A Novel High Capacity Approach for Reversible Audio Steganography

Hariom Dudhwal[1], Prof. Pankaj Kawadkar[2]

[1]Mtech Scholar, [2]Research Guide

Department of CSE, MIT, Bhopal

Abstract - The fast spread in digital information data utilization in numerous genuine applications have encouraged new and successful approaches to guarantee their security. Efficient secrecy can be achieved, at least in part, by implementing steganograhy techniques. The objective of steganographic frameworks is to acquire secure and robust approach to disguise high rate of secret information. This work mainly focus around digital audio steganography, which has risen as a promising source of information hiding over novel information and telecommunication technologies , for example, audio conferencing, secured voice-over-IP, and so forth. The huge number of steganographic criteria has prompted an awesome assorted variety in these framework design procedures. In this examination work, a novel high capacity approach for reversible audio steganography to enhance the performance of previous digital audio steganographic techniques and the performance of proposed approach is evaluate based on robustness, security and hiding capacity indicators. It is examined by simulation in MATLAB simulation environment that proposed technique outperforms against previous base work in terms of security and capacity.

Keywords - Audio, Reversible, Phase Encoding, Secret Text,

I. INTRODUCTION

The word steganography is derived from the Greek words stegos meaning cover and grafia meaning writing defining it as covered writing. In image steganography the information is hidden exclusively in images. Steganography is the art and science of secret communication .It is the practice of encoding/embedding secret information in a manner such that the existence of the information is invisible. The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message it is referred to as stego-medium. A stego-key is used for hiding/encoding process to restrict detection or extraction of the embedded data.

The majority of todays steganographic systems uses multimedia objects like im- age, audio, video etc as cover media because people often transmit digital pictures over email and other Internet communication. Modern steganography uses the opportunity of hiding information into digital multimedia files and also at the net- work packet level.

Text steganography hiding information in text file is the most common method of steganography. The method was to hide a secret message into a text message. After coming of Internet and different type of digital file formats it has decreased in importance. Text stenography using digital files is not used very often because the text files have a very small amount of excess data.

Image steganography Images are used as the popular cover medium for steganography. A message is embedded in a digital image using an embedding algorithm, using the secret key. The resulting stego-image is send to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego- image unauthenticated persons can only notice the transmission of an image but can't see the existence of the hidden message.

Audio steganography Audio steganography is concerned with embedding information in an innocuous cover speech in a secure and robust manner. Communication and transmission security and r obustness are essential for transmitting vital information to intended sources while denying access to unauthorized persons. An audible, sound can be inaudible in the presence of another louder audible sound .This property allows to select the channel in which to hide information. Existing audio steganography software can embed messages in WAV and MP3 sound files.

Watermarking and fingerprinting related to steganography are basically used for intellectual property protection. A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. The embedded information in a watermarked object is a signature refers the ownership of the data in order to ensure copyright protection. In fingerprinting, different and specific marks are embedded in the copies of the work that different customers are sup- posed to get. In this case, it becomes easy for the property owner to find out such customers who give themselves the right to violate their licensing agreement when they illegally transmit the property to other groups. Fig. 1.1 Shows the Scheme of Stegnography.

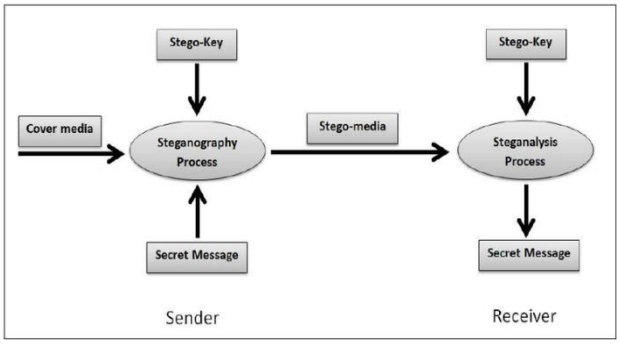

Fig. Basic Scheme of Stegnography.

II. AUDIO STEGANOGRAPHY

In Audio Steganography, the weakness of the Human Auditory System (HAS) is used to hide information in the audio. That is, while using digital images as cover files the difficulty of the human eye to distinguish colors is taken advantage of, while using digital audio one can count on the different sensitivity of the human ear when it comes to sounds of low and high intensity; usually, higher sounds are perceived better than lower ones and it is thus easier to hide data among low sounds without the human ear noticing the alteration. In audio steganography data is embedded in digital audio signal. Here secret message is embedded by small change in binary sequence of sound file. Audio file can be WAV, AU, or MP3 sound files. Audio steganography is more difficult than other methods of steganography.

