1

A Survey of Data Mining Techniques for Steganalysis

Farid Ghareh Mohammadi and Mohammad Saniee Abadeh
Faculty of Electrical and Computer Engineering, Tarbiat Modares University
Iran

1. Introduction

The skill of observing the invisible embedded messages in images, audio, video, text as multimedia and protocols called Steganalysis. An efficient steganalysis method should determine the existence of implanted messages and stego digital image and present some results about the used steganographic algorithm. The challenging problem of this study is a massive quantity of stego hosts to learn valuable knowledge. In this paper, we propose to study several current data mining approaches on steganalysis of images, audio, video, text and protocol. The main aim of this survey is to present the efficiency of using data mining techniques in steganalysis in comparison to the model based steganalysis approaches.

The skill and knowledge of identifying secret message concealed by steganography approach is called Steganalysis. Steganalysis is the skill of detecting the existence of the concealed data in digital images, texts, audios, videos, protocols (Nissar & Mir, 2010). Steganalysis can be categorized into two groups: (a) static and (b) dynamic. Guesstimate some parameter(s) of the embedded algorithm or the secret message is the target of dynamic steganalysis, identifies the existence/non-existence of a secret message is the aim of static steganalysis; in other word these two groups have additional definitions as below:

Static steganalysis: discovering the existence/non-existence of a concealed message in a stego file and recognizing the stego embedded algorithm.

Dynamic steganalysis: guesstimating the implanted message length, position(s) of the concealed message, the secret key used in implanting, some parameters of the stego implanting algorithm and take out the concealed message.

An operation that takes out a number of novel nontrivial patterns included in huge records or databases is called Data Mining. Data Mining includes the utilization of complicated data analysis, which means to find out earlier unidentified, forensic patterns and associations in myriad data set. Therefore, data mining involves analysis, forecast, gathering and organizing data. The aim of data mining is to realize hidden models, unforeseen styles or data, exploiting a mixture of methods from machine learning to bio-inspired meta-heuristic algorithms. Multiple main phases of data mining operation consist of (1) Scope perceptive; (2) Data choice; (3) Data pre-processing, clear out and training; (4) Realizing patterns; (5) Explanation; and (6) Exposure and utilizing revealed facts (Bhatt & Kankanhalli, 2011).

In this study, we will present the survey of using data mining techniques on steganalysis, with intention to establish the significant data mining methods such as classification, clustering and other data mining methods that have been applied for steganalysis purposes. We will review numerous classification methods containing Decision Tree (DT), Support Vector Machines (SVM), Naive Bayes (NB), K-nearest neighbour (KNN), Neural Network (NN) and also a major variety of clustering methods contain K-means, agglomeration and random algorithms.

The rest of this book chapter is organized as follows: In Section 2, we will review the general classification of data mining techniques on steganalysis. Section 3 discusses about applied data mining techniques in brief. In Section 4, we will discuss the applied data mining techniques for image steganalysis. We will study data mining techniques for steganalysis over audio, video, text and protocol domains in section 5. In section 6, we will summarize several previous investigations about the application of data mining techniques for steganalysis using several well-presented figures and tables. Section 7 concludes this book chapter.

2. General categorization of data mining techniques on steganalysis

The aim of this section is to present an immediate wide spread picture of the importance of mixing data mining techniques. By using data mining algorithms we detect secret and hidden concealed message through steganalysis. We have several kinds of data types assigned as Domain that should be considered such as: Image, Audio, Text, Video and Protocol. This classification is based on data mining techniques extended on steganalysis in this domain which are used to detect the presence of embedded messages in stego images by steganography techniques. Under each of them, the domains are further sub-divided into data mining techniques. The whole hierarchy of the categorization is shown in fig 1.

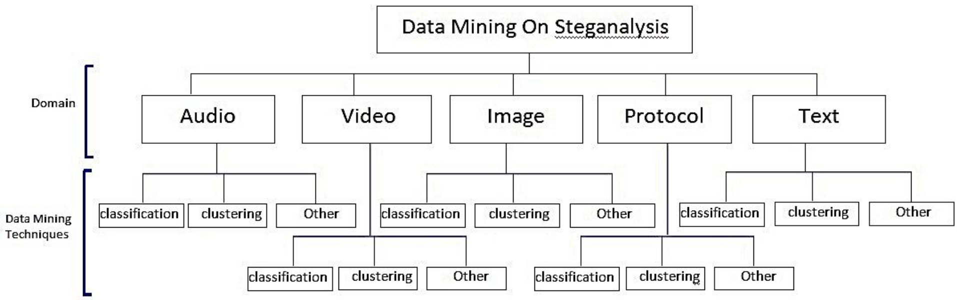

Fig. 1. The hierarchy of the General Categorization of Data Mining techniques on steganalysis.

These sub-domains (data mining techniques) are sub-divided into approaches which are applied in:

- Classification, which has been divided into neural network (NN), k-nearest neighbour (KNN), Support Vector Machine (SVM), Decision Tree (DT), Naive Bayes (NB) approaches. This category has itself a hierarchy which is shown in Fig. 2.

- Clustering, which has been divided into K-means, agglomeration and random algorithms.
- Other data mining tasks, such as regression approaches and etc.

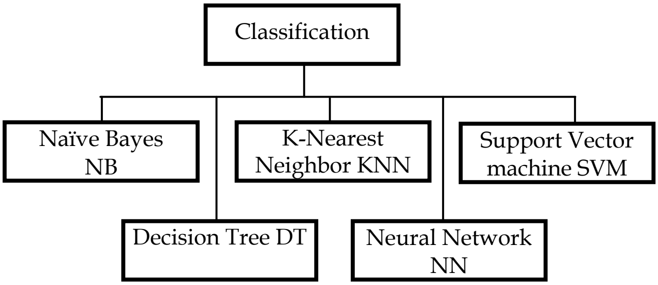

Fig. 2. The hierarchy of the category classification approach.

3. Overview of data mining techniques

As we aim to provide the general data mining techniques on steganalysis scheme, some definitions of applied techniques, need to be introduced:

Naive Bayes Classification (NB): A Naive Bayes classifier is a simple probabilistic classifier based on applying Bayes' theorem with strong independence assumptions. A more descriptive term for the underlying probability model would be an independent feature model. (Kaipa & Robila, 2010).

Decision Tree classification (DT): A Decision Tree, more properly a classification tree, is mostly used to learn a classification model which predicts the value of a dependent attribute (variable) given the values of the independent (input) attributes (variables). This solves a problem known as supervised classification since the dependent attribute and the number of classes (values) that it may have are given. (Kaipa&Robila, 2010). In decision tree structures, leaves signify classifications and branches signify a combination of characteristics that direct to those classifications (Duda et al, 2001).

Support Vector Machine (SVM) Classification: The aim of SVMs is to learn a model which forecasts class tag of cases in the testing set. This classification algorithm is one of the most robust classifiers for two-class classification. SVM can manage both linear and nonlinear classification problems. For linear discrete problems, SVM classifiers purely explore for a hyper-plane that distinguishes negative and positive instances (Cortes & Vapnik, 1995), (Vapnik, 1998), (Boser et al, 1992).

In the terminology of SVM literature, an attribute is a forecaster variable and a feature is an attribute which is applied to describe the hyper-plane. Feature selection is the operation of selecting the most appropriate attribute. SVM method is strongly correlated to neural networks. In fact, Support Vector Machine (SVM) methods have a close relation to traditional N-layer perceptron neural networks (Hernandez et al, 2008).

K-Nearest Neighbour classification (KNN): One kind of supervised classification techniques is called K-nearest neighbour classifier. KNN presented by Devijver and Kittler (Devijver &

Kittler, 1982), commonly use the Euclidean distance measure. For each row of the test set, the k nearest (in Euclidean distance) training set vectors are found, and the classification is decided by majority vote, with ties broken at random. If there are ties for the kth nearest vector, all candidates are included in the vote.

