Annales UMCS Informatica AI XII, 3 (2012) 121–139
DOI: 10.2478/v10065-012-0026-y

Annales UMCS
Informatica
Lublin-Polonia
Sectio AI
http://www.annales.umcs.lublin.pl/

Performance Evaluation of Different Universal Steganalysis Techniques in JPG Files

Ashraf M. Emam[1] , Mahmoud M. Ouf[2]

[1] *Associate Professor of Computer Science Institute of Graduate Studies and Research Alexandria University*
[2] *Lecturer of Programming Language Information Technology Institute Ministry of Communication and Information Technology*

Abstract – Steganalysis is the art of detecting the presence of hidden data in files. In the last few years, there have been a lot of methods provided for steganalysis. Each method gives a good result depending on the hiding method. This paper aims at the evaluation of five universal steganalysis techniques which are "Wavelet based steganalysis", "Feature Based Steganalysis", "Moments of characteristic function using wavelet decomposition based steganalysis", "Empirical Transition Matrix in DCT Domain based steganalysis", and "Statistical Moment using jpeg2D array and 2D characteristic function". A large Dataset of Images -1000 images- are subjected to three types of steganographic techniques which are "Outguess", "F5" and "Model Based" with the embedding rate of 0.05, 0.1, and 0.2. It was followed by extracting the steganalysis feature used by each steganalysis technique for the stego images as well as the cover image. Then half of the images are devoted to train the classifier. The Support vector machine with a linear kernel is used in this study. The trained classifier is then used to test the other half of images, and the reading is reported The "Empirical Transition Matrix in DCT Domain based steganalysis" achieves the highest values among all the properties measured and it becomes the first choice for the universal steganalysis technique.

1 Introduction

Steganography is the art of writing a hidden message in a way that no one except the sender and the receiver can realize that there is a hidden message [**1**]. This is the old definition, Today, Steganography includes concealment of digital information within seemingly innocuous carriers.

The success of the steganography plan refers to: the two parties must have a reason for communicating, and the behaviour of communication must not change.

Today's steganographic methods use images or audio files to hide data, the information that needs to be concealed is dispersed within the least significant bits of a carrier file, which serves as a hiding place. It is important that the carrier files do not lose their actual appearance during the embedding process.

All digital file formats can be used for Steganography, but the formats that are more suitable are those with a high degree of redundancy [**2**]. The redundant bits of an object are those bits that can be altered without the alteration being detected easily [**3**].

1.1 Image Steganographic techniques

Due to the high degree of redundancy present in digital images (despite compression), there has been an increased interest in using digital images as cover-objects for the purpose of steganography. There has been much more work on embedding techniques which make use of the transform domain or more specifically JPEG images due to their wide applicability.

Image steganography techniques can be divided into two groups: those in the Image Domain and those in the Transform Domain [**4**].

The image (spatial) domain techniques embed messages in the intensity of the pixels directly, while for the transform (frequency) domain, images are first transformed and then the message is embedded in the image [**5**].

The image domain techniques encompass bit-wise methods that apply bit insertion and noise manipulation and are sometimes characterized as "simple systems" [**6**]. The image formats that are most suitable for the image domain steganography are lossless. Steganography in the transform domain involves the manipulation of algorithms and image transforms [**6**]. These methods hide messages in more significant areas of the cover image, making it more robust [**7**]. Many transform domain methods are independent of the image format and the embedded message may survive conversion between lossy and lossless compression.

1.2 JPEG Steganography (Transform Domain)

Originally it was thought that it would not be possible to use Steganography with JPEG images because they use lossy compression which results in parts of the image data being altered. However, the most important characteristics of Steganography is that information is hidden in the redundant bits of an object and since redundant bits are left out when using JPEG, it was feared that the hidden message would be destroyed.

One of the properties of JPEG is exploited to make the changes to the image invisible to the human eye. During the DCT transformation phase of the compression algorithm, rounding errors occur in the coefficient data that are not noticeable [**8**]. Although this

property is what classifies the algorithm as being lossy, this property can be also used to hide messages.

It is neither feasible nor possible to embed information in an image that uses lossy compression, since the compression would destroy all information in the process.

1.2.1 Outguess

Outguess proposed by Provos [**9**] performs the embedding process in two steps. First, it identifies the redundant DCT coefficients that have minimal effect on the cover image, and then chooses bits in which it would embed the message.

1.2.2 F5

F5 [**10**] was proposed by Westfeld and embeds messages by modifying the DCT coefficients. The most important operation done by F5 is matrix embedding with the goal of minimizing the amount of changes made to the DCT coefficients.

1.2.3 Model Based Embedding Technique

The model-based technique, proposed by Sallee, [**11**] tries to model statistical properties of an image and preserves them during the embedding process. Sallee breaks down the transformed image coefficients into two parts and replaces the perceptually insignificant component with the coded message bits.

1.2.4 Image Steganalysis

Steganalysis is the art and science of detecting messages hidden using Steganography. The art of Steganalysis plays a major role in the selection of features or characteristics a typical stego message might exhibit while the science helps in reliable testing the selected features for the presence of hidden information [**12**].