Audio steganography is more challenging than others because audio files are larger than images or text and characteristics of human auditory system (HAS) like large power, dynamic range of hearing and large range of audible frequency.. HAS can perceive sound over a range of power greater than 109 to 1 and range of frequency greater than 103 to 1 [9]. Auditory perception is based on the critical band analysis in the inner ear where a frequency-to-location transformation takes place along the basilar membrane. The power spectra of the received sounds are not represented on a linear frequency scale but on limited frequency bands called critical bands. Range of sound frequencies which human ear can hear is 20 Hz to 20,000 kHz.

Many software implementations of these methods are available on the Web and are listed in the Links section. Some of the latter methods require previous knowledge of signal processing techniques, Fourier analysis, and other areas of high level mathematics. Figures and pseudo code are used in place of exact mathematical formulas in attempts to make the theory more accessible to readers possessing just a basic knowledge of steganography. Some commonly used methods of audio steganography are listed and discussed below in brief.

a. Least Significant Bit Coding

One of the earliest techniques studied in the information hiding of digital audio (as well as other media types) is LSB coding. In this technique LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message. It is the simplest way to embed information in a digital audio file. It allows large amount of data to be concealed within an audio file, or it allow high embedding rate without degrading quality of audio file.

b. Parity Coding

Instead of breaking a signal down into individual samples, the parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region.

c. Phase Coding:

Phase coding addresses the disadvantages of the noise-inducing methods of audio steganography. Phase coding relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is perceptible.

d. Spread Spectrum

In the context of audio steganography, the basic spread spectrum (SS) method attempts to spread secret information across the audio signal's frequency spectrum as much as possible. In SS we spread message in a signal using a code and this code is independent of actual signal. So at decode side we should know that code.

e. Echo Hiding

In echo hiding, information is embedded in a sound file by introducing an echo into the discrete signal. Like the spread spectrum method, it too provides advantages in that it allows for a high data transmission rate and provides superior robustness when compared to the noise inducing methods.

III. PROPOSED METHODOLOGY

MP3 or audio steganography is challenging because of its compressed form and the secret information should be retained under compression. Usually, the audio files are stored in a compressed form and the most commonly used form is MP3. When the audio frames are used for steganography appropriate frames should be selected to hide the secret information so that during compression the secret information is not lost. An MP3 file is made up of

multiple MP3 frames that consist of a header and a data block. Each frame contains 4-byte header, which consists of a sync word that identifies the beginning of a valid frame. To overcome the draw backs of previous audio steganography work based on LSB technique a new reversible technique has been reported in this work which is implemented and simulated in MATLAB simulation environment. Proposed technique uses reversible data hiding algorithm to recover the original data, from the embedded audio without any distortion or loss after the authentication.

a. Embedding Algorithm

In audio steganography technique the cover audio samples are segmented to get approximation and detailed coefficients. The secret message is encrypted dynamically using the statistics of the message. In the proposed method the length of the secret message is used for encryption. The encrypted secret message is hidden in the detailed coefficients of the cover. In the extraction phase, the stego audio samples are transformed using reversible approach. The encrypted secret message is retrieved from the detailed coefficients of the cover. Then it is decrypted using the same statistical information. Fig. 3.1 shows the block diagram of proposed algorithm and Fig. 3.2 shows the flow of process of embedding. The embedding procedure is as following-

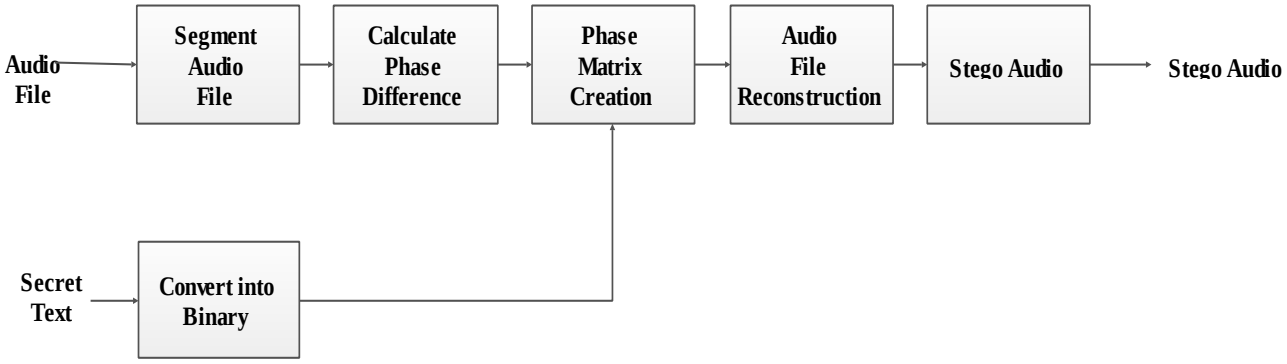

Fig.3.1 Block Diagram of Embedding Process.

