Investigation of Steganalysis Algorithms for Multiple Cover Media

Eng.Mohammed Ishaque[1] Eng.Fazal Qudus Khan[2] Dr.Syed Abdul Sattar[3]

[1, 2] Lecturer Department of Information Technology, King Abdul Aziz University,
Kingdom of Saudi Arabia, 21441.
[3]Dean Academics Royal Institute of Technology and Science, India.

ABSTRACT

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Steganalysis is the art and science of detecting messages hidden using steganography; this is analogous to cryptanalysis applied to cryptography. In this paper, we provide a critical review of the steganalysis algorithms available to analyze the characteristics of an image, audio or video stego media vis-à-vis the corresponding cover media (without the hidden information) and understand the process of embedding the information and its detection. It is noteworthy that each of these cover media has different special attributes that are altered by a steganography algorithm in such a way that the changes are not perceivable for the unintended recipients; but, the changes are identifiable using appropriate steganlysis algorithms. We anticipate that this paper can also give a clear picture of the current trends in steganography so that we can develop and improvise appropriate steganlysis algorithms.

Keywords: Steganalysis , Steganography , Cryptography , Information Hiding

1. INTRODUCTION

The Internet allows computer users to remotely access other computers and information stores easily, wherever they may be across the world. They may do this with or without the use of security, authentication and encryption technologies, depending on the requirements. File sharing is an example of transferring large amounts of data across the Internet. A computer file can be e-mailed to customers, colleagues and friends as an attachment. It can be uploaded to a website or FTP server for easy download by others. It can be put into a "shared location" or onto a file server for instant use by colleagues [1]. As the modern world is gradually becoming “paperless’ with huge amount of information stored and exchanged over the Internet, it is imperative to have robust security measurements to safeguard the privacy and security of the underlying data.

Cryptography techniques [2] have been widely used to encrypt the plaintext data, transfer the ciphertext over the Internet and decrypt the ciphertext to extract the plaintext at the receiver side. However, with the ciphertext not really making much sense when interpreted as it is, a hacker or an intruder can easily perceive that the information being sent on the channel has been encrypted and is not the plaintext. This can naturally raise the curiosity level of a malicious hacker or intruder to conduct cryptanalysis attacks on the ciphertext (i.e., analyze the ciphertext vis-à-vis the encryption algorithms and decrypt the ciphertext completely or partially) [2].

It would be rather more prudent if we can send the secret information, either in plaintext or ciphertext, by cleverly embedding it as part of a cover media (for example, an image, audio or video carrier file) in such a way that the hidden information cannot be easily perceived to exist for the unintended recipients of the cover media. This idea forms the basis for Steganography, which is the science of hiding information by embedding the hidden (secret) message within other, seemingly harmless images, audio, video files or any other media. Steganography protects the intellectual property rights and enables information transfer in a covert manner such that it does not draw the attention of the unintended recipients. embedding it as part of a cover media (for example, an image, audio or video carrier file) in such a way that the hidden information cannot be easily perceived to exist for the unintended recipients of the cover media. This idea forms the basis for Steganography, which is the science of hiding information by embedding the hidden (secret) message within other, seemingly harmless images, audio, video files or any other media. Steganography protects the intellectual property rights and enables information transfer in a covert manner such that it does not draw the attention of the unintended recipients.

Steganalysis is the science of detecting the presence of hidden data in the cover media files and is emerging in parallel with steganography. Steganalysis has gained prominence in national security and forensic sciences since detection of hidden (ciphertext or plaintext) messages can lead to the prevention of disastrous security incidents. Steganalysis is a very challenging field because of the scarcity of knowledge about the specific characteristics of the cover media (an image, an audio or video file) that can be exploited to hide information and detect the same. The approaches adopted for steganalysis also sometimes depend on the underlying steganography algorithm(s) used. In this paper, we review the steganalysis algorithms available for the three commonly used cover media: Image, Audio and Video. Image Steganalysis algorithms (refer Section 2) explore the strong inter-pixel dependencies that are characteristic of natural images [3]. Audio Steganalysis algorithms (refer Section 3) are based on characteristic aspects such as the distortion measure of the audio signal, high-order statistics and etc [4]. Video Steganalysis algorithms (refer Section 4) exploit the spatial and temporal redundancies in the video signals within the individual frames and at inter-frame level (e.g. [5]). Various algorithms proposed for these three types of steganalysis will be explored in detail in the rest of the paper. Section 5 concludes the paper. Throughout the paper, the terms ‘algorithm’, ‘approach’, ‘method’ and ‘technique’ are used interchangeably. They mean the same. Also, for discussion purposes, the term ‘cover’ is used to refer to a media devoid of any hidden secret information and the term ‘stego’ is used to refer to a media that has hidden secret information.

