High Capacity and Inaudibility Audio Steganography Technique

Amit Shivdas Dukare
Department of Computer Science & Engineering
Sagar Institute of Research & Technology, Bhopal (M.P.), India

Abstract – In computer science, information hiding is the principle of segregation of the design decisions in a computer program that are most likely to change, thus protecting other parts of the program from extensive modification if the design decision is changed. The protection involves providing a stable interface which protects the remainder of the program from the implementation. The techniques used for data hiding vary depending on the quantity of data being hidden and the required invariance of those data to manipulation.

Keywords: Steganography, Fingerprinting, Watermarking, Audio, Video Steganography.

I. INTRODUCTION

The rapid growth in modem communications needs the special means of security especially on computer network. The network security is becoming more important as the number of data being exchanged on the Internet increases. Therefore, the confidentiality and data integrity are required to protect against unauthorized access. This has resulted in an explosive growth of the field of data hiding [1].

Data hiding is a software development technique specifically used in object-oriented programming (OOP) to hide internal object details (data members). Data hiding ensures exclusive data access to class members and protects object integrity by preventing unintended or intended changes. Data hiding also reduces system complexity for increased robustness by limiting interdependencies between software components. Data hiding is also known as data encapsulation or information hiding[2].

II. SYSTEM MODEL

Modern Steganography is generally associated with embedding of secret information into the digital media like image, audio, video, and text rather than physical objects. Audio steganography is focused in hiding secret information in an innocent cover audio file or signal securely and robustly[3]. 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, the very 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. The secret message is concealed into the audio media by slightly changing the binary sequence of the audio file. Hiding secret information into digital audio media is generally more complicated than hiding secret information into other media, such as digital images. In order to hide secret information successfully, a range of techniques for inserting information into digital audio have been introduced. These techniques vary from simple ones that embed information as signal noises to more powerful ones that take advantage of complicated signal processing techniques to embed the secret message [4]. embedding of secret information into the digital media like image, audio, video, and text rather than physical objects. Audio steganography is focused in hiding secret information in an innocent cover audio file or signal securely and robustly[3]. 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, the very 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. The secret message is concealed into the audio media by slightly changing the binary sequence of the audio file. Hiding secret information into digital audio media is generally more complicated than hiding secret information into other media, such as digital images. In order to hide secret information successfully, a range of techniques for inserting information into digital audio have been introduced. These techniques vary from simple ones that embed information as signal noises to more powerful ones that take advantage of complicated signal processing techniques to embed the secret message [4].

III. PREVIOUS WORK

In R.Sridevi, Dr. A. Damodaram, Dr. Svl. Narasimham [5], proposed Enhanced Audio Steganography (EAS) which is based on audio Steganography and cryptography that ensures secure data transfer between the source and destination. EA Suses most powerful encryption algorithm in the first level of security, which is very complex to break. In the second level it uses a more powerful modified LSB (Least Significant Bit) Algorithm to encode the message into audio. It performs bit level manipulation to encode the message Jayaram P, Ranganatha H R, Anupama H S [6], describe Today's large demand of internet applications requires data to be transmitted in a secure manner. Bairagi, A.K, Mondal, S [7], propose a novel approach of substitution technique of audio steganography. Using genetic algorithm, message bits are embedded into multiple, vague and higher LSB layers, resulting in increased robustness. Kaliappan Gopalan and Stanley Wenndt[8], describe the technique of embedding data in an audio signal by inserting low power tones and its robustness to noise and cropping of embedded speech samples. Leaning towards designing a system that ensures high capacity or robustness and security of embedded data has led to great diversity in the existing steganographic techniques Swati Malviya, Krishna Kant Nayak, Manish Saxena[9], present a current state of art literature on audio steganographic techniques and how it's performed by different methods.

