AUDIO STEGANOGRAPHY IMPLEMENTATION VIA LSB ENCODING FOR SECURE COMMUNICATION

Charlotte Anderson[1], Liam Rodriguez[2], Zoe Taylor[3]
[1] Institute of Sociology, University of Southern California, USA
[2] Department of Engineering, University of Cambridge, UK
[3] Faculty of Arts, University of Melbourne, Australia

Steganographyis a technique of sending hidden data or secret messages over a public channel so that nobody can detect the presence of the secret messages.Speech signal can be used as a cover signal to hide very sensitive data in it. The proposed approach is criticalin military-warfare conditions, and in the defense related Information Communication. The covert nature is the desirable feature which declines any unauthorized user from getting sensitive information[1]. Steganography is a way of concealing data where secret messages are hidden inside computer files such as images, sound files, video files so that, no one except the sender and the receiver will guess the existence of information in it. Cryptography may also use in steganographywhere the message is first encrypted before it is hidden in another file. Generally, the messages appear like an image, sound or video so that the secret data transfer remains unsuspected. Steganography hides all evidence regarding the existence of communication. A simple technique which involves the embedding of information in the least significant bits of the cover-audio file is known as LSB Encoding Technique. Distortion will be minimum in this technique. The strength of steganography is in hiding the secret message by obscurity, hiding its existence in a non-secret file. The success of this technique depends on the ability to hide the message such that nobody would suspect it, the greatest effort must be to ensure that the message is not visible unless one knows what to look for.

KEYWORDS: LSB Encoding, Steganography, Cryptography.

1. INTRODUCTION

In the new era, organisations are becoming more and more dependent on their information systems. The people are very concerned about the proper use of information, especially personal data. There is an increase in threats to information systems from criminals and terrorists. Millions of people capture, store, transmit, and manipulate digital data every day. Steganography is the practice of hiding information “in plain sight”[2]. This technique depends on a message being encoded and hidden in a transport layer in such a way that the existence of the message is unknown to an observer. It is different from cryptography, which makes the content of the secret message unreadable while not preventing unintended observers from learning about its existence. The success of audio steganography depends on the capacity to hide the message such that an observer would not suspect it is there at all, the greatest effort must ensure that the message is invisible unless one knows what to look for. The way in which this is done will be different for the specific media that are used to hide the information. The power of a steganographic approach can be calculated by how much information can be concealed in a carrier before it becomes detectable.Both steganography and watermarking can hide information discretely but for different purposes. Steganography is for hiding data secretly for communication with another person. Data ranging from small to large. The most important criteria isnon-detection. Watermarking is to hide a trademark or identification for the use of determining ownership [7].The main difference between these two techniques is that watermarks are public and everybody knows their usage. Steganography deals with the ability of hiding digital information in multi-media. So the very existence of information exchange taking place between a sender and a receiver is disguised. Steganography hides all evidence regarding the existence of communication. A simple technique which requires the embedding of information in the least significant bits of the cover-audio file is known as LSB Encoding Technique. The most important advantage prevailing of this technique is the minimization of the distortion. When normal data is substituted with the secret data, it will be in very little size change for the host file. The message is hidden in the cover and the multimedia file so generated is called the Stego file.The success of this technique depends on the ability to hide the message. By hiding the information using a cover or host audio as a wrapper, the existence of the information is disguised during transmission. This is very critical in applications such as battlefield communications and bank transactions.

2. MATERIALS AND METHODS

ALGORITHM INVOLVED

A. Steganography

Steganography literally means, "Covered writing" which is derived from the Greek language. The word *steganography* combines the Ancient Greek words *steganos*, means "covered or protected", and *graphy* means "writing"[3]. It is away of communicating which hides the existence of the communication. In contrast to Cryptography, steganography 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". Both Steganography and Cryptography are used to protect information from unwanted people. Both are excellent means to accomplish this but neither technology alone is perfect and both can be broken. The most popular data formats used for steganography are .bmp, .doc, .gif, .jpeg, .mp3, .txt and .wav. These formats are very popular because of the relative ease by which redundant or noisy data can be removed from them and can be replaced with a hidden message. Steganographic technologies are a very important for the future of Internet security and privacy on open systems like the Internet [10]

