Steganalysis of YASS Using Huffman Length Statistics

Veena H Bhat[1,3], Krishna S[4], P Deepa Shenoy[1], Venugopal K R[1],
L M Patnaik[2]
[1] *Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore, India*
[2] *Vice Chancellor, Defence Institute of Advanced Technology, Pune, India*
[3] *IBS-Bangalore, Bangalore, India.*
[4] *Department of Electronics and Communication Engineering, University Visvesvaraya College of Engineering, Bangalore, India*
{veena.h.bhat, krishna.somandepalli}@gmail.com, shenoypd@yahoo.com

Abstract

This work proposes two main contributions to statistical steganalysis of Yet Another Steganographic Scheme (YASS) in JPEG images. Firstly, this work presents a reliable blind steganalysis technique to predict YASS which is one of recent and least statistically detectable embedding scheme using only five features, four Huffman length statistics (H) and the ratio of file size to resolution (FR Index). Secondly these features are shown to be unique, accurate and monotonic over a wide range of settings for YASS and several supervised classifiers with the accuracy of prediction superior to most blind steganalyzers in vogue. Overall, the proposed model having Huffman Length Statistics as its linchpin predicts YASS with an average accuracy of over 94 percent.

Keywords: *Statistical Steganalysis, Huffman Coding, YASS.*

1. Introduction

The art and science of hiding the very presence of communication by embedding the information (payload) in an innocent looking multimedia object (cover), is steganography. The detection of the presence of communication in such stego-objects is steganalysis. Steganalysis could either be designed with the knowledge of the steganographic scheme used (targeted steganalysis) or without any knowledge of either the cover object or the embedding strategy (blind steganalysis). Steganography in JPEG images has become popular in recent years mostly because of the complexity of steganalysis required for a lossy compression method such as JPEG. Several steganographic embedding schemes have been proposed over the years with varying degrees of complexity and security [1]. Among such embedding schemes, Yet Another Steganographic Scheme (YASS) proposed in 2007 is a novel scheme designed for JPEG images. Generally, the sensitivity to variation in the higher order statistics when images are subjected to steganography is an important aspect on which most steganalyzers thrive. Heuristics show the statistical un-detectability of YASS and its ability to elude most blind steganalyzers in vogue.

Feature extraction and a trained classifier to detect the data hidden are the most vital aspects of any steganalysis framework. Fridrich et al., proposes calibration of the extracted features for an efficient blind steganalyzer. Calibration refers to the difference between a specific (non-calibrated) functional calculated from a stego image and the same functional obtained from the corresponding cover image [2]. Based on this notion, blind steganalyzers

can be classified as those techniques that use calibration of features extracted from stego-images as predictors and those that don't use calibration. Some steganalyzers that don't use calibration adopt Markov processes to analyze the magnitudes of the quantized Block DCT (BDCT) coefficients of the JPEG images before and after embedding data (payload) in an image to detect any hidden data [3]. YASS is proven immune to both these kinds of attacks.

YASS is simple yet effective. Unlike prevalent steganographic methods, YASS does not embed data directly in JPEG coefficients. Instead, it uses the strategy of Quantization Index Modulation (QIM) to hide information in the quantized Discrete Cosine Transform (DCT) coefficients in randomly chosen 8×8 host blocks, whose locations may not coincide with the 8×8 grids used in JPEG compression. After embedding a payload, images are compressed back to JPEG format; this process of randomized embedding successfully evades attacks by calibrated steganalytic features [4]. Several techniques, blind and targeted attacks alike have been proposed for steganalysis of YASS. However, no blind steganalyzer is promising and most don't offer reliable detection over the range of block sizes used for YASS. Targeted steganalysis techniques aimed at attacking YASS that consider the randomness of block sizes have shown an efficient accuracy of detection [4, 5].

This work presents a blind steganalyzer that works on uncalibrated statistical features for reliable detection of YASS over a wide range of settings. Section 2 outlines the related work. To make this paper self contained we have described the YASS in detail in section 3. The feature extraction is explained in section 4. The image database and the exploratory data analysis conducted on the image database is explained in section 5. Section 5 also tests the hypothesis of whether the selected attributes can be used to predict the embedded payload size. Section 6 describes the implementation; the model and classifiers used. Results and performance analyses are described in section 7. Conclusions and future work is given in section 8.

2. Related Works

YASS, a JPEG steganographic technique, hides data in the non-zero DCT coefficients of randomly chosen 8×8 blocks [6]. YASS robustly embeds messages in digital images in a key dependent transform domain. This random embedding scheme remains resistant to most blind steganalyzers that employ analysis of higher order statistical features. YASS is further strengthened against statistical detection by the introduction of randomization, using a mixture based approach which is referred to as Extended YASS (EYASS) in [7, 8]. YASS and EYASS (explained in section 3) thus pose a new challenge to steganalysts to reconsider the predictor features extracted and algorithms designed for steganalysis so far.

The original proposers of YASS [6] evaluated its detectability against six popular blind steganalyzers [9, 10, 11, 12, 13, 14] using Support Vector Machines (SVM) as the classifier to demonstrate its robustness, however with a low embedding capacity. The improved YASS algorithm (EYASS) introduces more calculated randomness to the original YASS algorithm besides improving the embedding capacity [7]. K.Solanki et al., in their work [7] prove the non-detectability of EYASS by evaluating against two blind steganalyzers [9, 10]. The notion of employing self calibration features for statistical detection of YASS and its failure has been explored in [2].

