Scientific
Research
Publishing

A Survey on Different Feature Extraction and Classification Techniques Used in Image Steganalysis

John Babu[1*], Sridevi Rangu[2], Pradyusha Manogna[3]

[1]Department of CSE, Sreekavitha Engineering College, Khammam, India
[2]Department of CSE, JNTUH College of Engineering, Hyderabad, India
[3]Department of CSE, Vijaya Engineering College, Khammam, India
Email: *johnbabug@gmail.com

Abstract

Steganography is the process of hiding data into public digital medium for secret communication. The image in which the secret data is hidden is termed as stego image. The detection of hidden embedded data in the image is the foundation for blind image steganalysis. The appropriate selection of cover file type and composition contribute to the successful embedding. A large number of steganalysis techniques are available for the detection of steganography in the image. The performance of the steganalysis technique depends on the ability to extract the discriminative features for the identification of statistical changes in the image due to the embedded data. The issue encountered in the blind image steganography is the non-availability of knowledge about the applied steganography techniques in the images. This paper surveys various steganalysis methods, different filtering based preprocessing methods, feature extraction methods, and machine learning based classification methods, for the proper identification of steganography in the image.

Keywords

Steganalysis, Steganography, Feature Extraction, Classification

1. Introduction

The steganography is a process of making the presence of secret data undetectable in a carrier [1]. The secret messages are embedded within a larger cover in such a way that the observer cannot identify the presence of contents of the hidden message. Various carrier file formats are included but digital images are mostly used as carriers due to the redundancy of data in images and the fre-

quency of use on the internet. The steganalysis is the procedure of detecting the presence of hidden message embedded using steganography. The image steganalysis method utilizes the features that are affected by steganography and then a machine learning classification. To use this method, the steganalyst must extract the features from a training data set to train the classifier. Then, the classifier is validated by using a testing dataset. If the results are accurate, then the classifier is considered as an effective classifier.

The classification capability is decreased as the testing dataset differs from the training dataset. The data set acquired after feature extraction depends on the steganography algorithm used for hiding the data into cover source, feature extraction algorithm and the cover source properties. If similar cover source is employed, the feature extraction process delivers the data set with similar representation. Therefore, the results produced from the classifier would be satisfactory. Likewise, if different cover source is used, the obtained data set from feature extraction process is also different and the classification results are degraded.

Nowadays, the complexity of steganography algorithms is increased. So, the image steganalysis must be designed with high dimensional feature space [2]. Some of the ancient steganographic methods are invisible ink, spread spectrum communication, covert channel and microdot [3]. The fundamental requirement of steganographic system is that the hidden information causes only minor modifications in the cover object. The steganography methods are classified into two types.

- Spatial domain steganography,
- Transform domain steganography.

The spatial domain method is frequently used due to its high capacity of hidden information and easy implementation [4]. Here, the secret messages are embedded directly by altering the pixel intensity values of an image. This method is further divided into Least Significant Bit (LSB) insertion technique, Pixel Value Difference (PVD) method, mapping pixel to hidden data, Random Pixel Embedding (RPE) method, Edge Based data Embedding (EBE) method, Labeling or connectivity method, Histogram shifting method, Pixel intensity based method, Enhanced Least Significant Bit (ELSB) algorithm, and Texture based method. In LSB based methods, least significant bits of the pixels are replaced by the message bit for embedding. In block based method, the cover is divided into equal sized blocks before embedding the data. In Edge based method, the sharper edge regions are used for hiding the message. In these methods, ELSB algorithm offers more security. In grey level method, the host images are divided into blocks and the corresponding secret message bits are embedded into each block by using layers. The layers are prepared by the binary representation of pixel values. The spatial domain methods reduce the chance of degradation of original image and deposit larger information in an image. The disadvantages are that these methods are less robust, and hidden data may be lost in image manipulation and hidden data can be easily destroyed by simple attacks.

The transform domain method embeds the secret message information in the format of transform coefficients of the cover image [5]. Numerous transformations and algorithms are applied on the image for hiding the message information. Transform domain has advantages over spatial domain as the information hidden in the image is will not be affected by compression, cropping, and image processing. These methods are classified into following categories: Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT), Lossless or reversible method, and Embedding methods. Every steganography method employs a special mechanism to embed the secret data in the images. Therefore, it positions a distinct pattern on the stego images.

In general in a steganalysis scheme the stages are image preprocessing, feature extraction and classification. The preprocessing eliminates the noise present in the images. Feature extraction is an important concept in the image classification. The most relevant features are extracted from an image and used for the classification.

This paper is arranged as follows. Section 2 describes the steganalysis techniques. Section 3 discusses the filtering techniques for image preprocessing, Section 4 presents feature extraction techniques and Section 5 presents classification techniques. Section 6 discusses the results and conclusions based on the survey.

2. Steganalysis Techniques

The steganalysis techniques are categorized into two types, signature steganalysis and statistical steganalysis. This classification is based on the method used to detect the presence of hidden message in the image embedded by the steganography. The secret information hidden in the image or any other digital media, which is invisible to human, causes the modification of media properties that produces the degradation, unusual characteristics and patterns. These patterns and characteristics may act as a signature that is broadcasted with the embedded message. The signature steganalysis is further divided into specific signature steganalysis and universal signature steganalysis. The information hiding process changes the statistical properties of the cover, which a steganalyst attempts to detect. The process of attempting to detect such statistical traces is called statistical steganalysis. Statistical steganalysis is considered as a powerful tool as compared with signature steganalysis due to its sensitivity. Some of the methods based on statistical steganalysis are LSB embedding steganalysis, LSB matching steganalysis, spread spectrum steganalysis, JPEG compression steganalysis, addictive noise steganalysis, and transform domain steganalysis [6]. The following section of the paper discusses the recent steganalysis methods are presently used.