2. IMAGE STEGANALYSIS

Algorithms for image steganalysis are primarily of two types: Specific and Generic. The Specific approach represents a class of image steganalysis techniques that very much depend on the underlying steganographic algorithm used and have a high success rate for detecting the presence of the secret message if the message is hidden with the algorithm for which the techniques are meant for. The Generic approach represents a class of image steganalysis techniques that are independent of the underlying steganography algorithm used to hide the message and produces good results for detecting the presence of a secrete message hidden using new and/or unconventional steganographic algorithms. The image steganalysis techniques under both the specific and generic categories are often designed to detect the presence of a secret message and the decoding of the same is considered complementary not mandatory.

2.1. Specific Image Steganalysis Algorithms

Image steganography algorithms are more often based on an embedding mechanism called Least Significant Bit (LSB) embedding. Each pixel in an image is represented as a 24-bitmap value, composed of 3 bytes representing the R, G and B values for the three primary colors Red, Green and Blue respectively. A higher RGB value for a pixel implies larger intensity. For instance, a pixel p represented as FF FF FF16 is composed of all of these three primary colors at their maximum intensity and hence the color represented by this pixel is “white”. LSB embed ding exploits the fact that changing the least significant bit of each of the three bytes of a pixel would produce only a minor change in the intensity of the color represented by the pixel and this change is not perceptible to the human eye [6]. For example, changing the color values of pixel p to FE FE FE16 would make the color darker by a factor of 1/256. Steganography algorithms based on LSB embedding differ on the pattern of modification – a modification of randomly chosen pixels or modification restricted to pixels located in certain areas of the image.

Images can be represented in different formats, the three more commonly used formats are: GIF (Graphics Interchange Format), BMP (Bit Map) and JPEG (Joint Photographic Exchange Group). Each of these image formats behaves differently when a message is embedded in it. Accordingly, there exist different image steganalysis algorithms for each of these three image formats. We now discuss the algorithms for each of these formats.

2.1.1. Palette Image Steganalysis

Palette image steganalysis is primarily used for GIF images. The GIF format supports up to 8 bits per pixel and the color of the pixel is referenced from a palette table of up to 256 distinct colors mapped to the 24-bit RGB color space. LSB embedding of a GIF image changes the 24-bit RGB value of a pixel and this could bring about a change in the palette color (among the 256 distinct colors) of the pixel. The strength of the steganographic algorithm lies in reducing the probability of a change in the palette color of the pixel and in minimizing the visible distortion that embedding of the secret image can potentially introduce. The steganalysis of a GIF stego image is conducted by performing a statistical analysis of the palette table vis-à-vis the image and the detection is made when there is an appreciable increase in entropy (a measure of the variation in the palette colors). The change in entropy is maximal when the embedded message is of maximum length [7].