1.3 Steganalysis Techniques

The Steganalysis Techniques are classified into two categories:

1.3.1 Specific Steganalysis

The specific detection consists of subjective and statistical methods. The subjective methods make use of human eyes to look for suspicious artifacts in the image.

The statistical methods perform mathematical analysis of the images to find the discrepancy between the original and stego images.

1.3.2 Universal Steganalysis

The general Steganalysis detection methods provide detection regardless of the steganographic techniques. They involve the extraction of image features and the

classification of the input image into containing the embedded message or not having the hidden message. The following is the description of 5 states of the art universal Steganalysis techniques used to detect hidden data in the JPEG files and will be used during this research.

Wavelet based Steganalysis A Steganalysis approach is provided by Farid et al [**13**] to detect hidden messages in images based on wavelet-like decomposition to build higher order statistical models of natural images.

The decomposition is based on separable quadrature mirror filters (QMFs) [**14, 15, 16**]. This decomposition splits the frequency space into multiple scales and orientations. This is accomplished by applying separable lowpass and highpass filters along the image axes generating vertical, horizontal, diagonal and lowpass subbands. Subsequent scales are created by recursively filtering the lowpass subband.

Feature Based Steganalysis In her paper [**17**], Jessica provides a new steganalysis method which combines the concept of calibration with the feature-based classification to devise a blind detector specific to the JPEG images. By calculating the features directly in the JPEG domain rather than in the wavelet domain, it appears that the detection can be made more sensitive to a wider type of embedding algorithms because the calibration process increases the features' sensitivity to the embedding modifications while suppressing image-to-image variations. Another advantage of calculating the features in the DCT domain is that it enables more straightforward interpretation of the influence of individual features on detection as well as easier formulation of design principles leading to more secure Steganography.

Moments of characteristic function using wavelet decomposition based steganalysis: Shi et al. [**18**], proposed a new steganalysis technique depending on the statistical moments of characteristic functions of the image, its prediction-error image and their discrete wavelet subbands are selected as features. It has been shown that the usage of the moments of characteristic functions, the moments from all of wavelet subbands including the low-low (LL) subbands.

1.3.3 Empirical Transition Matrix in the DCT Domain based steganalysis

Fu et al [**19**] proposed a new steganalysis techniques, Markov empirical transition matrices are proposed to capture both intra-block and inter-block dependencies between the block-DCT coefficients in the JPEG image Since the hidden messages are sometimes independent of the cover data, the embedding process often decreases the dependencies exiting in the original cover data to some extent. Therefore, the proposed second order statistics can capture such kind of changes. To reduce high dimensionality of the proposed empirical transition matrices, a threshold technique is applied to generate efficient features. Some of the steganographic methods have made great efforts to maintain the marginal histogram of the block- DCT coefficients (first order statistics)

or try to keep the histogram appear unchanged by decreasing or increasing the DCT coefficient values by only one. This fact suggests that the steganalysis schemes based only on the first order statistics are not sufficient. In this method, they propose to employ higher order statistics for steganalyzing the JPEG steganography.

1.3.4 Statistical Moment using jpeg2D array and 2D characteristic function:

Chen et al [**20**], developed a new universal steganalysis method based on statistical moments derived from both image 2-D array and JPEG 2-D array. In addition to the first order histograms, the second order histograms are considered. Consequently, the moments of 2-D characteristic functions are also utilized for steganalysis.

1.4 Classifiers

There is a number of detectors for steganography. Some return a binary decision (something embedded / nothing embedded). In most cases this decision is based on comparison with a predefined threshold. The reliability can be judged by the detector's error rate.

The calculated feature vectors obtained from each universal steganalysis technique are used to train a classifier. We have used The Support Vector Machine:

1.4.1 Support Vector Machine (SVM)

The support vector machines (SVMs) are a set of related supervised learning methods used for classification and regression [**21**]. The support Vector Machine (SVM) is a classification and regression prediction tool that uses machine learning theory to maximize predictive accuracy while automatically avoiding over-fit to the data. The formulation uses the Structural Risk Minimization (SRM) principle, which is superior, to the traditional Empirical Risk Minimization (ERM) principle, used by the conventional neural networks. SVMs were developed to solve the classification problem [**22**]. A classification task usually involves training and testing data which consist of some data instances. Each instance in the training set contains one "target value" (class labels) and several "attributes" (features). The goal of SVM is to produce a model which predicts targets value of data instances in the testing sets which are given only the attributes.

2 Experimental Work

2.1 Prepare a set of Images to act as cover images

The data set used is a collection of 1000 images with the quality factor 80%, and the size $512 * 768$ or $768 * 512$.

2.2 Embed message in the different cover to get the stego

The DCT domain embedding techniques are very popular due to the fact that the DCT-based image format gives high compression and a small size image. JPEG is widely used in the public domain in addition to being the most common output format of digital cameras. Various steganographic embedding methods are proposed, with the purpose of minimizing the statistical artifacts introduced to the DCT coefficients.

Here, three embedding techniques, Outguess, F5 and Model based are used with the embedding rates of 0.05, 0.1, 0.2.

2.3 Get the Statistical properties of all images (cover and stego)

Implementation of different steganalysis techniques is made to get the statistical properties measured by each technique.

