ANOVA and Fisher Criterion based Feature Selection for Lower Dimensional Universal Image Steganalysis

Madhavi B. Desai *desaimadhavi30@gmail.com*
PhD student,
Computer Engineering Department,
Uka Tarsadia University,
Bardoli, 394350, India

S. V. Patel *patelsv@gmail.com*
Computer Application Department,
Sarvajanik College of Engineering and Technology
Surat, 395001, India

Bhumi Prajapati *bhumibprajapati18@gmail.com*
Electronics & Communication Department,
S.N. Patel Institute of technology and research Centre,
Umrakh, 394345, India

Abstract

Unethical uses of data hiding methods have made Image Steganalysis a very important area of research work in the field of Digital Investigations. Effectiveness of any Image Steganalysis algorithm depends on feature selection and feature reduction. The goal of this paper is to develop a reduced dimensional merged feature set for universal image steganalysis using Fisher Criterion and ANOVA techniques. Statistical features extracted from wavelet subbands and binary similarity patterns extracted from DCT of an image are merged to make combined feature set. Fisher criterion and ANOVA test are applied to evaluate the combined feature vector score and then only those features are selected which are found sensitive in both feature selection methods. These reduced dimensional 15-D feature vector is used to train SVM classifier with RBF kernel. The proposed algorithm is tested against steganography methods like F5, Outguess and LSB based method. Stego images are generated using widely available stego tools for two standard image databases: CorelDraw and BSDS500. Results are further validated using 10 fold cross validation process. The proposed algorithm achieves overall 97% detection accuracy against various steganography methods.
.

Keywords: Steganalysis, SVM, ANOVA, Fisher Criterion, DCT, DWT, Dimensionality Reduction.

1. INTRODUCTION

Internet has become an important communication channel through which information is transmitted, received and shared in form of emails, speech, images, videos etc. Terrorists see this as an opportunity to communicate secretly with each other by use of various image steganography methods. To break this unethical communication, steganalysis is required. Because of large number of redundant bits, image is most popular medium for steganography. This makes image steganalysis an active research area in the field of image forensics and digital investigations. Image Steganalysis can be classified into two categories: Specific Steganalysis and Universal Steganalysis. Specific steganalysis is used to break particular one steganography method while universal steganalysis works against different types of steganography methods. Performance of various image steganalysis algorithms depend on selection of features. The goal of this research work is to select most sensitive and effective features that can break different types of image steganography algorithms and propose most efficient reduced dimensional feature vector based universal image steganalysis algorithm. Section 2 describes existing image

steganalysis algorithms and highlights the scope of research work possible in the field. Section 3 explains feature identification criteria and section 4 describes feature selection and feature reduction based on Fisher criterion and ANOVA test. Last section highlights the effectiveness of proposed algorithm by analysis of various experimental results against popular image steganography methods like F5, Outguess and LSB based method..

2. LITERATURE SURVEY

Image steganalysis is an art of detecting hidden communication. Basic steps of image steganalysis algorithm are feature extraction and classification. In last decade, various authors have presented image steganalysis methods based on wavelet transform features [3,14,2,19], binary similarity based features[4,7], markov model based features[11,20,18,1] and co-occurrence matrix based features[9].

Shi Y. Q. and Chen W. [20] presented difference JPEG arrays and markov process based statistical features to break advanced JPEG image steganography methods. Difference JPEG 2-D Arrays along horizontal, vertical and diagonal directions are used and Markov process is applied to utilize second order statistics. Experimental results indicate that features extracted from horizontal and vertical directions are more effective compared to diagonal features. But when all the features are combined results are improved. Performance of algorithm was evaluated against F5, Outguess and MB1 steganography methods. Detection rate against F5 is lower compared to MB1 at same embedding rate. To make the steganalysis algorithm more effective against F5, Zou et.al [1] extracted the 2-D markov chain of thresholded prediction error image. Experiments were conducted using SVM classifier with linear and non-linear kernels. Results demonstrate the effectiveness of non-linear kernel with high dimensionality feature vector compared to linear kernel. Markov features are further extended by Wing W. Y. NG et al. [20]. Features are extracted from original, difference and second difference JPEG arrays. Experiments were conducted on two different image database BOWS2 [27] and UCID [28]. Training was done with one database and testing against second database. Combined markov features gives better results compared to method proposed by Fridrich [6] and Shi et. al [20] methods. Markov Features are further expanded to modified markov approach by R. Lakshmi Priya et al. [11]. They have extracted the features from intra block - DCT domain and inter block – DCT domain and also used the horizontal and vertical difference arrays along with DWT composition. To further increase the detection accuracy use of calibrated features was proposed. Experimental results are analyzed against MB1, MB2, JSTEG and F5 steganography methods. Detection accuracy of image steganalysis algorithm can be further improved by combining features from third markov chain and features of statistics from DCT domain.

Farid H.[3] used a different approach for feature extraction from grayscale images. The decomposition employed is based on separable quadrature mirror filters (QMFs). A statistical model is built which is composed of mean, variance, kurtosis, skew of sub-band coefficients and error statistics from an optimal linear predictor of coefficient magnitudes. A Fisher Linear Discriminant analysis is then used to discriminate between untouched and adulterated images. Lyu S. and Farid H. [14] extended the statistical model to first and higher order color wavelet statistics and exploited color statistics. OC-SVM is employed for detection of secret messages in digital images. One benefit of the higher order models employed here is that they are not as vulnerable to counter attacks that match first-order statistical distributions of the pixel intensity or transform coefficients. A steganalysis technique based on multiple features formed by statistical moments of wavelet characteristic functions was given by Xuan et al [2].39-D feature vector consisting of first three moments and three level Haar wavelet decomposition were proposed with Bayes classifier. This 39-D feature vector based image steganalysis method outperforms method proposed by Farid H. [3]. Author has given two observations: first, when x=0 the peak points of histogram of high frequency sub band should be considered to detect hidden message. Second, differentiation of histogram is more effective than integration of histogram for steganalysis. Author has also proved that the statistical moments of characteristic function wavelet sub band is much more effective than the features extracted from image in spatial domain as proposed in [8]. Wavelet features are further extended by Xiangyang Luo et al.[19]. In this paper, image is

decomposed into three scales through WPT (wavelet packet transformation) to obtain 85 coefficient sub bands together, and then 255-D multi-order absolute characteristic function moments of histogram are extracted from them as features. Experimental results clearly outperform other wavelet feature based methods proposed by Xuan et al. [2] and Wang method [23].

