International Journal of Engineering Research and General Science Volume 3, Issue 5, September-October, 2015
ISSN 2091-2730

Blind JPEG Steganalysis using Statistical Moment and Second Order Statistics

[1]Mrs. Swagota Bera, [2]Dr. Monisha Sharma

[1]Associate Professor, Dept. of Electronics & Tele. SSIET, Durg, India

[2]Professor, Dept. of Electronics & Tele. SSCET, Bhilai, India

Abstract - A blind steganalysis technique is developed to attack the JPEG steganographic schemes using DCT and optimized quantization. The proposed method exploits the correlations between block-DCT coefficients in both intra-block and inter-block sense and the Characteristic function of the test image is selected as features. The features are extracted from the BDCT JPEG 2-array. Support Vector Machine with cross-validation is implemented for the classification.The proposed scheme gives improved outcome in attacking Outguess, F5 and Jsteg stego images.

Key words: Steganography, Steganalysis, Cover image, Stego image, cover Image, Attack, Least Significant Bit (LSB), DCT,DWT

I.Introduction

Steganography is the science for secret data concealing. If the data hiding is done after applying DCT and quantization to the image pixel, comes under the transform domain steganography. 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 .Several steganographic in transform domain for JPEG images has been developed. In this paper we focus on attacking three well known and most advanced steganographic methods, i.e., Outguess [1], F5 [2] and Jsteg [11]. 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. In reverse process detection of hidden data is known as steganalysis. Various approaches are discussed by the different researchers in the area of steganalysis. Broadly, there are two approaches to the problem of steganalysis, and one is to come up with a steganalysis method specific to a particular steganographic algorithm known as embedding algorithm based steganalysis techniques. The other technique is more general class of steganalysis techniques pioneered independently can be designed to work with any steganographic embedding algorithm, even an unknown algorithm. Such techniques have been called universal steganalysis techniques or blind steganalysis techniques.

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. Prediction accuracy can be interpreted as the ability of the measure to detect the presence of a hidden message with minimum error on average. Similarly, prediction monotonicity signifies that the features should ideally be monotonic in their relationship to the embedded message size. This image features should be independent on the type and variety of images supplied to it .Embedding techniques affect different aspects of images.

Farid[3] proposed a universal steganalyzer based on image's high order statistics .Quadrature mirror filters are used to decompose the image into wavelet subbands and then the high order statistics are calculated for each high frequency subband. The second set of statistics is calculated for the errors in an optimal linear predictor of the coefficient magnitude.

In [6], Shi et al presented a universal steganalysis system. The statistical moments of characteristic functions of the image, its prediction-error image, and their discrete wavelet transform (DWT) subbands are selected as features. All of the low-low wavelet subbands are also used in their system. This steganalyzer can provide a better performance than [3] in general.

In [4], Fridrich has proposed a set of distinguishing features from the BDCT domain and spatial domain aiming at detecting information embedded in JPEG images.The statistics of the original image are estimated by decompressing the JPEG image followed by cropping the four rows and four columns on the boundary, and then recompressing the cropped image to JPEG format using the original quantization table. Designed specifically for detecting JPEG steganography. This scheme performs better than [3,5] in attacking JPEG steganography .

In [7], a new scheme is proposed, in which the inter-pixel and intra-pixel dependencies are used and a Markov chain model is adopted . The empirical transition matrix of a given test image is formed. The average transition probability matrix is calculated for the horizontal, vertical, main diagonal and minor diagonal difference JPEG 2-array[4].

The proposed technique is an improved steganalysis scheme to effectively attack the advanced JPEG steganographic methods. In our scheme, the correlations between block-DCT coefficients in inter-block sense and the statistical moments of characteristic functions of the test image is selected as features. The embedding process often decreases the dependencies of the intra and inter pixel values exiting in original cover data to some extent. These changes are captured by comparing these statistical parameters. The first and second order statistical parameters and statistical moment parameter is used as features which is calculated from JPEG 2-array. Finally we evaluate the proposed features with support vector machines (SVM) as classifier by conducting experiments over a diverse data set of 4000 JPEG images. The superior results have demonstrated the effectiveness of our proposed scheme.

