ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 11, May 2015

Audio Steganographic Approaches: A Review

Hiranlal T. H , Neenu Gopal and Sasikumar. V. V
Advanced Communication & Signal Processing Laboratory,
Department of Electronics & Communication Engineering,
Government College of Engineering
Kannur, Kerala , India-670 563

Abstract*— This review paper discusses various audio steganographic methods. The main focus of this paper is to make sure the confidentiality of the secret message. Towards the end of this paper a multi-layered model for audio steganography is discussed. The secret message to be transmitted is passed through two layers before it is embedded within the cover message in the third layer. The stego message is retrieved from the network by the receiver and the secret message is recovered by performing reverse operations in reverse order.

***Index Terms*—Secret transmission, information security, privacy, steganography, audio steganography.**

I. 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 eavesdropper. So the attractive solution for this problem is Steganography, which is the art and science of writing hidden messages in such a way that no one, apart from the sender and intend recipient, suspects the existence of the message, a form of security through obscurity. Audio steganography is the scheme of hiding the existence of secret information by concealing it into another medium such as audio file. The word steganography comes from the Greek Steganos, which means covered or secret and graphy means writing or drawing. Therefore, steganography means, literally, covered writing. Steganography is the art and science of hiding secret information in a cover file such that only sender and receiver can detect the existence of the secret information. A secret information is encoded in a manner such that the very existence of the information is concealed. The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. It is not only prevents others from knowing the hidden information, but it also prevents others from thinking that the information even exists. If a steganography method causes someone to suspect there is a secret information in a carrier medium, then the method has failed. The basic model of Audio steganography consists of Carrier (Audio file), Message and Password. Carrier is also known as a cover-file, which conceals the secret information. Audio steganography can be used to hide any text or audio secret message in an audio signal called as host message or cover message. Once the contents of the cover message are altered to contain a secret message, the resulting message is called a stego message. For any audio steganography technique to be successful there shouldn't be any detectable difference between the cover message and the stego message. Three parameters defining an audio steganography technique are capacity, transparency and robustness. Capacity means how much bits of the secret message can be embedded in the cover message; transparency indicates how securely the secret message is embedded while robustness is the ability of the stego message to withstand steganalysis attacks by intruders.

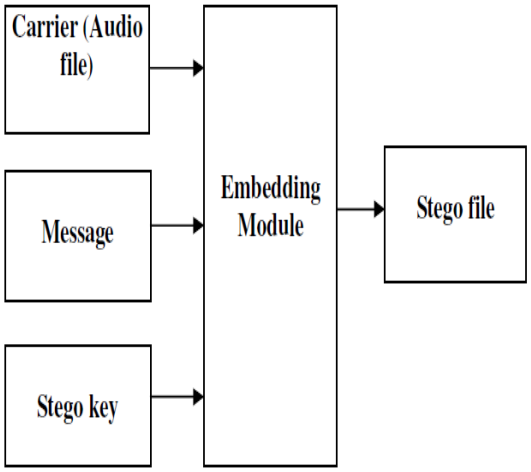

Fig. 1. Basic Audio Steganographic Model

The rest of the paper is organized as follows. In Section II, we present the current state of the art related to Audio steganography. In Section III, we discuss the various methods of Audio steganography. In Section IV we propose an Enhanced Least Significant Bit Modification Technique for Audio Steganography which is bundled in a three layered model and in Section V we discuss its applications. Finally Section V summarizes this paper with some concluding remarks. Basically, the model for steganography is shown in Fig 1. Message is the data that the sender wishes to remain it confidential. Message can be plain text, image, audio or any type of file. Password is known as a stego-key, which ensures that only the recipient who knows the corresponding decoding key will be able to extract the message from a cover-file. The cover-file with the secret information is known as a stego-file.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 11, May 2015