Neural Network classification (NN): One kind of classification techniques is called a neural network classifier. The important problem in a neural network is that convergence is not fast. Practically, this is the most important restriction of neural network applications, because data hiding method is not a linear method, if we only employ linear classification technique to categorize images. The neural network has an admirable facility to simulate any nonlinear correlation. Therefore, it has been used to categorize images. Neural network draws on three levels: input level, hidden level and output level (Liu et al, 2003).

Agglomerative Clustering: Agglomerative hierarchical clustering is a bottom-up clustering approach where clusters have sub-clusters, which in turn have sub-clusters, etc. The classic example of this is species taxonomy. Gene expression data might also demonstrate this hierarchical quality (e.g. Neurotransmitter gene families). Agglomerative hierarchical clustering begins with every single object (gene or sample) in a single cluster. This algorithm merges the closest pair of clusters in each iteration. This merging is accomplished by satisfying some similarity criteria, until all of the data are in a single cluster (Ker & Pevny, 2011).

4. Data mining techniques on steganalysis over the image

In this section we present data mining techniques in image domain that divided into three parts. In the first part, we introduce classification approaches in image steganalysis such as: support vector machine (SVM), k nearest neighbour (KNN), neural network (NN), naive Bayes (NB) and decision tree (DT). In the second part, we present clustering approaches in image steganalysis such as: K-means, random clustering, agglomerative and other data mining methods such as: Regression.

4.1 Classification techniques used on steganalysis

4.1.1 Support Vector Machine Classification (SVM)

Support vector machines (SVMs) have been broadly used as a categorizer device with an enormous deal of achievement from steganalysis to categorization of the presents of stego grams. The SVMs present supervised ML (machine learning) methods to generate a model which forecasts the goal values of the examination data specified only the experiment data attributes and discover the most favourable discrete hyper spheres which split the test data into two or N-groups for classification. A four-process sampling technique used to take out the image facial appearance (characteristic) for steganalysis. Applying a two-class SVM classifier, Lou and his colleagues are capable to make distinction cover images from the stego-images with an accuracy of 98.51%. Applying N-class SVM classifier, an estimator which is capable of detecting the secret key with an accuracy of 99.77% is created. See (Lou et al., 2011) for an example of SVM as the steganalysis technique.

A well-organized universal steganalysis plan is suggested by Lou and his colleagues to distinguish clear images from stego images in frequency and spatial domains (Lou et al, 2009). The suggested plan is executed in four phases: feature databases set, features mining, categorized from learning and length calculating approximately. The feature of databases would be explained in the first phase and the numerical features of the learning sets would be taken out in the following phase. After that, a number of two-class SVM based models would be learned by the mined features and the length of distrustful images would be recognized by the evaluation strategy in the final phase. The aim of SVMs was to discover the most favourable discriminate hyper sphere which shares the mined features into two collections in the utmost scope.

In (Joo et al, 2010), Joo and his colleagues suggest a steganalysis plan to disclose the presence of the concealed message like as the encoded data. The goal of this paper is to demonstrate that a distrustful image was customized by information concealing methods. Because the actual image has a high correlation amongst the adjacent pixels, the message put into modifies the pixel value and the diversity among the pixels. Thus, it builds the chunk effect and the correlation with the neighbouring pixels is broken. So, the diversity histogram of the 1- line cropped altered-image is different to that of the primary changed-image. Blind features suggested are the space measures among the diversity histogram of the main and the cut image. The presentation of the suggested steganalysis is verified throughout a huge and different image set. The Support Vector Machine (SVM) has used two categories that are normal and changed images. To identify that a distrustful image consists of an unseen message or not, the LIBSVM was used (Chang & Lin, 2001) as a strong two-class categorizer. All the images were equally shared non-overlap testing and learning subsets. The SVM categorizer was trained by the characteristic values of 1000 normal and 4000 changed-images.

In (Hernandez et al, 2008), numerical moment of wavelet feature function and neural network (NN) method is offered for a progress to the steganalysis as a classifier. Preceding research have declared that this steganalysis scheme has an excellent performance in the discovery of stego-image produced by diverse steganography techniques, but it has troubles to the steganography depend on bit plane complex segmentation (BPCS), this steganalysis has illustrated a little discovery speed of stego-image, produced by BPCS steganography, as a result, suggested effort offered to apply a support vector machine (SVM) as classifier instead of ANN. As a result, when SVM is applied instead to ANN investigation results descriptive significantly enhance of BPCS recognition rate (at least 20%).

In (Sajedi & Jamzad, 2008), the authors proposed a novel universal method for steganalysis, which utilizes numerical moments of contourlet coefficients as characteristics for examination. An SVM based non-linear classifier is applied to categorize stego and cover images. The efficiency of the suggested technique is determined by extensive tentative analysis. The suggested steganalysis technique is compared with two steganalyzers and versus usual steganography techniques. The results declared the prior performance of suggested technique.

In (Marvel et al, 2008), Marvel and his colleagues suggested blend N-rate-specific. The rate-specific categorizers SVM parameter (e.g., Far from every model over-plane) is utilized as entrance to the blending categorizer. Marvel and his colleagues determined the act of this practice and compare it with the universal categorizer and the rate-specific categorizer.

In (Mehrabiet al, 2007), the authors proposed a novel image steganalysis system which was depended on numerical moments of the histogram of N-level wavelet sub bands in frequency scope. Different frequencies of histogram have different sensitivity to various data embedding. The first three statistical moments of each band are selected to form a 78-dimensional feature vector for steganalysis. An SVM based classifier is then used to discriminate between stego and clear images.

In (Zou et al, 2006), the authors have suggested steganalysis scheme which depends on a 2-D Markov chain thresholded forecast-error image. Image pixels are forecasted with their adjacenting pixels, and the forecast-error image is produced by decreasing the calculated value of the pixel value and then thresholded with a predefined threshold. The practical conversion matrixes of Markov chains beside the vertical, horizontal, and crosswise instructions assist as structures for steganalysis. For feature ordering, the SVM with whether linear cores and also non-linear cores are utilized as categorizer. The non-linear as one of SVM methods executes considerably more superior than the linear SVM for their suggested structures. The trial outcomes have verified that the recommended steganalysis characteristics are more operative than that offered in (Sullivan et al, 2005) for proposed spread spectrum steganography techniques and more operative than the wavelet-base structures suggested in (Lyu et al, 2002) for LSB steganography methods.

Chen and his colleagues presented a novel universal steganalysis technique depends on numerical moments consequent from either JPEG 2-Dand an image 2-Darray. Furthermore, the head direction histogram, the second direction histogram is measured. The support vector machine (SVM) is applied in (Chen et al, 2006) as a classifier. The SVM used (Chen et al, 2006) as classifier instead of NN techniques with regard to its comparable act and more effective computation.

In (Liu & Sung, 2007), Liu & Sung presented a structure of steganalysis for LSB based steganography algorithms in blend black and white images. Their method depended on feature extracting and Neuro-fuzzy deduction schemes. Four kinds of features mined, based on DENFIS feature choice applied, and SVM-RFE applied to get better detection accuracy.

4.1.2 Naive Base and Decision Tree Classification (NB & DT)

In (Kaipa & Robila, 2010), suggested to plan and operate a scheme capable of categorizing the images into clear and stego images by typical shape classification methods like as Naive Bayes (NB) and Decision Trees (DT). Experiments have shown on a huge file set of images to specify the classification technique that executes the best comparing classification fault and achievement degrees in every item. Kaipa and Robila have used Weka, a software program application on data mining scope advanced in Java for suggested destination. Kaipa and Robila have also advanced a program by Weka Java library aimed at filling the files of the Images and categorize the images into clear images and stego-images.