Steganalysis of YASS / EYASS using four state-of-the-art steganalytic feature sets is proposed in [5]; CC-PEV, a 548 dimensional Cartesian-Calibrated Pevny feature set [5], 486 dimensional Markov process features (MP) [15], the Subtractive Pixel Adjacency Model (SPAM) feature set consisting of 686 features [14] and a combination of SPAM and CC-PEV to derive a 1,234 dimensional Cross-Domain Feature (CDF) set. These feature sets are used to

evaluate YASS / EYASS techniques against twelve different settings of YASS and resulted in prediction with an error probability of less than 15% even for payloads as small as 0.03 bpac (bits per non-zero AC coefficient) and in small images. Huang et al., in a study of the security performance of YASS proves that the Markov Process feature set [10, 15] is the most accurate in detecting YASS [8]. A targeted steganalysis approach that successfully predicts YASS with a high accuracy has been proposed in the work, Steganalysis of YASS [4]. This steganalyzer explores two weaknesses of YASS - the insufficient randomization of the locations of the embedding host blocks and the introduction of zero coefficients by the Quantization Index Modulation embedding. Fisher Linear Discriminant analysis is used for classification.

The proposed work is focused on deploying the blind steganalytic features introduced in our previous work [16] to detect YASS and to further attempt to predict the big block size used during YASS embedding. Our goal is to analyze the performance of this proposed steganalytic model as a universal blind steganalyzer in an attempt to establish a statistical model for a JPEG image. That only five predictor features are being used by our proposed model is very notable. These features are unique, consistent and monotonic in nature.

3. YASS – Yet Another Steganographic Scheme

Given an input image of resolution M×N, the embedding process of YASS consists of the following steps [5]:

a) An image is divided into non-overlapping consecutive B×B (B>8) blocks so as to get $M_B \times N_B$ blocks in the image where $M_B = M/B$ and $N_B = N/B$. Henceforth, B is referred to as 'Big block size'.

b) In each B-block, an 8×8 sub-block is randomly selected using a secret key shared only with the receiver.

c) Two quality factors - design quality factor $QF_{\mathbf{h}}$ and advertised quality factor $QF_{\mathbf{a}}$ of the final JPEG compression are identified.

d) For each sub-block selected in step 'b', a two-dimensional DCT is computed and these coefficients are further divided by quantization steps specified by $QF_{\mathbf{h}}$. This results in an output block with unrounded coefficients.

e) A QIM scheme [17] is employed for data hiding in predetermined non-zero low frequency alternate current (AC) DCT coefficients (called candidate embedding bands). The unrounded coefficients whose rounding values are zeros and un-rounded coefficients which are not in the candidate embedding bands are unaltered thereby preventing unnecessary visual as well as statistical artifacts being introduced. The resulting output blocks from step 'd' are embedded with data and are referred to as data embedded blocks.

f) The data embedded blocks are multiplied with the quantization steps specified by $QF_{\mathbf{h}}$ and further the 2-D inverse DCT is performed (termed as modified blocks).

g) Using the advertised quality factor $QF_{\mathbf{a}}$, the whole image is compressed using the standard JPEG format. Thus resulting in a 'stegged' image. A Repeat Accumulate (RA) encoding framework is used to correct the errors that are caused during JPEG image compression as described in [6].

EYASS introduces further randomness in two stages. Firstly, by randomly selecting the 8×8 embedding blocks from each of the big block size. Next, by the attack aware iterative embedding strategy, referred to as M1 [7], which lowers the error rate while increasing the embedding capacity as compared to the embedding capacity of YASS.

4. Feature Extraction – Huffman Length Statistics and FR Index

4.1. Huffman Length Statistics

Huffman coding, a data compression technique employed in JPEG image format, encodes DCT coefficients that are computed during JPEG compression with variable length codes assigned on statistical probabilities. A grayscale image employs 2 Huffman tables, one each for AC and DC portions. The number of particular lengths of the Huffman codes is unique for a given image of certain size, quality and resolution. The numerical statistics of the DC portion of the Huffman table is referred as Huffman length statistics (H). Almost 90% of the DCT coefficients of an image are encoded using Huffman codes of lengths ranging from 2 to 5 bits. The number of codes of lengths 6 to 16 bits is negligible. Hence we use only statistics of codes of length 2 to 5 bits denoted as H_2, H_3, H_4 and H_5. These features are generated using a Huffman decoder on decompression of the JPEG bit-stream using Matlab as a tool. A considerable variation can be observed in the Huffman code length statistics before and after embedding as illustrated in table 1.

Table 1. Huffman Length Statistics Before and After YASS for 507×788 Image.

Huffman Length Statistics	Notation	Before embedding	After embedding
No. of codes of length 1 bit	H_1	0	0
No. of codes of length 2 bits	$\boldsymbol{H_2}$	**1287**	**3275**
No. of codes of length 3 bits	$\boldsymbol{H_3}$	**549**	**2514**
No. of codes of length 4 bits	$\boldsymbol{H_4}$	**360**	**318**
No. of codes of length 5 bits	$\boldsymbol{H_5}$	**158**	**125**
No. of codes of length 6 bits	H_6	187	104
No. of codes of length 7 bits	H_7	6	0
.	.	.	.
.	.	.	.
No. of codes of length 16 bits	H_{16}	0	0

Some of the scoring features of the proposed Huffman Length Statistics for reliable detection of YASS are as follows:

a) The pseudo random number generator used to locate the 8×8 block in the B×B block successfully confuses a steganalyzer looking for anomalies related to synchronous blocks, however the proposed Huffman Length Statistics reflect the extra bits that are embedded by YASS irrespective of the complexity it uses to distort the steganalyzer's perception of synchronous blocks.

b) The randomized embedding strategy of YASS can successfully evade detection when calibrated features are used as predictors. In contrast to this the Huffman Length Statistics identified by [18], are non-calibrated and are computed from both cover and stego images and are used as predictors for supervised learning.

c) One of the important characteristics of the Huffman coding algorithm is its 'unique prefix property' that is no code is a prefix to any other code, making the codes assigned to the symbols unique. This fact further supports our choice of Huffman Length Statistics as predictor features. The correlation between these

statistics is low as shown in table 4 which reflects on the non-linear nature of these features.