2.4 Choosing a classifier

From the defined classifiers, the Support Vector Machine is used in this research because it is more powerful, but on the other hand, it requires more computational power, especially if a nonlinear kernel is employed. To avoid high computational cost and to obtain a reasonable success, a linear SVM has been used. There are two classes for the cover image, and the others for the stego image. To train and use the classifier, LIBSVM [**23**], is used. LIBSVM is a library for SVM, contains classes that perform training, and classification.

2.5 Training the classifier

- Half of the images (cover and stego) are used for training
- The Problem class encapsulates a problem, or a set of vectors which must be classified. Its constructor takes
  - Number of training data
  - Cover or stego value
  - Calculated features
  - Number of calculated features
- The Parameter class contains various parameters which can affect the way in which SVM is learned (i.e. the kernel function)
- The Model class encapsulates the SVM model. It has no constructor but its object is always created using the static member Train of the class Training.
- The Train method (static member of the Training class) takes 2 objects: object from the Problem class, and object from the Parameter class and return an object from the Model class which contains the trained SVM Model.

2.6 Use the trained classifier to distinguish between the cover and the stego file

The class Prediction has a static method named Predict which takes an object from the Model class which contains the trained SVM Model, and the feature of the image that we want to classify. The Predict Method returns a value representing cover or a stego image.

2.7 Analyzing the results

Most of the universal steganalysis techniques return binary decision (contain hidden data / do not contain hidden data). In most cases the decision is based on comparison with a predefined threshold.

In the research, after training the classifier, and testing an image, one of the following results can be obtained. The classifier gives right data, or the classifier gives wrong data even if it classifies the image with hidden data and actually it does not contain hidden data or, if it classifies the image without hidden data and actually it contains hidden data. This can be summarized in the contingency table. Table 1.

Table 1. Contingency table.

Actual Image	Classifier result	Classification
Contain Hidden Data	Contain Hidden Data	True
Contain Hidden Data	No Hidden Data	Error (Type I)
No Hidden Data	Contain Hidden Data	Error (Type II)
No Hidden Data	No Hidden Data	True

Here appear two types of error:

Error (Type I)

This type of error is called also False Positive (FP), because it gives a false indication (No Hidden Data) while the actual image is Positive (Contains Hidden Data)

Error (Type II)

This type of error is called False Negative (FN) because it gives a false indication (Contains Hidden Data) and the actual image is Negative (No Hidden Data) From the contingency table we can get several evaluation metrics.

2.8 False Positive Rate (FPR)

Tthe proportion of negative instances that were reported as being positive is:

$$FPR = \frac{FP}{N} = \frac{FP}{FP - TN}. \tag{1}$$

2.9 True Positive Rate (TPR)”Sensitivity"

This is equivalent to sensitivity, which measures the proportion of actual positives which are correctly identified.

$$TPR = \frac{TP}{P} = \frac{TP}{TP - FN}. \tag{2}$$

2.9.1 Specificity

It measures the proportion of negatives which are correctly identified; it is equal to 1 – False Positive Rate

$$Specificity = \frac{TN}{P} = \frac{TN}{FP - TN}. \tag{3}$$

2.9.2 Accuracy

Accuracy is the degree of conformity of a measured or calculated quantity to its actual (true) value. Accuracy is closely related to precision.

$$Accuracy = \frac{TP + TN}{P + N}. \tag{4}$$

Sensitivity and specificity are statistical measures of the performance of a binary classification test. The relationship between sensitivity and specificity, as well as the performance of the classifier, can be visualized and studied using the ROC curve.

3 Experimental Results

Each experiment has been repeated 10 times and the average is taken. 1000 pictures are used and hiding data with different rates in these samples gives 2000 pictures in each rate (1000 covers and 1000 stegoes). The half of these samples is used for training, and the other half is used for testing.

3.1 The Wavelet Based Steganalysis

The above Table 2 presents the data obtained when applying the wavelet based steganalysis with different steganographic method techniques used (Outguess, F5, and Model Based) and the embedding rates (0.05, 0.1. 0.2)

3.2 The Feature Based Steganalysis

Table 3 presents the data obtained when applying the feature based steganalysis on different steganographic method techniques used (Outguess, F5, and Model Based) with the embedding rates (0.05, 0.1. 0.2).

Table 2. The data of Wavelet Based Steganalysis.

Hiding Method	Embedding rate	True Negative (TN)	True Positive (TP)	False Positive (FP)	False Negative (FN)
OutGuess	0.05	295	288	205	212
	0.1	350	318	150	182
	0.2	409	376	91	124
F5	0.05	278	248	222	252
	0.1	278	242	222	258
	0.2	278	277	222	223
Model Based	0.05	243	266	257	234
	0.1	260	262	240	238
	0.2	262	284	238	216

Table 3. The data of Feature Based Steganalysis.