The block based steganalysis method [7] provides an accurate steganalytic performance without increasing the amount of features. It has two phases, training process and testing process. In training, an image is decomposed into smaller blocks and each block is considered as the basic unit for steganalysis. The stego image is obtained by embedding the secret image into the cover image. This process is implemented on every cover image to acquire the cover-

stego image pairs. This image pair is decomposed into smaller blocks of size. A set of desired features are extracted from each image block and a tree structured clustering algorithm is applied to classify the blocks into various classes based on their extracted features. In testing, same block decomposition and feature extraction are carried out on the test images. Then, the blocks are classified into single block class and the decision is taken to identify the stego block. The decision of multiple blocks are integrated into a single decision based on the majority voting rule. If the number of cover blocks is larger or smaller than the stego blocks, then it is declared as stego image.

The Spatio-Color Rich Model comprises of two different components, the Spatio Rich Model (SRMQ1) and Color Rich Model (CRMQ1) [8]. The SRMQ1 and the CRMQ1 features are calculated and used efficiently for the detection of steganography in images. The SRM noise residuals are calculated by using linear and non-linear local pixel predictors. The residuals are further classified into five classes on the basis of the structure of filters: first order, second order, third order, edge kernels and square kernels. The Collaborative Representation (CR) [9] utilizes all the training samples from both cover and stego for the representation of testing samples to solve the least square problem. The regularization term is changed from l_1 norm to l_2 norm for regularizing the coding vector and producing lower complexity.

The Least Significant Bit (LSB) matching steganalysis operates from the difference of neighboring pixels before data embedding and after data embedding [10]. The significant information of neighboring pixels are gathered to create patterns. Then, the numbers of patterns present in the image are calculated and the random data is embedded into the test image. The number of patterns are again calculated after completing embedding. The relationship among number of patterns in each case is varied, based on whether the test image is cover or stego. The accurate detection of steganography in color images is achieved by the Difference Histogram Characteristics Function (DHCF) [11]. If the distance among the pixels are high, then the difference between the pixel gray values are smoothed by the stego bits obtained by LSB matching. The extracted features from the difference of the non-adjacent pixels are used to train the classifier.

3. Image Preprocessing Techniques

The preprocessing is applied to images to remove the redundant and irrelevant content present in the image [12]. The noise incorporated into the image is also eliminated.

3.1. Discrete Wavelet Transform (DWT)

The Discrete Wavelet Transform (DWT) based preprocessing technique improves the security of steganography [13], which embeds the secret message in the frequency domain of the cover image. It hides the messages in substantial areas of the cover image to make it more robust to the attacks.

3.2. Vector Rank M-Type L Filter (VRML)

The Vector Rank M-type L (VRML) filter removes the impulsive noise and speckle noise from the color images and video sequences [14]. This filter consists of two estimators such as Median-M type (MM) and Ansari-Bradley Siegel-Tukey M-type (AM) for providing robustness in the filtering technique. The impulsive noise detectors are also included to improve the properties of noise suppression in the low and high densities of impulsive noise. It has edge preservation property and power in noise detection during the presence of impulsive noise.

3.3. Successive Mean Quantization Transform (SMQT)

The Successive Mean Quantization Transform (SMQT) extracts the structure of data in robust manner [15]. Here, the capacity of the embedding is identified from the non-zero Discrete Cosine Transform (DCT) coefficients. In Boosted Steganography Scheme (BSS), a cover image is preprocessed in two stages, once in preprocessing stage and then in embedding stage. In preprocessing stage, the image processing techniques such as contrast enhancement, SMQT and other manipulation methods are applied on the cover images.

3.4. Scale Invariant Feature Transform (SIFT)

The image saliency detection based preprocessing technique utilizes the quaternion transform. The region segmentation and Scale Invariant Feature Transform (SIFT) are considered as the preprocessing technique to extract the accurate features by removing the irrelevant features[16].The textural features like contrast, coarseness, directionality, regularity and roughness are traced.

3.5. Anisotropic Diffusion (AD)

The Anisotropic Diffusion (AD) based pre-processing performs the image smoothing and image enhancement [17]. The matrix representing the image is flipped left to right in the vertical axis.

3.6. Chirp Z-Transform (CZT)

The combination of Chirp Z-Transform (CZT) and Goertzel algorithm are used as the preprocessing technique to normalize the image [18]. The input image is divided into specific number of same sized blocks and CZT is applied to every individual blocks. The CZT calculates the Z transform at M points in Z-plane and it transforms the image into Z-domain. Then, the Goertzel algorithm is applied to the transformed image as a reconstruction algorithm that is produced an image with the inversion of an original image. The normalized images is acquired after completion of reconstruction process.

3.7. Other Filters

The 2 Dimensional (2D) Wiener filter is an adaptive noise removal filter that performs low pass filtering of a gray scale image.

A Gaussian filter is a low pass filter with minimum time bandwidth product.

The Gamma Intensity Correlation (GIC) enhances the local dynamic range of the image in the dark or shadowed region during compression.

4. Feature Extraction Techniques

The feature extraction is the process of extracting the essential information or characteristics from the original image [19]. Some of the feature extraction techniques are discussed in this section.

4.1. Relative Auto Decorrelation (RAD)

Relative Auto-Decorrelation (RAD) feature extraction method extracts the intrinsic features that improve the detection of stegos from the cover [20]. The appropriate features like Local Entropies Sum (LES) and Clouds Min Sum (CMS) are acquired to obtain fast detection accuracy and improves the steganalysis results. The common part of an image is processed by a smart partioning procedure known as two-dimensional Decorrelation of the received images (2D). The presence of secret message is identified by the quadratic estimator that provides the estimation of embedding rate. The rate estimation is modified by the thresholds derived from the RAC, LES, and CMS. This type of steganalysis consists of three stages such as image clouding, RAD feature extraction and quadratic rate estimation. The clouding splits the input image into luminance aware slices. Every cloud has same luminance pixels in an edge free region of the image.