4.2. FR Index: Ratio of File Size to Resolution of an Image

When an image is compressed to the JPEG format, based on the resolution of the image, its quality, the compression ratio and few other factors, the resulting JPEG file takes up a particular file size. This indicates that the file size and the resolution of an image and further its quality are interrelated. Thus the ratio of file size of the image in bytes to that of its resolution is found to be unique and in a certain range for a given resolution, this functional is termed 'FR Index'. In our cover image database, the FR index ranges from 0.0162 to 0.921.

5. Image Database

One of the important aspects of performance evaluation of any steganalyzer is the nature of image database employed in implementation. JPEG images are a popular format for storing, presenting and exchanging images. Grayscale JPEG images are selected for our study as it is harder to detect hidden data in grayscale images as compared to color images where steganalysis can utilize dependencies between color channels. The images used span across a wide vagary of sizes, resolutions and textures.

Table 2. Embedding Setting of YASS and Notations Used (QFh - Quality Factor, QFa - Advertised Quality Factor and B the Big Block Size).

QF_h / QF_a	B (big block size)	Notation
rand(50,60,70) / rand(50,60,70)	9	YASS1
	10	YASS2
	12	YASS3
	14	YASS4
75 / 75	9	YASS5
	10	YASS6
	12	YASS7
	14	YASS8
50 / 75	9	YASS9
	10	YASS10
	12	YASS11
	14	YASS12
50 / 50	9	YASS13
	10	YASS14
	12	YASS15
	14	YASS16

The entire image database used in the experiments consists of over 20,000 images among which over 2,000 are used as cover images. The cover images are taken from the database provided by Memon et al [18]. A subset of 1000 cover images is embedded with 16 different combinations of YASS settings. Embedding with YASS was carried out in Matlab using the

code provided by Anindya Sarkar [7]. This code implements EYASS which is an improvement to YASS. Figure 1 shows a sample of the images that are used in this work.

Three parameters are used in these 16 settings namely; the design quality factor (QF_h), the advertised quality factor (QF_a) and big block size (B). Big block sizes of 9, 10, 12 and 14 are tested against two sets of quality factor settings. The first setting is where QF_h and QF_a are chosen randomly from a combination of 50, 60 and 70, the second set being combinations of quality factors 50 and 75 for QF_h and QF_a respectively. For convenience, in this work we denote these settings of YASS as YASS1, YASS2 upto YASS16. The embedding parameters and its corresponding notation are detailed in table 2. In table 2, 'rand(50,60,70)' implies that the quality factors are chosen randomly amongst these three numbers.

Fig. 1. Images of Different Resolution and with Varying Properties.

5.1 Exploratory Data Analysis of the Image Database

The preliminary data analysis on the image database employed shows that it would be difficult to differentiate between stego and cover images using first order histogram statistics as predictor features to train a classifier. The features described in the previous section are adopted for predictor features.

Table 3. Descriptive Statistics of the Images of QFh/QFa = 50/50 Across Block Sizes 9,10,12,14.

Block Size 9					
	FR Index	H_2	H_3	H_4	H_5
Min	0.0164	18	159	0	0
Max	0.9214	9456	9468	2432	2517
Mean	0.2104	1073.5	4132.7	532.79	357.45
Std Dev.	0.1568	1241.7	1363.7	434.54	429.71
Skewness	1.5378	2.6029	0.2387	1.0495	1.28
Kurtosis	2.3593	8.7716	0.7552	0.7282	1.3049
Block Size 10					
	FR Index	H_2	H_3	H_4	H_5
Min	0.0162	18	163	0	0
Max	0.9214	9456	9468	2432	2517
Mean	0.2105	1071.6	4134.6	532.74	357.47
Std Dev.	0.1568	1241.7	1364.4	434.59	429.7
Skewness	1.5387	2.6123	0.2375	1.0493	1.2801
Kurtosis	2.362	8.8287	0.749	0.7274	1.3052
Block Size 12					
	FR Index	H_2	H_3	H_4	H_5
Min	0.0163	18	158	0	0
Max	0.9214	9456	9468	2432	2517
Mean	0.2104	1069.6	4136.6	532.81	357.47
Std Dev.	0.1568	1241.9	1365.8	434.49	429.7
Skewness	1.5388	2.6268	0.2345	1.0499	1.28
Kurtosis	2.3595	8.9151	0.7386	0.7293	1.3051
Block Size 14					
	FR Index	H_2	H_3	H_4	H_5
Min	0.0162	18	156	0	0
Max	0.9214	9456	9468	2432	2517
Mean	0.2103	1069.5	4136.7	532.89	357.5
Std Dev.	0.1569	1244.7	1367.3	434.46	429.68
Skewness	1.5386	2.6308	0.2325	1.0499	1.2802
Kurtosis	2.357	8.9096	0.7336	0.7296	1.3055

The five identified image features which serve as the inputs for the blind steganalyzer are the FR Index and the Huffman bit code length statistics H_2, H_3, H_4 and H_5. The descriptive statistics along with the first order statistics of the images for the quality factor ratio QF_h/QF_a = 50/50 across the block sizes 9,10,12 and 14 are as shown in table 3.