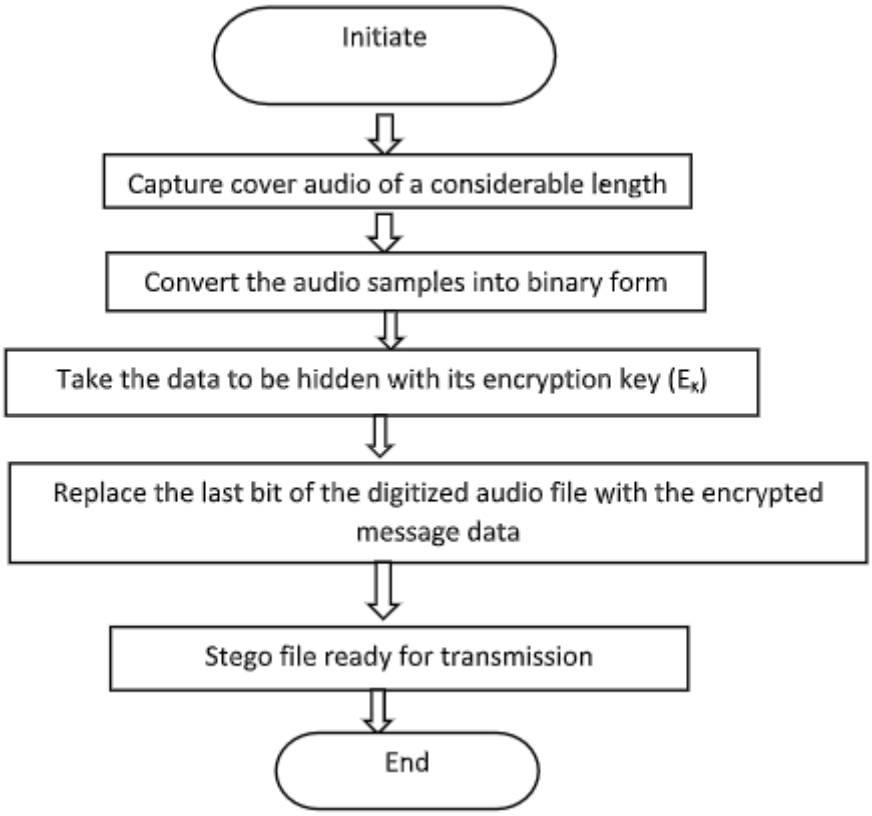


Fig I .Flow chart representing the sequential steps involved in the LSB Hiding Technique

B. STEGANOGRAPHIC REQUIREMENTS

By employing steganography in digital communication, we can guarantee two main directions in information hiding - protection against the detection of the existence of information and hiding the data.

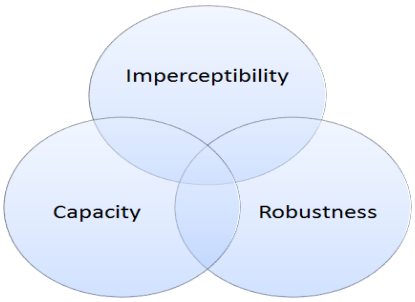


Figure II Steganographic Requirements

The integrity of the hidden information after it has been embedded inside the stego object must be correct [6]. To the naked eye the stego object must remain unchanged or almost unchanged. Imperceptibility refers to security of the hidden communication. Another crucial requirement is robustness against malicious and unintentional attacks.

C. WHY HIDE IN AUDIO

The importance of hiding data in audio files results from the common use of audio signals as information medium in our day today life. It is assumed that the cover utilized to hide messages should not raise any suspicion to enemies. Audio files are used to carry hidden information because of their availability and the popularity. In addition to this most of the steg analysis efforts are mostly directed towards digital images leaving audio

steganalysis relatively unexplored. Data hiding in audio files is challenging because of the sensitivity of the HAS. However, HAS permits common alterations in small differential ranges. For example, piercing sounds tend to mask out quiet sounds. In addition to this there are some common environmental distortions. These properties have led people to explore the utilization of audio signals as carriers for data hiding.