IV. PROPOSED METHODOLOGY

In the proposed method the carrier file is taken as audio format and the secret message may be a text or audio format files. Our system provides a very friendly User Interface where the user had to specify just the required inputs (audio, text).After embedding or extracting the user can save /open or just discord the output of that particular operation according to their wish. In view of providing security by preventing unauthorized person to access the software password facility is provided to the user in order to work with the software. To provide more security by avoiding an intruder to extract the embedded data a security key is used while embedding and extracting message.

There are two methods in Audio steganography

1) Encoding

2) Decoding

Encoding is a process of hiding the message in the audio. Decoding is a process of retrieving the message from the audio. Proposed Message Hiding System.

One encode/decode library would be used to implement Algorithm is used to encode the message into audio. It performs bit level manipulation to encode the message. The following steps are:

A. Preprocessing

a) Input secret message and cover signal:

Proposed method starts by inputting the secret message which is to be embedding into 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 going 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. Check whether the size of the audio file is greater or less than the text file. If the size of the audio file is less than the size of the selected text file then print the error message, otherwise it is possible to embed the text file into selected audio file

b) Encryption of Message:

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.

B. Cover Signal Segmentation:

Let the input cover signal consist of R samples, this signal is segmented into two categories:

1. Used segment

2. Unused segment.

The size of used segment is depending on the size of message bits. The Used segments are consisting of Z samples where the size of Z is power of 2. they are used for embed the message N cover signal, the rest samples is called unused

samples, Next the useful part is partitioned into segments of size same as size of message bits that is N segments; each segment has length of Z samples .

C. Segment Decomposition and Secret Message Embedding Stage:

Each segment of the input audio cover signal is decomposed using L level of DCT to obtain 2^L signals, each one of the produced signal has length of Z/2^L samples. one represents the DC signal and the others represent AC signals.

Secret message embedding stage is based on comparison of two samples in a segment .the detail working is given below:

if the secret message bit that is to be embedded is 0 then compare the Pth and Qth samples and if Pth sample is less than Qth sample ,then interchange both the samples. if it is not so then there is no need to interchange the samples

If the secret message bit that is to be embedded is 1 and if Pth sample is greater than Qth sample, then swaps both the samples otherwise there is no need to interchange the samples.

Incase if both the samples are same means Pth and Qth and embed data bit is 0 then subtract the k from the qth sample and add k in pth sample and if embed data bit is 1 then k subtract from pth sample and add k in qth sample.

The pseudo code for above data hiding processing is given below:

```
if (Message(i)==0)
    if(Segment(i,p)<Segment(i,q))
        swap(Segment(i,p),Segment(i,q));
    elseif(Segment(i,p)==Segment(i,q))
        Segment(i,p)=Segment(i,p)+k/2;
        Segment(imp)=Segment(imp)-k/2;
    end
elseif (Message(i)==1)
    if(Segment(i,p)>Segment(imp))
        swap(Segment(i,p),Segment(imp));
    elseif(Segment(i,p)==Segment(imp))
        Segment(i,p)=Segment(i,p)-k/2;
        Segment(imp)=Segment(imp)+k/2;
    end
```

D. Stego-Signal Reconstruction Stage

In this stage all the modified segments, are converted back from frequency domain to spatial domain. The IDCT is used to reconstruct the segments of stego- signal based on modified AC samples and unmodified DC samples. The reconstructed segments will fed to segment collecting step to reconstruct the final stegonagraphy algorithm output.

E. Message Recovery Algorithm

- Input Audio stego signal:

In the message recovery algorithm, first we select the Audio stego signal from which data is to be extracted.

- Stego Signal Segmentation:

Again, the stego signal is segmented into two categories:

1. Used segment
2. Unused segment.

The size of Used segment is known to receiver with the help of size of message bit .it is calculate by multiplying the size of message bits with 2^L where L is the decomposition level. Next the used part is segmented again into N segments; each segment has length of Z samples.

