LOSSLESS AUDIO CONVERSION TECHNIQUE TO PROPOGATE SENSITIVE INFORMATION

Bharathy.B

Student, Department of Electronics and Communication Engineering

Shri Krishnaa College of Engineering and Technology, Pondicherry

bbharathy1997@gmail.com

Nandhini.K

Student, Department of Electronics and Communication Engineering

Shri Krishnaa College of Engineering and Technology, Pondicherry

Nandhini126@gmail.com

Mr.V.Murugan

Associate Professor, Department of Electronics and Communication Engineering

Shri Krishnaa College of Engineering and Technology, Pondicherry

murugan4570@gmail.com

Abstract

Our proposed approach is a novel reversible audio text embedding to achieve homogeneous steganography scheme over encrypted domain to achieve maximum unaltered audio after secret message embedding. We have encoder/Decoder separate coding scheme to get both results separately using binary bit shift techniques. We have designed a powerful decoder to distinguish encrypted and non-encrypted audio patches, allowing us to jointly decode the embedded message and the original audio signal. Compared with the state-of-the-art methods, the proposed approach provides higher embedding capacity and is able to perfectly reconstruct the original audio as well as the embedded message. We performed several tests to check the real time usability of the project are provided to validate the superior performance of our scheme. There were several attempts to obtain the correct result using audio steganography but none of them were successful due to multimedia complexity and technicality. No guarantee of data transmission over internet securely as hacking information is quite easy today. If any data is encrypted in any file as in olden systems then also it can be easily tracked because the quality of the source where it was hidden reduces. So many cryptographic techniques are used before but then too the guarantee of 100% secrecy rate is not obtained. Audio quality reduces if any data is hidden inside and can be easily detected for information hiding. In our system we are going to initiate for 100% secrecy rate for Audio with text hiding audio quality degrades , Size of text message to be hidden in audio should be very small, Key , Security Concerns.

Keywords: Secrecy Rate, Security Concerns, Multimedia Complexity

1. INTRODUCTION

Audio

Audio is sound within the acoustic range available to humans. An audio frequency (AF) is an electrical alternating current within the 20 to 20,000 hertz (cycles per second) range that can be used to produce acoustic sound. Sound is a sequence of naturally analog signals that are converted to digital signals by the audio card, using a microchip called an analog-to-digital converter (ADC).When sound is played, the digital signals are sent to the speakers where they are converted back to analog signals that generate varied sound.

Processing

Movement of data or material towards a known goal or end result by passing it through a series of stages or a sequence of actions is termed as processing.

Audio Processing

Audio signal processing, sometimes referred to as audio processing, is the intentional alteration of auditory signals, or sound, often through an audio effect or effects unit. As audio signals may be electronically represented in either digital or analog format, signal processing may occur in either domain. Analog processors operate directly on the electrical signal, while digital processors operate mathematically on the digital representation of that signal.

Steganography

Steganography (pronounced STEHG-uh-NAH-gruhf-ee, from Greek steganos, or "covered," and graphie, or "writing") is the hiding of a secret message within an ordinary message and the extraction of it at its destination.

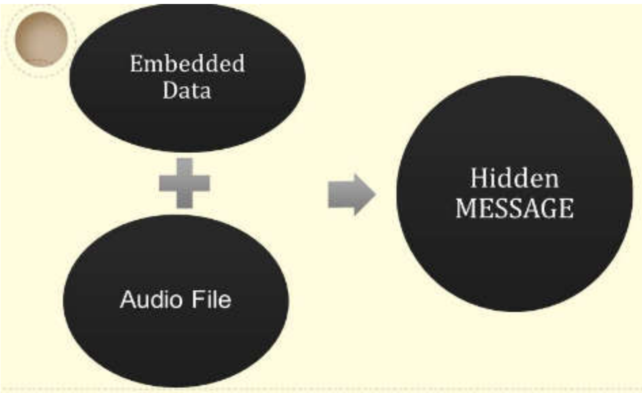


Fig.1 – Audio Steganography

The main difference between cryptography and steganography is cryptography deals with messages which are secured by some codes or physical arrangements. Anybody can easily doubt the possibility of message hidden inside the simple terms but steganography is way far advanced. In steganography secret messages are hidden inside any simple image, audio or video but we can't doubt the possibility of hidden message.