4.2. Discrete Cosine Transform (DCT)

The differential Discrete Cosine Transform (DCT) coefficients extracts the absolute values of the Neighboring Joint probability density (absNJ) features [21]. This is done by applying P^{th} power of DCT coefficients instead of their first power gains, which differentiates the stego images from the cover image. The inter block and intra block features of DCT coefficients are extracted, which provides different types of features. The intra block features extracts the frequency dependencies of DCT coefficients and the inter block features extracts the spatial dependencies among DCT blocks. Through the extension of original features to the extended versions, the most complicated relations between the coefficients are extracted to produce the final features.

4.3. Gabor Wavelet Transform

The Shannon entropy of 2-Dimensional (2D) Gabor wavelet feature extraction model has joint localization properties in spatial domain [22]. The image texture characteristics are captured by the spatial frequency. The Shannon entropy values of image filtering coefficients are considered as steganalysis features. Initially, JPEG image is decompressed to the spatial domain without quantizing the pixel values to avoid the information loss. The image is decomposed into 8×8 DCT blocks and each block has 64 different DCT modes. Each filtered image can be subsampled to form a sub image. The decompressed image is filtered through 2D Gabor wavelets. Then, the entropy features are extracted from all filtered

images. The entropy is the randomness measure that is used to characterize the image texture. The classifier is trained by the selected entropy features.

4.4. Spectrum Based Feature Extraction

The spectrum based feature extraction utilize the combination of DCT and Discrete Fourier Transform (DFT) [23]. The input image contains many features and the transformation of the image in frequency domain is applied to reduce the redundancy information present in the image. The subset of transformed coefficients are required to reserve the desired important features for recognition. The DFT is applied on the pre-processed image. The low frequency components are situated in the center of the spectrum. The center portion is extracted by using centered rectangular mask. Then, the DCT is applied to the DFT spectrum to enhance the recognition rate. The DWT-Dual subband Frequency domain Feature Extraction (DDFFE) includes the combination of DWT, DFT and DCT for efficient extraction, translation and illumination of invariant features [24]. The DWT utilize the approximation coefficients along with the horizontal coefficients of 2-dimensional images. The DFT is applied to compensate the translation variance problem of DWT, which extracts the frequency characteristics of the image. The low frequency components present in the center of the DFT spectrum are extracted by the quadruple ellipse mask around spectrum center. The DFT includes the information of both magnitude and phase that is extracted separately. DFT is applied on the preprocessed image and the low frequency components at the corner of the image spectrum is shifted into the center of the spectrum.

4.5. Perturbed Quantization (PQ)

The Perturbed Quantization (PQ) steganography analyzes the special positions of the feature extraction [25]. The changes of the global, local and dual histogram features are extracted from the DCT coefficients. The PQ is applied to the double compressed JPEG image and its DCT coefficients may be changed after completing PQ embedding. The global histogram is developed from all DCT coefficients and it is referred as the first order statistic feature to reflect the overall distribution of DCT coefficients. The local histogram reveals the distribution of all DCT blocks. The dual histogram exposes the distribution of the distinct value in some local positions of all DCT blocks. All histogram features are calculated and combined to form the enhanced histogram features to improve the detection performance.

4.6. Non-Sampled Contourlet Transform (NSCT)

The Logarithmic Non-Sampled Contourlet Transform(NSCT) extracts the invariant features like strong edges, weak edges and noise in the image [26]. Through the extraction and recombination of these features, two types of components are produced such as illumination component and reflectance component. The low pass subband of the image and the low frequency part of strong edges are in-

cluded as the illumination component. The pathetic edges and high frequency part of strong edges are denoted as the reflectance component. The face image is polluted by the noise and the reflectance component is applied to remove such noise. The NSCT algorithm is include to effectively capture contour in the original image.

5. Machine Learning Based Classification Techniques

The steganalyst trains the classifier with increasing more complex cover model and large data set to achieve more accurate and robust detectors.

5.1. Ensemble Classifier

The Ensemble classifier allows the fast construction of steganography detector with improved detection accuracy [27]. To build a detector, the model for the cover source is selected for the detection of steganography. Such covers are represented in a lower dimensional feature space before training the classifier. The ensemble classifier includes many base learners that is trained on a set of cover and stego images. The concluding decision is made by aggregating the decisions of every individual base learners.

5.2. Ensemble Based Extreme Learning Machine (EN-ELM) Classifier

The Ensemble based Extreme Learning Machine (EN-ELM) algorithm is required, where the ensemble learning and cross validation are implanted into the training phase [28]. The ensemble is constructed with several predictors on the training set by various set of random parameters. The learning is started by partioning the entire training set into number of subsets. Each learner is trained with the reduced subset. The parameters of every predictor is updated according to particular conditions. The decision is made by the testing samples by majority voting scheme. After completion of training, all predictors present in the ensemble are stored on the basis of its norm in an increasing order. The first half of the ensemble is utilized for making the decisions through majority voting scheme. The class receives the highest vote is treated as the predicted label and the total vote received by the each class is computed.