Further, we employ correlation between the features extracted to derive insight into the nature of the feature space which could further aid the choice of the classifier. The correlation between the features selected, that is the FR Index and the H_2, H_3, H_4 and H_5

extracted from the images, shown in Table 4, for the images where the QF_h/QF_a = 50/50 and the block size being 9.

Table 4. Correlation Values for the Input Attributes Selected for Steganalysis.

	FR Index	H_2	H_3	H_4	H_5
FR Index	1				
H_2	-0.455	1			
H_3	-0.356	-0.175	1		
H_4	0.701	-0.445	-0.101	1	
H_5	0.805	-0.382	-0.305	0.906	1

5.2 Hypotheses Testing in Attempt to Predict the Big Block Size Used.

As explained earlier, one of the main contributions of YASS is the concept of using randomized embedding block size, which is quantitatively measured by 'B', the big block size. If a blind steganalyzer capable of detecting the presence of YASS can also predict big block size used, it would take this work one step further down steganalysis. This is to infer that the steganalyzer not only detects the presence but could also be able to extract the data hidden, atleast the metadata of the data hidden. Hence we test if the features extracted to detect YASS can also be used to predict B amongst the instances predicted positive of steganography. In this section, we test hypotheses to analyze the nature of the predictor features.

Table 5. Descriptive Statistics of the Input Attributes of the 'Stegged' Image Database.

	FR Index	H_2	H_3	H_4	H_5
Mean	0.10268	1566.506	4533.919	218.1265	28.85425
Standard Error	0.00062	21.27569	18.42347	2.400869	0.510775
Median	0.09794	1145.5	4641	185	20
Mode	0.08879	1217	4828	190	0
Standard Deviation	0.03925	1345.593	1165.202	151.8443	32.30423
Sample Variance	0.00154	1810620	1357697	23056.68	1043.563
Kurtosis	0.78522	6.179448	1.158532	2.195515	19.98233
Skewness	0.69407	2.255164	0.108432	1.252017	3.103356
Range	0.26401	8436	9087	1054	392
Minimum	0.0162	177	156	0	0
Maximum	0.28021	8613	9243	1054	392

As the data is non-linear in nature, we selected the Student t-test to test our hypotheses. The mean, standard error, standard deviation, sample variance, kurtosis and skewness of the data under test for the four groups and for the attributes FR Index and H2 is shown in table 6. The results show that it is difficult to differentiate between the groups which vary based on the selected block size.

Table 6. Descriptive Statistics of the Attributes Across the Block Size.

Block	Variable	Mean	Std. Error	Std. Dev.	Sample Variance	Kurtosis	Skewness
9	FR Index	0.102784	0.001248	0.039455	0.001557	0.77117	0.693034
	H_1	1571.439	42.4637	1342.82	1803166	6.157431	2.244415
	H_2	4529.064	36.79504	1163.561	1353875	1.179146	0.116173
	H_3	218.089	4.80496	151.9462	23087.64	2.213984	1.254626
	H_4	28.813	1.021135	32.29112	1042.717	19.82591	3.097035
10	FR Index	0.102866	0.001246	0.039386	0.001551	0.77327	0.688747
	H_1	1567.695	42.50649	1344.173	1806802	6.194359	2.252526
	H_2	4532.863	36.80851	1163.987	1354866	1.170278	0.115298
	H_3	217.993	4.807237	152.0182	23109.53	2.247229	1.260559
	H_4	28.854	1.020254	32.26325	1040.918	19.93517	3.092471
12	FR Index	0.102627	0.001239	0.039174	0.001535	0.80308	0.695695
	H_1	1563.56	42.56516	1346.029	1811793	6.258299	2.267266
	H_2	4536.858	36.86279	1165.704	1358865	1.158694	0.106988
	H_3	218.136	4.798966	151.7566	23030.08	2.176596	1.248134
	H_4	28.851	1.023527	32.36678	1047.608	20.51955	3.138523
14	FR Index	0.102442	0.001235	0.039049	0.001525	0.823497	0.701735
	H_1	1563.328	42.73305	1351.338	1826114	6.218399	2.266519
	H_2	4536.89	36.97586	1169.279	1367214	1.161783	0.09585
	H_3	218.288	4.802985	151.8837	23068.67	2.195138	1.250366
	H_4	28.899	1.02281	32.3441	1046.141	19.96285	3.099141

The result of the 2-tailed t-test gives a Fischer's Test value of 0.027, and a '**t**' value of 0.366, which is not significant, indicating that the null hypotheses (that the sample means are different) cannot be accepted. By this we infer that the big block size (B) cannot be estimated using the input features FR Index, H_2, H_3, H_4 and H_5. However, experiments show that the proposed feature space is effective in detecting YASS.

6. Implementation

6.1. Model

Figure 2 illustrates the Huffman feature extraction model used by the proposed steganalyzer. The model is designed to extract the four Huffman Length Statistics; H_2, H_3, H_4 and H_5 from a grayscale JPEG image using a Huffman decoder. A fast Huffman decoder is used to extract the two Huffman tables, one each of AC and DC portions, the code buffer holds all the codes decoded from which the required statistics (number of 2 to 5 bit code lengths from DC portion only) are selectively separated and fed to the functional space of the classifier.

