An Experimental Analysis of Feature Based Blind Steganalysis Techniques

Swagota Bera, Monisha Sharma, Bikesh Singh

Abstract: Steganalysis is the finding of the hidden information in an image. Steganalysis is named as blind steganalysis if hidden data is searched without any restriction to any specific algorithm. Many research works has been done in this area for more than one decade. The detection algorithms are software tools mostly developed using MATLAB and C-language codes. Among the various approaches, feature extraction and classification based blind steganalysis is proved to be significant. This paper presents few well-known approaches among them.

Keywords: DCT, DWT, Steganography, Steganalysis, JPEG

List of Abbreviations:

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOSS</td>
<td>Break Our Steganographic Scheme</td>
</tr>
<tr>
<td>bpac</td>
<td>Bit Per Non-Zero A.C Coefficient</td>
</tr>
<tr>
<td>bpnz</td>
<td>Bit Per Non-Zero Coefficient</td>
</tr>
<tr>
<td>CC-JRM</td>
<td>Cartesian Calibrated JPEG Rich Model</td>
</tr>
<tr>
<td>CCPEV</td>
<td>Cartesian Calibrated Features Extracted by Penvy</td>
</tr>
<tr>
<td>DCT</td>
<td>Discrete Cosine Transformation</td>
</tr>
<tr>
<td>DCTR</td>
<td>Discrete Cosine Transformation Residual</td>
</tr>
<tr>
<td>DWT</td>
<td>Discrete Wavelet Transformation</td>
</tr>
<tr>
<td>FLD</td>
<td>Fisher Linear Discriminate</td>
</tr>
<tr>
<td>GFB</td>
<td>Gabor Filter Based</td>
</tr>
<tr>
<td>GFR</td>
<td>Gabor Filter Rich</td>
</tr>
<tr>
<td>GRF</td>
<td>Gabor Rich Filter</td>
</tr>
<tr>
<td>GLCM</td>
<td>Grey Level Co-occurrence Matrix</td>
</tr>
<tr>
<td>JPEG</td>
<td>Joint Photographic Expert Group</td>
</tr>
</tbody>
</table>

I. INTRODUCTION

1. BACKGROUND AND MOTIVATION

Electronic communication applications provide quick and easy correspondence between the worldwide which is making our life very smoother but must not be at the cost of security. So inculcation of security technique to preserve privacy and authentication is mandatory. Cryptography, steganography and watermarking are the well-known information security techniques. Cryptography maintains the secrecy by changing the data in other form but couldn’t hide the presence of hidden information, but steganography is the concealing of data inside a cover medium in such a way that the existence of any communication itself is undetectable. Watermarking is also somewhat information hiding purposefully for providing authentication. In the designing of information hiding techniques there exist trade-off between payload, robustness and undetectability parameters. Among the three of them, steganography designing is more concerned to maintain undetectability whereas watermarking is more concerned about robustness. Steganography is also known as data hiding or data embedding. The confidentiality, integrity and availability are the three major paradigms for the analysis of the security of the technique. Cryptography provides confidentiality and integrity, but steganography provides all the three (Stalling, 2005).
Since historical time, this has been in practice to communicate the secret information as evidence by the practice of using invisible ink and tattoo under the hair. Digital steganography introduced a revolution in the secret data transmission in which the secret data is hidden in various multimedia sources such as image, video and audio. Suppose any image is known as cover or clean image if it does not contain any hidden data embedded in it and otherwise the image it is known as stego image. Steganography can be used in a large amount of data formats in the digital world of today. The most popular data formats used are .bmp, .doc, .gif, .jpeg, .mp3, .txt and .wav. These formats are popular in Internet because its tools can be applied on the standard format & relative ease by which redundant or noisy data can be removed from them and replaced with a hidden message (Bera et al., 2012).

In the figure (1.1), the model of the Steganographic system is represented in which hiding algorithm is used to embed the secret data in such a way that there is no visual differences between the cover image and the stego image. An authorized person at the receiver can decode the secret data by implementing the decoding algorithm to the stego image with help of key.

The steganalytic is the person who tries to detect and recover the hidden information either text or image from the cover image by applying detection coding to the stego image.

**Figure: 1.1 Model of Steganographic system**

Application of steganography will be a legal or illegal. It is also having wide applications in smart id generation, forgery detection in forensic department. The Japanese firm Fujitsu is working on this information security technique for encoding and decoding data in mobile phone. It is also having wide applications in smart id generation, forgery detection in forensic department. The Japanese firm Fujitsu is working on this information security technique for encoding and decoding data in mobile phone (Cheddad et al., 2010).This technique is illegally using by the terrorist to communicate the information among their community people as per the various happenings as stated below.

**WASHINGTON---Hidden in the X-rated pictures on several phonographic web sites and the posted comments on sports chat rooms may lie the encrypted blueprints of the next terrorist attack against the United States or its allies. It sounds farfetched, but U.S officials and experts say it’s the latest method of communication being used by Osama bin Laden, indicated in the bombing in 1998 of two U.S embassies in East Africa and others are hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other web sites, U.S and foreign officials say.

Above is reported in USA TODAY AP by Jack Kelley brought the world’s attention to the use ofsteganography. Greater still was the impact to come from the devastation on the 11 September 2001 of the World Trade Centre. The result of this destructive act also consistently motivating usto explore in the secret data detection (Kelly, 2001).

When a suspected al-Qaed member was arrested in Berlin in May of 2011, he was found with a Memory card with a password-protected folder and the files with-in it were hidden. But, as the German newspaper Die Zeit reports, computer forensics experts from the GermanFederal Criminal Police (BKA) claim to have eventually uncovered its contents—what appeared to be a pornographic video called "KickAss.”

Within that video, they discovered 141 separate text files, containing what officials claim are documents detailing al-Qaed operations and plans for future operations—among them, three entitled "Future Works," "Lessons Learned," and "Report on Operations"(Gallagher, 2012).

ISIS, Al-Qaeda use steganography to pass on secret messages
- Encrypting coded messages in porn pictures the safest way for terrorists to communicate
- Messages have been encrypted on eBay and Reddit also
- A nightmare for investigators to track the use of steganography.

When investigators from the United States of
America dug deep into the Al-Qaeda’s network it was found that they had extensively used steganography to pass on messages. Groups such as the Hizbollah, Hamas and Al-Qaeda had used steganography to pass on messages between each other. Once the messages were encrypted, the Al-Qaeda members downloaded the files using various software to execute several terrorist plots.

Detection is difficult: For an investigating officer detecting steganography is a nightmare. There is absolutely no record to show that the sender and the receiver had ever communicated. They do not exchange calls or emails. What investigating agencies have been doing is keeping a track of all downloaded pictures on the web. Pictures that are downloaded in places where the terrorist networks are strong are part of the data base. They would then keep a watch on these pictures closely to see if there are messages coded into them (Nanjappa, 2015).

The figure (1.2) below represents the world wide increasing terrorist activities as per the data base provided by global terrorism database (GTD) provided by university of Maryland (Roser et al., 2018).

![Worldwide Fatalities Report from Terrorism](image)

**Figure: 1.2 Worldwide Fatalities Report from Terrorism**

Internet has become a means for the increasing terrorist activities through which they communicate to each other’s. They use it to share information, coordinate attacks, spread propaganda, raise funds etc. This technique will be helpful for prior information of any terrorist act which is going to be happen and hence can save social and economic tragedies. In modern times, terrorism is considered a major threat to society. So development of any application for detecting any hidden data is in favour of mankind. The reverse technique of steganography is the detection of the hidden information in an image is termed as image steganalysis.

Inthewebsite http://dde.binghamton.edu/download.edu/download/syndrome/ of Binghamton University, digital data embedding laboratory provides a convenient platform for the researches from where the present state of art steganography and steganalysis and classifier coding are available. The steganography analysis and research center (SARC) having website www.sarc-wv.com is a center of excellence within backbone security. It is a DSD Laboratories affiliate company in U.S.A, focused exclusively on steganography research and the development of advanced steganalysis is helpful for digital investigation specialists and information technology security personnel in law enforcement government, military, intelligence etc. also provides certificate training on steganography and steganalysis. Also there are many real time detection tools and hands on training on are provided to the forensic investigators and learners by different organizations such as http://www.ilook-forensics.org/training.html and https://www.deepdotweb.com/2017/01/02/steganalysis-finding-hidden-data-images/.

### 1.2 JPEG Compression and JPEG Steganography

Joint photographic expert group (JPEG) is the most well-known image compression technique and widely used for storing and sharing of digital images, over the digital media. After compression the image is stored in .jpg format. JPEG compression technique was introduced in which the image is first divided into blocks of 8 x 8 pixels then discrete cosine transformation (DCT) is applied and frequency components of the image are obtained known as transform image. Then quantization step is introduced which further compress the data as the absolute values increases and then entropy coding (lossless compression) is done for further compressing the image data (Wallace, 1991).

