An Extensive Literature Survey on Audio Steganography

Priyanka Sengar[1], Prof. Bhupchandra Kumhar[2]
[1]M-Tech Research Scholar, [2]Research Guide & HOD,
IES College of Science & Technology, Bhopal

Abstract- The word Steganography strictly means covered or hidden writing. Its ancient origins can be traced back to 440 BC. Although the term steganography was only coined at the end of the 15th century, the use of steganography dates back several millennia. In ancient times, messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves. Invisible ink has been in use for centuries for fun by children and students and for serious undercover work by spies and terrorists. The majority of today's steganographic systems uses multimedia objects like image, audio, video etc as cover media because people often transmit digital pictures over email and other Internet communication. In this research work we have been studying different aspects of Digital Image Steganography in order to improve the strength of this demandable methodology for security proposes.

Keywords- Audio Steganography, Sound Pressure level (SPL), DWT, LSB & PSNR.

I. INTRODUCTION

Steganography The word steganography is derived from the Greek words stegos meaning cover and grafia meaning writing [1] defining it as covered writing. In image steganography the information is hidden exclusively in images. Steganography is the art and science of secret communication .It is the practice of encoding/embedding secret information in a manner such that the existence of the information is invisible. The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message it is referred to as stego-medium. A stego-key is used for hiding/encoding process to restrict detection or extraction of the embedded data [2].

Steganography

- *Steganography Hide the messages inside the Cover medium, Many Carrier formats.*

- *Breaking of steganography is known as Steganalysis.*

- *Cryptography Encrypt the message before sending to the destination, no need of carrier/cover medium.*

- *Breaking of cryptography is known as Cryptanalysis.*

Steganographying and fingerprinting related to steganography are basically used for intellectual property protection. A digital steganography is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. The embedded information in a steganography object is a signature refers the ownership of the data in order to ensure copyright protection. In fingerprinting, different and specific marks are embedded in the copies of the work that different customers are supposed to get. In this case, it becomes easy for the property owner to find out such customers who give themselves the right to violate their licensing agreement when they illegally transmit the property to other groups [1].

II. SYSTEM MODEL

Frequency masking is a frequency domain phenomenon where a low level signal, e.g. a pure tone, can be made inaudible by a simultaneously appearing stronger signal (the masker), e.g. a narrow band noise, if the masker and maskee are close enough to every other in frequency. A masking threshold can be derived below that any signal will not be audible. The masking threshold depends on the masker and on the characteristics of the masker and maskee (narrowband noise or pure tone). The masking threshold for the sound pressure level equal to 60 dB, the masker in Fig. 1 at around 1 kHz, the SPL of the maskee can be surprisingly high - it will be masked as long as its SPL is below the masking threshold. The slope of the masking threshold is steeper toward lower frequencies; in other words, higher frequencies tend to be more easily masked than lower frequencies. It should be pointed out that the distance between masking level and masking threshold is smaller in noise-masks- tone experiments than in tone-masks-noise experiments due to HAS's sensitivity toward additive noise. Noise and low-level signal components are masked inside and outside the particular critical band if their SPL is below the masking threshold. Noise contributions can be coding noise, inserted steganography sequence, aliasing distortions, etc. Without a masker, a signal is inaudible if its SPL is below the threshold in quiet, that depends on frequency and covers a dynamic range of more than 70 dB as depicted in the lower curve of Fig 1. The qualitative sketch of Fig 1 gives more details about the masking threshold. The distance between the level of the masker (given as a tone in Fig 1) and the masking threshold is called signal-to-mask ratio.