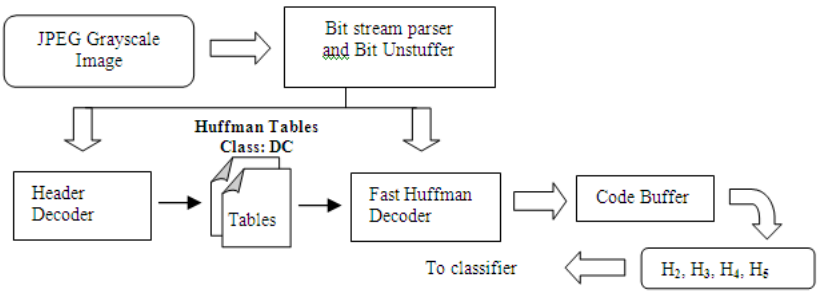


Fig. 2. Proposed Steganalyzer Model Illustrating Huffman Feature Extraction.

6.2. Classification

In any blind statistical steganalyzer, the classifier used for pattern recognition plays a pivotal role. In this work we use three different classifiers to evaluate the features extracted; Artificial Neural Networks (ANN), Support Vector Machines (SVM) and Random Forests (RF). The functional space for these classifiers consists of five variables, the four Huffman Length Statistics; H_2, H_3, H_4 and $H_5$and FR Index and is designed for binary classification to distinguish stego images from genuine ones.

To train and test each classifier for each of the 16 combinations of YASS settings, the following steps are followed:

- The image database is divided into several combinations of training and testing sets for each of the 16 YASS settings tested. In each trial, 60% of the data is used for training the classifier.
- To evaluate the accuracy of the model, the minimal total average probability of error (P_e) is computed, given by:

$$P_e = (P_{FP} + P_{FN})/2 \quad (1)$$

where P_{FP} and P_{FN} are the probability of false positives and false negatives of the test images respectively.

Artificial Neural Networks (ANN) is a computational model that simulates an interconnected group of artificial neurons to process the data [19]. ANNs can be efficiently used for pattern recognition and classification problems. In this work we use a feed forward back-propagation neural network with a single hidden layer of 3 neurons with radial basis function as the activation function. Softmax function is used in the output layer to aid binary classification.

Support Vector Machines (SVM) are a set of related supervised learning methods used for classification and regression. This technique constructs one or more hyperplanes for classification. A good separation is achieved by the hyperplane that has the largest functional margin which leads to a lower generalization error of the classifier [20]. In this work we employ a C type binary class SVM with a Gaussian kernel; the two hyper-parameters of the C-SVMs; penalty parameter C and kernel width γ are estimated using a 10-fold cross-validation employing grid-search over the following multiplicative grid.

$$(C, \gamma) \in [(2i, 2j)| \, i \in \{1, \ldots, 10\}, j \in \{-10, \ldots, 2\}] \quad (2)$$

Random Forests (RF) is an ensemble classifier that comprises of many decision trees and outputs the class that is the mode of the individual tree's output. This method combines Breiman's "bagging" idea and the random selection of features [21] to construct an ensemble of decision trees. The number of trees is kept constant at 500 and the maximum number of nodes is varied from 3 to 9 for a sufficiently low Out-of-Bag (OOB) error with 2 variables tried at each split, these values are computed and assigned by a tune function proposed in R [22].

These techniques are selected to evaluate the proposed model as they can classify non-linear data with a huge number of instances effectively. The performance of each of these classifiers across different bock sizes are described in section 7**,** further error probability (P_e) and ROC are computed, evaluated and compared with existing works in section 7.

7. Results and Performance Analyses

Table 7 illustrates the error probability P_e for all the 16 settings of YASS tested across the classifiers - ANN, SVM and RF. It can be observed that ANN Classifier gives the best and consistent performance of detecting YASS.

Table 7. Error Probability for Various YASS Settings Using ANN, SVM and RF.

YASS Setting	Error Probability P_e (%) for Classifiers		
	ANN	SVM	RF
YASS1	4.83	5.16	4.81
YASS2	3.83	6.67	5.62
YASS3	5.00	6.76	5.56
YASS4	4.50	6.76	5.53
YASS5	4.33	6.89	6.66
YASS6	4.66	6.76	6.19
YASS7	4.83	6.65	5.96
YASS8	4.83	6.65	6.08
YASS9	4.16	7.35	6.55
YASS10	4.16	7.22	6.78
YASS11	4.33	6.89	6.55
YASS12	4.33	7.01	6.55
YASS13	0.50	2.07	0.92
YASS14	0.16	2.07	0.92
YASS15	0.16	2.07	1.03
YASS16	0.16	2.07	1.03

Over all we conclude that the proposed model detects YASS with an accuracy of more than 99% for both QF_h and QF_a set to 50 and for all four big block sizes; 9, 10, 12 and 14. Further, it can be observed the error probability is consistent for several settings of YASS that shows the reliability of the proposed steganalyzer.

The confusion matrix, ROC curve and the accuracy plot for the best (YASS4) and least accuracy (YASS14) of the proposed steganalyzer are shown in figure 3. The 60% of the input data set was selected as the training set, to train the ANN classifier and 40% was used for testing the classifier. Figure 4a shows the scatter plot of the parameters H_5 and FR Index against the target attribute and figure 4b against the predicted target attribute for YASS4 setting. As the accuracy of the proposed model is high, the difference in the scatter plots illustrating the mapping of the attributes (H_5 and FR Index) against the actual target and the predicted target is minimal.