D. Audio Steganography

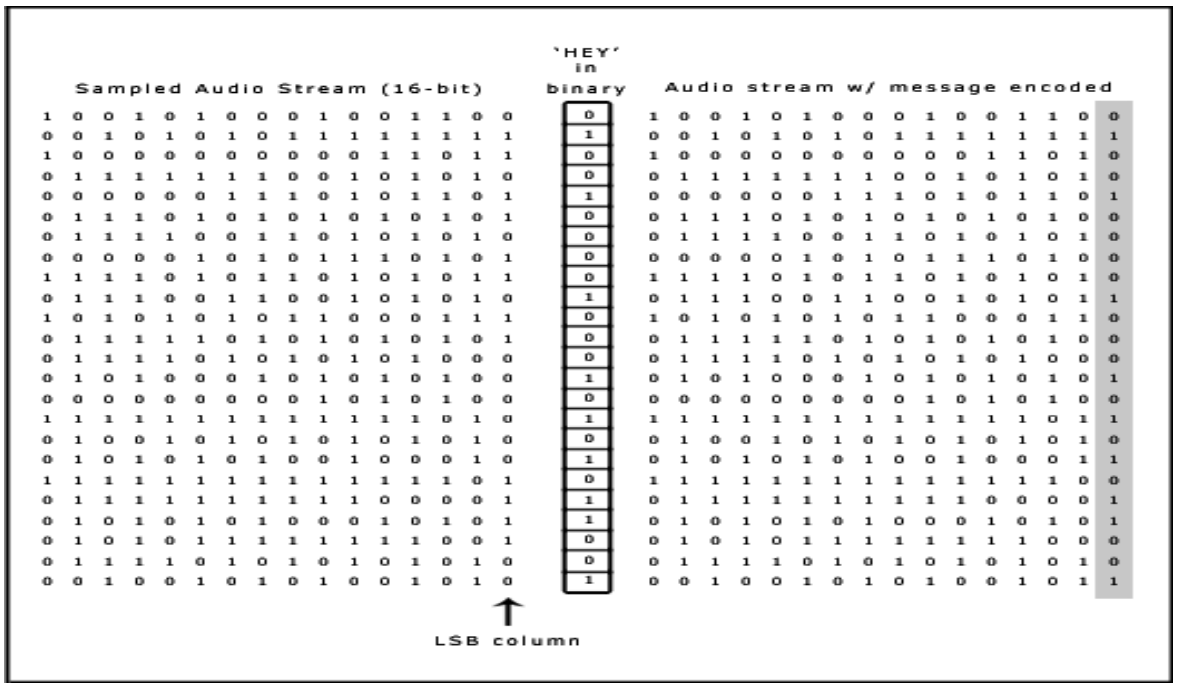
Audio steganography is anxious about hiding information in a cover (host) audio signal in an imperceptible way. Hidden information from the stego, or data-embedded audio signal, is retrieved using a key similar to the one that was employed during the hiding phase. Least Significant Bit (LSB) modification technique is the a simple and efficient method used for audio steganography

E. Audio Steganographic Methods

There are many techniques for hiding information or messages in audio signal. Common approaches are,

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 audio file to hide a sequence of bytes containing the hidden data. Fig (IV) illustrates how the message 'HEY' is encoded in a 16-bit CD quality sample using the LSB method [7]. The secret information is ‘HEY’ and audio file is the cover file. We have to embed HEY is inside the audio file. Initially the secret information ‘HEY’ and the cover audio file are converted into bit stream. The least significant column of the audio file is replaced by the bit stream of secret information ‘HEY’. After embedding secret information ‘HEY’, the resulting file is called the Stego-file.



Fig(III). LSB coding example

B. Parity Coding

Parity coding is one of the robust audio steganographic techniques. This technique breaks a signal into separate samples and embeds each bit of the secret message from a parity bit. If the parity bit of a particular region does not match the secret bit to be encoded, the process inverts the LSB of one of the samples in that region. Thus, the sender gets more choices in encoding the secret bit.

C. ***Phase Coding***

In this technique 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. One of the drawback of the phase coding method is a low payload because only the first block is used for secret message (M) to be embedded. In addition, the M is not distributed over C – that means it is localized data and thus can be removed easily by the cropping attack[2].

D. ***Spread Spectrum***

In audio steganography, the basic spread spectrum (SS) method tries to spread secret information across the audio signal's frequency spectrum. This is similar to a system which uses an implementation of the LSB that spreads the message bits randomly over the entire sound file [9]. The Spread Spectrum method expands the secret information over the frequency spectrum of the entire sound file using a code which is independent of the actual signal. As a result of this the final signal occupies a bandwidth which is more than the required bandwidth for transmission. The SS method has a better performance in some areas compared to other techniques in that it offers a moderate data transmission rate and high degree of robustness against removal techniques. One of the main disadvantage of this system is that it can introduce noise into a sound file[5].

E. Echo Hiding

Echo hiding technique embeds secret information in a sound file by introducing an echo into the discrete signal.Only one bit of secret information could be encoded if there is only one echo was produced from the original signal. Before the encoding process the original signal is broken down into small blocks. After the encoding process, the blocks are concatenated back together to create the final signal.

G. Audio Steganographic Applications

Audio data hiding can be used anytime to hide data,. There are many reasons to hide data but most important is to prevent unauthorized persons from becoming aware of the existence of a message. Audio data hiding can be used to hide a secret chemical formula or plans for a new invention in the business field. Audio data hiding can also be used in the non-commercial sector to hide information that someone wants to keep private. Terrorists can also use Audio data hiding to keep their communications secret and to coordinate attacks. Data hiding in video and audio, is of interest for the protection of copyrighted digital media. It can also be used in forensic applications for inserting hidden data into audio files for the authentication of spoken words and other sounds [10].