Binary similarity measures are also effective features used for image steganalysis. Basic idea behind this technique is that, the correlation between lower bit planes gets affected if we embed anything into image. Avcibas Ismail [4] presented a steganalysis technique based on binary similarity measures. 18 different binary similarity measures were obtained for each image to construct 18-D feature vector. These vectors were then used to train and test the SVM classifier. This method provided better results for LSB like methods compare to method proposed by Farid H. [3] in which higher order statistics of wavelet components are used for detecting hidden messages. But the Farid H.[3] method provided better performance against JPEG steganography methods. To overcome this drawback, Jing-Qu Lin et al. [7] proposed to extract binary similarity measures from seventh and eighth bit planes of the non-zero DCT coefficients. Use of binary similarity measures in DCT domain improved the performance against various JPEG steganography methods compared to method proposed by Avcibas I. [4].

Correlation based features are further extended by use of co-occurrence matrix. Kodovsky et al. [9] designed 7850-dimensional features that are produced from the co-occurrence matrices of DCT coefficient pairs and called as CF features. Since both the intra-block and inter-block dependencies are represented by the features, the steganalysis method can effectively detect the hidden data in JPEG images. An ensemble classifier mechanism is presented to solve the problem, in which the individual Fisher Linear Discrimination (FLD) classifiers are trained in a random feature subspaces with low dimensions, and the final decision on a suspicious medium is made by fusing the individual FLD decisions with majority voting strategy. Both the good classification performance and the satisfactory computational complexity are ensured by this approach.

To compete against newly developing image steganography methods we need to make use of merged features. But as discussed in literature, performance of image steganalysis algorithm do not depend on higher dimensional feature vector but it depends on effectiveness of features and sensitivity of combined feature vector. That's why the goal of this research work is to present a reduced dimensional feature vector by Fisher criteria and ANOVA test that can break various image steganography methods. To make image steganalysis algorithm universal we need to extract features not only from DCT and DWT domains but we need to make use of properties like correlation between pixels. Considering this fact we propose to extract statistical features from DWT domain and binary similarity measures from DCT domain. Out of these merged feature set most sensitive features are selected using Fisher criteria and then features are further reduced based on ANOVA test. To make the results more generalized, performance of the algorithm is evaluated against two standard image databases: BSDS500 [29] and CorelDraw database [24]. Stego images are generated by stego tools widely available on internet [25, 26].

3. FEATURE IDENTIFICATION

Feature extraction and feature selection are two main parts of image steganalysis process. Features are extracted from wavelet transform sub bands as given in [3, 14, 2, 22] and Binary similarity measures as given in [4, 7]. Section 3.1 demonstrates feature extraction from wavelet subbands and Binary similarity measures. Most sensitive features are selected from this merged feature set for classification process.

3.1 Statistical Measures from Discrete Wavelet Transform Methods

Wavelet transform is well-known for multi-resolution decomposition and de-correlation of wavelet transform co-efficient. The coefficients of different subbands at the same level are independent to each other. Therefore the features generated from different wavelet subbands at the same level

are independent to each other as well. We can say that M-D feature vector from this different sub-bands are suitable for image steganalysis.

Statistical analysis, detects changes in patterns of the pixels and the frequency distribution of the intensities. This analysis can detect whether an image was modified by checking to see if its statistical properties deviate from a norm. Hence, it intends to find out even slight alterations in the statistical behavior caused by steganography embedding. First moment is nothing but mean which describes the average difference between cover and stego image. Second moment is variance which can also be effective feature. Third moment is skewness describes lopsidedness and distribution. While 4^{th} moment measures heaviness or tail of distribution. These first four moments can be considered as effective features for image steganalysis.

Inverse transform of characteristic function produces the PDF (here, the histogram) as follows.

$$h(x) = \int_{-\infty}^{\infty} H(f) e^{-j2\pi fx} df \quad (1)$$

We can derive nth derivative of the histogram evaluated at the origin, x=0 as follows [2]:

$$\left| \left(\frac{d^n}{dx^n} h(x) |_{x=0} \right) \right| \leq 1(2\pi) \int_0^{\infty} f^n |H(f)| df \quad (2)$$

As indicated by Eq. 2, n-th derivative of histogram at x=0 is equal to moment obtained from the histogram. This makes histogram moment as one of the effective feature in the image steganalysis process. The change observed in moments extracted from DFT of histogram i.e. characteristic function is more compared to moments directly extracted from histogram [2]. This makes characteristic moment an effective feature for image steganalysis algorithm.

3.2 Features based on Local Binary Patterns

Binary statistics within bit planes and between lower order biplanes are affected by data hiding methods. Extraction of binary statistics from lower order bit planes can give strong cue for image steganalysis purpose. Straightforward bit plane correlations cannot be used for the steganalysis purpose as the evidence of any change is too weak, if we measure only bit correlations across bit planes. So it is more relevant to make comparisons based on binary texture statistics. Various binary similarity measures were proposed by V. Batagelj et al. [17] in 1992. Three types of BSM are extracted as features. (a).Similarity based measures between lower order bit planes (b) Histogram and entropy based measures (c) Local binary pattern based measures.