An improved JPEG compression technique was introduced which is popularly known as JPEG 2000 in which wavelet transformation (WT) is implemented to obtain the frequency components of the image instead of DCT and initial division of the image into 8x8 blocks is omitted. The compression ratio is almost increased by 20 % by the introduction of WT (Skodras et al., 2001).

Figure (1.3) presents the JPEG compression methodology through block diagram. Wavelet transform is the multi-resolution analysis represents image in different resolution levels. After transformation the coefficient obtained are also known as transformed coefficients.

![Block Diagram of JPEG Compression](image)

**Figure: 1.3 Block Diagram of JPEG Compression**

**Input Image** → **Image Transform** → **Quantization** → **Entropy Coding** → **Compressed Image**
The thresholding in the compression means to set the value of transformed coefficient to zero whose values are less than threshold value decided. Higher the threshold value, the more is the number of zero and compression is more. For the lower threshold value, the visual image quality is better for both DCT and DWT but for higher threshold value, the compression performance is better in case of DWT than DCT. Steganography techniques are categorized on the basis of the type of cover media as shown in figure (1.4). Any type of digital cover file formats is suitable but the preferable is the presence of high degree of redundant bits.

**Figure: 1.4 Classifications of Steganography Techniques**

The spatial domain steganography provides the higher capacity of hiding the data more easily detectable by simple statistical attack as compared to frequency domain hiding technique (Saha et al., 2012). Broadly, image steganography techniques can be classified in two categories. They are spatial domain steganography and transform domain steganography. In spatial domain steganography, the secret data is embedded by replacing the least significant bits in the pixel values of the image such that the pixel values get changed by a small amount which causes no visual changes. The frequency components of an image can be obtained by applying mathematical transformation functions such as DCT, WT. The frequency components are categorized as dc, low frequency a.c components and high frequency a.c components. In transform domain steganography, the secret data is embedded by modifying the frequency components to avoid any visual changes in the image. The non-zero-coefficients are less in medium and high frequency. Medium frequency is more or less statistically unimportant, so can be used for hiding the secret bits. JPEG steganography is transform domain steganography in which secret data is embedded after the quantization step in the JPEG compression steps and then entropy coding is done. The embedded data can be extracted after entropy decoding in the receiver side. Though visual changes may not occur but there comes changes in the statistical parameters. The presence of hidden data can be detected by measuring the variations in the other statistical parameters. There is always a challenge for the developer of steganography is undetectability by an unauthorized person which can be achieve by introducing embedding technique which will cause very low variations in the statistical parameters of an image. If there is no change in any statistical parameters before and after hiding then it is to be said as statistical restoration in steganography (Kipper, 2004).

The possibility of the attacking will decreases if there are increases in the statistical restoration of the image during hiding. It is always observed that there is always a tradeoff between the embedding secret data capacity and its statistical restoration capability. The performance of a steganographic technique is evaluated with the parameters such as PSNR, MSE, embedding data capacity and the capability to prevent from the steganalytic attacks (Kumar, 2012).

Various JPEG steganographic techniques are Jsteg (Upham, 1998), F5 (Westfeld, 2001), Outguess (Provos, 2001), WT Based (Dewangan et al., 2013), nsf5 (Fridrich et al., 2007). JPEG UNIversalWAvelet Relative Distortion (JUNIWARD) (Holub et al., 2014) is the recent powerful hiding technique is the adaptive steganography which is based on the syndrome trellis code (STC) as the secret bits are embedded in the complex content of the image which is very hard to model.

### 1.3 Image Steganalysis

Image steganalysis is the science for the detection of hidden data in image. In images, there are strong statistical correlations which get distorted when any secret data is embedded in it. This distortion calculation becomes the key point for the designing of steganalysis technique. Various image processing tools i.e. filtering, rotation, flipping of the images pixel bits, lossy compression, cropping can affect the embedded data. The LSB’s of the pixels can be modify which will permanently destroy the secret content which happens in passive steganalysis but active steganalysis aims to retrieve the hidden data. For the data retrieval, information about the hiding technique is required which has been used. So, a smart detector of high detection accuracy is needed. Image steganalysis can be classified as shown in the figure (1.5). Steganalysis technique is also named as data detection technique. If the detection technique is applied on the coefficients of the image pixel obtain from mathematical transformations such as DCT, DWT are known as transform domain technique. If the detection technique algorithm target for detecting any particular hiding technique then the technique is targeted steganalysis which is very effective in detection and data retrieval.

**Figure: 1.5 Broad Classification of Image Steganalysis**

If the detection technique is universal that means it can detect any type of hiding algorithm then it is under the category of universal or blind steganalysis. Blind steganalysis requires no priori information of the targeted steganography which is based on learning based strategy. In semi blind...
steganalysis, only specific hiding techniques are targeted. The detection technique provides the information about the hiding algorithm if the detection model has been trained with that particular hiding technique. The blind steganalysis is very powerful and versatile technique in which pattern recognition classifiers are being used. The smoothness, regularity, continuity, consistency and periodicity among the pixels in an image get deviates which can be characterized by various statistical formulae. The statistical correlations among the image coefficients are the pattern of image which gets deviates due to the hiding. These statistics includes global histogram, individual histogram, inter and intra block dependencies etc. are the first and second order statistics of the image are known as image features. The statistical parameters are classified as first order, second order and higher order statistics. The first order statistics such as local histogram, global histogram, dual histogram, mean, variance, skewness, kurtosis and, statistical moment measure the gray level distribution within the image whereas the higher order statistics such as co-occurrence, DCT features, Zipf’s law and Markov’s transition probability matrix (TPM) measure the variations in the gray level values in the specific order within an image.

The classifiers are trained first with image patterns of the clean image and of the stego images obtained from different steganography techniques and then the same classifier is implement to test an arbitrary image to decide whether there is any hidden data or not. Blind steganalysis is a feature based detection methodology (Kumar, 2012). The present work is blind steganalysis in transform domain for detecting popular JPEG steganography techniques. Initially, the databases of stego images and cover images are developed by implementing various steganography techniques. The image database is divided into training set and testing set. Then image features are extracted from the images of specific dimensions depending on the feature extraction technique owned. These image features of training set are used to train the classifier to identify the clean image and infected image. Then the performance of the detection technique is evaluated by measuring prediction parameters such as accuracy, precision, specificity, area under receiver operating curve (ROC) etc. when tested on the image features of testing set (Eman et al., 2012).

Classification of the blind steganalysis techniques depends on the type of feature extraction and the data mining techniques. Various researches in blind steganalysis techniques reports using wavelet features, DCT features, Markov’s feature, moment based features, co-occurrence based features, decompressed JPEG Image based features and merged features.

2.1 Blind Steganalysis Techniques Reports Using Wavelet Features
(Farid, H. 2002) first time proposed feature extraction using first order statistics i.e. mean, variance, skewness and kurtosis. The image is decomposed using quadrature mirror filter (QMF) into vertical, horizontal, diagonal and lowpass components of three First order statistics are calculated from all the high frequency subbands and also from the prediction log error. Feature dimension is of 72 on 1800 JPEG images. The classification is done using FLD. JPEG hiding techniques i.e. Jsteg, Outguess, Ezstego and LSB substitution are detected and classified. It detects Jsteg having detection percentage 95.7 % of message of size 128 x 128 and 63.4 % of detection ratio for outguess of size 128 x 128.

(Lyu, S., 2003) proposed feature extraction using first order statistics i.e. mean, variance, skewness and kurtosis. The image is decomposed using QMF into vertical, horizontal, diagonal and lowpass components of three first order statistics are calculated from all the high frequency subbands and also from the prediction log error. Feature dimension is of 72 on 1800 JPEG images. The classification is done using FLD. JPEG hiding techniques i.e. Jsteg, Outguess, Ezstego and LSB substitution are detected and classified. It outperforms (Farid, H., 2002) in all the cases such as detection accuracy is increased by 3.4 % in case of Jsteg and by 0.2 % in case of Zipf’s law (Laimeche et al., 2017).
outguess having 128 x 128 size hidden data. (Lyu, S., 2006) proposed feature extraction using magnitude statistics from wavelet decomposed using QMF into vertical, horizontal, diagonal and lowpass components and phase statistics from harmonic decomposed image named as local angular harmonic decomposition (LAHD). Feature dimension is of 432 on 40000 JPEG images. The classification is done using linear SVM, non-linear SVM and one-class SVM. It outperforms (Fridrich, J., 2005) by increasing detection rate by 32.8 % in case of 0.5 bpnc F5 and 8% in case of 01 bpnc F5. (Zhan, S. H., 2007) proposed feature extraction using higher order statistics from four level wavelet decomposing using QMF into vertical, horizontal, diagonal and lowpass components and also from the prediction log error. Feature dimension is of 72 on 1000 JPEG images. The classification is done using linear SVM. Feature selection ANOVA is used which provides better in the detection accuracy. JPEG hiding techniques F5 is detected and classified. The higher value of F-scores are obtained using ANOVA.