In (Liu et al., 2006), the authors presented various numerical design detection techniques which are used to train and categorize the characteristic sets. Comparison of suggested technique and another, shows suggested technique is extremely efficient. It is vastly effectual for color image steganalysis. It is also fit for black and white color steganalysis in the little image density and intricacy scope.

In (Benton & Chu, 2005), the authors presented using decision trees (DT) and neural networks (NN) to categorize the images into stego and clear images. Ryan and Henry investigated by applying decision trees (DT) for discovering message concealed in the LSBP of an image and compare their outcomes to those achievements applying N-layered feed frontward NN.

In (Berg et al., 2003), Berg and his colleagues showed the possibility of utilizing a data mining and machine learning (DM/ML) method to robotically construct as steganalysis methods. For either compression-based (JPEG) or content-based (GIF) an image form, DM/ML methods are so magnificently capable to separate clean files from stego-ones. The suggested method is depending on an image figure of the media form that builds obvious completion of the structures that can be applied for steganographic implanting. They have revealed how this could be blended with a group of features chosen for the picture depicts. In suggested effort, that contains value happening chances, and either conditional or unconditional entropies. These structures were positively applied, for each JEPG and GIF types, and by the use a number of diverse training processes, to discovery concealed message carrying out files. They find out that the three training methods attempted consist of artificial neural network (ANN), decision trees (DT) and naive Bayes (NB) classifiers accomplished suggestively more improved than arbitrary estimating in a diversity of conditions.

4.1.3 K-Nearest Neighbour Classification (KNN)

Presented an approach for steganalysis scheme depends on a group of 193 features with two major aims: first, demonstrates adequate amount of images of operative training of a categorizer in they got upper-dimensional space, and second, utilizes feature selection to select greatest related structures for the favoured categorization. Dimensionality reduction is achieved applying a frontward selection and decreases the primary 193 feature fixed by element of 13, using totally similar performance. In (Miche et al, 2007) two diverse kinds of categorizers have mostly been applied: the first one, K-nearest neighbours (KNN), for its totally efficient presentation even in upper dimensional space, but totally, since it is very speedy. SVM approach was similarly selected because it is amongst the classifiers presented the greatest outcomes. The main disadvantage is of process the calculating time.

In (Miche et al, 2006), the authors presented an approach to choice structures earlier learning and test a classifier depend on Support Vector Machines (SVM) approach. In suggested work 23 features provided by Fridrich were evaluated. K-Nearest-Neighbours (KNN) is a feature grading that is achieved applying a quick classifier mixed with a forward selection. The product of the feature selection is subsequently verified on support vector machine (SVM) to choose the optimum amount of features. Suggested technique is tried by the Outguess steganographic approach and 14 features are chosen while supporting the equal classification performances. Outcomes approve that the chosen features are well-organized for an extensive variety of implanting rates. The similar approach is used for F5 and Steghide method to conceive if feature selection is capable on suggested process.

4.1.4 Neural Network Classification (NN)

In (Shaohui et al, 2003), the authors presented a novel technique based on neural network (NN) to get numerical features of images to detect the essential concealed data. Shaohui and his colleagues discovered that neural network (NN) approach cannot be applied to linear problems and is more practical to nonlinear problems, so in their suggested paper Shaohui and his colleagues utilize BP neural network (NN) to simulate and train images. Suggested BP neural network (NN) applied a three layer NN consists of an input layer, hidden layer and output layer. This technique discovers statistically indicates after original images has been concealed message, then utilizing the ability of estimation of neural network (NN)for demonstrating either an image is non-stego or stego image.

A blind image steganalysis scheme is proposed, in which feature is consists of the numerical moments of characteristic functions of the test image, the prediction-error image and their wavelet sub bands. The approach of categorizer is another main factor in steganalysis. In (Shi et al, 2005), the feed forward NN with BP learning process is utilized as the categorizer. It is the strong training ability influenced by using the NN will overtake the linear categorizers. In the examining step, the non-linear NN outputs offers lower classification rate than the linear outputs.

In (Liul et al, 2004), the authors presented actual features through means of quality analysis from clear images and stego images, after that, applying neural network(NN) approach as a separator to differentiate non-stego-images and stego-images. Liul and his colleagues utilized BP neural network (NN) to approve their approach. The first phase is to learn and test neural network (NN) to acquire network parameters. In spite these parameters, they could simulate the outcomes. This BP neural network (NN) applies three layers: input one, hidden one and output one. In neural network (NN), they adjust a number of characteristics as the certain nerve cells of the input layer.

In (kobsi & merouani, 2007), the authors presented methods depend on Neural Network (NN) that are acceptable to distinguish its efficiency for steganalysis.

In (Holoska et al., 2010), the authors suggested a blind steganalysis method which depends on a universal neural network (NN) approach and matches it to Stegdetect – a kind of tool that uses a linear classification device.

In (Sabeti et al, 2010), the authors presented Five different N-level perceptron neural network (NN) approaches trained to discover diverse layers of implanting. Every image is served to all systems and electing scheme classifies the image as either cover images or stego images. The operation outcomes show 88.6% achieved in the true classification of the test images that involved in at least 20% embedding rate and the rest 14% success in the true classification of the test images involved at most 20% imbedding rate. Every system in the categorizer was independently trained with feature groups mined from 150 stego-images and 150 cover images embedded with the used fraction of capacity. Every test image was applied once as clear and about five times, through diverse layers of implanting, as a stego image.

4.2 Clustering and other data mining techniques applied over the images

In (Ker &Pevny, 2011), the authors suggested a technique which depends on clustering more preferably than classification. This new presented method efficiently evaluates the performance of performers by supposing that the greatest of them are cleared: after applying the agglomerative hierarchical clustering method, the guilty performer(s) is clustered distinct from the non-guilty majority. Suggested paper training indicates that is used in the instance of JPEG images.

In (Tuia et al, 2010), the authors presented non-passive sampling to tag pixels set with hierarchical clustering. The goal of suggested technique is to compare the data relations exposed by the clustering process. Explorations the trimming of the hierarchy diagram as a tree is performed by an active learning process which best matches the tags of the sampled cases. By selecting the portion of the tree to model according to trimming's indecision, instance selecting is concentrated in utmost indecision clusters.

In (Rodriguez et al, 2007), the authors presented a study of the method and essential attentions integral in the expansion of a novel technique used for the discovery of concealed files into digital images. Rodriguez and his colleagues determined the efficiency of one of clustering methods called Learning Vector Quantization (LVQ) that supports in discriminating clean images from abnormal or non-clear images. This comparison is treated applying 7 features (Agaian et al, 2006) over a less group of 200 explanations with different layers of embedded data from 1% up 10% in increases of 1%. The outcomes determined that LVQ as clustering method not only, more perfectly detect when an image includes LSB concealed data when matched to another clustering method such as: k-means or utilizing the primary feature sets, but also gives a simple technique for demonstrating the fraction of imbedding given non-high data imbedding fractions.

In (Avcıbas et al, 2003), the authors presented methods for steganalysis of images that both the active and passive warden frameworks have been possibly exposed to steganographic processes. Then proposed a categorizer between stego images and non-stego-images which are made applying multivariate regression method on the designated quality metrics and is trained depends on an appraisal of the primary image. Simulation outcomes with the selected feature group and recognized steganographic methods show that suggested method is capable with realistic truthfulness to discriminate between stego-images and non-stego images.

In (Cho et al, 2010), the authors aimed to plan one n-classifier that categorizes non-clear images based on their steganographic processes in order to distinctive cover images from stego-images. This organization is depending on steganalysis outcomes of disintegrated image chunks. As an actual image frequently contains non-homogeneous areas, its disintegration will toward lesser image chunks, each of that is more non-heterogeneous. Cho and his colleagues classified those image chunks into N-classes and discover a categorizer for per class to decide either a chunk is from a non-stego image or a stego image with a certain steganographic process.

