Volume 2, No. 4, April 2011

Journal of Global Research in Computer Science

ISSN-2229-371X

REVIEW ARTICLE

Available Online at www.jgrcs.info

A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier

Souvik Bhattacharyya*[1], Indradip Banerjee[2] and Gautam Sanyal[3]

*[1] Department of Computer Science and Engineering, University Institute of Technology
The University of Burdwan, Burdwan, India.
souvik.bha@gmail.com[1]
[2] Department of Computer Science and Engineering, University Institute of Technology
The University of Burdwan, Burdwan, India.
ibanerjee2001@yahoo.com[2]
[3] Department of Computer Science and Engineering, National Institute of Technology
Durgapur, India.
nitgsanyal@gmail.com [3]

Abstract: The staggering growth in communication technology and usage of public domain channels (i.e. Internet) has greatly facilitated transfer of data. However, such open communication channels have greater vulnerability to security threats causing unauthorized information access. Traditionally, encryption is used to realize the communication security. However, important information is not protected once decoded. Steganography is the art and science of communicating in a way which hides the existence of the communication. Important information is firstly hidden in a host data, such as digital image, text, video or audio, etc, and then transmitted secretly to the receiver. Steganalysis is another important topic in information hiding which is the art of detecting the presence of steganography. This paper provides a critical review of steganography as well as to analyze the characteristics of various cover media namely image, text, audio and video in respects of the fundamental concepts, the progress of steganographic methods and the development of the corresponding steganalysis schemes.

Keywords: Cover Image, Steganography,Image

INTRODUCTION

Steganography is the art and science of hiding information by embedding messages within other, seemingly harmless messages. Steganography means “covered writing” in Greek. As the goal of steganography is to hide the presence of a message and to create a covert channel, it can be seen as the complement of cryptography, whose goal is to hide the content of a message. Another form of information hiding is digital watermarking, which is the process that embeds data called a watermark, tag or label into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. The object may be an image, audio, video or text only. A famous illustration of steganography is Simmons’ Prisoners’ Problem [1].An assumption can be made based on this model is that if both the sender and receiver share some common secret information then the corresponding steganography protocol is known as then the secret key steganography where as pure steganography means that there is none prior information shared by sender and receiver. If the public key of the receiver is known to the sender, the steganographic protocol is called public key steganography [4], [7] and [8].For a more thorough knowledge of steganography methodology the reader may see [9], [24].Some Steganographic model with high security features has been presented in [28-33]. Almost all digital file formats can be used for steganography, but the image and audio files are more suitable because of their high degree of redundancy [24]. Fig. 1 below shows the different categories of steganography techniques.

Fig. 1. Types of Steganography

Among them image steganography is the most popular of the lot. In this method the secret message is embedded into an image as noise to it, which is nearly impossible to differentiate by human eyes [10, 14, 16]. In video steganography, same method may be used to embed a message [17, 23]. Audio steganography embeds the message into a cover audio file as noise at a frequency out of human hearing range [18]. One major category, perhaps the most difficult kind of steganography is text steganography or linguistic steganography [3]. The text steganography is a method of using written natural language to conceal a secret message as defined by Chapman et al. [15]. A block diagram of a generic steganographic system is given in Fig. 2.

© JGRCS 2010, All Rights Reserved

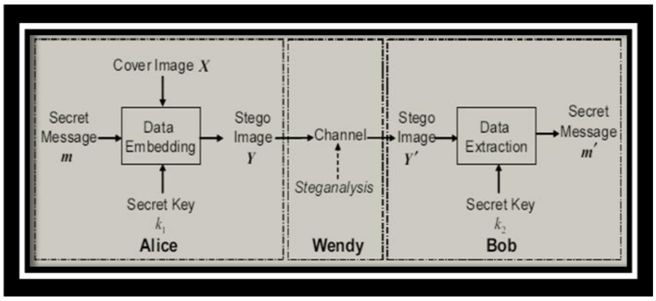
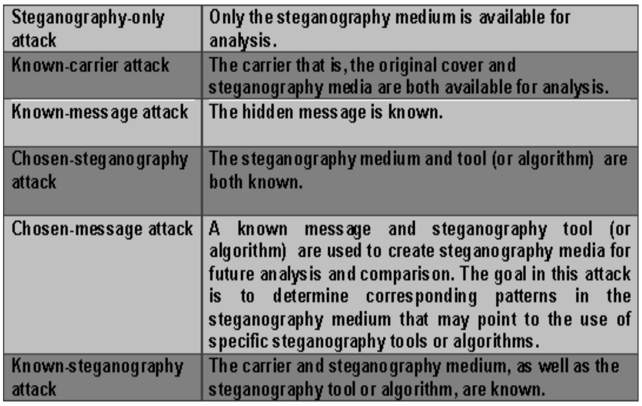


Fig. 2. Generic form of Steganography and Steganalysis

Steganalysis, from an opponent's perspective, is an art of deterring covert communications while avoiding affecting the innocent ones. Its basic requirement is to determine accurately whether a secret message is hidden in the testing medium. Further requirements may include judging the type of the steganography, estimating the rough length of the message, or even extracting the hidden message. The challenge of steganalysis is that: Unlike cryptanalysis, where it is evident that intercepted encrypted data contains a message, steganalysis generally starts with several suspect information streams but uncertainty whether any of these contain hidden message. The steganalyst starts by reducing the set of suspect information streams to a subset of most likely altered information streams. This is usually done with statistical analysis using advanced statistics techniques.

Types of Attacks: Attacks and analysis on hidden information may take several forms: detecting, extracting, and disabling or destroying hidden information. An attack approach is dependent on what information is available to the steganalyst (the person who is attempting to detect steganography-based information streams).



Steganography-only attack	Only the steganography medium is available for analysis.
Known-carrier attack	The carrier that is, the original cover and steganography media are both available for analysis.
Known-message attack	The hidden message is known.
Chosen-steganography attack	The steganography medium and tool (or algorithm) are both known.
Chosen-message attack	A known message and steganography tool (or algorithm) are used to create steganography media for future analysis and comparison. The goal in this attack is to determine corresponding patterns in the steganography medium that may point to the use of specific steganography tools or algorithms.
Known-steganography attack	The carrier and steganography medium, as well as the steganography tool or algorithm, are known.

Fig. 3. Types of Steganography Attacks

This paper aims to provide a comprehensive review on different kinds of steganographic schemes and possible steganalysis methods for various cover carrier like image, text, audio and video.

The remaining portion of the paper has been organized as following sections: Section II describes the Image Steganography technique along with Image Steganalysis Technique. Section III describes Text Steganography methodology along with analysis. Section IV deals with some related works on Audio Steganography and Steganalysis. Section V describes the Video Steganography technique along with Video Steganalysis Technique. Various Steganographic Tools are described in Section VI. Section VII contains the analysis of the results and Section VIII draws the conclusion.

IMAGE STEGANOGRAPHY TECHNIQUES

The various image steganographic techniques are: (i) Substitution technique in Spatial Domain: In this technique only the least significant bits of the cover object is replaced without modifying the complete cover object. It is a simplest method for data hiding but it is very weak in resisting even simple attacks such as compression, transforms, etc. (ii)Transform domain technique: The various transform domains techniques are Discrete Cosine Transform (DCT), Discrete Wavelet Trans- form (DWT) and Fast Fourier Transform (FFT) are used to hide information in transform coefficients of the cover images that makes much more robust to attacks such as compression, filtering, etc. (iii) Spread spectrum technique: The message is spread over a wide frequency bandwidth than the minimum required bandwidth to send the information. The SNR in every frequency band is small. Hence without destroying the cover image it is very difficult to remove message completely. (iv) Statistical technique: The cover is divided into blocks and the message bits are hidden in each block. The information is encoded by changing various numerical properties of cover image. The cover blocks remain unchanged if message block is zero. (v) Distortion technique: Information is stored by signal distortion. The encoder adds sequence of changes to the cover and the decoder checks for the various differences between the original cover and the distorted cover to recover the secret message. Some common Image Steganography Technique in Spatial and Transform Domain [146] has been discussed below.

A. Spatial Domain Steganographic Method

1) **Data Hiding by LSB**: Various techniques about data hiding have been proposed in literatures. One of the common techniques is based on manipulating the least-significant-bit (LSB) [34-37] planes by directly replacing the LSBs of the cover-image with the message bits. LSB methods typically achieve high capacity but unfortunately LSB insertion is vulnerable to slight image manipulation such as cropping and compression.

2) **Data Hiding by MBPIS**: The Multi Bit Plane Image Steganography (MBPIS) was proposed by Nguyen, Yoon and Lee [38] at IWDW06. This algorithm is designed to be secure against several classical steganalysis methods like RS steganalysis. The main goal of this paragraph is to detail this steganography algorithm which is dedicated to un-compressed images.

3) **Data Hiding by MBNS**: In 2005, Zhang and Wang [42] also presented an adaptive steganographic scheme with the Multiple-Based Notational System (MBNS)

based on human vision sensitivity (HVS). The hiding capacity of each image pixel is determined by its so-called local variation. The formula for computing the local variation takes into account the factor of human visual sensitivity. A great local variation value indicates the fact that the area where the pixel belongs is a busy/edge area, which means more secret data can be hidden. On the contrary, when the local variation value is small, less secret data will be hidden into the image block because it is in a smooth area. This way, the stego image quality degradation is very invisible to the human eye.

4) **Data Hiding by QIM**: Quantization index modulation (QIM) [43] is a commonly used data embedding technique in digital watermarking and it can be employed for steganography. It quantizes the input signal x to the output y with a set of quantizers, i.e., Q_m (.). Using which quantizer for quantization is determined by the message bit m.

5) **Data Hiding by PVD**: The pixel-value differencing (PVD) method proposed by Wu and Tsai [39] can successfully provide both high embedding capacity and outstanding imperceptibility for the stego-image. The pixel-value differencing (PVD) method segments the cover image into non overlapping blocks containing two connecting pixels and modifies the pixel difference in each block (pair) for data embedding. A larger difference in the original pixel values allows a greater modification. In the extraction phase, the original range table is necessary. It is used to partition the stego-image by the same method as used to the cover image. Based on PVD method, various approaches have also been proposed. Among them Chang et al. [44] proposes a new method using tri-way pixel value differencing which is better than original PVD method with respect to the embedding capacity and PSNR.

6) **Data Hiding by GLM** : In 2004, Potdar et al.[41] proposes GLM (Gray level modification) technique which is used to map data by modifying the gray level of the image pixels. Gray level modification Steganography is a technique to map data (not embed or hide it) by modifying the gray level values of the image pixels. GLM technique uses the concept of odd and even numbers to map data within an image. It is a one-to-one mapping between the binary data and the selected pixels in an image. From a given image a set of pixels are selected based on a mathematical function. The gray level values of those pixels are examined and compared with the bit stream that is to be mapped in the image.