2.1.2. Raw Image Steganalysis

The Raw image steganalysis technique is primarily used for BMP images that are characterized by a lossless LSB plane. LSB embedding on such images causes the flipping of the two gray-scale values. The embedding of the hidden message is more likely to result in averaging the frequency of occurrence of the pixels with the two gray-scale values. For example, if a raw image has 20 pixels with one gray-scale value and 40 pixels with the other gray-scale value, then after LSB embedding, the count of the pixels with each of the two gray-scale values is expected to be around 30. This approach was first proposed by Westfield and Pfitzmann [8], and it is based on the assumption that the message length should be comparable to the pixel count in the cover image (for longer messages) or the location of the hidden message should be known (for smaller messages). Dumitrescu et. al [9] proposed another steganalysis algorithm for gray-scale images. This algorithm assumes an image to be made up of horizontally adjacent pixels and classifies the set of all such pixel pairs (a, b) into four subsets depending on whether a and b are odd or even and whether a < b, a > b or a = b. The pixel values get modified when message embedding is done in the LSB plane, thereby leading to membership modifications across these four subsets. A statistical analysis on the changes in the membership of the pixels in the stego image leads to the detection of the length of the hidden message.

Fridrich et. al. [10] proposed a steganalysis technique that studies color bitmap images for LSB embedding and it provides high detection rates for shorter hidden messages. This technique makes use of the property that the number of unique colors for a high quality bitmap image is half the number of pixels in the image. The new color palette that is obtained after LSB embedding is characterized by a higher number of close color pairs (i.e., pixel pairs that have a maximum difference of one count in either of the color planes). We say that two colors (R1, G1, B1) and (R2, G2, B2) are close if $|R1-R2| \leq 1$ and $|G1-G2| \leq 1$ and $|B1-B2| \leq 1$. Let P be the ratio of the close color pairs to the total number of unique colors in the cover image, P’ be the ratio of close color pairs to the total number of unique colors in a stego image obtained by embedding a new message of particular length in a cover image and P’’ be the ratio of the close color pairs to the total number of unique colors when the cover image is further embedded in the stego image. If the hidden message is of considerable length, it has been observed that P’ > P and P’’ ~ P. For shorter messages, the values of P and P’ will be closer and detection may not be possible. Also, the above technique will not work if the cover image stored in lossless format has a higher number of unique colors (more than half the number of pixels).

2.1.3. JPEG Image Steganalysis

JPEG is a popular cover image format used in steganography. Two well-known Steganography algorithms for hiding secret messages in JPEG images are: the F5 algorithm [11] and Outguess algorithm [12]. The F5 algorithm uses matrix embedding to embed bits in the DCT (Discrete Cosine Transform) coefficients in order to minimize the number of changes to a message. However, F5 mutates the histogram of DCT coefficients. Fridrich et. al [7] propose a technique for estimating the unaltered histogram to find the number of changes and length of the secret message. The process involves cropping the JPEG image by four columns and then applying a quantization table to re-compress the image. The resulting DCT coefficient histogram will be a close estimate of the original. Fridrich et. al [7] also propose a technique to attack the Outguess embedding algorithm. The Outguess algorithm makes a random walk and embeds its message bits in the LSB of some of the DCT coefficients. The other DCT coefficients are then adjusted to keep the original histogram intact. As a result, the F5 steganalysis method involving estimation of the original histogram will be useful in the steganalysis of the Outguess algorithm. Also, the process of embedding a message into an unadulterated image introduces noise in the DCT coefficients, leading to increased spatial discontinuities in the 8x8 JPEG image blocks and partial cancellation of the changes made to the LSB of DCT coefficients. Furthermore, when another message is embedded into a stego image, the increase in discontinuities tends to be smaller. The nature of the increase or decrease in discontinuities is widely employed to gauge the size of the hidden message.