In (Lin et al, 2004), the authors proposed a technique of identifying the presence of embedded messages, that are arbitrarily spread in the least significant hits (LSB) of 1byteblack and white images and 3byte RGB colour images. The proposed discover scheme depends on the one of data mining techniques like support vector regression (SVR) technique. It is revealed that the quantity of a designated group of characteristic models a n-dimensional feature space that permits approximation of the size of concealed messages imbedded in the LSB of non-stego images with most accuracy.

5. Data mining techniques on steganalysis over multimedia and protocol

In this section we present several data mining techniques used to steganalysis over Audio, Text, Video and Protocol domains. The percentage of papers referenced to data mining approaches over these domains are about 20% and its lesser than image, for this reason we separate our work into two parts, which in the previous part we proposed data mining techniques on steganalysis over Image that contains 80% of all paper that used and referenced, and in this part, we survey data mining approaches over Audio, Text, Video and Protocol domains.

5.1 Data mining techniques on steganalysis over Audio

In (Geetha et al, 2010), the authors present a useful forensic steganalysis method for audio signals which can appropriately evaluate the measurements troubled by non-clear imbedding and categorize them to designate recent steganographic approaches. A summary of a rule based approach with six kinds of decision tree categorizer like as: Decision Stump, Naive Bayes, Alternating Decision Tree, Fast Decision Tree, J48 Tree and Logical Model Tree initiate, presented to achieve the discovery of the audio subliminal network. The assessment of the decision tree model and the boosted feature space, on a dataset include 4800 non stego and stego audio archives are accomplished for the traditional stenographic approach.

In (Kraetzer et al, 2007), the authors presented a method for digital media forensics to demonstrate the utilized microphones and the situations around of recorded digital audio examples of utilizing recognized audio steganalysis characteristic. Suggested main assessment is depended on a restricted prototypical test group of 10 diverse kinds of audio reference signals listed as single audio records using four microphones in 10 diverse places with 2byte digitalization and 44.1 kHz arbitrary model ratio. Suggested opinion was primarily determined through the presence steganalysis features and the request of usages in a restricted test and the first set. In the suggested tests, an inter-tool inquiry and evaluation with diverse tool features is achieved while intra-tool assessments are unconsidered. One kind of the data mining tools is WEKA that used for categorization consists of K-means approach as a kind of the clustering method and Naive Bayes (NB) approach as a kind of classification method are used with the aim to assess their categorization in respect to the categorization correctness on recognizing audio steganalysis features.

In (Ruetal, 2005), the author presented a steganalysis technique that can consistently discover messages concealed in WAV records. This is performed by accomplishing a four-layer 1-Dimensioal wavelet decay of the audio signals, applying support vector machines (SVMs) approach to identify the presence of concealed messages because of its excellent performance. Ru and his colleagues utilized a group of audios contain both of non-stego ones and stego ones as the learning and testing statistics to create the SVM categorizer. SVM is depends on Vapnik's geometric learning scheme (Vapnik, 1995). It generates a high border hyper plane that discrete the training vectors from diverse classes. When the border is full-sized, the probabilistic test fault range is un-maximized. Non-linear categorizer can be generated by way of mapping the primary entrance space into an upper dimensional characteristic space using a non-linear core task.

In (Kraetzer & Dittmann, 2007), the authors presented a method in audio steganalysis with a huge of information hiding processes is directed. The employed learned and tested recognizer method, utilizing a support vector machine (SVM) approach depends classification of characteristic collections produced by fusion both by Mel-Cepstral and time scope features, is assessed for its value as a kind of steganalysis method like as universal steganalysis implement as like as used another kind of steganalysis method like as specific steganalysis implement for voice over internet protocol (VoIP) steganography.

In (Qiao et al, 2009), a support vector machine (SVM) approach is used for diverse feature collections for classification and pattern inquiry. In (Liu et al, 2009), the authors applied a support vector machine (SVM) to distinguish the features of transferring stego -signals from non-stego-signals.

5.2 Data mining techniques on steganalysis over Text

In (Zhao et al, 2009), the authors proposed a novel steganalysis technique to discover the presence of concealed data utilizing feature replacement in contexts. This is performed by the use of SVM (Support Vector Machine) technique as a classifier to categorize the feature vector entrance into SVM. In the suggested discovery process, the purpose of SVM is to categorize feature vector, in order to separate normal (non stego) texts from stego (non-clear) texts. Depend on measurement training principle of VC–D and operational hazard minimization danger in (Chang and Lin, 2001), SVM is better than another method to answering ML (machine learning) problematic in a formal of non-big models, refining simplification acts, answering nonlinear and the most-D (dimensional) problems, etc. The discovery process can be partitioned into two portions. The first one is the training method and the second one is the classification method.

In (Chen et al, 2011), the authors provided a novel steganalysis scheme in contrast with replacement-based verbal steganography based on text suitable and declared how to utilize the measurements of text suitable values to differentiate among non-stego from stego texts. Also presented the SVM approach as a classifier besides the learning and testing corpus that needs two text groups named SVM training text group and SVM testing text group, both of that have subsections entitled non-stego and stego text.

5.3 Data mining techniques on steganalysis over Video

In (Kancherla & Mukkamala, 2009a, 2009b), the authors suggested a video steganalysis technique utilizing neural networks (NN) approach and support vector machines (SVM) approach to discover concealed data by investigating both the temporal redundancies and spatial redundancies. In their model supposed the non-stego video and the concealed data are not dependent and utilizes the probability quantity function of the inter-frame diversion signal to show the labelling influence caused by embedding files. In (Liu et al, 2008), presented an inter-frame correlation based on compacted video steganalysis techniques, applies collusion to the main feature from like video frames of a solo scene, and utilizes the blind classifier using a feed forward neural network (NN) abilitiy of non-linear character mapping.

5.4 Data mining techniques on steganalysis over Protocol

In (Huang et al, 2011), the authors presented a different steganalysis technique that uses regression investigation and the second discovery. The suggested technique not only can identify the concealed message imbedded in a compacted VoIP (voice over Internet protocol), but also precisely estimate the imbedded message length. The suggested technique depends on the second measurements, i.e. Performing a second steganography (imbedding data in an instant speech at an imbedding ratio tracked by imbedding extra data at a diverse layer of data imbedding) so as to estimate the concealed message length. Several repetitive trains were performed, in order to permit the establishment of the arithmetic relation between the imbedding rate and the rate of frequency point. Regression investigation was selected to try to find for the arithmetic rule, i.e. A numerical between the imbedding rate and the rate of frequency point, as exposed in (1)

$$T = e_0 + e_1 n + e_2 n^2 + e_3 n^3 \tag{1}$$

Where T is the imbedding ratio, n is rated of the frequency point of the sequence Z and e_0, e_1, e_2 and e_3 are the coefficients.

6. Discussion and analysis

In this section, the survey brief indicates that steganalysis with employed data mining techniques evaluate over Image, Audio, Text, Video and Protocol. It also Shows several graphs, figures and tables about performance and evaluates data mining techniques.

In fig. 3. We show a number of employed papers on data mining techniques on steganalysis based on discrimination of years corresponding to fig. 3. To have general survey of data mining techniques on steganalysis in this book chapter, it illustrates that this issue before than 15 years ago is important and this issue recently got more important than before and the number of research papers has been increased considerably.