II. CURRENT STATE OF THE ART

Audio Steganography is an application to embed a data file in audio data. In the past few years, several techniques for data hidden in audio sequences have been presented. All developed techniques take benefit of the perceptual properties of the human auditory system (HAS). Muhammad Asad et. al. in 2012 [1] proposes a three layered model for audio steganography based on least significant bit replacement. The secret message to be transmitted is passed through two layers before it is embedded within the cover message in the third layer. The stego message is retrieved from the network by the receiver and the secret message is recovered by performing reverse operations in reverse order. The main focus of the paper is to make sure the confidentiality of the secret message. Implementation issues of the three layered model with respect to different parameters including capacity, transparency and robustness are discussed. Lovey Rana et. al. in 2013 [2] proposed an audio steganographic system that provides improved security. To achieve this, dual layer randomization approach is used. First layer of randomization is achieved by randomly selecting the byte number or samples. An additional layer of security is provided by randomly selecting the bit position at which embedding is done in the selected samples. Using this proposed algorithm the transparency and robustness of the steganographic technique is increased. Kirti Gandhi et. al. proposed a modified LSB audio steganography approach in 2012 [3] in which two bits (2^{nd} and 3rd LSBs) are used for hiding message. This will increase the data hiding capacity also. A custom filter is designed so as to minimize the changes occurred in stego file. The stego file along with the filtered file thus obtained is used to generate a unique key. The filtered file and the generated key will be transmitted to receiver. The key will derive to extract the correct message at receivers end. Bankar Priyanka R. et al. in 2012 [4] presented a novel approach of submission technique of audio Steganography. Using genetic algorithm, message bits are embedded into multiple and higher LSB layer values, resulting in increased robustness. The robustness specially would be increased against those international attacks which try to reveal the hidden message and also some unintentional attacks like noise addition as well. Ashwini Mane et. al. in 2012 [5] presented a Least Significant Bit (LSB) method. In LSB method consecutive LSBs in each sample of cover audio is replaced with secret message bit. LSB method is very easy to implement but have low robustness. They also compare the spectra of original audio signal before embedding and audio signal after embedding. A method of hiding text in audio using multiple LSB steganography and provide security using cryptography is discussed by S.S. Divya and M. Ram Mohan Reddy in 2012 [6]. Steganography is an art and science of writing hidden messages in such a way that no one apart from the intended recipient knows the existence of the message. The maximum number of bits that can be used for LSB audio steganography without causing noticeable perceptual distortion to the host audio signal is 4 LSBs, if 16 bits per sample audio sequences are used. The research has proposed two novel approaches of substitution technique of audio steganography that improves the capacity of cover audio for embedding additional data. Using these methods, message bits are embedded into multiple and variable LSBs. These methods utilize up to 7 LSBs for embedding data. Results showed that both these methods improve capacity of data hiding of cover audio by 35. Gunjan Nehru et. al. in 2012 [7] paper has studied a detailed look of audio steganography techniques using LSB and genetic algorithm approach. Ajay.B.Gadicha in 2011 [8] has explored a new 4th bit rate LSB audio Steganography method that reduces embedding distortion of the host audio. Using the proposed algorithm, message bits are embedded into 4th LSB layers, resulting in increased robustness against noise addition. In addition, listening tests showed that perceptual quality of audio is higher in the case of the proposed method than in the standard LSB method. Mazdak Zamani et.al in 2009 [9] proposed a aecure audio steganography. They described the problems faced by substitution technique and solution to the problems. The main problem is low robustness against attacks. Two types of attacks are there. One type of attack tries to reveal the hidden message and other tries to destroy the hidden message. In conventional LSB method secret message is embedded in the least significant bit. This method is more vulnerable to attack. So by embedding message in bits other than LSB more security can be achieved. More robustness can be achieved if message is embedded into deeper bits. But the problem is that as one move into the MSBs the host audio signal gets altered. This problem can be solved by an intelligent algorithm which embeds the message bits in the MSB and alter other bits to decrease the error. Using this intelligent algorithm message bits can be embedded into multiple MSBs to achieve higher capacity and robustness R Sridevi et al. in 2009 [10] proposed an efficient method of audio steganography by modified LSB algorithm and strong encryption key with enhanced security. In the current internet community, secure data transfer is limited due to its attack made on data communication. So more robust the rescue is the Audio Steganography. But existing audio steganographic systems have poor interface, very low level implementation, difficult to understand and valid only for certain audio formats with restricted message size. Enhanced Audio Steganography (EAS) is a system which is based on audio Steganography and cryptography, ensures secure data transfer between the source and destination. EAS uses most powerful encryption algorithm in the first level of security, which is very complex to break. In the second level it uses a more powerful modified LSB (Least Significant Bit) algorithm to encode the message into audio. It performs bit level manipulation to encode the message. The basic idea behind this research has to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safer manner. Though it is well modulated software it has been limited to certain restrictions. The quality of sound depends on the size of the audio which the user

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 11, May 2015

selects and length of the message. Though it shows bit level deviations in the frequency chart, as a whole the change in the audio cannot be determined. Nedeljko Cvejic et. al. in 2004 [11] presented a novel high bit rate LSB audio watermarking method. The basic idea of the proposed LSB algorithm is watermark embedding that causes minimal embedding distortion of the host audio. Using the proposed two-step algorithm, watermark bits are embedded into higher LSB layers, resulting in increased robustness against noise addition or MPEG compression. Listening tests showed that the perceptual quality of watermarked audio is higher in the case of the proposed method than in the standard LSB method. Hence, up to date the main challenge in digital audio steganography is to obtain robust high capacity steganographic systems. Leaning towards designing a system that ensures high capacity or robustness and security of embedded data has led to great diversity in the existing steganographic techniques

III. METHODS OF AUDIO STEGANOGRAPHY

The various methods for audio steganography are LSB coding, Parity coding, phase coding, spread spectrum (SS) method and echo hiding.