The rest of this paper is organized as follows. Section II discusses the proposed scheme for feature generation. Classification performance results are presented in Section III and conclusions are drawn in Section IV.

II. Proposed Scheme for Feature Generation

Steganographic embedding causes disturbance on the smoothness, regularity, continuity, consistency and periodicity and therefore correlation among the cover image pixels get distorted. There exist inter and intra block correlation among the image pixel which maintain the above features of the image. Any statistical parameter which includes these relationship may become a good tool for the detection purpose.

First Order Features

The statistical features are calculated from the DCT coefficient .The simplest first order statistic of DCT coefficients is the histogram. Suppose , $d_k(i, j)$ is the DCT coefficient array with quantized value . Q(i, j), i, j = 1,…,8, k = 1, …, B represents the quantized value of the JPEG file .The symbol $d_k(i, j)$ denotes the (i, j)-th quantized DCT coefficient in the k-th block (there are total of B blocks). The global histogram of all 64k DCT coefficients will be denoted as H_r, where r = L, …, R, L = $\min_{k,i,j} d_k(i, j)$ and R = $\max_{k,i,j} d_k(i, j)$. Many of the steganographic programs preserves the global histogram but fails to preserve the histogram of the individual DCT modes.Thus, we add individual histograms for low frequency DCT modes to our set of functionals. For a fixed DCT mode (i, j), let

h_r^{ij} , r =L, …, R, denote the individual histogram of values $d_k(i, j)$, k = 1, …, B. We only use Histograms of low frequency DCT coefficients because histograms of coefficients from medium and higher frequencies are usually statistically unimportant due to the small number of non-zero coefficients. For a fixed coefficient value d, the dual histogram is an 8×8 matrix g_{ij}^{d} where δ(u,v)=1 if u=v and 0 otherwise. In words , g_{ij}^{d} is the number of how many times the value d occurs as the (i, j)-th DCT coefficient over all B blocks in the JPEG image. The dual histogram captures how a given coefficient value d is distributed among different DCT modes[4].

$$g_{ij}^{d} = \sum_{k=1}^{B} \delta\big(d, d_k(i,j)\big) \qquad (1)$$

Second Order Features

The natural images can exhibit higher-order correlations over distances larger than 8 pixels, individual DCT modes from neighboring blocks are not independent. Thus, the features that capture inter-block dependencies can be violated by the various steganographic algorithms. Let I_r and I_c denote the vectors of block indices while scanning the image "by rows" and "by columns", respectively. The first functional capturing inter-block de-pendency is the "variation" V defined as

$$V = \frac{\sum_{i,j=1}^{8}\sum_{k=1}^{|I_r|-1}\left|d_{I_{r(k)}}(i,j) - d_{I_{r(k+1)}}(i,j)\right| + \sum_{i,j=1}^{8}\sum_{k=1}^{|I_c|-1}\left|d_{I_{c(k)}}(i,j) - d_{I_{c(k+1)}}(i,j)\right|}{|I_r| + |I_c|} \qquad (2)$$

Most steganographic techniques in some sense add entropy to the array of quantized DCT coefficients and thus are more likely to increase the variation V than decrease. Embedding changes are also likely to increase the discontinuities along the 8×8 block boundaries. In fact, this property has proved very useful in steganalysis in the past . Thus, we include two blockiness measures B_α, α = 1, 2, to our set of functionals. The blockiness is calculated from the decompressed JPEG image and thus represents an "integral measure" of inter-block dependency over all DCT modes over the whole image:

$$B_\alpha = \frac{\sum_{i=1}^{[(M-1)/8]}\sum_{j=1}^{N}\left|x_{8i,j} - x_{8i+1,j}\right|^{\propto} + \sum_{j=1}^{[(N-1)/8]}\sum_{i=1}^{M}\left|x_{i,8j} - x_{i,8j+1}\right|^{\propto}}{N[(M-1)/8] + M[(N-1)/8]} \qquad (3)$$

In the expression above, M and N are image dimensions and x_{ij} are grayscale values of the decompressed JPEG image[4].

