Data Hiding In Audio by Using Audio Steganography

Pooja Kengale[1], Rakhi Kadam[2], Rajkumar Chaudhari[3], Prof. Sagare Sir

[1,2,3]*B.E Final year, Sinhgad Institute of Technology, Lonavala, Maharashtra, India*

Abstract: **In this paper, a robust substitution technique is used to implement proposed work of audio steganography. Steganography is an art and science methodology of writing hidden messages such a way that no one apart from the intended reciever knows the existence of the secret message data. This technique resolves the various inherent issues ,after that it increases the data hiding capacity while being also achieve robustness from various intentional as well as unintentional hacking attacks.like this it provides privacy to data. The strength of our algorithm is depend on the segment size and its used to achieve very high embedding capacity for different data type that can reach up to 25% from the input audio file size.We are developing two novel approaches of substitution technique of audio steganography that improves the capacity of cover audio which for embedds additional data. Using these methods, messages are embedded into multiple LSB bits. This technique utilizes up to 7 LSBs for embedding data. Results show that both these techniques improve data hiding capacity of cover audio by 25% to 85% These latest approaches for increasing capacity show better results as compared to the existing techniques.**

Keywords: Steganography, capacity, robustness, data hiding, cryptography, LSB

I. INTRODUCTION

The usage of the internet terminologies are increases rapidly and the huge revolution in digitization of data are happened.due to this overall scenario of modern communication is changed.Because of this revolution in software industry the hardware as well as the software are becomes more user-friendly it and flexible.and enables consumer to communicate multimedia data.and able to transmit large multimedia files through broadband connection of internet.

Data hiding is a technique of providing data security.Using audio file as a cover medium instead of image is more tedious,as Human auditory System(HAS) is more sensitive than Human Visual system (HVS).audio files are available anywhere.thats why it becomes very easier to hide data by using audio and therefore requires to develop many techniques which provide security to data which are in audio files.By using steganography we can able to provide security to provide data.Steganography is an art of secret communication.Stegangraphy is a word derived from the ancent Greek words steganos,which means covered and graphia,which in means writing.hiding information such that its presence can not be detected.sender hides the secret information such that its presence can not be detected.sender hides the secret information in some carrier file and then transmitted on reciever side ,the carrier file can be image,audio file,text file,video file. At the reciever's end,the secret data can be recovered from the stego signal using different algorithmic technique.

We can able to speak that given data is secured only when it follows the following requrements.The first requirement is perceptual transperancy,i.e:cover object(object not containing any additional data) and stego object(object containing secret message) must be perceptually indiscernible.The second constraint is
high data rate of the embedded data.
robustness:it measures the ability of the embedded data to withstand against intentional and unintentional attacks.
Unintentional attacks:attacks generally include common data manipulation such as re-sampling,re-quantization etc.
Intentional attacks include addition of noise,resizing,rescalling etc.
Data rate(capacity):It refers to the amount of information that a data hiding scheme can successfully embed without introducing perceptual distortion.

In other words the bits rate of message is the no of the embedded bits within a unit of time and is usually given in bits per second(bps).audio steganography can be performed in time domain as well as frequency domain.we present 2novel approaches of LSB coding that increase capacity of cover audio so as embed large data and section II:describes the proposed methods,which uses different substitution techniques like LSB Encoding,Parity Coding,Phase coding,spread spectrum,secret message recovery stage,reverse encryption.

Steganography has wide range of applications such as covert communication,digital watermarking,access control,digital rights managements etc.Through this method,the audio steganographic problems are studied and creating a powerful secure solution for it,and therefore the security issue in modern communication is successfully resolved.

1.1 Fundamental Concepts On (Domain):

In the data hiding the secret message can be need to transfer on receiver side by using audio file.for the data hiding purpose we used steganography technique which is nothing but a cover writing.and also uses a cryptogrphy concept for encryption send decryption purpose.sender has a public key and receiver has a private key.and through lsb algorithm we are embedding the audio secret message bits into the audio file.and through substitution technique we are provide security to the secret message whch is transfer through the carrier over the network.but at the receiver side by using the decryption key it decodes the message and get the secret message from the audio but that time original file of audio remains same.

