ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A REVIEW ON VARIOUS AUDIO STEGANOGRAPHY TECHNIQUES FOR AUDIO SIGNALS

Rubby Garg*, Dr.Vijay Laxmi
* A research scholar M-Tech, Computer Science and Engineering,Guru Kashi University,India
Dean, UCCA, Guru Kashi University, India

DOI: 10.5281/zenodo.160886

ABSTRACT

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 works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, HTML, or even floppy disks) 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.

KEYWORDS: Stegnography, Audio Stegnography, Improved LSB, Text Hiding, Text Compression.

INTRODUCTION

People use cryptography to send secret messages to one another without a third party overseeing the message. Steganography is a type of cryptography in which the secret message is hidden in a digital picture. While cryptography is preoccupied with the protection of the contents of a message or information, Steganography concentrates on concealing the very existence of such messages from detection.

The term Steganography is adapted from the Greek word *steganographia*, meaning “covered writing” and is taken in its modern form to mean the hiding of information inside other information. Naturally these techniques date back throughout history, the main applications being in couriering information during times of war.
With the invention of digital audio and images files this has taken on a whole new meaning; creating new methods for performing “reversible data hiding” as it is often dubbed. This has many possible applications including the copyright watermarking of audio, video and still image data. In digital media, Steganography is mainly oriented around the undetectable transmission of one form of information within another. In order for a data hiding technique to be successful it must adhere to two rules:

[1] The embedded data must be undetectable within its carrier medium (the audio or image file used). The carrier should display no properties that flag it as suspicious, whether it is to the human visual/auditory system or in increased file size for the carrier file.

[2] The embedded data must maintain its integrity within the carrier and should be easily removable, under the right circumstances, by the receiving party.

The existing system of Audio Steganography poses more restrictions on the choosing of audio files. User can select only wav files to encode. Further embedding information into sound files is
generally considered more difficult than images; according to the human ear is extremely sensitive to perturbations in sound and can in fact detect such turbulence as low as one part in 10 million. The four methods discussed further provide users with a large amount of choice and makes the technology more accessible to everyone.

LITERATURE SURVEY

M.Baritha Begum [1],Compression algorithm is what reduces the redundancy of data representation and decreases the data storage capacity. Data compression plays a vital role in reducing the communication cost making use of available bandwidth. The compressed data from the security aspect is transmitted through internet. It is, however very much vulnerable to a multitude of attacks. To propose a new dictionary based text compression technique for ASCII texts for the purpose of obtaining good performance on various document sizes. Dictionary based compression bits are hidden into the Lsb bit of audio signals and to calculate the signal to noise ratio (SNR). This audio Steganography is conducted for various compression algorithms with dictionary based compression. Audio Steganography based dictionary compression achieves better value of signal to noise ratio (SNR).

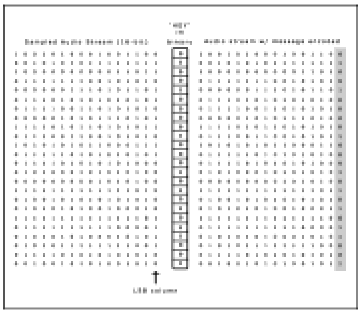
Kamal Pradhan [2], Data transmission in public communication system is prone to the interception and improper manipulation by eavesdropper. Audio Steganography is the procedure of hiding the existence of secret information by zipping it into another medium such as audio file. This paper explores the innovative audio Steganography technique in a practical way in order to conceal the preferred information. The proposed system uses LSB (least significant bit) technique for embedding text into an audio file. The text is encrypted using AES (Advanced encryption standard) encryption function and md5 hash function which is used for verifying data integrity of the audio file. The performance of this system is evaluated through a more secure process based on robustness, security and data hiding capacity.