5.3. Extreme Learning Machine (ELM) Classifier

The Extreme Learning Machine (ELM) [29] produces the best performance in multi-label classification of large dataset. It is applied for the Single hidden Layer Feed forward Neural networks (SLFN). The hidden node parameters are created randomly from the continuous sampling distribution and it is need not to be tuned. This technique reaches the smallest training error and smallest norm of output weights to produce better generalization performance. The minimized norm of output weight leads to maximize the distance of two different classes in the ELM feature space. The ELM implementation procedure includes the minimal norm least square method. The ELM provides a unified learning platform

with a large type of feature mappings that can be applied to the regression and multi class classification [30]. It utilizes the single output node and the class label that is closer to the output value is considered as the predicted class label of the input data. The solution of binary classification case is became a specific case of multiclass solution. If the ELM utilizes multi output nodes, the index of the output node with highest output value is chosen as the label for the input data. The ELM involves the reduced human intervention than Support Vector Machine (SVM). If the feature mapping is known to the user, only one parameter is required to specify the user.

5.4. Differential Evolution (DE) Based ELM Classifier

The Differential Evolution (DE) based ELM includes the cross validation accuracy as the performance indicator to determine the optimal ELM parameters [31]. The integration of spatial context information in the learning process produces an enhanced classification results. The hyper spectral images are categorized by high dimensional spectral features. Initially, the feature reduction is applied to reduce the dimensionality of the data. Then, the morphological operations are included for this feature. The mode selection issue associated with the ELM is addressed with the simple grid selection procedures. The required kernel matrix is calculated from the training samples.

5.5. Cognitive Ensemble ELM Classifier

The cognitive ensemble ELM classifier is based on the hinge loss function [32]. Here, the individual ELM classifier is established on the basis of hinge error loss function. The cognition is obtained by the weighted sum of individual classifiers through the enhancement of wining classifier. The performance of the ELM classifier is affected by the random choice of centers and widths. The Gaussian center is distributed in the entire range of input space. The cognition of the ensemble calculates the output of all classifiers and listed the correctly classified samples. The samples that are correctly classified repeatedly are denoted as winning samples. The misclassified samples by many classifier is referred as losing samples. Finally, the output is obtained by the weighted sum of all contributing classifiers for all samples.

5.6. Support Vector Machine (SVM) Classifier

The Support Vector Machine (SVM) classifier is a standard classifier of the machine learning algorithm for binary classification [33]. The optimal linear decision surface is found through the minimization of training feature vectors. The feature vectors are planned in the high dimensional feature space. The maximum margin hyperplane is established by the SVM that divides the different class feature vectors with maximum margin. If the margin between the vectors is high, then the classification performance is improved. The LIBSVM offers a penalty additional function for unbalanced class, which has 4 kernel functions. The kernel function helps to project the input vector in the high dimensional feature

space. Generally, the kernel functions are categorized as radial basis function, polynomial, linear and sigmoid. The LIBSVM utilizes the radial basis function as the kernel function, which non-linearly moves the input feature vector into high dimensional feature space.

The difference of the detection performance and the relationship of detection results of sub-classifiers are learned by the fusing SVM classifier [34]. It has three phases: training of sub-classifiers, training of fusing classifier and testing of fusion classifier. The extracted features are divided into various groups regarding the correlation of features. The fusion classifier is trained on the basis of the detection results. The detection accuracy of steganalysis is improved by increasing the classifiers.

5.7. Bayesian Ensemble Classifier

In Bayesian ensemble classifier, the Bayesian estimation method is incorporated with the ensemble classifier for the improvement of classification performance [35]. The extracted features are applied to train the various sub-classifiers. The training set has original images and stego images. The relevant features are extracted from each image to formulate a feature vector. A series of low dimensional classifiers are employed to avoid the classification in high dimensional space. The Fisher Linear Discriminate (FLD) classifier is trained by the sub vectors and its threshold is found by the minimal sum of false alarm and detection rate. The sub classifiers is denoted as FLD, which is trained with the feature vectors are integrated to make the optimized decisions by the Bayesian mechanism.

6. Results & Discussion

From this survey, it is evident that the existing VRML, SMQT, SIFT and AD preprocessing techniques has less probability to detect hidden data, increased computational complexity with reduced speed. The folding based median filter provides the better reduction of noise. Also, the LNSCT, DCT, Shannon entropy methods has slow processing speed and the complex regions are not extracted. The texture patterns are extracted by the symmetrical pattern based extraction method. Moreover, the ELM and SVM classifiers have increased number of feature vectors. The machine learning classifier efficiently classifies the labels in the steganography. The results of this survey is depicts in the Table 1. The overall process flow of the steganography is shown in the Figure 1. The median testing error for various stegmethod is shown in the Table 2 and its corresponding graphical representation is depicts in Figure 2. Likewise, the median testing error for various feature extraction method is represented in Table 3 and its graphical representation describes in Figure 3.

7. Conclusion and Future Work

In this paper, various techniques for preprocessing, feature extraction and classification of image steganography are surveyed. The existing preprocessing techniques have less probability to detect the hidden data and reduced speed of op-

Table 1. Information about different preprocessing, feature extraction and classification techniques.

