New Optimal Based Steganalysis Solutions for Embedding the Hidden Information in Audio Cover Media

Ahlem Fatnassi
FSG, Northern Border University, KSA
National School of Computer Science
Manouba University, Tunisia
Email: ahlemfatn@yahoo.fr

Hamza Gharsellaoui
National Engineering School of Carthage
Carthage University, Tunisia
LISI INSAT, Carthage University, Tunisia
Email: gharsellaoui.hamza@gmail.com

Sadok Bouamama
FCIT, Jeddah University, KSA
National School of Computer Science
Manouba University, Tunisia
Email: Sbouamama.hamza@uj.edu.sa

***Abstract*—This paper deals with the study of interest in the fields of Steganography and Steganalysis. Steganography involves hiding information in a cover media to obtain the stego media in such a way that the cover media is perceived not to have any embedded message for its unintended recipients. Steganalysis is the mechanism of detecting the presence of hidden information in the stego media and it can lead to the prevention of disastrous security incidents. In this paper, we provide a critical review of the steganalysis algorithms available to analyze the characteristics of a text, an image and audio stego media against the corresponding cover media and understand the process of embedding the information and its detection. 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 steganalysis algorithms.**

***Index Terms*—Optimization, Heuristics and Metaheuristics Algorithms, Embedded Systems, Low-power Consumption, Steganalysis Heuristic Approach.**

I. Introduction

Nowadays, one of the driving forces behind the increased use of hidden information is the growth of the Internet which has allowed text, image, audio and video to become available in digital form. This provides an additional way to distribute material to consumers to be made and distributed. Indeed, there are many different protocols and embedding approaches that enable us to hide data in a given cover media. However, all of the protocols and approaches must satisfy a number of requirements so that steganography, which is the science of hiding information by embedding the hidden message within other, can be applied correctly. The first step of embedding and hiding data is to pass both the secret message and the cover message into the cover media. Inside the cover media, one or several protocols will be implemented to embed the secret data into the cover message.

In other words, multiprocessor architectures provide a rich computing environment from which a wide range of problem domains, including real-time applications can benefit [1]. The Internet, for example, has revolutionized the modern world and the numerous Internet based applications that get introduced these days add to the high levels of comfort and connectivity in every aspects of human life [3]. 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 [5] 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 against the encryption algorithms and decrypt the ciphertext completely or partially) [5]. 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 can not be easily perceived to exist [4] 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. Indeed, steganography and Steganalysis have many features [2]. Steganography means also the ability of hiding the information in all the way. It is an art of sending hidden data or secret messages over a public channel so that a third party cannot detect the presence of the secret messages. The approaches adopted for steganalysis also sometimes depend on the underlying steganography algorithm(s) used. 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.

In this paper, we review the steganalysis algorithms available for the used cover media: Audio, in Section II. We

present the audio steganography algorithms in Section III and the audio steganalysis algorithms in Section IV. Our original approach is well described in Section V. Then, we describe the simulation results and discussion in Section VI. Finally, Section VII concludes the paper.

II. Background and State of the Art

Steganography is the art of passing information through original files in a manner that the existence of the message is unknown. The term steganography is arrived from Greek word means, "Covered Writing". The innocent files can be referred to as text, image, audio or video as appropriate. After embedding the secret message it is referred to as stego-medium. Also, with the development of digital signal processing (DSP), the boost in computer power, the internet and with information theory and coding theory, steganography has gone "digital". The objective of this section work is to present and describe performance enhancements over the steganography cover mediums and methods proposed in the literature.

A. 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 [15]. 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.

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 [15]. A higher RGB value for a pixel implies larger intensity. For instance, a pixel p represented as FF FF FF_{16} is composed of all of these three primary colors at their maximum intensity and hence the color represented by this pixel is white. LSB embedding 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]. 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) 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 [15]. 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 [7].

3) 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 grayscale 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 Westfeld 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 grayscale 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).

4) 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 and Outguess algorithm [11]. 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.

B. 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 [14]. 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. In [12], the authors 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.

III. Audio Steganography Algorithms

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. 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]. First, we list some preliminary observations.

