International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 16
June 2018

Literature Review on Audio Steganography

Reena Antil & Dr. Mamta Sachdeva

[1]Department of Computer Science
South Point Institute of Technology and Management (SITM),
Deenbandhu Chhotu Ram University of Science & Technology (DCRUST), Sonepat
[1]arun.nangal98@gmail.com

[2]Department of Computer Science
South Point Institute of Technology and Management (SITM),
Deenbandhu Chhotu Ram University of Science & Technology (DCRUST), Sonepat
[2]southpointin@gmail.com

Abstract— *Audio steganography is concerned with embedding information in an innocuous cover speech in a secure and robust manner. Communication and transmission security and robustness are essential for transmitting vital information to intended sources while denying access to unauthorized persons. Encoding secret messages in audio is the most challenging technique to use when dealing with steganography. This is the most challenging because of the human ability to distinguish small variations in sounds. The range of the human auditory power is dynamic. Humans can distinguish small changes in the audio with crystal clarity. Audio steganography is a useful means for transmitting covert military information via a cover audio signal which is virtually untraceable. The two primary criteria for successful embedding of a covert message are that the stego signal resulting from embedding is perceptually indistinguishable from the host audio signal, and the embedded message is recovered correctly at the receiver. In this paper we provide a review on various audio steganography techniques.*

Keywords— Spatial Domain, Frequency Domain, Patchwork, Spread Spectrum

I. INTRODUCTION

The rise of internet plays an important role in information technology. Nowadays use of internet has been increasing day by day. Providing security has also become important issue due to the use of internet. Cryptography [1] and Steganography [2] are the ways to provide the security to the information. Cryptography is used to encrypt the message so that it is protected from any third parties. Steganography is a method that is used to hide information in a cover so that nobody can guess it. The cover can be any image, text, audio or video. Steganography [3] defines from Greek word 'Stegnos' means secret and 'Graphy' means writing so overall means secret writing. The goal of Steganography is to hide the information whereas cryptography is used to protect the information from intruder or hacker. Due to the availability image file has been popularly used as the carrier.

Steganography works by replacing bits of useless or unused data in regular computer files such as graphics, sound, text, HTML, or even video with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images. In a computer-based audio Steganography system, secret messages are embedded in digital sound. The secret message is embedded by slightly altering the binary sequence of a sound file. Existing audio Steganography software can embed messages in WAV, AU, and even MP3 sound files. Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images. These methods range from rather simple algorithms that insert information in the form of signal noise to more powerful methods that exploit sophisticated signal processing techniques to hide information.

In this paper we provide a review on various audio steganography techniques.

II. AUDIO STEGANOGRAPHY TECHNIQUES

A. Temporal domain

1) LSB:
LSB is one of the earliest and simplest methods for hiding information in audio signals. It is the commonly used technique for audio steganography. In LSB encoding, the least significant bits of the cover media/original audio is altered to include the secret message. Even though this is a simple method, an attacker can easily extract the secret message from the steganos object [4].

2) Parity coding:
Parity coding technique operates on a group of samples instead of individual samples. Here
Individual samples are grouped and parity of each group is calculated. For inserting message bit one by

one, check the parity bit of a group of samples. If the parity bit and message bit matches do nothing. Otherwise change the LSB's of any one of the individual samples in that group to make the parity bit equal to the message bit [4].

3) Echo hiding:
In echo hiding method data is embedded in the echo part of the host audio signal [4]. The echo is a resonance added to the host signal and hence the problem with the additive noise is avoided here. While using echo hiding three parameters are to be considered: they are initial amplitude, offset (delay), and decay rate, so that echo is not audible. The main disadvantage of this method is lenient detection and low detection ratio.

B. Frequency domain:
Frequency domain techniques and wavelet domain technique comes under transform domain. The main techniques under frequency domain are: tone insertion, phase coding and spread spectrum technique.

1) Tone insertion:
Frequency masking property is exploited in tone insertion method. A weak pure tone is masked in the presence of a stronger tone. This property of inaudibility is used in different ways to embed information.

2) Phase coding:
Phase coding method is based on the fact that the phase components are not audible to human as noise components. This method embeds the secret message bits as phase shift in the phase spectrum of the original audio signal. The method tolerates better signal distortion, better robustness but it does not survive low pass filtering. Here the secret message is inserted only at the phase vector of the first signal segment.

III. LITERATURE REVIEW

Rashid Ansari et. Al. [5] proposed a novel perception-based data hiding technique for digital audio. In this paper, a novel method is proposed to exploit the HAS property that human auditory perception is largely insensitive to audio phase distortion in a certainrange of audible frequencies. In this method audio is decomposed into subband signals some of which are selected for embedding data with a controlled alteration of phase.