Fatiha Djebbar[3],The rapid spread in digital data usage in many real life applications have urged new and effective ways to ensure their security. Efficient secrecy can be achieved, at least in part, by implementing steganograhy techniques. Novel and versatile audio steganographic methods have been proposed. The goal of steganographic systems is to obtain secure and robust way to conceal high rate of secret data. We focus in this paper on digital audio steganography, which has emerged as a prominent source of data hiding across novel telecommunication technologies such as covered voice-over-IP, audio conferencing, etc. The multitude of steganographic criteria has led to a great diversity in these system design techniques. In this paper, we review current digital audio steganographic techniques and we evaluate their performance based on robustness, security and hiding capacity indicators. Another contribution of this paper is the provision of a robustness-based classification of steganographic models depending on their occurrence in the embedding process. A survey of major trends of audio steganography applications is also discussed in this paper.

EXISTING TECHNIQUES FOR IMAGE WATERMARKING

LSB CODING

Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded. The following diagram illustrates how the message 'HEY' is encoded in a 16-bit CD quality sample using the LSB method:


Sampled Audio Stream (16-bit)
"HEY" in binary
Audio stream w/ message encoded
LSB column

Standard LSB ALGORITHM:

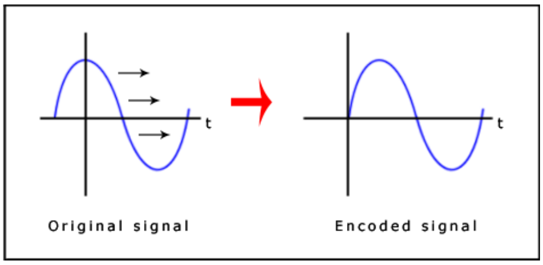
It performs bit level manipulation to encode the message. The following steps are
a. Receives the audio file in the form of bytes and converted in to bit pattern.
b. Each character in the message is converted in bit pattern.
c. Replaces the LSB bit from audio with LSB bit from character in the message.

In LSB coding, the ideal data transmission rate is 1 kbps per 1 kHz. In some implementations of LSB coding, however, the two least significant bits of a sample are replaced with two message bits. This increases the amount of data that can be encoded but also increases the amount of resulting noise in the audio file as well. Thus, one should consider the signal content before deciding on the LSB operation to use. For example, a sound file that was recorded in a bustling subway station would mask low-bit encoding noise. On the other hand, the same noise would be audible in a sound file containing a piano solo.

The main advantage of the LSB coding method is low computational complexity of the algorithm while its major disadvantage : 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. Low Bit Encoding is therefore an undesirable method, mainly due to its failure to meet the Steganography requirement of being undetectable.

PHASE CODING

Phase coding addresses the disadvantages of the noise-inducing methods of audio Steganography. Phase coding relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is. Rather than introducing perturbations, the technique encodes the message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to-perceived noise ratio.



The phase coding method breaks down the sound file into a series of N segments. A Discrete Fourier Transform (DFT) is applied to each segment to create a matrix of the phase and magnitude. The phase difference between each segment is calculated, the first segment (s0) has an artificial absolute phase of p0 created, and all other segments have newly created phase frames. The new phase and original magnitude are combined to get the new segment, Sn. These new segments are then concatenated to create the encoded output and the frequency remains preserved. In order to decode the hidden information the receiver must know the length of the segments and the data interval used. The first segment is detected as a 0 or a 1 and this indicates where the message starts. This method has many advantages over Low Bit Encoding, the most important being that it is undetectable to the human ear. Like all of the techniques described so far though, its weakness is still in its lack of robustness to changes in the audio data. Any single sound operation or change to the data would distort the information and prevent its retrieval.

ECHO HIDING

Echo hiding embeds its data by creating an echo to the source audio. Three parameters of this Artificial echo are used to hide the embedded data, the delay, the decay rate and the initial amplitude. As the delay between the original source audio and the echo decrease it becomes harder for the human ear to distinguish between the two signals until eventually a created carrier sound’s echo is just heard as extra resonance.