A. Echo Hiding Approach

With echo hiding [17], 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).

B. Phase Coding Approach

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 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).

C. Spread Spectrum Coding Approach

The basic Spread Spectrum (SS) coding method [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.

D. Low-bit Encoding Approach

In Low-bit encoding [20], 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.

IV. 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].

A. 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.

B. 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.

C. 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--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].

D. 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 denoised 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], the authors 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 [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.

V. Hybrid Proposed Approach

in the following section we will describe our proposed approach for hiding secret information into audio cover media with a high security level.

A. Motivation and Description

In our original proposed work, audio steganography has been done for transmission of hidden information that represents secret data over the transmission channel. Here the transmission channel is an audio file used as a cover media. The secret information may be a text message, an image or an audio file. In our proposed work many steps for hiding of

secret data behind the cover media, have been used, in such away the data can be transmitted in secure manner.
At first, when the transmitted data is an image, so the secret image embedded into an audio cover media can be reconstructed from a stego image based on some rules described in our previous work reported in [2].
After that, when the transmitted data is a text (message), we use the Phase Coding Approach if the text data to be transmitted is a small text. In this case, message bits are encoded as phase shifts in the phase spectrum of a digital signal and the secret message gets camouflaged in the audio signal, not detectable by the steganalysis methods based on SPNR which lets to avoid the disadvantages of the noise-inducing methods presented by audio steganography. In contrast and when the text data to be transmitted is a big file, we use in our proposed approach the Low-bit Encoding Approach when the binary version of the secret data message is substituted with the LSB of each sample of the audio cover file. Also, this method is simple and can be used to embed larger messages with a small modifications tolerance. These modifications are due a format conversion or lossy compression. At the reception, the text has been encrypted using the Advanced Encryption Standard (AES) algorithm that converts originality of the text message. An audio file is embedded also in secure manner over an audio file which is used here as a cover media due to the human ear to hide information unnoticeable. Indeed, in the presence of another louder audible sound, an audible sound can be inaudible and this property allows us to select the audio channel in which to hide information. For the encryption method, if the transmitted file is a small one, then our proposed method will be based on the basic Spread Spectrum (SS) coding method which randomly spreads the bits of the secret data message across the frequency spectrum of the audio signal using a code that is independent of the actual cover signal. This SS coding method can perform better by virtue of a moderate data transmission rate coupled with a high level of robustness. In contrast, for the big files and in the case when the SS method may introduce noise to the audio file, our approach uses the echo hiding approach where the information is embedded by introducing an echo into the discrete audio signal and echo hiding allows for a higher data transmission rate and provides superior robustness.

B. Algorithm

The following algorithm demonstrates the way of embedding encrypted image, text and audio files.

Begin
1) **Par** = **value**; Read file into **buffer**
2) While **file** is in [image, text, audio] and **buffer** is not empty,
if **image**
3) Remove all data before the header
4) Convert **image** data to binary by using **OLSB** encoding algorithm
if **text**

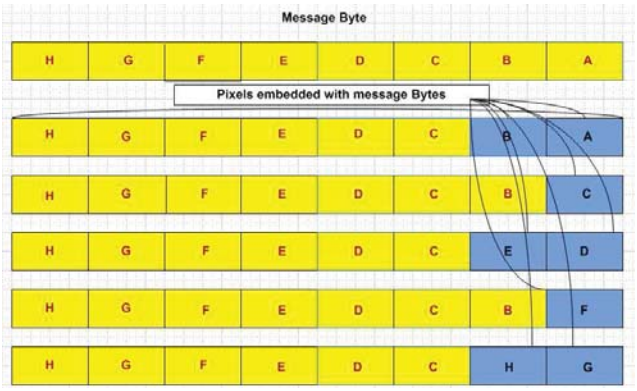

Fig. 1. Proposed OLSB Algorithm

if **text size** $\leq$ **Par** then
Convert **text** data to binary by using **Phase Coding** algorithm
else Convert **text** data to binary by using **Low-bit encoding** algorithm
if **audio**
if **audio size** $\leq$ **Par** then
Convert audio data to binary by using **Spread Spectrum** algorithm
else
Convert **audio** data to binary by using **Echo Hiding** algorithm

5) Read remaining and store
End.