Though the image database is implemented using EYASS, we evaluate against the YASS too as the features extracted in this work do not depend on the further randomization attributed by EYASS. We adopt a four-fold methodology to evaluate the performance of the proposed blind steganalyzer against existing methods. First, the proposed model is compared with the set of 6 blind steganalyzers tested in [6]; secondly, the 2 steganalyzers reported EYASS [7] are used to evaluate. The results are further compared against steganalysis using the four schemes described in [5] for the twelve settings of YASS. Finally, we compare the proposed method against the work in [8] where security performance of YASS against four state-of-the-art blind JPEG steganalyzers is reported.

7.1. Comparison of the Proposed Model Against Blind Steganalyzers Tested in YASS [6]

The original authors of YASS evaluate its steganographic security against the following 6 blind steganalysis schemes [6]. The numbers following the name of the scheme indicate the number of features used in the prediction model; we adopt the same notation as used in [6]. The comparison results are shown in table 8.

1. **Farid-72:** uses wavelet based features for steganalysis [23].
2. **PF-23:** uses DCT based steganalytic feature vectors [24].
3. **PF-274:** uses a combination of Markov and DCT features [9].
4. **DCT hist:** Histogram of DCT coefficients from a low-frequency band [11].
5. **Xuan-39:** uses spatial domain features for steganalysis [12].
6. **Chen-324:** Steganalysis based on statistical moments [13].

7.2. Comparison of Our Proposed Model Against Blind Steganalyzers Used in EYASS [7].

EYASS evaluates the settings for YASS1 using the steganalyzers, PF-274 [9] and Chen-324 [13]. The detection accuracy using PF-274 is found to be 59% and Chen-324 to be 58% whereas the proposed steganalyzer model yields a detection accuracy of 90.34% which is superior to the compared methods.

Table 8. Comparison of the Proposed Model with Blind Steganalyzers Tested in [6].

YASS Settings	Steganalyzer Detection Accuracy						
	Farid-72	PF-23	PF-274	DCT hist	Xuan-39	Chen-324	Proposed Model
YASS5	0.52	0.53	0.59	0.55	0.52	0.54	0.913
YASS6	0.51	0.57	0.60	0.54	0.54	0.55	0.907
YASS7	0.52	0.53	0.62	0.55	0.53	0.53	0.903
YASS8	0.52	0.52	0.54	0.53	0.52	0.53	0.903
YASS9	0.55	0.59	0.77	0.64	0.63	0.75	0.917
YASS10	0.55	0.59	0.79	0.64	0.64	0.65	0.917
YASS11	0.54	0.56	0.74	0.60	0.57	0.60	0.913
YASS12	0.51	0.60	0.65	0.54	0.53	0.55	0.913
YASS13	0.52	0.56	0.58	0.53	0.54	0.57	0.990
YASS14	0.51	0.55	0.56	0.53	0.56	0.51	0.997
YASS15	0.52	0.54	0.53	0.51	0.54	0.55	0.997
YASS16	0.51	0.54	0.55	0.53	0.51	0.54	0.997

7.3. Comparison of Our Proposed Model Against Steganalytic Feature Sets Tested in [5].

A 1,234 dimensional Cross Dimensional Feature (CDF) set for steganalysis is proposed in [5]. Table 9 shows the comparative analysis. The CDF feature set is a combination of three other steganalytic feature sets - MP-486 (uses Markov process features for steganalysis) [10], CC-PEV-548 (uses Cartesian-calibrated Pevny feature set) [5] and SPAM-686 (uses second order Markov chain based features) [14].

Table 9. Comparison of our proposed model with blind steganalyzers tested in [5].

Steganalyzer	MP-486	CC-PEV-548	SPAM-686	CDF-1234	Proposed Model
YASS5 P_e (%)	15.5	16.4	15.2	9.7	4.33
YASS6 P_e (%)	27	26	14.5	12.4	4.66

7.4. Comparison of Our Proposed Model Against Steganalytic Feature Sets Tested in [8].

YASS is tested against four state-of-the-art steganalyzers in [8]. Chen-324, MP-486, PF-274 are tested besides a fourth steganalyzer that uses the same features of PF-274 but without calibration, we denote this steganalyzer as NonClbPF-274. The comparative results are shown in table 10. The classification results obtained using only the ANN classifier only is tabulated.

8. Conclusions and Future Work

The proposed work evaluates the proposed blind steganalyzer to attack YASS; the performance analyses show that the detection accuracy is consistent over a wide range of YASS settings and much superior to most other blind steganalyzers in vogue..

The features used in this statistical steganalyzer are unique when evaluated against several classifier techniques; moreover the proposed model employs only a 5-dimensional feature vector as compared to several reliable attacks that use several hundreds of features.

Our future work includes analyzing settings of the variance parameter in Extended YASS. Further we attempt to extend the existing model to a multi-class classification problem to predict block size by using extra features.

Table 10. Comparison of Our Proposed Model with Blind Steganalyzers Tested in [8].