In addition, offset is varied to represent the binary message to be encoded. One offset value represents a binary one, and a second offset value represents a binary zero. If only one echo was produced from the original signal, only one bit of information could be encoded. Therefore, the original signal is broken down into blocks before the encoding process begins. Once the encoding process is completed, the blocks are concatenated back together to create the final signal. The blocks are recombined to produce the final signal.

To extract the secret message from the stego-signal, the receiver must be able to break up the signal into the same block sequence used during the encoding process. Then the autocorrelation function of the signal's spectrum (the spectrum is the Forward Fourier Transform of the signal's frequency spectrum) can be used to decode the message because it reveals a spike at each echo time offset, allowing the message to be reconstructed.

Much like phase encoding this has considerably better results than Low Bit Encoding and makes good use of research done so far in psychoacoustics. As with all sound file encoding, we find that working in audio formats such as WAV is very costly, more so than with bitmap images in terms of the “file size to storage capacity” ratio.

The transmission of audio files via e-mail or over the web is much less prolific than image files and so is much more suspicious in comparison. It allows for a high data transmission rate and provides superior robustness when compared to the noise inducing methods.

SPREAD SPECTRUM

Spread spectrum systems encode data as a binary sequence which sounds like noise but which can be recognised by a receiver with the correct key. The technique has been used by the military since the 1940s because the signals are hard to jam or intercept as they are lost in the background noise. Spread spectrum techniques can be used for watermarking by matching the narrow bandwidth of the embedded data to the large bandwidth of the medium.

Two versions of SS can be used in audio Steganography: the direct-sequence and frequency-hopping schemes. In direct-sequence SS, the secret message is spread out by a constant called the chip rate and then modulated with a pseudorandom signal. It is then interleaved with the cover-signal. In frequency-hopping SS, the audio file's frequency spectrum is altered so that it hops rapidly between frequencies. Spread Spectrum Steganography has significant potential in secure communications – commercial and military. Audio Steganography in conjunction with Spread Spectrum may provide added layers of security.

Spread spectrum encoding techniques are the most secure means by which to send hidden messages in audio, but it can introduce random noise to the audio thus creating the chance of data loss. They have the potential to perform better in some areas than LSB coding, parity coding, and phase coding techniques in that it offers a moderate data transmission rate while also maintaining a high level of robustness against removal techniques

CONCLUSION

In this paper we have presented various techniques for audio stegnography. Various techniques for audio stegnography has been discussed in this paper along with there advantages and disadvantages. It is concluded that a more robust audio stegnography technique is required so embed the secret message into the audio signals.

REFERENCES

[1] M.Baritha Beguma ,Y.Venkataramanib ,LSB Based Audio Steganography Based On Text Compression,Procedia Engineering 30 (2012) 703 – 710

[2] Kamal Pradhan,Chinmaya Bhoi, Robust Audio Steganography Technique using AES algorithm and MD5 hash,International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163, Volume 1 Issue 10 (November 2014)

[3] Fatiha Djebbar, Beghdad Ayad, Karim Abed Meraim and Habib Hamam, Comparative study of digital audio steganography techniques

[4] Swati Malviya1, Manish Saxena2, Dr. Anubhuti Khare3,Audio Steganography by Different Methods, International Journal of Emerging Technology and Advanced Engineering, Volume 5, Issue 4, 2015

[5] 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, August 2011

[6] 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

[7] Walter Bender, Daniel Gruhl, Norishige Morimoto, Anthony Lu, ”Techniques for Data Hiding”, IBM Systems Journal, vol. 35, no. 3 and 4 pp. 313-336, 1996.

[8] E. Zwicker and H. Fastl, Psychoacoustics, Springer Verlag, Berlin, 1990.

[9] K. Gopalan, ”Audio steganography using bit modification”, Proceedings of International Conference on Multimedia and Expo, Vol. 1, pp.629-632, 6-9 July 2003.