A. LSB coding

A very popular methodology is the LSB (Least Significant Bit) algorithm, which replaces the least significant bit in some bytes of the cover file to hide a sequence of bytes containing the hidden data. That's usually an effective technique in cases where the LSB substitution doesn't cause significant quality degradation. 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 (rightmost) position. The application decoding the cover reads the Least Significant Bits of those bytes to recreate the hidden byte. As you may realize, using this technique let you hide a byte every eight bytes of the cover. Note that there's a fifty percent chance that the bit you're replacing is the same as its replacement, in other words, half the time, the bit doesn't change, which helps to minimize quality degradation.

B. Parity coding

Parity coding is one of the robust audio steganographic techniques. Instead of breaking a signal into individual samples, this method breaks a signal into separate samples and embeds each bit of the secret message from a parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process inverts the LSB of one of the samples in the region. Thus, the sender has more of a choice in encoding the secret bit. Figure 2, shows the parity coding procedure.

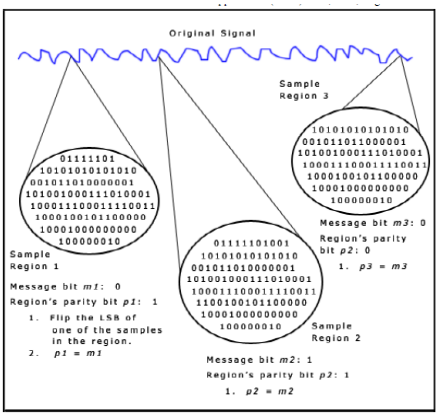

Fig. 2. Parity coding

C. Phase coding

The phase coding technique works by replacing the phase of an initial audio segment with a reference phase that represents the secret information. The remaining segments phase is adjusted in order to preserve the relative phase between segments. In terms of signal to noise ratio, Phase coding is one of the most effective coding methods. When there is a drastic change in the phase relation between each frequency component, noticeable phase dispersion will occur. However, as long as the modification of the phase is sufficiently small, an inaudible coding can be achieved. This method relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is.

D. Spread spectrum method

In audio steganography, the basic spread spectrum (SS) method attempts to spread secret information across the frequency spectrum of the audio signal. This is similar to a system which uses an implementation of the LSB that spreads the message bits randomly over the entire sound file. However, unlike LSB coding, the Spread Spectrum method spreads the secret information over the frequency spectrum of the sound file using a code which is independent of the actual signal. As a result, the final signal occupies a bandwidth which is more than what is actually required for transmission. The Spread Spectrum method is capable of contributing a better performance in some areas compared to LSB coding; phase coding, and parity coding techniques in that it offers a moderate data transmission rate and high level of robustness against removal techniques. However, the Spread Spectrum method has one main disadvantage that it can introduce noise into a sound file.

E. Echo hiding

Echo hiding technique embeds secret information in a sound file by introducing an echo into the discrete signal. Echo hiding has advantages of providing a high data transmission rate and superior robustness when compared to other methods. Only one bit of secret information could be encoded if only one echo was produced from the original signal. Hence, before the encoding process begins the original signal is broken down into blocks. Once the encoding process

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 11, May 2015

is done, the blocks are concatenated back together to create the final signal. Echo Hiding is shown in Figure 3.

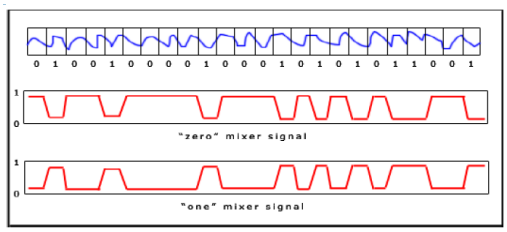

Fig. 3. Echo Hiding

IV. PROPOSED SYSTEM

The proposed methodology is comprised of three different layers to fight against steganalysis; character encoding, encryption and enhanced steganography. As shown in Figure 4, the message transmitted by sender will pass through character encoding, encryption and enhanced steganography layers before it is transmitted over the network. On the receiver side, the same operations are performed but in reverse order. The three layered model focuses more on security of secret messages which are related to transparency and robustness parameters of the steganographic technique.

