Survey on Real Time Audio Steganography

Mr.S.Rajesh, Mr.Vinay Jain

***Abstract*— Today huge demand of digital world requires data to be transmitted in a secure manner.Data transmission in public communication is not secure because of interception.The best solution for this problem is steganography.**
Audio steganography is the process of hiding the secret information by concealing in into another medium such as audio file. Least Significant Bit (LSB) modification technique is the most simple and efficient technique.

***Index Terms*— Steganography ,Audio Steganography,LSB,carrier & Data Hiding**

INTRODUCTION

Today's large demand of internet applications requires data to be transmitted in a secure manner. Data transmission in public communication system is not secure because of interception and improper manipulation by eaves dropper. In present day to day life, effective data hiding methods are needed due to attack made on data communication. The idea of communicating secretly is as old as communication itself. Information security is becoming very important part of our life now-a-days. Information hiding is the fundamental of information security. Security is defined as the degree of protection against danger, damage, loss, and criminal activity. Particularly when a sensitive message is to be delivered to a destination, authentication and confidentiality are required. Providing security for electronic documents is an important issue. In information security, confidential information or confidential data must only be used, accessed, disclosed or copied by users who have the authorization, and only when there is a real need. The term "Security through Obscurity" or "Security by Obscurity" is the belief that a system of any sort can be secure so long as nobody outside of its implementation group is allowed to find out anything about its internal mechanisms. Data hiding is considered as "Security by Obscurity" systems

Steganography or Stego as it often referred to in the IT community, literally means, "Covered writing" which is derived from the Greek language. Steganography is defined as follows,

"Steganography is the art and science of communicating in a way which hides the existence of the communication. The goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present".

In a digital world, Steganography and cryptography are both intended to protect information from unwanted parties. Both Steganography and Cryptography are excellent means by which to accomplish this but neither technology alone is perfect and both can be broken. It is for this reason that most experts would suggest using both to add multiple layers of security[3].

In this section we will discuss Steganography at length. We will start by looking at the different types of Steganography generally used in practice today along with some of the other principles that are used in Steganography.

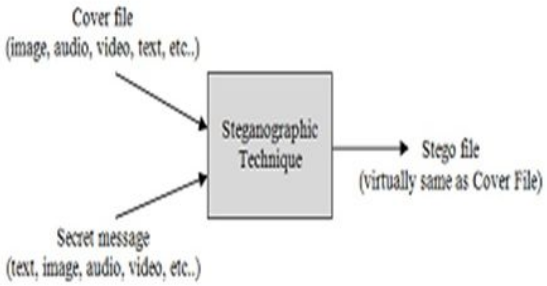

Figure 1 Steganography

There are basically three types of steganographic protocols used. They are Pure Steganography, Secret Key Steganography, and Public Key Steganography.

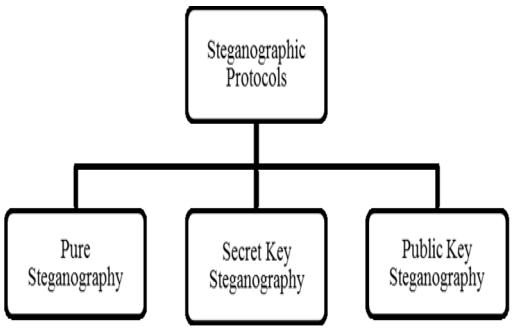

Figure 2 Steganographic Protocol

Audio Steganography Methods

Audio steganography is focused in hiding secret information in an innocent cover audio file or signal securely and robustly. Communication security and robustness are vital for transmitting important information to authorized entities while denying access to not permitted ones. By embedding secret information using an audio signal as a cover medium, the very existence of secret information is hidden away during communication. This is a serious and vital issue in some applications such as battlefield communications and banking transactions.

