of Additive-Noise Modelable Information Hiding," Proceedings of the SPIE on Security and Watermarking of Multimedia Contents V, 5020:131–142, 2003

[26] J. Fridrich, "Feature-Based Steganalysis for JPEG Images and its Implications for Future Design of Steganographic Schemes," 6th International Workshop on Information Hiding, 3200:67–81, 2004

[27] Pritesh Pathak, s. selvakumar, " Blind Image Steganalysis of JPEG images using feature extraction through the process if dilation," Elsevier, Digital Investigation,1-11 2014

[28] Ji-cang Lu , Fen-lin liu, " Selection of image features for steganalysis based on the fisher criterion," Elsevier, Digital Investigation, 1-10,2014

[29] Xiaodan Hou, Tao Zhang,Gang et al, " A Novel Steganalysis Framework of Heterogeneous Image Based on GMM Clustering," Elsevier, Signal processing: Image communication,10.1016,2014

[30] Vojtech Holub and Jessica Fridrich, "Random projections of residual for digital image Steganalysis," IEEE transaction on inforatmion forensics and security ,Vol 8 No 12 , 2013

[31] Erkan Bostanci, Nadia Kanwal and Adrian F, " Spatial statistics of image features for performance comparison," IEEE transaction on Image processing , Vol 23, no 1 , 2014