C. Example: image Principle

Based on [14], a digital image is described using a 2-D matrix of the color intestines at each grid point (i.e. pixel). Typically gray images use 8 bits, whereas colored utilizes 24 bits to describe the color model, such as RGB model. The Steganography system uses an audio file as the cover, consequently, the spatial domain techniques are simple and easy to implement. The Least Significant Bit (LSB) is one of the main techniques in spatial domain image Steganography. The LSB is the lowest significant bit in the byte value of the image pixel. The LSB based image steganography embeds the secret in the least significant bits of pixel values of the cover image (CVR).

The concept of LSB Embedding is simple. It exploits the fact that the level of precision in many image formats is far greater than that perceivable by average human vision. Therefore, an altered image with slight variations in its colors will be indistinguishable from the original by a human being, just by looking at it [14]. In conventional LSB technique, which requires eight bytes of pixels to store 1 byte of secret data.

In contrast, in our optimal Least Significant Bit (OLSB) technique, just five bytes of pixels are sufficient to hold one message byte. Rest of the bits in the pixels remains

Fig. 2. Secret Image

the same. So, in our optimal proposed example, we need 5 bytes against 8 bytes in conventional LSB technique. For security reasons, only encryption may not be enough, hence our optimal proposed approach includes Steganography where in encrypted data is hid into the audio and then audio is transmitted in the network.

Encryption method: Read the secret and cover audio and convert them, then check to handle the principle constraint of the size. This constraint mentions that size of the secret image, text or audio should be less than cover audio. For example, for the image encryption, decryption process, we will adopt the [14]method principle for the encryption, decryption process. Encode the secret image into binary using bit gate command and divide it into RGB parts then substitute MSB bits of secret image into LSB bits of cover image. Hide the password with Stego image and send using the network transmission medium.

Decryption method: The reverse process takes place at the receiving end, Stego audio can be decrypted using password. We use in our work MATLAB due to its high-performance as a language for technical computing. Matlab function is an easy to use, user interface function (HMI) that guides a user through the process of either encoding & decoding a message into or from the audio respectively. In this work, Matlab is implemented for processing OLSB, phase coding, low-bit encoding, spread spectrum and echo hiding steganography techniques with different frame size 256*256, 128*128, 64*64 and simulation results are generated. There are mainly four steps involved in implementing OLSB steganography as shown below.

VI. Simulation Results and Discussion

To evaluate the performance of our hybrid proposed data hiding approach, we describe all the four steps needed for our hybrid proposed approach process. To apply the proposed OLSB algorithm, consider that we have to hide the secret image "Fig. 2" in cover audio.

A. Conversion of Image to Matrix

In the conversion process of text, image or audio to matrix, we convert the input cover audio into matrix values which is stored in a text file. Firstly an audio file is read from computer, the original image as an example of hidden data, is in the form of RGB which is converted into grey image. The grey image is resized to a particular size of 256*256. Each image has intensity values for every pixel, here these intensity values are stored into a text file.

B. Embedding Process

After completion of image to matrix the next step is to embed a message into an audio. The audio file obtained during this process is called as stegano-embed audio file. The message is embedded into the intensity values of image obtained during image to matrix conversion for the image use case example.

C. Conversion of Matrix to Audio

In this stage intensity values are converted back to audio. The audio obtained has message embedded into it. The cover audio and the text, image or audio obtained here have to be identical. Hence the objective of Steganography is satisfied.

D. Extraction Process

In this process we extract the message which was embedded during embedding process. At first declare a message byte, here the size of the message is 8 bits. Read a pixel from the array starting from address = 0. Extract the LSB and replace the i^{th} bit in the message byte where i = 1 to 8 Address = address =1. When i = 8, a byte is extracted. Repeat for extracting next byte and to respect the method of 2 bits by one bit in every two successive bytes.