(Savoldi, A., 2007) proposed feature extraction using higher order statistics from wavelet decomposed using QMF into vertical, horizontal, diagonal and lowpass components and also from the prediction log error. Feature dimension is of 360 on 60000 JPEG images. The classification is done using linear SVM. JPEG hiding techniques i.e. Jsteg, Outguess and F5 are detected and classified. In case of F5 and Outguess, the detection accuracy is above 90% for 1% and 12% hidden data.

(Wang, Y., 2007) proposed feature extraction using probability density functions (PDFs) and empirical moments of characteristic functions of the PDFs from the three level wavelet decomposed image using Haar filter on 600 JPEG images. The classification is done using FLD. Feature selection is done on the basis of Bhattacharyya distance. All the moments whose Bhattacharyya distance is positive are considered for steganalysis. Feature selection algorithm called sequential forward floating selection (SFFS) is used and better performance is obtained. Hiding techniques i.e. F5 and LSB substitution are detected and classified. It outperforms (Farid, H., 2002) and (Xuan, G., Shi, Y.Q., 2005). The false detection alarm is 0.6 by proposed as compared to 0.09 in case of (Xuan, G., Shi, Y.Q., 2005) and 0.08 in case of (Farid, H., 2002).

(Stith, C. B., 2007) proposed feature extraction using noise variance by calculating median absolute deviation of the wavelet coefficient on 912 JPEG images. For testing the significance of each feature, an analysis of variance (ANOVA) was performed. ANOVA is a fundamental tool in statistics to determine if measurements taken from different groups are statistically different. The classification is done using SVM. JPEG Hiding techniques i.e. F5, MB and Jsteg are detected and classified.

(Huang, J., 2008) proposed feature extraction using mean square error from the three level decomposed wavelet subbands of dimension 9 on 500 JPEG images. The classification is done using SVM. JPEG Hiding techniques i.e. F5, JP hide and seek (JPHS) are detected and classified. F5 is more detectable than JPHS. It provides 90% detection accuracy which concludes that this technique is competitive for steganalysis purpose.

(Luo, X., 2008) proposed feature extraction using multi-order absolute characteristic function moments of histogram from the three level decomposed wavelet subbands of dimension known as wavelet packet transform (WPT) of dimension 255 on 1014 images. The classification is done using back propagation neural network (BPNN). Hiding techniques SS is detected and classified. JPEG hiding techniques i.e. F5 and Jsteg are detected and classified. It outperforms (Farid, H., 2002) such as by increasing the detection accuracy by 18 % in case of F5 having payload of 64x64.

(Dong, J., 2008) proposed feature extraction using moments of CF of the three types of image run length histogram (RLH) from the three level decomposed wavelet subbands of dimension 36 on 1142 JPEG images. The classification is done using SVM. Hiding techniques SS and LSB embedding are detected and classified. It outperforms (H. Farid,2002) and (Chen, X., 2006) such as detection accuracy is increased by value 6.2 % from (H. Farid,2002) in case of 5% FPR.

(Leng, C.K. and Pieprzyk, J., 2008) proposed feature extraction using first three moments of CF of from the three level decomposed wavelet subbands obtained by using Haar filter from the stego image and also from estimated cover image of dimension 72 on 2037 images. It is the improved version of the blind steganalysis proposed by (Xuan, G., Shi, Y.Q., Gao, J., 2005). The estimated cover image is obtained by decompressing the stego image, transforming the decompressed image and recompressing back. The classification is done using SVM. Hiding techniques F5, outguess and MB1 are detected and classified. It outperforms (Xuan, G., Shi, Y.Q., Gao, J., 2005) by increasing the AUC.

(Yang, X., Lei, Y., 2009) proposed feature extraction using statistical analysis for the test image and their wavelet packet sub-bands obtained after wavelet packet decomposition (WPD) of dimension 213 on 1000 images. The first three orders statistical moment and first step Markov’s empirical transition matrix are used as statistical features. The intra-scale and inter-scale dependencies of the wavelet coefficients are captured using Markov’s empirical transition matrix is used. The classification is done using FLD. Hiding techniques F5, outguess and Jsteg are detected and classified. It outperforms (Lyu, S. and Farid, H., 2003).

(Sun, Z., Li, H., 2009) proposed feature extraction using three order statistical moment from CF from the three level decomposed wavelet coefficients of 102 dimension on 596 images. In this work, the diagonal elements are further decomposed and features. The classification is done using BPNN. Hiding techniques F5, outguess and Jsteg are detected and classified. It outperforms (Lyu, S. and Farid, H., 2003) in all cases except for the Jsteg.

(Kumar, G., 2010) proposed feature extraction using first order statistics i.e. mean,
varying, skewness and kurtosis from the three level decomposed wavelet subbands of dimension 108 on 6500 JPEG images. The classification is done using SVM. Hiding techniques SS is detected and classified.

(Arivazhagan, S., 2010) proposed feature extraction using mean, standard deviation co-occurrence matrix from first, second, third and fourth order DWT subbands of dimension 105 on 500 JPEG images. The detection accuracy is reached more than 65%.

(Hui, L., 2011) proposed feature using characteristic function which is probability mass function (PMF) extracted three level decomposed wavelet subbands of dimension 102 on 1300 JPEG images. The classification is done using SVM. PCA based feature selection technique is used for improving the performance which reduces the feature dimension from 102 to in the range of 40 to 50 with increased detection rate. JPEG hiding techniques i.e. F5 and Jsteg are detected and classified. The detection accuracy is increased by 17.5% when PCA based feature selection method is adopted for 102-dimensional feature for low embedding capacity F5 hiding technique.

2.1.2 Blind Steganalysis Techniques Reports Using DCT Features

(Fridrich, J., 2005) first time proposed feature extraction using DCT features (first and second order statistics) from input image and calibrated image of dimension 23 on 1814 Greenspun JPEG images and classification is done using FLD. DCT features are the L1 norm i.e. the absolute values of all vectors and matrix elements. Global histogram and dual histogram is the first order statistics whereas variance, blockiness and co-occurrence are the second order statistics. Among all dual histogram performance is better. Histogram and co-occurrence are the marginal statistics. The cropping and recompression of the stego image produce a calibrated image with the most macroscopic features similar to the original cover image. Detection becomes sensitive to wider range of steganography with the inculcation of calibration process. Calibrated image has macroscopic feature similar to the original cover image. The search of the data is in the non-zero coefficients. So, medium and higher frequency DCT coefficients are statistically unimportant. Therefore, the statistical properties of the DCT coefficients of the calibrated image are approximately same as its cover image. For steganalysis of JPEG images, features derived directly in the embedding domain from DCT Coefficients. JPEG hiding techniques i.e. F5, MB, Outguess are detected and classified. It outperforms (Lyu, S., 2003) in all the cases and MB is more detectable. The detection rate for outguess is increased by 2.6% for 0.05 bpnz and 4.4% for 0.2 bpnz.

(Wahab, A.W., 2009) proposed feature extraction using conditional probability matrix in the three directions i.e. vertical, horizontal and diagonal from each block of the image DCT coefficients of dimension 54 on 5235 images. The classification is done using SVM. JPEG hiding techniques F5 is detected and classified. It outperforms (Shi, Y.Q., Chen, C., 2006) by increasing detection accuracy by 2.6% for 618 bytes of hidden data in 640x480 image size.

(Quan, X., 2009) proposed feature extraction using based on the manifold-learning method in which non-linearity dimensionality reduction method i.e., Isometric Feature Mapping (ISOMAP) is used for feature reduction on 8000 images. The classification is done using FLD. JPEG hiding techniques MB, outguess and Jsteg are detected and classified. It provides better detection accuracy such as 99.2% and 96.5% in case of Jsteg for 80% and 20% embedded data respectively.

(Lin, J. Q., and Zhong, S. P., 2009) proposed feature extraction using by capturing the seventh and eighth bit planes of the non-zero DCT coefficients from JPEG images and based on binary similarity measure proposed by (Avcibas, I., 2003) of dimension 14 on 1000 images. The classification is done using SVM. JPEG hiding techniques MB, outguess and F5 are detected and classified. It outperforms (Avcibas, I., 2003) by increasing detection accuracy. One of the cases is increasing detection accuracy by 46.2% for F5 having 25% payload in it. But the proposed technique does not outperform (Fridrich, J., 2005).

(Bhat, V. H., 2010) proposed feature extraction using combination of huffman bit code length (HBCL) Statistics and File size to resolution ratio (FR) Index known as the huffman bit file index resolution (HUFFIRE) algorithm on 2000 images. The classification is done using SVM. JPEG hiding techniques F5, outguess, MB1 and MB2 are detected and classified. The model gives detection accuracy of 100% for MB for 1KB, 2KB and 5KB payloads.