YASS Setting	Chen-324	MP-486	PF-274	NoClbPF-274	Proposed Model
YASS5	79.1	80.4	87.2	83.2	91.3
YASS6	80.8	80.4	86.3	85.4	90.7
YASS7	69.3	71.7	77.8	73.8	90.3
YASS8	61.5	63.4	68.9	66.3	90.3
YASS9	96.3	97.2	96.6	97.2	91.7
YASS10	98.5	98.7	98.6	98.7	91.7
YASS11	93.2	94.4	95.3	94.4	91.3
YASS12	82.1	83.0	88.0	85.5	91.3
YASS13	83.9	85.8	87.7	88.0	99.0
YASS14	84.1	86.0	89.5	89.4	99.7
YASS15	72.4	75.0	81.1	79.7	99.7
YASS16	64.4	67.2	72.5	70.6	99.7

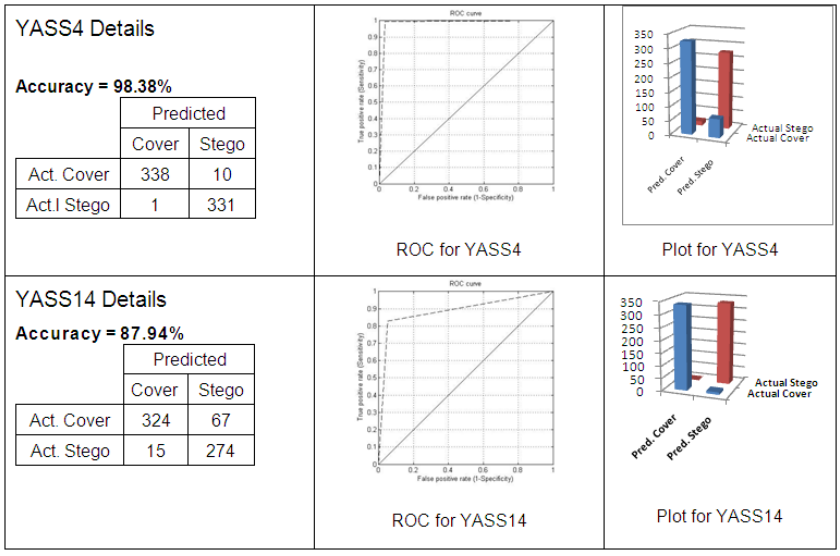
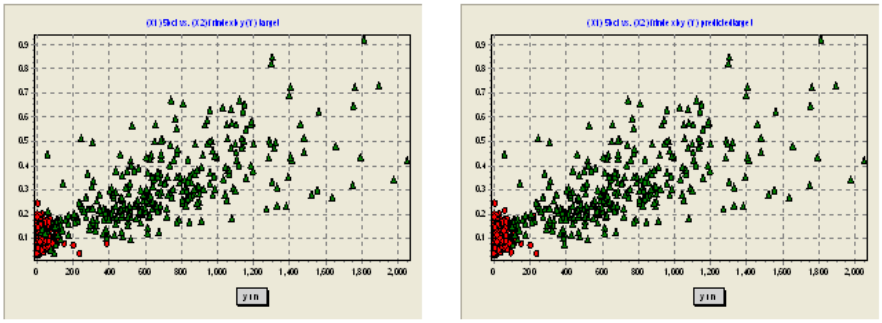


Fig. 3. Confusion Matrix, ROC Curve, Accuracy Plot for the Best and Least Accuracy of the Proposed Steganalyzer.



(4a) (4b)

Fig. 4. Scatter Plots Depicting H5 (X axis) and FR Index (Y axis) Against Actual Target (4a) and Predicted Target (4b) for YASS1.

References

[1] B.Li, J.He, J.Huang and Y.Q.Shi, "A Survey on Image Steganography and Steganalysis", Journal of Information Hiding and Multimedia Signal Processing, vol.2, number 2, April 2011.

[2] J. Kodovsk´y and J.Fridrich, "Calibration Revisited", In Proceedings of the 11th ACM Workshop on Multimedia and Security, New York, USA, 2009, pp. 63–74.

[3] D.Fu, Y.Q.Shi, D.Zou and G.Xuan, "JPEG Steganalysis using Empirical Transition Matrix in Block DCT Domain", In International Workshop on Multimedia Signal Processing, Victoria, BC, Canada, 2006.

[4] Li Bin, Huang Jiwu and Shi Qing Yuni, "Steganalysis of YASS", In IEEE Transactions on Information Forensics and Security, 2009, vol. 3, pp. 369-382.

[5] J.Kodovsky, T.Pevny and J.Fridrich, "Modern Steganalysis can Detect YASS", In Proceedings of SPIE, Electronic Imaging, Media Forensics and Security XII, San Jose, CA 2010.

[6] K.Solanki, A.Sarkar and B.S.Manjunath, "YASS: Yet Another Steganographic Scheme that Resists Blind Steganalysis", In Proceedings of 9th International Workshop on Information Hiding, 2007, pp. 16-31.

[7] K.Solanki, A.Sarkar, A and B.S.Manjunath, "Further Study on YASS: Steganography based on Randomized Embedding to Resist Blind Steganalysis", In Proceedings of SPIE, San Jose, CA, 2008, vol. 6819, pp. 16-31.

[8] F.Huang, J.Huang, and Y.Q.Shi, "An Experimental Study on the Security Performance of YASS", In IEEE press.

[9] T.Pevn´y and J.Fridrich, "Merging Markov and DCT Features for Multi-class JPEG Steganalysis", In Proceedings of SPIE, 2007, vol. 6505, pp. 03-04.

[10] Y.Q.Shi, C.Chen and W.Chen, "A Markov Process based Approach to Effective Attacking JPEG Steganography", In 8th International Workshop on Information Hiding, LNCS- Springer-Verlag, Alexandria, VA , 2006, vol. 4437, pp. 249–264.

[11] K.Solanki, K.Sullivan, U.Madhow, B.S.Manjunath and S.Chandrasekaran, "Probably Secure Steganography: Achieving Zero K-L Divergence using Statistical Restoration", In Proceedings of ICIP, Atlanta, GA, USA, 2006, pp. 125–128.

