# Audio Steganography Using Mod 4 Method (M4M)

Souvik Bhattacharyya, Arko Kundu, Kaushik Chakraborty and Gautam Sanyal

**Abstract**— Steganography is an emerging area which is used for secured data transmission over any public media. Considerable amount of work has been carried out by different researchers on steganography. In this work the authors propose a novel steganographic method for hiding information in an audio file. The proposed approach is developed based on M16M [10] approach on image steganography whih works on wav and mp3 format of audio files. The proposed approach works by selecting the embedding positions using some mathematical function and maps each two bit of the secret message in each of the selected positions in a specified manner. A pseudo random number generator is used here to locate the embedding positions of the message bits randomly. This solution is independent of the nature of the data to be hidden and produces a stego audio with minimum degradation.

**Index Terms**—Cover Audio, Mod 4 Method (M4M), Stego Audio.

## 1 INTRODUCTION

A significant interest for hiding and enciphering systems has appeared during the last decade, mainly due to tworeasons. Firstly, telecommunication and publishing industries have become interested in hiding copyright marks (watermarks) in digital media such as audio, video, documents etc., foreseeing the urgent need for intellectual property protection. Secondly, decisions by various governments to consider strong encryption algorithms out of law, have motivated people to study methods by which enciphered messages can be embedded in seemingly innocuous cover media [2].Furthermore the need for privacy and sufficient security in several applications such as e-banking, mobile telephony, medical data interchanging etc., is rapidly increasing.

To confront the content security problem cryptography and steganography were proposed. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret [5, 6]. Although steganography is an ancient subject, the modern formulation of it comes from the prisoner's problem proposed by Simmons [1].An assumption can be made based on this model is that if both the sender and receiver share some common secret information then the corresponding steganography protocol is known as then the secret key steganography where as pure steganography means that there is none prior information shared by sender and receiver. If the public key of the receiver is known to the sender, the steganographic protocol is called public key steganography [3, 4]. For a better understanding about the steganography technique the reader may see [5, 6]. Although all digital file formats can be used for steganography, but the image and audio files are more suitable because of their high degree of redundancy [6]. Fig. 1 below shows the different categories of file formats that can be used for steganography techniques.Some steganography model with high security features has been presented in [7,8] and [9].

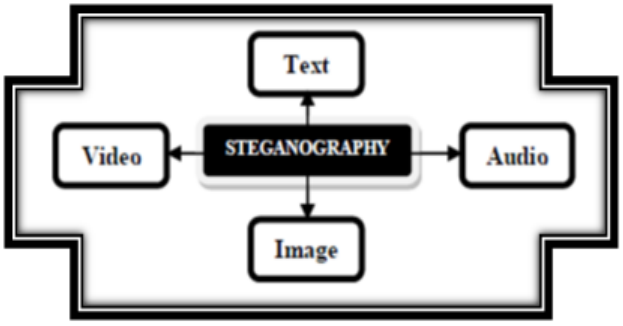


Figure 1: Types of Steganography

A block diagram of a generic audio steganographic system is given in Fig. 2. Amessage is embedded in a cover audio through an embedding algorithm, with the help of a secret key. The resulting stego audio may be transmitted over a channel to the receiver where it is processed by the extraction algorithm using the same key. During transmission the stego audio, it can be monitored by unauthenticated viewers who will only notice the transmission of an audio without discovering the existence of the hidden message. In this work a specific audio based steganographic method has been proposed. In this method instead of embedding the secret message into the cover audio a mapping technique has been incorporated to generate the stego audio. This method is capable of extracting

- *Souvik bhattacharyya is with the Department of CSE, University Institute of Technology, The University of Burdwan, Burdwan, India.*
- *Arko Kundu is with the Department of CSE, Bengal Engineering and ScienceUniversity, Shibpur, Kol.*
- *Kaushik Chakraborty is working as a Software Engineer at Tavant Technologies (HQ Santa Clara, California), Bangaluru, and India.*
- *Gautam Sanyal is with the Department of CSE, National Institute of Technology, Durgapur, India.*

the secret message without the presence of the cover audio.