Hiding Method	Embedding rate	True Negative (TN)	True Positive (TP)	False Positive (FP)	False Negative (FN)
OutGuess	0.05	249	377	251	123
	0.1	345	417	155	83
	0.2	450	468	50	32
F5	0.05	230	305	270	195
	0.1	292	317	208	183
	0.2	387	386	113	114
Model Based	0.05	335	267	165	233
	0.1	351	290	149	210
	0.2	388	340	112	160

3.3 The Moments of characteristic function using the wavelet decomposition based steganalysis

The above Table 4 presents the data obtained when applying the data of moments of characteristic function using the wavelet decomposition based steganalysis on different steganographic method techniques used (Outguess, F5, and Model Based) with embedding rates (0.05, 0.1. 0.2).

3.4 Empirical Transition Matrix in the DCT Domain based Steganalysis

Table 5 presents the data obtained when applying the data of Empirical Transition Matrix in the DCT Domain based steganalysis on different steganographic method

Table 4. The data of the moments of characteristic function using the wavelet decomposition Based Steganalysis.

Hiding Method	Embedding rate	True Negative (TN)	True Positive (TP)	False Positive (FP)	False Negative (FN)
OutGuess	0.05	278	293	222	207
	0.1	307	332	193	168
	0.2	362	388	138	112
F5	0.05	290	225	210	275
	0.1	273	250	227	250
	0.2	298	316	202	184
Model Based	0.05	285	246	215	254
	0.1	288	283	212	217
	0.2	316	333	184	167

Table 5. The data of Empirical Transition Matrix in the DCT Domain based steganalysis.

Hiding Method	Embedding rate	True Negative (TN)	True Positive (TP)	False Positive (FP)	False Negative (FN)
OutGuess	0.05	365	371	135	129
	0.1	433	447	67	53
	0.2	481	483	19	17
F5	0.05	283	285	217	215
	0.1	331	340	169	160
	0.2	418	429	82	71
Model Based	0.05	364	376	136	124
	0.1	439	445	61	55
	0.2	486	485	14	15

techniques used (Outguess, F5, and Model Based) with the embedding rates (0.05, 0.1. 0.2).

3.5 Statistical Moment using the jpeg2D array and 2D characteristic function

The above Table 6 presents the data obtained when applying the data of the Statistical Moment using the jpeg2D array and 2D characteristic function on different steganographic method techniques used (Outguess, F5, and Model Based) with the embedding rates (0.05, 0.1. 0.2).

Table 6. The data of the Statistical Moment using the jpeg2D array and 2D characteristic function.

Hiding Method	Embedding rate	True Negative (TN)	True Positive (TP)	False Positive (FP)	False Negative (FN)
OutGuess	0.05	278	293	222	207
	0.1	307	332	193	168
	0.2	362	388	138	112
F5	0.05	290	225	210	275
	0.1	273	250	227	250
	0.2	298	316	202	184
Model Based	0.05	285	246	215	254
	0.1	288	283	212	217
	0.2	316	333	184	167

3.6 Parameter calculation

The data recorded from Table 2 to Table 6, describes the effects of different steganalysis techniques on different Steganographic techniques in terms of "True Negative", "True Positive", "False Negative", False Positive". But these data itself can not be an indication. So, some calculation has to be done to convert these data to some distinguished properties such as "Sensitivity", "Accuracy", and "Specifity".

3.6.1 Sensitivity

As indicated before, Sensitivity or "True Positive Rate" measures the proportion of actual positives which are correctly identified.

$$TPR = \frac{TP}{p} = \frac{TP}{TP + FN}. \tag{5}$$

Table 7. Sensitivity values of different steganalysis techniques applied to different steganographic techniques with different embedding rates.

Figs 1, 2 and 3 show the sensitivity of the steganalysis techniques studied with the embedding rates 0.05, 0.1, 0.2 for Outguess, F5 and Model Based respectively

3.6.2 Accuracy

Accuracy is the degree of conformity of a measured or calculated quantity to its actual (true) value. Accuracy is closely related to precision.

$$Accuracy = \frac{TP + TN}{P + T}. \tag{6}$$

Table 7. Calculated True Positive Rate for different steganalyses.

		Wavelet Based			Feature Based			Moment of CF			Empirical Transition			JPEG 2D Array and 2D CF		
	Embedding rate	TP	FN	TPR	TP	FN	TPR	TP	FN	TPR	TP	FN	TPR	TP	FN	TPR
OG	0.05	288	212	0.576	377	123	0.754	293	207	0.586	371	129	0.742	354	146	0.708
OG	0.1	318	182	0.636	417	83	0.834	332	168	0.664	447	53	0.894	437	63	0.874
OG	0.2	376	124	0.752	468	32	0.936	388	112	0.776	483	17	0.966	478	22	0.956
F5	0.05	248	252	0.496	305	195	0.61	225	275	0.45	285	215	0.57	272	228	0.544
F5	0.1	242	258	0.484	317	183	0.634	250	250	0.5	340	160	0.68	308	192	0.616
F5	0.2	277	223	0.554	386	114	0.772	316	184	0.632	429	71	0.858	381	119	0.762
MB	0.05	266	234	0.532	267	233	0.534	246	254	0.492	376	124	0.752	295	205	0.59
MB	0.1	262	238	0.524	290	210	0.58	283	217	0.566	445	55	0.89	379	121	0.758
MB	0.2	284	216	0.568	340	160	0.68	333	167	0.666	485	15	0.97	453	47	0.906

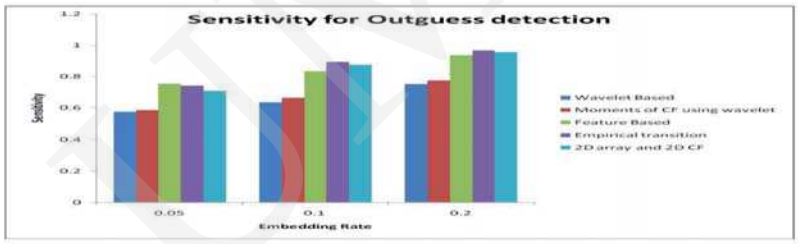

Fig. 1. Sensitivity for Outguess detection.

