Performance Analysis & Evaluation at Wav Audio File in Steganography Using Tone Insertion Technique

Author

Neha Trivedi[1], Amit Singh[2]

[1]*(Research Scholar/Department of CSE/AKTU, Lucknow)*
[2]*(Asst. Professor/Department of CSE/SR Group of Institutions, Lucknow)*

Abstract : *Wave steganography is focused in hiding secret information in an innocent cover 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. Existing audio steganography software can embed messages in WAV, AU, and even MP3 sound files.*
With the this technique we have calculate the result of frequency fluctuation at the time of text embedding. Basically we user frequency modulation for decrease sound movement after embedding text message in wave file

Key Words :

1. Introduction to Data Hiding In Wave

The rising possibilities of modem communications need 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 information hiding. Information hiding is the process of hiding the details of an object or function. The hiding of these details results in an abstraction, which reduces the external complexity and makes the object or function easier to use.
Steganography is an art and a science of communicating in a way, which hides the existence of the communication. It is also called as “covered writing”, because it uses a “cover” of a message for sending any important secret message . Steganography serves as a means for private, secure and sometimes malicious communication. Steganography is the art to hide the very presence of communication by embedding the secret message into the innocuous looking cover media objects, such as images using the human's visual, aural redundance or media objects' statistical redundance. Steganography is a powerful tool which increases security in data transferring and archiving. In the steganographic scenario, the secret data is first concealed within another object which is called “cover object”, to form “stego object” and then this new object can be transmitted or saved. Using different techniques, we can send secret data in the form of an image, a music file or even a video file by embedding it into the carrier, forming a stego signal. At the receiver’s end, the secret data can be recovered from the stego signal using different algorithms.

There are basically two to audio steganography

a) Embedding
b) Extracting

a) Algorithm For Embedding Text Content Into Audio File At The Sender Side

1. Select a Wave file as input audio.
2. Select an output audio file.
3. Select data/message to embedded.
4. Enter Key file to message.
5. Verify process of embedding
6. Embedding data in wave file
7. Exit

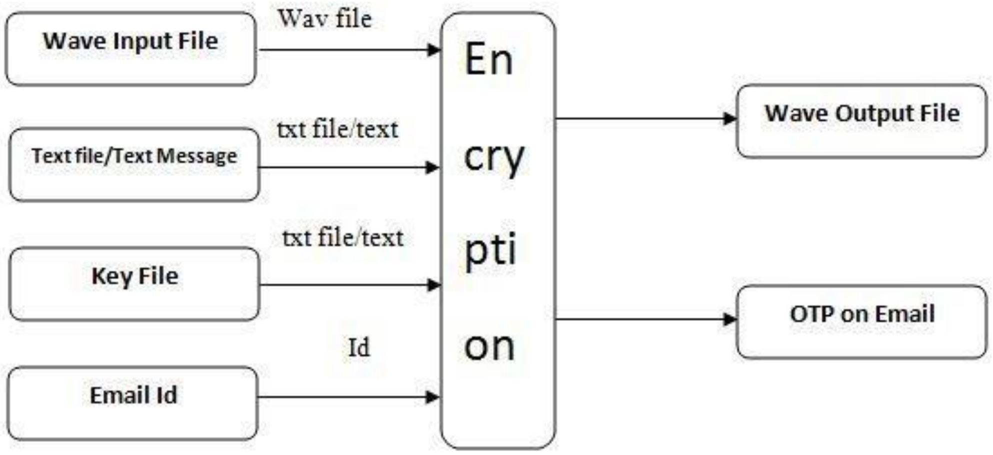

Fig:1.1

b) Algorithm for Extracting the Embedded text from Audio file at the Receiver Side:

1. Select the Embedded Audio file for extracting the secret message.
2. Enter new text file to find message
3. Enter key file to extract message.
4. Verify option for file extracting.
5. Extracting data from audio encrypted file.
6. exit

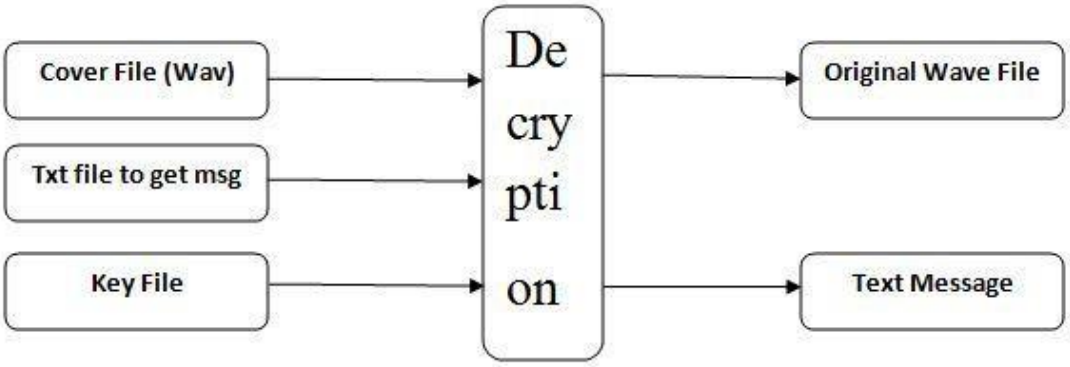

Fig:1.2

2. Technique

Tone insertion techniques rely on the inaudibility of lower power tones in the presence of significantly higher ones. Embedding data by inserting inaudible tones in cover audio signals is presented. To embed one bit in an audio frame, this research suggests a pair of tones which is generated at two chosen frequencies f0 and f1. The power level of the two masked frequencies (pf 0 and pf 1) is set to a known ratio of the general power of each audio frame p i where: i=1 to n and n is the frame number as shown in Figure. By inserting tones at known frequencies and at low power level, concealed embedding and correct data extraction are achieved. To detect the tones and thus the hidden information from the stego-audio frames, the power p i for each frame is computed as well as the power pf 0 and pf 1 for the chosen frequencies f0 and f1.