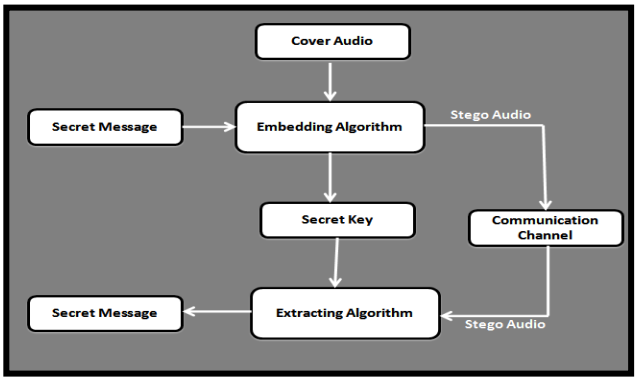


Figure 2: Generic form of Audio Steganography

This paper has been organized as following sections: Section II describes basics of audio steganography. Section III reviews the previous work on audio steganography.Section IV describes the proposed scheme along with data embedding and extraction methodology.Section V presents the solution methodology along with the system algorithm.Evaluation of the system done in Section VI and Section VII draws the conclusion.

## 2 AUDIO STEGANOGRAPHY

Like the document or images, the audio files may be modified for information hiding using the properties of the Human Auditory System (HAS). The HAS perceives the additive random noise and also the perturbations in an audio file can also be detected. But it has disadvantage also. Although the HAS have a large dynamic range, but it has a fairly small differential range also which results loud sounds tend to mask out quiet sounds.The process of converting analog audio into digital audio involves two sub processes: sampling and quantization. Sampling is the process in which the analogue values are only captured at regular time intervals.Quantization converts each input value into one of a discrete value. Popular sampling rates for audio include 8 kHz, 9.6 kHz, 10 kHz, 12 kHz, 16 kHz, 22.05 kHz and 44.1 kHz.

The most popular audio file formats are Windows Audio-Visual (WAV) and the Audio Interchange File Format (AIFF). There are two main areas of modification in an audio for data embedding. First, the storage environment, or digital representation of the signal that will be used, and second the transmission pathway the signal might travel [4, 11]. In order to conceal secret messages successfully, a variety of methods for embedding information in digital audio have been introduced. These methods range from rather simple algorithms that insert information in the form of signal noise to more powerful methods that exploit sophisticated signal processing techniques to hide information.

### 2.1 Digital Representation of Audio

There are two critical parameters involved in digital audio representations: sample quantization method and temporal sampling rate. The most popular format for representing samples of high-quality digital audio is a 16-bit linear quantization e.g. Windows Audio-Visual (WAV) and Audio Interchange File Format (AIFF) [4, 11].Another popular format for lower quality audio is the logarithmically scaled 8-bit m-law. These quantization methods introduce some signal distortion, somewhat more evident in the case of 8-bit m-law. Popular temporal sampling rates for audio include 8 kHz (kilohertz), 9.6 kHz, 10 kHz, 12 kHz, 16 kHz, 22.05 kHz, and 44.1 kHz. For most data-hiding techniques developed, usable data space increases at least linearly with increased sampling rate [11].

There are many different transmission environments that a signal might experience on its way from encoder to decoder.Four general classes for illustrative purposes shown in Figure 3 [11, 14]. The first is the digital end-to-end environment in Figure 3.1. This class puts the least constraints on data-hiding methods [11, 12]. The next considerations is when a signal is re-sample to a higher or lower sampling rate, but remains digital throughout as shown in Figure 3.2 This transform preserves the absolute magnitude and phase of most of the signal, but changes the temporal characteristics of the signal. The third case is when a signal is played into an analog state, transmitted on a reasonably clean analog line and re-sample shown in Figure 3.3. Absolute signal magnitude, sample quantization, and temporal sampling rate are not preserved. In general, phase will be preserved. The last case is when the signal is played into the air and re-sample with a microphone as shown in Figure 3.4. The signal will be subjected to possibly unknown nonlinear modifications resulting in phase changes, amplitude changes, drift of different frequency components, echoes, etc. Signal representation and transmission pathway must be considered when choosing a data-hiding method.