2.2. Generic Image Steganalysis Algorithms

The generic steganalysis algorithms, usually referred to as Universal or Blind Steganalysis algorithms, work well on all known and unknown steganography algorithms. These steganalysis techniques exploit the changes in certain innate features of the cover images when a message is embedded. The focus is on to identify the prominent features of an image that are monotonic and changes statistically as a result of message embedding. The generic steganalysis algorithms are developed to precisely and maximally distinguish these changes. The accuracy of the prediction heavily depends on the choice of the right features, which should not vary across images of different varieties. Avcibas et. al [13] use a set of Image Quality Metrics (IQMs) to develop a discriminator algorithm that differentiates cover images from stego images. The authors use IQMs as a steganalysis tool rather than as an indicator of image quality or algorithmic performance. The ANOVA (Analysis of Variance) statistical test is used to rank the IQMs based on their F-scores and identify the embedding of the message. The success of the approach lies in the identification of IQMs that are very sensitive to steganography and whose changes as a result of message embedding can be measured well. To increase the chances of a successful detection, several IQMs are normally employed to measure the distortions at different levels of sensitivity. For example, the mean square values for the Human Visual System (HVS)-weighted errors demonstrate more sensitivity to pure blur; while the Gradient measure responds to changes in the texture and the image periphery. The message embedding steganography algorithms differ in the changes brought to the different IQMs. Avcibas et. al [14] propose another steganalysis technique that analyzes every seventh and eighth bit planes of an image and measures their binary similarity. The technique measures the correlation between the adjacent bit planes that gets affected as a result of message embedding. The hypothesis is that message embedding decreases the correlation between two contiguous bit planes.

2.2. Generic Image Steganalysis Algorithms

The generic steganalysis algorithms, usually referred to as Universal or Blind Steganalysis algorithms, work well on all known and unknown steganography algorithms. These steganalysis techniques exploit the changes in certain innate features of the cover images when a message is embedded. The focus is on to identify the prominent features of an image that are monotonic and changes statistically as a result of message embedding. The generic steganalysis algorithms are developed to precisely and maximally distinguish these changes. The accuracy of the prediction heavily depends on the choice of the right features, which should not vary across images of different varieties. Avcibas et. al [13] use a set of

Image Quality Metrics (IQMs) to develop a discriminator algorithm that differentiates cover images from stego images. The authors use IQMs as a steganalysis tool rather than as an indicator of image quality or algorithmic performance. The ANOVA (Analysis of Variance) statistical test is used to rank the IQMs based on their F-scores and identify the embedding of the message. The success of the approach lies in the identification of IQMs that are very sensitive to steganography and whose changes as a result of message embedding can be measured well. To increase the chances of a successful detection, several IQMs are normally employed to measure the distortions at different levels of sensitivity. For example, the mean square values for the Human Visual System (HVS)-weighted errors demonstrate more sensitivity to pure blur; while the Gradient measure responds to changes in the texture and the image periphery. The message embedding steganography algorithms differ in the changes brought to the different IQMs. Avcibas et. al [14] propose another steganalysis technique that analyzes every seventh and eighth bit planes of an image and measures their binary similarity. The technique measures the correlation between the adjacent bit planes that gets affected as a result of message embedding. The hypothesis is that message embedding decreases the correlation between two contiguous bit planes.

Farid et. al [15] advocate the use of higher order statistics in the generic steganalysis techniques vis-à-vis the first-order statistics (such as the histogram DCT coefficients) employed by the specific steganalysis techniques, discussed in Section 2.1. Steganalysis techniques that tap the changes in the first-order statistics for detecting the presence of hidden messages fail if a steganography algorithm keeps the first-order statistics intact. Farid et. al propose the use of Quadratic Mirror Filters (QMF) to decompose an image into sub-bands and then evaluate higher-order statistics metrics such as the mean, variance, kurtosis and skewness to each of the sub-bands obtained. In addition to the above, generic steganalysis techniques that use a MMSE Linear Predictor [13], Fisher Linear Discriminant [13] and a Support Vector Machine (SVM) [15] have been proposed to accurately differentiate between clean and stego images.

3.AUDIO STEGANOGRAPHY AND STEGANALYSIS

Rapid advancement of the Voice over Internet Protocol (VoIP) and various Peer-to-Peer (P2P) audio services offer numerous opportunities for covert communication. Minor alteration in the binary sequence of audio samples with existing steganography tools can easily make covert communication, a reality. 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.

3.1. Audio Steganography Algorithms

In this section, we first describe the four major audio steganography algorithms: Low-bit encoding, Phase encoding, Spread spectrum coding and Echo data hiding. The disadvantages associated with these algorithms can be exploited for steganalysis [16].

3.1.1. Low-bit Encoding

In Low-bit encoding (e.g., [17]), 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.