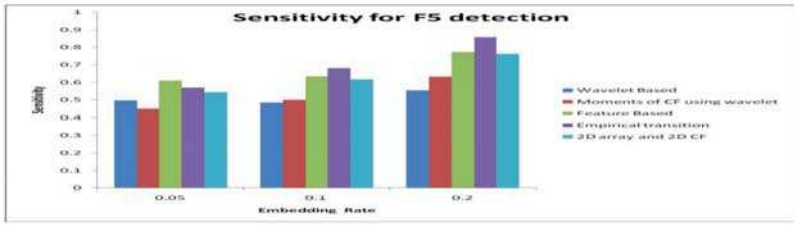

Fig. 2. Sensitivity for F5 detection.

Table 8. The Accuracy values of different steganalysis techniques applied to different steganographic techniques with different embedding rates.

Figs 4, 5 and 6 show the accuracy of the steganalysis techniques studied with the embedding rates 0.05, 0.1, 0.2 for Outguess, F5 and Model Based respectively

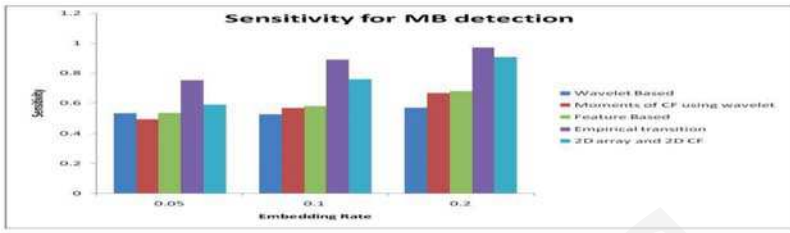

Fig. 3. Sensitivity for MB detection.

Table 8. Calculated Accuracy for different steganalyses.

		Wavelet Based			Feature Based			Moments of CF using wavelet			Empirical transition			2D array and 2D CF		
	Embedding rate	TN	TP	Acc	TN	TP	Acc	TN	TP	Acc	TN	TP	Acc	TN	TP	Acc
OG	0.05	295	288	0.583	249	377	0.626	278	293	0.571	365	371	0.736	356	354	0.71
OG	0.1	350	318	0.668	345	417	0.762	307	332	0.639	433	447	0.88	422	437	0.859
OG	0.2	409	376	0.785	450	468	0.918	362	388	0.75	481	483	0.964	465	478	0.943
F5	0.05	278	248	0.526	230	305	0.535	290	225	0.515	283	285	0.568	266	272	0.538
F5	0.1	278	242	0.52	292	317	0.609	273	250	0.523	331	340	0.671	294	308	0.602
F5	0.2	278	277	0.555	387	386	0.773	298	316	0.614	418	429	0.847	364	381	0.745
MB	0.05	243	266	0.509	335	267	0.602	285	246	0.531	364	376	0.74	326	295	0.621
MB	0.1	260	262	0.522	351	290	0.641	288	283	0.571	439	445	0.884	375	379	0.754
MB	0.2	262	284	0.546	388	340	0.728	316	333	0.649	486	485	0.971	434	453	0.887

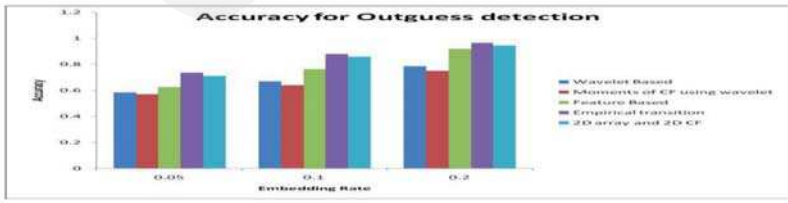

Fig. 4. Accuracy for Outguess detection.

3.7 Specifity

It measures the proportion of negatives which are correctly identified, it is equal to 1 – False Positive Rate

$$Specificity = \frac{TN}{P} = \frac{TN}{FP + TN}. \tag{7}$$

Table 9. The specifity values of different steganalysis techniques applied to different steganographic techniques with different embedding rates.

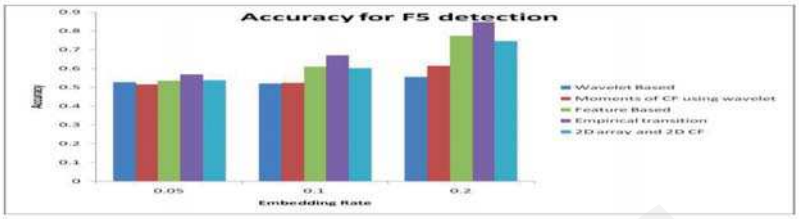

Fig. 5. Accuracy for F5 detection.