Fist the audio file is processed in MATLAB environment the audio files is segmented and phase differences are calculated and based on phase difference calculation a matrix of phase is created and a secret information which is to be embed in audio are converted into its equivalent binary form and added in audio file. The audio file is reconstructed again an embedded stego audio is obtained as an output of embedded block.

The reversible steganography technique is used in the spatial domain technique. In this spatial domain technique it uses the modulo addition technique to embed the text into the cover audio. It is used for the authentication purpose. The aim of reversible watermarking is to embed the secret massage into the multi- media content audio in proposed work. The performance of reversible steganography is evaluated in the ability to detect the of modification. Basically the loss-less compression technique is used to embed.

b. Extraction Algorithm

At the receiver end the embed text file is extracted. If the extracted text and the stego text match then the audio is accepted at the receiver end. Fig. 3.3 shows the block representation of proposed extraction algorithm. The process flow of proposed work has given in Fig. 3.4.

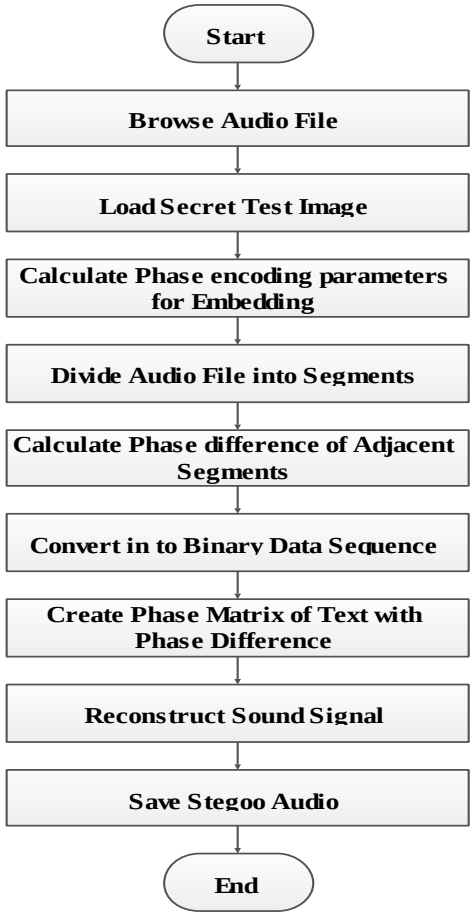

Fig.3.2 Flow Chart of Embedding Process.

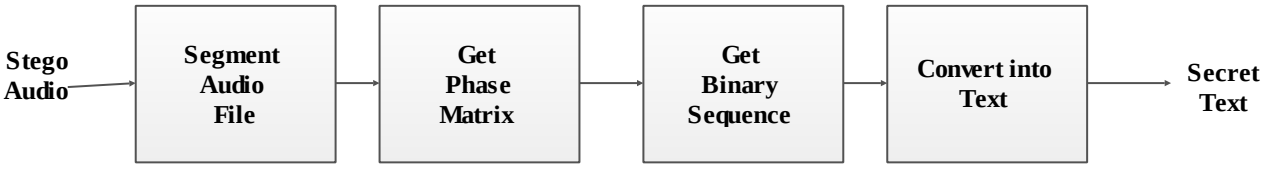

Fig.3.3 Block Diagram of Extraction Process.