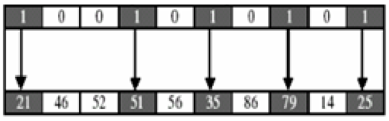


Fig. 4. Data Embedding Process in GLM

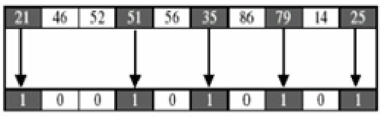


Fig. 5. Data Extraction Process in GLM

7) **Data hiding by the method proposed by Ahmad T et al.**: In this work [40] a novel Steganographic method for hiding information within the spatial domain of the grayscale image has been proposed. The proposed approach works by dividing the cover into blocks of equal sizes and then embeds the message in the edge of the block depending on the number of ones in left four bits of the pixel.

B. Transform Domain Steganographic Method

Transform Domain methods hides messages in significant areas of cover image which makes them robust against various image processing operations like compression, enhancement etc. Many transform domain methods exist. The widely used transformation functions include Discrete Cosine Transformation (DCT), Fast Fourier Transform (DFT), and Wavelet Transformation. The basic approach to hiding information with DCT, FFT or Wavelet is to transform the cover image, tweak the coefficients, and then invert the transformation. If the choice of coefficients is good and the size of the changes manageable, then the result is pretty close to the original.

1) **DCT based Data Hiding**: DCT is a mechanism used in the JPEG compression algorithm to transform successive 88-pixel blocks of the image from spatial domain to 64 DCT coefficients each in frequency domain. The least significant bits of the quantized DCT coefficients are used as redundant bits into which the hidden message is embedded. The modification of a single DCT coefficient affects all 64 image pixels. Because this modification happens in the frequency domain and not the spatial domain, there are no noticeable visual differences. The advantage DCT has over other transforms is the ability to minimize the block-like appearance resulting when the boundaries between the 8x8 sub-images become visible (known as blocking artifact). The statistical properties of the JPEG files are also preserved. The disadvantage is that this method only works on JPEG files since it assumes a certain statistical distribution of the cover data that is commonly found in JPEG files. Some common DCT based steganography methodologies are described below.

JSteg/JPHide: JSteg [45] and JPHide [46] are two classical JPEG steganographic tools utilizing the LSB embedding technique. JSteg embeds secret information into a cover image by successively replacing the LSBs of non-zero quantized DCT coefficients with secret message bits. Unlike JSteg, the quantized DCT coefficients that will be used to hide secret message bits in JPHide are selected at random by a pseudo-random number generator, which may be controlled by a key. Moreover, JPHide modifies not only the LSBs of the selected coefficients; it can also switch to a mode where the bits of the second least significant bit-plane are modified.

F5: F5 steganographic algorithm was introduced by Westfield [47]. Instead of replacing the LSBs of quantized DCT coefficients with the message bits, the absolute value of the coefficient is decreased by one if it is needed to be modified. The F5 algorithm embeds message bits into randomly-chosen DCT coefficients and employs matrix embedding that minimizes the necessary number of changes to hide a message of certain length. In the embedding process, the message length and the number of non-zero AC coefficients are used to determine the best matrix embedding that minimizes the number of modifications of the cover image.

OutGuess: OutGuess [48] is provided by Provos as UNIX source code. There are two famous released versions: OutGuess-0.13b, which is vulnerable to statistical analysis and OutGuess-0.2, which includes the ability to preserve statistical properties. When we talk about the OutGuess, it is referred to OutGuess-0.2. The embedding process of OutGuess is divided into two stages. Firstly, OutGuess embeds secret message bits along a random walk into the LSBs of the quantized DCT coefficients while skipping 0’s and 1’s. After embedding, corrections are then made to the coefficients, which are not selected during embedding, to make the global DCT histogram of the stego image match that of the cover image. OutGuess cannot be detected by chi-square attack [49].

YASS: Yet Another Steganographic Scheme (YASS) [50] belongs to JPEG steganography but it does not embed data in JPEG DCT coefficients directly. Instead, an input image in spatial representation is firstly divided into blocks with a fixed large size, and such blocks are called big blocks (or B-blocks). Then within each B-block, an 8x8 sub-block, referred to as embedding host block (or H-block), is randomly selected with a secret key for performing DCT. Next, secret data encoded by error correction codes are embedded in the DCT coefficients of the H-blocks by QIM. Finally, after performing the inverse DCT to the H-blocks, the whole image is compressed and distributed as a JPEG image. For data extraction, image is firstly JPEG-decompressed to spatial domain. Then data are retrieved from the DCT coefficients of the H-blocks. Since the location of the H-blocks may not overlap with the JPEG 8x8 grids, the embedding artifacts caused by YASS are not directly reflected in the JPEG DCT coefficients. The self-calibration process [51, 52], a powerful technique in JPEG steganalysis for estimating the cover image statistics, is disabled by YASS. Another advantage of YASS is that the embedded data may survive in the active warden scenario. Recently Yu et al [53] proposed a YASS-like scheme to enhance the security performance of YASS via enhancing block randomization. The comparative security performance of YASS, F5 and MB against state-of-the-art steganalytic methods can be found in recent work of Huang et al [54].

Model Based Steganography: This method [147] presents an information-theoretic method for performing steganography and steganalysis using a statistical model of the cover medium. The methodology is general, and can be applied to virtually any type of media. It provides answers for some fundamental questions which have not been fully addressed by previous steganographic methods, such as how large a message can be hidden without risking detection by certain statistical methods, and how to achieve this maximum capacity. Current steganographic methods have been shown to be insecure against fairly simple statistical attacks. Using the model-based methodology, an example steganography method is proposed for JPEG images which achieves a higher embedding efficiency and message capacity than previous methods while remaining secure against first order statistical attacks.

2) DWT based Data Hiding: Wavelet-based steganography [55-60] is a new idea in the application of wavelets. However, the standard technique of storing in the least significant bits (LSB) of a pixel still applies. The only difference is that the information is stored in the wavelet coefficients of an image, instead of changing bits of the actual pixels. The idea is that storing in the least important coefficients of each 4 x 4 Haar transformed block will not perceptually degrade the image. While this thought process is inherent in most steganographic techniques, the difference here is that by storing information in the wavelet coefficients, the change in the intensities in images will be imperceptible.

IMAGE BASED STEGANALYSIS

Steganalysis is the science of detecting hidden information. The main objective of Steganalysis is to break steganography and the detection of stego image is the goal of steganalysis. Almost all steganalysis algorithms rely on the Steganographic algorithms introducing statistical differences between cover and stego image. Steganalysis deals with three important categories: (a) Visual attacks: In these types of attacks with a assistance of a computer or through inspection with a naked eye it reveal the presence of hidden information, which helps to separate the image into bit planes for further more analysis. (b) Statistical attacks: These types of attacks are more powerful and successful, because they reveal the smallest alterations in an images statistical behavior. Statistical attacks can be further divided into (i) Passive attack and (ii) Active attack. Passive attacks involves with identifying presence or absence of a covert message or embedding algorithm used etc. Mean while active attacks is used to investigate embedded message length or hidden message location or secret key used in embedding. (c) Structural attacks: The format of the data files changes as the data to be hidden is embedded; identifying this characteristic structure changes can help us to find the presence of image.

A. Types of Image Based Steganalysis

Steganalysis can be regarded as a two-class pattern classification problem which aims to determine whether a testing medium is a cover medium or a stego one. A **targeted steganalysis** technique works on a specific type of stego-system and sometimes limited on image format. By studying and analyzing the embedding algorithm, one can find image statistics that change after embedding. The results from most targeted steganalysis techniques are very accurate but on the other hand, the techniques are inflexible since most of the time there is no path to extend them to other embedding algorithms. Also, when a targeted steganalysis is successful, thus having a higher probability than random guessing, it helps the steganographic techniques to expand and become more secure. A **blind steganalysis** technique is designed to work on all types of embedding techniques and image formats. In a few words, a blind steganalysis algorithm 'learns' the difference in the statistical properties of pure and stego images and distinguishes between them. The 'learning' process is done by training the machine on a large image database. Blind techniques are usually less accurate than targeted ones, but a lot more expandable. **Semi-blind steganalysis** works on a specific range of different stego-systems. The range of the stego-systems can depend on the domain they embed on, i.e. spatial or transform.

B. Some Specific Approaches of Image Based Steganalysis

A specific steganalytic method often takes advantage of the insecure aspect of a steganographic algorithm. Some specific steganalytic methods for attacking the steganographic schemes are introduced in this section.

a. **Attacking LSB steganography**: LSB steganography has been one of the most important spatial steganographic techniques. Accordingly, much work has been done on steganalyzing LSB steganography in the initial stage of the development of steganalysis. And many steganalytic methods toward LSB steganography have been proved most successful, such as Chi-square statistical attack [61, 62], RS analysis [63], sample pair analysis (SPA) analysis [64], weighted stego (WS) analysis [65], and structural steganalysis [66, 67], etc.

b. **Attacking LSB Matching Steganography**: It may be noted that the equal trend of the frequency of occurrence of PoVs no longer exists for LSB matching steganography. Thus many steganalytic methods toward LSB steganography turn out to be invalid. LSB matching, or more general ±k steganography, may be modeled in the context of additive noise independent of the cover image. The effect of additive noise steganography to the image histogram is equivalent to a convolution of the histogram of the cover image and the stego-noise PMF. It may be analyzed more conveniently in the frequency domain [68].

c. **Attacking Stochastic Modulation Steganography**: In [69] it has shown that the horizontal pixel difference histogram of a natural image can be modeled as a generalized Gaussian distribution (GGD). However, as stated in stochastic modulation steganography adds stego-noise with a specific probability distribution into the cover image to embed secret message bits. The embedding effect of adding stego-noise may disturb the distribution of the cover natural image. A quantitative approach to steganalyse stochastic modulation steganography was presented in [70, 71].

d. **Attacking the BPCS Steganography**: In BPCS steganography, the binary patterns of data-blocks are random and it is observed that the complexities of the data-blocks follow a Gaussian distribution with the mean value at 0.5 [72]. For some high significant bit-planes (e.g., the most significant bit-plane to the 5th significant bit-plane) in a cover image, the binary patterns of the image blocks are not random and thus the complexities of the image blocks do not follow a Gaussian distribution.

e. **Attacking the Prediction Error Based Steganography**: If there is no special scheme to prevent Wendy retrieving the correct prediction values, it is quite easy for Wendy to detect the steganographic method which utilizes prediction errors for hiding data, such as PVD steganography. Zhang et al. [73] proposed a method for attacking PVD steganography based on observing the histogram of the prediction errors.

f. **Attacking the MBNS Steganography**: It's hard to observe any abnormality between a cover image and its MBNS stego image through the histogram of pixel values and the histogram of pixel prediction errors. In [74] the authors observed and illustrated that given any base value, more small symbols are generated than large symbols in the process of converting binary data to symbols. Since the remainders of the division of pixel values by bases are equal to the symbols, the conditional probability $P_{D|B}$ can be used to discriminate the cover images and stego images, where B and D denote the random variable of the base and the remainder, respectively.

g. **Attacking QIM/DM**: The issue in steganalysis of QIM/DM has been formulated into two sub-issues by Sullivan et al. [75]. One is to distinguish the standard QIM stego objects from the plain-quantized (quantization without message embedding) cover objects. Another is to differentiate the DM stego objects from the unquantized cover objects.

h. **Attacking the F5 Algorithm**: Some crucial characteristics of the histogram of DCT coefficients, such as the monotonicity and the symmetry, are preserved by the F5 algorithm. But

F5 does modify the shape of the histogram of DCT coefficients. This drawback is employed by Fridrich et al. [76] to launch an attack against F5.

i. **Attacking OutGuess**: OutGuess preserves the shape of the histogram of DCT coefficients and thus it may not be easy to employ a quantitative steganalyzer to attack OutGuess with the statistics of DCT coefficients as that in attacking F5. Fridrich et al. [77] found a new path to detect OutGuess quantitatively by measuring the discontinuity along the boundaries of 8x8 JPEG grid. A spatial statistical feature, named blockiness, for an image has been proposed. It is observed that the blockiness linearly increases with the number of altered DCT coefficients. Suppose that some data are embedded into an input image. If the input image is innocent, the change rate of the blockiness between the input image and the embedded one will be large. If the input image already contains some data, the change rate will be smaller. The change rate of the blockiness can be used to estimate the embedding rate.

j. **Attacking MB**: MB steganography uses a generalized Cauchy distribution model to control the data embedding operation. Therefore, the histogram of the DCT coefficients will fit the generalized Cauchy distribution well in a stego image. Bohme and Westfeld [78] observed that the histogram of the DCT coefficients in a natural image is not always conforming the distribution. There exist more outlier high precision bins in the histogram in a cover image than in a stego image. Judging from the number of outlier bins, cover images and stego images can be differentiated.

k. **Attacking YASS**: The locations of the H-blocks of YASS are determined by a key, which is not available to Wendy. Therefore, it may not be straightforward for Wendy to observe the embedding artifacts. Li et al. [79] proposed a method for attacking the YASS.