3.1.2. Phase Coding

Phase coding [18] 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 signal's 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).

3.1.3. Spread Spectrum Coding

The basic Spread Spectrum (SS) coding method (e.g., [19]) 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.

3.1.4. Echo Hiding

With echo hiding (e.g. [20]), 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).

3.2. Audio Steganalysis Algorithms

Not a significant amount of literature is available on audio steganalysis. This can be attributed to 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 [21].

3.2.1. Phase and Echo Steganalysis

Zeng et. al proposed steganalysis algorithms to detect phase coding steganography based on the analysis of phase discontinuities [22] and to detect echo steganography based on the statistical moments of peak frequency [23]. 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 [24]. 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.

3.2.2. Universal Steganalysis based on Recorded Speech

Johnson et. al [25] 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.

3.2.3. Use of Statistical Distance Measures for Audio Steganalysis

H. Ozer et. al [26] calculated the distribution of various statistical distance measures on cover audio signals and stego-audio signals vis-à-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 [27] 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 [28]. 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 [26] 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.

3.2.4. Audio Steganalysis based on Hausdorff Distance

The audio steganalysis algorithm proposed by Liu et. al [29] uses the Hausdorff distance measure [30] 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 [31] at different levels of resolution. The Hausdorff 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 [32], 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.

3.2.5. Audio Steganalysis for High Complexity Audio Signals

More recently, Liu et. al [33] 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 [21], widely used in speech recognition, for audio steganalysis.

4. VIDEO STEGANALYSIS

Direct application of image steganalysis techniques to video sequences on a frame-by-frame basis yielded low performance results. Like audio steganalysis, very few video steganalysis methods are available in the literature.

4.1. Video Steganalysis Exploring the Temporal Correlation between Frames

Budia et. al [34] 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. Figure 1 illustrates the video steganography and steganalysis system used in [34]. To start off, the sender embeds a secret binary message vector into the cover video sequence to produce a stego video sequence that seems identical to the cover video. The secret message bits are embedded into the cover video by modulating it into a signal known as the Watermark. The stego video is then communicated via the Internet to the receiver. Using the stego video and the secret key, the receiver extracts the hidden message. En route to the receiver, the message may be intercepted by a vigilant steganalyst. Detection of the watermark will imply the presence of hidden information in the medium. Even though the watermark is inserted in a non-spatial domain (like DCT), it is defined over the same domain as the cover.

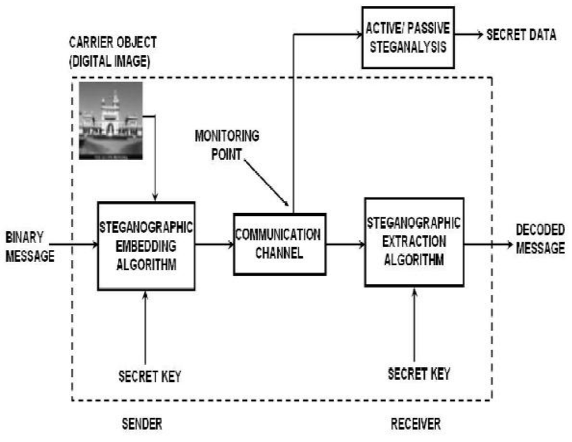

Figure 1: Video Steganography and Steganalysis (Source: [34])

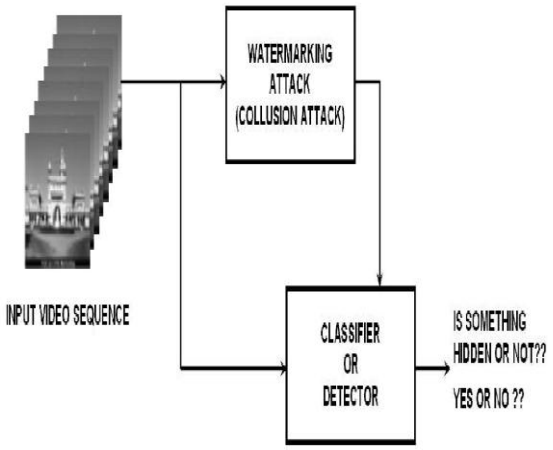
INPUT VIDEO SEQUENCE
WATERMARKING ATTACK (COLLUSION ATTACK)
CLASSIFIER OR DETECTOR
IS SOMETHING HIDDEN OR NOT??
YES OR NO ??