The secret message is concealed into the audio media by slightly changing the binary sequence of the audio file. Hiding secret information into digital audio media is generally more

Manuscript received April 30, 2016
S.Rajesh ,ME RESEARCH SCHOLAR SSGI BHILAI
Mr.Vinay Jain,Associate professor ,SSGI BHILAI

complicated than hiding secret information into other media, such as digital images.

In order to hide secret information successfully, a range of techniques for inserting information into digital audio have been introduced. These techniques vary from simple ones that embed information as signal noises to more powerful ones that take advantage of complicated signal processing techniques to embed the secret message.

II LITERATURE REVIEW

S.NO	TITLE	AUTHOR	NAME OF JOURNAL	REMARKS	CONCLUSION DRAWN
1	Audio steganography using LSB	Bankar Priyanka,Patil Komal,Shashikant	International Journal of electronics, Communication & Soft Computing Science & Engineering	In this proposed novel approach of submission technique of audiosteganography . Use-genetic algorithm.	To provide more security the original data file is encrypted Firstbefore embedding. And second purpose of this system is to increase robustness in case of security.
2	Audio Steganalysis With Content-Independent Distortion Measures	˙Ismail Avcıbas¸, *Member, IEEE*	IEEE signal processing letters, vol. 13, no. 2, february 2006	Contentindependent distortion measures are utilized as features for the classifier (steganalyzer)design.Experimental results show that the removal of content dependency from features enhances their discriminatory power	This methodology was Then used for audio steganalysis, where content-independent Distortion measures were used as features in the design Of linear regression classifier
3	Audio Steganography Using AES Algorithm	Mahalakshmi., Selvarani, Thilagam., N.Tharmini e	International Journal of Innovative Research in Science, Engineering and Technology(IJIRSET)	In this paper When performing data hiding on audio, first the data Is encrypted by password based encryption using AES algorithm to generate the cipher text. Now the cipher text is kept Hidden in the audio file using low bit encoding method. When extracting the data from audio first cipher text is Separated from audio then the plain text is generated by decrypting the cipher text	AES is a new cryptographic algorithm that can be used to protect electronicdata.Specifically, AES is an iterative,Symmetric-key block cipher that can use keys of 128, 192, and 256 bits, and encrypts and decrypts data in blocks of 128 bits(16 bytes). Unlike public-key ciphers, which use a pair of keys, symmetric key ciphers use the same key to Encrypt and decrypt data.
4	Efficient Method to Increase Robustness in Audio Steganography	DeepakD, Karthik M L , ManjunathAE	International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol.	In the modified LSB algorithm proposed here, instead of stuffing bit of the message only in the least significant bit in the consecutive bytes of wav file, a	In the proposed system , we made use of pattern while stuffing secret message in a channel of a wav file. In a similar fashion, we can even use a pattern to select channels of wav file to stuff the secret data and make it harder to be cracked. We

			1, Issue 6, December 2012	pattern is used to stuff bits. The same pattern can be made use to decode the file to get back the hidden message	can even make use of encryption and decryption algorithms and stuff cipher text instead of plain text and make it more robust
5	LSB Modification and Phase Encoding Technique of Audio Steganography Revisited	Prof. Samir Kumar, Bandyopadhyay Barnali, Gupta Banik	International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 4, June 2012	The basic idea is to split the original audio stream or cover File(C) into blocks and embed the whole message data Sequence into the phase spectrum of the first block	Disadvantages associated with phase coding are a low dataTransmission rate due to the fact that the secret message isEncoded in the first signal segment only and to extract the Secret message from the sound file
6	Increasing the Hiding Capacity of Low-Bit Encoding Audio Steganography Using a Novel Embedding Technique	R.F. Olanrewaju, Othman Khalifa and Husna binti Abdul Rahman	World Applied Sciences Journal 21 (Mathematical Applications in Engineering): 79-83, 2013	The proposed scheme uses text as the secret data to be hidden in the LSB of audio file taken as cover object because the size of the file is generally small compared to the size of the audio file in which it must be taken	The method does not Changed the size of file even after encoding process, thus This method is suitable for hiding any type of audio data
7	Audio Steganography using Parity Method at higher LSB layer as a variant of LSB Technique	Jyoti Bahl1, Dr. R. Ramakishore2	International Journal of Innovative Research in Computer And Communication Engineering Vol. 3, Issue 7, July 2015	In this variant parity method is used for encryption of text and text hiding is implemented at higher LSB layer to achieve High security, high data rate and robustness	The paper has possibility of improvements with respect to different type of data hiding like hiding of image into audio,Hiding of audio inside audio
8	An Efficient Method for Image and Audio Steganography using Least Significant Bit (LSB) Substitution	Ankit Chadha, Neha Satam, Rakshak Sood, Dattatray Bade	International Journal of Computer Applications (0975 – 8887) Volume 77– No.13, September 2013	Data hiding in audio, Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) both are used. All the results displayed prove to be time-efficient and effective Also the algorithm is tested for various numbers of bits. For those values of bits,	The use of only one LSB of the host audio sample gives capacity of 44.1 kbps. The obvious disadvantage is the extremely low robustness of the method, due to fact that random changes of the lsbs destroy the coded watermark