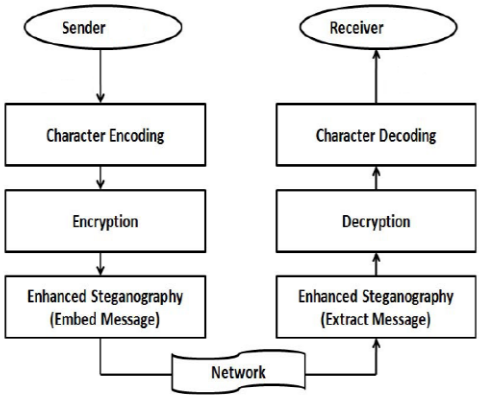

Fig. 4. Multi Layered Model.

V. CONCLUSION

The conventional LSB modification techniques used are prone to steganalysis. A new three layered model for audio steganography is presented in this paper. On the sender side, the first layer maps characters of the secret message to bits. The compression provided by this layer increases capacity. The second layer applies encryption to secret message bits, thus changing representation of the secret message. The change in representation increases robustness, but the transmission of key decreases capacity. However, the decrease in capacity becomes negligible for longer secret messages. The third layer samples the cover message, embeds the secret message in it and transmits the resultant stego message over the network to the receiver. The third layer increases transparency and robustness, but decreases capacity which can be easily overcome by advance broadband networks. The receiver retrieves the stego message from the network and passes it through all three layers but in reverse order with each layer performing reverse operations. At the end, the same secret message is available to the receiver.

REFERENCES

[1] Muhammad Asad, Junaid Gilani, Adnan Khalid,, "Three Layered Model for Audio Steganography," International Conference on Emerging Technologies (ICET), 2012.

[2] Lovey Rana, Saikat Banerjee,, 'Dual Layer Randomization in Audio Steganography Using Random Byte Position Encoding," International Journal of Engineering and Innovative Technology, Volume 2, Issue 8, 2013.

[3] Kirti Gandhi, Gaurav Garg, "Modified LSB Audio Steganography Approach" International Journal of Emerging Technology and Advanced Engineering, Volume 3,Issue 6,2012

[4] Bankar Priyanka R., Katariya Vrushabh R, Patil Komal K, "Audio Steganography using LSB," International Journal of Electronics, Communication and Soft Computing Science and Engineering, , 2012.

[5] Ashwini Mane, Gajanan Galshetwar, Amutha Jeyakumar, "Data Hiding Technique: Audio Steganography using LSB Technique," International Journal of Engineering Research and Applications, Vol.2, No.4, pp. 1123–1125, 2012.

[6] S.S. Divya, M. Ram Mohan Reddy, "Hiding Text In Audio Using Multiple LSB Steganography And Provide Security Using Cryptography," International Journal of Scientific Technology Research, Vol. 1, pp. 68–70, 2012.

[7] Gunjan Nehru and Puja Dhar, "A Detailed Look Of Audio Steganography Techniques Using LSB And Genetic Algorithm Approach," International Journal of Computer Science (IJCSI), Vol. 9, pp. 402–407, 2012.

[8] Ajay.B.Gadicha, "Audio wave Steganography,," International Journal of Soft Computing and Engineering (IJSCE), Vol. 1, pp. 174–177, 2011.

[9] Mazdak Zamani et.al, "A Secure Audio Steganography Approach," International Conference for Internet Technology and Secured Transactions, 2009.

[10] R Sridevi, Dr. A Damodaram and Dr.Svl. Narasimham, "Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key With Enhanced Security,,," Journal of Theoretical and Applied Information Technology , 2009.

[11] Nedeljko Cvejic, Tapio Seppanen,, "Increasing Robustness Of LSB Audio Steganography Using A Novel Embedding Method," The International Conference on Information Technology , 2004.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 11, May 2015

AUTHOR BIOGRAPHY

Hiranlal T. H. received the B-Tech degree in electronics and communication engineering in 2012 from Kannur University, Currently doing Mtech degree in signal processing and embedded system at kannur university kerala

Neenu Gopal received the B-Tech degree in electronics and communication engineering in 2012 from M G university. Currently doing Mtech degree in signal processing and embedded system at kannur university kerala

Sasi kumar V. V. received the B- tech degree in electronics and communication at kerala university**,** and master's degree at college of engineering Trivandrum. Currently working as an associate professor in government college of engineering Kannur.