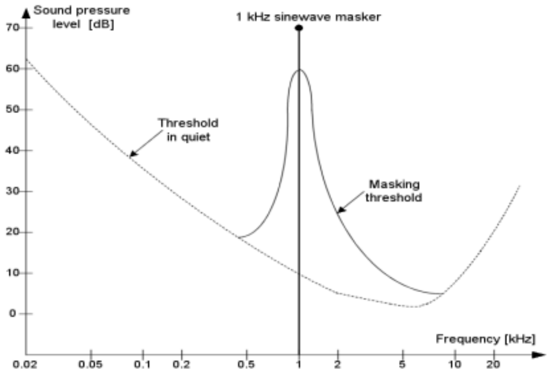

Fig.1. Frequency masking in the human auditory scheme (HAS), reference sound pressure level is $p_0 \;=\; 2 \,\cdot\, 10^{-5}\, Pa$.

Its maximum value is at the left border of the critical band. Within a critical band, noise caused by steganography embedding will be audible as long as signal-to-noise ratio (SNR) for the critical band is higher than its SMR. Let SNR(m) be the signal-to-noise ratio resulting from steganography insertion in the critical band m; the perceivable distortion in a given subband is then measured by the noise to mask ratio:

NMR (m) = SMR-SNR (m)

The noise-to-mask ratio NMR (m) expresses the difference between the steganography noise in a given critical band and the level where a distortion may just become audible; its value in dB should be negative.

III. LITERATURE REVIEW

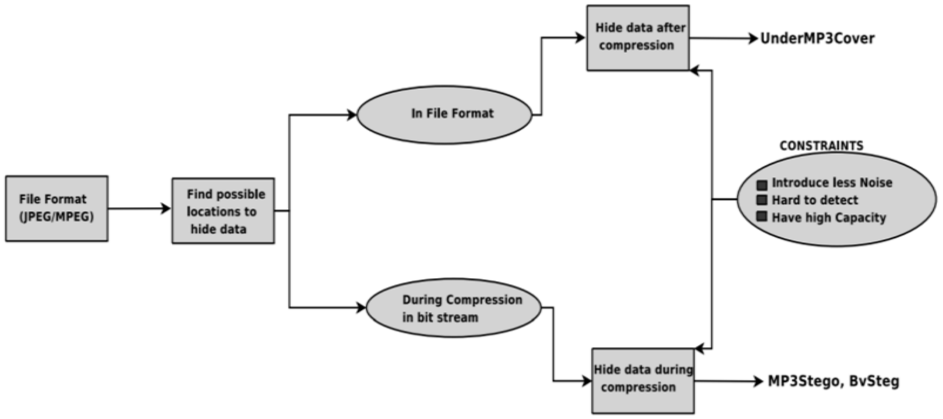

Fig.2. Shows BvSteg tool method in the work is a MP3 steganography

The term steganography came into use in 1500s after the appearance of Trithemius book on the subject Steganographic [3]. The word Steganography strictly means covered or hidden writing. Its ancient origins can be traced back to 440 BC. Although the term steganography was only coined at the end of the 15th century, the use of steganography dates back several millennia. In ancient times, messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves. Invisible ink has been in use for centuries for fun by children and students and for serious undercover work by spies and terrorists [9].

The majority of today’s steganographic systems uses multimedia objects like image, audio, video etc as cover media because people often transmit digital pictures over email and other Internet communication. Modern steganography uses the opportunity of hiding information into digital multimedia files and also at the network packet level[4]. Hiding information into a medium requires following elements [2]

I. The cover medium(C) that will hold the secret message.

II. The secret message (M), may be plain text, digital image file or any type of data.

III. The steganographic techniques

IV. A stego-key (K) may be used to hide and unhide the message.

In modern approach, depending on the cover medium, steganography can be divided into five types:

a. Text Steganography
b. Image Steganography
c. Audio Steganography
d. Video Steganography
e. Protocol Steganography

• Text steganography Hiding information in text file is the most common method of steganography. The method was to hide a secret message into a text message. After coming of Internet and different type of digital file formats it has decreased in importance. Text stenography using digital files is not used very often because the text files have a very small amount of excess data.