				Mean Square Error (MSE) and Peak-Signal-to-Noise-Ratio (PSNR) are calculated and plotted.	
9	Information hiding using audio Steganography – a survey	Jayaram , Ranganatha, Anupama	The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011	In computing, the least significant bit (LSB) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The LSB is sometimes referred to As the right-most bit, due to the convention in positional notation of writing less significant digit Further to the right. It is analogous to the least significant digit of a decimal integer, which is the Digit in the ones (right-most) position	In this paper we have introduced a robust method of imperceptible audio data hiding. Thus we Conclude that audio data hiding techniques can be used for a number of purposes other than covert Th International Journal of Multimedia & Its Applicationscommunicatio-n or deniable data storage, information tracing and finger printing, tamper Detection. As the sky is not limit so is not for the development. Man is now pushing away its own Boundaries to make every thought possible
10	An Optimized Method for Concealing Data using Audio Steganography	Md. Shafakhatullah Khan, V.Vijaya Bhasker, V. Shiva Nagaraju	International Journal of Computer Applications (0975 – 8887) Volume 33– No.4, November 2011	Basically this method calculates the frequency masking Threshold using psycho acoustic model, data signal is spread by a M-sequence code, and the spread signal is embedded in audio below the frequency masking threshold	This proposed system is to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safe manner
11	A Steganography Method Based on Hiding secrete data in MPEG/Audio Layer III	Mohammed Salem Atoum, Mamoun Suleiman Al Rababaa, Dr. Subariah Ibrahim	IJCSNS International Journal of Computer 184 Science and Network Security, VOL.11 No.5, May 2011	In Proposed a method by compressing MP3 and modifying Spectrum values of audio layers to embed secret information Into audios especially music files in MP3.This method can Extract secret information without original audio and it has	It is also considered highly secure since data is Encrypted using RSA algorithm before embedding data Which makes the system secure especially agents Passive attack.