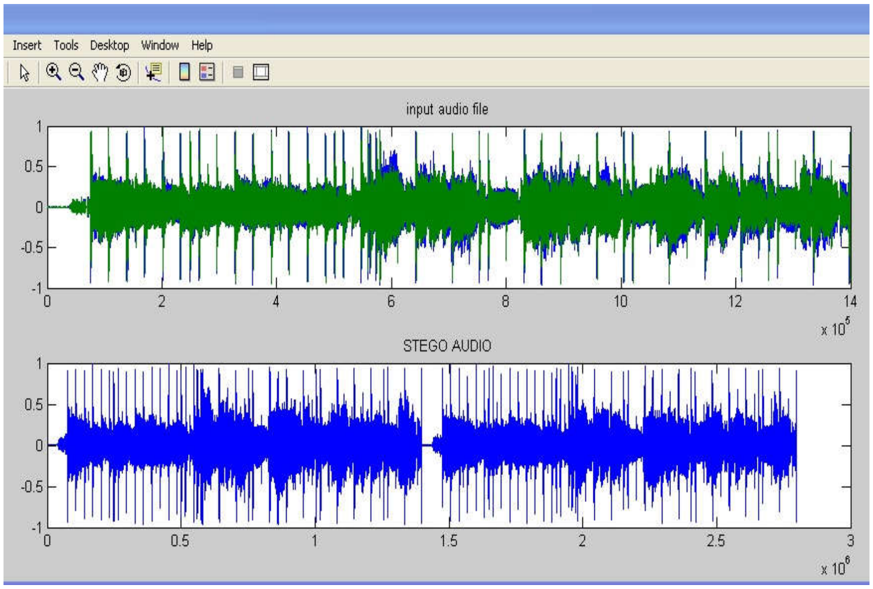


Fig.2 – Problem In existing Audio Steganography Systems

As we can see above audio plot before steganography in input original audio file and after hiding the secret message. We find audio is not same after hiding message its quality and strength degraded drastically. Our main aim is to avoid the error and create a system which should be efficient so that after hiding information in audio then too quality of audio should not degrade. Our aim is to achieve the quality displayed in **Fig.3**.

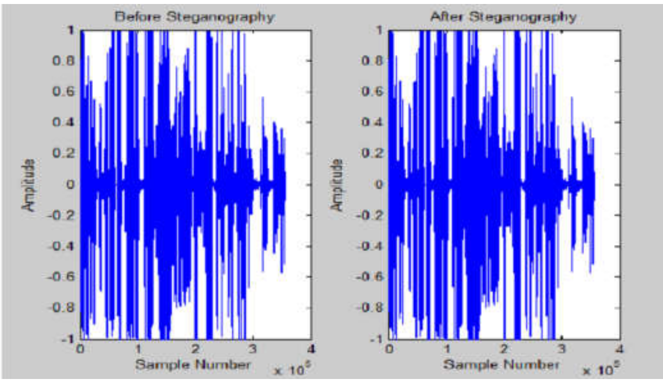


Fig. 3 – Expected achievable audio quality after embedding secret message

2. PROPOSED APPROACH

In audio steganography; secret message is embedded in the digital sound by slightly altering the binary sequence of the sound file. Existing audio steganography software deal with WAV, AU, and even MP3 sound files. Embedding secret messages in the digital sound is usually a more difficult process than embedding messages in other forms, such as digital images.

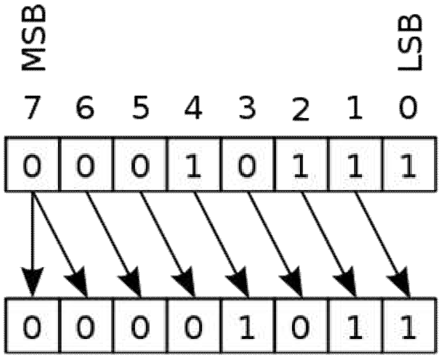


Fig. 4 – Binary Bit Shifting with LSB

Audio steganography uses different algorithms, but (LSB) least significant bit and binary bit shifting technique is applied in this paper. The quality of sound is depended on the size of the audio which the user selects and length of the message.

LSB Insertion

The most basic of LSBs insertion for 24-bit pictures inserts 3 bits/pixel. Since every pixel is 24 bits, we can hide

3 hidden_bits/pixel / 24 data_bits/pixel = 1/8 hidden_bits/data_bits

So for this case we hide 1 bit of the embedded message for every 8 bits of the cover image.