• Image steganography Images are used as the popular cover medium for steganography. A message is embedded in a digital image using an embedding algorithm, using the secret key. The resulting stego-image is send to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego- image unauthenticated persons can only notice the transmission of an image but may not see the existence of the hidden message.

• Audio steganography 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. An audible, sound can be inaudible in the presence of another louder audible sound .This property allows to select the channel in which to hide information [2]. Existing audio steganography software can embed messages in WAV and MP3 sound files. The list of methods that are commonly used for audio steganography are listed and discussed below. • LSB coding

- *Parity coding*
- *Phase coding*
- *Spread spectrum*
- *Echo hiding*
- *Video steganography Video Steganography is a technique to hide any kind of files in any extension into a carrying Video file.*
- *Protocol steganography The term protocol steganography is to embedding information within network protocols such as TCP/IP.*

IV. APPLICATIONSOF STEGANOGRAPHY

Secret Communications -The use steganography does not advertise secret communication and therefore avoids scrutiny of the sender, message, and recipient. A trade secret, blueprint, or other sensitive information can be transmitted without alerting potential attackers. Feature Tagging Elements may be embedded inside an image, such as the names of individuals in a photo or locations in a map. Copying the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features. Copyright Protection Copy protection mechanisms that prevent data, usually digital data, from being copied.

The insertion and analysis of steganography to protect copyrighted material is responsible for the recent rise of interest in digital steganography and data embedding. Steganography signature in the host image, algorithm will instead try to prove that the adversary’s image is derived from the original steganography image. Such an algorithm provides indirect evidence that it is more probable that the real owner owns the disputed image, because he is the one who has the version from which the other two were created. Authentication and tampering detection In the content authentication applications, a set of secondary data is embedded in the host multimedia signal and is later used to determine whether the host signal was tampered. The robustness against removing the steganography or making it undetectable is not a concern as there is no such motivation from attacker’s point of view. However, forging a valid authentication steganography in an unauthorized or tampered host signal must be prevented. In practical applications it is also desirable to locate (in time or spatial dimension) and to discriminate the unintentional modifications (e.g. distortions incurred due to moderate MPEG compression) from content tampering itself. In general, the steganography embedding capacity has to be high to satisfy the need for more additional data than in ownership protection applications. The detection must be performed without the original host signal because either the original is unavailable or its integrity has yet to be established. This kind of steganography detection is usually called a blind detection.

Fingerprinting Additional data embedded by steganography in the fingerprinting applications are used to trace the originator or recipients of a particular copy of multimedia file. Steganography carrying different serial or identity numbers are embedded in different copies of music CDs or DVDs before distributing them to a large number of recipients. The algorithms implemented in fingerprinting applications must show high robustness against intentional attacks and signal processing modifications such as loss compression or filtering. Fingerprinting also requires good anti-collusion properties of the algorithms, i.e. it is not possible to embed more than one ID number to the host multimedia file, and otherwise the detector is not able to distinguish which copy is present. The embedding capacity required by fingerprinting applications is in the range of the capacity needed in copyright protection applications, with a few bits per second. Broadcast monitoring a variety of applications for audio steganography are in the field of broadcasting.

V. RESEARCH PROPOSAL

Steganography is an obvious alternative method of coding identification information for an active broadcast monitoring. It has the advantage of being embedded within the multimedia host signal itself rather than exploiting a particular segment of the broadcast signal. Thus, it is compatible with the already installed base of broadcast equipment, including digital and analogue communication channels. The primary drawback is that embedding process is more complex than a simple placing data into file headers. There is also a concern, especially on the part of content creators, that the steganography would introduce distortions and degrade the visual or audio quality of multimedia. A number of broadcast monitoring steganography-based applications are already available on commercial basis. These include program type identification, advertising research, broadcast coverage research etc. Users are able to receive a detailed proof of the performance information that allows them to:

I. Verify that the correct program and its associated promos aired as contracted.

II. Track barter advertising within programming.
III. Automatically track multimedia within programs using automated software online. Copy control and access control in the copy control application; the embedded steganography represents a certain copy control or access control policy.