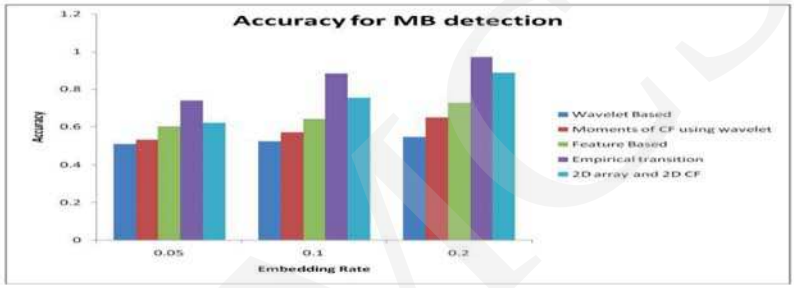

Fig. 6. Accuracy for MB detection.

Table 9. Specifity Calculation for different steganalyses.

		Wavelet Based			Feature Based			Moments of CF using wavelet			Empirical transition			2D array and 2D CF		
	embedding rate	TN	FP	Spec.	TN	FP	Spec.	TN	FP	Spec.	TN	FP	Spec.	TN	FP	Spec.
OG	0.05	295	205	0.59	249	251	0.5	278	222	0.556	365	135	0.73	356	144	0.712
OG	0.1	350	150	0.7	345	155	0.7	307	193	0.614	433	67	0.866	422	78	0.844
OG	0.2	409	91	0.82	450	50	0.9	362	138	0.724	481	19	0.962	465	35	0.93
F5	0.05	278	222	0.56	230	270	0.5	290	210	0.58	283	217	0.566	266	234	0.532
F5	0.1	278	222	0.56	292	208	0.6	273	227	0.546	331	169	0.662	294	206	0.588
F5	0.2	278	222	0.56	387	113	0.8	298	202	0.596	418	82	0.836	364	136	0.728
MB	0.05	243	257	0.49	335	165	0.7	285	215	0.57	364	136	0.728	326	174	0.652
MB	0.1	260	240	0.52	351	149	0.7	288	212	0.576	439	61	0.878	375	125	0.75
MB	0.2	262	238	0.52	388	112	0.8	316	184	0.632	486	14	0.972	434	66	0.868

Figs 7, 8 and 9 present the specifity of the steganalyses techniques studied with the embedding rates 0.05, 0.1, 0.2 for Outguess, F5 and Model Based respectively

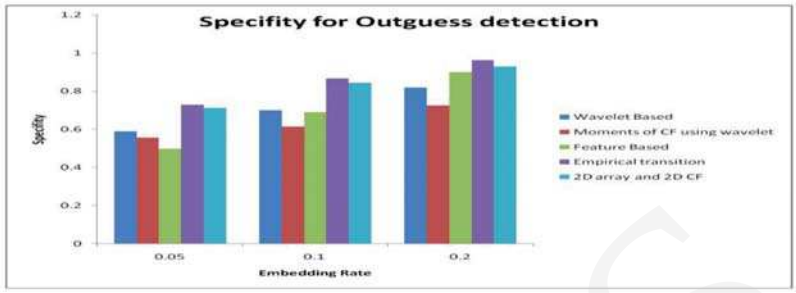

Fig. 7. Specifity for Outguess detection.

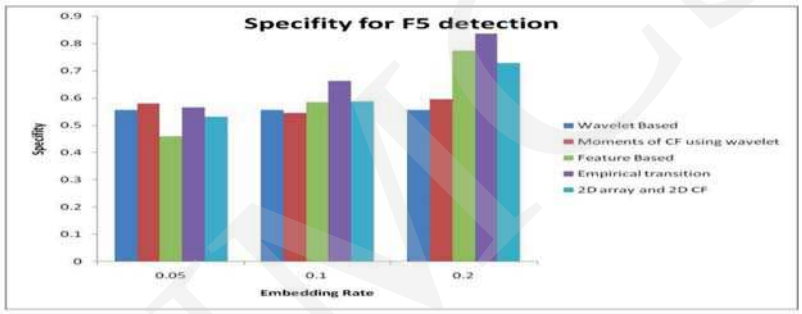

Fig. 8. Specifity for F5 detection.

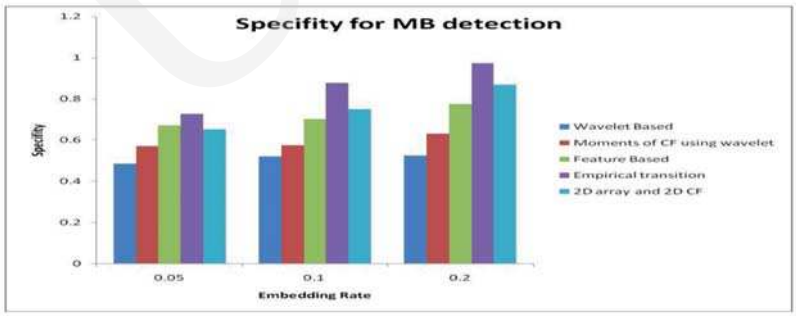

Fig. 9. Specifity for MB detection.