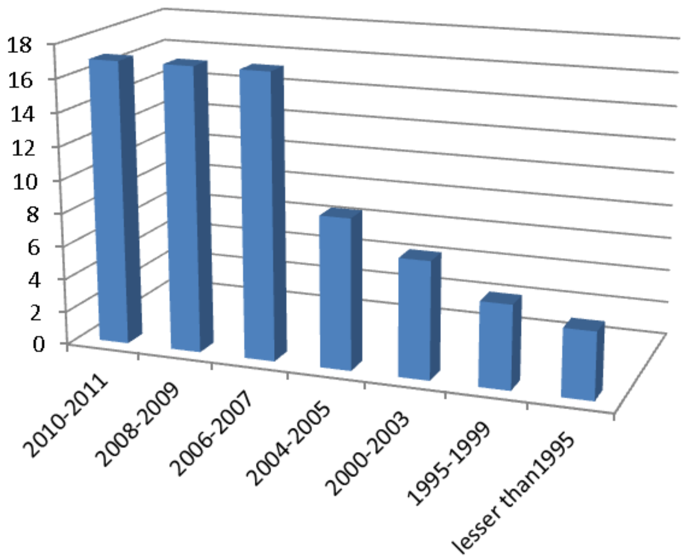

Fig. 3. Variety of employed Paper of data mining techniques on steganalysis.

Besides, in fig. 4. We have presented domain categorization based on recently published papers. It shows that image domain has the most extra spread domain (the first) and text domain is the least spread domain (the fourth).

We have another figure which indicates that data mining techniques have been used. In this figure (fig. 5) 75% of research works are devoted to classification problems, the rest (i.e. 25%) includes 12% deals with regression problems, 9% relate to clustering problems and the remained 4% relate to other problems.

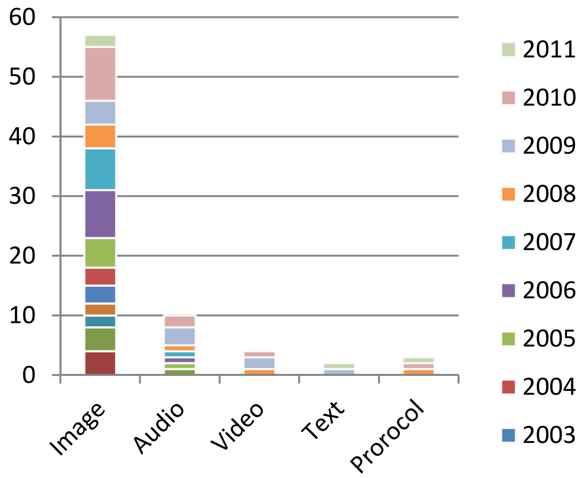

Fig.4. A glance of general categorization data mining techniques in steganalysis domain.

In fig. 5, by using kind of bar plot, we are going to show the rate of papers approximately in the scope of data mining techniques on steganalysis. It illustrates that SVM as one of classification techniques has involved maximum number of papers and also DT and KNN as a kind of classification techniques and cluster techniques which have involved a minimum number of papers.

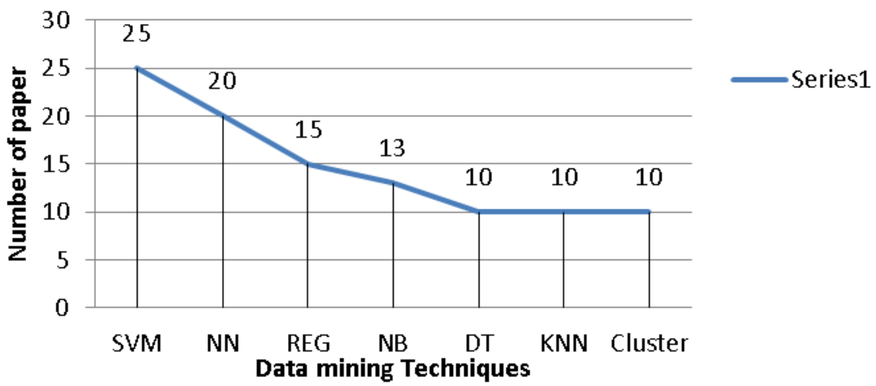

Fig.5. A parallel plot of variety of employed Paper of data mining techniques on steganalysis.

Fig. 6. Shows a parallel plot of the variety of employed papers of data mining techniques on steganalysis. According to this figure we can see that classification is the most important task in data mining which has been focused by researchers in steganalysis field.

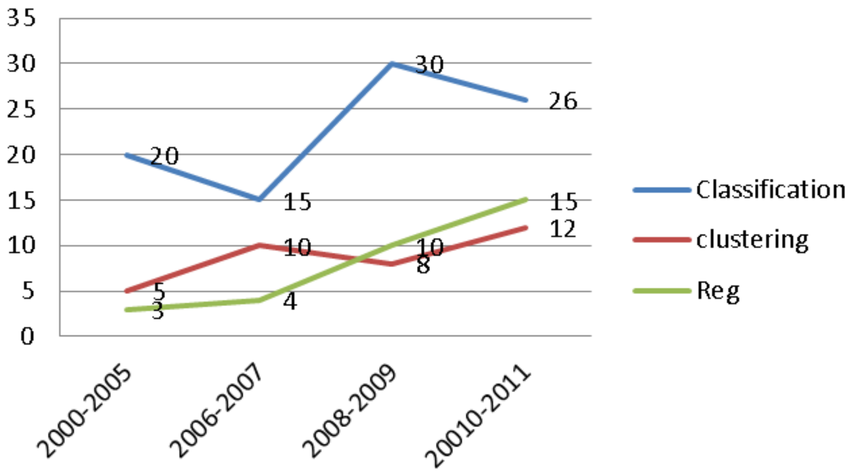

Fig. 6. A parallel plot of variety of employed papers of data mining techniques on steganalysis.

According to fig. 7. Classification approach consists 75% of overall approaches that the most technique was used, for this reason we intend declare in fig. 8 Classification methods that involves of: support vector machine (SVM), neural network (NN), K nearest neighbour (KNN), naive Bayes (NB) and decision tree (DT) approaches.

Fig.8. Shows that 46% of overall classification methods is SVM, 27% is related to NN, 11% to NB, 11% to DT and 5% to KNN.

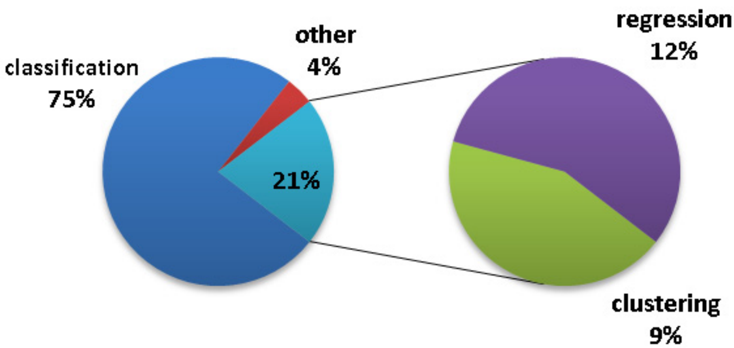

Fig. 7. Distribution of used data mining techniques.

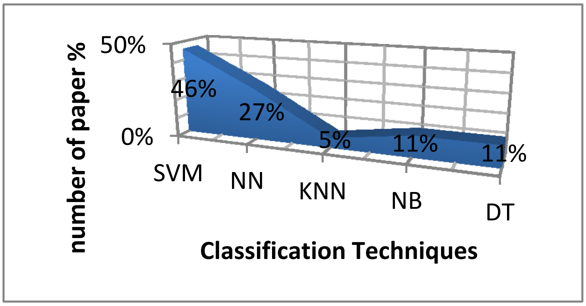

Fig. 8. Type of classification techniques.

Each method has its own self features and utilizes special data set and depends on diverse formats, thus in Table 1 we have a goal to review four new nested approaches that used the second detection method. Second detection is the newest method in steganalysis that performs after hiding message detection or discrimination of stego file from the non - stego file. This method depends on dynamic steganalysis problems that consist of estimate length of concealed message, detect security key stego files, estimate amount of MPVD and etc.