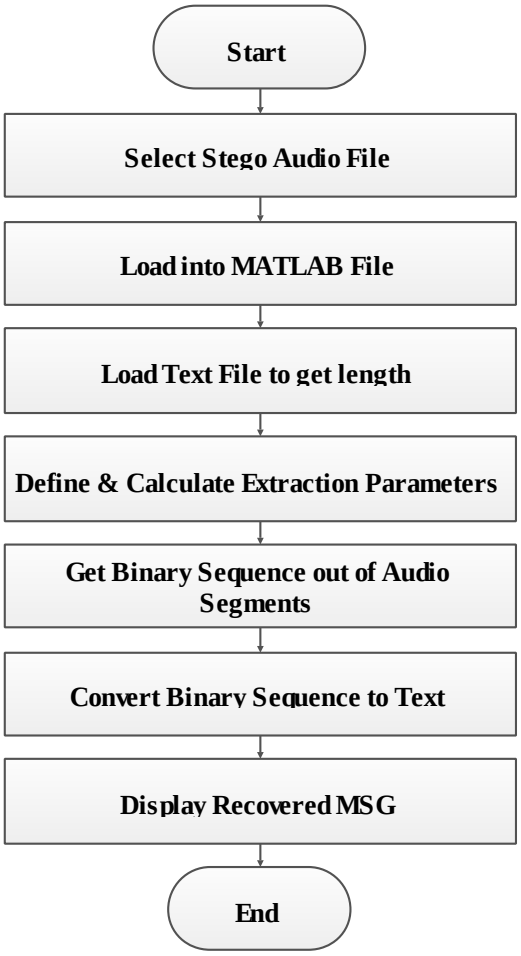

Fig.3.4 Flow Chart of Extraction Process.

At the extraction end the stego audio is processed to recover secret information embedded in stego audio file. Firstly the stego audio file segmented to get phase matrix and further phase matrix is processed to get its equivalent binary sequence. The binary sequence extracted from audio file is than converted in its actual text file. Hence fourth the secret information is obtained.

IV. SIMULATION OUTCOMES

The secret information is encrypted using reversible stegnography approach, which enhances the security and reduces the complexity of the technique. Results for different audio files with different amount of data hidden are presented. Quality of the stego audio is measured using PSNR.

The performance of this technique is evaluated with three kinds of payload capacity: large, medium, and small. The cover audio signal is a music file and the secret file is a text file, both having fixed bit samples. Keeping cover audio samples constant, the secret text samples size are varied to assess the performance of the technique and thus the variation of the security with capacity is studied. Enough number of samples is considered for cover audio, and the secret text samples are taken as half, same, and double that of the cover audio. The secret text file is compressed and indirectly encrypted by reversible algorithm. The entire process has completed in MATLAB simulation.

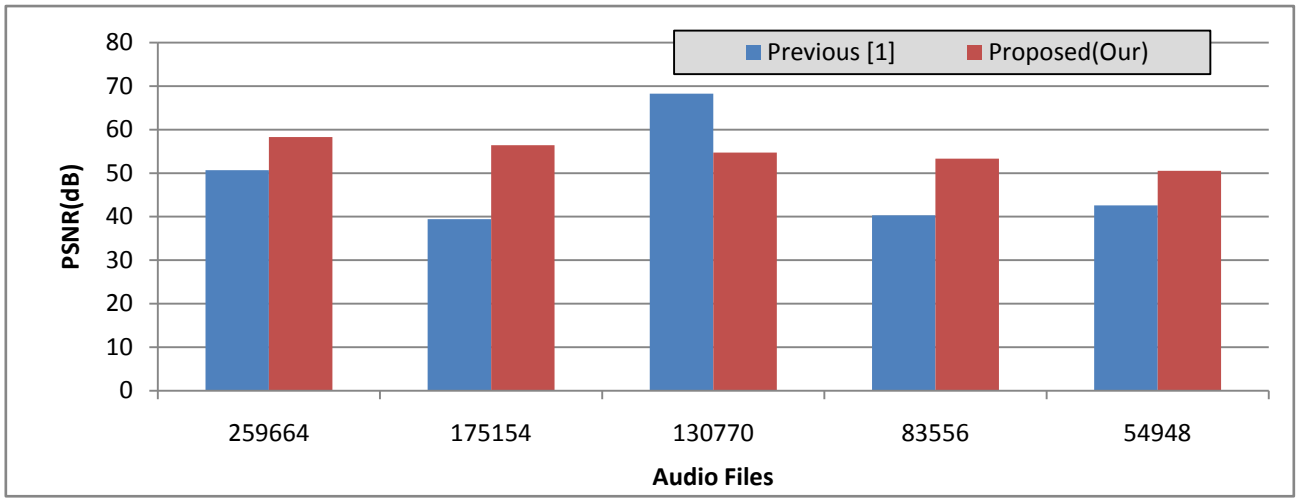

Fig.4.1 PSNR Comparison Chart.

The comparative analysis of proposed work with existing base work has given in Table 1 where previous work from base paper [1] has taken as reference and proposed work as extension of base work. The comparison has examined in terms of PSNR value in dB for various secret message size and audio file size.

For audio file size 259664, secret message of length 100 byte has previous PSNR 50.67 has extended in proposed work to 145 bite of secret text size for filed audio file size achieved PSNR 66.02dB. The above examination based on simulation has carried out for different audio samples such as 175154, 130770, 83556, 54948. The corresponding PSNR for all samples for fixed message 150 byte has achieved better performance against previous base work.

