AUDIO STEGANOGRAPHY FOR SECURE DATA COMMUNICATION: A REVIEW

[1]Aakash Vishwakarma, [2]Prof. Neeta Nathani

[1]M.Tech. Scholar, [2]Assistant Professor,
GGCT, Jabalpur

Abstract: **Today there are various applications of information hiding. Knowledge of data hiding might be used either in ethical or unethical ways. However, data hiding algorithms cannot easily be categorized either in steganography or watermarking categories as there is no transparent boundary between these two terms & mostly classification relies on application of algorithm. Therefore regardless classifying data hiding most common data hiding applications are fingerprinting, secret communication, secure storage, covert communication, & copyright protection. Cryptography modify messages so it can't be understood. Main advantages of cryptography includes secured data, different size key for data hiding, fast & flexible ease of design. The main disadvantage of cryptography is that it is not god for internet and is limited to devices like mobile phones, has complex hardware and its cipher patterns is not typical. Steganography is an ancient art of hiding information. This paper presents a survey on audio steganography and its recent researches.**

Keywords: **Mean Square Error, Signal to Noise, Cover audio, Stegno object**

I. INTRODUCTION

The specific word steganography originates from Greek 'Steganos', which refers to covered or secret & 'graphy' refers to writing or drawing. Thus, steganography means, covered writing literally. Steganography is a science of data hiding information in manner that its presence cannot be observed when communication is happening. Private information is encoded in a specific way such that very existence of information is disguised. Along with existing communication methods, steganography is useful to carry out hidden exchanges. The steganography model is shown in Figure 1. Message or actual data is that which a user wishes to transmit and to make it confidential. It may be a plain text, edited text, some image, or anything that can be present as a bit stream like as a copyright mark, a communication document, or a serial number.

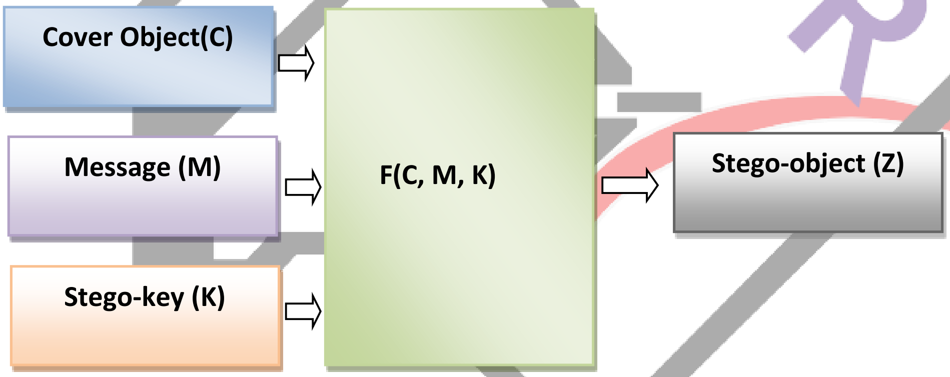

Figure 1 Basic Steganography Model

This method uses a password known as steganography-key. It makes sure that only receiving end user who holds corresponding decoding key will be able to detect message from a cover-object. Message carrier with securely embedded message is then called 'stenography object' (SO).

The aim of steganography is to avoid having suspicion to even existence of a hidden message. This method of information hiding technique has recently become critical in a number of application areas. Digital video, audio, & pictures are generally furnished with distinguishing imperceptible marks which can contain a hidden copyright notice or a serial number or also help to prevent unwanted copying directly.

The implementation of cryptographic & steganography (Audio) tools of hiding information which can be text & image files. Audio part will be an interleave scaled data hiding. Two types of approaches being explored first modulo approach of cryptography cipher generation & second sliced audio steganography.

II. LITERATURE WORK

Qilin Qi et al et al [1] they presented an active audio attacking method that can modify the audio signal to make the hidden information unable to be recovered while keeping the audio in a tolerable distortion level. The attacking method is based on a proposed transform called discrete spring transform which disables the synchronization of the hidden information. The analysis and simulation results show that the proposed method outperforms some of existing audio steganogtaphy methods which are resist to the time scale modification.

B.Geethavani et al [2]they proposed system is considered to be an efficient method for hiding text in audio files such that data can reach the destination in a safe manner without being modified. PSNR and MSE values for various types of audio files have been recorded. Using the method of embedding technique by DWT along with the encryption and decryption of the secret message using Blowfish algorithm, makes data more secure and transparency is minimized. Jayaram P et al [3] they have introduced a robust method of imperceptible audio data hiding. Thus they conclude that audio data hiding techniques can be used for a number of purposes other than covert communication or deniable data storage, information tracing and finger printing, tamper detection.