Every data hiding method modifies lower order bit planes of an image. This is the reason why one should extract binary similarity measures from lower order bit planes. As most of the transform domain image steganography methods hide data in either DCT or DWT frequency bands, they are robust against BSM extracted directly from the image. To make the features sensitive against various transform domain methods as well, it is suggested to extract binary similarity measures from transform domain [7].

4. BLOCK SCHEMATIC OF PROPOSED FEATURE EXTRACTION METHOD

Block schematic of the proposed merged feature extraction process is given in figure 1. As discussed in section 3 statistical features extracted from discrete wavelet domain and discrete cosine transform provides a useful clue for existence of hidden information in an image. Similarly, statistical patterns extracted from binary image planes also provide a strong cue that can be used to break image Steganography methods.

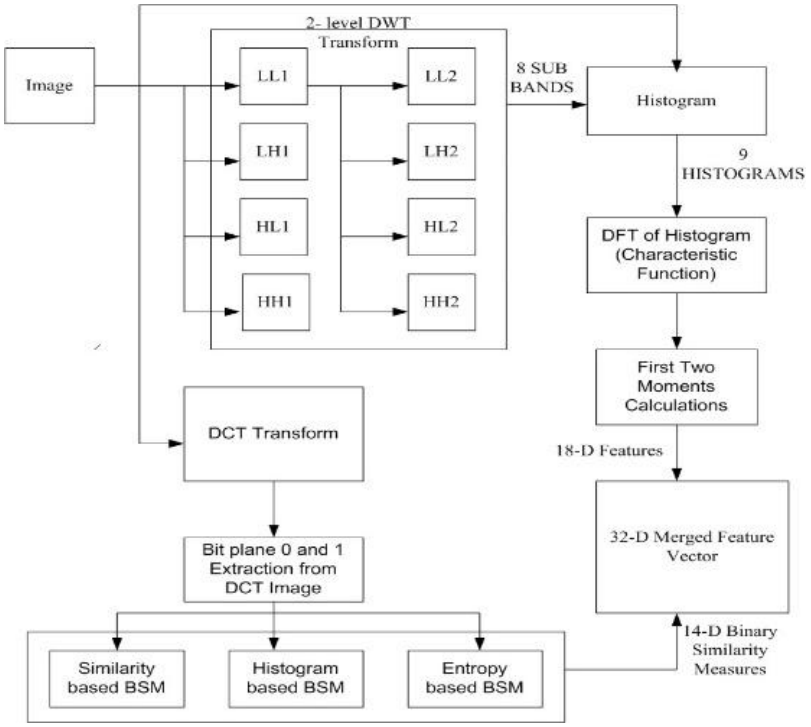

FIGURE 1: Block Schematic of Proposed Merged Feature Extraction.

Steps for merged feature extraction algorithm as shown in figure 1 are summarized as follows:

Step 1: 2-level discrete wavelet transform is applied to obtain 8 subbands i.e. LL1, LH1, HL1, HH1, LL2, LH2, HL2 and HH2. This gives total 9 subbands including original image as LL0.

Step 2: Characteristic functions (i.e. DFT of Histogram) of each of these 9 subbands are obtained.

Step 3: Find 1^{ST} and 2^{nd} order moments from each of these characteristic functions. That makes total of 18-D feature vector.

Step 4: Obtain DCT of a given image.

Step 5: Find out lower order bit planes (bit plane 0 and bit plane 1) of DCT of an image.

Step 6: Find out Binary Similarity Measures [7] based on similarity, based on histogram and entropy from lower order bit planes of DCT of an image. This makes total of 14-D features.

Step 7: Combining DWT, DCT and Binary similarity measure based features makes total of 32-D feature vector.

Step 8: Find out sensitivity of each of these features as described in next section and select most sensitive and effective set of feature vector for classification process

4.1 Combined Feature Set Evaluation based on Fisher Criteria

Effective features are one which have a high degree of separability between two classes. We suggest to use fisher criterion to analyze the separability of features. Separability of each feature is evaluated using Eq. 3. Larger the Fscore better is the feature.

$$Fscore(d) = \frac{(\mu_d^C - \mu_d^S)^2}{(\sigma_d^C)^2 - (\sigma_d^S)^2} \quad (3)$$

Where and are mean values of d-th feature in cover and stego feature set respectively while, and are standard deviations. Numerator in Eq.1 is the between class variance of cover and stego feature set while denominator is with in class variance. The value of fisher score will be larger when between classes variance will be larger and with-in class variance will be smaller. We evaluated Fscore for each of these 32 features and reordered them based on Fscore values. Figure 2 demonstrates the block schematic of fisher based feature vector selection process [5].

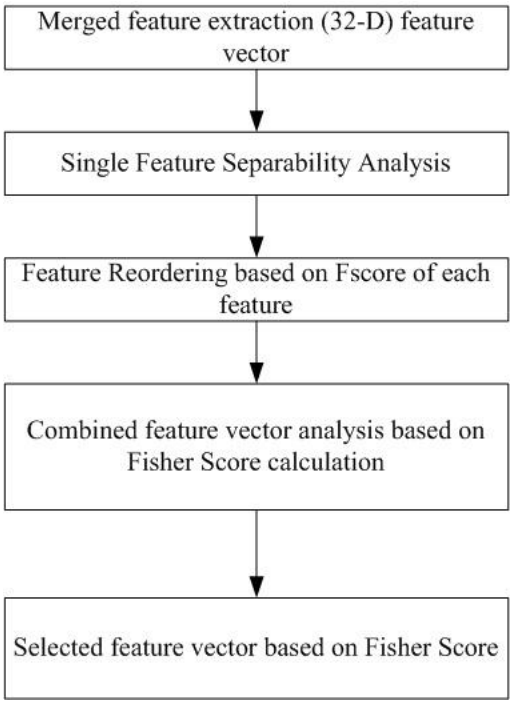

FIGURE 2: Block schematic of fisher criterion based feature selection [5]