Mark Sterling et. Al. [6] described an application of spread spectrum techniques in audio data hiding for watermarking and steganography. The method is self-synchronizing, cover dependent and operates in the time domain. The Author use a special class of frequency-hop signal known as a Welch-Costas Array. Welch-Costas Arrays have the properties of range and Doppler resolution. This allows us to recover embedded data with a matched filter.

XUE-MIN RU et. al. [7] presented a steganalytic method that can reliably detect messages hidden in WAV files using the steganographic tool Steghide. The key element of the method is mining the correlation between wavelet coefficients in a short-duration (about 20ms) in each subband. This is done by performing a four-level 1-D wavelet decomposition of the audio signals, using a linear predictor for the magnitude of wavelet subband coefficients to extract significant statistics features, and employing support vector machines to detect the existence of hidden messages. Experimental results indicate that the messages embedded as small as 5% of the steganographic capacity can be reliably detected.

Anand Gupta et. al. [8] described that Steganography is the science of writing hidden messages in such a way that no one apart from the sender andintended recipient even realizes if there is any hidden message. Most of the research done before in this area is focused on images, audios, and videos but a less amount of work has been done on MS-Word documents which are identified with certain shortcomings. One of the major short coming in the previous method being large number of degenerations which were produced to embed a message, making it susceptible to active warden attack.

Cairong Li et. al. [9] proposed that Audio steganalysis has attracted more attentions recently. DSSS steganalysis is one of the most challenging research fields. In this paper, a novel algorithm to detect DSSS steganography in audio signal is proposed. Firstly, it takes DWT transform of special segment of audio and takes the detail sub-band coefficients, and then uses GMM to model the coefficients. Secondly, in order to monitor the effect of DSSS hiding, The Author calculated the GMM PDF (possibility density function) as to measure the difference. Thirdly, considering the two variables composed of wavelet coefficients and GMM PDF, the multivariate skewness and kurtosis were taken as features. Lastly, the SVM classifier is utilized for classification. All of the 800 various audios are trained and tested in our experimental work. With various embedding parameters for training and testing audios, the proposed algorithm can achieve a good classification, and the correct rate of detecting is up to 80%.

Zhiping Zhang et. al. [10] designs an audio covert communication system based on spread spectrum (SS) data hiding technology. Considering the characteristics of covert communication, some

methods were proposed to solve the key problems in the system. Firstly, the system employed M-array SS coding combining with return-to-zero base band code to embed hiding data. In addition, the sender embedded the base band clock in audio signal for synchronization. Furthermore, Reed Solomon (RS) channel coding was applied in the system for error correction. This system was tested through an audio line and a FM audio broadcast platform as communication channels. Experiment results showed that the data error rates were 0.024% via audio line and 0.288% via FM audio when the hiding data rate was 7.8 bytes/s.

Kaliappan Gopalan et. al. [11] described that Audio steganography using bit modification of time domain audio samples is a simple technique for multimedia data embedding with potential for large payload. Depending on the index of the bit used to modify the samples in accordance with the data to be hidden, the resulting stego audio signal may become perceptible and/or susceptible to incorrect retrieval of the hidden data. This paper presents some results of the trade off between the conflicting requirements of data robustness, payload and imperceptibility. Experimental results on both clean and noisy host audio signals indicate that while the payload can be as high as over 3000 bits/s – much higher rate than common audio data embedding techniques –notice ability of embedding is decreased and noise tolerance increased by using higher bit indices than the traditional least significant bit.

Marcus Nutzinger et. al. [12] proposed that Steganography is used to embed secret messages in cover media. This is especially important in areas, where the use of cryptography is prohibited. In this paper, The Author introduced a novel hybrid steganographic algorithm for digital audio data. The Author enhanced a direct sequence spread spectrum (DSSS) system with aspects of frequency hopping to vary the carrier frequency of the binary phase shift keying (BPSK) signal, representing the secret message. Further, The Author adopted the number of chips per secret bit. These modifications give a more secure steganographic system, making guesses about the bit-rate or message length less feasible.

Rizky M. Nugraha et. al. [13] described that image steganography has widely developed. There are also many algorithm developed for it. Mean while, the interest in using audio data as cover object in steganography can be spelled out late emergence than image data. This paper discussed the implementation of steganography in audio data using Direct Sequence Spread Spectrum method. Spread Spectrum method is often used to send hidden message through radio waves. This message is transmitted through noise-like wave. The same method can be applied to embed message in audio data. The embedded audio data will be heard as noise. The Spread Spectrum method used in this paper is Direct Sequence Spread Spectrum. A key is needed to embed messages into noise, this key is used to generate pseudo-noise wave.