Techniques	Author & Reference	Year	Description	Quality measurement	Advantages/Disadvantages
Preprocessing Techniques					
2-nd level Daubechies (db4) Discrete Wavelet Transform	Carvajal-Gamez, *et al* [13]	2013	The pixels are classified using threshold based on the standard deviation of the local complexity of the cover image. Three types of color spaces are used to provide the difference between cover images and stego images	1. Peak Signal to Noise Ratio (PSNR) 2. Mean Absolute Error (MAE) 3. Normalized Color Difference (NCD) 4. Cross-Correlation (CC) 5. Quality index (Q) 6. Hiding Capacity (HC)	*Advantage* 1. Efficient and feasible for adaptive steganography applications *Disadvantage* 1. Less probability to detect hidden data
Vector Rank M-type L (VRML)-filter	Gallegos-Funes, *et al.* [14]	2012	The impulsive noise detector is presented to enhance the properties of noise suppression. It combines L algorithm with the Rank M-type(RM) estimator	1. Peak Signal to Noise Ratio (PSNR) 2. Mean Absolute Error (MAE) 3. Mean Chromaticity Error (MCRE) 4. Normalized Color Difference (NCD)	*Advantage* 1. Better impulsive noise suppression *Disadvantage* 1. Increased computational complexity
Successive Mean Quantization Transform (SMQT)	Sajedi and Jamzad [15]	2010	The cover image is processed into two stages such as preprocessing and embedding. An automatic structural breakdown of information is achieved. The organization of the structure the data is revealed by removing gain and bias properties	1. Detection accuracy 2. Embedding capacity	*Advantage* 1. Enhanced image quality 2. Improved security *Disadvantage* 1. Detection is not reliable 2. Local enhancement is not detected easily
Quaternion Transform and Scale Invariant Feature Transform (SIFT)	Hussain, *et al.* [16]	2016	The textural features are extracted in both online and offline mode. In online, the large data sets are obtained from website and search engines. In offline, data sets are acquired from large stored database	1. Region Of Interest (ROI) 2. Reduction in number of regions 3. Reduction in SIFT features	*Advantage* 1. Improved accuracy 2. Increased efficiency *Disadvantage* 1. Reduced speed 2. The complex images are not considered
Anisotropic Diffusion (AD) technique	Abhishree, *et al.* [17]	2015	The successive diffusion is performed on the basis of more and more blurring image. the entire process is divided into preprocessing, feature extraction and feature selection	1. Variation in Pose 2. Illumination 3. Face expression	*Advantage* 1. Reduced testing time 2. High recognition rate *Disadvantage* 1. Not suitable for real time application 2. Low speed computational methods are used
Chirp Z-Transform (CZT) and Goertzel algorithm	Varadarajan, *et al.* [18]	2015	The input image is enhanced by applying CZT. The problem is optimized by improving the candidate solution with respect to their quality.	1. Average recognition rate 2. Number of selected features 3. testing time	*Advantage* 1. Optimal recognition rate *Disadvantage* 1. Image enhancement is not satisfied
Feature Extraction Techniques					
Logarithmic non-subsampled contourlet transform (LNSCT)	Farhat and Ghaemmaghami [20]	2015	The strong edges, weak edges and noise are extracted from the images. Every images are distributed into five subsets regarding the angle between light source direction and camera axis	1. Recognition rate 2. Equal Error Rate (EER)	*Advantage* 1. Robust extraction of features *Disadvantage* 1. Slower computation time 2. Increased computational complexity
Discrete Cosine Transform (DCT)	Karimi, *et al.* [21]	2015	The original features are extended as the extended version to extract the more complicated relation among the coefficients. The ANOVA F-test is applied to compare the mean of sampled data.	1. Median testing error 2. Embedding rate	*Advantage* 1. Superior performance 2. The hidden data can be extracted with low embedding rate *Disadvantage* 1. Increased dimensionality

Continued

Shannon Entropy of 2 Dimensional (2D) Gabor wavelet	Song, *et al.*[22]	2016	The image is filtered by 2D Gabor wavelet then the features are extracted. This wavelet can effectively captures the image texture and edge properties from different scale and orientations.	1. Detection error rate 2. Entropy value	*Advantage* 1. Effectively capturing the changes in image texture *Disadvantage* 1. Reduced detection accuracy
Discrete Fourier Transform (DFT) and Discrete Cosine Transform (DCT)	Deepa, *et al.* [23]	2012	The transformation of facial images in frequency domain used to reduce the image redundancy. Five images are randomly selected for training and another five images are selected for testing.	1. Recognition rate 2. Training time 3. Testing time 4. Euclidean distance	*Advantage* 1. Dimensionality reduction 2. Higher recognition rate *Disadvantage* 1. Reduced sustainability 2. Simple classifier is used
Enhanced histogram features method	Song, *et al.* [25]	2015	The Perturbed Quantization (PQ) is applied for double compression JPEG images. The global, local and dual histogram features of DCT coefficients and its differences are calculated.	1. True positive rate 2. False positive rate 3. Detection accuracy	*Advantage* 1. High detection accuracy *Disadvantage* 1. Constrained for complex image regions