Once the separability of each single feature is evaluated, their combined fisher score is calculated as proposed by Ji-cand Lu et al [5]. Separability of feature vectors will be analyzed and evaluated using fisher score combined with measurement of the Euclidean distance. For cover and stego feature set F^C and F^S respectively, the euclidean distance between mean values of the feature vectors can be measured by

$$\Omega(\mu^C, \mu^S) = \sqrt{\sum_{d=1}^{D} (\mu_d^C, \mu_d^S)^2} \quad (4)$$

When the feature vector is evaluated as a whole, the fisher score is given by,

$$Fscore = \frac{\Omega(\mu^C, \mu^S)^2}{\frac{1}{N}\sum_{n=1}^{N} \Omega(F_n^C, \mu^C)^2 + \frac{1}{N}\sum_{n=1}^{N} \Omega(F_n^S, \mu^S)^2} \quad (5)$$

Where F_n^C and F_n^S are feature vectors of n-th sample from cover and stego feature set respectively and denominator is sum of variances of two classes of feature vectors. Steps for feature selection are summarized as follows:

Step 1: Find out Fscore for individual feature using Eq.1

Step 2: Reorder features in descending order based on Fscore obtained in step 1.

Step 3: Find out combined Fscore after adding first d features from 32-D using Eq. 5.

Step 4: Find out combined Fscore for feature vectors by increasing d step by step ($0 \leq d \leq D$).

Step 5: Find out the point of highest Fscore out of all combinations.

Step 6: Select combination of features where Fscore is maximum value.

Step 7: Find out combination of features for each steganography method during training phase using Eq. 5. Reject all features which are not effective during training phase. We did the analysis for F5, Outguess and LSB based steganography methods and finally selected 27-D features which are having effective combined Fscore for all steganography methods used during training phase. Figure 3 shows the combined fisher score for feature vector evaluated against steganography methods F5, Outguess and LSB.

Figure 3 demonstrates the Fscore obtained for various combinations of features against different types of steganography methods. CorelDraw [24] image database is used for the experimental purpose. All images are of size 256x256 and stego images are generated by widely available stego tools [25, 26].As shown in figure 3 after reordering of features based on individual Fscore when we combine features combined Fscore value increases. It will reach a point at which maximum combined Fscore is obtained. Features after this point are rejected for further analysis. We repeated the experiment with all methods and rejected 5-D features out of 32-D merged features as explained previously.

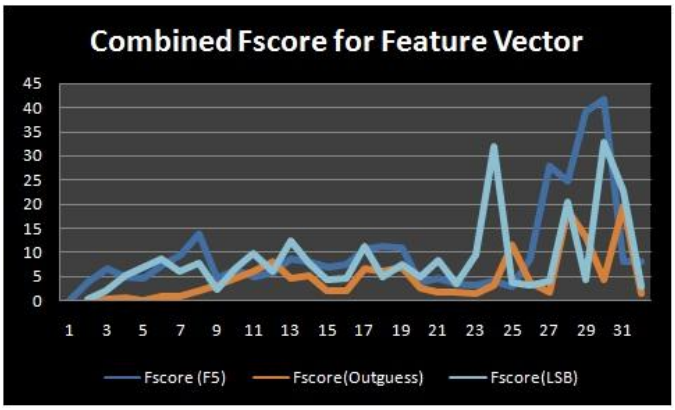

FIGURE 3: Combined Fscore for feature vector using Fisher Criterion.

This makes 27-D combined feature vector which are further analyzed by ANOVA test for feature reduction. Next section describes ANOVA process and demonstrates the results of various experiments conducted.

4.2 Feature Reduction using ANOVA Test

Similar to fisher criterion ANOVA test is a variance test used to find out the separability of individual features between two classes. We have used ANOVA test to further reduce the dimensionality of features. ANOVA test is used to check the sensitivity of each feature and most sensitive features out of remaining 27-D features after fisher criterion are used for classification process. ANOVA test is used to identify how much sensitive the feature has been to distinguish two classes: cover and stego. ANOVA test gives two values: F-statistic and p-statistic. The F-statistic is the ratio of the mean squares. The p-value is derived from the CDF of F. F-statistic is the ratio of "between sample sum of squares (due to the means)" and "within sample sum of squares" while, p-value is the CDF of F-statistic.

Consider m independent samples, each of size n, where the members of the i^{th} sample X_{i1}, X_{i2}…,X_{im} are normal random variables with unknown mean μ_i and unknown variance σ^2 .In this Hypothesis is testing, $H_0 : \mu_1 = \mu_2 = ... = \mu_m$ VersusH_1: Not all the means are equal. Now, Sum of squares between samples can be given by,

$$SS_w = \sum_{i=1}^{m} \sum_{j=1}^{n} (X_{ij} - X_i)^2 \quad (6)$$

Where, variable X_i is the sample mean of the i^{th} sample. Now, Sum of squares between samples can be given by,

$$SS_b = \sum_{i=1}^{m} (X_{ij} - X_i)^2 \quad (7)$$

F statistic is given by eq. 8 and reject H_0 when F-statistic is sufficiently large. P-value is the CDF of F-statistic.

$$F = \frac{SS_w(m-1)}{SS_b(nm-m)} \quad (8)$$

ANOVA test is conducted for all 32-D features against F5, Outguess and LSB steganography methods. F-statistic values obtained from ANOVA test are normalized and % F-statistic values are shown for BSM features extracted from DCT domain and statistical features extracted from DWT domain in Figure 4 and figure 5 respectively. Larger the value of F-statistic better is the feature. Feature has to be equally sensitive against various types of image steganography methods. Considering these two facts feature selection is done as follows:

- Effective Features from both DWT and DCT domain are selected based on ANOVA test. Merged Features from both domains will make image steganalysis algorithm equally effective against various steganography methods.
- Select the features whose F-statistic value is large.
- Remove feature for further analysis if its F-statistic value is very less for any of the methods used for experimentation.