Statistical Moment Feature

The histogram of an image is essentially the probability mass function (pmf) of the image . Multiplying each component of the

pmf by a correspondingly shifted unit impulse results in the probability density function (pdf). The pf pdf is exchangeable. Thus, the pdf can be thought as the normalized version of a histogram. The characteristic function (CF) is the Fourier transform of the pdf .The statistical moment get varies for different JPEG 2-array coeffiecient . This property is desirable for steganalysis. The statistical moments of the CFs of an image is defined as follows.

$$\mathrm{Mn} = \frac{\sum_{j=1}^{\binom{N}{2}} f_j^n \,|H(f_i)|}{\sum_{j=1}^{\binom{N}{2}} |H(f_i)|} \qquad (4)$$

where *H(fi)* is the characteristic function component at frequency *fi*, *N* is the total number of points in the horizontal axis of the histogram. Note that we have purposely excluded the zero frequency component of the CF, i.e., *H(f0)*, from calculating the moments because it represents only the summation of all components in the discrete histogram. For an image, it is the total number of pixels. For a JPEG 2-array, it is the total number of the coefficients[6] .

III. Experiments

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.(1).

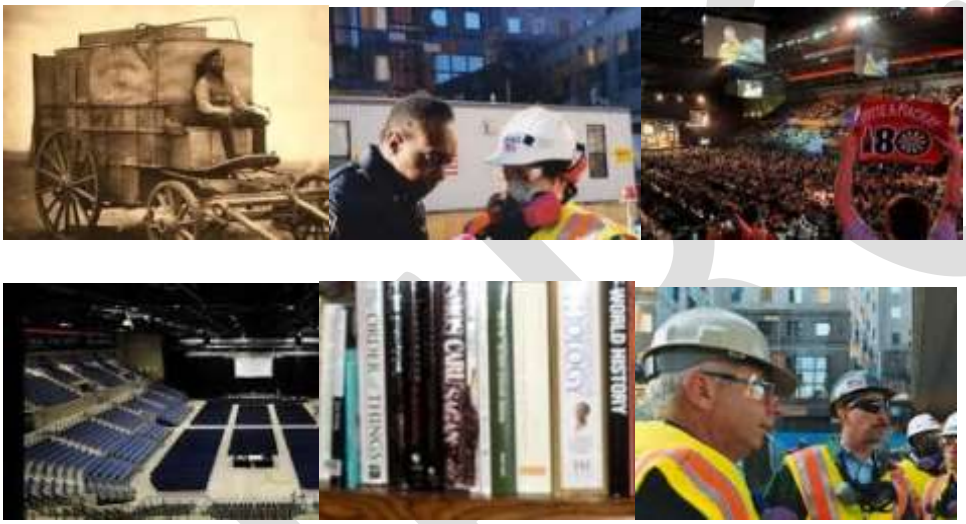

Fig.(1) Some Sample Images used in this Experimental Work

Stego images generation

On the basis of above approaches the steganalysis algorithm is designed using the MATLAB software and implemented to the stego image database , where database includes few different images of different size and formats encoded with JPEG Steganography technique Outguess, F5 and Jsteg of different capacities 0.05 , 0.1, 0.2 bpnc are used[1,2,11].

Experimental results for first and second order statistics

The images from the database has been used for both training and testing of the SVM classifier. The cross-validation technique is used in which 90 % of the data is used for training and rest 10 % is used for testing purpose. All the images in the dataset becomes the training and testing data simultaneously. Fridrich's first and second order[4] , shi's statistical moment[6] and proposed steganalyzer is

implemented for the detection of Jsteg[11], F5[2] and outguess[1] on randomly used 100 images .The classification result is shown in the Table 1. for the proposed scheme and the obtained result is compared with the existing one in Table 2.

Table 1. Performance of the SVM classifier for the proposed one where bpnc stand for bit per non zero coefficient, Sen. stands for sensitivity, Pre. stands for precision, Accu. stands for accuracy, Speci. stands for specifity and Detec. Relia. Stands for detection reliability.