C. Universal Approaches

Unlike specific steganalytic methods which require knowing the details of the targeted steganographic methods, universal steganalysis [80] requires less or even no such priori information. A universal steganalytic approach usually takes a learning based strategy which involves a training stage and a testing stage. The process is illustrated in Figure below.

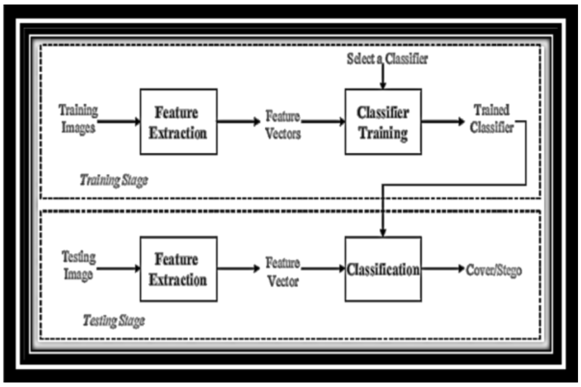


Fig. 6. The process of a universal steganalytic method

During the process, a feature extraction step is used in both training and testing stage. Its function is to map an input image from a high-dimensional image space to a low- dimensional feature space. The aim of the training stage is to obtain a trained classifier. Many effective classifiers, such as Fisher linear discriminant (FLD), support vector machine (SVM), neural network (NN), etc., can be selected. Decision boundaries are formed by the classifier to separate the feature space into positive regions and negative regions with the help of the feature vectors extracted from the training images. In the testing stage, with the trained classifier that has the decision boundaries, an image under question is classified according to its feature vector's domination in the feature space. If the feature vector locates in a region where the classifier is labeled as positive, the testing image is classified as a positive class (stego image). Otherwise, it is classified as a negative class (cover image). In the following, some typical universal steganalytic features has been discussed.

a. **Image Quality Feature**: Steganographic schemes may more or less cause some forms of degradation to the image. Objective image quality measures (IQMs) are quantitative metrics based on image features for gauging the distortion. The statistical evidence left by steganography may be captured by a group of IQMs and then exploited for detection [81]. In order to seek specific quality measures that are sensitive, consistent and monotonic to steganographic artifacts and distortions, the analysis of variance (ANOVA) technique is exploited and the ranking of the goodness of the metrics is done according to the F-score in the ANOVA tests. And the identified metrics can be defined as feature sets to distinguish between cover images and stego images.

b. **Calibration Based Feature**: Fridrich et al. [82] applied the feature-based classification together with the concept of calibration to devise a blind detector specific to JPEG images. Here the calibration means that some parameters of the cover image may be approximately recovered by using the stego image as side information. As a result, the calibration process increases the features' sensitivity to the embedding modifications while suppressing image-to-image variations. Applying calibration to the Markov process based features described in [83] and reducing their dimension, Pevny et al. merged the resulting feature sets to produce a 274-dimensional feature vector [84]. The new feature set is then used to construct a multi-classifier capable of assigning stego images to six popular steganographic algorithms.

c. **Moment Based Feature**: The impact of steganography to a cover image can be regarded as introducing some stego-noise. As noise is added, some statistics of the image may be changed. It is effective to observe these changes in wavelet domain. Lyu and Farid [85] used the assumption that the PDF of the wavelet subband coefficients and that of the prediction error of the subband coefficients would change after data embedding. In ref. [68], a 3-level wavelet decomposition, the first four PDF moments, i.e., mean, variance, skewness, and kurtosis, of the subband coefficients at each high-pass orientation (horizontal, vertical and diagonal direction) of each level are taken into consideration as one set of features. The same kinds of PDF moments of the difference between the logarithm of the subband coefficients and the logarithm of the coefficients' cross-subband linear predictions at each high-pass orientation of each level are computed as another set of features. These two kinds of features provide satisfactory results when the embedding rate is high.

d. **Correlation Based Feature**: Data embedding may disturb the local correlation in an image. Here the correlation is mainly referred to the inter-pixel dependency for a spatial image, and the intra-block or inter-block DCT coefficient dependency for a JPEG image. Sullivan et al. [86] modeled the inter-pixel dependency by Markov chain and depicted it by a gray-level co-occurrence matrix (GLCM) in practice.

TEXT STEGANOGRAPHY TECHNIQUES

Text steganography can be broadly classified into three types- format-based, random and statistical generations and Linguistic method.

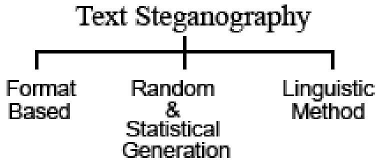


Fig. 7. Three broad categories of text steganography

A. **Format-based methods** use and change the formatting of the cover-text to hide data. They do not change any word or sentence, so it does not harm the 'value' of the cover-text. A format-based text steganography method is open space method [87]. In this method extra white spaces are added into the text to hide information. These white spaces can be added after end of each word, sentence or paragraph. A single space is interpreted as"0" and two consecutive spaces are interpreted as" 1". Although a little amount of data can be hidden in a document, this method can be applied to almost all kinds of text without revealing the existence of the hidden data. Another two format-based methods are word shifting and line shifting. In word shifting method, the horizontal alignments of some words are shifted by changing distances between words to embed information [88]. These changes are hard to interpret because varying distances between words are very common in documents. Another method of hiding information in manipulation of white spaces between words and paragraph [89].In line shifting method, vertical alignments of some lines of the text are shifted to create a unique hidden shape to embed a message in it [90].

B. **Random and statistical generation methods** are used to generate cover-text automatically according to the statistical properties of language. These methods use example grammars to produce cover-text in a certain natural language. A probabilistic context-free grammar (PCFG) is a commonly used language model where each transformation rule of a context- free grammar has a probability associated with it [91]. A PCFG can be used to generate word sequences by starting with the root node and recursively applying randomly chosen rules. The sentences are constructed according to the secret message to be hidden in it. The quality of the generated stego-message depends directly on the quality of the grammars used. Another approach to this type of method is to generate words having same statistical properties like word length and letter frequency of a word in the original message. The words generated are often without of any lexical value.

C. **Linguistic method**: The linguistic method [92] considers the linguistic properties of the text to modify it. The method uses linguistic structure of the message as a place to hide information. Syntactic method is a linguistic steganography method where some punctuation signs like comma (,) and full-stop (.) are placed in proper places in the document to embed a data. This method needs proper identification of places where the signs can be inserted. Another linguistic steganography method is semantic method. In this method the synonym of words for some pre-selected are used. The words are replaced by their synonyms to hide information in it.

D. Other methods

Many researchers have suggested many methods for hiding information in text besides above three categories such as feature coding, text steganography by specific characters in words, abbreviations etc. [93] or by changing words spelling [94].

TEXT BASED STEGANALYSIS

The usage of text media, as a cover channel for secret communication, has drawn more attention [95]. This attention in turn creates increasing concerns on text steganalysis. At present, it is harder to find secret messages in texts compared with other types of multimedia files, such as image, video and audio [96-101]. In general, text steganalysis exploits the fact that embedding information usually changes some statistical properties of stego texts; therefore it is vital to perceive the modifications of stego texts. Previous work on text steganalysis could be roughly classified into three categories: format- based [102, 103], invisible character-based [104-106] and linguistics, respectively. Different from the former two categories, linguistic steganalysis attempts to detect covert messages in natural language texts. In the case of linguistic steganography, lexical, syntactic, or semantic properties of texts are manipulated to conceal information while their meanings are preserved as much as possible[107].Due to the diversity of syntax and the polysemia of semantics in natural language, it is difficult to observe the alterations in stego texts. So far, many linguistic steganalysis methods have been proposed. In these methods, special features are designed to extend semantic or syntactical changes of stego texts. For example , Z.L. Chen[108] et al. designed the N-window mutual information matrix as the detection feature to detect semantic steganagraphy algorithms. Furthermore, they used the word entropy and the change of the word location as the semantic features [109,110], which improved the detection rates of their methods. Similarly, C.M. Taskiran et al [111] used the probabilistic context-free grammar to design the special features in order to attack on syntax steganography algorithms. In the work mentioned above, designed features strongly affect the final performances and they can merely reveal local properties of texts. Consequently, when the size of a text is large enough, differences between Natural texts (NTs) and Stego texts (STs) are evident, thus the detection performances of the mentioned methods are acceptable. Whereas, when the sizes of texts become small, the detection rates decrease dramatically and can not be satisfied for applications. In addition, some steganographic tools have been improved in the aspects of semantic and syntax for better camouflage [112]. Therefore, linguistic steganalysis still needs further research to resolve these problems. Some more work on Text Steganalysis has been discussed below.

A. Linguistic Steganalysis Based on Meta Features and Immune Mechanism [148]

Linguistic steganalysis depends on efficient detection features due to the diversity of syntax and the polysemia of semantics in natural language processing. This paper presents a novel linguistics steganalysis approach based on meta features and immune clone mechanism. Firstly, meta features are used to represent texts. Then immune clone mechanism is exploited to select appropriate features so as to constitute effective detectors. Our approach employed meta features as detection features, which is an opposite view from the previous literatures. Moreover, the immune training process consists of two phases which can identify respectively two kinds of stego texts. The constituted detectors have the capable of blind steganalysis to a certain extent. Experiments show that the proposed approach gets better performance than typical existing methods, especially in detecting short texts. When sizes of texts are confined to 3kB, detection accuracies have exceeded 95.