(Bhat, V. H., Krishna, S. and Shenoy, P.D., 2010) proposed feature extraction using combination of huffman bit code length (HBCL) Statistics and File size to FR Index known as the HUFFIRE algorithm on 30000 images. The classification is done using steganalysis using random forests (SURF). Hiding techniques LSB and MB are detected and classified. The SURF algorithm of random forest proves to be having better performance than SVM.

2.1.3 Blind Steganalysis Techniques Reports Using Markov’s Feature

(Fu, D., 2006) proposed feature extraction using Markov’s transition probability matrix (second order statistics) from intrablock and interblock correlation from DCT coefficients of an image of dimension 324 on 7560 JPEG images. The classification is done using SVM. The features extracted from difference JPEG 2-D arrays along horizontal, vertical and diagonal directions. JPEG hiding techniques i.e. F5, MB, Outguess are detected and classified. It outperforms (Farid, H., 2002), (Fridrich, J., 2005) and (Shi, Y.Q., 2005) steganalysis algorithm in all cases such as detection accuracy is increased by 6% from (Fridrich, J., 2005) steganalysis algorithm and by 21% from (Shi, Y.Q., 2005) in case of outguess for 0.20 bpnz.

(Shi, Y.Q., 2007) proposed feature extraction using Markov’s transition probability matrix (second order statistics) from intrablock difference array of JPEG 2-D array of DCT coefficients of an image of dimension 324 on 7560 JPEG images. The classification is done using SVM. The features extracted...
An Experimental Analysis of Feature Based Blind Steganalysis Techniques

from difference JPEG 2-D arrays along horizontal, vertical and diagonal directions. The similar features are also extracted from calibrated images. So, final feature dimension is 648 which is reduced to 162 because the average value is taken. JPEG hiding techniques i.e. F5, MB, Outguess are detected and classified. It outperforms (Fridrich, J., 2005) and (Shi, Y.Q., 2005) steganalysis algorithm in all cases such as detection accuracy is increased by 6 % from (Fridrich, J., 2005) steganalysis algorithm and by 22.8 % from (Shi, Y.Q., 2005) in case of outguess for 0.20 bpnz. The success in the proposed technique is due to the introduction of following measures i.e. taking the absolute values forming JPEG 2-D arrays and thresholding in the calculation of TPM. The considered threshold value is 4.

(Xuan, G., Shi, Y.Q., Huang, C., 2006) proposed feature extraction using multidimensional Markov’s model of JPEG 2-D array of DCT coefficients of an image of dimension 360 on 1096 JPEG images. The classification is done using class-wise non principal component analysis (CNPCA) and SVM. The features extracted from difference JPEG 2-D arrays along zig-zag directions. JPEG hiding techniques i.e. F5, MB1 and MB2 are detected and classified. CNPCA achieved competitive classification results as SVM but CNPCA required less execution time. The detection accuracy is tested for the 5, 6, 7, 8 and 9 threshold values. It outperforms (Fridrich, J., 2005) and (Xuan, G., Shi, Y. Q., 2005) steganalysis algorithm for 1 KB, 2 KB and 4 KB hidden data for all the hiding techniques.

(Xuan, G., 2007) proposed feature extraction using multidimensional Markov’s model of JPEG 2-D array of DCT coefficients of an image of dimension 360 on 1096 JPEG images. The classification is done using CNPCA and SVM. The features extracted from difference JPEG 2-D arrays along zig-zag, horizontal, vertical and diagonal directions. JPEG hiding techniques i.e. F5, MB1 and MB2 are detected and classified. CNPCA achieved competitive classification results as SVM but CNPCA required less execution time. The detection accuracy is tested for the 5, 6, 7, 8 and 9 threshold values. It outperforms (Fridrich, J., 2005) and (Xuan, G., Shi, Y. Q., 2005) steganalysis algorithm for 1 KB, 2 KB and 4 KB hidden data for all the hiding techniques such as detection accuracy is increased by 3 % from (Fridrich, J., 2005) steganalysis algorithm and by 8 % from (Xuan, G., Shi, Y. Q., 2005) in case of F5 for 4 KB payload and provide 100 % detection result for 2 KB and 4 KB payload for outguess. Outguess is more detectable than F5.

(Chen, C. and Shi, Y.Q., 2008) proposed feature extraction using first step Markov’s TPM from intra-block and inter-block JPEG BDCT array from the horizontal, vertical, minor diagonal and major diagonal difference matrix of dimension 486 on 7560 JPEG images. Hiding techniques i.e. outguess, MB and F5 are detected and classified. The classification is done using SVM. It performs (Fridrich, J., 2005), (Shi, Y.Q., 2006) and (Penzy, T., 2007) in all cases.

(Wang, Y., Liu, J.F., 2009) proposed feature extraction using first step Markov’s TPM having threshold value of 7 from the calibrated image and predicted calibrated image of dimension 96-dimensional vector on 1000 images. The concept of microscopic and macroscopic calibration is used. Hiding techniques i.e. outguess and F5 are detected and classified. The classification is done using SVM. It performs (Fu, D., 2006), (Fridrich, J., 2005) and (Shi, Y.Q., 2006) in case of outguess but in case of F5 the proposed technique outperforms and (Fu, D., 2006) and (Shi, Y.Q., 2006) but have similar result as (Fridrich, J., 2005).

(Penzy,T., Bas,P., 2010) proposed feature extraction using Markov’s TPM from the difference pixel matrix calculated from all eight directions of the spatial domain image having threshold value of 8 and 5 which is named as first order subtractive pixel adjacency model (SPAM) features and named as second order SPAM features which is having threshold value of 3 of dimension 686 on 264000 JPEG images. Hiding techniques i.e. PQ, nsF5 and F5 are detected and classified. The classification is done using SVM.

(Huang, F., Li., B., 2008) proposed feature extraction using first step Markov’s TPM of threshold value 4. These statistical features are calculated from BDCT JPEG 2-D array in zig-zag, row and column scanning. Microscopic and macroscopic calibration method is introduced for calibration the local and global distribution of the quantized DCT. The dimension is 324 on 2881 images. Hiding techniques i.e. F5, MB1 and Outguess are detected and classified. The classification is done using SVM. It outperforms (D. Fu, 2006), (Shi, Y.Q., 2006) and (Penzy, T., 2007) in all the cases except for 0.5 bpnc MB in case of (Penzy, T., 2007), 0.1 bpnc MB in case of (Shi, Y.Q., 2006). It increases the detection accuracy by 1% for 0.05 bpnc F5 from the detection accuracy provided by (Penzy, T., 2007).

(Liu, Q., Sung, A. H., 2008) proposed feature extraction using first step expanded Markov’s TPM of threshold value 4 and also the polynomial fitting features on the histogram of the DCT coefficients. These statistical features are calculated from BDCT JPEG 2-D array from both intra-block and inter-block coefficients. The features are calculated from original image as well as from calibrated images. The dimension is 810 on 5000 images. Hiding techniques i.e. F5 and MB are detected and classified. The classification is done using SVM. It outperforms (Shi,Y.Q., 2007) with respect to detection accuracy.

(Kodovsky, J. and Fridrich, J. 2009) proposed modified calibration which improves the detection accuracy of (Penzy, T., 2007) of dimension 274 on 6500 images. JPEG hiding techniques i.e. nsF5, YASS and Jsteg are detected and classified. The classification is done using SVM. The paper concludes that calibration does not always provide an estimate of cover image features. It becomes a good tool for detection but somewhere it fails.

(Zhou, Z., 2009) proposed feature extraction using bidirectional Markov’s TPM from difference JPEG 2-D array on 800 images. The DCT image coefficients are divided in blocks and then each block are zig-zag scanned. The scanned coefficients are arranged in array with low frequency coefficient first.
and then high frequency coefficients which are generally zero. Then first 20 coefficients are considered. The intra-block and inter-block Markov’s TPM is calculated incorporating the thresholding technique. The classification is done using SVM. Hiding techniques i.e. F5, outguess and MB are detected and classified. (Chen, C. and Shi, Y.Q., 2008) fails to detect F5 for low embedding rate. This drawback is overcome with the proposed technique. It outperforms (Xuan, G., 2005) and (Chen, C. and Shi, Y.Q., 2008) by increasing detection accuracy in all cases except 0.1 outguess when compared to (Chen, C. and Shi, Y.Q., 2008). The detection accuracy is increased to 5% in case of 0.05bpcn F5 as compared to (Chen, C. and Shi, Y.Q., 2008). (Lin, J.Q., 2009) proposed feature extraction using one-step Markov’s TPM from JPEG 2-D array of BDCT along horizontal, vertical, minor diagonal and major diagonal considering threshold value 4 of dimension 324 on 1000 images. The feature selection and reduction is adopted using forward selection algorithm with F-score method which reduce the feature dimension from 324 to 26. JPEG hiding techniques i.e. F5, MB and Outguess are detected and classified. The classification is done using SVM. It’s detection rate is similar to (Shi,Y.Q., 2007) and (Pevny, T., 2007) but classification time requirement is low such as time requirement is 50 min less by proposed method as compared to (Shi,Y.Q., 2007).