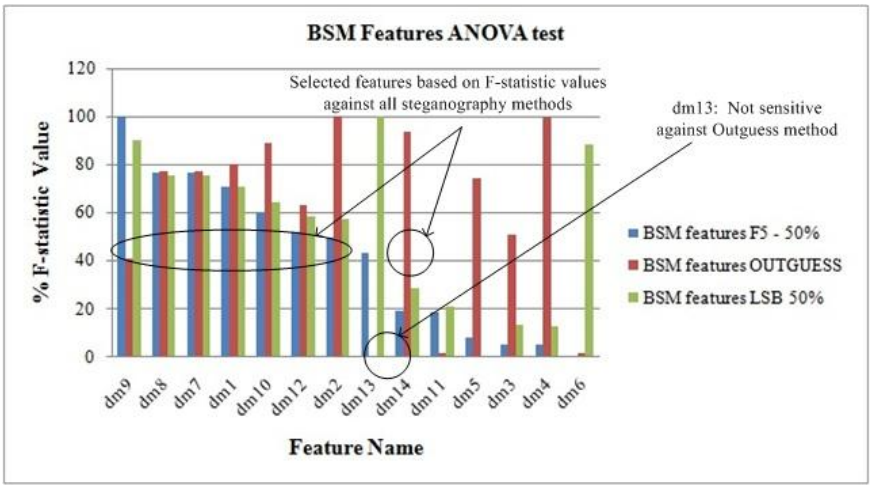

FIGURE 4: F-statistic value for BSM features against F5 method with50% embedding rate, Outguess and LSB with 50% embedding rate.

As shown in figure 4, first 7 BSM features show larger values of F-statistic against all steganography methods. F-statistic value of feature 8 (dm13) is zero against outguess method although it shows larger values against other two methods. That's why feature 8 is rejected from final combined feature vector. First 7 BSM features and feature 9 are selected from ANOVA test results shown in figure 4.

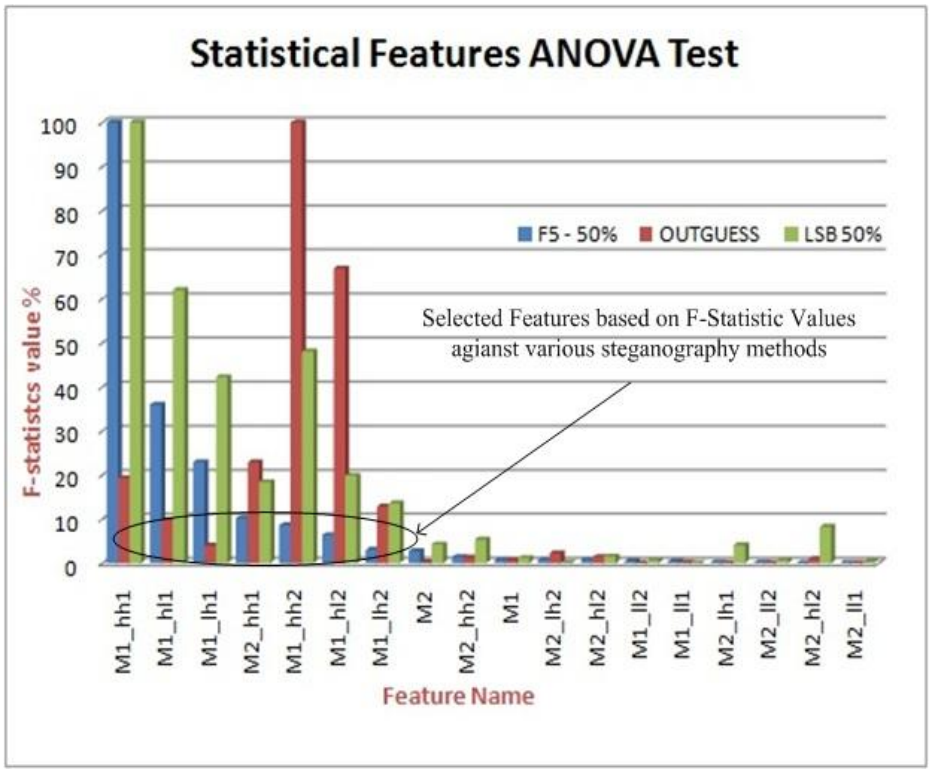

FIGURE 5: F-statistic value for statistical features extracted from DWT domain against F5 method with50% embedding rate, Outguess and LSB with 50% embedding rate.

Figure 5 shows that first 7 statistical features are sensitive against all steganography methods used for experimentation, while for other features F-statistic values are near to zero. Only first 7

statistical features are selected and combined with selected BSM features to form final merged feature set. Binary similarity measures extracted from DCT domain shows very good separability against F5 and Outguess steganography methods. Moments of characteristic functions extracted from wavelet domain also provides very useful information for identification of existence of hidden message. Summary of selected 15-D features based on ANOVA test are as follows:

1. **$M1_{LH1}$, $M1_{HL1}$, $M1_{HH1}$:** First moment extracted from LH, HL and HH band of DWT decomposition of an image.

2. **$M1_{LH2}$, $M1_{HL2}$, $M1_{HH2}$:** First moment extracted from LH2, HL2 and HH2 band of 2^{nd} level of DWT decomposition of an image.

3. **$M2_{HH1}$:** Second moment extracted from HH1 band of 1^{st} level of DWT decomposition of an image.

4. **dm1, dm2, dm7, dm8, dm9, dm10:** BSM based on similarity criteria

5. **dm12, dm14:** BSM based on histogram and entropy

5. EXPERIMENTS AND RESULT ANALYSIS

To evaluate the performance of proposed image steganalysis algorithm we have used two standard databases: BSDS500 [29] and CorelDraw database [24].All images used for experiments are of size 250x250. Each database contains 700 images of different textures with animal, architecture, background, business, landscape and natural images. Quantitative evaluation of proposed algorithm is done using Confusion Matrix as shown in Table 1.