B. Research on Steganalysis for Text Steganography Based on Font Format[149]

In the research area of text steganography, algorithms based on font format have advantages of great capacity, good imperceptibility and wide application range. However, little work on steganalysis for such algorithms has been reported in the literature. Based on the fact that the statistic features of font format will be changed after using font-format-based steganographic algorithms, we present a novel Support Vector Machine-based steganalysis algorithm to detect whether hidden information exists or not. This algorithm can not only effectively detect the existence of hidden information, but also estimate the hidden information length according to variations of font attribute value. As shown by experimental results, the detection accuracy of our algorithm reaches as high as 99.3 percent when the hidden information length is at least 16 bits.

AUDIO STEGANOGRAPHY METHODOLOGY

In audio steganography, secret message is embedded into digitized audio signal which result slight alteration of binary sequence of the corresponding audio file. Moreover, audio signals have a characteristic redundancy and unpredictable nature that make them ideal to be used as a cover for covert communications to hide secret messages [150].

A. Audio Steganography Algorithms

In this section, the four major audio steganography algorithms: Low-bit encoding, Phase encoding, Spread spectrum coding and Echo data hiding are described.

a. **Low-bit Encoding**: In Low-bit encoding (e.g., [113]), the binary version of the secret data message is substituted with the least significant bit (LSB) of each sample of the audio cover file. Though this method is simple and can be used to embed larger messages, the method cannot protect the hidden message from small modifications that can arise as a result of format conversion or lossy compression.

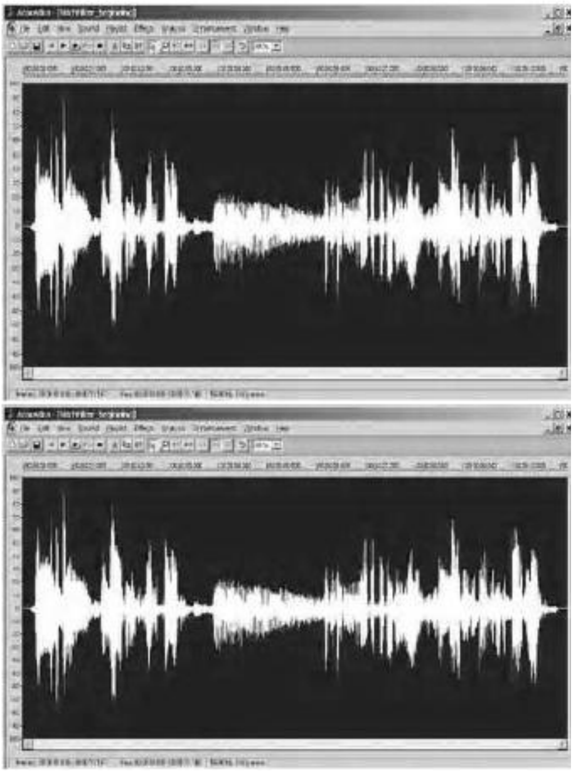


Fig. 8. The signal level comparisons between a WAV carrier file before (above) and after (below) the Low- bit Encoding.

b. **Phase Coding**: Phase coding [114] is based on the fact that the phase components of sound are not as perceptible to the human ear as noise is. Message bits are encoded as phase shifts in the phase spectrum of a digital signal. This leads to inaudible encoding in terms of the Signal-to-Perceived Noise Ratio (SPNR) and the secret message gets camouflaged in the audio signal, not detectable by the steganalysis methods based on SPNR. Thus, phase coding addresses the disadvantages of the noise-inducing methods of audio steganography. The sequence of steps involved in phase coding is as follows:

   i. The original audio signal is decomposed into smaller segments such that their length equals the size of the message that needs to be encoded.
   ii. A Discrete Fourier Transform (DCT) is then applied to each segment in order to create a phase matrix.
   iii. Phase differences between every pair of consecutive segments are computed.
   iv. Phase shifts between adjacent segments are identified. Although, the absolute phases of the segments can be altered, the relative phase differences between consecutive segments must be unchanged.
   v. The new phase matrix is created using the new phase of the signals first segment and the set of original phase differences.
   vi. Based on the new phase matrix and the original magnitude matrix, the sound signal is regenerated by using inverse DFT and then by joining the sound segments together. The receiver is mandated to know the message length in order to use DFT and extract the embedded message from the cover signal.

   A characteristic feature of phase coding is the low data transmission rate owing to the fact that the secret message is encoded only in the first segment of the audio signal. On the contrary, an increase in the length of the segment would have a ripple effect by altering the phase relations between the frequency components of the segment; thereby making detection easier. Hence, the phase coding method is normally used only when a small amount of data (e.g., watermark needs to be masked).

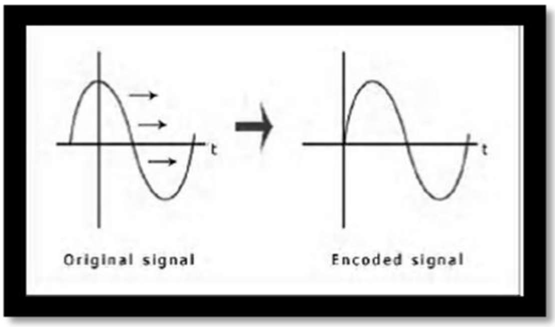


Fig. 9:The signals before and after Phase coding procedure

c. **Spread Spectrum Coding**: The basic Spread Spectrum (SS) coding method (e.g., [115]) randomly spreads the bits of the secret data message across the frequency spectrum of the audio signal. However, unlike LSB coding, the SS coding method spreads the secret message using a code that is independent of the actual cover signal. The SS coding method can perform better than LSB coding and phase coding techniques by virtue of a moderate data transmission rate coupled with a high level of robustness against steganalysis techniques. However, like the LSB coding method, the SS method can introduce noise to the audio file. This vulnerability can be tapped for steganalysis.

d. **Echo Hiding**: With echo hiding (e.g. [116]), information is embedded by introducing an echo into the discrete audio signal. Like SS coding, echo hiding allows for a higher data transmission rate and provides superior robustness when compared to the noise-inducing methods. To successfully hide the data, three parameters of the echo need to be altered: amplitude, decay rate and offset (delay time) from the original signal. The echo is not easily resolved as all the three parameters are set below the human audible threshold limit. Also, the offset is altered to represent the binary message to be hidden. The first offset value represents a one (binary), and the second offset value represents a zero (binary).

AUDIO STEGANALYSIS ALGORITHMS

Audio steganalysis is very difficult due to the existence of advanced audio steganography schemes and the very nature of audio signals to be high-capacity data streams necessitates the need for scientifically challenging statistical analysis [117].

A. Phase and Echo Steganalysis

Zeng et. al [118] proposed steganalysis algorithms to detect phase coding steganography based on the analysis of phase discontinuities and to detect echo steganography based on the statistical moments of peak frequency [119]. The phase steganalysis algorithm explores the fact that phase coding corrupts the extrinsic continuities of unwrapped phase in each audio segment, causing changes in the phase difference [120]. A statistical analysis of the phase difference in each audio segment can be used to monitor the change and train the classifiers to differentiate an embedded audio signal from a clean audio signal. The echo steganalysis algorithm statistically analyzes the peak frequency using short window extracting and then calculates the eighth high order center moments of peak frequency as feature vectors that are fed to a support vector machine, which is used as a classifier to differentiate between audio signals with and without data.

B. Universal Steganalysis based on Recorded Speech

Johnson et. al [121] proposed a generic universal steganalysis algorithm that bases it study on the statistical regularities of recorded speech. Their statistical model decomposes an audio signal (i.e., recorded speech) using basis functions localized in both time and frequency domains in the form of Short

Time Fourier Transform (STFT). The spectrograms collected from this decomposition are analyzed using non-linear support vector machines to differentiate between cover and stego audio signals. This approach is likely to work only for high-bit rate audio steganography and will not be effective for detecting low bit-rate embeddings.

C. Use of Statistical Distance Measures for Audio Steganalysis

H. Ozer et. al [122] calculated the distribution of various statistical distance measures on cover audio signals and stego audio signals vis--vis their versions without noise and observed them to be statistically different. The authors employed audio quality metrics to capture the anomalies in the signal introduced by the embedded data. They designed an audio steganalyzer that relied on the choice of audio quality measures, which were tested depending on their perceptual or non-perceptual nature. The selection of the proper features and quality measures was conducted using the (i) ANOVA test [123] to determine whether there are any statistically significant differences between available conditions and the (ii) SFS (Sequential Floating Search) algorithm that considers the inter-correlation between the test features in ensemble [124]. Subsequently, two classifiers, one based on linear regression and another based on support vector machines were used and also simultaneously evaluated for their capability to detect stego messages embedded in the audio signals. The features selected using the SFS test and evaluated using the support vector machines produced the best outcome. The perceptual- domain measures considered in [122] are: Bark Spectral Distortion, Modified Bark Spectral Distortion, Enhanced Modified Bark Spectral Distortion, Perceptual Speech Quality Measure and Perceptual Audio Quality Measure. The non-perceptual time-domain measures considered are: Signal-to-Noise Ratio, Segmental Signal-to-Noise Ratio and Czenakowski Distance. The non-perceptual frequency-domain measures considered are: Log-Likelihood Ratio, Log-Area Ratio, Itakura- Satio Distance, Cepstral Distance, Short Time Fourier Random Transform Distance, Spectral Phase Distortion and Spectral Phase Magnitude Distortion.

D. Audio Steganalysis based on Hausdorff Distance

The audio steganalysis algorithm proposed by Liu et. al [125] uses the Hausdorff distance measure [126] to measure the distortion between a cover audio signal and a stego audio signal. The algorithm takes as input a potentially stego audio signal x and its de-noised version x as an estimate of the cover signal. Both x and x are then subjected to appropriate segmentation and wavelet decomposition to generate wavelet coefficients [127] at different levels of resolution. The Haus- dorff distance values between the wavelet coefficients of the audio signals and their de-noised versions are measured. The statistical moments of the Hausdorff distance measures are used to train a classifier on the difference between cover audio signals and stego audio signals with different content loadings. However, the above approach of creating a reference signal via its own de-noised version causes content-dependent distortion. This can lead to a situation where the variations in the signal content itself can eclipse the classifier from detecting the distortions induced during data hiding. In [128], Avcibas proposed an audio steganalysis technique based on content- independent distortion measures. The technique uses a single reference signal that is common to all the signals to be tested.

E. Audio Steganalysis for High Complexity Audio Signals

More recently, Liu et. al [129] propose the use of stream data mining for steganalysis of audio signals of high complexity. Their approach extracts the second order derivative based Markov transition probabilities and high frequency spectrum statistics as the features of the audio streams. The variations in the second order derivative based features are explored to distinguish between the cover and stego audio signals. This approach also uses the Mel-frequency cepstral coefficients [117], widely used in speech recognition, for audio steganalysis.