Figure 2: Framework for Steganalysis (Source: [34])

Budia et. al evaluated the importance of exploiting temporal correlations for video steganalysis. They created a framework (Figure 2) based on the steganalysis of Gaussian Spread Spectrum-based steganographic methods [35, 36]. There are two essential blocks: (i) A Watermarking attack stage to estimate the cover media from the possibly watermarked stego media and (ii) A Pattern recognition stage for the detection of the steganographic activity. Different algorithms can be substituted for each of the blocks to produce steganalysis techniques for a variety of applications. The block-based approach also facilitates the use of the recent advanced algorithms for Watermark attacks and Pattern recognition.

Budia et. al developed a steganalysis algorithm that takes advantage of the temporal redundancy inherent in video. Noticeably, it demonstrated improved performance over the spatial methods that operate on a frame-by-frame basis. Simple linear collusion has been observed to be advantageous because of low complexity and suitability for real-time applications. The framework also demonstrates how statistical redundancy in the cover video can be useful in detecting hidden watermarks. Greater inter-frame correlation improves collusion performance. It has been also observed that the rate of steganalytic detection increases when the watermark embedding strength shoots up, implying that robustness increases the chances of detection. However, a very low embedding strength makes the watermark vulnerable for easy removal. Hence, a moderate value for the watermark embedding strength should be used.

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

Jainsky et. al [37] proposed a video steganalysis algorithm that incorporates asymptotic relative efficiency [38]-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) [38], 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.

4.3. Video Steganalysis based on Mode Detection

Su et. al [39] propose a video steganalysis algorithm that targets the Moscow State University (MSU) stego video [40] 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.

4.4. Video Steganalysis based on Spatial and Temporal Prediction

Pankajakshan and Ho propose a video steganalysis scheme [41] for the MPEG video coding standard in which a given frame is predicted from its neighboring reference frames using motion compensation [42]. The MPEG coding scheme supports two types of predicted frames: the P-frames (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 P-and B-frames are then coded using transform coding techniques. The PEFs exhibit spatio-temporal 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.

4.5. Other Video Steganalysis Algorithms

Kancherla and Mukkamala [5] 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 [43] propose a steganalysis 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 [44] 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.

5. CONCLUSIONS

In this paper, we have investigated the steganalysis algorithms available for multiple cover media of steganography (Image, Audio and Video). Image steganalysis algorithms can be classified into two broad categories: Specific and Generic. The Specific steganalysis algorithms are based on the format of the digital image (e.g. GIF, BMP and JPEG formats) and depend on the underlying steganography algorithm used. The Generic image steganalysis algorithms work for any underlying steganography algorithm, but require more complex computational and higher-order statistical analysis. The audio steganalysis algorithms exploit the variations in the characteristic features of the audio signal as a result of message embedding. Audio steganalysis algorithms that detect the discontinuities in phase (as a result of phase coding), variations in the amplitude (as a result of Echo hiding) and the changes in the perceptual and non-perceptual audio quality metrics as a result of message embedding have been proposed. The video steganalysis algorithms that utilize the temporal redundancies at the frame level and inter-frame level have been observed to be more effective than algorithms based on spatial redundancies. Nevertheless, video steganalysis algorithms that simultaneously exploit both the temporal and spatial redundancies have also been proposed and shown to be effective. In summary, each carrier media has its own special attributes and reacts differently when a message is embedded in it. Therefore, the steganalysis algorithms have also been developed in a manner specific to the target stego file and the algorithms developed for one cover media are generally not effective for a different media. This paper would cater well to providing an overview of the steganalysis algorithms available for the three commonly used domains of steganography.