				Characteristics that information hiding technique must beresponsible for prerequisites	
12	Information hiding by using Multiple techniques of audio Steganography	Ramandeep kaur, ,Jitender Sharma	Icrtedc, vol. 1, spl. Issue 2 (may, 2014)	This paper deals with the Idea that LSB coding is done with xoring method in Which data embedding is done by xoring the LSB's. By Using this method the recovery at receiver end is 100%.	This paper analyses the different techniques of audio Steganography for embedding and security, we conclude That every technique has some advantages and Disadvantages also.
13	A Unique Approach for Data Hiding Using Audio Steganography	Tanmaiy G. Verma1, Zohaib Hasan2, Dr. Girish Verma3	International Journal of Modern Engineering Research (IJMER) Vol. 3, Issue. 4, Jul - Aug. 2013 pp-2098-2101	Steganography and Cryptography are considered as one of the techniques which are used to protect the important information, but both techniques have their pro's and con's	Both the cryptography and steganography have their own respective pros and cons, but the combination of both the model provides better protection of the data from the intruders
14	Audio Wave Steganography	Ajay.B.Gadicha	International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-5, November 2011	As the number of used lsbs during LSB coding increases Or, equivalently, depth of the modified LSB layer becomes Larger, probability of making the embedded message Statistically detectable increases and perceptual transparency Of stego objects is decreased.	If the 4th LSB Layer is used, the absolute error value ranges from 1 to 4 QS,While the standard method in the same conditions cause Constant absolute error of 8 QS. The average power of Introduced noise is therefore 9.31 db smaller if the proposed LSB coding method is used
15	Review of an Improved Audio Steganographic Technique over LSB through Random Based Approach	Bhagyashri A. Patil1, Vrishali A. Chakkarwar	IOSR Journal of Computer Engineering (IOSR-JCE) E-ISSN: 2278-0661, p-ISSN: 2278-8727Volume 9, Issue 1 (Jan. - Feb. 2013), PP 30-34	Input given to the system is secret message which is either a text file or image file or an audio file. After this a cover object i.e. Audio file (.WAV format) is selected to perform encryption as well as to hide the Encrypted data. Secret message file is converted to binary file format	This proposed method is one of the tool Which allows the user to embed text or image or an audio data in cover media which is nothing but an audio Signal under a single platform. There is no need to go for different methods of steganography
16	Hiding text in		International	These methods	Using multiple lsbs were tested

	audio using multiple lsb steganography and provide security using cryptography	S.S. Divya, M. Ram Mohan Reddy	journal of scientific & technology research volume 1, issue 6, july 2012	check the msbs of the samples, and then number of lsbs for data hiding is decided. In this way, multiple and variable lsbs are used for embedding secret data. These proposed methods remarkably increase the capacity for data hiding as compared to standard LSB without causing any noticeable distortion to the data	with audio sequences were with sampling frequency 44100 Hz audio file represented by 16 bits per sample. Duration of the clips ranged from 2 to 8 seconds. This method analyzed in terms of PSNR (peak signal to noise ratio), incr_cap (Increased Capacity) and MSE
17	Secure Audio Steganography for Hiding Secret information	K.Sakthisudhan, P.Prabhu, P.Thangaraj	International Conference on Recent Trends in Computational Methods, Communication and Controls (ICON3C 2012)	In the proposed method the carrier file is taken as audio format and the secret message may be a text or audio format files. Here a key is taken at the transmitter with that a pseudo sequence is generated and this sequence is performed a logical operation with the secret message.	The message signal is transmitted with utmost security and can be retrieved without any loss in transmission in this method. Apart from lossless transmission this method easily blinds the hackers securing from data piracy. The key can be both public and private depending upon the user and serves better in both aspects.
18	Real-time Attacks on Audio Steganography	M. Nutzinger	Journal of Information Hiding and Multimedia Signal Processing, Volume 3, Number 1, January 2012	This algorithm works in the frequency domain. One bit is embedded by.The introduction of a configurable mean phase difference between two adjacent partsof a Configurable frequency interval for each block of the cover audio signal.	A comparison with the stirmark for Audio benchmark further showed that our approaches do have novel elements and while Stir Mark for Audio also has successful attacks, it does not control the audioquality preservation in general, which was one of our main design goals. These results demonstrate the significance of our implementation besides stirmark for Audio

CONCLUSION

It is a robust mehtod of imperceptible audio data hiding.This paper implement real time LSB based steganography .At future work data hiding in audio signal may be extended to other steganographic technique like dct based Steganography

ACKNOWLEDGMENT

i thankful to mr .vinay jain sir for supporting in this project .