If we pushed the insertion to include the second LSBs, the formula would change to:

6 hidden_bits/pixel / 24 data_bits/pixel = 2/8 hidden_bits/data_bits

And we would hide 2 bits of the embedded message for every 8 bits of the cover image. Adding a third-bit insertion, we would get:

9 hidden_bits/pixel / 24 data_bits/pixel = 3/8 hidden_bits/data_bits

Acquiring a data rate of 3 embedded bits every 8 bits of the image.

The data rate for insertion in 8-bit images is analogous to the 1 LSB insertions in 24-bit images, or 1 embedded bit every 8 cover bits.

We can see the problem in another light, and ask how many cover bytes are needed to send an embedded byte.

For 1-LSB insertion in 24-bit images or in 8-bit images this value would be 8/1*8 = 8 Bytes, for 2-LSBs insertion in 24-bit pictures it would be 8/2*8 = 4 Bytes, for 3-LSBs insertion it would be 8/3*8 = 21.33 Bytes.

3 Outputs

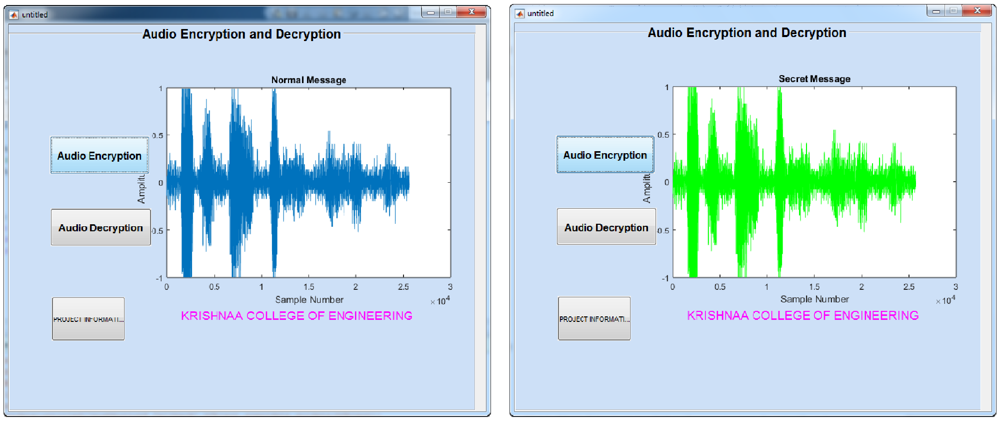
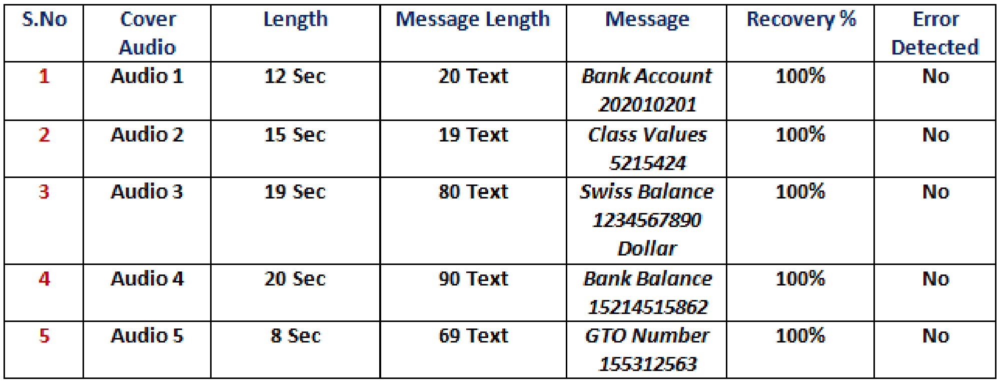


Fig 5: GUI (Original Audio, Stego Audio)

Advantages

- It can hide text in Audio files also without disturbing Audio which can be used over internet or can be used in phones as ringtones but they have large files hidden inside.
- Uses bit shifting technique to create the space for secret information as bit size of text is very small compared to audio.