Machine Learning Based Classification Techniques

|					
Ensemble Classifier	Kodovsky, *et al.* [27]	2012	The ensemble classifier provides the fast construction of the steganography detector. The steganalyst are allowed to work on the high dimensional feature space with large dataset.	1. Detection error 2. Median (MED) 3. Median Absolute Deviation (MAD)	*Advantage* 1. Improved accuracy *Disadvantage* 1. Increased computational complexity
Ensemble based Extreme Learning Machine (EN-ELM)	Liu and Wang [28]	2010	The decisions are made by the cross validation scheme. The Discrete Cosine Transform (DCT) reduces the dimensionality.	1. Classification accuracy 2. testing accuracy 3. Training time	*Advantage* 1. Alleviate overfitting 2. Higher testing accuracy *Disadvantage* 1. Increased training time 2. Increased computational burden
Extreme Learning Machine (ELM) classifier	Huang, *et al.* [29]	2010	The ELM is based on the Karush-Kuhn-Tucker (KKT) theorem. All training data are linearly separable in the ELM feature space. ELM is less sensitive to learning parameters.	1. Testing rate 2. Training time 3. Testing deviation	*Advantage* 1. Easily implemented 2. Minimized testing error *Disadvantage* 1. Average testing accuracy
Differential Evolution based Extreme Learning Machine (DE-ELM)	Bazi, *et al.* [31]	2014	An automatic solution based Differential Evolution (DE) algorithm is developed in associated with the ELM classifier. The Principal Component Analysis (PCA) is applied to reduce the dimensionality of the data.	1. Overall (OA) standard deviation 2. Average (AA) standard deviation 3. Sensitivity	*Advantage* 1. Faster solution *Disadvantage* 1. Reduced classification accuracy
Support Vector Machine (SVM) classifier	Shankar, *et al* [36]	2012	The block dependency features (inter and intra features) are used for the classification of steganography.	1. classification percentage 2. Embedding percentage	*Advantage* 1. Faster solution *Disadvantage* 1. Message length is not detected
Hinge loss function based cognitive ensemble of Extreme Learning Machine (ELM)	Sachnev, *et al.* [32]	2015	The classifier performance is depended on the choice of classifier and weightage of each classifier. The quality of extracted features defines the performance of binary classifier.	1. Number of hidden neurons 2. Testing efficiency	*Advantage* 1. Improved classification performance 2. Best testing efficiency *Disadvantage* 1. Geometric features are not recognized
Bayesian Ensemble Classifier	Li, *et al.* [35]	2013	The high dimensional feature vector is calculated from each JPEG image in a training set. The feature vectors are trained by the sub-classifier and it is integrated to make final decisions.	1. Average computation time 2. detection percentage	*Advantage* 1. Low computational complexity *Disadvantage* 1. Increased number of feature vector 2. Required large training set
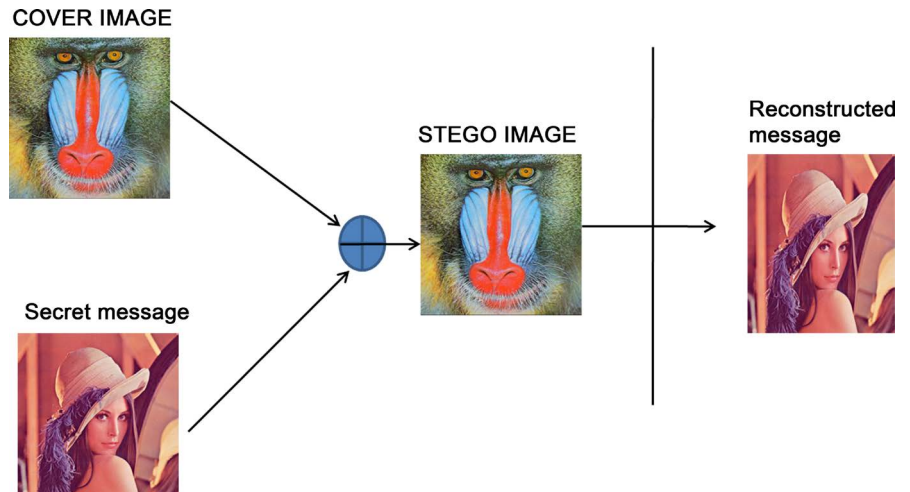
Figure 1. Overall process flow of steganography.

Table 2. Median testing error for various steg method.

Steg method	$F_f 1$ P = 1	$F_f 2$ P = 1	$F_f 3$ P = 1
F5	0.0275	0.03125	0.02375
JSteg	0.18375	0.19	0.175
MB1	0.0575	0.055	0.0425
nsF5	0.16675	0.1675	0.1475
YASS	0.1175	0.1575	0.1325
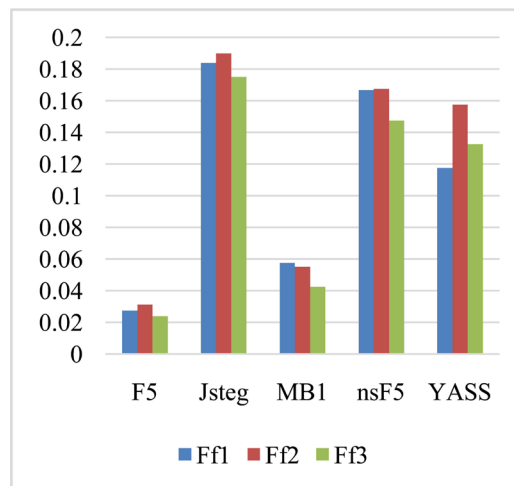
Figure 2. FMedian testing error (PE) for various Stego methods.

Table 3. Median testing error for various feature extraction method.

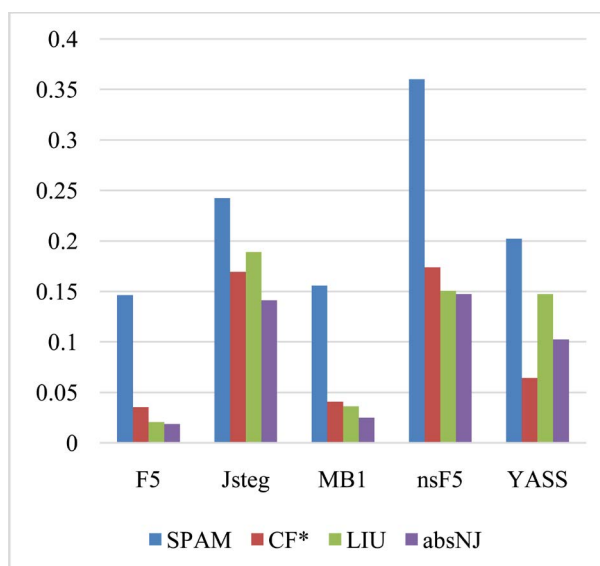| Steg method	SPAM [37]	CF * [27]	LIU [38]	absNJ [21]
F5	0.14625	0.03525	0.02075	0.01875
JSteg	0.24225	0.1695	0.189	0.141
MB1	0.15575	0.04075	0.03625	0.025
nsF5	0.36025	0.17375	0.1505	0.1475
YASS	0.20225	0.06425	0.1475	0.1025

Figure 3. Median testing error (PE) for various Feature extraction methods.

eration. The traditional feature extraction techniques do not provide the efficient detection of stego images and the complexity of the message retrieval is also increased. The previous classification methods are very difficult to understand and do not provide the exact classification result. Some of the disadvantages of these classification algorithms are computational complexity, large computational time and requires large training set. To overcome the above mentioned drawbacks, the folded version of mean filter will be developed as the preprocessing technique for smoothening the image. The symmetrical pattern based feature extraction for effectively extracting the large number of features from the image and the integrated machine learning classification method for accurate classification of steganography methods will be implemented in future.