E. Stego Segment Decomposition and Secret Message Recovery Stage:

Again, Each segment of the Stego audio signal is decomposed using L level of DCT to obtain 2^L signals, each one of the produced signal has length of Z/2^L samples. One represents the DC signal and the others represent AC signals.Secret message recovery stage is very simple and based on comparison of two samples in a segment. If the pth sample is greater than Qth sample it means that data is 0 otherwise the Message bit is 1

```
If (Segment(i,p)>Segment(imp))
    Message(i)=0;
elseif(Segment(i,p)<Segment(imp))
    Message(i)=1;
else
    error("there is problem in Stegno Signal");
end
```

F. Proposed Block Diagram:

Figure 4.1 presents the block diagram of proposed message hiding system .the input of this message hiding system are audio file as cover signal and text message which is to be embedded into cover signal. The output of proposed system is stego audio cover file in which message is hidden.

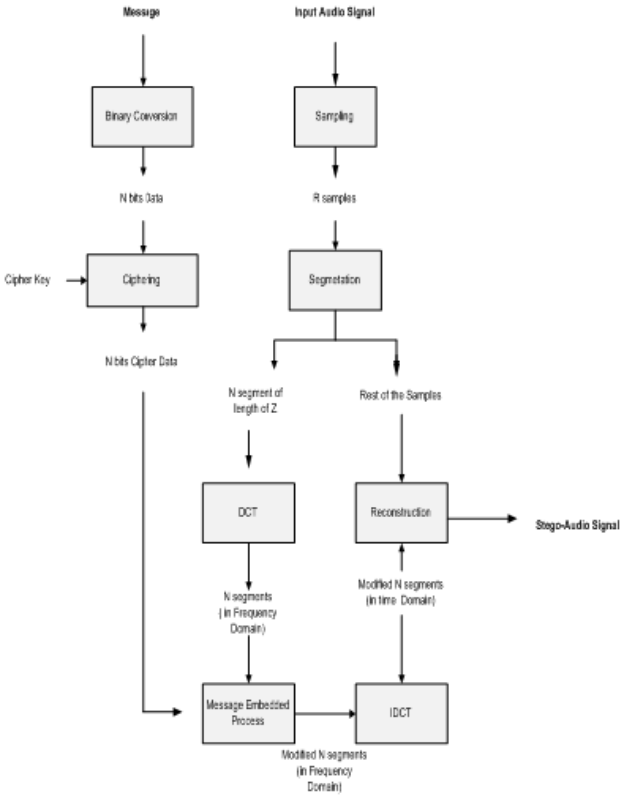

Fig.4.1.the General Structure of the Proposed Hiding Scheme

V. Simulation/Experimental Results

Basically measurement is categories into perceptual and non-perceptual groups, and furthermore, the non-perceptual group into time-domain and frequency-domain measures. Here we used the time domain measurement for quality purpose. The original signal (the cover document) is denoted while the distorted signal (the stego-document) as . In some cases the distortion is calculated from the overall data. However most of the case, the distortion is calculated for small segments and by averaging these, the overall measure is obtained.

Time-Domain Measures (SNR, SNRseg) compare the two waveforms in the time domain.

- Segmental Signal-to-Noise Ratio (SNRseg):

SNRseg is defined as the average of the SNR values over short segments:

$$SNRseg = \frac{10}{M}\sum_{m=0}^{M-1}\log_{10}\sum_{i=Nm}^{Nm+N-1}\left(\frac{x^2(i)}{(x(i)-y(i))^2}\right)$$

Where (i) is the original audio signal, y (i) is the distorted audio signal. The length of segments is typically 15 to 20 ms for speech. The SNRseg is applied for frames which have energy above a specified threshold in order to avoid silence regions.