Hiding Method	Bpnc.	Sen.	Pre.	Accu.	Speci.	Detec. Relia.
Outguess	0.05	0.657	0.442	65.5629	0.66	0.014
	0.1	0.656	0.444	65.667	0.66	0.02
	0.2	0.663	0.455	66.333	0.67	0.02
F5	0.05	0.666	0.443	66.5541	0.67	0
	0.1	0.669	0.447	66.8896	0.67	0
	0.2	0.679	0.783	67.893	0.68	0.02
Jsteg	0.05	0.661	0.456	66.1017	0.67	0.024
	0.1	0.674	0.459	67.4497	0.68	0.004
	0.2	0.695	0.483	69.5205	0.70	0

Table 2. Comparision of the Accuracy of the proposed detection technique with the reference. where bpnc stand for bit per non zero coefficient

Hiding Method	bpnc	Fridrich's	Shie et al's	Proposed
Outguess	0.05	64.90	58.00	65.5629
	0.1	65.33	58.61	65.667
	0.2	65.67	60.00	66.333
F5	0.05	66.81	57.19	66.5541

	0.1	66.89	57.43	66.8896
	0.2	67.56	66.89	67.893
Jsteg	0.05	63.73	60.00	66.1017
	0.1	63.76	60.07	67.4497
	0.2	65.75	62.67	69.5205

IV. Discussion and Conclusions

(1) In [6] the statistical moment of the test image and their wavelet subbands are used as features and in [4] the first order and second order statistical parameters are calculated from the JPEG-2 array of the test image. Since JPEG which use DCT and quantization is widely used for the data restoration and its transmission, so in the proposed scheme the statistical moment is calculated form the JPEG-2 array of the image.For the feature extraction the MATLAB software.

(2) 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.

(3) For developing Jsteg [11] stego image set , the optimized quantization table is used on the Block DCT coefficient for the implementation of conventional jsteg.

(4) For F5, Jsteg and Ouguess hiding technique , the detection accuracy is higher than [6] but slightly higher than [4].

(5) Among all the four the value is high for Jsteg[11] for the proposed one since it is an conventional one which does not restore the global histogram , but other two outguess[1] and F5[2] have the global restoration property.

REFERENCES:

[1] http://www.outguess.org/

[2] http://wwwrn.inf.tu-dresden.de/~westfeld/f5.html.

[3] Siwei Lyu "Detecting Hidden Messages using Higher-Order Statistics nd Support Vector Machines" Information Hiding, Springer,

Pg. No. 340–354, 2003.

[4] Jessica Fridrich "Feature Based Steganalysis for JPEG Images and its Implications For Future Design of Steganographic Schemes"

Information Hiding, Springer, Pg. No. 67–81, 2005.

[5] Farid . Hany. and Siwei Lyu " Steganalysis using Higher Order Image Statistics" IEEE Trasactions on Information Forensics and

Security. Vol. No.1, Issue No.1, Pg. No. 111–119, 2006.

[6] Chunhua Chen, Yun Q. Shi , Wen Chen and Guorong Xuan "Statistical Moments Based Universal Steganalysis using Jpeg 2-D Array

and 2-D Characteristic Function" IEEE international conference on image processing, Pg. No.105-108, 2006.

[7] Yun Q. Shi, Chunhua Chen and Wen Chen " A Markov Process Based Approach to Effective Attacking JPEG Steganography"

Lecture Notes in Computer Science , Information Hiding, Springer, pg. No. 249–264, 2007.

[8] Dongdong Fu, Yun Q. Shi, Dekun Zou and Guorong Xuan " JPEG Steganalysis using Empirical Transition Matrix in Block DCT

Domain" IEEE Workshop on Multimedia Signal Processing, Pg. No. 310–313, 2007.

[9] Chunhua Chen and Yun Q. Shi "JPEG Image Steganalysis Utilizing Both Intrablock and Interblock Correlations" IEEE International

Symposium on in Circuits and Systems, Pg. No. 3029- 3032, 2008.

[10] Mahendra Kumar "Steganography and Steganalysis of Joint Picture Expert Group (JPEG) Images " Ph.D. Thesis, University of

Florida, 2011.

[11] Swagota Bera and Monisha Sharm"Frequency Domain Steganography System using Modified Quantization Table" International

Journal of Advanced and Innovative Research,Vol. No.1, Issue No.1, Pg. No. 193-196, 2012.

[12] Swagota Bera and Monisha Sharma " Development and Analysis of Stego Image Using Discrete Wavelet Transform" International Journal of Science & Research ,Vol. No.2, Issue No.1, Pg. No. 142-148, 2013