References

[1] Lerch-Hostalot, D. and Megías, D. (2016) Unsupervised Steganalysis Based on Artificial Training Sets. *Engineering Applications of Artificial Intelligence*, **50**, 45-59. https://doi.org/10.1016/j.engappai.2015.12.013

[2] Wu, A., Feng, G., Zhang, X. and Ren, Y. (2016) Unbalanced JPEG Image Steganalysis via Multiview Data Match. *Journal of Visual Communication and Image Representation*, **34**, 103-107. https://doi.org/10.1016/j.jvcir.2015.10.013

[3] Sajedi, H. (2016) Steganalysis Based on Steganography Pattern Discovery. *Journal of Information Security and Applications*, **30**, 3-14. https://doi.org/10.1016/j.jisa.2016.04.001

[4] Kanan, H.R. and Nazeri, B. (2014) A Novel Image Steganography Scheme with High Embedding Capacity and Tunable Visual Image Quality Based on a Genetic Algorithm. *Expert Systems with Applications*, **41**, 6123-6130. https://doi.org/10.1016/j.eswa.2014.04.022

[5] Djebbar, F., Ayad, B., Meraim, K.A. and Hamam, H. (2012) Comparative Study of Digital Audio Steganography Techniques. *EURASIP Journal on Audio, Speech, and Music Processing*, **2012**, 1-16. https://doi.org/10.1186/1687-4722-2012-25

[6] Mandal, P.C. (2012) An Extensive Review of Current Trends in Steganalysis. *Inter-*

national Journal of Advanced Research in Computer Engineering & Technology, **1**, 215.

[7] Cho, S., Cha, B.-H., Gawecki, M. and Kuo, C.-C.J. (2013) Block-Based Image Steganalysis: Algorithm and Performance Evaluation. *Journal of Visual Communication and Image Representation*, **24**, 846-856. https://doi.org/10.1016/j.jvcir.2013.05.007

[8] Goljan, M., Fridrich, J. and Cogranne, R. (2014) Rich Model for Steganalysis of Color Images. 2014 *IEEE International Workshop on Information Forensics and Security* (*WIFS*), 185-190. https://doi.org/10.1109/WIFS.2014.7084325

[9] Guo, J., Guo, Y., Li, L. and Li, M. (2014) A Universal JPEG Image Steganalysis Method Based on Collaborative Representation. *International Conference on Security, Pattern Analysis, and Cybernetics* (*SPAC*), 285-289.
https://doi.org/10.1109/spac.2014.6982700

[10] Lerch-Hostalot, D. and Megías, D. (2013) LSB Matching Steganalysis Based on Patterns of Pixel Differences and Random Embedding. *Computers & Security*, **32**, 192-206.

[11] Xia, Z., Wang, X., Sun, X., Liu, Q. and Xiong, N. (2016) Steganalysis of LSB Matching Using Differences between Nonadjacent Pixels. *Multimedia Tools and Applications*, **75**, 1947-1962. https://doi.org/10.1007/s11042-014-2381-8

[12] Aneesh, M., Masand, A.A. and Manikantan, K. (2012) Optimal Feature Selection Based on Image Pre-Processing Using Accelerated Binary Particle Swarm Optimization for Enhanced Face Recognition. *Procedia Engineering*, **30**, 750-758.

[13] Carvajal-Gamez, B.E., Gallegos-Funes, F.J. and Rosales-Silva, A.J. (2013) Color Local Complexity Estimation Based Steganographic (CLCES) Method. *Expert Systems with Applications*, **40**, 1132-1142.

[14] Gallegos-Funes, F.J., Rosales-Silva, A.J. and Toledo-Lopez, A. (2012) Multichannel Image Processing by Using the Rank M-Type L-Filter. *Journal of Visual Communication and Image Representation*, **23**, 323-330.

[15] Sajedi, H. and Jamzad, M. (2010) BSS: Boosted Steganography Scheme with Cover Image Preprocessing. *Expert systems with Applications*, **37**, 7703-7710.

[16] Hussain, C.A., Rao, D.V. and Masthani, S.A. (2016) Robust Pre-Processing Technique Based on Saliency Detection for Content Based Image Retrieval Systems. *Procedia Computer Science*, **85**, 571-580.

[17] Abhishree, T., Latha, J., Manikantan, K. and Ramachandran, S. (2015) Face Recognition Using Gabor Filter Based Feature Extraction with Anisotropic Diffusion as a Pre-Processing Technique. *Procedia Computer Science*, **45**, 312-321.

[18] Varadarajan, K., Suhasini, P., Manikantan, K. and Ramachandran, S. (2015) Face Recognition Using Block Based Feature Extraction with CZT and Goertzel-Algorithm as a Preprocessing Technique. *Procedia Computer Science*, **46**, 1458-1467.

[19] Lavangnananda, K. and Waiwing, S. (2015) Effectiveness of Different Preprocessing Techniques on Classification of Various Lengths of Control Charts Patterns. *Procedia Computer Science*, **69**, 44-54.