REFERENCES

[1] http://en.wikipedia.org/wiki/Internet

[2] D. Stinson, Cryptography: Theory and Practice, 2nd Edition, Chapman and Hall/ CRC, February 2002.

[3] 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*, vol. 1, no. 2, pp. 275 – 287, June 2006.

[4] X-M. Ru, H-J Zhang and X. Huang, "Steganalysis of Audio: Attacking the Steghide," *Proceedings of the 4th International Conference on Machine Learning and Cybernetics*, vol. 7, pp. 3937 – 3942, Guangzhou, China, August 2005.

[5] 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.

[6] N. F. Johnson and S. Jajodia, "Steganalysis of Images Created using Current Steganography Software," *Lecture Notes in Computer Science*, vol. 1525, pp. 32 – 47, Springer Verlag, 1998.

[7] J. Fridrich, M. Goljan, D. Hogea and D. Soukal, "Quantitative Steganalysis of Digital Images: Estimating the Secret Message Length," *ACM Multimedia Systems Journal*, Special issue on Multimedia Security, vol. 9, no. 3, pp. 288 – 302, 2003.

[8] A. Westfeld and A. Pfitzmann, "Attacks on Steganographic Systems," *Proceedings of the 3rd International Workshop on Information Hiding*, pp. 61 – 76, 1999.

[9] S. Dumitrescu, X. Wu and N. Memon, "On Steganalysis of Random LSB Embedding in Continuous tone Images," *Proceedings of the International Conference on Image Processing*, vol. 3, pp. 641 – 644, June 2002.

[10] J. Fridrich and M. Long, "Steganalysis of LSB Encoding in Color Images," *Proceedings of the IEEE International Conference on Multimedia and Expo* (ICME), vol. 3, pp. 1279 – 1282, New York, NY, USA, July –

August 2000.

[11] A. Westfeld, "F5 – A Steganographic Algorithm," *Lecture Notes in Computer Science*, vol. 2137, pp. 289 – 302, January 2001.

[12] Outguess Universal Steganography: http://www.outguess.org

[13] I. Avcibas, N. Memon and B. Sankur, "Steganalysis using Image Quality Metrics," *IEEE Transactions on Image Processing*, vol. 12, no. 2, pp. 221 – 229, February 2003.

[14] I. Avcibas, N. Memon and B. Sankur, "Image Steganalysis with Binary Similarity Measures," *Proceedings of the IEEE International Conference on Image Processing*, vol. 3, pp. 645 – 648, June 2002.

[15] S. Lyu and H. Farid, "Detecting Hidden Messages using Higher-order Statistics and Support Vector Machines," *Lecture Notes in Computer Science*, vol. 2578, pp. 340 – *354, 2002.*

[16] M. Arnold, S. Wolthusen and M. Schmucker, Techniques and Applications of Digital Watermarking and Content Protection, Artech House, Norwood, MA, 2003.

[17] 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*.

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

[19] 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.*

[20] 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.

[21] 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.

[22] 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.

[24] 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.

[25] 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.*

[26] 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.

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

[28] 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.

[29] 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.

[30] 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, *Sep 1993.*

[31] 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.

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

[33] 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.

[34] 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.

[35] I. Cox, J. Kilian, F. Leighton and T. Shamoon, “Secure Spread Spectrum Watermarking for Multi-media,” *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673 – 1687, December 1997.

[36] L. Marvel, C. B. Jr., and C. Retter, “Spread Spectrum Image Steganography,” *IEEE Transactions on Image Processing*, vol. 8, no. 8, pp. 1075 – 1083, August 1999.

[37] 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.

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

[39] Y. Su, C. Zhang, L. Wang and C. Zhang, “A New Video Steganalysis based on Mode Detection,” *Proceedings of the International Conference on Audio, Language and Image Processing*, pp. 1507 – 1510, Shanghai, China, July 2008.

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

[41] 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.

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

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

[44] *B.Liu , F.Liu and P.Wang ,”Inter Frame Corellation based compression video Steganalysis”, Proceedings of the Congress on Image and Signal Processing*, vol. 3, pp. 42 – 46, May 2008.