True Positives(TP)	False Positives(FP)
False Negatives(FN)	True Negatives(TN)

TABLE 1: Confusion Matrix.

Where, TP: stego image is correctly classified as stego image. TN: cover image is correctly classified as cover image. Detection Accuracy can be given by Eq. 9.

$$DetectionAccuracy = \frac{TP + TN}{TP + FN + TN + FP} \tag{9}$$

Detection Accuracy can also be given by averaging the TP and TN rate. TP and TN rate can be given as follows,

$$T\,\mathrm{P}\_rate = \frac{TP}{TP + FN} \tag{10}$$

$$TN\_rate = \frac{TN}{TN + FP} \tag{11}$$

Figure 6 shows the experimental set up used for analysis and testing. SVM is used as classifier with RBF kernel. During training phase cover and stego images generated with the help of stego tools [25, 26] are given to SVM classifier and 15-D features are extracted from each image set. These cover and stego feature set are used to train the classifier. Once the classifier is trained testing images consisting of cover and stego images are given to the trained classifier. Results

are quantitatively analyzed to see the performance of the proposed feature vector based universal image steganalysis algorithm.

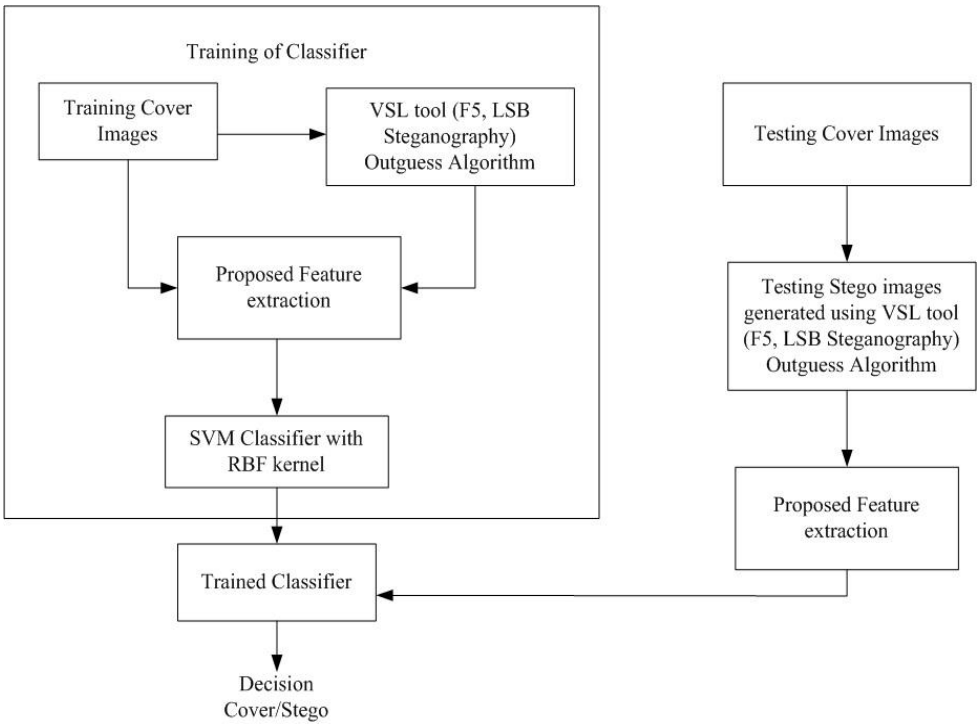

FIGURE 6: Experimental Setup for evaluation of proposed Image Steganalysis Algorithm.

VSL Tool is used to make stego images with F5 and LSB based steganography methods. SVM classifier with non-linear RBF kernel is used for classification. Features are given to SVM classifier which is used to for training the classifier. Once the classifier is trained testing image features are given to the trained classifier and results are obtained. To make the results more generalized experiments are conducted with two different databases and results are shown in table 2 and table 3.

Steganography method	**Detection Accuracy in shown in %**					
	72-D Features [13]	**39-D Features [2]**	**18-D Features [21]**	**BSM in DCT domain [7]**	**27-D features after Fisher Criterion**	**15-D proposed Features after ANOVA**
F5-100% embedding	52.5	62.69	68.08	97.31	97.69	98.85
F5-50% embedding	50	63.47	66.54	97.31	97.69	98.85
Outguess 0.04 bpp embedding	58.75	86.54	92.69	94.23	97.69	98.85
LSB-100% embedding	50	71.54	82.31	100	99.62	99.62
LSB-50% Embedding	50	66.54	76.54	99.62	97.69	98.46

TABLE 2: Comparison between detection accuracy of proposed image steganalysis algorithm with existing methods against F5, Outguess and LSB based steganography methods with different embedding rates conducted on CorelDraw Database.

As shown in Table 2, results were obtained for F5 steganography with 100% and 50% embedding rate, Outguess steganography with 0.04 bpp (bits per pixels) embedding rate and LSB steganography with 100% and 50% embedding rate using proposed reduced dimensional merged feature based universal image steganalysis algorithm.

To show the effectiveness of proposed merged feature set we compared the results with image steganalysis based on features derived from DWT domain and BSM obtained from DCT domain. Results mentioned in Table 2 clearly show that 27-D feature vector obtained after fisher criterion out performs image steganalysis methods based on individual features. Final set of 15-D feature vector obtained after ANOVA test further improves the detection accuracy of image steganalysis. To further authenticate the results 10-fold cross validation is done. Table 3 shows the results of 10-Fold Cross validation for proposed method against various image steganography methods F5 with 100% embedding, F5 with 50% embedding, Outguess with 0.04 bpp embedding, LSB with 100% embedding and LSB with 50% embedding.