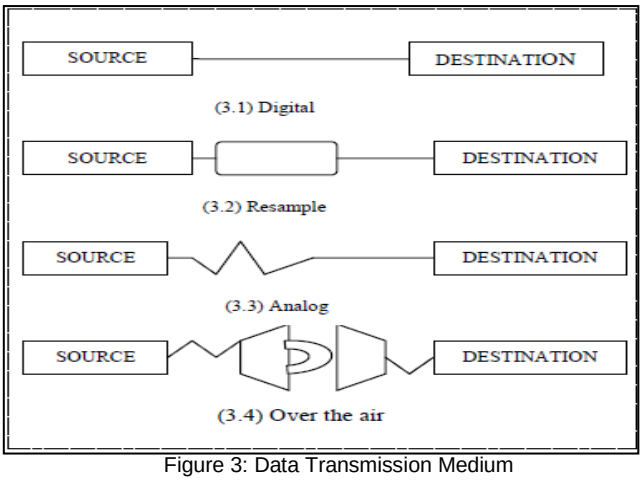


Figure 3: Data Transmission Medium

## 3 Review of Audio Data Hiding Techniques

This section presents some existing techniques of audio data hiding namely Least Significant Bit Encoding, Phase Coding Echo Hiding and Spread Spectrum techniques. There are two main areas of modification in an audio for data embedding. First, the storage environment, or digital representation of the signal that will be used, and second the transmission pathway the signal might travel [4, 11].

### 3.1 Least Significant Bit Encoding

Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded. In LSB coding, the ideal data transmission rate is 1 kbps per 1 kHz. In some implementations of LSB coding, however, the two least significant bits of a sample are replaced with two message bits. This increases the amount of data that can be encoded but also increases the amount of resulting noise in the audio file as well.A novel method which increases the limit up to four bits by Nedeljko Cvejic Et al. [13, 16]. To extract secret message from an LSB encoded sound file, the receiver needs access to the sequence of sample indices used in the embedding process. Normally, the length of the secret message to be encoded is smaller thran the total number of samples in a sound file.

There are two main disadvantages associated with the use of methods like LSB coding. The human ear is very sensitive and can often detect even the slightest bit of noise introduced into a sound file, Second disadvantage however, is that this is not robust. If a sound file embedded with a secret message using either LSB coding was re sample, the embedded information would be lost.

### 3.2 Phase Coding

Phase coding [11, 16] addresses the disadvantages of the noise inducing methods of audio steganography. Phase coding relies on the fact that the phase components ofsound are not as perceptible to the human ear as noise is. Rather than introducing perturbations, the technique encodes the message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to-noise ratio.In figure 4 below original and encoded signal are shown.

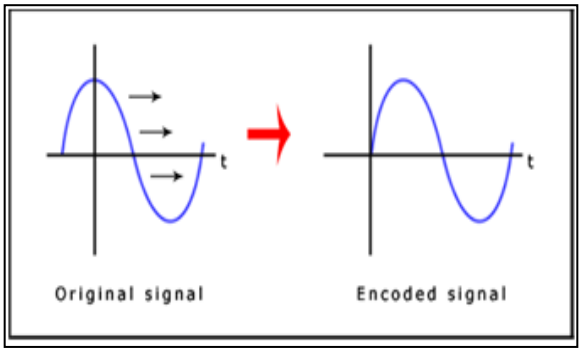


Figure 4: The original signal and encoded signal of phase coding technique.

The principle of Phase coding technique is summarized as under:

- The original sound signal is broken up into smaller segments whose lengths equal the size of the message to be encoded.
- A Discrete Fourier Transform (DFT) is applied to each segment to create a matrix of the phases and Fourier transform magnitudes.
- Phase differences between adjacent segments are calculated.
- Phase shifts between consecutive segments are easily detected. In other words, the absolute phases of the segments can be changed but the relative phase differences between adjacent segments must be preserved.

Therefore the secret message is only inserted in the phase vector of the first signal segment as follows:

$$phase\_new = \begin{cases} \pi/2 & if \ \ message \ \ bit = 0 \\ -\pi/2 & if \ \ message \ \ bit = 1 \end{cases}$$

- A new phase matrix is created using the new phase of the first segment and the original phase difeerences.
- Using the new phase matrix and original magnitude matrix, the sound signal is reconstructed by applying the inverse DFT and then concatenating the sound segments back together.

To extract the secret message from the audio file, the receiver must know the segment length. The receiver can then use the DFT to get the phases and extract the information.

One disadvantage associated with phase coding is a low data transmission rate due to the fact that the secret message is encoded in the first signal segment only. This might be addressed by increasing the length of the signalsegment. However, this would change phase relations between each frequency component of the segment more drastically, making the encoding easier to detect. As aresult, the phase coding method is used when only a small amount of data, such as a watermark, needs to be concealed.

