International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X;pISSN:2321-2241 Volume: 4; Issue: 1; January -2015

Steganography of Audio data into Audio using Matlab & transmission over zigbee

Sandeep Singh R
M.Tech,SJCIT
sandeepec035@gmail.com

Naresh S
M.Tech,SJCIT
mail4naresh07@gmail.com

Veena S
ECE Dept., SJCIT
veenasdl@gmail.com

Abstract-Steganography is a data hiding process in which information is secured, while transferring data from sender to receiver. In audio steganography, encoding process is carried out through an application developed to embed an Audio data in to another audio signal. It is concerned with embedding information in an innocuous cover Speech in a secure and robust manner. This system makes the Files more secure by using the concepts Steganography. 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. Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images. In order to conceal secret messages successfully, a variety of methods for embedding information in digital audio have been introduced. 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. The next section discusses these methods in greater detail.

In this paper, we present a novel high bit rate LSB audio data hiding method that reduces embedding distortion of the host audio. Using the proposed two-step algorithm, hidden bits are embedded into the higher LSB layers, resulting in increased robustness against noise addition.

Keywords: Audio Steganography, Matlab, Techniques for Data Hiding.

1. Introduction

As the need of security increases only encryption is not sufficient. So steganography is the supplementary to encryption. It is not the replacement of encryption. But Steganography along with encryption gives more security to data. The word steganography is of Greek origin and means "concealed writing" from the Greek words stegnos meaning "covered or protected", and graphics meaning "writing". Steganography is the technique to hide the information in some media so that third party can't recognize that information is hidden into the cover media. That media may be text, image, audio or video. The information that to be hidden is called stego and the media in which the information is hidden is called host. The stego object can be text, image, audio or video. When the information is hidden into the audio then it is called Audio steganography. Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The difference between the two is that Steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information.

2. Audio Steganography

Steganography process does not modify the content of data rather it hides only the data. The aim of steganography is to hide the information in an undetectable manner such that information hidden cannot be predicated other than the receiver

[1]. Audio steganography is the practice of hiding the message into another medium such as hiding the information into the audio file. The confidential information is hidden in an audio. Though information is hidden, the perception of an audio does not change; hence the intruders can never find that data is hidden as shown in the Fig.l.

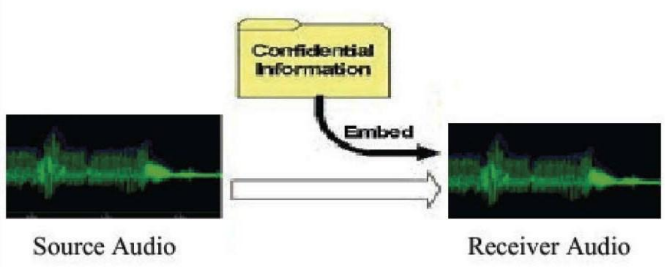

Fig.1. Steganography scenario

The basic model of audio steganography consists of cover file, data which we need to hide, stego key. Parameter, of the basic model is shown in the Fig.2. The term cover file refers to the medium that require iding the data into audio. Message that has to be hidden are in various forms like video, audio, images. Secret information is embedded into the cover message by the secret key called stego key. Stego file is a collective term for cover file with secret information [2].

.

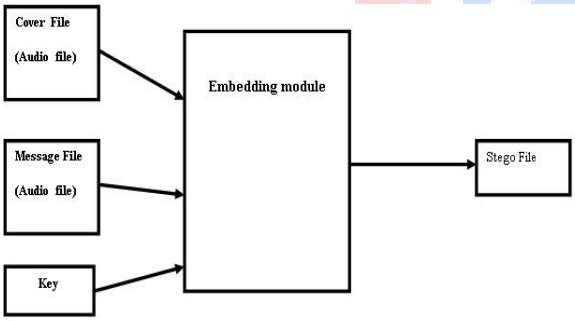

Fig.2. Basic Audio Steganography

The sound files may be modified in such a way that they contain hidden information, like copyright information; those modifications must be done in such a way that it should be impossible for a pirate to remove it, at least not without destroying the original signal. The methods that embeds data in sound files use the properties of the Human Auditory System (HAS). The HAS perceives the additive random noise and also the perturbations in a sound file can also be detected. But there are some "holes" we can exploit. While the HAS have a large dynamic range, it has a fairly small differential range.

a. Technique for Data Hiding in Audio

There are four techniques for hiding data in Audio as following:

(i) Least Significant Bit (LSB) Encoding:

When files are created there are usually some bytes in the file that aren't really needed, or at least aren't that important. These areas of the file can be replaced with the information that is to be hidden, without significantly altering the file or damaging it. This allows a person to hide information in the file and make sure that no human could detect the change in the file. The LSB method works best in Picture files that have a high resolution and use many different colors, and with Audio files that have many different sounds and that are of a high bit rate. The LSB method usually does not increase the file size, but depending on the size of the information that is to be hidden inside the file, the file can become noticeably distorted. The main advantage of the LSB coding method is a very high watermark channel bit rate; use of only one LSB of the host audio sample gives capacity of 44.1 kbps (sampling rate 44 kHz, all samples used for data hiding) and a low computational complexity. The obvious disadvantage is considerably low robustness, due to fact that simple random changes of the LSBs destroy the coded watermark. 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, such as in 24-bit bitmaps. 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 rightmost 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.