[12] G.Xuan, et al. "Steganalysis based on Multiple Features Formed by Statistical Moments of Wavelet Characteristic Functions", In Proceedings of 7th International Workshop on Information Hiding, LNCS, 2005.

[13] C.Chen, Y.Q.Shi, W.Chen and G.Xuan, "Statistical Moments based Universal Steganalysis using JPEG-2D Array and 2-D Characteristic Function", In Proceedings of ICIP, Atlanta, GA, USA, 2006, pp.105–108.

[14] T.Pevný, P.Bas and J.Fridrich, "Steganalysis by Subtractive Pixel Adjacency Matrix", In Proceedings of the 11th ACM Multimedia and Security Workshop, Princeton, 2009, pp. 75–84.

[15] C.Chen and Y.Q.Shi, "JPEG Image Steganalysis Utilizing both Intrablock and Interblock Correlations" , In Proceedings of International Symposium on Circuits and Systems, 2008, pp. 3029–3032.

[16] V.H.Bhat, S.Krishna, P.D.Shenoy, K.R.Venugopal and L.M.Patnaik, "JPEG Steganalysis using HBCL Statistics and FR Index", In Intelligence and Security Informatics, LNCS- Springer-Verlag,, 2010, vol. 6122/2010, pp. 105-112.

[17] B.Chen and G.W.Wornell, "Quantization Index Modulation: A class of Provably Good Methods for Digital Watermarking and Information Embedding", In IEEE Transactions on Information Theory, 2001, vol. 47, pp. 1423-1443.

[18] M.Kharrazi, H.T.Sencar, N.Memon, "A Performance Study of Common Image Steganography and Steganalysis Techniques", Journal of Electronic Imaging, 2006, vol. 15, issue 4.

[19] C.Bishop, "Neural Networks for Pattern Recognition", Oxford, Oxford University, UK, 1995.

[20] C.Burges, "A Tutorial on Support Vector Machines for Pattern Recognition", Data Mining and Knowledge Discovery, 1998, vol. 2, pp. 121-167.

[21] Ho.Tin, "Random Decision Forest", In Third International Conference on Document Analysis and Recognition, 1995, pp. 278-282.

[22] Random Forests, http://debian.mc.vanderbilt.edu/R/CRAN/web/packages/ randomForest/ randomForest.pdf

[23] S.Lyu and H.Farid, "Detecting Hidden Messages using Higher-order Statistics and Support Vector Machines", In Proceedings of 5th International Workshop on Information Hiding, LNCS- Springer-Verlag, 2002, vol. 2578.

[24] T.Pevny and J.Fridrich, "Multi-class Blind Steganalysis for JPEG Images", In Proceedings of SPIE, San Jose, CA, 2006, vol. 6072 pp. 1-13.

Authors

Veena H Bhat is a research scholar, currently pursuing Ph.D in the area of Data Mining. She is working as a Professor at IBS-Bangalore in Department of IT and Systems. She has completed her Bachelors in Electronics and Communications (1991) from Karnataka Regional Engineering College, Surathkal and Masters in Information Technology (2005) from University Visvesvaraya College of Engineering, Bangalore University, Bangalore. Her stint in the software industry, working with PSI-Bull India, Tata Consultancy Services and Titan Industries Limited has helped her to have a good industry-academics perspective. Her research interests include Data Mining, Business Intelligence and Digital Forensics.

Krishna S is pursuing his Bachelors in Electronics and Communication Engineering at University Visvesvaraya College of Engineering, Bangalore University, Bangalore. His research interests include Data Mining, Image Processing and Signal Processing.

P Deepa Shenoy obtained her Ph.D in Computer Science and Engineering from the Bangalore University. Currently she is working as a Professor, Department of Computer Science and Engineering, at University Visvesvaraya College of Engineering, Bangalore University, Bangalore. She received Bachelors and Masters degree from Bangalore University. She has published more than seventy research papers in international conferences and journals. Her research interests are Soft Computing, Data Mining and Bio-metrics.

K R Venugopal is currently Principal, University Visvesvaraya College of Engineering (U.V.C.E), Bangalore University, Bangalore. He obtained his Bachelor of Engineering from U.V.C.E. He received his Masters degree in Computer Science and Automation from Indian Institute of Science, Bangalore. He was awarded Ph.D in Economics from Bangalore University and Ph.D in Computer Science from Indian Institute of Technology, Chennai. He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science and Journalism. He has authored 27 books on Computer Science and Economics which include Petro Dollar and World Economy, Mastering C, Microprocessor Programming, Mastering C++ etc. He has also been serving as Professor and Chairman, Department of Computer Science and Engineering, U.V.C.E, Bangalore University, Bangalore. During his three decades of service at U.V.C.E, he has over 250 research papers to his credit. His research interests include Computer Networks, Parallel and Distributed Systems, Digital Signal Processing and Data Mining.

L M Patnaik is Vice Chancellor, Defence Institute of Advanced Technology, Pune, India. He was a Professor with Department of Computer Science and Automation, Indian Institute of Science (IISc) - Bangalore since 1986. During the past 35 years of his service at IISc, he has over 600 research publications in refereed international journals and conference proceedings. He is a Fellow of all the four leading science and engineering academics in India, Fellow of IEEE and the Academy of Science for the Developing World. He has received twenty national and international awards, notable among them is the IEEE Technical Achievement Award for his significant contributions to High Performance Computing and Soft Computing. His areas of research interests have been Parallel and Distributed Computing, Mobile Computing, CAD for VLSI circuits, Soft Computing and Computational Neuroscience.