Watermarking of audio signals is more challenging as compared to the watermarking of images or video sequences, due to wider dynamic range of the HAS in comparison with human visual system (HVS) by Bender W et al [5]. The HVS perceives sounds over a range of power greater than 109:1 and a range of frequencies greater than 103:1. The sensitivity of the HAS to the additive white Gaussian noise (AWGN) is high as well as this noise in a sound file can be detected as low as 70 dB below ambient level Nedeljko Cvej [6]. Some commonly used methods of audio steganography are listed and discussed below in brief [7,8]. One of the earliest techniques studied in the information hiding of digital audio (as well as other media types) is Least Significant Bit (LSB) coding. In this technique, LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message. In Echo data hiding, text can be embedded in audio data by introducing an echo to the original signal [7]. The data is then hidden by varying three parameters of the echo: initial amplitude, decay rate, and offset. If only one echo is produced from the original signal, then only one bit of information could be encoded.

Spread Spectrum (SS) by Akram M. Zeki et al attempts to spread out the encoded data across the available frequencies as much as possible [8]. This is analogous to a system using an implementation of the LSB coding that randomly spreads the message bits over the entire sound file. However, unlike LSB coding, the SS method spreads the secret message over the sound file's frequency spectrum, using a code that is independent of the actual signal. As a result, the final signal occupies a bandwidth in excess of what is actually required for transmission. It offers the advantage of moderate data transmission rate while maintaining a high level of robustness. It can introduce noise into a sound file which offers a disadvantage.

Nedeljko Cvejic et al [14] presents another high bit rate LSB audio watermarking and steganography method. The basic idea of the proposed LSB algorithm is a watermark embedding that causes minimal embedding distortion of the host audio. Using the two-step algorithm, watermark bits are embedded into higher LSB layers, resulting in increased robustness against noise addition or MPEG compression. It has been observed in Listening tests that the perceptual quality of watermarked audio is higher in this case than in the standard LSB method.

Ajay.B.Gadicha [15] explores another fourth bit rate LSB audio steganography method that reduces embedding distortion of the host audio. Using the proposed algorithm, message bits are embedded into fourth LSB layer, resulting in increased robustness against noise addition. They developed a novel method that is able to shift the limit for transparent data hiding in audio from the first LSB layer to the fourth LSB layer, using a two-step approach. In the first step, a watermark bit is embedded into the 4th LSB layer of the host audio using a novel LSB coding method. In addition to decreasing objective quality measure, expressed as signal to noise ratio (SNR) value, proposed method introduces noise shaping in order in the second step of embedding to increase perceptual transparency of the method. A table of literature review is mentioned in Table1.

Table 1: Literature Review

Author name with year	**Paper Title**	**Algorithm Used**	**Advantages**	**Disadvantages**
Qilin Qi, IEEE, 2017	An Active Audio Steganography Attacking Method using Discrete Spring Transform	discrete spring transform for decomposing audio	acceptable audio distortion level then scale modification method	discrete spring transform is a complex and time consuming method
B.Geethavani, IEEE, 2016	A New Approach for Secure Data Transfer in Audio Signals Using DWT	discrete wavelet transform for decomposing audio	Less distortion and fast	audio distortion level is moderate
Jayaram P, IEEE,2016	Information hiding using audio steganography – a survey	Key based Audio scaling according to data	Very fast and high throughput	Suitable for known audio file, high audio distortion level

III. PROBLEM FORMULATION

the problems in Audio steganography can be categorised as below

Encryption Keys: As known, data encryption is became necessary task of an IT specialist. More data encryption keys require are more tough IT administrative tasks of managing all of keys can be. If someone loses key to encryption, it is considered as lost data associated with it.

Expense: Data encryption can prove to be more costly because it requires systems that maintain data encryption it must have capability & upgrades to perform such kind of tasks. Without such capable systems, systems operations can be somewhat compromised.

Unrealistic Requirements: If an industry does not understand some of restraints use by data encryption technology, it is simple to set unrealistic standards & need which could affect data encryption security.

Compatibility: Data encryption technology can be tedious when someone layering it with closing programs & applications. This can negatively affect routine operations inside systemNetwork monitoring & surveillance systems will not flag messages & files that have steganography data. So, if someone needs to steal hidden confidential data, they could conceal it within different file & send it in a simple looking email.

