ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Audio Steganography Using Least Significant Bit

Sudha Lakshmi N

M.E., Dept. of CSE, Sri Krishna College of Engineering and Technology, Coimbatore, India

ABSTRACT: Steganography is the art of hiding messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. Audio signals are more challenging compared to the images or videos. Audio Steganography is the technology which uses to hide information in audio files. This project describes a high-capacity steganography algorithm for embedding data in the inactive frames of low bit rate audio streams encoded which is used extensively in Voice over Internet Protocol (VoIP). This study reveals that, contrary to existing thought, the inactive frames of VoIP streams are more suitable for data embedding than the active frames of the streams that is steganography in the inactive audio frames attains a larger data embedding capacity than that in the active audio frames under the same imperceptibility. A new algorithm for steganography is proposed in different parameters of the inactive frames. Consumption of time to encode and decode is reduced when compared to existing system.

I INTRODUCTION

DOMAIN INFORMATION

Streaming media, such as Voice over Internet Protocol (VoIP) streams, are broadcast live over the Internet and delivered to end users. Security remains one of the main challenges with this new technology. With the upsurge of VoIP applications available for use in recent years, VoIP stream s become one of the most interesting cover objects for modern steganography. Digital steganography in low bit rate audio streams is commonly regarded as a challenging topic in the field of data hiding.

Steganography and its Applications:

Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data. Steganography has various useful applications. However, like any other science it can be used for ill intentions. It has been propelled to the forefront of current security techniques by the remarkable growth in computational power, the increase in security awareness by, e.g., individuals, groups, agencies, government and through intellectual pursuit.

Types of Steganography

Text-based Steganography: The text-based Steganography is limited in capacity and hence it use visible text to hide the message. In addition, there is no measurement can be used in text-based steganography to assure the confidentiality of the secure message.

Image-based Steganography: The Image-based Steganography is tried to improve the capacity where in literature more than 50% of the original image size is used to hide the secure message. Since, there is some limitation on how much information can be hidden into image.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Audio-based steganography: In audio-based Steganography secret messages are embedded in digital sound. The secret message is embedded by slightly altering the binary sequence of a sound file.

Video-based Steganography: The video-based Steganography has been found to overcome the capacity problem. Video actually is the sequence of picture, where each picture is consisted by an array of pixels. Use of video-based Steganography has advantage as the discloser will facing a problem to attack the image since the sequence of the image within the video is unknown for the attacker, so the attacker need to check all the images within the video which make it more difficult to attack the secure message.

Steganography in Audio

Data hiding in audio signals is especially challenging, because the Human Auditory System (HAS) operates over a wide dynamic range. The HAS perceives over a range of power greater than one billion to one and a range of frequencies greater than thousand to one. Sensitivity to additive random noise is also acute.

The perturbations in a sound file can be detected as low as one part in ten million which is 80dB below ambient level. However there are some 'holes' available. While the HAS has a large dynamic range, it has a fairly small differential range. As a result, loud sounds tend to mask out the quieter sounds.

Additionally, the HAS is unable to perceive absolute phase, only relative phase. Finally there are some environmental distortions so common as to be ignored by the listener in most cases.To exploit these traits to the advantage in the methods discussed further while being careful to bear in mind the extreme sensitivities of the HAS.