### 3.3 Echo Hiding

In echo hiding [14, 15, 16], information is embedded in a audio 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. If only one echo was produced from the original signal, only one bit of information could be encoded.Therefore, the original signal is broken down

into blocks before the encoding process begins. Once the encoding process is completed, the blocks are concatenated back together to create the final signal.

To extract the secret message from the final stego-signal, the receiver must be able to break up the signal into the same block sequence used during the encoding process. Then the autocorrelation function of the signal's cepstrum (the cepstrum is the Forward Fourier Transform of the signal's frequency spectrum) can be used to decode the message because it reveals a spike at each echo time offset, allowing the message to be reconstructed.

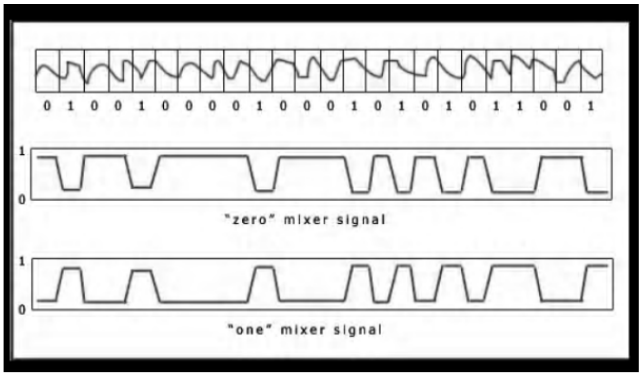


Figure 5: Echo Hiding Methodology.

### 3.4 Spread Spectrum

In the context of audio steganography, the basic spread spectrum (SS) [16] method attempts to spread secret information across the audio signal's frequency spectrum as much as possible. This is analogous to a system using an implementation of the LSB coding that randomly spreads the message bits over the entire audio file. However, unlike LSB coding, the SS method spreads the secret message over the sound file's frequency spectrum, using a code that is independent of the actual signal. As a result, the final signal occupies a bandwidth in excess of what is actually required for transmission. Two versions of SS can be used in audio steganography: the direct sequence and frequency-hopping schemes. In direct sequence SS, the secret message is spread out by a constant called the chip rate and then modulated with a pseudo random signal. It is then interleaved with the cover-signal. In frequency-hopping SS, the audio file's frequency spectrum is altered so that it hops rapidly between frequencies. The SS method has the potential to perform better in some areas than LSB coding, parity coding, and phase coding techniques in that it offers a moderate data transmission rate while also maintaining a high level of robustness against removal techniques. However, the SS method shares a disadvantage with LSB and parity coding in that it can introduce noise into a sound file.

## 4 Proposed Scheme

In this section the authors propose a new method for imperceptible audio data hiding for an audio file of **wav** or **mp3** format. This approach based on the Mod 16 Method (M16M) [10] designed for image named Mod 4 Method (M4M) along with a Number Sequence Generator Algorithm to avoid embedding data in the consecutive indexes of the audio, which will eventually help in avoiding distortion in the audio quality.The input messages can be in any digital form, and are often treated as a bit stream.Embedding positions are selected based on some mathematical function which de-ends on the data value of the digital audio stream. Data embedding is performed by mapping each two bit of the secret message in each of the seed position, based on the remainder of the intensity value when divided by 4. Extraction process starts by selecting those seed positions required during embedding. At the receiver side other different reverse operation has been carried out to get back the original information.

### 4.1 Data Embedding Method

Mod 4 Method (M4M) Sending Algorithm is described as:

- Input: Sampled Audio Data Matrix (a), Message.
- msg = Message converted to binary ;
- Initialize m = n = cnt = x =1 and l=cnt;
- Begin for loop starting with i=1, incrementing 2 and till msize;
- Increment cnt and l by 1 and assign i to count;
- msg0=0; msg1=1;
- let cvr contains the value at a(m,n);
- if cvr is negative then sgn = -1 else sgn = 1;
- R is the absolute remainder after dividing cvr by 4;
- msgx1=binmsg(count) and increment count by 1;
- msgx2=binmsg(count) and increment count by 1;
- If(msgx1=msg0 and msgx2=msg0)
- cvr = cvr - R;
- Elseif (msgx1=msg0 and msgx2=msg1)
- cvr = cvr - R + 1;
- Elseif (msgx1=msg1 and msgx2=msg0)
- cvr = cvr - R+ 2;
- Elseif (msgx1=msg1 and msgx2=msg1)
- cvr = cvr - R +3;
- Divide cvr by 1000;
- If sgn = -1 then cvr = cvr * -1;
- Set the value of cvr at a(m,n);
- Let r be the remainder after dividing x by 4;
- If r = val then m = m + r+1; where val = 0, 1 , 2 and 3;
- x = x + 1;
- End For loop