4 Conclusions

4.1 Sensitivity

The sensitivity measures the proportion of actual positives indication of the classifier trained by different steganalysis techniques for different embedding rates and different embedding techniques.

For the outguess embedding technique. The great difference in sensitivity is found between the "Wavelet Based Steganalysis" and the "Moments of CF using Wavelet" as a part, and the "Feature based steganalysis", "Empirical Transition Matrix" and "2D array and 2D CF" as the other part

- At the low embedding Rate "0.05 the "Feature based steganalysis" has higher sensitivity than the two others in the same group.
- At the embedding rate of "0.1", "The Empirical Transition Matrix" and "2D array and 2D CF" are more sensitive, and this continues to the embedding rate "0.2"

For the F5 embedding technique, the difference in sensitivity between the "Wavelet Based Steganalysis" and the "Moments of CF using Wavelet" as a part, and the "Feature based steganalysis", "Empirical Transition Matrix" and "2D array and 2D CF" as the other part in the embedding rate "0.1" and above is found.

- At the low embedding Rate "0.05 the "Feature based steganalysis" has higher sensitivity than the two others in the same group.
- At the embedding rate of "0.1", "The Empirical Transition Matrix" sensitivity continues to increase with the increasing rate and is higher than that of others. "The feature based has a very small increase, and the "2D array and 2D CF" increase with the increasing rates but do not reach the "Feature based".

For the Model Based steganographic embedding technique, great difference in sensitivity between the "Empirical Transition Matrix" and the other steganalysis methods is found.

- As the embedding rate increases, the sensitivity of all steganalysis methods increases except the "Wavelet based", it decreases till the embedding rate "0.1" is reached and then increases.
- The increasing sensitivity rate of the "2D array and 2D CF" is higher than the other,one but still does not reach the sensitivity of the "Empirical Transition Matrix".

4.2 Accuracy

It measures the true indication of the classifier related to the entire tested sample. When using the Outguess as a hiding technique, the great difference in accuracy between the "Wavelet Based Steganalysis", "Moments of CF using Wavelet" and the "Feature based steganalysis" as a part, and the, "Empirical Transition Matrix" and "2D array and 2D CF" as the other part is found.

- At the low embedding Rate "0.05 the "Empirical Transition Matrix" has higher accuracy than the "2D array and 2D CF".
- With the increase in the embedding rate, all the steganalysis accuracy rates increase.
- The "Empirical Transition Matrix" and the "2D array and 2D CF" appear to increase with the same rate.

- The "Feature based" accuracy increases with very high rates. And at the "0.02" embedding rate it almost reaches the "Empirical Transition Matrix" and "2D array and 2D CF".

When using the F5 as a hiding technique, it appears that the accuracy of all steganalysis techniques is very similar differing in about 2%. The embedding rate is "0.05".

- With the increase of the embedding rates, the accuracy of the steganalysis assumes different behaviour:
  - "Wavelet based" provides a little increase, and "Moments of CF using wavelet" almost remain constant.
  - The "Feature based" and "2D array and 2D CF" increase with the same rate till the embedding rate reaches"0.1", then the "Feature based" gains higher increase in accuracy than the "2D array and 2D CF". Thistakes place at the embedding rate "0.2".
  - The "Empirical transition matrix", gets a high rate increase in the accuracy compared to that of the embedding rate.

When using the MB as a hiding technique, the "Empirical Transition Matrix" has the highest accuracy in all the other techniques.

- The "2D array and 2D CF" and "Feature Based" have almost the same accuracy at the embedding rate "0.05", but the increase rate of the "2D array and 2D CF", is greater than that ofthe "Feature Based" .
- The "Moment of CF using wavelet" has a low increasing rate at the embedding rate from "0.05" to "0.1", which is by "0.1" to "0.2".

4.3 Specifity

It measures the proportion of negatives which are correctly identified by the classifier.

Using the Outguess as a hiding technique, The "Empirical Transition Matrix" and the "2D array and 2D CF", are the highest in specifity and almost get the same increase rate.

The "Feature Based" is the worst in specifity for the low embedding rate, but increases significantly in Specifity with the increase of the embedding rate.

Using the F5 as a hiding technique.

- All the steganalysis techniques except the"Feature Based" have almost the same Specifity at the low embedding rate "0.05".
- The "Moments of CF using wavelet" Specifity decreases with the increase of the embedding rate up to "0.1", then increases with the increasing embedding rate.
- The "Wavelet based" remains constant.
- The "Empirical Transaction Matrix" and "2D array and 2D CF" Specifity increases gradually with the increase of the embedding rate.

- The "Feature Based" has low Specifity at a low embedding rate, but it increases signifiacantly with the increase of the embedding rate. It reaches the "2D array and 2D CF" specifity at the embedding rate of "0.1".

Using the MB as a hiding technique.