Iteration No.	**Detection accuracy in % against various image Steganography methods**				
	F5 100% embedding	**F5 with 50% embedding**	**Outguess 0.04 bpp embedding**	**LSB-100% embedding**	**LSB-50% embedding**
1st iteration	97	97	96	99	96
2nd iteration	100	98	95	100	99
3rd iteration	98	98	98	97	96
4th iteration	100	96	97	100	100
5th iteration	98	98	99	98	98
6th iteration	99	96	100	98	99
7th iteration	93	96	99	99	96
8th iteration	99	99	99	100	100
9th iteration	94	98	94	100	99
10th iteration	97	99	97	100	97
Average result	97.5	97.5	97.4	99.10	98

Table 3: 10-fold Cross validation results for proposed 15-D merged feature based image Steganalysis method against various state of art image Steganography algorithms.

In statistics, a typical task is to learn a classifier from available data. The problem with evaluating such a classifier is that it may reveal enough prediction capability on the training data, but might fail to predict future unseen data. Cross-validation is a procedure for estimating the generalization performance in this context.10-Fold Cross validation is used for estimating the accuracy in general. Process of 10-fold cross validation is : (a first break the data into 10 sets of size n/10 (b train on 9 dataset and test on 1 dataset (c repeat 10 times by changing the training and testing dataset Also be careful that test dataset is taken at once for testing. Finally, take mean accuracy result. We have also divided our database images into 10 sets. Then one set is considered for testing and other 9 set we have considered for testing. For each iteration we have changed the training and testing set. Than at end we have taken the average result. Results of proposed 15-D features based image steganalysis method gives overall 97% detection rate against various data hiding methods with various training and testing images. Similar experiment is conducted with BSDS500 [29] image database and results are demonstrated in Table 4. To check the generalization capabilities of proposed algorithm experiment is repeated with another standard BSDS500 [29] image database.

Steganography method	Detection Accuracy in shown in %					
	72-D Features [13]	39-D Features [2]	18-D Features [21]	BSM in DCT domain [7]	27-D features after Fisher Criterion	15-D proposed Features after Fisher Criterion & ANOVA
F5	50.50	56	61.50	97	95.50	97
Outguess 0.04 bpp embedding	49.50	78.50	83.50	81.50	90	92.5

TABLE 4: Steganalysis Results against BSDS500 Database [29].

Table 4 clearly shows that by changing image dataset, results with individual feature set are reduced by more than 10% while proposed method gives comparable results as obtained with CorelDraw image database. 18-D statistical features extracted from DWT domain outperforms previously proposed methods as demonstrated in papers [13,2]. But only DWT based features suffer against F5 steganography method. Results are improved by extraction of binary patterns from DCT domain using BSM features as shown in paper [7]. The goal of this paper is to further improve the performance of steganalysis algorithm by merging both DWT features and DCT domain BSM features and selecting only most sensitive features out of them. For feature selection two methods were used: Fisher Criterion based feature selection and ANOVA based feature selection. 27-D features are set of features which were found sensitive after fisher criterion. As shown in table 4 these 27-D features improves the steganalysis results compared to DCT-BSM features [7]. ANOVA test was used to further validate the feature selection process. Finally 15-D features were selected which were found sensitive in both feature selection methods. Both the feature selection methods identify sensitivity of the feature based on variance analysis between stego and cover features. Proposed 15-D features out performs all the state of art methods based on DWT and DCT features based steganalysis methods. Table 5 gives the performance comparison between existing and proposed image steganalysis methods against different steganography algorithms

Sr. No.	Steganalysis Method	Detection accuracy in % against various image Steganography methods		
		LSB (0.25-0.5 bpp)	F5	Outguess
1	18-D [21]	91	NA	NA
2	Farid et al. [3]	43- 90	NA	NA
3	39-D G. Xuan et al. [2]	94.1	NA	NA
4	78-D Shi Y. Q. et al. [22]	98.9	NA	NA
5	Wing W. Y. Ng et al [18]	NA	74.52	96.14
6	R. Lakshmi Priya et al.[11]	NA	99.40	NA
7	Xiangyang et al. [19]	84.1	96.40	NA
8	Penvy T., & Fridrich J.[16]	NA	99.80	100
9	Liu S. et al.[12]	99.85	NA	49.20
10	Proposed 15-D features	98.4	98.85	98.85 (0.4bpp)

TABLE 5: Comparison with existing image Steganalysis methods.

Comparison of various algorithms should be done on the basis of number of data hiding methods used for testing purpose and types of embedding rates considered during the analysis. Proposed 15-D feature vector based image steganalysis method gives overall 98% detection accuracy against all steganography methods used for analysis. Results in Table 5 clearly demonstrate the effectiveness of proposed method against various states of art image steganalysis methods. It proves that more number of features doesn't guarantee better results. With this reduced dimensionality of features, classification complexity is also reduced.

6. FUTURE WORK

Proposed image steganalysis algorithm is tested against two different datasets including various types of images with different textures. This paper also demonstrated the use of ANOVA and fisher criterion for feature selection and improved the steganalysis results compared to previous algorithms. In future one can go for blind image steganalysis method where unknown steganography method based stego images shall be used for testing purpose which will not used during training phase. One can also check the performance of the steganalysis algorithm against stego images with variable embedding rate. It will be interesting to develop an image steganalysis algorithm that can work against images with sizes other than size used for training purpose i.e. it should work irrespective of resolution of an image.

7. CONCLUSION

This paper presents universal image steganalysis method based on merged features extracted from statistical features from DWT domain and similarity features from DCT domain. As demonstrated by various experiments in section 5, proposed 15-D reduced dimensional feature vector based image steganalysis algorithm gives overall 97% of detection accuracy against various types of data hiding methods. Use of combined feature evaluation based on Fisher Criterion and ANOVA test improves the sensitivity of various image features that enhances the performance of existing image steganalysis algorithm. Accuracy of the proposed algorithm was also evaluated on two different standard image databases to further authenticate the results. BSM extracted from DCT are most sensitive features against various JPEG domain steganography methods but use of statistical moments extracted from DWT subbands make this algorithm universal against various DWT and spatial domain steganography methods also. Results shown in Table 2 and Table 3 clearly demonstrate the effectiveness of proposed 15-D feature vector based universal image steganalysis algorithm.