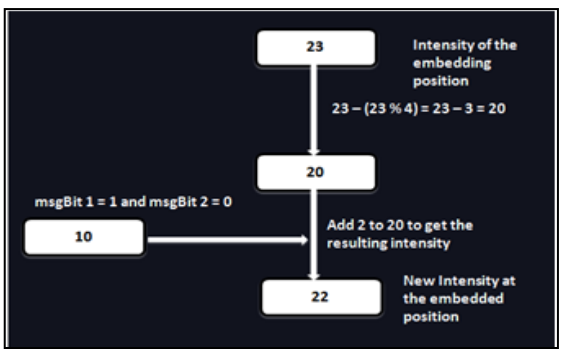

Figure 6: A snapshot of data embedding process.

### 4.2 Data Extraction Method

Mod 4 Method (M4M) Receiving Algorithm is described as: Input: Sampled Audio Matrix (a), Message size

- Initialize m = n = x = count =1;
- binmsg1=";
- Begin for loop starting with i=1, incrementing 2 and till msgsize
- V = value of a(m,n) ;
- let R be the remainder after dividing V by 4;
- if(R==0)
- binmsg1(count)=char (0);
- count=count+1;
- binmsg1(count)=char (0);
- count=count+1;
- elseif(R==1)
- binmsg1(count)= char(0);
- count=count+1;
- binmsg1(count)= char(1);
- count=count+1;
- elseif(R==2)
- binmsg1(count)= char( 0);
- count=count+1;
- binmsg1(count)= char (1);
- count=count+1;
- elseif(R==3)
- binmsg1(count)= char(0);
- count=count+1;
- binmsg1(count)= char (1);
- count=count+1;
- End if
- Let R1 be the remainder after dividing x by 4;
- If R1 = val then m = m + R1 +1; where val = 0, 1 , 2 and 3;
- x = x + 1;
- Initialize msgx=msg1="and k=0;
- Begin for Loop with incrementing i by 1 and till Message size
- Begin for Loop with incrementing j by 1 and till 8
- Increment k by 1;
- msgx(j) = char(binmsg1(k));
- End For loop
- End For loop

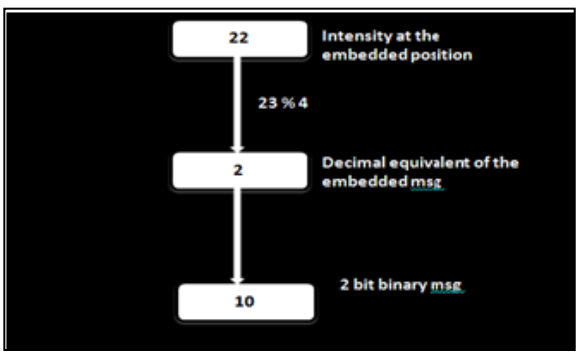


Figure 7: A snapshot of data extraction process.

## 5 Solution Methodology

The proposed system consists of following two windows, one at the SENDER SIDE and the other at the RECEIVER SIDE.The user should be able to select secret message as a file, another audio file has to be used as the carrier (cover audio) and then use the proposed M4M method, which will hide the selected message in the selected carrier audio and will form the stego audio. The user at the receiver side should be able to extract the secret message from the stego audio with the help ofdifferent reverse process in sequential manner.

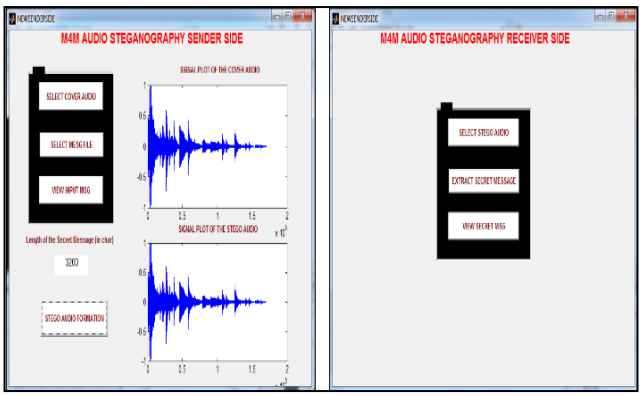


Figure 8: GUI of the proposed steganography system.