(Yang, G. and Zhang, H., 2009) proposed feature extraction using improved Markov’s TPM from JPEG 2-D array of BDCT along horizontal, vertical, minor diagonal and major diagonal considering threshold value 4 of dimension 324 on 80000 images. To improve that conventional Markov Process based approach, several variants based scheme has been proposed both for intra-block and inter-block images. JPEG hiding techniques i.e. F5 and Jsteg are detected and classified. The classification is done using SVM. It outperforms Shi,Y.Q., 2007).

(Pevny,T., 2010) proposed feature extraction using one-step Markov’s TPM from JPEG 2-D array of BDCT along horizontal, vertical, minor diagonal and major diagonal considering threshold value 4 of dimension 686 on 30800 images. JPEG hiding techniques i.e. F5, MB1, MB2 and Outguess are detected and classified. The classification is done using SVM. It outperforms statistical moment based wavelet features by decreasing error by 0.010 %. (Pan, X., 2010) proposed feature extraction using one-step Markov’s TPM from JPEG 2-D array of BDCT obtained through three form of Hilbert scanning considering threshold value 4 of dimension 324 on 1338 images. Both intrablock and interblock features are extracted. The similar features are obtained from JPEG image coefficients as well as from its calibrated image. JPEG hiding techniques i.e. F5 and MB are detected and classified. The classification is done using FLD. It outperforms (Penvy, T., 2007) by increasing detection accuracy of our proposed method by at least 2.3% and up to 9% for the embedding rate of 10% and 20%. But for 50% and 80% embedding rate the detection accuracy improves by 1% to 4.3% in case of F5 but in case of MB, the performance is similar. (Kodovsky, J. and Fridrich, J., 2011) proposed feature extraction using Markov’s transition probability matrix (second order statistics) from intrablock and interblock correlation from DCT coefficients of an image of dimension 48600 on 6500 JPEG images. High dimensionality causes degradation in the analysis by the classifier. The problems comes are high complexity of training, degradation of generalization abilities, lack of robustness to cover source, and saturation of performance below its potential. The classification is done using SVM. JPEG hiding techniques nsF5 is detected and classified. It outperforms (Farid, H., 2002), (Fridrich, J., 2005) and (Shi,Y.Q., 2005) steganalysis algorithm in all cases such as detection accuracy is increased by 6 % from (Fridrich, J., 2005) steganalysis algorithm and by 21% from (Shi,Y.Q., 2005) in case of outguess for 0.20 bpnz. (Ng, W.W.Y., 2011) proposed feature extraction using one-step Markov’s TPM from original JPEG co-efficient, JPEG 2-D array of BDCT, second difference JPEG array along horizontal, vertical, minor diagonal and major also from calibrated images. diagonalconsidering threshold value 3 of dimension 147 on 2338 images. JPEG hiding techniques i.e. F5, MB1 and MB2 and Outguess are detected and classified. Localized generalization error model (L-GEM) approach for the selection of radial basis function neural network (RBFNN) is used for classification. It outperforms (Fridrich, J., 2005) such as detection accuracy is increased by 41.94% and (Shi,Y.Q., 2007) such as detection accuracy is increased by 27.09 % in case of 0.05 bpc outguess. (Gul, G., 2013) proposed feature extraction using multivariate p.d.f. estimates along with Markov Random Field (MRF) cliques which uses three step Markov’s TPM from original image, row, column and Zigzag scanning paths considering threshold value 10 of dimension 970 on 321,912 JPEG images. Symmetry downsampling feature selection and reduction technique is used to reduce 930 numbers of features to value 657. JPEG hiding techniques F5, Outguess, MB1 and MB2 are detected and classified. It outperforms DCT domain steganalysis i.e. (Fu, D., 2006), (Xuan, G., Shi, Y.Q., Huang, C., 2006), (Xuan, G., 2007), (Penvy, T., 2007).

(Jinyang, S., 2015) proposed feature extraction using two step intrablock and interblock Markov’s TPM from original image, calibrated image and the row, column, Zigzag and Hibernet scanning paths considering threshold value 3 of dimension 686 on 500 Greenspun and Corel draw library JPEG images. The classification is done using SVM. JPEG hiding techniques Outguess and MB are JUNIWARD are detected. It outperforms (Penvy, T., 2007) i.e CCPEV for all the cases but shows 0.1 % decrease in the detection accuracy for 0.1 bpnz payload Outguess. 2.1.4 Blind Steganalysis Techniques Reports Using Moment Based Features (Xuan, G., 2005) proposed feature extraction using statistical moment DFT of the three level decomposed wavelet subbands from...
frequency domain and from spatial domain of dimension 39 on 1096 JPEG images. In SS and LSB steganography, secret data embedded are additive and Gaussian but in F5, outguess and others this noise is non-AGN. For analyzing AGN, DCT and DWT are good but in case of non-AGN, DFT sequence is non-increasing. The upper band of n-moment which is a DFT function of characteristic function (CF) is non-increasing. So, moments of characteristic function will be a good detection tool. The classification is done using SVM. JPEG hiding techniques i.e. F5, JP hide and Jsteg are detected and classified. It outperforms (Farid, H., 2002) for all the cases such as detection accuracy is increased by 9% in case of Jsteg, by 8% in case of F5 and 3% in case of outguess with 4K of hidden data. 

(Shi, Y.Q., Xuan, G.,Zou, D.,Gao, J.,2005) proposed feature extraction using statistical moment of characteristic moment of two level decomposed wavelet subbands of dimension 18 on 1096 JPEG images. The classification is done using Bayesian classifier. Spread spectrum (SS) hiding techniques are detected and classified. It outperforms (Farid, H., 2002) by increasing detection accuracy by 21\%.

(Shi, Y.Q., Xuan, G.,Zou, D., Yang, C., 2005) proposed feature extraction using statistical moment (DFT) of characteristic function of the three level decomposed wavelet subbands of dimension 78 on 1096 JPEG images. The features are also calculated after the image prediction. This prediction-error image removes various information other than that caused by data hiding, thus making the steganalysis more efficient. The classification is done using Bayesian and neural network classifier. SS and LSB hiding are detected and classified. It outperforms (Farid, H., 2002) by increasing detection accuracy by 33\% in case of SS and 21\% in case of LSB.

(Chen, X., 2006) proposed feature extraction using statistical moment of characteristic function from decomposed wavelet subbands of dimension 108 on 700 JPEG images. The features are also calculated after the image prediction. This prediction-error image removes various information other than that caused by data hiding, thus making the steganalysis more efficient. The classification is done using SVM. It provides detection accuracy of 98\% and 99\% in case of SS, LSB hiding methods.

(Chen, C., 2006) proposed feature extraction using statistical moment DFT of characteristic function from the three level decomposed wavelet subbands, spatial domain and prediction error of dimension 390 on 7560 JPEG images. This prediction-error image removes various information other than that caused by data hiding, thus making the steganalysis more efficient. The classification is done using SVM. Outguess, F5 and MB hiding are detected and classified. It outperforms (Farid, H., 2002), (Shi, Y.Q., Xuan, G.,Zou, D., Yang, C., 2005) and (Fridrich, J., 2005) such as by increasing detection accuracy by 2.5\% in case of 0.2 bpcn outguess and 0.2 \% in case of 0.05 bpcn F5 except 0.1, 0.2 and 0.4 bpcn F5. F5 is more efficiently detected by (Fridrich, J., 2005).

(Mehrabi, M. A., 2007) proposed feature extraction using statistical moments from the three-level wavelet decomposed image using Haar filter of dimension 78 on 860 JPEG images. The performance is improved by using statistical moments i.e. DFT of the histogram in low and high frequency of wavelet subbands. The first three moments is calculated from each frequency band. The classification is done using SVM. Hiding techniques i.e. SS and LSB substitution are detected and classified. It outperforms (Farid, H., 2002) by increasing detection accuracy by 22.6 \% in case of LSB hiding techniques.

(Mehrabi, M. A., 2008) proposed feature extraction using statistical moments from the three-level wavelet decomposed image using Haar filter of dimension 39 on 1600 JPEG images. The performance is improved by using statistical moments i.e. DFT of the histogram in low and high frequency of wavelet subbands. The first three moments is calculated from each frequency band. The performance is improved than (Mehrabi, M. A., 2008) by using statistical moments are extracted from the images such that some of their most significant bit planes are removed. The classification is done using SVM. Hiding techniques i.e. SS and LSB substitution are detected and classified. It outperforms (Farid, H., 2002) by increasing detection accuracy by 19.4 \% and outperforms (Shi, Y.Q., Xuan, G.,Zou, D.,Gao, J., 2005) by increasing detection accuracy by 4.8 \% in case of LSB hiding techniques.