Performance Metric Based on Real-time Test



S.No	Cover Audio	Length	Message Length	Message	Recovery %	Error Detected
1	Audio 1	12 Sec	20 Text	*Bank Account 202010201*	100%	No
2	Audio 2	15 Sec	19 Text	*Class Values 5215424*	100%	No
3	Audio 3	19 Sec	80 Text	*Swiss Balance 1234567890 Dollar*	100%	No
4	Audio 4	20 Sec	90 Text	*Bank Balance 15214515862*	100%	No
5	Audio 5	8 Sec	69 Text	*GTO Number 155312563*	100%	No

CONCLUSION

Thus we created a system of efficient stenographic content and verified it for its usability. We use bit shifting to shift the bits in audio to hide it on appropriate location. The system is checked for its working in real time scenario on different audio and text length. In all the tests it performed acceptable results. In our future enhancement we plan to create the common server to share the secret message over encrypted cloud domain.

Acknowledgments

I thank Mr. Raushan Kumar Singh, SPECTRUM SOLUTIONS, Pondicherry to help me in creating this paper with his Sincere Guidance and Technical support in the field of Signal Processing. I thank my guide Mr.V.Murugan, A.P/ECE, Shri Krishnaa College of Engineering and Technology, Pondicherry, for his great support. The help of Mr.S.Seenuvasamurthi, HOD, Department of Electronics and Communication Engineering, Shri Krishnaa College of Engineering and Technology, is really immense and once again I thank for his great motivation. I thank SKCET, Pondicherry for providing me such a standard educational environment so that I am able to understand the minute concepts in the field of Engineering and Technology.

References

[1]C. Yeh, C. Kuo, (October 1999) ***Digital Watermarking Through Quasi M- Array***s, Proc. IEEE Workshop On Signal Processing Systems, Taipei, Taiwan, Pp. 456-461.

[2] Dr. D Mukhopadhyay, A Mukherjee, S Ghosh, S Biswas, P Chakarborty (2005.) ***An Approach for Message Hiding using Substitution Techniques and Audio Hiding in Steganography***, IEEE

[3] E. Zwicker, "P***sychoacoustics***", Springer Verlag, Berlin, 1982.

[4] Mazen Abu Zaher ***Modified Least Significant Bit (MLSB) Published by Canadian Center of Science and Education*** Vol. 4, No. 1; January 2011

[5] Nedeljko Cvejic, Tapio Seppben (, IEEE 2002) ***Increasing the Capacity of LSB-Based Audio Steganography***

[6] Steganographic Techniques and their use in an Open-Systems Environment- Bret Dunbar, ***The information Security reading Room***, SANS Institute 2002http://www.sans.org/reading room/whitepapers/covert/677.php

[7]Mansour Sheikhan et al, ***High Quality Audio steganography by Floating Substitution of LSBs in Wavelet Domain,*** world applied science Journal IDOSI publications, 2010

[8] Y.V.N.***Tulasi et al., Steganography -Security through Images***

[9] ***On Embedding of Text in Audio – A case of Steganography*** Pramatha Nath Basu, 2010 International Conference on Recent Trends in Information, Telecommunication and Computing

Appendix

Matlab (Matrix Laboratory) is a high-performance language for scientific and technological calculations. It integrates computation, visualization and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation. It is a complete environment for high-level programming, as well as interactive data analysis. Some typical applications are

- system simulations,
- algorithm development,
- data acquisition, analysis, exploration, and visualization, as well as
- Modeling, simulation and prototyping.

Matlab was originally designed as a more convenient tool (than BASIC, FORTRAN or C/C++) for the manipulation of matrices. It was originally written to provide easy access to matrix software developed by the LINPACK and EISPACK projects. After- wards, it gradually became the language of general scientific calculations, visualization and program design. Today, Matlab engines incorporate the LAPACK and BLAS libraries, embedding the state of the art in software for matrix computations. It received more functionalities and it still remains a high-quality tool for scientific computation. Matlab excels at numerical computations, especially when dealing with vectors or matrices of data.

Bharathy.B was born in Pondicherry, India on 29 January 1997. She received her Graduate degree *in Electronics and Communication Engineering from Shri Krishnaa College of Engineering and Technology, Pondicherry in 2018.*

Nandhini.K was born in Pondicherry, India on 11 June 1997. She received her Graduate degree *in Electronics and Communication Engineering from Shri Krishnaa College of Engineering and Technology*, Pondicherry in 2018.

Mr.V.Murugan was born in Pondicherry, India on 4 May 1970. He is currently working as Associate Professor for the department of Electronics and Communication Engineering in Shri Krishnaa College of Engineering and Technology, Pondicherry. He had published many papers during the period of working and also had given many guest lectures.