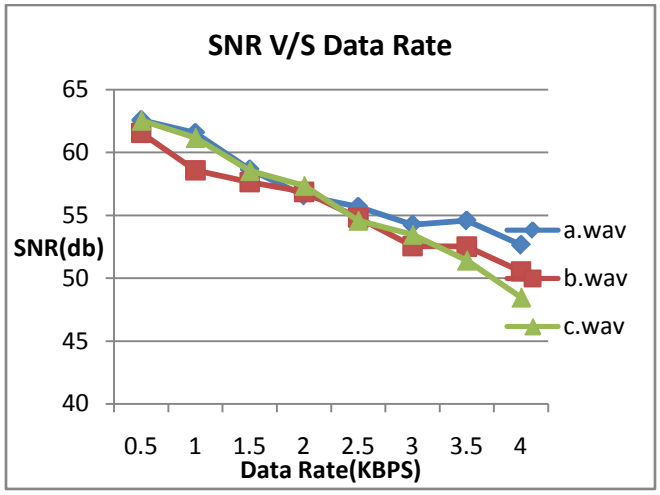

Fig.5.2.the Relationship between SNR and Embedding Capacity for Different Cover Signals and different Data Type

Signal-to-Noise Ratio (SNR), is a special case of SNRseg, when M=1 and one segment encompasses the whole record. The SNR is very sensitive to the time alignment of the original and distorted audio signal. The SNR is measured as

$$SNR = 10\log_{10}\frac{\sum_{i=1}^{N}x^2(i)}{\sum_{i=1}^{N}(x(i)-y(i))^2}$$

Here N represents the number of samples in both signals. Experimental result

VI. Conclusion

In this way we have presented a high capacity and high stego-signal quality audio steganography scheme based on samples comparison in DCT domain where two samples of a segment are compared and based on comparison bits are embedded. The strength of our algorithm is depend on the segment size and their strength are enabled the algorithm to achieve very high embedding capacity for different data type that can reach up to 25 % from the input audio file size with lest of 50 dB SNR for the output stego signal.

The proposed scheme was tested for different hiding capacity and the results showed that it has excellent output quality. From the tests we find the proposed algorithm support high

capacity rate reach up to 4 kb/sec and that is form above 25% from the size of the input audio cover file at SNR above 50 dB for the output signal.

VII. FUTURE SCOPES

Our ability to discover hidden information during our investigations is vital, especially as new and innovative methods continue to evolve.

During the past decade, data hiding technologies have advanced from limited use to ubiquitous deployment. With the rapid advancement of smart mobile devices, the need to protect valuable proprietary information has generated a plethora of new methods and technologies for both good and evil. Most dangerous among these are those that employ hiding methods along with cryptography, thus providing a way to both conceal the existence of hidden information while strongly protecting the information even if the channel is discovered.

These new techniques provide hybrid solutions that combine the best of cryptography with the best of steganography. The interest, innovation, and advancement of these threats continue to go unchecked for the most part.

REFERENCES

[1] Zaidoon Kh., AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi," Overview: Main Fundamentals for Steganography ", journal of computing, volume 2, issue 3, March 2010.
[2] http://www.techopedia.com/definition/14738/data-hiding.
[3] W. Bender,D. Gruhl, N. Morimoto,"Techniques for data hiding",IBM SYSTEMS JOURNAL, VOL 35, NOS 3&4, 1996.
[4] H. B. Kekre, A. Athawale, B. S. Rao and U. Athawale," Increasing the Capacity of the Cover Audio Signal Using Multiple LSBs for Information Hiding", Emerging Trends in Engineering and Technology (ICETET), p.p.196-201, 19-21 Nov. 2010
[5] Sridevi, R. Damodaram, A. Narasimham, S,"Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key with Enhanced Security",Journal of Theoretical and Applied Information Technology ,pp. 768 – 771,Vol. 5, No. 6, , June 2009
[6] Jayaram P, Ranganatha H R, Anupama H S," Information Hiding Using Audio Steganography".
[7] Bairagi, A.K, Mondal, S," An Approach to Improve the Robustness of Substitution Techniques of Audio Steganography",Informatics, Electronics & Vision (ICIEV), International Conference on May 2012.
[8] KaliappanGopalan and Stanley Wenndt," Audio Steganography for Covert Data Transmission by Imperceptible Tone Insertion ",
[9] International Journal of Electronics Communication and Computer Technology," Audio Steganography in a Nutshell", Vol.2 Issue 5 (September 2012) ISSN:2249-7838.