VIDEO STEGANOGRAPHY METHODOLOGY

Several new approaches are studied in video data steganography literature. In this section, some of the most well-known approaches have been discussed. First of all, the most common method is Least Significant Bit method (LBS) which hide secret data into the least significant bits of the host video [130], [131] and [132]. This method is simple and can hide large data but the hidden data could be lost after some file transformations. Another well-known method which has been still researching is called Spread Spectrum [132], [133]. This method satisfies the robustness criterion [132]. The amount of hidden data lost after applying some geometric transformations is very little. The amount of hidden lost is also little even though the file is compressed with low bit-rate. This method satisfies another criterion is security [133]. There are also some introduced methods that base on multi-dimensional lattice structure, enable a high rate of data embedding, and are robust to motion compensated coding [131] or enable high quantity of hidden data and high quantity of host data by varying the number of quantization levels for data embedding [134]. Wang et. al. presented a technique for high capacity data hiding [151] using the Discrete Cosine Transform (DCT) transformation. Its main objective is to maximize the payload while keeping robustness and simplicity. Here, secret data is embedded in the host signal by modulating the quantized block DCT coefficients of I- frames. Lane proposed a vector embedding method [152] that uses a robust algorithm with video codec standard (MPEG-I and MPEG-II). This method embeds audio information to pixels of frames in host video. Moreover, a robust against rotation, scaling and translation (RST) method was also proposed for video watermarking [135]. In this method, secret information is embedded into pixels along the temporal axis within a Watermark Minimum Segment (WMS).Some more work on Video Steganalysis has been discussed below.

A. Application of BPCS Steganography to WAVELET Compressed Video[153]

This paper presents a steganography method using lossy compressed video which provides a natural way to send a large amount of secret data. The proposed method is based on wavelet compression for video data and bit-plane complexity segmentation (BPCS) steganography. In wavelet based video compression methods such as 3-

D set partitioning in hierarchical trees (SPIHT) algorithm and Motion- JPEG2000, wavelet coefficients in discrete wavelet transformed video are quantized into a bit-plane structure and therefore BPCS steganography can be applied in the wavelet domain. 3-D SPIHT-BPCS steganography and Motion- JPEG2000-BPCS steganography are presented and tested, which are the integration of 3- D SPIHT video coding and BPCS steganography, and that of Motion-JPEG2000 and BPCS, respectively. Experimental results show that 3-D SPIHT-BPCS is superior to Motion- JPEG2000-BPCS with regard to embedding performance.

B. An Optical Video Cryptosystem with Adaptive Steganography[154]

In this paper, an optical cryptosystem with adaptive steganography is proposed for video sequence encryption and decryption. The optical cryptosystem employs a double random phase encoding algorithm to encrypt and decrypt video sequences. The video signal is first transferred to RGB model and then separated into three channels: red, green, and blue. Each channel is encrypted by two random phase masks generated from session keys. For higher security, an asymmetric method is applied to cipher session keys. The ciphered keys are then embedded into the encrypted video frame by a content- dependent and low distortion data embedding technique. The key delivery is accomplished by hiding ciphered data into the encrypted video frame with a specific hiding sequence generated by the zero-LSB sorting technique. Experimental results show that the adaptive steganography has a better performance than the traditional steganography in the video cryptosystem.

C. A Secure Covert Communication Model based on VIDEO Steganography[155]

This paper presents a steganographic model which utilizes cover video files to conceal the presence of other sensitive data regardless of its format. The model presented is based on pixel-wise manipulation of colored raw video files to embed the secret data. The secret message is segmented into blocks prior to being embedded in the cover video. These blocks are then embedded in pseudo random locations. The locations are derived from a re-orderings of a mutually agreed upon secret key. Furthermore, the re-ordering is dynamically changed with each video frame to reduce the possibility of statistically identifying the locations of the secret message blocks, even if the original cover video is made available to the interceptor. The paper also presents a quantitative evaluation of the model using four types of secret data. The model is evaluated in terms of both the average reduction in Peak Signal to Noise Ratio (PSNR) compared to the original cover video; as well as the Mean Square Error (MSE) measured between the original and steganographic files averaged over all video frames. Results show minimal degradation of the steganographic video file for all types of data, and for various sizes of the secret messages. Finally, an estimate of the embedding capacity of a video file is presented based on file format and size.

D. Lossless Steganography on AVI File using Swapping Algorithm[156]

In this paper a comparative analysis between Joint Picture Expert Group (JPEG) image stegano and Audio Video Inter- leaved (AVI) video stegano by quality and size was performed. The authors propose to increase the strength of the key by using UTF-32 encoding in the swapping algorithm and lossless stegano technique in the AVI file. However, payload capacity is low.

E. A New Invertible Data Hiding in Compressed Videos or Images[157]

An adaptive invertible information hiding method for Moving Picture Expert Group (MPEG) video is proposed. Hidden data can be recovered without requiring the destination to have a prior copy of the covert video and the original MPEG video data can be recovered if needed. This technique works in frequency domain only. It has the advantages of low complexity and low visual distortion for covert communication applications. However, it suffers from low payload capacity.

VIDEO STEGANALYSIS METHODOLOGY

A. Video Steganalysis Exploring the Temporal Correlation between Frames

Budia et. al [136] proposed a technique for video steganalysis by using the redundant information present in the temporal domain as a deterrent against secret messages embedded by spread spectrum steganography. Their study, based on linear collusion approaches, is successful in identifying hidden watermarks bearing low energy with good precision. The simulation results also prove the superiority of the temporal- based methods over purely spatial methods in detecting the secret message.

B. Video Steganalysis based on Asymptotic Relative Efficiency (ARE)

Jainsky et. al [137] proposed a video steganalysis algorithm that incorporates asymptotic relative efficiency [138]-based detection. This algorithm is more suited for applications in which only a subset of the video frames are watermarked with the secret message and not all of them. The stego video signal is assumed to consist of a sequence of correlated image frames and obeys a Gauss-Markov temporal correlation model. Steganalysis comprises of a signal processing phase followed by the detection phase. The signal processing phases emphasizes the presence of hidden information in the sequence of frames using a motion estimation scheme. The detection phase is based on asymptotic relative efficiency (ARE) [138], wherein both the cover-video and the watermarked secret message are considered to be random variables. The ARE-based detector is memory less in nature and uses an adaptive threshold for the video characteristics that are used to differentiate a cover- video from a stego-video. The video characteristics (e.g. size, standard deviation and correlation coefficient) considered are those that vary from one sequence of frames to another. The number of frames in a sequence to be analyzed at each passing into the detector was also considered as a parameter for detection.

C. Video Steganalysis based on Mode Detection

Su et. al [139] propose a video steganalysis algorithm that targets the Moscow State University (MSU) stego video [140] software, which is one of the very few available video steganographic tools that can embed any file in AVI (Audio Video Interleave) format and the embedded messages can be extracted correctly even after the stego-videos are compressed. The steganalysis algorithm uses the correlation between adjacent frames and detects a special distribution mode across the frames. The embedding unit is a 32 x 32 pixel block and the four 16 x 16 blocks within a unit form a chessboard-like distribution pattern. After correlation analysis between adjacent frames, if the ratio of number of 32 x 32 pixel blocks with a specific distribution mode to the total number of 32 x 32 pixel blocks in a video sequence is determined to be above a threshold value, then the video signal is predicted to carry an embedded message.

D. Video Steganalysis based on Spatial and Temporal Prediction

Pankajakshan and Ho propose a video steganalysis scheme [141] for the MPEG video coding standard in which a given frame is predicted from its neighboring reference frames using motion compensation [142]. The MPEG coding scheme supports two types of predicted frames: the Pframes (uses a single past frame as the reference frame) and the B-frames (uses a past frame and a future frame as reference frames). The prediction-error frames (PEFs) corresponding to the Pand B-frames are then coded using transform coding techniques. The PEFs exhibit spatiotemporal correlation between the adjacent frames. The PEFs of a test video signal are decomposed using the 3-level DWT (Discrete Wavelet Transform) method and the first three moments of the characteristic functions (CFs) in each of the sub-bands are computed. The resulting feature vectors are fed to train a pattern classifier to discriminate between the stego and non-stego videos.

E. Other Video Steganalysis Algorithms

Kancherla and Mukkamala [143] propose a video steganalysis method using neural networks and support vector machines to detect hidden information by exploring the spatial and temporal redundancies. Zhang et. al [144] propose a steganal- ysis approach against video steganography based on spread spectrum techniques. Their model assumes the cover-video and the hidden data are independent and uses the probability mass function of the inter-frame difference signal to reveal the aliasing effect (distortion) caused by embedding data. Liu et. al [145] propose an inter frame correlation based compressed video steganalysis algorithm that employs collusion to extract features from similar video frames of a single scene and uses a feed forward neural network capable of non-linear feature mapping as the blind classifier.

CONCLUSION

In this paper, authors have analyzed the steganalysis algorithms available for four commonly used domains of steganography i.e. Image, Text, Audio and Video. Image steganalysis algorithms can be classified into two broad categories: Specific and Universal. The Specific steganalysis algorithms are based on the format of the digital image (e.g. GIF, BMP and JPEG formats) and depend on the respective steganography algorithm used. The Universal image steganalysis algorithms work on any steganography algorithm, but require more complex computation and higher-order statistical analysis. Work on text steganalysis could be roughly classified into three categories: format-based, invisible character-based and linguistics, respectively. The audio steganalysis algorithms exploit the variations in the characteristic features of the audio signal as a result of message embedding. The video steganalysis algorithms that simultaneously exploit both the temporal and spatial redundancies have been proposed and shown to be effective. Thus it may be concluded that steganalysis algorithms developed for one cover media may not be effective for another media. This paper gives an overview of steganography and steganalysis methods available in four common cover areas. The research to device strong steganographic and steganalysis technique is a continuous process and still going on.

REFERENCES

[1] Gustavus J. Simmons, "The Prisoners' Problem and the Subliminal Channel", in Proceedings of CRYPTO '83, pp 51-67. Plenum Press (1984).

[2] P. Wayner, “*Strong Theoretical Steganography*”, Cryptologia, XIX(3), July 1995, pp. 285-299.

[3] J.T. Brassil, S. Low, N.F. Maxemchuk, and L. O’Gorman, "Electronic Marking and Identification Techniques to Discourage Document Copying", *IEEE Journal on Selected Areas in Communications*, vol. 13, Issue. 8, October 1995, pp. 1495-1504.

[4] “Stretching the Limits of Steganography", RJ Anderson, in Information Hiding, Springer Lecture Notes in Computer Science v 1174 (1996) pp 39-48.

[5] Kahn, The Codebreakers - the comprehensive history of secret communication from ancient times to the Internet, Scribner, New York (1996).

[6] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding", *IBM Systems Journal*, vol. 35, Issues 3&4, 1996, pp. 313-336.

[7] Scott Craver, "On Public-key Steganography in the Presence of an Active Warden," in Proceedings of 2nd International Workshop on Information Hiding, April 1998, Portland, Oregon, USA. pp. 355 - 368.

[8] Ross J. Anderson and Fabien A.P. Petitcolas, "On the limits of steganography," IEEE Journal on Selected Areas in Communications (J-SAC), Special Issue on Copyright & Privacy Protection, vol. 16 no. 4, pp 474-481, May 1998.

[9] N. F. Johnson and S. Jajodia, "Steganography: seeing the unseen," IEEE Computer.,Feb., 26-34 (1998).

[10] L. M. Marvel, C. G. Boncelet, Jr. and C. T. Retter, "Spread spectrum image steganography," IEEE Trans. on Image Processing, 8(8), 1075-1083 (1999).

[11] Digital Watermarking :A Tutorial Review S.P.Mohanty ,1999.