1.2 Contributions:

Audio steganography is a data hdding technique.Now a days there are many techniques are available to provide security for hiding data in audio by using steganography.But there are many drawbacks are in that techniques,so there is need to provide solution on that all.

We are making the improvement in that techniques, which are hiding data in audio by using steganography. In our technique we are handling the many issues related to that techniques.Like in previous techniques after hiding data because of quantization and compression, the noise was created in the original audio file.And due to this the size of audio file was increases.

By using our latest substitution technique, without performing any compression and quantization we are hiding the data in audio file.For that various latest LSB and steganographic algorithms we are using.And therefore the size of audio get not changed,and quality of original audio is maintained.Because of modern steganography techniques we are able to provide security to data from vulnerable attacks and able to hide data very securely in audio without any modification in original audio.

II. LITERATURE SURVEY

2.1 Existing System:

The literature survey paper gives an overview about data hiding which is compressed in the audio signals.and the source for compression is a AAC format file.

In the AAC MPEG4 data hiding scheme is performed based on the human auditory system.In this data hiding is performed mainly in the quantization process of MDCT phase method of the AACcoding.and hidden data capacity can be easily achieved without any modification into the original audio file.but the implementation is very complicated because of the quantization and compression process.

This scheme alters the quantization and coding process by modifying the scale factors to produce more bits,in which redundant bits of audio file xan be replaced with the hidden data.The basic structure of the system includes all the relevant parts of the AAC MPEG-4 perceptual encoding.in this it performs various steps like domain conversion RS and SPA detection frequency and perceptual domain measurement.

This scheme enables optimal coordination between the quantization process of the encoder and the data hiding.The scheme vary the data hiding capacity by adjusting no of coefficients for the quantization.and thus,this scheme provides data hiding.When the embedded data bit rate needs to be changed, that time this scheme can change the quantization parameters also.hence it affects on the original quality of the original audio file signals.

The coefficients which are carry the hidden data are picked as per the pseudo random mechanism which is unlikely to be intercepted by a third party.in this sender can able to embed only one bit at a time.hence,very poor performance it has and because of quantization orginal audio size also changes which creates the noise and create bad impact for data hiding.

2.2 Solution

2.2.1 Conflict:

When the data hiding performed into the aac audio file, at that time need to compressed audio signals.and also all secret data hiding purpose low bit rating was performed.which is very time consuming and complicated task.because of compression the noise is generated into the audio file.for the embedding low bit rating technique is used.therefore the size of audio file is increases. .hence, the receiver can not get the original audio. hence,project seeks to grow.and its community needs to manage all this major conflict. And need to generate the solusion for that.

2.2.2 Substitution

XU shexhung finds a method for data hiding in aac audio file,in that it performed quantization and the compression of audio.because of that the size of audio file was increases and receiver can’t get the original contents.Hence, the dr a.r kekre and uttara athwale studies this problem and they develop the LSB algorithm technique for the bit embedding purpose.because of that doesn’t need to compressed audio file.hence, the size of algorithm is does not varies as per the secret msg.

But this is not the fine solution ,need to do more improvement into that.sender can send the msg over the network securely for that purpose we are adding steganographic technic.and also performs some security purpose substitution steps at a time of bit embedding.Because of that substitution algorithm sender can able to send message through carrier over the network very securely.and when the receiver get the message it can able to get original audio and secret message as it is.because of substitution algorithm hacker can not able to perform any modification into the audio file.

III. PROPOSED SYSTEM

- We are using steganography for hiding data in audio. in which we will be handling the issues according to issue type..
- We handle the issues fast with the help of the issues status.
- We will handle the issues according to their priorities.

- With the help of game data hide steganography technique and substitution technique we will solve the issues fastly and arrange them according to the issue resolution.