VI. CONCLUSION

In this review work we have studied about steganography detector that usually integrated in a recording or playback system, like in the proposed DVD copy control algorithm or during the development Secure Digital Music Initiative in order to improve the efficiency of steganography method. After a steganography has been detected and content decoded, the copy control or access control policy is enforced by directing particular hardware or software operations such as enabling or disabling the record module. These applications require steganography algorithms resistant against intentional attacks and signal processing modifications, able to perform a blind steganography detection and capable of embedding a non-trivial number of bits in the host signal. Information carrier the embedded steganography in this application is expected to have a high capacity and to be detected and decoded using a blind detection algorithm. While the robustness against intentional attack is not required, a certain degree of robustness against common processing like MPEG compression may be desired.

REFERENCES

[1] Gupta, N.; Sharma, N., "Dwt and Lsb based Audio Steganography", Process of IEEE Optimization, Reliabilty, and Information Technology (ICROIT), 2014 International Conference on , vol., no., pp.428,431, 6-8 Feb. 2014.

[2] Bugár, G.; Bánoci, V.; Broda, M.; Levický, D.; Dupák, D., "Data hiding in still images based on blind algorithm of steganography" Radioelektronika (RADIOELEKTRONIKA), In proc. 24th IEEE International Conference , vol., no., pp.1,4, 15-16 April 2014.

[3] Geethavani, B.; Prasad, E.V.; Roopa, R., "A new approach for secure data transfer in audio signals using DWT" In Proc. IEEE Advanced Computing Technologies (ICACT), 15th International Conference on , vol., no., pp.1,6, 21-22 Sept. 2013.

[4] Khademi, Mahdi; Tinati, M.A., "Audio steganography by using of linear predictive coding analysis in the safe places of discrete wavelet transform domain" In Proc. IEEE Electrical Engineering (ICEE), 19th Iranian Conference on , vol., no., pp.1-5, 17-19 May 2011.

[5] Zhang Kexin, "Audio steganalysis of spread spectrum hiding based on statistical moment" In Proc. IEEE Signal Processing (ICSPS), 2nd International Conference on , vol.3, no., pp.V3-381,V3-384, 5-7 July 2010.

[6] Cairong Li; Wei Zeng; Haojun Ai; Ruimin Hu, "Steganalysis of Spread Spectrum Hiding Based on DWT and GMM" In Proc. IEEE Networks Security, Wireless Communications and Trusted Computing, NSWCTC '09. International Conference on , vol.1, no., pp.240,243, 25-26 April 2009.

[7] Wang Junjie; Mo Qian; Mei Dongxia; Yao Jun, "Research for Synchronic Audio Information Hiding Approach Based on DWT Domain" In Proc. IEEE E-

Business and Information Scheme Security. EBISS '09. International Conference on , vol., no., pp.1,5, 23-24 May 2009.

[8] Johnson N & Jajodia S, Steganalysis: the investigation of hidden information. In: Proc. IEEE Information Technology Conference, Syracuse, NY, p 113–116, 3 Sept. 1998.

[9] Katzenbeisser S & Petitcolas F, Information Hiding Techniques for Steganography and Digital Steganography. Artech House, Norwood, MA. 1999.

[10] Bender W, Gruhl D & Morimoto N, Anthony lu, “Techniques for data hiding”. IBM Journal 35(3): p 313–336,1996.

[11] M. Wu, B.Liu. "Multimedia Data Hiding", Springer-Verlag New York, 2003

[12] R. Anderson, F .Petitcol as: Onthelimits of the steganography, IEEE Journal Selected Areas in Communications, VOL .16, NO. 4 , MAY 1998.

[13] N F. Johnson. Steganography tools. Available from: http://www.jjtc.com/Security/stegtools.htm 2005.