V. Table 1: Comparison of Performance between Previous[1] and Proposed Work(Our).

Audio File Size	***Previous [1]***		***Proposed(Our)***	
	Secret Message Size (bytes)	***PSNR (dB)***	***Secret Message Size (bytes)***	***PSNR(dB)***
259664	100	50.67	150	58.31
175154	100	39.43	150	56.44
130770	100	68.25	150	54.72
83556	100	40.31	150	53.35
54948	100	42.60	150	50.55

The graphical representation of comparative analysis of proposed work and previous base work has shown in Fig. 4.1 in terms of PSNR in dB. It can be concluded to analyze bar chart that proposed work has better performance against existing work.

VI. CONCLUSION AND FUTURE SCOPE

In proposed audio steganography, audio is the cover and the secret information is a text file implemented and simulated in MATLAB. The audio steganography techniques proposed in this examination uses audio as the cover. The audio steganography technique is used to hide text file in audio file. An image is hidden in an audio file using reversible audio steganography technique. A high capacity audio steganography technique is used to hide secret text file in audio, which uses an audio for cover and secret text to embed in it. In proposed techniques, the performance of the stego audio is evaluated using the metrics PSNR and compared with previous work.

In future proposed reversible stegnography technique can be extended for image as a secret file. This may address to the increasing of the embedding capacity. Another extension may be tamper localization enhanced by doing some special operation to the every bin of the histogram image.

REFERENCES

[1] R. Indrayani, H. A. Nugroho and R. Hidayat, "An evaluation of MP3 steganography based on modified LSB method," 2017 International Conference on Information Technology Systems and Innovation (ICITSI), Bandung, 2017, pp. 257-260.

[2] B. Datta, P. K. Pal and S. K. Bandyopadhyay, "Multi-bit Data Hiding in Randomly Chosen LSB Layers of an Audio," 2016 International Conference on Information Technology (ICIT), Bhubaneswar, 2016, pp. 283-287.

[3] M. T. Al-Bayati and M. M. Al-Jarrah, "DuoHide: A Secure System for Hiding Multimedia Files in Dual Cover Images," 2016 9th International Conference on Developments in eSystems Engineering (DeSE), Liverpool, 2016, pp. 138-142.

[4] V. Sharma and R. Thakur, "LSB modification based Audio Steganography using Trusted Third Party Key Indexing method," 2015 Third International Conference on Image Information Processing (ICIIP), Waknaghat, 2015, pp. 403-406.

[5] E. T. B. Abdelsatir, N. C. Debnath and H. Abushama, "A multilayered scheme for transparent audio data hiding," 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), Marrakech, 2015, pp. 1-6.

[6] A. Binny and M. Koilakuntla, "Hiding Secret Information Using LSB Based Audio Steganography," 2014 International Conference on Soft Computing and Machine Intelligence, New Delhi, 2014, pp. 56-59.

[7] A. K. Mandal, M. Kaosar, M. O. Islam and M. D. Hossain, "An approach for enhancing message security in audio steganography," Computer and Information Technology (ICCIT), 2013 16th International Conference on, Khulna, 2014, pp. 383-388.

[8] K. Srinivasan, V. Ramamurthi, and K. S. Chatha, "A technique for energy versus quality of service trade-off for MPEG-2 decoder," in IEEE Computer society Annual Symposium on VLSI, 2004, 2004, pp. 313-316.

[9] A. Delforouzi and M. Pooyan, "Adaptive and efficient audio datahiding method in temporal domain," in 7th International Conference on Information, Communications and Signal Processing (ICICS) 2009 2009, pp. 1-4.

[10] H. B. Kekre, A. Athawale, B. S. Rao, and U. Athawale, "Increasing the capacity of the cover audio signal by using multiple LSBs for information hiding," in 2010 3rd International Conference on Emerging Trends in Engineering and Technology (ICETET), 2010, pp. 196-201.

[11] R. Sridevi, A. Damodaram, and S. Narasimham, "Efficient Method Of Audio Steganography By Modified Lsb Algorithm And Strong Encryption Key With Enhanced

Security," Journal of Theoretical & Applied Information Technology, vol. 5, 2009.

[12] M. S. Atoum, M. Suleiman, A. Rababaa, S. Ibrahim, and A. Ahmed, "A Steganography Method Based on Hiding secrete data in MPEG/Audio Layer III," Journal of Computer Science, vol. 11, pp. 184-188, 2011.