[12] J. Shi and J. Malik, "Normalized cuts and image segmentation.,"IEEE Trans. PAMI, vol. 22, no. 8, pp. 888-905, 2000.

[13] Y. K. Lee and L. H. Chen, "High capacity image steganographic model," IEE Proc.-Vision, Image and Signal Processing, 147(3), 288-294 (2000).

[14] Analysis of LSB Based Image Steganography Techniques ,R. Chandramouli, Nasir Memon, Proc. IEEE ICIP, 2001.

[15] M.Chapman, G. Davida, and M. Rennhard, “A Practical and Effective Approach to Large-Scale Automated Linguistic Steganography”, *Proceedings of the Information Security Conference*, October 2001, pp. 156-165.

[16] An Evaluation of Image Based Steganography Methods,Kevin Curran, Kran Bailey, International Journal of Digital Evidence,Fall 2003.

[17] G. Doërr and J.L. Dugelay, "A Guide Tour of Video Watermarking", *Signal Processing: Image Communication*, vol. 18, Issue 4, 2003, pp. 263-282.

[18] K. Gopalan, "Audio steganography using bit modification", *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, (ICASSP '03)*, vol. 2, 6-10 April 2003, pp. 421-424.

[19] M. Niimi, S. Minewaki, H. Noda, and E.Kawaguchi, "A Framework of Text-based Steganography Using SD-Form Semantics Model", *Pacific Rim Workshop on Digital Steganography 2003*, Kyushu Institute of Technology, Kitakyushu, Japan, July 3-4, 2003.

[20] Y. Kim, K. Moon, and I. Oh, "A Text Watermarking Algorithm based on Word Classification and Inter-word Space Statistics", *Proceedings of the Seventh International Conference on Document Analysis and Recognition (ICDAR'03),* 2003, pp. 775–779.

[21] Silvia Torres Maya,Mariko Nakano and Ruben Vazquez Medina "Robust Steganography using Bit Plane Complexity Segmentation" 1st International Conferenceon Electrical and Electronics Engineering ,2004.

[22] A.M. Alattar and O.M. Alattar, "Watermarking electronic text documents containing justified paragraphs and irregular line spacing ", *Proceedings of SPIE - Volume5306, Security, Steganography, and Watermarking of Multimedia Contents VI*, June 2004, pp- 685-695.

[23] G. Doërr and J.L. Dugelay, "Security Pitfalls of Frameby-Frame Approaches to Video Watermarking", *IEEE Transactions on Signal Processing*, Supplement on Secure Media, vol. 52, Issue 10, 2004, pp. 2955-2964.

[24] T Mrkel,JHP Eloff and MS Olivier ."An Overview of Image Steganography,"in proceedings of the fifth annual Information Security South Africa Conference ,2005

[25] M.H. Shirali-Shahreza and M. Shirali-Shahreza, "Text Steganography in Chat", *Proceedings of the Third IEEE/IFIP International Conference in Central Asia on Internet the Next Generation of Mobile, Wireless and Optical Communications Networks (ICI 2007),* Tashkent, Uzbekistan, September 26-28, 2007.

[26] L.Y. Por and B. Delina, "Information Hiding: A New Approach in Text Steganography", *7th WSEAS International Conference on Applied Computer & Applied Computational Science,* April 2008, pp- 689-695.

[27] MohammadShirali-Shahreza: "Text Steganography by Changing Words Spelling" at ICACT 2008.

[28] "Study of Secure Steganography model" by Souvik Bhattacharyya and Gautam Sanyal at the proceedings of "International Conference on Advanced Computing & Communication Technologies (ICACCT-2008),Nov, 2008, Panipat, India"

[29] **"**An Image based Steganography model for promoting Global Cyber Security" by Souvik Bhattacharyya and Gautam Sanyal at the proceedings of "International Conference on Systemics,Cybernetics and Informatics (ICSCI-2009),Jan, 09,Hyderabad,India."

[30] **"**Implementation and Design of an Image based Steganographic model" by Souvik Bhattacharyya and Gautam Sanyal at the proceedings of " IEEE International Advance Computing Conference "(IACC-2009)"

[31] A Novel Approach to Develop a Secure Image based Steganographic Model using Integer Wavelet Transform" at the proceedings of International Conference on Recent Trends in Information, Telecommunication and Computing (ITC 2010)" by Souvik Bhattacharyya, Avinash Prasad Kshitij and Gautam Sanyal. (Indexed by IEEE Computer Society).

[32] A Steganographic Method for Images using Pixel Intensity Value (PIV))" by Souvik Bhattacharyya and Gautam Sanyal at the proceedings of National Conference on Computing & Systems 2010 held at The University of Burdwan in January 2010.

[33] "Hiding Data in Images Using Pixel Mapping Method (PMM) by Souvik Bhattacharyya and Gautam Sanyal accepted as a regular research paper at SAM'10 - 9th annual Conference on Security and Management under The 2010 World Congress in Computer Science, Computer Engineering, and Applied Computing to be held on July 12-15, 2010, USA (The proceedings will be indexed in Inspec / IET / The Institute for Engineering and Technology; DBLP / Computer Science Bibliography, and others.)

[34] Y. Hsiao. C.C. Chang. and C.-S. Chan. Finding optimal least significant- bit substitution in image hiding by dynamic programming strategy. Pattern Recognition, 36:1583–1595, 2003

[35] C.K. Chan. and L. M.Cheng. Hiding data in images by simple lsb substitution. Pattern Recognition, 37:469–474, 2004.

[36] Y. K. Lee. and L. H.Chen. High capacity image steganographic model. IEE Proc.-Vision, Image and Signal Processing, 147:288–294, 2000.

[37] C.F. Lin. R.Z. Wang. and J.C. Lin. Image hiding by optimal lsb substitution and genetic algorithm. Pattern Recognition, 34:671–683, 2001.

[38] B.C. Nguyen, S.M. Yoon et H.-K. Lee : Multi bit plane image steganography. Proc. Digital Watermarking, 5th International Workshop, IWDW 2006, volume 4283 de Lecture Notes in Computer Science, pages 61–70, Jeju Island, Korea, novembre 2006. Springer**.**

[39] D.C. Wu. and W.H. Tsai. A steganographic method for images by pixel value differencing. Pattern Recognition Letters, 24:1613–1626, 2003.

[40] Ahmad T. Al-Taani. and Abdullah M. AL-Issa. A novel steganographic method for gray-level images. International Journal of Computer, Information, and Systems Science, and Engineering, 3, 2009.

[41] Potdar V.and Chang E. Gray level modification steganography for secret communication. In IEEE International Conference on Industria l Informatics. pages 355–368, Berlin, Germany, 2004.

[42] Xinpeng Zhang and Shuozhong Wang. Steganography using multiple-base notational system and human vision sensitivity. IEEE Signal Processing Letters, 12(1):67{70, 2005.

[43] B. Chen and G.W. Wornell. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. IEEE Transactions on Information Theory, 47(4):1423{1443, 2001.

[44] P Huang. K.C. Chang., C.P Chang. and T.M Tu. A novel image steganography method using tri-way pixel value differencing. Journal of Multimedia, 3, 2008.

[45] Derek Upham. Jsteg, http://zooid.org/~paul/crypto/jsteg/..

[46] Allan Latham. Jphide, http://linux01.gwdg.de/~alatham/ stego.html.

[47] Andrew Westfeld. F5-a steganographic algorithm: high capacity despite better steganalysis. In Proceedings of the 4th Information Hiding Workshop, volume 2137 of LNCS, pages 289{302. Springer, 2001.

[48] J. Fridrich, M. Goljan, and D. Hogea. Attacking the outguess. In Proceedings of 2002 ACM Workshop on Multimedia and Security, pages 3{6. ACM Press, 2002.

[49] A. Westfeld and A. P¯tzmann. Attacks on steganographic systems - breaking the steganographic utilities ezstego, jsteg, steganos, and s-tools-and some lessons learned. In Proceedings of the 3rd Information Hiding Workshop, volume 1768 of LNCS, pages 61{76. Springer, 1999.

[50] K. Solanki, A. Sarkar, and B. S. Manjunath. Yass: Yet another steganographic scheme that resists blind steganalysis. In Proceedings of the 9th Information Hiding Workshop, volume 4567 of LNCS, pages 16{31. Springer, 2007.

[51] J. Fridrich. Feature-based steganalysis for jpeg images and its implications for future design of steganographic schemes. In Proceedings of the 6th Information Hiding Workshop, volume 3200 of LNCS, pages 67{81. Springer, 2004.

[52] Tom¶a·s Pevn¶y and Jessica Fridrich. Merging markov and dct features for multi-class jpeg steganalysis. In Proceedings of SPIE: Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, volume 6505, pages 3{14. SPIE, 2007.

[53] Lifang Yu, Yao Zhao, Rongrong Ni, and Yun Q. Shi. A high-performance yass-like scheme using randomized big-blocks. In Proceedings of the IEEE International Conference on Multimidea & Expo (ICME 2010), 2010.

[54] Fangjun Huang, Jiwu Huang, and Yun Qing Shi. An experimental study on the security performance of yass. IEEE Transactions on Information Forensics and Security, 5(3):374 { 380, 2010

[55] Ali Al-Ataby and Fawzi Al-Naima. A modified high capacity image steganography technique based on wavelet transform. The International Arab Journal of Information Technology, 7:358–364, 2010.

[56] Bo Yang and Beixing Deng. Steganography in gray images using wavelet. In Proceedings of ISCCSP 2006.

[57] Po-Yueh Chen and Hung-Ju Lin. A dwt based approach for image steganography. International Journal of Applied Science and Engineering, 4:275–290, 2006.

[58] Dr.S.T.Gandhe K.T.Talele and Dr.A.G.Keskar. Steganography security for copyright protection of digital images using dwt.

(IJCNS) International Journal of Computer and Network Security, 2:21–26, 2010.

[59] V. Kumar and D. Kumar. Performance evaluation of dwt based image steganography. In Proceedings of Advance Computing Conference (IACC), 2010 IEEE 2nd International, pages 223–228, 2010.

[60] H S Manjunatha Reddy and K B Raja. High capacity and security steganography using discrete wavelet transform. International Journal of Computer Science and Security (IJCSS), 3:462–472.

[61] A. Westfeld and A. P¯tzmann. Attacks on steganographic systems - breaking the steganographic utilities ezstego, jsteg, steganos, and s-tools-and some lessons learned. In Proceedings of the 3rd Information Hiding Workshop, volume 1768 of LNCS, pages 61{76. Springer, 1999.

[62] Niels Provos and Peter Honeyman. Detecting steganographic content on the internet. In Proceedings of NDSS'02: Network and Distributed System Security Symposium, pages 1{13. Internet Society, 2002.

[63] Jessica Fridrich, Miroslav Goljan, and Rui Du. Reliable detection of lsb steganography in color and grayscale images. In Proceedings of 2001 ACM workshop on Multimedia and security: new challenges, pages 27{30. ACM Press, 2001.

[64] S. Dumitrescu, X. L. Wu, and Z. Wang. Detection of lsb steganography via sample pair analysis. IEEE Transactions on Signal Processing, 51(7):1995{2007, 2003.