REFERENCES

[1] priyanka r. katariya vrushabh r. patil komal k. shashikant m. pingle sanghavi mahesh r.“audio steganography using lsb” ,1st international conference on recent trends in engineering & technology, mar-2012

[2] Dr .Dular Kar ,Dr laungjuang li and Dr.Ajay katangur, “A stegnographic application using audio files”,TEXAS A.M University ,2009 .

[3] Mahalakshmi., Selvarani, Thilagam , and N.Tharminie, “AUDIO STEGNOGRAPHY USING AES”, International Journal of Innovative Research in Science, Engineering and Technology,4SEPT2015.

[4] Deepak, Karthik, AND Manjunath , “ Efficient Method to Increase Robustness in Audio Steganography”, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 1, Issue 6, December 2012

[5] Prof. Samir Kumar, BandyopadhyayBarnali, and Gupta Banik. “LSB Modification and Phase Encoding Technique of Audio Steganography Revisited”, International Journal of Advanced Research in Computer

and Communication Engineering Vol. 1, Issue 4, June 2012.

[6] R.F. Olanrewaju, Othman Khalifa and Husna binti Abdul Rahman Suliman, "Increasing the Hiding Capacity of Low-Bit Encoding Audio Steganography Using a Novel Embedding Technique", World Applied Sciences Journal 21 (Mathematical Applications in Engineering): 79-83, 2013

[7] Jyoti Bahl and Dr. R. Ramakishore"Audio Steganography using Parity Method at higher LSB layer as a variant of LSB Technique",International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 7, July 2015.

[8] Ankit Chadha, Neha Satam, Rakshak Sood and Dattatray Bade," An Efficient Method for Image and Audio Steganography using Least Significant Bit (LSB) Substitution",International Journal of Computer Applications (0975 – 8887) Volume 77– No.13, September 2013.

[9] Jayaram,Ranganatha,and Anupama,"Information hiding using audio Steganography – a survey", The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011

[10] Md. Shafakhatullah Khan , V.Vijaya Bhasker and V. Shiva Nagaraju. "An Optimized Method for Concealing Data using Audio Steganography". International Journal of Computer Applications (0975 – 8887) Volume 33– No.4, November 2011.

[11] Mohammed Salem Atoum, Mamoun Suleiman Al Rababa, Dr. Subariah Ibrahim, and OsamahAbdulgader Ahmed,"A Steganography Method Based on Hiding secrete data in MPEG/Audio Layer III", IJCSNS International Journal of Computer 184 Science and Network Security, VOL.11 No.5, May 2011.

[12] Ramandeep kaur,and Jitender Sharma**, "**Information hiding by using Multiple techniques of audio steganography", ICRTEDC-2014.

[13] Tanmaiy G. Verma,Zohaib Hasan,and Dr. Girish Verma, " A Unique Approach for Data Hiding Using Audio Steganography" International Journal of Modern Engineering Research (IJMER) ,Vol. 3, Issue. 4, Jul - Aug. 2013 pp-2098-2101.

[14] Ajay.B.Gadicha, "Audio Wave Steganography", International Journal of Soft Computing and Engineering (IJSCE), Volume-1, Issue-5, November 2011.

[15] Bhagyashri A. Patil and Vrishali A. Chakkarwar,"Review of an Improved Audio Steganographic Technique over LSB through Random Based Approach", *IOSR Journal of Computer Engineering (IOSR-JCE),Volume 9, Issue 1 (Jan. - Feb. 2013).*

[16] S.S. Divya and M. Ram Mohan Reddy,"Hiding text in audio using multiple lsb steganography and provide security using cryptography",International journal of scientific & technology research volume 1, issue 6, july 2012, IJSTR2012

[17] K.Sakthisudhan ,P.Prabhu and P.Thangaraj " Secure Audio Steganography for Hiding Secret information", International Conference on Recent Trends in Computational Methods, Communication and Controls ,ICON3C 2012.

[18] M. Nutzinger, " Real-time Attacks on Audio Steganography", Journal of Information Hiding and Multimedia Signal Processing ,Volume 3, Number 1, January 2012.