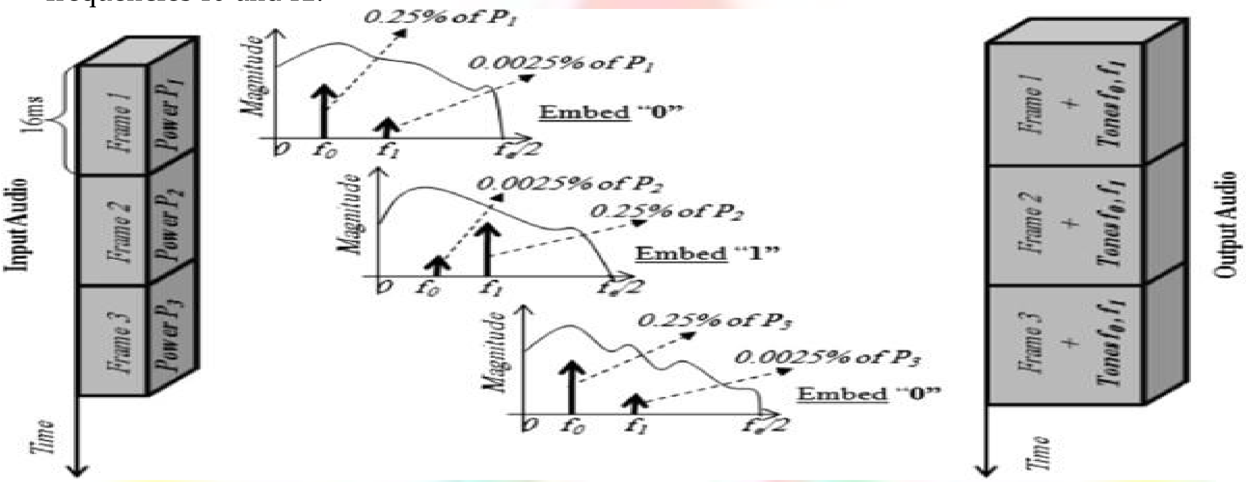

Fig 2: Tone Insertion Technique

3. Result

There are several method for audio steganography to perform research work here we use tone insertion for audio steganography which shows comparability of different technique use for this in given both table of analysis.

Method	Tone insertion	Phase coding	Amplitude coding	Cepstral Domain	SS	APFs	DWT
imperceptibility	✓ [31]	✓ [32, 33]	✓ [34]	✓ [36]	✓ [22,23]	✓ [37, 38]	✓ [24, 30]
Amplification	-	✓ [33]	-	✓ [26]	-	-	-
Noise addition	-	-	-	✓ [36]	✓ [22]	✓ [37, 38]	-
Low pass filtering	✓ [31]	-	-	✓ [36]	-	✓ [37, 38]	-
Requantization	-	✓ [32, 33]	-	-	-	✓ [37, 38]	-
Re-sampling	-	-	-	-	-	✓ [37, 38]	-
Compression	-	✓ [32]	-	✓ [26, 36]	-	✓ [37, 38]	-

Table – 1 : Comparability of Different Technique

Hiding Domain	Methods	Embedding Techniques	Advantages	Drawbacks	Hiding rate
Transform Domain	Magnitude spectrum	Use frequency bands to hide data	Longer message to hide and less likely to be affected by errors during transmission	Low robustness to simple audio manipulations	20Kbps
	Tone insertion	insertion of inaudible tones at selected frequencies	Imperceptibility and concealment of embedded data	Lack of transparency and security	250bps
	Phase spectrum	Modulate the phase of the cover signal	Robust against signal processing manipulation and data retrieval needs the original signal	Low capacity	333bps
	Spread spectrum	Spread the data over all signal frequencies	Provide better robustness	Vulnerable to time scale modification	20 bps
	Cepstral domain	Altering the cepstral coefficients for embedding data	Robust against signal processing operations	Perceptible signal distortions and low robustness	54bps
	Wavelet	Altering wavelet coefficients for embedding data	Provide high embedding capacity	lossy data retrieval	70kbps

4. Conclusion

This technique is an example of moderately pure Steganography because it send public key only to receive email at the time of encryption of wave file .hiding of file/data in audio file is more secure than image or behind the text file.

5. Future Work

This technique remove distortion of wave flow by frequency adjustment .we are hiding our text message in wave file .next improvement of research is hiding text file in wave file up to size of wave file with random password generator. With this technique we can discover pure steganography.

References

[1]. Wu M & Liu B (2003) Multimedia Data Hiding. Springer Verlag, New York, NY.

[2]. Kundur D (2001) Watermarking with diversity: Insights and implications. IEEE Multimedia 8(4): p 46–52.

[3]. Vijay kumar Implementation of Audio Steganogarphy Using C# ijtmh volume1,issue-1(2015).

[4]. Anderson (ed.) RJ: Information hiding: 1st international workshop, volume 1174 of Lecture Notes in Computer Science, Isaac Newton Institute. Springer-Verlag, Berlin, Germany; 1996.View Article

[5]. Bender W, Gruhl D, Morimoto N, Lu A: Techniques for Data Hiding. IBM Syst. J 1996, 35(3 and 4):313-336.View Article

[6]. Zwicker E, Fastl H: Psychoacoustics. Springer Verlag, Berlin; 1990.