[20] Farhat, F. and Ghaemmaghami, S. (2015) Towards Blind Detection of Low-Rate Spatial Embedding in Image Steganalysis. *IET Image Processing*, **9**, 31-42.
https://doi.org/10.1049/iet-ipr.2013.0877

[21] Karimi, H., Shayesteh, M.G. and Akhaee, M.A. (2015) Steganalysis of JPEG Images Using Enhanced Neighbouring Joint Density Features. *IET Image Processing*, **9**, 545-552. https://doi.org/10.1049/iet-ipr.2013.0823

[22] Song, X., Li, Z., Chen, L. and Liu, J. (2016) Entropy Feature Based on 2D Gabor Wavelets for JPEG Steganalysis. In: Wang, G., Ray, I., Alcaraz Calero, J. and Tham-

pi, S., Eds., *Security*, *Privacy and Anonymity in Computation, Communication and Storage. SpaCCS 2016. Lecture Notes in Computer Science*, Vol. 10067, Springer, Cham, 59-72. https://doi.org/10.1007/978-3-319-49145-5_7

[23] Deepa, G., Keerthi, R., Meghana, N. and Manikantan, K. (2012) Face Recognition Using Spectrum-Based Feature Extraction. *Applied Soft Computing*, **12**, 2913-2923.

[24] Krisshna, N.A., Deepak, V.K., Manikantan, K. and Ramachandran, S. (2014) Face Recognition Using Transform Domain Feature Extraction and PSO-Based Feature Selection. *Applied Soft Computing*, **22**, 141-161.

[25] Song, X., Liu, F., Luo, X., Lu, J. and Zhang, Y. (2015) Steganalysis of Perturbed Quantization Steganography Based on the Enhanced Histogram Features. *Multimedia Tools and Applications*, **74**, 11045-11071.
https://doi.org/10.1007/s11042-014-2217-6

[26] Xie, X., Lai, J. and Zheng, W.-S. (2010) Extraction of Illumination Invariant Facial Features from a Single Image Using Nonsubsampled Contourlet Transform. *Pattern Recognition*, **43**, 4177-4189.

[27] Kodovsky, J., Fridrich, J. and Holub, V. (2012) Ensemble Classifiers for Steganalysis of Digital Media. *IEEE Transactions on Information Forensics and Security*, **7**, 432-444. https://doi.org/10.1109/TIFS.2011.2175919

[28] Liu, N. and Wang, H. (2010) Ensemble Based Extreme Learning Machine. *IEEE Signal Processing Letters*, **17**, 754-757. https://doi.org/10.1109/LSP.2010.2053356

[29] Huang, G.-B., Ding, X. and Zhou, H. (2010) Optimization Method Based Extreme Learning Machine for Classification. *Neurocomputing*, **74**, 155-163.

[30] Huang, G.-B., Zhou, H., Ding, X. and Zhang, R. (2012) Extreme Learning Machine for Regression and Multiclass Classification. *IEEE Transactions on Systems*, *Man*, *and Cybernetics*, *Part B* (*Cybernetics*), **42**, 513-529.
https://doi.org/10.1109/TSMCB.2011.2168604

[31] Bazi, Y., Alajlan, N., Melgani, F., AlHichri, H., Malek, S. and Yager, R.R. (2014) Differential Evolution Extreme Learning Machine for the Classification of Hyperspectral Images. *IEEE Geoscience and Remote Sensing Letters*, **11**, 1066-1070.
https://doi.org/10.1109/LGRS.2013.2286078

[32] Sachnev, V., Ramasamy, S., Sundaram, S., Kim, H.J. and Hwang, H.J. (2015) A Cognitive Ensemble of Extreme Learning Machines for Steganalysis Based on Risk-Sensitive Hinge Loss Function. *Cognitive Computation*, **7**, 103-110.
https://doi.org/10.1007/s12559-014-9268-x

[33] Choi, J.-H., Lee, H.-Y. and Lee, H.-K. (2013) Color Laser Printer Forensic Based on Noisy Feature and Support Vector Machine Classifier. *Multimedia Tools and Applications*, **67**, 363-382. https://doi.org/10.1007/s11042-011-0835-9

[34] Liu, P., Liu, F., Yang, C. and Song, X. (2015) Improving Steganalysis by Fusing SVM Classifiers for JPEG Images. *International Conference on Computer Science and Mechanical Automation* (*CSMA*), Hangzhou, 23-25 October 2015, 185-190.
https://doi.org/10.1109/csma.2015.44

[35] Li, F., Zhang, X., Chen, B. and Feng, G. (2013) JPEG Steganalysis with High-Dimensional Features and Bayesian Ensemble Classifier. *IEEE Signal Processing Letters*, **20**, 233-236. https://doi.org/10.1109/LSP.2013.2240385

[36] Shankar, D.D., Gireeshkumar, T., Praveen, K., Jithin, R. and Raj, A.S. (2012) Block Dependency Feature Based Classification Scheme for Uncalibrated Image Steganalysis. In: Kannan, R. and Andres, F., Eds., *Data Engineering and Management. Lecture Notes in Computer Science*, Vol. 6411, Springer, Berlin, Heidelberg, 189-195.
https://doi.org/10.1007/978-3-642-27872-3_28

[37] Pevny, T., Bas, P. and Fridrich, J. (2010) Steganalysis by Subtractive Pixel Adjacency matrix. *IEEE Transactions on Information Forensics and Security*, **5**, 215-224. https://doi.org/10.1109/TIFS.2010.2045842

[38] Liu, Q., Sung, A.H. and Qiao, M. (2009) Improved Detection and Evaluation for JPEG Steganalysis. *Proceedings of the* 17*th ACM International Conference on Multimedia*, Beijing, 19-24 October 2009, 873-876. https://doi.org/10.1145/1631272.1631436