Paper	Feature	DM Technique	Type of steganalysis	Domain	First detection	Second detection
Steganalysis of compressed speech to detect covert voice over Internet protocol channels		Regression	Static, Dynamic	Protocol	Discover embeds message	Length of concealing message
Message estimation for universal steganalysis using multi-classification support vector machine		SVM	Static, Dynamic	Image	Stego/ clear image	Length of concealing message
Steganalysis of HMPD reversible data hiding scheme		SVM	Static, Dynamic	Image	Stego / clear image	Security key stego
Steganalysis and payload estimation of embedding in pixel differences using neural networks		Neural Networks (NN)	Static, Dynamic	Image	Stego / clear image	MPVD

Table 1. A Brief review of four new nested methods.

In table 2, we show some data sets that used in the papers; they are different with each other so we can't compare them. There were seldom featured vectors in papers therefore table 3 just shows three feature vectors.

No	Paper	Data set
1	(Yang et al, 2011)	Downloaded 3000 originally very high resolution color images in format "tiff" from http://photogallery.nrcs.usda.gov, and partitioned them into 15 groups averagely
2	(Davidson et al, 2005)	There are total of 1300 images, which had been cleared of copyright issues. (http://www.datahiding.org), courtesy of Dr. Edward Delp, Purdue University
3	(Tan et al, 2006)	Three hundred images are randomly selected from human, architecture and landscape categories of photo.net image database, one hundred images from each category.
4	(Zhou et al, 2010), (Kobsi& Merouani, 2007)	1096 sample images CorelDraw image database. Included in the CorelDRAW (www.corel.com).
5	(Chou et al, 2010)	The uncompressed color image database (UCID) consists of 1338 was used as the cover images in the training set. The INRIA Holidays dataset has 1491 images was used for the cover images in the testing set.
6	(Michael et al, 2006)	Set of 5075 images from 5 different digital cameras (all over 4 megapixels).
7	(Xuan et al, 2007)	1096 BMP images with size of 768x512 in the CorelDraw-www.corel.com
8	(Liu & H. Sung, 2007)	5000 TIFF raw format digital pictures from Olympus C740. These images are 24-bit, 640*480 pixels, lossless true color and never compressed
9	(Miche et al, 2007)	13 000 images of natural scenes, coming from 5 different digital cameras.
10	(Liu et al, 2006)	The original images in our experiments are 5000 TIFF raw format digital pictures from Olympus C740, taken in U.S.A, across spring to winter.
11	(Liua et al, 2008)	The original images in our experiments are 5000 TIFF raw format digital pictures, taken in USA during 2003–2005.
12	(Mehrabi et al, 2007)	860 gray levels PGM images.
13	(Sajedi & Jamzad , 2008)	Used 315 images randomly selected from Washington university image database http://www.cs.washington.edu/research/image database
14	(Joo et al , 2010)	2000 color images from the USDA NRCS Photo Gallery
15	(Lou et al , 2009)	860 color images in JPEG format from content based image Retrieval (CBIR) University of Washington, July 30 2007 http://www.cs.washington.edu/research/imagedatabase/groundtruth
16	(Cho et al, 2010)	Among these 3580 images, 570 images were randomly downloaded from the image database
17	(Qiao et al, 2009)	The dataset contains 1000 mono MP3 audio files with the bit rate of 128 kbps and the sample rate of 44 KHz. Each audio has the duration of 18 seconds

18	(Liu et al, 2009)	1000 WAV audio signals files covering different types such as digital speech, on-line broadcast, and music, etc.
19	(Zou et al, 2006)	Used 2812 images download from the website of Vision Research Lab, University of California, Santa Barbara.

Table 2. The list of different used Date sets.

No	Paper	Feature vector
1	(Gujar Madhavan, 2006)	There are 9 feature vector that includes: $\mu_1(W)=\sum_{k=1}{}^{4}(\max(f(k,j))-\min(f(k,j)))2^{4(k+1)}$ $\mu_2(W)=\sum 2^{C_i}L_i$ $\mu_3(W)=2^{\#1(b_0)}+2^{\#1(b_0+b_1)}+2^{\#1(b_1+b_2)}+2^{\#1(b_2+b_3)}$ $\mu_4(W)=(\sum_{k=0}{}^{31}\lvert f_j\rvert^2)^{1/2}$ μ5 (W) = Weighted Hadamard transform. Using an 8x8 Hadamard matrix (H) and the operation y = Hx μ6(W), μ7(W), μ8(W), $\mu9(W)=\sum p_j \log p_j$
2	(Geetha et al, 2010)	$F=(f_1{}^P, f_2{}^P,\ldots f_5{}^P, f_1{}^P, f_2{}^{P+1},\ldots f_5{}^{P+1}, \ldots,f_1{}^{P+4}, f_2{}^{P+4}, \ldots, f5^{P+4},Type)$
3	(Zhou et al, 2010)	$F_{xb}(U,V,C)=J_{m(U,V)}/N^*(\min\lvert v_i-v_j\rvert^2)$

Table 3. The list of used feature vectors.

7. Conclusion and future work

In this book chapter, we have proposed a survey for data mining techniques on steganalysis. As it was mentioned in the presented chapter, different medias have been used as the cover media such as: image, audio, text, protocol and video. This survey has reviewed several published data mining techniques for steganalysis. We showed that SVM, as a type of classification method, got the best results in comparison to other classification techniques.

The future work in steganalysis would be the employment of advanced bio-inspired metaheuristic algorithms, such as Genetic Algorithms, Ant Colony Optimization, Particle Swarm Optimization and Artificial Immune Systems, to construct efficient learning classifier systems. This employment enables us to explore the huge search space more efficiently and discover more accurate steganalysis knowledge.

8. Reference

Avcibas, I. and Memon, N. and Sankur, B. (2002). Image steganalysis with binary similarity measures, *Image Processing. 2002. Proceedings. 2002 International Conference on,* Vol. 3, no., pp. 645- 648, ISBN: 0-7803-7622- June 2002.

Avcıbas, I and Memon, N and Sankur, B.(2003). Steganalysis Using Image Quality Metrics, *ieee transactions on image processing,* VOL. 12, NO. 2, pp.221-229

Avcibas, I.(2006). Audio steganalysis with content-independent distortion measures, *Signal Processing Letters, IEEE,* vol.13, no.2, pp. 92- 95, ISSN : 1070-9908, Feb. 2006

Baragada, S.R. and Ramakrishna, S. and Rao, MS and Purushothaman, S.(2008). Implementation of Radial Basis Function Neural Network for Image Steganalysis, *International Journal of Computer Science and Security (IJCSS),* Vol.2, No.1, pp.12-22, ISSN : 1985-1553.

Benton, R. and Chu, H. (2005). Soft Computing Approach to Steganalysis of LSB Embedding in Digital Images, *Information Technology: Research and Education, 2005. ITRE 2005. 3rd International Conference on*, pp.105-109, ISBN: 0-7803-8932-8, June2005

Berg, G. and Davidson, I. and Duan, M.Y. and Paul, G. (2003). Searching For Hidden Messages: Automatic Detection of Steganography, *Proceedings of the 15th Innovative Applications of AI Conference,* pp.51-56, August, 2003, Acapulco, Mexico.

Bhatt, C.A. and Kankanhalli, M.S.(2011). Multimedia data mining: state of the art and challenges, *Multimedia Tools and Application,* Vol.51, No.1, pp.35-76.