Sarosh K. Dastoor [14] proposed that Secure data exchange is inevitable in the current era of Information Technology, for avoiding the eave-droppers. To substantiate the same, various Steganography techniques are presented in this paper to be employed with the mobile communication. Steganography deals with the skill of concealing digital information in multi-media. Audio Steganography using Low Bit encoding method, Modified Least Significant Bit (LSB) method, Alternate LSB method, Spread Spectrum method and Echo-hiding method are presented here. All the methods described above are well in existence, so a novel method of Alternate Bit Encoding is also presented with its comparison to the available methods. Usually, human ears perceive higher sounds better than the lower ones, and it is thus easier to hide data among low sounds without the human ear noticing the alteration.

Bo Liu et. al. [15] described that Nowadays, enterprises and individuals are increasing tending to store their data in the cloud storage systems yet, these sensitive data will face serious security threats. Currently, cloud storage service providers mainly adopt encryption and authentication to protect sensitive data, and a lot of approaches have been proposed to ensure data security in cloud storage systems. Recently, audio steganography has been regarded as serious attacking measures to threaten cloud storage systems. Nevertheless, little research has been focused on thwarting the Audio steganography Attacks in Cloud Storage Systems.

Muhammad Asad et. al. [16] proposed that increased use of electronic communication has given birth to new ways of transmitting information securely. Audio steganography is the science of hiding some secret text or audio information in a host message. The host message before steganography and stego message after steganography have the same characteristics. Least Significant Digit (LSD) modification technique is the most simple and efficient technique used for audio steganography. The conventional LSD modification technique is vulnerable to steganalysis.

Samples of Host Message = 8 * Bits of Secret Message

The stego message formed on the basis of proposed methodology cannot be differentiated from host message. The secret message on the receiver side can be extracted from the stego message as well.

Saswati Ghosh et. al. [17] presents a double layered secure data transfer technique using Cryptography and Audio Steganography for mobile network. Firstly, the characters of secret text message are converted to bit values and are encrypted by XOR operation using a Symmetric key. Then using a secret key-box, it is again scrambled and then divided into 2 bit blocks. These blocks from MSB are replaced by the Left Significant two bits of each byte of cover audio bit stream.

Pooja P. Balgurgi et. al. [18] stated that security has its importance and application in wide area. It is a measure of human negligence, in desire to seize the latest technological inventions. This measure may have adverse effect on human perception to the deployment of application, which needs serious concern in terms of security. Audio steganography is a technique used to transmit hidden information by modifying an audio signal in an imperceptible manner. The main challenge in audio steganography is to obtain robust high capacity steganographic systems. This paper provides implementation of two level encryption of user data by combining two areas of network security, cryptography and steganography.

Ming Li et. al. [19] states that the problem of extracting blindly data embedded over a wide band in a spectrum (transform) domain of a digital medium (image, audio, video). The Author developed a novel multi carrier signature iterative generalized least-squares (M-IGLS) core procedure to seek unknown data hidden in hosts via multi carrier spread-spectrum embedding. Neither the original host nor the embedding carriers are assumed available. Experimental studies on images show that the developed algorithm can achieve recovery probability of error close to what may be attained with known embedding carriers and host auto correlation matrix. The Author considered the problem of blindly extracting unknown messages hidden in image hosts via multicarrier/signature spread-spectrum embedding. Neither the original host nor the embedding carriers are assumed available.

In [20] authors provided the comparison of available steganography technology hiding text in an image file using Least Significant Bit (LSB) based Steganography, Discrete Cosine Transform (DCT) based Steganography and Discrete Wavelet Transform (DWT) based steganography. The LSB algorithm is implemented in spatial domain in which the payload bits are embedded into the least significant bits of cover image to derive the stego-image whereas DCT & DWT algorithm are implemented in frequency domain in which the stego -image is transformed from spatial domain to the frequency domain.

In [21] author described an efficient method to audio steganography based on modification of Least Significant Bit Technique using Random Keys. This approach maintains high data hiding capacity like LSB substitution but maintains a much better security level, which is not present in LSB substitution as LSB substitution technique is predictable. As the hidden information is highly randomized, so it is difficult for attacker to retrieve the secret information from stego object.

IV. CONCLUSION

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. Steganography is not a new form of science. Steganography works by replacing bits of useless or unused data in regular computer files such as graphics, sound, text, HTML, or even video with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images. In a computer-based audio Steganography system, secret messages are embedded in digital sound. The secret message is embedded by slightly altering the binary sequence of a sound file. Existing audio Steganography software can embed messages in WAV, AU, and even MP3 sound files. Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images. These methods range from rather simple algorithms that insert information in the form of signal noise to more powerful methods that exploit sophisticated signal processing techniques to hide information. In this paper we provide a literature review on various audio steganography techniques.