(Zhang, H. L., 2008) proposed feature extraction using statistical moments from the three-level wavelet decomposed image using second-order Butterworth high-pass filter of dimension 39 on 1000 JPEG images. In this work emphasis is on high frequency filtering along with histogram equalization method. The classification is done using linear and non-linear SVM. JPEG Hiding techniques i.e. F5, outguess and MB1 are detected and classified. It provides similar detection result as (Fridrich, J., 2005) with reduced execution time.

(Liu, S., Ma, L., 2009) proposed feature extraction using statistical moments from the from reorganized block DCT coefficient. The proper reorganization of the block based DCT is having characteristics similar to wavelet transform of dimension 228 on 1000 images. The classification is done using SVM. Hiding techniques i.e. SS and LSB hiding are detected and classified. It outperforms (Farid, H., 2202) and (Shi, Y.Q., Xuan, G.,Zou, D., Yang, C., 2005) by increasing detection accuracy by 1.95 \% from Shi, Y.Q., Xuan, G.,Zou, D., Yang, C., 2005) and by 22 \% from (Farid, H., 2202) in case of SS.

(Hui, L., 2011) proposed feature extraction using characteristic function of the three-level decomposed wavelet subbands of dimension 102 on 1300 JPEG images. The features are calculated after the image prediction. This prediction-error image removes information other than that caused by data hiding, thus making the steganalysis more efficient. The feature dimension is reduced from 102 to 50 by implementing PCA. The classification is done using SVM. JPEG hiding
techniques i.e. F5, outguess and Jsteg are detected and classified. The detection accuracy is increased by using PCA such as by the value 17.5% in case of F5 for low payload.

2.1.5 Blind Steganalysis Techniques Reports Using Co-Occurrence Based Features

(Xuan, G. R., Shi, Y.Q. and Huang, C., 2006) proposed feature extraction using global average co-occurrence matrices from DCT co-efficients after zig-zag scanning low and middle inter block co-occurrence from DCT coefficients of dimension 120 on 3908 JPEG images. JPEG hiding techniques i.e. Jsteg, outguess, F5 and MB are detected and classified. The classification is done using CNPCA. It outperforms (Farid, H., 2002) and (Fridrich, J., 2005) by increasing the detection accuracy except for 1 KB and 2KB payload when compared from (Fridrich, J., 2005). The detection accuracy increases such as in case of 1KB F5, the performance increase by 20%.

(Ke, K., 2010) proposed feature extraction using (Xuan, G. R., Shi, Y.Q. and Huang, C., 2006). JPEG hiding techniques i.e. F5, Outguess, Jsteg and MB are detected and classified on 2000 images. The classification is done using BPNN. Bhattacharyya distance concept is used to reduce the dimension from 120 to 24. Basis of the selection is detection accuracy. The detection accuracy is increased by 3% for F5 as compared to (Xuan, G. R., Shi, Y.Q. and Huang, C., 2006).

(Wang, P., Liu, F. Wang, G., 2008) proposed feature extraction using co-occurrence matrices from inter block co-occurrence from DCT coefficients. It improves the efficiency of blind steganalysis proposed by (Xuan, G. R., Shi, Y.Q. and Huang, C., 2006) by introducing feature selection technique using Bhattacharyya distance of dimension 120 on 2000 JPEG images. The selected feature dimension is reduced to 24 from 120. JPEG hiding techniques i.e. Jsteg, outguess, F5 and MB are detected and classified. The classification is done using BPNN. The detection accuracy is 100% for many cases such as for Jsteg, F5 and outguess. The detection accuracy is 99.8% in case of MB.

(Kodovsky, J. and Fridrich, J., 2012) proposed feature extraction using co-occurrence matrices from inter block co-occurrence in spatial domain and intra block co-occurrence in DCT domain from input image and from its cartesian calibrated image of dimension 22510 on 6500 JPEG images. The introduction of cartesian calibration with the JPEG domain rich model, the feature is named as cartesian calibrated feature for JPEG domain rich model (CC-JRM). The classification is done using ensemble classifier. JPEG hiding techniques i.e. nsF5 and MB are detected and classified. It outperforms (Lyu, F., 2003) and (Penvy, T., 2007) for all the cases.

(Kodovsky, J., Fridrich, J. and Holub, V. 2012) proposed feature extraction using co-occurrence matrices from inter block co-occurrence in spatial domain and intra block co-occurrence in DCT domain from input image and from its cartesian calibrated image of dimension 7850 on 6500 JPEG images. JPEG hiding techniques i.e. nsF5 and MB are detected and classified. The introduction of random forest as ensemble classifier as machine learning tool, the computational cost with respect to execution time get reduced by large amount such as required execution time is 1 min in case of RF as compared to 5 min in case of SVM for nsF5 having 0.1 bpc payload. The feature selection is included such as adaboost and majority voting technique. The ensemble features are named as cartesian calibrated feature. The classification is done using ensemble classifier. It outperforms (Lyu, F., 2003) and (Penvy, T., 2007) for all the cases.

(Li, F., 2013) proposed feature extraction using co-occurrence matrices from inter block co-occurrence in spatial domain and intra block co-occurrence in DCT domain from input image and from its cartesian calibrated image i.e. 7850 CF features from the images and also from its calibrated images having total dimension of 15700 on 5000 BOSSbase images. JPEG hiding techniques i.e. nsF5 and MB are detected and classified. The introduction of Bayesian classifier as machine learning tool, the computational cost with respect to execution time get reduced by large amount such as required execution time is 142 sec in case of Bayesian as compared to 18 min in case of SVM for nsF5. Bayesian classifier integrates a number of sub-classifiers as an ensemble classifier with a Bayesian mechanism. The ensemble features are named as difference features. It outperforms (Kodovsky, J., Fridrich, J. and Holub, V. 2012) in case of MB by increasing detection accuracy by 2% for 0.03 bpc payload but fails in case of nsF5.

2.1.6 Blind Steganalysis Techniques Reports Using Merged Features

(Cia, H., 2006) proposed feature extraction using intensity gradient from spatial and DCT frequency domain of dimension 390 on 1000 JPEG images. The classification is done using SVM. The classification is done using SVM. JPEG hiding techniques F5 is detected.

(Penvy, T., 2007) proposed feature extraction using extended DCT features and reduced Markov’s transition probability matrix from intrablock difference array of JPEG 2-D array of DCT coefficients of an image and from calibrated image of dimension 274 on 3400 JPEG images. These merged features are known as CCPEV (Cartesian Calibrated features extracted by Penvy). The classification is done using SVM. The features extracted from difference JPEG 2-D arrays along horizontal, vertical and diagonal directions. Extended DCT features model inter-block dependencies between DCT coefficients. JPEG hiding techniques i.e. F5, MB, Outguess are detected and classified. It outperforms (Fridrich, J., 2005) and (Shi, Y.Q., 2007) steganalysis algorithm in all cases such as detection accuracy is increased by 1.64% from (Fridrich, J., 2005) steganalysis algorithm and by 1.12% from (Shi, Y.Q., 2007) in case of outguess for 50% message length except for MB of 50% and 100% message length in case of (Fridrich, J., 2005).
(Xu, B., 2007) proposed feature extraction using image quality matrices proposed by Ismail Avcibas (Avcibas, I., 2003) from DCT, DWT and independent component analysis (ICA) domain of dimension 26 on 1000 JPEG images. The classification is done using SVM. Feature selection technique ANOVA is used which reduces feature from 26 to 8. Stego images are obtained by various hiding techniques. The characteristic of the data embedding is similar for spatial and DCT domain. So, it is difficult to distinguish between spatial domain and DCT domain stego images. But there is lower fault in distinguishing DWT and ICA stego images. For 5% hidden data, the detection accuracy is 63% for spatial domain, 56% for DCT domain, 85% for DWT domain and 81% for ICA domain.

(Liu, Y., 2008) proposed feature extraction using Robert gradient energy from spatial domain, variance of Laplacian from DCT domain and first order statistics from DWT domain of dimension 26 on 1014 JPEG images. The classification is done using NN. JPEG hiding techniques Jsteg is detected and classified. It provides 90% detection accuracy for 100%, 75%, 50% and 25% payload.

(Leng, C.K., 2008) proposed feature extracting by merging image quality matrix proposed by (Avcibas, I., 2003), moments of the wavelet subbands proposed by (Lyu, S. and Farid, H., 2003) and DCT features proposed by (Fridrich, J., 2005) on 2037 images. Feature selection technique sequential forward floating selection technique (SFFS) is used finally after comparing the selection results obtained by using T-test and Bhattacharya distance. JPEG hiding techniques F5, MB and outguess are detected and classified. NN is finally selected as classifier after comparing the results with SVM, FLD and MR. Outguess is easily detectable among others. It outperforms (Farid, H., 2003) by increasing area under ROOC curve by the value 0.11345.