IV. RELATED WORK

Many researchers have investigated what factors indicate the secure data transmission .audio file containing secret data while transmitting if it doesn’t contain any noise will be transferred securely at the receiver with same audio quality. They also noted that the techniques like quantization increase the size of original audio file. So we have to use latest techniques to avoid such quanflicts. Audio steganography is focused in hiding secret information in an audio file or signal securely and strongly. Communication security and robustness are vital for transmitting important information to authorized entities, while denying access to not permitted ones. By embedding secret information using an audio signal as a cover medium, existence of secret information is hidden away during communication. This is a serious and vital issue in some applications such as battlefield communications and banking transactions[9]. 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.

V. IMPORTANT COMPONENTS (MODULES)

5.1 Input secret message and cover signal

The secret message can be any text file or image or any audio wave file and then inputting the cover signal in which data is to be embedded. This cover signal must be sufficient large to cover the message. After selection of input secret message and cover signal next, we find out the length of the audio file as well as length of the text file.The secret msg can be any text data or audio mp4 file and the input cover medium where the data is embedded.after taking the input fo the data hiding purpose as per that text length need to choose appropriate audio file for hiding that data.

5.2 Encryption

Before hiding the secret message into cover signal it must be converted into the other form so that it can’t be interpretable by intruder. To do so first, we convert the secret data or message into its binary form. Let suppose the length of message is N bits long, Next use the random number to generate the private key of length same as the length of message because the size of encrypt message is equal to the original message, then apply X-OR operator to generate the cipher message of length N bits.

```
for k = 1: N
if mod (k, 4) == 0
M (k) = 1;
else
M (k) = 0;
End
Cipher Text= S (XOR) M
```

5.3 LSB

In LSB method it checks the value of first two MSB bits for the cover audio file for data embedding.For e.g we want to encode the msg ‘HELLO’ into 16bit sample format by LSB method.

1)secret msg ’hello’ and the cover audio fie is converted into the bit stream format.like

HELLO=1000110011(bit stream).

2)least significant bit(LSB) column of audio file is replaced with stream of bits of secret msg ‘HELLO’.

Audio file bit stream=bits of secret message()

3)after the embedding the secret bits into the empty bit slt of audio msg that file is called as a 'STEGO-FILE'.

5.4 substitution and data hiding

after the senders secret msg is embedded into the audio file.that data needs to transfer on the network via root it reaches to the exact reciever.but between that network there are many chances to loose and hacking of data through hackers.hence need to provide security to that data.hence substitution technique is used here.in this technique after performing cryptography encryption.in steganography sender has a public key by which it hides the data and send over the network but that data can be decrypt only a authenticated valid reciever who has a private key of that sg which is assigned by a particular sender.hence,acept that authenticated reciever no on can able to perform manipulation on that data.
for eg.
1)after the secret msg is hided into the audio file.sender assign a private key to reciever for decryption of that msg.
2)sender send that audio file to reciever.
3)after file reaches to particular valid reciever.it decrypt that cipher message by using the private key.which is assigned by the sender.

VI. DISCUSSION AND FUTURE WORK

In this project we are hide data in the audio file.before this we can able to hide data in audio file, but there are many security issues and capacity problems are occurred in that.Hence we are finding all that problems.discuss on them.and we established our substitution technique for revealing all the problems which are in the previous method.in previous method,we are able to embbed only one bit data into the empty slot of audio file.but in our technique we can embbed two bits into the empty slot of audio.but for that we are not performing any compression.hence,the original size of the audio does not increased and for that we are using our substitution technique and LSB algorithm.with the help of that we eliminating the major quality problems of audio.and also with the help of steganography key we provide roboust security to secret msg which hide in the audio file.With the helpf our substitution algorithm the work will be progressed fast.

VII. CONCLUSION

This paper Customization of audio steganography will help sender to send a secret information using an audio file to send to receiver effectively and efficiently. This software will troubleshoot the errors for secure data transmission. which is used for writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. This proposed technique overcomes all the limitation of exiting software. The algorithm will hide the message as per
the proposed solution . The method currently uses 2 bits per byte of audio sample. It may provide higher capacity and robustness.