3. RESULTS AND DISCUSSION

Proposed Audio Steganography system is a method of data hiding in the least significant bits of each byte of the audio carrier file. Before embedding in the carrier, the message is first encrypted. The system has following four steps: Encryption, Encoding, Decoding, and Decryption. Powerful Encryption Algorithm is used to enhance the security further.

The basic idea behind this is to provide a good, efficient method for hiding the data from hackers and sent to the destination in safe manner. However it is a well-modulated system it has been limited to certain restrictions .The size of the audio which the user selects, determines the quality of sound and length of the message. The key is generated randomly every time , so even if a hacker gets to know the encryption key for one encryption it may not be able to decode the other messages being encrypted by this algorithm. The key which is used for encoding is also used for decoding .This is a secret key where the both user have to agree up on a single common key. This proposed system provides a good, efficient method for the data hiding from hackers and sent to the destination in a safe manner. This proposed system will not change the size of the file even after encoding and also the quality of the audio file is preserved. Both Encryption and Decryption techniques makes the security system robust. For the decryption of the audio signal to retrieve the message, the encrypted audio from SD card must be selected and the decryption key (which is same in this case due to symmetric key cryptography) should be entered. Then the decrypted message will be obtained. Here DES encryption is used to give security which is a symmetric key cryptography. The same key is used for encryption and decryption.

Advantages of the proposed system

- Provision for encryption of message before encoding it into the audio file to enhance the security.
- Provision of encryption key and complex encryption algorithm.
- The encryption key is modified by the algorithm to get a new key which is used for encrypting the message. An intruder cannot break the code even if the key is known to him.

4. CONCLUSION

This method of Steganography plays a vital role in providing covert communication by hiding digital information in the multimedia. The defense and military related information can be secured using this technique of Steganography. This proposed system provides a good, systematicway for hiding the data from hackers and sent to the destination in a safe manner. This proposed system will not change the file size even after encoding. Also the quality of the audio file is conserved. Encryption and Decryption techniques have been used to make the security system robust.Covert communication by embedding a message or data file in a cover medium has

been increasingly gaining importance in the all-encompassing field of information technology. Audio steganography is concerned with embedding information in a safe cover speech in a secure and robust manner. Communication, transmission security and robustness are essential for transmitting essential information to intended sources while opposing access to unauthorized persons.

By hiding the information using a cover or host audio as a wrapper, the existence of the information is disguised during transmission which is critical in applications such as communications in battlefield and bank transactions. The escalation of digital data in their various formats has attracted a special interest from researchers to ensure their security. Encryption and watermarking techniquesare already used in this regard. However, the need for new techniques and new algorithms to counter constantly-changing malicious attempts to the integrity of digital data has become a necessity in today's digital world. Steganography has drawn more attention in the last few years. Its primary goal is to hide the fact that a communication is taking place between two people. Steganography has its place in security. Steganography, is now gaining popularity among the people.

REFERENCES

[1] Vintesh Patel, Sarosh K. Dastoor, A novel android based mobile application as a virtue of covert communication for concealing information in the speech signal, 2012 1st International Conference on Emerging Technology Trends in Electronics, Communication and Networking.

[2] Ashwini Mane, Gajanan Galshetwar, Amutha Jeyakumar, Data hiding technique: Audio steganography using lsb technique, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp.1123-1125

[3] Zameer Fatima1 and Tarun Khanna, Audio Steganography Using DES Algorithm, Proceedings of the 5th National Conference; INDIACom-2011

[4] Jayaram P, Ranganatha H R, Anupama H S, Information hiding using audio steganography – a survey, The International Journal of Multimedia & Its Application (IJMA) Vol.3, No.3, August 2011

[5] C. Parthasarathy, Dr. S.K.Srivatsa, Increased robustness of lsb audio steganography by reduced distortion lsb coding, Journal of Theoretical and Applied Information Technology © 2005 - 2009 JATIT, Vol 7. No 1.

[6] Prof. Sonal K. Jagtap, Pooja P. Balgurgi, Intelligent Processing : An Approach of Audio Steganography, 2012 International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 19-20, Mumbai

[7] Kaliappan Gopalan,Audio steganography using bit modification Proceedings of the 2003 IEEE international Conference on Acoustics, Speech, &Signal Processing, Apnl 6-10.2003

[8] Vittapu Sravan Kumar, Dr.A.Narendra Babu,Embedding Cypher Text In Audio Signal Using Steganography Technique,International Journal of Engineering Trends and Technology (IJETT) - Volume4 Issue7- July 2013

[9] Fatiha Djebbar, Beghdad Ayady, Habib Hamamz and Karim Abed-Meraimx ,A view on latest audio steganography techniques, ,International Conference on Innovations in Information Technology

[10] Harish Kumar, Anuradha, Enhanced LSB technique for Audio Steganography, ICCCNT'12, July 2012, Coimbatore, India.