### III. RESULTS AND DISCUSSIONS

(Li, Z., Lu, K., 2009) proposed feature extraction using additional DCT coefficients other than proposed by (Fridrich, J., 2005) from DCT coefficients and spatial domain of 82-dimensional feature vector on 2544 images. Characteristic functions and center of mass (COM) is used to select statistics and measure the features. The features are also calculated from calibrated images. The JPEG hiding techniques Jsteg, F5 and outguess are detected and classified. The classification is done using SVM. It outperforms (Lyu, S. and Farid, H., 2003) and (Fridrich, J., 2005).

(He, Z.M., 2010) proposed feature extraction using by merging Markov’s one-step TPM and DCT features. Markov’s TPM is calculated from DCT coefficients of JPEG difference matrix in the horizontal, vertical and diagonal directions for threshold value of 3 having dimension 147. Including 23 DCT features, 170 features are the total dimension on 1000 images. JPEG hiding techniques F5 and outguess are detected and classified. The classification is done using RBFNN. The architecture of RBFNN is selected by minimizing the localized generalization error (L-GEM) which improves the generalization capability of the RBFNN for steganalysis.

(Cho, S., 2010) proposed feature extraction by merging Markov’s and DCT features. Instead of single decision, repeated block decomposition process is implemented, and a classifier is selected to make decision whether an image is a cover or a stego. The majority voting rule is used to make final decision on 2829 images. The classification is done using SVM. JPEG hiding techniques PQ and MB are detected and classified. It outperforms (Penyv, T., 2007) by increasing detection accuracy by 15% in case of MB for 0.2 bpcn. The decision reliability increases from 77.98% with 0 – 5 voting difference to 99.76% with 21 – 48 voting difference.

(Cho, S., Wang, J., 2010) proposed feature extraction by merging Markov’s and DCT features. Instead of single decision, repeated block decomposition process is implemented, and a classifier is selected to make decision whether an image is a cover or a stego. Blocks are selected by random sampling and the tree-structured vector quantization (TSVQ) technique is adopted to classify blocks into multiple classes. The majority voting rule is used to make final decision on 2829 images. The classification is done using SVM. JPEG hiding techniques outguess, F5, and MB are detected and classified. It outperforms (Cho, S., 2010) such as the detection accuracy improved by 25.9% in case of outguess.

(Quinijje, C., 2010) proposed feature extraction using Markov extended feature and co-occurrence matrix feature on 1400 images. The classification is done using modified SVM. JPEG hiding techniques Jsteg, F5, outguess, MB1 and MB2 are detected and classified. The modified SVM result is compared with classic SVM and better result is obtained such as 1.8% increment in detection accuracy in case of F5.

(Liu, C., 2010) proposed feature extraction by merging image gradient energy and entropy features in spatial domain and marginal statistics from the three level decomposed wavelet subbands suggested by (Farid, H., 2002) of dimension 74 on 1600 images. The classification is done using SVM. It outperforms (Farid, H., 2002) by increasing the detection accuracy.

(Yu, W., 2010) proposed feature extraction by using nine additive noise steganography in the spatial domain by using statistical models are constructed from the DCT and the COM of the histogram characteristic of dimension 486 on 1640 images. JPEG hiding techniques outguess, MB1 and MB2 are detected and classified. The classification is done using SVM. It outperforms (Fridrich, J., 2005), (Shi, Y.Q., Chen, C., 2006) and (Fu, D., 2006) such as detection accuracy is increased by 32% from (Shi, Y.Q., Chen, C., 2006) in case of 0.05 bpcn outguess.

(Kodovsky, J. and Fridrich, J. 2011) proposed merging of of 548-dimensional features of (Penyv, T., 2007), 648-dimensional features of (Shi, Y.Q., 2007) and 48000 dimensional features of co-
occurrences. JPEG hiding techniques nsF5 is detected and classified. Instead of SVM multiclass trained FLD removes the drawbacks of SVM. Using feature reduction technique, the final feature dimension is of 48600 on 90,000 images. Among the 274 features, selected 300 features of CCPEV are used for the steganalysis. So, the feature set is named as cartesian calibrated co-occurrence of dimension 300 (CC-C300). The proposed modification in the classification technique, the detection of nsF5 is improved.

(Kumar, M., 2012) proposed feature extraction using expanded DCT features and two step inter and intra block Markov’s transition probability matrices from difference array of JPEG 2-D array of DCT coefficients of an image and also from its calibrated image of dimension 261 on 3000 camera images. The considered threshold value is 4. The classification is done using SVM. JPEG hiding techniques i.e. F5, nsF5, MB, Outguess, PQ are detected and classified. The proposed steganalysis algorithm outperforms (Fridrich, J., 2005) state of art steganalysis algorithm from 36 % to 47 % transforms stego images of 0.2 bpnz. It outperforms (Fridrich, J., 2005) method in all cases such as in case of outguess detection accuracy rate increases by 1.7 % for 0.05 bpnz and 1.5% for 0.2 bpnz except nsF5 where the proposed algorithm’s detection rate was around 36% at 0.05 bpnz.

(Chen, B., 2014) proposed feature extraction by merging image features proposed by (Shi,Y.Q., 2007) of dimension 648, (Penvy, T., 2007) of dimension 548 and (Kodovsky, J., Fridrich, J. and Holub, V. 2012) from DCT coefficients of dimension 7850 on 2000 BOSSbase images. The features of (Shi,Y.Q., 2007) of dimension 648 and 386 extended DCT features and final 1034 dimensional features are obtained named as PS features. The 3750 features of (Kodovsky, J., Fridrich, J. and Holub, V. 2012) are selected and merged with PS features and finally 4784 dimensional features are obtained which is named as PSC features. The classification is done using ensemble classifier. JPEG hiding techniques i.e. MB and nsF5 are detected and classified. It outperforms (Shi,Y.Q., 2007) and (Kodovsky, J., Fridrich, J. and Holub, V. 2012) for all cases except 0.01 bpc, 0.02 bpc, 0.04 bpc and 0.05 bpc payload MB as compared when compared to (Kodovsky, J., Fridrich, J. and Holub, V. 2012).

(Pathak, P., 2014) proposed feature extraction by merging spatial domain, DCT domain and wavelet domain image features of dimension 309 on 300 JPEG images. JPEG images are first decompressed to obtain spatially transformed image (STI) and calibrated image is obtained which is named as calibrated spatially transformed (CSTI). The first order statistics i.e. mean, variance, skewness, kurtosis, global histogram, histogram of a.c. coefficients, co-occurrence matrix are calculated from STI, CSTI, frequency transformed CSTI, and wavelet image proposed by (Shi,Y.Q., 2007) of dimension 648, (Penvy, T., 2007) of dimension 548 and (Kodovsky, J., Fridrich, J. and Holub, V. 2012) from DCT transformed CSTI. The classification is done using SVM. JPEG hiding techniques i.e. F5 and outguess are detected and classified. It provides detection accuracy of 88% for very low payload of 0.09 % embedding value.

(Mohammadi, F. G., 2014) proposed feature extraction by merging 686 dimensional SPAM features proposed by (Pevny,T., 2010) and 548 dimensional CCPEV features proposed by (pevny.t., 2007) on 10,000 images. Image steganalysis feature selection artificial beecolony (IFABC) feature selection method is implemented to reduce the feature dimension and then SVM is used for classification. The 686 dimensions of SPAM is reduced to 80 and 548 dimension of CCPEV is reduced to 250. The value of the reduced dimension is decided according to the detection accuracy results. In case of SPAM detection accuracy is increased by 2.98 % and in case of CCPEV, the detection accuracy is increased by 3.22% with the implementation IFABC.

2.1.7 Blind Steganalysis Techniques Reports Using Decompressed JPEG Image Based Features

(Holub, V., 2015) introduced the decompressed JPEG image-based JPEG blind steganalysis in which features are extracted by computing 64 convolutions of the decompressed JPEG image with 64 8 × 8 kernels and forming histograms of dimension 8000 on 10,000 BOSSbase images. The features can also be interpreted in the DCT domain and named as discrete cosine transform residual (DCTR) features. This approach provides low feature dimension with low complexity. The classification is done using FLD ensemble. JPEG hiding techniques i.e. nsF5 and JUNIWARD are detected and classified. JUNIWARD is the adaptive JPEG hiding technique by modifying DCT coefficients provides high payload capacity. It outperforms (Kodovsky, J. and Fridrich, J. 2012) i.e. CC-JRM for both nsF5 and JUNIWARD for payload from 0.05 to 0.5 bpnz for different quality factor. The DCTR also provides quite competitive detection for nsF5 and provides better results as compared to the 22,510-dimensional JRMs. The extraction of the DCTR feature vector for one BOSSbase image is twice as fast as JRMs provides low complexity.