Chen, C. and Shi, Y.Q. and Chen, W. and Xuan, G. (2006). statistical moments based universal steganalysis using jpeg 2-d array and 2-d characteristic function, *Image Processing, 2006 IEEE International Conference on,* Vol.6, ISBN: 1-4244-0481-9 pp.105-108, Atlanta, GA, USA

Chen, Z. and Huang, Land Miao, H. and Yang, W. and Meng, P. (2011).Steganalysis against substitution-based linguistic steganography based on context clusters, *Computer and Electrical Engineering,* Vol.37, No.6, pp.1071-1081, ISSN = 0045-7906.June 2011

Cho, S. and Wang, J. and Kuo, C.C.J. and Cha, B.H. (2010). BLOCK-BASED IMAGE STEGANALYSIS FOR A MULTI-CLASSIFIER, *Multimedia and Expo (ICME), 2010 IEEE International Conference on*, Vol.0, pp.1457-1462, ISBN: 978-1-4244-7491-2 July 2010, Singapore,

Cortes, C and Vapnik, V. (1995) Support-vector networks, *in Machine Learning*, Vol.20, No.3, pp. 273-297, ISSN: 0885-6125.

Davidson, J. and Bergman, C. and Bartlett, E. (2005). An artificial neural network for wavelet steganalysis, *Proceedings of SPIE - The International Society for Optical Engineering, Mathematical Methods in Pattern and Image Analysis,*, vol. 5916, pp. 1-10. ISBN 0-8194-5921-6, August 2005, San Diego, California, USA.

Geetha, S. and Ishwarya, N. and Kamaraj, N. (2010).Audio steganalysis with Hausdorff distance higher order statistics using a rule based decision tree paradigm .*Expert Systems with Applications*, Vol.37, No.12, pp. 7469-7482, ISSN 0957-4174

Guorong, X and Xia, C and Shi, Y.Q. and Wen, C and Xuefeng, T and Cong, H.(2007).JPEG Steganalysis Based on Classwise Non-Principal Components Analysis and Multi-Directional Markov Model, *Multimedia and Expo, 2007 IEEE International Conference on,* pp.903-906, ISBN : 1-4244-1017-7, Beijing, July 2007.

Huang, Y. and Tang, S. and Bao, C. and Yip, Y.J.(2011). Steganalysis of compressed speech to detect covert voice over Internet protocol channels, *Information Security, IET,* vol.5, no.1, pp.26-32, ISSN: 1751-8709.

Holoska, J, Oplatkova, Z, Zelinka, I and Senkerik, R (2010).Comparison Between Neural Network Steganalysis And Linear Classification Method Stegdetect, *Computational Intelligence, Modeling and Simulation (CIMSiM), 2010 Second International Conference on, .Vol.10, pp.*15-20, ISBN: 978-0-7695-4262-1, Sept. 2010, Bali

Joo, J.C. and Oh, T.W. and Choi, J.H. and Lee, H.K. (2010). Steganalysis scheme using the difference image of calibrated sub-sampling, *Intelligent Information Hiding and*

Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on, pp.51-54, ISBN : 978-0-7695-4222-5, Darmstadt, Oct. 2010

Kaipa, B. and Robila, S.A.. (2010). Statistical Steganalyis of Images Using Open Source Software, *Applications and Technology Conference (LISAT), 2010 Long Island Systems*, pp.1-5, ISBN: 978-1-4244-5550-8, May 2010, Farmingdale, NY

Kancherla, K.; Mukkamala, S.(2009).Video steganalysis using motion estimation, *Neural Networks, 2009. IJCNN 2009. International Joint Conference on.*, pp.1510-1515, ISBN : 978-1-4244-3549-4, Atlanta, GA June 2009.

Ker, A.D. and Pevny, T. (2011). A New Paradigm for Steganalysisvia Clustering. *Proc. SPIE Media Watermarking, Security, and Forensics XIII*, Vol.7880, pp. 78800U-78813U, Bellingham, ISBN 978-0-8194-8417-8.

KOBSI, N. and MEROUANI, H.F. (2007). Neural Network Based Image Steganalysis: A Comparative Study, *Neural Networks for Signal Processing [1994] IV. Proceedings of the 1994 IEEE Workshop*, pp:423-430, ISBN: 0-7803-2026-3, Sep 1994, Ermioni,

Kodovský, J and Fridrich, J.(2012). Ensemble Classifiers for Steganalysis of Digital Media, *ieee transactions on information forensics and security*, VOL. 7, NO. 2, pp.432-444, ISBN: 1556-6013

Kraetzer, C. and Dittmann, J. (2007). Pros and Cons of Mel-cepstrum based Audio Steganalysis using SVM Classification, *Proceedings of the 9th international conference on Information hiding*, Vol., No., pp.359-377, ISBN: 978-3-540-77369-6, June, 2007, Saint Malo, France

Kraetzer, C. and Dittmann, J.(2008). Cover Signal Specific Steganalysis: the Impact of Training on the Example of two Selected Audio Steganalysis Approaches, *Proceedings of the Electronic Imaging Conf. on Security, Forensics, Steganography, and Watermarking of Multimedia Contents*, Vol. 6819.

Kraetzer, C. and Dittmann, J.(2009). The impact of information fusion in steganalysis on the example of audio steganalysis. *Proceedings of the Media Forensics and Security XI. Electronic Imaging Conference*, Vol.7254, ISBN 9780819475046, February 2009

Kraetzer, C. and Oermann, A. and Dittmann, J. and Lang, A. (2007). Digital Audio Forensics: A First Practical Evaluation on Microphone and Environment Classification, *Proceedings of the 9th workshop on Multimedia & security*, pp.63-74, ISBN: 978-1-59593-857-2, New York, NY, USA

Laxman, S. and Sastry, P.S.(2006). A survey of temporal data mining, Sadhana, *Academy Proceedings in Engineering Sciences*, Vol.31, No.2, pp.173-198,

Lin, E. and Woertz, E. and Kam, M.(2004). LSB steganalysis using support vector regression, *Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC.*, pp.95-100, June 2004, ISBN:0-7803-8572-1

Liu, Q. and Sung, A. and Qiao, M.(2009).Spectrum steganalysis of WAV audio streams, *Machine Learning and Data Mining in Pattern Recognition*, Vol. 5632, pp. 582-593, ISBN:978-3-642-03070-3-44. Berlin Heidelberg 2009

Liu, Q. and Sung, A.H. (2007). Feature Mining and Neuro-Fuzzy Inference System for Steganalysis of LSB Matching Stegangoraphy in Grayscale Images, *Proceedings of the 20th international joint conference on Artifical intelligence*, pp.2808-2813, January, 2007, Hyderabad, India

Liu, Q. and Sung, A.H. and Chen, Z. and Xu, J. (2008). Feature mining and pattern classification for steganalysis of LSBmatching steganography in grayscale images, *Pattern Recognition*, Vol.41, No.1, pp.56-66, ISSN: 00313203

Liu, Q. and Sung, A.H. and Xu, J. and Ribeiro, B.M. (2006). Image Complexity and Feature Extraction for Steganalysis of LSB Matching Steganography, *Pattern Recognition, 2006. ICPR 2006. 18th International Conference on,* Vol.2, pp.267-270, ISBN:0-7695-2521-0, Hong Kong September 2006

Liu, Q. and Sung, A.H.(2007).Feature mining and nuero-fuzzy inference system for steganalysis of LSB matching steganography in gray scale images, *Proceedings of the 20th international joint conference on Artificial intelligence*, pp.2808-2813, Hyderabad, India, January

Liu, S. and Yao, H. and Gao, W. (2004).Steganalysis Based on Wavelet Texture Analysis and Neural Network, *Intelligent Control and Automation, 2004. WCICA 2004. Fifth World Congress on*, Vol.5, pp.4066--4069

Lopez-Hernandez, J. and Martinez-Noriega, R. and Nakano-Miyatake, M. and Yamaguchi, K. (2008).Detection of BPCS-steganography using SMWCF steganalysis and SVM, *Information Theory and Its Applications, 2008.ISITA 2008. International Symposium on,* pp.1-5, ISBN: 978-1-4244-2069-8 Dec. 2008

Lou, D.C. and Hu, C.H. and Chou, C.L. and Chiu, C.C. (2011). Steganalysis of HMPD reversible data hiding scheme, *Optics Communications*(June 2011), Vol.284, pp.5406-5414, ISSN:0030-4018

Lou, D.C. and Liu, C.L. and Lin, C.L. (2009).Message estimation for universal steganalysis using multi-classification support vector machine, *Computer Standards& Interfaces*, Vol.31, No.2, (March 2008)pp.420-427, ISSN: 0920-5489

Lyu, S. and Farid, H. (2004). Steganalysis Using Color Wavelet Statistics and One-Class Support Vector Machines, *SPIE Symposium on Electronic Imaging*, Vol.5306, pp35-46, ISBN : 0-8194-5209-2, San Jose CA, USA, April 2004

Marvel, L. and Henz, B. and Boncelet, C. (2008). Fusing Rate-Specific SVM Classifiers for ±1 Embedding Steganalysis, *Information Sciences and Systems, 2008. CISS 2008. 42nd Annual Conference on,* vol., no., pp.361-364, ISBN: 978-1-4244-2247-0, Princeton, NJ, March 2008.