REFERENCES

[1] V. K. Pachghare, Cryptography & Information Security, Prentice-hall of India Pvt Ltd.

[2] Eric Cole, Hiding in Plain Text, Wiley Publishing, Inc. : 2003.

[3] Stefan Katzenbeisser and Fabien A. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, Inc., Norwood, MA, USA, 2000.

[4]. Bhagyashri A. Patil, Vrishali A. Chakkarwar, “Review of an Improved Audio Steganographic Technique over LSB through Random Based Approach”. IOSR Journal of Computer Engineering

(IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727 Volume 9, Issue 1 (Jan. - Feb. 2013), PP 30-34 www.iosrjournals.org.

[5]. Rashid Ansari, Hafiz Malik, AshfaqKhokhar," Data-Hiding in Audio Using Frequency-Selective Phase Alteration".0-7803-8484-9/04/$20.00, 4004 IEEE, V-389, ICASSP 2004.

[6]. Mark Sterling, Edward L. Titlebaum, Xiaoxiao Dong, Mark F. Bocko, "An Adaptive Spread Spectrum Data Hiding Technique For Digital Audio". 0-7803-8874-7/05/$20.00 ©2005 IEEE, V – 685, ICASSP 2005.

[7]. Xue-Min RU , Hong-Juan Zhang , Xiao Huang, "Steganalysis of Audio: Attacking The Steghide". Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou, 18-21 August 2005.

[8]. Anand Gupta, Deepak Kumar Barr, DeepaliSharma, "Mitigating the Degenerations in Microsoft Word Documents: An Improved Steganographic Method". 978-1-4244-3314-809$25.00 2009 IEEE.

[9]. Cairong Li, Wei Zeng, Haojun Ai, RuiminHu, "Steganalysis of Spread Spectrum Hiding Based on DWT and GMM". 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing.

[10]. Zhiping Zhang Xihong Wu ," An Audio Covert Communication System for Anolog Channels". 2010 International Conference on Electrical and Control Engineering".

[11]. Kaliappan Gopalan, "Audio Steganography using Bit Modification – A Tradeoff on Perceptibility and Data Robustness for Large Payload Audio Embedding". 978-1-4244-7116-4/10/$26.00 ©2010 IEEE.

[12]. Marcus Nutzinger, Christian Fabian, Marion Marschalek, "Secure Hybrid Spread Spectrum System for Steganography in Auditive Media". 2010 sixth International conference on Intelligent Information Hiding and Multimedia Signal Processing.

[13].Rizky M. Nugraha, "Implementation of Direct Sequence Spread Spectrum Steganography on Audio Data". 2011 International Conference on Electrical Engineering and Informatics 17-19 July 2011, Bandung, Indonesia.

[14]. Sarosh K. Dastoor, "Comparative Analysis of Steganographic Algorithms intacting the information in the Speech Signal for enhancing the Message Security in next Generation Mobile devices" . 978-1-4673-0126-8/11/$26.00_c 2011 IEEE.

[15]. Bo Liu, ErciXu, Jin Wang, Ziling Wei, LiyangXu, Baokang Zhao, Jinshu Su , "Thwarting Audio Steganography Attacks in Cloud Storage Systems". 2011 International Conference on Cloud and Service Computing.

[16]. Muhammad Asad, JunaidGilani, Adnan Khalid, "An Enhanced Least Significant Bit Modification Technique for Audio Steganography". 978-1-61284-941-6/111$26.00 ©2011 IEEE.

[17]. Saswati Ghosh, Debashis De, DebdattaKandar, "A Double Layered Additive Space Sequenced Audio Steganography Technique for Mobile Network", International Conference on Radar, Communication and Computing (ICRCC), 21 - 22 Dec, 2012. pp.29-33.

[18]. Pooja P. Balgurgi, Prof. Sonal K. Jagtap, "Intelligent Processing : An Approach of Audio Steganography".2012 International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 19-20, Mumbai, India.

[19]. Ming Li,, Michel K. Kulhandjian, Dimitris A. Pados, *E*, Stella N. Batalama and Michael J. Medley, "Extracting Spread-Spectrum Hidden Data From Digital Media", IEEE Transactions On Information Forensics And Security, VOL. 8, NO. 7, JULY 2013.

[20] Navneet Kaur, Sunny Behal, "A Survey on various types of Steganography and Analysis of Hiding Techniques", International Journal of Engineering Trends and Technology (IJETT) – Volume 11 Number 8 - May 2014.

[21] Ali M. Meligy, "An Efficient Method to Audio Steganography based on Modification of Least Significant Bit Technique using Random Keys", I. J. Computer Network and Information Security, pp. 24-29, June 2015.