- The "Empirical Transition Matrix" has the highest specifity for the three embedding rates.
- The "2D array and 2D CF" specifity is less than that of the "Feature Based" at the embedding rate of "0.05", but it increases more than the "Feature Based" with the increase of the embedding rate.
- The "Moments of CF using wavelet" and "wavelet based" are very low regarding the other steganalysis techniques.

From the above observations, the "Empirical Transition Matrix in the DCT domain based Steganalysis" gives the best values compared with the other four methods. This result matches thos e of the experiments applied by Fu et al. [**19**] while a different image data set is used.

The "Empirical Transition Matrix in DCT domain based Steganalysis" is better than the others, not only because it uses high order statistics, but because of the feature extraction which is the dependency among the quantized block DCT Coefficient. It uses the Markov empirical transition matrices to capture the intra block and inter block dependencies between the block DCT coefficients.

The "Feature Based Steganalysis" comes second for F5 because the co-occurrence matrix is used to capture the dependency between the DCT coefficient pairs from the neighbouring block. This method is successful to some extent because it takes into consideration only the inter-block. The intra-block is not considered.

The "Statistical Moments Based Universal Steganalysis Using JPEG 2-D Array and 2-D characteristic function" comes second for the Outguess and MB, because it uses discrete the Wavelet Transform (DWT) subbands and the characteristic function of each of these subbands. It also, employs the Second order histogram. This success with Outguess and MB, depends on many factors calculated by this method, also due to the methodology of Outguess and MB which attempts to make less change in the image histogram. But it does not give a good result with the F5, because it tries to keep the histogram unchanged by decreasing or increasing the coefficient value by one.

References

[1] Kharrazi M., Sencar H. T., Memon N. , Benchmarking steganographic and Steganalysis techniques, Security, steganography, and watermarking of multimedia contents VII, San Jose CA (2005).

[2] Morkel T., Eloff J.H.P., Olivier M.S., An Overview of Image Steganography, Proceedings of the Fifth Annual Information Security South Africa Conference, Sandton, South Africa (2005).

[3] Anderson R. J., Petitcolas F. A. P., On The Limits of Steganography, IEEE Journal of Selected Areas in Communications, Special Issue on Copyright & Privacy Protection 474-48116 (1998).

[4] Silman J., Steganography and Steganalysis: An Overview, as part of the Information Security Reading Room, Copyright © SANS Institute (2001).
[5] Lee Y.K., Chen L.H., High capacity image steganographic model, Vision, Image and Signal Processing, IEE Proceedings 147 (2000): 288.
[6] Johnson N. F., Jajodia S., Steganalysis of Images Created Using Current Steganography Software, Lecture Notes in Computer Science 1525 (1998): 273.
[7] Wang H., Wang S., Cyber Warfare: Steganography vs. Steganalysis, Communications of the ACM 47 (10) (2004): 76.
[8] Johnson N. F., Jajodia S., Exploring Steganography: Seeing the Unseen, IEEE Computer Journal 31 (2) (1998): 24.
[9] Provos N., Defending Against Statistical Steganalysis, a research supported by DARPA grant number F30602- 99- 1- 0527.
[10] Westfeld A., F5 a Steganographic Algorithm: High Capacity despite better Steganalysis, 4th International Workshop on Information Hiding. (2001).
[11] Sallee P., Model – based Steganography, International Workshop on Digital Watermarking, Seoul, Korea (2003).
[12] Chandramouli R., Subbalakshmi K. P., Current Trends in Steganalysis: A Survey, Department of ECE Stevens Institute of Technology.
[13] Farid H., Detecting Hidden Messages Using Higher – Order Statistical Models.
[14] Adelson E. H., Simoncelli E. P., Subband image coding with three-tap pyramids, In Picture Coding Symposium, publisher MIT Media Laboratory (1990).
[15] Vaidyanathan P., Quadrature mirror filter banks, M-band extensions and perfect-reconstruction techniques, ASSP Magazine IEEE 4 (3) (1987): 4.
[16] Vetterli M., A theory of multi rate filter banks, Acoustics, Speech and Signal Processing, IEEE Transactions 35 (3) (1987): 356.
[17] Fridrich J., Feature-Based Steganalysis for JPEG Images and its Implications for Future Design of Steganographic Schemes.
[18] Shi Y.Q., Xuan G., Zou D., Gao J., Ch. Yang Ch., Zhang Z., Chai P., Chen W., Chen C., Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network, IEEE International Conference 6 (8) (2005).
[19] Fu D., Shi Y. Q., Zou D., Xuan G., JPEG Steganalysis Using Empirical Transition Matrix in Block DCT Domain, Multimedia Signal Processing, 2006 IEEE 8th Workshop (2006).
[20] Chen C., Shi Y. Q., Chen W., Xuan G., Statistical Moments Based Universal Steganalysis Using JPEG 2-D array and 2-D Characteristic Function (2005).
[21] Support vector machine; http://en.wikipedia.org/wiki/Support_vector_machine; last visited 12/2007.
[22] Hsu C. W., Chang C. C., Lin C. J., A practical guide to support vector classification, Technical report, Department of Computer Science, National Taiwan University (2003).
[23] LIBSVM – A Library for Support Vector Machines; http://www.csie.ntu.edu.tw/∼cjlin/libsvm/, last visited 2/2008.