Meghanathan, N and Nayak, L.(2010).steganalysis algorithms for detecting the hidden information in image, audio and video cover media, *International Journal of Network Security & Its Application (IJNSA),* Vol.2, No.1, ISSN: 0975- 2307

Mehrabi, M.A. and Faez, K. and Bayesteh, A.R. (2007). Image Steganalysis Based on Statistical Moments of Wavelet Subband Histograms in Different Frequencies and Support Vector Machine, *Natural Computation, 2007. ICNC 2007. Third International Conference on*, Vol.1, pp.587-590, ISBN: 0-7695-2875-9, Aug. 2007.

Miche, Y. and Bas, P. and Lendasse, A. and Jutten, C. and Simula, O. (2007). Advantages of Using Feature Selection Techniques on Steganalysis Schemes, *Computational and Ambient Intelligence*, pp.606-613, ISBN: 978-3-540-73006-4,

Miche, Y. and Roue, B. and Lendasse, A. and Bas, P. (2006).A Feature Selection Methodology for Steganalysis, *Multimedia Content Representation, Classification and Security*, pp.49-56, ISBN = 3-540-39392-7, 978-3-540-39392-4, Istanbul, Turkey,

Nissar, A. and Mir, A.H.(2010). Classification of steganalysis techniques A study, *Digital Signal Processing,* Vol.20, No.6, pp.1758-1770, ISSN 1051-2004

Qiao, M. and Sung, A.H. and Liu, Q.(2009).Steganalysis of mp3stego, *Neural Networks, 2009. IJCNN 2009. International Joint Conference on,* pp.2566-2571, ISSN: 1098-7576, Atlanta, GA, June 2009

Rodriguez, B.M. and Peterson, G.L. and Bauer, K.W. and Agaian, S.S..(2006). Steganalysis Embedding Percentage Determination with Learning Vector Quantization. s*ystems, Man and Cybernetics, 2006. SMC'06. IEEE International Conference on*, V. 3, pp 1861-1865, ISBN: 1424400996

Ru, X.M. and Zhang, H.J. and Huang, X.(2005) Steganalysis of audio: Attacking the steghide, *Machine Learning and Cybernetics, 2005. Proceedings of 2005 International Conference on,* Vol.7, pp.3937-3942, ISBN: 0-7803-9091-1, Aug. 2005

Sabeti, V. and Samavi, S. and Mahdavi, M. and Shirani, S. (2009).Steganalysis of Embedding in Divergence of Image Pixel Pairs by Neural Network, *the ISC Intel Journal of Information Security ISeCure*, Vol.1, No.1, pp.17-26, ISSN: 2008-2045

Sabeti, V. and Samavi, S. and Mahdavi, M. and Shirani, S. (2010). Steganalysis and payload estimation of embedding in pixel differences using neural Networks, *Pattern Recognition*, Vol.43, No.1, pp.405-415, ISSN: 0031-3203,

Sajedi, H and Jamzad, M.(2008). A Steganalysis Method Based on Contourlet Transform Coefficients, *Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP '08 International Conference on*, pp.245-248, ISBN: 978-0-7695-3278-3, Aug. 2008

Shaohui, L. and Hongxun, Y. and Wen, G. (2003). neural network based steganalysis in still images, *Proceedings of the 2003 International Conference on Multimedia and Expo*, Vol.1, pp.509-512, ISBN:0-7803-7965-9, July, 2003

Shi, Y.Q. and Xuan, G. and Zou, D. and Gao, J. and Yang, C. and Zhang, Z. and Chai, P. and Chen, W. and Chen, C. (2005). Image Steganalysis Based on Moments of Characteristic Functions Using Wavelet Decomposition, Prediction-Error Image, and Neural Network, *ICME(ICMCS) - International Conference on Multimedia Computing and Systems/ International Conference on Multimedia and Expo*, pp. 269-272, July 2005, ISBN: 0-7803-9332-5

Tan, S. and Huang, J. and Yang, Z. and Shi, Y.Q. (2006). steganalysis of jpeg2000 lazy-mode steganography using the hilbert-huang transform based sequential analysis hilbert-huang transform based sequential analysis, *Image Processing, IEEE International Conference on*, Vol.0, pp.101-104, Oct. 2006. Atlanta, GA, ISSN: 1522-4880.

Tuia, D. and Kanevski, M. and Munoz Mari, J. and Camps-Valls, G. (2010). cluster-based active learning for compact image classification, *Geoscience and Remote Sensing Symposium (IGARSS), 2010 IEEE International*, Vol., pp.2824-2827, ISSN : 2153-6996, Honolulu, HI, July 2010.

Xiao, Y.Y and Aiming, W.(2009).An Investigation of Genetic Algorithm on Steganalysis Techniques, Intelligent *Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP '09. Fifth International Conference on*, pp.1118-1121, ISBN : 978-0-7695-3762-7, Kyoto, Sept. 2009.

Xiao.Y. Y and Aiming W. (2009).Steganalysis Based on Regression Model and Bayesion Network, *Multimedia Information Networking and Security, 2009. MINES '09. International Conference on,* vol.1, pp.41-44, ISBN: 978-1-4244-5068-8, Hubei, Nov. 2009

Xuan, G. and Shi, Y. and Huang, C. and Fu, D. and Zhu, X. and Chai, P. and Gao, J. (2006). Steganalysis using high-dimensional features derived from co-occurrence matrix and class-wise non-principal components analysis (CNPCA), *Proceedings of the 5th international conference on Digital Watermarking*, pp.49-60, ISBN: 3-540-48825-1, 978-3-540-48825-5, Jeju Island, Korea, 2006

Yang, C. and Liu, F. and Luo, X (2011). Error Correction of Sample Pair Analysis Based on Support Vector Regression, *Multimedia Information Networking and Security (MINES), 2011 Third International Conference on,* pp.633-636 Shanghai, Nov, 2011, ISBN: 978-0-7695-4559-2

Zhao, X and Huang, L. and Li, L. and Yang, W. and Chen, Z. and Yu, Z. (2009). Steganalysis on Character Substitution Using Support Vector Machine, *Proceedings of the 2009 Second International Workshop on Knowledge Discovery and Data Mining*, No.5, pp.84-88, ISBN:978-0-7695-3543-2, Moscow, Jan. 2009

Zhou, Z, Zhang, X, Chen, Z. (2010). A Universal Steganalysis Based on One-Class Classification, *Journal of Computational Information Systems,* VOl.6, No.9, pp.2941-2948, ISBN: 1553-9105

Zou, D. and Shi, Y.Q. and Su, W. and Xuan, G. (2006). Steganalysis Based on Markov Model of Thresholded Prediction-Error Image, *Multimedia and Expo, 2006 IEEE International Conference on (ICME)*, Vol.6, pp.1365-1368, ISBN: 1-4244-0367-7, July, 2006, Toronto