8. REFERENCES

[1] D. Zou, Y. Q. Shi, W. Su and G. Xuan. "Steganalysis based on markov model of threshold prediction-error image." in Proc. of the 2012 IEEE Int. Conf. on Multimedia and Expo. Toronto, Canada, 2006, pp. 1365-1368.

[2] G. Xuan. "Steganalysis based on multiple features formed by statistical moments of wavelet characteristic functions." in Lecture Notes in Computer Science, 3727, Springer-Verlag, Berlin, pp.262–277, 2005.

[3] H. Farid. "Detecting hidden messages using higher-order statistical models." in Proc. IEEE Int. Conf. Image Processing, Rochester, NY, 2002, pp. 905-908.

[4] I. Avcıbas, M. Kharrazi, N. Memon and B. Sankur. "Image steganalysis with binary similarity measures." EURASIP Journal on Applied Signal Processing, pp.2749–2757, 2005.

[5] J.-C Lu, F.-L. Liu and X.-Y. Luo. "Selection of image features for steganalysis based on the Fisher criterion." Digital Investigation, vol. 11(1), pp. 57–66, 2014.

[6] J. Fridrich. "Feature-based steganalysis for jpeg images and its implications for future design of steganographic schemes." in Proc. of Information Hiding Workshop, Lecture Notes in Computer Science, Springer, 3200, 2004, pp.67–81.

[7] Jing-Qu Lin and Shang-Ping Zhong. “Jpeg image steganalysis method based on binary similarity measures.” in Proc. of Eighth International Conference on Machine Learning and Cybernetics, Baoding, July 2009, pp. 2238-2243.

[8] J. J. Harmsen. “Steganalysis of additive noise modelable information hiding.” Master Thesis of Rensselaer Polytechnic Institute, Troy, New York, 2003.

[9] J. Kodovsky, J. Fridrich and V. Holub. “Ensemble classifier for steganalysis of digital media.” IEEE Trans. Inf. Forensics Security, vol. 7(2), pp.432–444, 2012.

[10] K. Sullivan, U. Madhow, S. Chandrasekaran and B. S. Manjunath.”Steganalysis of spread spectrum data hiding exploiting cover memory.” SPIE, pp.38-46, 2005.

[11] R. Lakshmi Priya, P. Eswaran and S. L Ponnambli Kamakshi. “Blind Steganalysis with Modified Markov Features and RBFNN.” IJERT, vol. 2(5), pp. 2278-0181, 2013.

[12] S. Liu, L. Ma, H. Yao and D. Zhao. “Universal steganalysis based on statistical models using reorganization of block-based dct coefficients.” presented at fifth Int. Conf. Information Assurance and Security,2009.

[13] S. Lyu and H. Farid. “Detecting hidden messages using higher-order statistics and support vector machine.” Lecture Notes in Information Hiding, Springer Berlin Heidelberg, pp.340-354, 2003.

[14] S. Lyu and H. Farid. “Steganalysis using color wavelet statistics and one-class vector support machines.” in Proc. of SPIE Security, Steganography, Watermarking of Multimedia Contents, 2004, pp.35–45.

[15] S. S. Ekhande, S. P. Sonavane and P. J. Kulkarni. “Universal steganalysis using feature selection strategy for higher order image statistics,” International Journal of Computer Applications, vol. 1(19), pp. 52-55, 2010.

[16] T. Penvy and J. Fridrich. “Merging Markov and dct features for multi-class JPEG Steganalysis.” in Proc. of SPIE, San Jose, CA, 2007.

[17] V. Batagelj and M. Bren. “Comparing resemblance measures,” in Proc. International Meeting on Distance Analysis (DISTANCIA’92), Rennes, France, June,1992.

[18] Wing W. Y. NG, Zhi-Min He, Patrick P.K. Chan and Daniel S. Yeung. “Blind steganalysis with high generalization capability for different image databases l-gem.” in Proc. of the 2011 Int. Conf. on Machine Learning and Cybernetics, Guilin, July 2011, pp. 1690-1695.

[19] X. Luo, F. Liu, J. Chen and Y. Zhang. “Image universal steganalysis based on wavelet packet transform,” Multimedia Signal Processing, IEEE 10th Workshop on Digital, pp.780 – 784, 2008.

[20] Y. Q. Shi, C. Chen and W. Chen. “A markov process based approach to effective attacking jpeg steganography.” in Proc. of the 8th International Workshop, Springer, Berlin, 2006, pp. 249-264.

[21] Y. Q. Shi, G. Xuan, C. Yang, G. Gao, Z. Zhang and P. Chai. “Effective steganalysis based on statistical moments of wavelet characteristic function” in Proc. of the Int. Conf. on Information Technology: Coding and Computing, 2005, pp. 768-773.

[22] Y. Q. Shi, G. Xuan, D. Zou and J. Gao. “Steganalysis based on moments of characteristic function using wavelet decomposition, prediction error image and neural network.” in Proc. of IEEE ICME, 2005, pp. 269-272.

[23] Y. Wang and P. Moulin. “Optimized feature extraction for learning based image steganalysis,” IEEE Trans in Forensics Security, vol. 2(1), pp. 262-277, 2005.

[24] CorelDraw Database: http://www.corel.com

[25] Outguess: http://www.outguess-rebirth.com/

[26] http://vsl-virtual-steganographiclaboratory.soft112.com/download.html

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

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

[29] BSDS500ImageDataset.http://www.eecs.berkeley.edu/Research/Projects/CS/vision/grouping/segbench/