1	0	0	1	0	1	1	0

Figure (2) Binary Representation of Decimal 125

The binary representation of decimal 149, with the LSB highlighted. The MSB in an 8-bit binary number represents a value of 128 decimal. The
LSB represents a value of 1. For example, to hide the letter "a" (ASCII code 97, which is 01100001) inside eight bytes of a cover, you can set the LSB of each byte like this:

10010010
01010011
10011011
11010010
10001010
00000010
01110010
00101011

The application decoding the cover reads the eight Least Significant Bits of those bytes to recreate the hidden byte—that is 0110001—the letter "a." 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. Data transmission

Here for data transmission, we are using ZigBee module because it's more secure. ZigBee is used in applications that require a low data rate, long battery life, and secure networking. ZigBee has a defined rate of 250kbit/s, best suited for periodic or intermittent data or a single signal transmission from a sensor or input device. ZigBee networks are secured by 128 bit symmetric encryption, distances range from 10 to 100 meters line-of-sight.

ZigBee is new specification for a suite of high level communication protocols used to create personal area networks built from small, low-power digital radios. ZigBee is based on an IEEE 802.15 standard. The Zigbee Alliance is a group of companies that maintain and publish the Zigbee standard. The term Zigbee is a registered trademark of this group, not a single technical standard. The Alliance publishes application profiles that allow multiple OEM vendors to create interoperable products. The relationship between IEEE 802.15.4 and Zigbee is similar to that between IEEE 802.11 and the Wi-Fi Alliance.

Zigbee devices are of three types:

- Zigbee Coordinator (ZC): The most capable device, the Coordinator forms the root of the network tree and might bridge to other networks. There is exactly one Zigbee Coordinator in each network since it is the device that started the network originally (the Zigbee Light Link specification also allows operation without a Zigbee Coordinator, making it more usable for over-the-shelf home products). It stores information about the network, including acting as the Trust Center & repository for security keys.
- Zigbee Router (ZR): As well as running an application function, a Router can act as an intermediate router, passing on data from other devices.
- Zigbee End Device (ZED): Contains just enough functionality to talk to the parent node (either the Coordinator or a Router); it cannot relay data from other devices. This relationship allows the node to be asleep a significant amount of the time thereby giving long battery life. A ZED requires the least amount of memory, and therefore can be less expensive to manufacture than a ZR or ZC.
- The current ZigBee protocols support beacon and non-beacon enabled networks. In non-beacon-enabled networks, an unslotted CSMA/CA channel access mechanism is used. In this type of network. In beacon-enabled networks, the special network nodes called ZigBee Routers transmit periodic beacons to confirm their presence to other network nodes. Nodes may sleep between beacons, thus lowering their duty cycle and extending their battery life. Beacon intervals depend on data rate; they may range from 15.36 milliseconds to 251.65824 seconds at 250 kbit/s, from 24 milliseconds to 393.216 seconds at 40 kbit/s and from 48 milliseconds to 786.432 seconds at 20 kbit/s. However, low duty cycle operation with long beacon intervals requires precise timing, which can conflict with the need for low product cost.

4. Proposed Technique

Here we will discuss the disadvantages of the previous procedure and how those are different with present method. The main disadvantages associated with the use of existing methods like echo hiding, spread spectrum and LSB hiding are, human ear is very sensitive to noise and it can often detect even the slightest bit of noise introduced into a sound file and another problem is robustness. LSB coding has main disadvantage of low data transmission rate because of the fact that the secret message is encoded only in the first signal segment. Hence this method is used only when a small amount of data needs to be transferred. Among different information hiding techniques proposed to embed secret information within audio file, Least Significant Bit (LSB) coding method is the simplest way to embed secret information in a digital audio file by replacing the least significant bit of audio file with a binary message. Hence LSB method allows large amount of secret information to be encoded in an audio file.

Steps to hide secret information using LSB are:
a. Covert the audio message file into bit stream.
b. Covert the audio mask file into bit stream.
c. Replace the LSB bit of audio message file with the LSB bit of audio mask file

This proposed method provides greater security and it is an efficient method for hiding the secret information from hackers and sent to the destination in a safe and undetectable manner. This proposed system also ensures that the size of the file is not changed even after encoding and it is also suitable for any type of audio file format.