[65] J. Fridrich and M. Goljan. On estimation of secret message length in lsb steganography in spatial domain. In IS&T/SPIE Electronic Imaging: Security, Steganography, and Watermarking of Multimedia Contents VI, volume 5306, pages 23{34. SPIE, 2004.

[66] D. Ker. Fourth-order structural steganalysis and analysis of cover assumptions. In IS&T/SPIE Electronic Imaging: Security, Steganography, and Watermarking of Multimedia Contents VIII, volume 6072, pages 1{14. SPIE, 2006.

[67] A. D. Ker. A general framework for the structural steganalysis of lsb replacement. In Proceedings of the 7th Information Hiding Workshop, volume 3727 of LNCS, pages 296{311. Springer, 2005.

[68] J. Harmsen and W. Pearlman. Steganalysis of additive noise modelable information hiding. In IS&T/SPIE Electronic Imaging: Security, Steganography, and Watermarking of Multimedia Contents V, volume 5020, pages 131{142. SPIE, 2003.

[69] Jinggang Huang and David Mumford. Statistics of natural images and models. In Proceedings of IEEE Computer Society Conference on Computer Vision and Pattern Recognition, volume 1, pages 541{547, 1999.

[70] J. H. He, J. W. Huang, and G. P. Qiu. A new approach to estimating hidden message length in stochastic modulation steganography. In Proceedings of the 4th Internation Workshop on Digital Watermarking, volume 3710 of LNCS, pages 1{14. Springer, 2005.

[71] J. H. He and J. W. Huang. Steganalysis of stochastic modulation steganography. Science in China Series: F-Information Sciences, 49(3):273{285, 2006.

[72] M. Niimi, R. O. Eason, H. Noda, and E. Kawaguchi. Intensity histogram steganalysis in bpcs steganography. In IS&T/SPIE Electronic Imaging: Security and Watermarking of Multimedia Contents III, volume 4314, pages 555{564. SPIE, 2001.

[73] X. P. Zhang and S. Z. Wang. Vulnerability of pixel-value di®erencing steganography to histogram analysis and modi¯cation for enhanced security. Pattern Recognition Letters, 25(3):331{339, 2004.

[74] Bin Li, Yanmei Fang, and Jiwu Huang. Steganalysis of multiple-base notational system steganography. IEEE Signal Processing Letters, 15:493{496, 2008.

[75] K. Sullivan, Z. Bi, U. Madhow, S. Chandrasekaran, and B. S. Manjunath. Steganalysis of quantization index modulation data hiding. In Proceedings of 2004 IEEE International Conference on Image Processing, volume 2, pages 1165{1168, 2004.

[76] J. Fridrich, M. Goljan, and D. Hogea. Steganalysis of jpeg images: Breaking the f5 algorithm. In Proceedings of the 5th Information Hiding Workshop, volume 2578 of LNCS, pages 310{323. Springer, 2002.

[77] J. Fridrich, M. Goljan, and D. Hogea. Attacking the outguess. In Proceedings of 2002 ACM Workshop on Multimedia and Security, pages 3{6. ACM Press, 2002.

[78] R. BÄohme and A. Westfeld. Breaking cauchy model-based jpeg steganography with first order statistics. In Proceedings of the 9th European Symposium On Research in Computer Security, volume 3193 of LNCS, pages 125{140. Springer, 2004.

[79] Bin Li, Yun Q. Shi, and Jiwu Huang. Steganalysis of yass. In Proceedings of the 10th ACM workshop on Multimedia and security (MM&Sec'08), pages 139{148. ACM Press, 2008.

[80] X. Y. Luo, D. S.Wang, P.Wang, and F. L. Liu. A review on blind detection for image steganography. Signal Processing, 88(9):2138{2157, 2008.[67] I. Avcibas, N. Memon, and B. Sankur. Steganalysis using image quality metrics. IEEE Transactions on Image Processing, 12(2):221{229, 2003.

[81] I. Avcibas, N. Memon, and B. Sankur. Steganalysis using image quality metrics. IEEE Transactions on Image Processing, 12(2):221{229, 2003.

[82] J. Fridrich. Feature-based steganalysis for jpeg images and its implications for future design of steganographic schemes. In Proceedings of the 6th Information Hiding Workshop, volume 3200 of LNCS, pages 67{81. Springer, 2004.

[83] Y. Q. Shi, C. Chen, and W. Chen. A morkov process based approach to effective attacking jpeg steganography. In Proceedings of the 8th Information Hiding Workshop, volume 4437 of LNCS, pages 249{264. Springer, 2006.

[84] Tomas Pevny and Jessica Fridrich. Merging markov and dct features for multi-class jpeg steganalysis. In Proceedings of SPIE: Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, volume 6505, pages 3{14. SPIE, 2007.

[85] Lyu Siwei and H. Farid. Detecting hidden message using higher-order statistics and support vector machines. In Proceedings of the 5th Information Hiding Workshop, volume 2578 of LNCS, pages 131{142. Springer, 2002.

[86] K. Sullivan, U. Madhow, S. Chandrasekaran, and B. S. Manjunath. Steganalysis for markov cover data with applications to images. IEEE Transactions on Information Forensics and Security, 1(2):275{287, 2006.

[87] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding", IBM Systems Journal, vol. 35, Issues 3&4, 1996, pp. 313-336.

[88] Y. Kim, K. Moon, and I. Oh, "A Text Watermarking Algorithm based on Word Classification and Inter-word Space Statistics", Proceedings of the Seventh International Conference on Document Analysis and Recognition (ICDAR’03), 2003, pp. 775–779.

[89] L.Y. Por and B. Delina, “Information Hiding: A New Approach in Text Steganography”, 7th WSEAS International Conference on Applied Computer & Applied Computational Science, April 2008, pp- 689-695.

[90] A.M. Alattar and O.M. Alattar, "Watermarking electronic text documents containing justified paragraphs and irregular line spacing ", Proceedings of SPIE - Volume5306, Security, Steganography, and Watermarking of Multimedia Contents VI, June 2004, pp- 685-695.

[91] P. Wayner, “Strong Theoretical Steganography”, Cryptologia, XIX(3), July 1995, pp. 285-299.

[92] M. Niimi, S. Minewaki, H. Noda, and E.Kawaguchi, "A Framework of Text-based Steganography Using SD-Form Semantics Model", Pacific Rim Workshop on Digital Steganography 2003, Kyushu Institute of Technology, Kitakyushu, Japan, July 3-4, 2003.

[93] M.H. Shirali-Shahreza and M. Shirali-Shahreza, "Text Steganography in Chat", Proceedings of the Third IEEE/IFIP International Conference in Central Asia on Internet the Next Generation of Mobile, Wireless and Optical Communications Networks (ICI 2007), Tashkent, Uzbekistan, September 26-28, 2007.

[94] MohammadShirali-Shahreza: “Text Steganography by Changing Words Spelling” at ICACT 2008.

[95] F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn, “Information hiding - a survey”, Proceedings of the IEEE, Vol.87, No.7, pp.1062–1078, 1999.

[96] C. Kraetzer, J. Dittmann, “Pros and cons of melcepstrum based audio steganalysis using SVM classification”, The 9th International Workshop on Information Hiding, Saint Malo, France, pp.359–377, 2007.

[97] M.E. Choubassi, P. Moulin, “Noniterative algorithms for sensitivity analysis attacks”, IEEE Transactions on Information Forensics and Security, Vol.2, No.3, pp.113–126, 2007.

[98] O.H. Kocal, E. Avcibas, “Chaotic-type features for speech steganalysis”, IEEE Transactions on Information Forensics and Security, Vol.3, No.4, pp.651–661, 2008.

[99] Z.J. Wu, Y. Hu, X.X. Niu, H.X. Duan, X. Li, “Information hiding technique based speech secure communication over PSTN”, Chinese Journal of Electronics, Vol.15, No.1, pp.108–112, 2009.

[100]H. Shan, K. Darko, “An estimation attack on content-based video fingerprinting”, Transactions on Data Hiding and Multimedia Security II, Vol.4499, No.2007, pp.35–47, 2007.

[101]R. Bohme, “Weighted stego-image steganalysis for JPEG covers”, The 10th International Workshop on Information Hiding, Santa Barbara, California, USA, pp.178–194, 2008.

[102]L.J. Li, L.S. Huang, X.X. Zhao, W. Yang, Z.L. Chen, “A statistical attack on a kind of word-shift text-steganography”, The 4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Harbin, China, pp.1503–1507, 2008.

[103]L.Y. Xiang, X.M. Sun, G. Luo, C. Gan, “Research on steganalysis for text steganography based on font format”, The 3rd International Symposium on Information Assurance and Security, Manchester, United Kingdom, pp.490–495, 2007.

[104]J.W. Huang, X.M. Sun, H. Huang, G. Luo, “Detection of hidden information in webpages based on randomness”, The 3rd International Symposium on Information Assurance and Security, Manchester, United kingdom, pp.447–452, 2007.

[105]H.J. Huang, X.M. Sun, Z.H. Li, G. Sun, “Detection of steganographic information in tags of webpage”, The 2nd International Conference on Scalable Information Systems, Brussels, Belgium, pp.325–328, 2007.

[106]H.J. Huang, S.H. Zhong, X.M. Sun, “Steganalysis of information hidden in webpage based on higher-order statistics”, Proceedings of the International Symposium on Electronic Commerce and Security, ISECS 2008, Guangzhou, China, pp.957–960, 2008.

[107]M. Chapman, G.I. Davida, M. Rennhard, “A practical and effective approach to large scale automated linguistic steganography”, The 4th International Conference on Information and Communications Security, Venice, Italy, pp.156–165, 2007.

[108]Z.L. Chen, L.S. Huang, Z.Z. Yu, W. Yang, L.J. Li, X.L. Zheng, X.X. Zhao, “Linguistic steganography detection using statistical characteristics of correlations between words”, The 11th International Workshop on Information Hiding, Darmstadt, Germany, pp.224–235, 2008.

[109] Z.L. Chen, L.S. Huang, Z.S. Yu, X.X. Zhao, X.L. Zheng, “Effective linguistic steganography detection”, The 8th IEEE International Conference on Computer and Information Technology Workshops, Sydney, Australia, pp.224–229, 2008.

[110] Z.L. Chen, L.S. Huang, Z.S. Yu, L.J. Li, W. Yang, “A statistical algorithm for linguistic steganography detection based on distribution of words”, The 3rd International Conference on Availability, Security, and Reliability, Barcelona, Spain, pp.558–563, 2008.

[111]C.M. Taskiran, U. Topkara, M. Topkara, E.J. Delp, “Attacks on lexical natural language steganography systems”, Proceedings of SPIE International Society for Optical Engineering, Society of Photo-Optical Instrumentation Engineers, San Jose, USA, pp.97–105, 2006.

[112]K. Bennett, “Linguistic steganography: Survey, analysis, and robustness concerns for hiding information in text”, Purdue University, Indiana, USA, 2004.

[113]R. Sridevi, A. Damodaram and S.V.L. Narasimham, “Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key with Enhanced Security,” Journal of Theoretical and Applied Information Technology, vol. 5, no. 6, pp. 768 – 771, June 2009.

[114]W. Bender, D. Gruhl and N. Morimoto, “Techniques for Data Hiding,” IBM Systems Journal, vol. 35, no. 3, pp. 313 – 336, 1996.