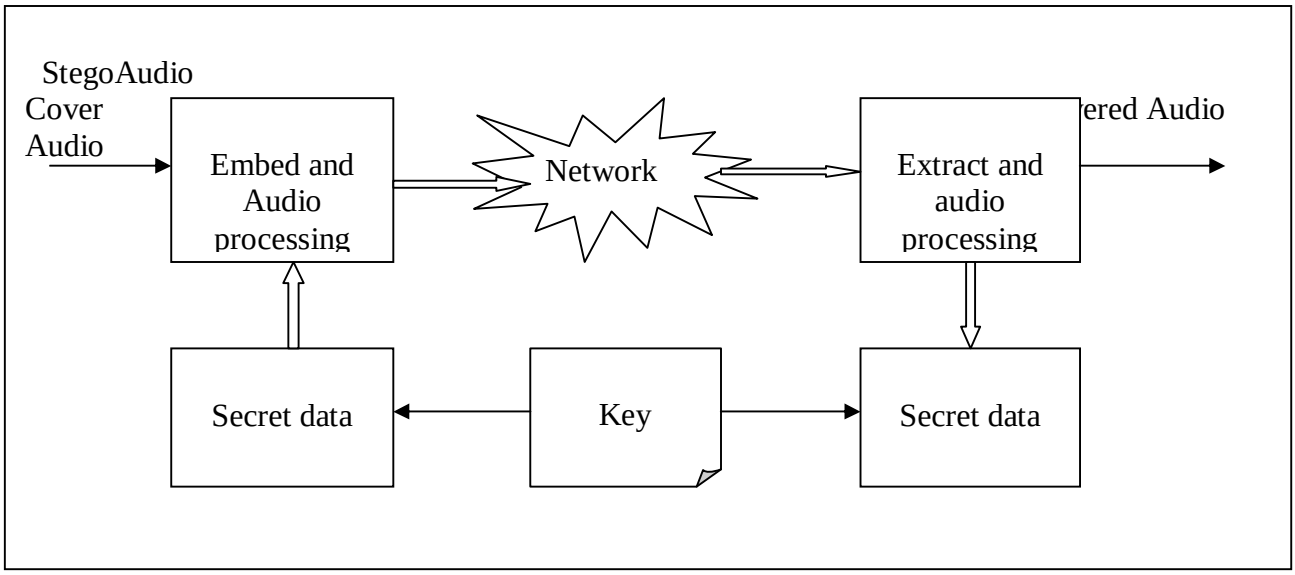

Fig no: 1.1 Block diagram for audio steganography

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

II SYSTEM ANALYSIS

EXISITING SYSTEM

Streaming media, such as Voice over Internet Protocol (VoIP) streams, are broadcast live over the Internet and delivered to end-users. Security remains one of the main challenges with this new technology. With the upsurge of VoIP applications available for use in recent years, VoIP streams become one of the most interesting cover objects for modern steganography. Digital steganography in low bit rate audio streams is commonly regarded as a challenging topic in the field of data hiding.

There have been several steganography methods of embedding data in audio streams. For example, Wu et al. suggested a G.711-based adaptive speech information hiding approach. Aoki [2] proposed a technique of lossless steganography in G.711 encoded speeches. Ma et al. framed a steganography method of embedding data in G.721 encoded speeches. All these methods adopt high bit rate audio streams encoded by the waveform codec as cover objects, in which plenty of least significant bits exist.

THE DISADVANTAGES OF EXISTING SYSTEM

- Non-Provision of encryption key
- Length of the message is limited to 500.
- Absence of frequency chart to show the variations.
- Lack in good user interface.
- Consume much time to encode and decode.
- Non-Provision of sending the file to the destination.
- User needs to understand better to know the operations.

PROPOSED SYSTEM

VoIP are usually transmitted over low bit rate audio streams encoded by the source codec like ITU G.723.1 codec to save on network bandwidth. Low bit rate audio streams are less likely to be used as cover objects for steganography since they have fewer least significant bits than high bit rate audio streams. Little effort has been made to develop algorithms for embedding data in low bit rate audio streams. Chang et al. [4] embedded information in G.729 and MELP audio streams. Huang et al. [5] proposed a steganography algorithm for embedding information in low bit rate audio streams. But these steganography algorithms have constrains on the data embedding capacity; that is, their data embedding rates are too low to have practical applications. Thus the main focus of this study was to work out how to increase the data embedding capacity of steganography in low bit rate audio streams. Discussing the possibility of embedding data in the inactive frames of low bit rate audio streams. The imperceptibility of the steganography algorithm for embedding data in the inactive audio frames is analyzed.

THE ADVANTAGES OF PROPOSED SYSTEM

- Provision of encryption key and performs simple encryption algorithm.
- The encryption key is modified by a strong algorithm to get a new key, which is used to encrypt the message. So even if the key is known for an intruder, he cannot break the code with that key.
- Presence of frequency chart to show the variations that helps the user to determine.
- Consumption of time to encode and decode is reduced.
- Provision of sending the file to the destination is given so that after encoding the user can send the file by giving destination IP address.

III . SYSTEM IMPLEMENTAION

System Architecture and its Description

The fig2.1 shows the architecture of the project which consist of embedding process and extraction process. Embedding process is done by inserting secret data into the audio file with the secret key. The Stego audio file is recovered

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

in the next process called extraction process. Here the secret data is recovered from the stego audio file with the help of secret key. These two processes will be explained briefly in next phase respectively.