5. Implementation

Flow-chart below show the implementation of the system, steps involved in the same. Later part we have explained how we are encrypting and decrypting the data

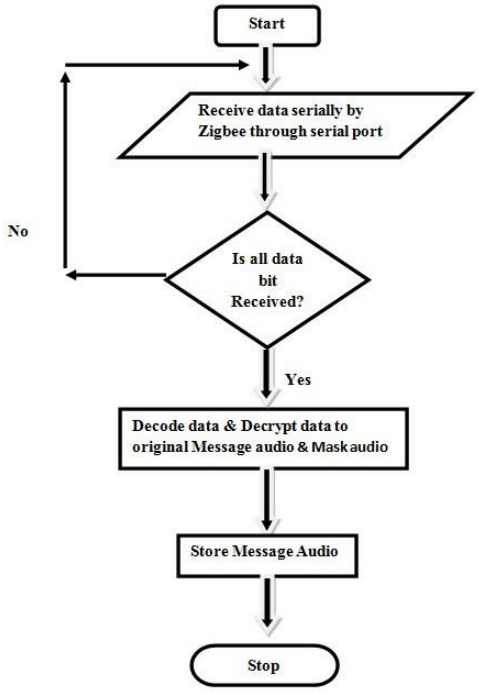

Fig.a Encryption Algorithm

a. Hide text

This Steganography is implemented in Matlab 2012b. First a wav file is opened using fopen. Then the header part (first 40 bytes) of wav file is copied to variable "header". Byte no. 41 contains 32 bit data size of file this is copied to variable data_size. Then data samples starts from byte no.44 to the end. Copy the data samples to variable "dta" using fread and close the file. Convert the Audio message and the length of Audio message to binary. Hide three content in data samples identifier, length of Audio message and Audio message itself. Identifier helps in the recovery of text. If identifier is not in the file then code stop execution assuming that the wav file has no hidden Audio message. Here the identifier is binary 10101010. LSB of first 8 data samples have the identifier. LSB of next 10 data samples have length of Audio message. LSB of next 10 data samples have width of text message. Then all the LSB of data samples after this have bits of binary Audio message. Open a new wav file in write mode, copy the header original wav file to this file, and then copy the 32 bit data_size to the new file. At last the copy "dta" the

data samples containing the hidden text message bits to the new file.Close the file. The new wav file is in the current directory.

Recovery Test

The procedure to recover Audio is reverse of hiding the text. Open the wav file. Then directly copy the data samples starting from 44th byte to the end of file. Take out the LSB of first 8 data samples and check for the identifier 10101010.If identifier is not present then the file has no hidden text. Take out next 10 LSB which is the length of Audio message and next 10 LSB which is the width of text message. Now take out the LSB of data samples upto the length of message. Convert to text and then reshape them.

6. Conclusions

In this paper, I have introduced a robust method of imperceptible audio data hiding. This system is to provide a good, efficient method for hiding the data 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 suitable for wav type of audio file format. Thus we 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. Audio Steganography is a really interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day. But it is also quite real; this is not just something that's used in the lab or an arcane subject of study in academia. Stego may, in fact, be all too real — there have been several reports that the terrorist organization attacks in New York City, Washington, D.C., and outside of Pittsburgh used audio steganography as one of their means of communication.

REFERENCES

1 R. Sridevi, DR. A. Darnodaram, and DR. SVL. Narasimham~" Efficient method of audio steganography by modified LSB algorithm and strong encryption key with enhanced security '\ in JATIT [Journal of Theoretical and Applied Information Technology] , 2005-2009 .

2 P. Jayaram, H. R. Ranganatha, H. S. Anupama "' Information hiding using audio steganography-a survey", 3rd ed., vol. 3. l11vlA

3 Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key with Enhanced Security 1r Sridevi, 2dr. A Damodaram, 3dr. Svl.Narasimham Assoc. Prof., Department Of Computer Science And Engineering, Jntuceh, Hyderabad Prof., Department Of Computer Science And Engineering, ntuceh, Hyderabad Prof., School Of Information Technology, Jntuh, Hyderabad.

4 Audio Steganography using Matlab, Rashmi Mishra1, Rupal chauhan2, Poonam Jhariya3, Priya Mishra4, Vaishali Yadav5, Tazeem A Hazra6, International Journal of Engineering, Applied and Management Sciences Paradigms, Vol. 02, Issue 01, April 2013 ISSN (Online): 2320-6608

5 "ZigBee Specification FAQ". *Zigbee Alliance*. Zigbee Alliance. Retrieved 14 June 2013.

6 "ZigBee Wireless Networking", Drew Gislason (via EETimes)

7 "Frequently Asked Questions". Zigbee Alliance. Retrieved March 23, 2013.

8 "ZigBee: Wireless Technology for Low-Power Sensor Networks". Commsdesign.com. Retrieved 2012-10-18.

9 "The ZigBee Alliance". Zigbee.org. Retrieved 2012-10-18.

10 "Wireless Sensor Networks Research Group". Sensor-networks.org. 2008-11-17. Retrieved 2012-10-18.

11 "Wireless Sensor Networks Research Group". Sensor-networks.org. 2010-04-15. Retrieved 2012-10-18.

12 "Wireless Sensor Networks Research Group". Sensor-networks.org. 2009-02-05. Retrieved 2012-10-18.