E. Discussion and Interpretations

Here we send secret text, image or audio + cover audio = stego audio from PC to Controller. Then controller decodes original hidden data from cover audio and transmit to PC. We need new powerful Steganalysis techniques that can detect messages without prior knowledge of the hiding algorithm (blind detection). The detection of very small messages is also a significant problem. Finally, we need adaptive techniques that do not involve complex training stages. The comparison between the LSB and other methods from the state of the art studies and our hybrid proposed method OLSB, phase coding, low-bit encoding, spread spectrum and echo hiding using experimental results demonstrates that our original and optimal proposed approach keeps distortion low and uses a low memory capacity and a less execution time due to the reduced number of needed bytes, 5 against 8 in conventional LSB technique and to many other parameters like security, time and highly resistant against the attacks.

VII. Conclusion

In this paper, we have analyzed the steganalysis algorithms available for many domains of steganography (Text, Image, audio). Steganalysis algorithms can be classified into two broad categories: Specific and Generic. The hybrid OLSB, phase coding, low-bit encoding, spread spectrum and echo hiding techniques described in this paper help to successfully hide the secret data into the cover audio with minimum distortion made to the cover audio and with a minimum of memory space used. This method is essential for construction

of accurate targeted and blind steganalysis methods for JPEG, BMP and PNG images; texts and audio files. Experimental results of the modified method shows that our original hybrid proposed approach is greater than the conventional method of LSB replacement and other classical methods for both text and audio files. In summary and as a future work, we will try to propose best and original other steganalysis algorithms for the other domain of steganography covers (video).

REFERENCES

[1] H. Gharsellaoui, M. Khalgui, S. Ben Ahmed. Preemptive Hard Real-time Scheduling of Reconfigurable OS Tasks on Multiprocessors Embedded Control Systems. *PECCS - Proceedings of the 4th International Conference on Pervasive and Embedded Computing and Communication Systems*, 192–197, Lisbon, Portugal, 7-9 January, 2014.

[2] A. Fatnassi, H. Gharsellaoui and S. Bouamama. *A New Hybrid Steganalysis Based Approach for Embedding Image in Audio and Image Cover Media*. Proceedings of the IFAC-PapersOnLine 49-12(2016), 1809-1814, December, 2016.

[3] H. Kekre, A. Athawale, T. Sarode, S. Thepade and K. Sagvekar. *Steganography Using Dictionary Sort on Vector Quantized Codebook*. International Journal of Computer Science and Security (IJCSS), vol. 4, no. 4, pp. 392–402, 2010.

[4] V. Michopoulos, L. Guan, G. Oikonomou, I. Phillips. DCCC6: Duty Cycle-aware congestion control for 6LoWPAN networks. *Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, 278–283, 2012.

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

[6] N. 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] 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.

[13] 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.

[14] N. Champakamala, K. Padmini, D.K. Radhika. Least Significant Bit algorithm for image steganography. *International Journal of Advance Computer Technology, vol(3), N. 4*, pages 34–38, 2013.

[15] N. Meghanathan and L. Nayak. Steganalysis Algorithms For Detecting The Hidden Information In Image, Audio And Video Cover Media. *International Journal of Network Security & Its Application (IJNSA), Vol.2, No.1*, pp. 43–55, 2010.

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

[17] 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*, 2003.

[18] W. Bender, D. Gruhl and N. Morimoto. Techniques for Data Hiding. *IBM Systems Journal, (IBMSJ), 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, (IEEE TSP), Vol.51, No.4*, pp. 1020–1033, April 2003.

[20] 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, (JTAIT), Vol.5, No.6*, pp. 768–771, June 2009.

[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, June 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.

[23] W. Zeng, H. Ai and R. Hu. An Algorithm of Echo Steganalysis based on Power Cepstrum and Pattern Classification. *Proceedings of the 6th International Conference on Information and Automation*, pp. 1667–1670, June 2008.

[24] I. Paraskevas and E. Chilton. Combination of Magnitude and Phase Statistical Features for Audio Classification. *Acoustical Research Letters Online, Acoustical Society of America*, pp. 111–117, July 2004.

[25] M. K. Johnson, S. Lyu and 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, September 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. *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.