[115]D. Kirovski and H. Malvar, “Spread spectrum Watermarking of Audio Signals,” IEEE Transactions on Signal Processing, vol. 51, no. 4, pp. 1020 – 1033, April 2003.

[116]D. Huang and T. Yeo, “Robust and Inaudible Multi-echo Audio Watermarking,” Proceedings of the IEEE Pacific-Rim Conference on Multimedia, pp. 615 – 622, Taipei, China, December 2002.

[117]C. Kraetzer and J. Dittmann, “Pros and Cons of Mel cepstrum based Audio Steganalysis using SVM Classification,” Lecture Notes in Computer Science, vol. 4567, pp. 359 – 377, January 2008.

[118]W. Zeng, H. Ai and R. Hu, “A Novel Steganalysis Algorithm of Phase Coding in Audio Signal,” Proceedings of the 6th International Conference on Advanced Language Processing and Web Information Technology, pp. 261 – 264, August 2007.

[119]W. Zeng, H. Ai and R. Hu, “An Algorithm of Echo Steganalysis based on Power Cepstrum and Pattern Classification,” Proceedings of the International Conference on Information and Automation, pp. 1667 – 1670, June 2008.

[120]I. Paraskevas and E. Chilton, “Combination of Magnitude and Phase Statistical Features for Audio Classification,” Acoustical Research Letters Online, Acoustical Society of America, vol. 5, no. 3, pp. 111 – 117, July 2004.

[121]M. K. Johnson, S. Lyu, H. Farid, “Steganalysis of Recorded Speech,” Proceedings of Conference on Security, Steganography and Watermarking of Multimedia, Contents VII, vol. 5681, SPIE, pp. 664– 672, May 2005.

[122]H. Ozer, I. Avcibas, B. Sankur and N. D. Memon, “Steganalysis of Audio based on Audio Quality Metrics,” Proceedings of the Conference on Security, Steganography and Watermarking of Multimedia, Contents V, vol. 5020, SPIE, pp. 55 – 66, January 2003.

[123]A. C. Rencher, Methods of Multivariate Data Analysis, 2nd Edition, John Wiley, New York, NY, March 2002.

[124]P. Pudil, J. Novovicova and J. Kittler, “Floating Search Methods in Feature Selection,” Pattern Recognition Letters, vol. 15, no. 11, pp. 1119 – 1125, November 1994.

[125]Y. Liu, K. Chiang, C. Corbett, R. Archibald, B. Mukherjee and D. Ghosal, “A Novel Audio Steganalysis based on Higher-Order Statistics of a Distortion Measure with Hausdorff Distance,” Lecture Notes in Computer Science, vol. 5222, pp. 487 -501, September 2008.

[126]D. P. Huttenlocher, G. A. Klanderman and W. J. Rucklidge, “Comparing Images using Hausdorff Distance,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, no. 9, pp. 850– 863, September 1993.

[127]T. Holotyak, J. Fridrich and S. Voloshynovskiy, “Blind Statistical Steganalysis of Additive Steganography using Wavelet Higher Order Statistics,” Lecture Notes in Computer Science, vol. 3677, pp. 273 – 274, September 2005.

[128]I. Avcibas, “Audio Steganalysis with Content-independent Distortion Measures,” IEEE Signal Processing Letters, vol. 13, no. 2, pp. 92 – 95, February 2006.

[129]Q. Liu, A. H. Sung and M. Qiao, “Novel Stream Mining for Audio Steganalysis,” Proceedings of the 17th ACM International Conference on Multimedia, pp. 95 – 104, Beijing, China, October 2009.

[130]C.S. Lu: Multimedia security: steganography and digital watermarking techniques for protection of intellectual property. Artech House, Inc (2003).

[131]J.J. Chae and B.S. Manjunath: Data hiding in Video. Proceedings of the 6th IEEE International Conference on Image Processing, Kobe, Japan (1999).

[132]Provos, N., Honeyman, P.: Hide and Seek: An Introduction to Steganography. IEEE Security & Privacy Magazine 1 (2003).

[133]I.J.Cox, J. Kilian, T. Leighton, T.Shamoon: Secure spread spectrum watermarking for multimedia. Proceedings of IEEE Image processing (1997).

[134]J.J. Chae, D. Mukherjee and B.S. Manjunath: A Robust Data Hiding Technique using Multidimensional Lattices. Proceedings of the IEEE Forum on Research and Technology Advances in Digital Libraries, Santa Barbara, USA (1998).

[135]X. Niu, M. Schmucker and C. Busch: Video watermarking resisting to rotation, scaling, and translation. Proceedings of SPIE Security and Watermarking of Multimedia Contents IV (2002).

[136]U. Budia, D. Kundur and T. Zourntos, “Digital Video Steganalysis Exploiting Statistical Visibility in the Temporal Domain,” IEEE Transactions on Information Forensics and Security, vol. 1, no. 4, pp. 502 – 516, December 2006.

[137]J. S. Jainsky, D. Kundur and D. R. Halverson, “Towards Digital Video Steganalysis using Asymptotic Memoryless Detection,” Proceedings of the 9th International Workshop on Multimedia and Security, pp. 161 – 168, Dallas, TX, USA, 2007.

[138]E. L. Lehmann and J. P. Romano, Testing Statistical Hypotheses, 3rd edition, Springer Texts in Statistics, 2005.

[139]Y. Su, C. Zhang, L. Wang and C. Zhang, “A New Video Steganalysis based on Mode Detection,” Proceedings of the

© JGRCS 2010, All Rights Reserved

International Conference on Audio, Language and Image Processing, pp. 1507 – 1510, Shanghai, China, July 2008.

[140] MSU Stego Video: http://www.compression.ru/video/stego_video/index.html

[141] V. Pankajakshan and A. T. S. Ho, “Improving Video Steganalysis using Temporal Correlation,” Proceedings of the 3rd International Conference on Intelligent Information Hiding and Multimedia Signal Processing, vol. 1, pp. 287 – 290, November 2007.

[142] Y. Wang, J. Osterman and Y-Q. Zhang, Video Processing and Communication, Prentice Hall, 2001.

[143] K. Kancherla and S. Mukkamala, “Video Steganalysis using Spatial and Temporal Redundancies,” Proceedings of International Conference on High Performance Computing and Simulation, pp. 200–207, June 2009.

[144] C. Zhang, Y. Su and C. Zhang, “Video Steganalysis based on Aliasing Detection,” Electronic Letters, vol. 44, no. 13, pp. 801 – 803, June 2008.

[145] B. Liu, F. Liu and P. Wang, “Inter-frame Correlation based Compression Video Steganalysis,” Proceedings of the Congress on Image and Signal Processing, vol. 3, pp. 42 – 46, May 2008.

[146] Bin Li, Junhui He, Jiwu Huang and Yun Qing Shi, “A Survey on Image Steganography and Steganalysis,” Journal of Information Hiding and Multimedia Signal Processing, vol. 2, ,number 2, April 2011.

[147] P. Sallee. Model-based steganography . In *Proceedings of the 2nd Internation Workshop on Digital Watermarking*, volume 2939 of *LNCS*, pages 154{167. Springer, 2003.

[148] YANG Hao and CAO Xianbin “ Linguistic Steganalysis Based on Meta Features and Immune Mechanism “Chinese Journal of Electronics,Vol.19, No.4, Oct. 2010

[149] Lingyun Xiang, Xingming Sun, Gang Luo, Can Gan. “Research on Steganalysis for Text Steganography Based on Font Format”, The Third International Symposium on Information Assurance and Security (IAS 2007), Manchester, United Kingdom , August 2007.

[150] Natarajan Meghanathan and Lopamudra Nayak “STEGANALYSIS ALGORITHMS FOR DETECTING THE HIDDEN INFORMATION IN IMAGE, AUDIO AND VIDEO COVER MEDIA” at International Journal of Network Security & Its Application (IJNSA), Vol.2, No.1, January 2010.

[151] Y. Wang, E. Izquierdo, “High-Capacity Data Hiding in MPEG-2 Compressed Video”, 9th International Workshop on Systems, Signals and Image Processing, UK, 2002.

[152] D.E. Lane “Video-in-Video Data Hiding”, 2007.

[153] Hideki Noda, Tomonori Furuta, Michiharu Niimi, Eiji Kawaguchi. Application of BPCS steganography to wavelet compressed video. In Proceedings of ICIP'2004. pp.2147-2150

[154] Cheng-Hung Chuang and Guo-Shiang Lin, “An Optical Video Cryptosystem with Adaptive Steganography”, Proceedings of International Association for Pattern Recognition (IAPR) Conference on Machine Vision Applications (MVA’09), pp. 439-442, Keio University, Yokohama, Japan, May 20-22, 2009. (NSC97-2221-E-468-006

[155] Amr A. Hanafy, Gouda I. Salama and Yahya Z. Mohasseb “A Secure Covert Communication Model Based on Video Steganography,” in Military Communications Conference, 2008. MILCOM. IEEE on 16-19 Nov. 2008.

[156] R. Kavitha, A. Murugan, "Lossless Steganography on AVI File Using Swapping Algorithm," Computational Intelligence and Multimedia Applications, International Conference on, vol. 4, pp. 83-88, 2007 International Conference on Computational Intelligence and Multimedia Applications, 2007.

[157] Yueyun Shang, "A New Invertible Data Hiding In Compressed Videos or Images," icnc, vol. 5, pp.576-580, Third International Conference on Natural Computation (ICNC 2007), 2007

ABOUT THE AUTHORS

Souvik Bhattacharyya received his B.E. degree in Computer Science and Technology from B.E. College, Shibpur, India, presently known as Bengal Engineering and Science University (BESU) and M.Tech degree in Computer Science and Engineering from National Institute of Technology, Durgapur, India. Currently he is working as an Assistant Professor in Computer Science and Engineering Department at University Institute of Technology, The University of Burdwan. He has a good no of research publication in his credit. His areas of interest are Natural Language Processing, Network Security and Image Processing.

Indradip Banerjee received his MCA degree from IGNOU in 2009, PGDCA from IGNOU in 2008, MMM from Annamalai University in 2005 and BCA (Hons.) from The University of Burdwan in 2003. Currently he is working as a Technical Assistant in Computer Science and Engineering Department at University Institute of Technology, The University of Burdwan. His areas of interest are Network Security and Image Processing.

Gautam Sanyal has received his B.E and M.Tech degree National Institute of Technology (NIT), Durgapur, India. He has received Ph.D (Engg.) from Jadavpur University, Kolkata, India, in the area of Robot Vision. He possesses an experience of more than 25 years in the field of teaching and research. He has published nearly 50 papers in International and National Journals / Conferences. Two Ph.Ds (Engg) have already been awarded under his guidance. At present he is guiding six Ph.Ds scholars in the field of Steganography, Cellular Network, High Performance Computing and Computer Vision. He has guided over 10 PG and 100 UG thesis. His research interests include Natural Language Processing, Stochastic modeling of network traffic, High Performance Computing, Computer Vision. He is presently working as a Professor in the department of Computer Science and Engineering and also holding the post of Dean (Students’ Welfare) at National Institute of Technology, Durgapur, India.