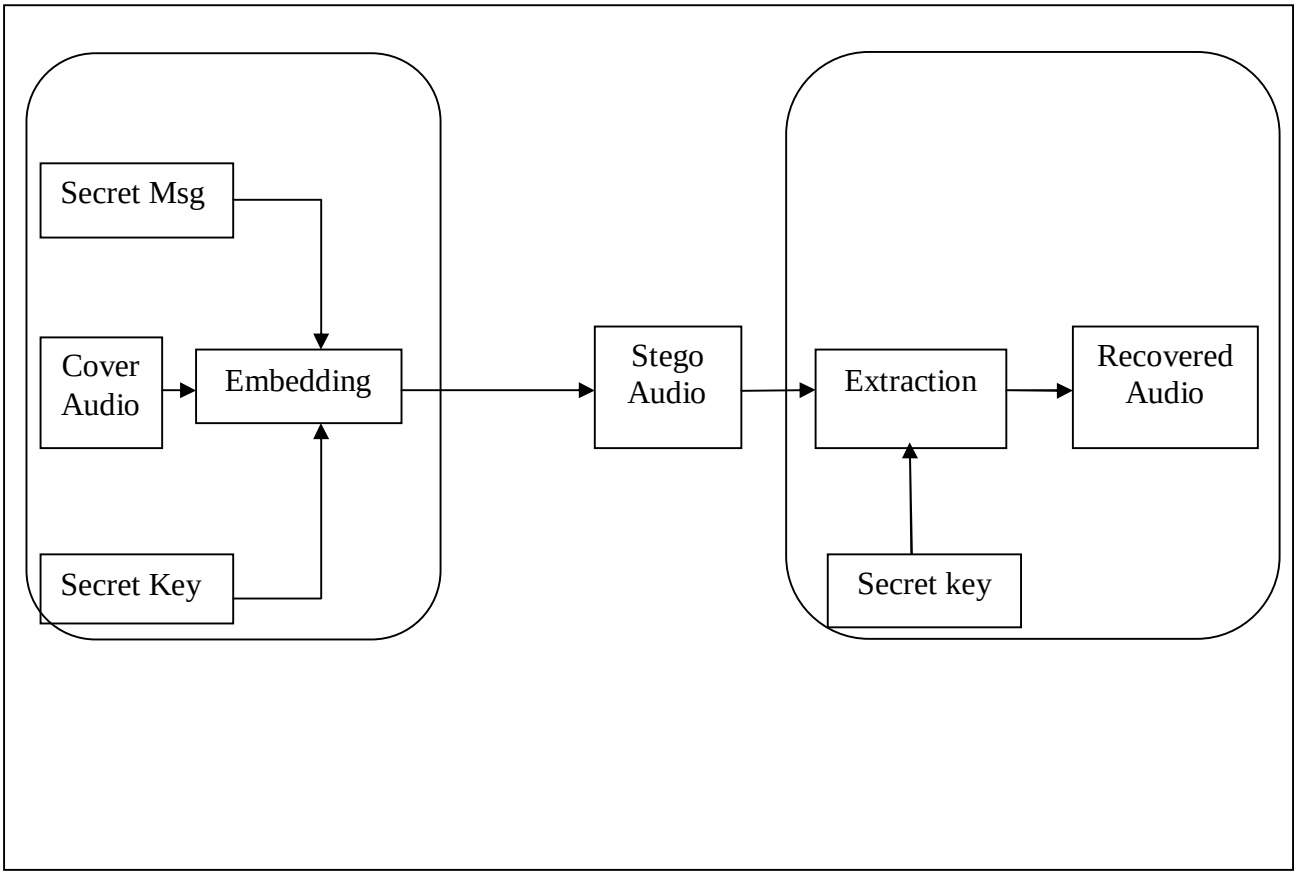

Fig: 2.1 architecture of the project

IV . CONCLUSION

A high-capacity steganography algorithm for inactive frames of low bit rate audio streams. The data embedding rate of our proposed algorithm was much higher than those of the other algorithms. This is because the proposed steganography algorithm made good use of the redundancy in the inactive frames of low bit rate audio streams.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

V . FUTURE WORK

The embedding process has been done in this phase and the extraction process of a stego audio file will be done as a future work. In this phase WAV file has been chosen as a cover file, later the other audio file formats such as Mp3, Real Audio, WMA and MIDI may also use as a cover file.

REFERENCES

[1] Z.Wu andW. Yang, "G.711-based adaptive speech information hiding approach," Lecture Notes Comput. Sci., vol. 4113, pp. 1139–1144,2006.
[2] N. Aoki, "A technique of lossless steganography for G.711 telephony speech," in Proc. 2008 4th Int. Conf. Intelligent Inf. Hiding Multimedia Signal Process. (IIH-MSP), Harbin, Aug. 2008, pp. 608–611.
[3] L. Ma, Z. Wu, and W. Yang, "Approach to hide secret speech information in G.721 scheme," Lecture Notes Comput. Sci., vol. 4681, pp. 1315–1324, 2007.
[4] P. Chang and H. Yu, "Dither-like data hiding in multistage vector quantization of MELP and G.729 speech coding," in Proc. Conf. Rec. 36th Asilomar Conf. Signals, Syst. Comput., Nov. 2002, vol. 2, pp.1199–1203.
[5] B. Xiao, Y. F. Huang, and S. Tang, "An approach to information hiding in low bit rate speech stream," in Proc. IEEE GLOBECOM 2008, Dec. 2008, pp. 371–375, IEEE Press.