(Song, X., 2015) proposed feature extraction using histogram from the 64 filtered subimages obtained by convolution of the decompressed JPEG image with 8 × 8 2D Gabor filter of dimension 17,000 on 10,000 BOSSbase images. The features are named as Gabor filter rich (GFR) feature. The classification is done using ensemble classifier. JPEG hiding techniques JUNIWARD is detected. The merging of the histogram was done which reduces the feature dimension. The parameters of the gabor filter is set according to the value of the classification error. It outperforms (Kodovsky, J. and Fridrich, J. 2012) i.e. CC-JRM and (Holub, V., 2015) i.e. DCTR for JUNIWARD for payload from 0.05 to 0.5 bpc for different quality factor. The classification error is also evaluated by combining CC-JRM, DCTR and GFR. It is observed that the combination of different steganalysis features only can improve the detection performance.
slightly. GFR provides better detection capability with fast computation time.

(Song, X., 2016) proposed feature extraction using histogram, scale, orientation, intra-block and inter-block co-occurrence from the 64 filtered subimages obtained by convolution of the decompressed JPEG image with \( 8 \times 8 \) 2D Gabor filter of dimension 31756 on 10,000 BOSSBase images. The features are named as Gabor rich filter (GRF) feature. The classification is done using ensemble classifier. JPEG hiding techniques JUNIWARD is detected. The merging of the histogram was done which reduces the feature dimension. The parameters of the gabor filter is set according to the value of the classification error. It outperforms (Lyu, F., 2003), (Penvy, T., 2007) i.e. CCPEV, (Kodovsky, J. and Fridrich, J. 2012) i.e. CC-JRM, (Holub, V., 2015) i.e. DCTR and (Song, X., 2015) i.e. GFR for JUNIWARD for payload from 0.05 to 0.5 bpc for different quality factor such as the payload is 0.2 bpc and QF is 75, the improvement is 13.39 %, 6.06 %, 2.03 % and 1.31 % with respect to CC-JRM, DCTR and GFR, respectively. When the QF is 95, the improvement is 9.18 %, 5.12 %, 3.06 % and 1.71 %, respectively.

2.1.8 Blind Steganalysis Techniques Reports Using Zipf’s Law

(Laimeche, L., 2017) proposed feature extraction using Zipf’s law of the three level decomposed wavelet subbands of dimension 56 on 1338 JPEG images. Zipf’s curve characterizes the structural complexity of the texture of an image. The classification is done using RF. JPEG hiding techniques Outguess is detected. It outperforms (Li, F., 2013) in case of spatial steganography but not in case of JPEG steganography.

2.1.9 Blind Steganalysis Techniques Reports Using Contourlet Transform

(Sajedi, H., 2008) proposed feature extraction using statistical moments of three level contourlet coefficients in eight directions of dimension 64 on 315 JPEG images. The contourlet transformation is an advanced transformation to the wavelet transforms using two dimensions using non-separable and directional filter banks. The textural characteristics of an image are very well captured by contourlet as compared to wavelet transformation. The first four moments is calculated from all the eight subbands in the third level and also from difference between actual and linear predicted coefficients as feature vector. The developed technique is named as contourlet based steganalysis (CBS) The classification is done using SVM. JPEG hiding techniques i.e. MB and YASS are detected and classified. It outperforms (Farid, H., 2006) and (Fridrich, J., 2005) in cases except for 8 KB payload of YASS. The detection accuracy is increased by 4.9 % from (Fridrich, J., 2005) and by 8.7 % from (Farid, H., 2006) for 8KB payload MB. (Sheikhan, M., 2010) proposed feature extraction using first order statistics and co-occurrence matrix from contourlet transformation. Contourlet filter bank is a combination of a Laplacian pyramid and a directional filter bank which is an advanced transformation to the wavelet transforms. ANOVA is used to evaluate the discrimination ability of features in discriminating groups which which reduces the feature dimension further. The classification is done using SVM. JPEG hiding techniques i.e. OutGuess, Jsteg and MB are detected and classified. Feature dimension is 576 among which 384 features are co-occurrence statistics of Contourlet coefficients, 96 features are statistical moments of Contourlet coefficients, and 96 features are statistical moments of Contourlet predicted magnitude coefficients. 102 features are selected by ANOVA. It outperforms (Sajedi, H., 2010) by increasing detection accuracy by 11 %.

IV. CONCLUSION

- In the designing of steganography technique, there is always trade-off between the payload and the detection rate. It is always tried to minimize this trade-off.
- In steganalysis, the detection accuracy increases if payload increases. So, the performance of any newly designed detection technique is analyzed on the increment in the value of detection accuracy for different payload values. The performance is also analyzed on the basis of complexity which depends on the computation time.
- Embedding data means addition of noise. The detection methodology depends on the nature calculation of this noise.
- According to Cachin, for e-security, if Kullback-Leibler distances also known as relative distance between the distribution of stego and cover images is zero. If their exist relationships among the image coefficients, then only detected by Cachin’s definition. Other well-known distance calculations are Bhattacharya distance, Manhattan distance, Euclidean distance between two histograms.
- There is scope of research in feature based steganalysis using various statistical parameters extracted from DCT or DWT co-efficient of the image or from residual of image filter such as DCT residual, Gabor filter.
- Difference JPEG 2-D arrays along horizontal, vertical, diagonal and minor diagonal directions is obtained of DCT coefficients which enlarged changes caused by steganographic methods. Using DCT coefficients, as compared to F5, outguess is breaked more easily than outguess as in F5 matrix coding is used.
- Thresholding technique applied to handle transition probability matrices has greatly reduced dimensionality of feature vectors to a manageable extent.
- Markov’s TPM from JPEG 2-D arrays is higher order statistics provides better detection results. The two step Markov’s
process gives better result than one-step. Because increasing the stepsizes explore more statistical correlation among the pixels of an image.

- Secure steganographic schemes must preserve as many statistics of DCT co-efficients as possible. It is not enough to preserve the marginal statistics, e.g., the histograms. DCT coefficients exhibit block-to-block dependencies that must be preserved as well. In outguess, it is tried to preserve the higher statistics. So for the detection of outguess more correlation statistics are required. Statistical features from the DCT features provide better detection capability of outguess.

- Even though a scheme may preserve a specific statistic $\zeta(X)$ of the cover JPEG image $X$, the calibrated statistic $\zeta(\text{Compress(Crop}(X)))$ calculated from the cropped/recompressed image may not necessarily be preserved, thus opening the door for attacks. Future steganographic schemes should add cali-brated statistics to their set of preserved statistics. So the image calibration introduces better detection capability.

- Image calibration is not always a good idea especially for smaller payloads. To solve this problem, cartesian products of features from calibrated images are adopted for feature extraction.

- The prediction-error image is used to erase the cover image content. The features extracted from prediction-error image have smaller relativity, and it can enhance the sensitivity of steganalysis.

- The decompressed JPEG image based JPEG blind steganalysis provides low complexity, fast computation time, relatively small dimension yet provides competitive detection performance across all JPEG steganographic algorithms.

- The combination of the steganalysis methods does not improve much the detection accuracy.

- Embedding capacity is more in F5 than outguess because in outguess large portion of bits are used for statistical restoration of first order and second order.

- In most of the cases, nsF5 is difficult to detect because it resolves the shrinkage problem and adopted the matrix coding for hiding the data bits.

- In MB steganography, preserves marginal statistics of DCT coefficients and the co-occurrence matrix which captures block-to-block dependencies to resist attack. But the co-occurrence matrix feature is able to break this type of hiding technique. The image is split into two parts. One half is used to model the distribution of parameters and according to which the data are embedded in the second part. MB1 and MB2 perform better than F5 and outguess because the marginal statistics in the edge of an image is preserved. But embedding capacity decreases because most of the non-zero coefficients are involved in statistical preservation. Due to embedding, the discontinuities increases along the 8 x 8 block boundaries. This property helps in designing detection capability of MB steganography. MB2 performs better than MB1. MB2 preserves blockiness but does not preserves co-occurrence.

- The generation of 2D Gabor filters is very important, in the future, the effect of 2D Gabor filter construction for steganalysis of adaptive JPEG steganography will be studied to improve the detection accuracy further. In case of Gabor based feature extraction, the scale and orientation parameters of 2D Gabor filters are very important. The parameter selection will be studied to improve the detection accuracy further. In addition, for feature dimension reduction, the random projection (RP) is an important method. Therefore, the dimensionality of the feature extracted by 2D Gabor filters may be reduced further while the detection accuracy is preserved. There is scope of reducing the feature dimension with no comprising with the value detection accuracy.

REFERENCES


An Experimental Analysis of Feature Based Blind Steganalysis Techniques

Hiding and Multimedia Security.


114. An Experimental Analysis of Feature Based Blind Steganalysis Techniques


www.cse.psu.edu/~rc12/CSE486/lecture06.pdf.


170. Li, F., Zhang, X., Chen, B. and Feng, G. 2013. JPEG Steganalysis with High-Dimensional Features and Bayesian

358

Published By: Blue Eyes Intelligence Engineering & Sciences Publication
An Experimental Analysis of Feature Based Blind Steganalysis Techniques