Lot of data has to be transmitted which arises suspiciousness to hackers & intruders:

1. The solution for first problem: Making more difficult discovering which bits are embedded by modifying the bits else sending LSBs in samples, and selecting the samples to modify privately-not all samples.

2. The solution for second problem: Embedding the message bits in deeper layers and other bits alteration to decrease the amount of the error.

IV. CONCLUSION

This review paper is a literature study of available audio steganography methods. This paper mentions audio steganography and investigation of some recent approaches. Different methods like Modifying Quantized Spectrum Values of MPEG/Audio Layer III, Embedding data between frames in MP3 file, Quantized frequency domain embedding and reversible integer transforms, Information hiding in audio signals using Considering Parity and XORing of LSB's, Genetic-Algorithm- Based audio steganography, Increasing robustness of LSB audio steganography, Audio Wave Steganography were mentioned. On the basis of the literature survey, it can be concluded that there are some limitations of the available method in terms of amount of data to be hidden inside the audio file.

REFERENCES

[1] Qilin Qi, Aaron Sharp, Dongming Peng, Yaoqing Yang, and Hamid Sharif, An Active Audio Steganography Attacking Method using Discrete Spring Transform, IEEE 24th International Symposium on Personal, Indoor and Mobile Radio Communications: Services, Applications and Business Track, Vol. 05, Issue 07, IEEE, 2017

[2] B.Geethavani, E.V.Prasad, R.Roopa, A New Approach for Secure Data Transfer in Audio Signals Using DWT, IEEE, Advanced Computing Technologies (ICACT), DOI:10.1109/ICACT.2016.6710492, Vol 02, Issue 09, 21-22 Sept. 2016.pp 1-6

[3] Jayaram P, Ranganatha H R, Anupama H S, information hiding using audio steganography – a survey, The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, IEEE, August 2016

[4] Gunjan Nehru, Puja Dhar, A Detailed look of Audio Steganography Techniques using LSB and Genetic Algorithm Approach, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012

[5] Linu Babu, Jais John S, Parameshachari B D,Muruganantham C, H S DivakaraMurthy, Steganographic Method for Data Hiding in Audio Signals with LSB & DCT, International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 2, Issue. 8, August 2013, pg.54 – 62

[6] Nedeljko Cvej, Tapio Seppänen, Algorithms for audio watermarking and steganography, Oulu 2004, ISBN: 9514273842, IET-2004.

[7] Sos S. Agaian, David Akopian, Sunil A. D'Souza, Two algorithms in digital audio steganography using quantized frequency domain embedding and reversible integer transforms, Audio, Speech, and Language Processing,IEEE Transactions on, vol. 16, no. 3, pp. 629 –638, march 2008.

[8] Akram M. Zeki, and Shahidan Abdullah, "audio steg: methods", IEEE Transactions on, vol. 11, no. 5, pp. 834 –842, aug.2009.

[9] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee and Poulami Das, "A Tutorial Review on Steganography", in Acoustics, Speech, and Signal Processing, 2001. Proceedings. (ICASSP '01). 2001 IEEE International Conference on, vol. 3, 2001, pp. 1341–1344 vol.3..

[10] Beixing Deng, Jie Tan, Bo Yang, Xing Li, A Novel Steganography Method Based on Modifying Quantized Spectrum Values of MPEG/Audio Layer III, Proceedings of the 7th WSEAS International Conference on Applied Informatics and Communications, Athens, Greece, August 24- 26, 2007.

[11] Alaa Ismat Al-Attili, Osamah Abdulgader Al-Rababah, New technique for hiding data in audio file, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.7, July 2010.

[12] utsav kumar malviya, vivek singh rathore, champalal lalani, eight adjacent regression based image interpolation for hr images, international journal for research trends and innovation, 2019 ijrti | volume 4, issue 3 | issn: 2456-3315

[13] H.B.Kekre, Archana Athawale, Swarnalata Rao, Uttara Athawale, Information Hiding in Audio Signals, International Journal of Computer Applications (0975 – 8887) Volume 7– No.9, October 2010.

[14] Mazdak Zamani, Azizah A. Manaf, Rabiah B. Ahmad, A Genetic-Algorithm-Based Approach for Audio Steganography World Academy of Science, Engineering and Technology, Information Theory, IEEE Transactions on, vol. 47, no. 4, pp. 1423 –1443, may 2009.

[15] Nedeljko Cvejic, Tapio Seppänen, Increasing Robustness of LSB Audio Steganography Using a Novel Embedding Method, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04).

[16] Ajay.B.Gadicha1, Audio Wave Steganography, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume- 1, Issue-5, November 2011.