In this paper, two new approaches to increase the capacity of the cover audio have been planned. Instead LSB coding method, these methods embed data in multiple and variable LSBs depending on the MSBs of the cover audio samples. The main advantages of the proposed methods are that they are simple in logic and the hidden information is recovered without any error. We have offered a high capacity and high stego-signal worth audio steganography scheme. This proposed system has been tested for different hiding capacity and it gives excellent output. Great level of security is achieved using this algorithm. Modified LSB algorithm for data transmission algorithm can be used where high security file with secret data transmission required in public forums. It is used for secure data transmission. This is a serious and vital issue in some applications such as battlefield communications and banking transactions.

REFERENCES

[1] Zamani M., Ahmad R.B., Manaf A.B.A., Zeki A.M., “An Approach to Improve the Robustness of Substitution Techniques of Audio Steganography”, *in Proc. IEEE International Conference on Computer Science an Information Technology*, ICCSIT pp: 5-9, 2009.

[2] Zaidoon Kh. A.A.Zaidan, B.B.Zaidan and Hamdan . O.Alanazi, Overview: Main Fundamentals for Steganography, journal of computing, volume 2, issue 3, march 2010, ISSN 2151-9617.

[3] Sos S. Agaian, David Akopian and Sunil A. DÆSouzaö” TWO ALGORITHMS IN DIGITAL AUDIO STEGANOGRAPHY USING QUANTIZED FREQUENCY DOMAIN EMBEDDING AND REVERSIBLE INTEGER TRANSFORMS” Non-linear Signal Processing Lab, University of Texas at SanAntonio,Texas 78249, USA

[4] Ashwini Mane, Gajanan Galshetwar and Amutha Jeyakumar,”DATA HIDING TECHNIQUE: AUDIO STEGANOGRAPHYUSING LSB TECHNIQUE” International Journal of Engineering Research and Applications (IJERA),Vol. 2, Issue 3, May-Jun 2012, pp.1123-1125

[5] Neil Jenkins, Jean Everson Martina ,ö Steganography in Audioö Anais do IX Simp≤sio Brasileiro em Seguranτa da Informaτπo e de Sistemas Computacionais page: 269-278,2007

[6] Gruhl D, Lu A, Bender W. Echo hiding. Lecture Notes in Computer Science, 1996, 1174: 295-315.

[7] Dumitrescu S, Wu Xiaolin, Wang Zhe. Detection of LSB steganography via sample pair analysis. IEEE Transactions on Signal Processing, 2003, 51(7): 1995-2007.

[8] R SRIDEVI, DR. A DAMODARAM, DR. SV L.NARASIMHAM, " Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key with Enhanced Security", in Proc. J A TIT PP:768-77 1,2005-2009.

[9] Gopalan, K. and S. Wenndt, Audio Steganography for Covert Data Transmission by imperceptible Tone Insertion. in Proc. The IASTED International Conference on Communication Systems and Application (CSA 2004), Banff, Canada, July 8-10, 2004.

[10] Bret Dunbar, "A Detailed Look at Steganographic Systems and their Use in Open-Systems Environment" in SANS Institute Infosec Readingroom, August 0I, 2002,url:http://www.sans.org/readingroom/whitepapers/covertldetailed-steganographic-techniques-open-systemsenvironment- 677

[11] Neil Jenkins, Jean Everson Martina ,ö Steganography in Audioö Anais do IX Simp≤sio Brasileiro em Seguranτa da Informaτπo e de Sistemas Computacionais page: 269-278,2007

[12] Zamani M., Ahmad R.B., Manaf A.B.A., Zeki A.M., ôAn Approach to Improve the Robustness of Substitution Techniques of Audio Steganographyö, in Proc. IEEE International Conference on Computer Science and Information Technology, ICCSIT pp: 5-9, 2009.

[13] ôaudio steg : overviewö, Internet publication on www.snotmonkey.com http://www.snotmonkey.com/work/school/405/overview.html.

[14] Nedeljko Cvejic , Algorithms for audio watermarking and Steganography http//herkules.oulu.fi/isbn9514273842/isbn9514273842.pdf.