### 5.1 Computer Algorithm

In this section the two algorithimic approach is discussed one for the function of the Sender Side and another for the Receiver Side.

**Sender Side**

- Select the cover audio from the set of audio files.
- Select the secret message in text form.
- Embed the secret message through the M4M sending method to generate the Stego Audio.

**Receiver Side**

- Select the stego audio from the set of audio files.
- Extract the secret message through the M4M receiving method.
- Display the secret message.

## 6 System Evaluation

In this section the authors present the experimental result of the proposed method based on two benchmarks techniques to evaluate the hiding performance. First one is the capacity of data hiding and another one is the imperceptibility of the stego audio, also called the quality of stego audio. The quality of stego-audio should be acceptable by human ears. The authors also present detailed study of the proposed method by computing embedding capacity, mean square error (MSE) and peak signal-to noise ratio (PSNR).In this section experimental result of stego audio are shown based on two audio formats viz. **wav** and **mp3**, having a total of different six audio files, three of each

format. Fig. 9 shows the length and maximum embeddingcapacity of each of the audio files.

| Audio file | Length | Maximum Embedding Capacity |
|---|---|---|
| chimes.wav | 00:00:07 | 8498 |
| heartbeat.wav | 00:00:13 | 31583 |
| johncena.wav | 00:01:51 | 38850 |
| gaanwala.mp3 | 00:02:45 | 139308 |
| jagorone.mp3 | 00:03:46 | 188440 |
| yaaron.mp3 | 00:04:25 | 212901 |

Figure 9: Maximum Embedding Capacity Varying with format and size of the audio.

### 6.1 Peak Signal to Noise Ratio (PSNR) and Mean Squared Error (MSE) of a signal

The peak signal-to-noise ratio (PSNR) is the ratio between a signal's maximum power and the power of the signal's noise. Engineers commonly use the PSNR to measure the quality of reconstructed signals that have been compressed.Signals can have a wide dynamic range, so PSNR is usually expressed in decibels, which is a logarithmic scale. In statistics, the **mean squared error (MSE)** of an estimator is one of many ways to quantify the difference between values implied by an estimator and the true values of the quantity being estimated. MSE is a risk function, corresponding to the expected value of the **squared error loss** or **quadratic loss**. MSE measures the average of the squares of the "errors." The error is the amount by which the value implied by the estimator differs from the quantity to be estimated.

| Audio | | Data Size | | | | | |
|---|---|---|---|---|---|---|---|
| | | 100 | 500 | 1000 | 2500 | 5000 | 10000 |
| chimes.wav | PSNR | 67.1593 | 60.8245 | 57.9941 | 54.0638 | 51.0484 | N.A |
| | MSE | 0.0125 | 0.0538 | 0.0538 | 0.2551 | 0.5108 | |
| heartbeat.wav | PSNR | 74.0891 | 66.8539 | 63.7689 | 59.6869 | 56.7102 | 53.6966 |
| | MSE | 0.0025 | 0.0134 | 0.0273 | 0.0699 | 0.1387 | 0.2776 |
| johncena.wav | PSNR | 73.1188 | 67.0395 | 64.2669 | 60.3983 | 57.4135 | 54.4213 |
| | MSE | 0.0032 | 0.0129 | 0.0243 | 0.0593 | 0.1180 | 0.2349 |
| gaanwala.mp3 | PSNR | 79.3587 | 72.9449 | 70.0694 | 66.1954 | 63.1914 | 60.1326 |
| | MSE | 7.5372e-004 | 0.0033 | 0.0064 | 0.0156 | 0.0312 | 0.0631 |
| jagorone.mp3 | PSNR | 80.6707 | 74.2569 | 71.3813 | 67.5074 | 64.5033 | 61.4194 |
| | MSE | 5.5721e-004 | 0.0024 | 0.0047 | 0.0115 | 0.0231 | 0.0469 |
| yaaron.mp3 | PSNR | 80.4089 | 74.1413 | 71.5498 | 67.7883 | 64.8967 | 61.9353 |
| | MSE | 5.9182e-004 | 0.0025 | 0.0046 | 0.0108 | 0.0211 | 0.0416 |

Figure 10: PSNR and MSE values of six audio files at different message sizes.

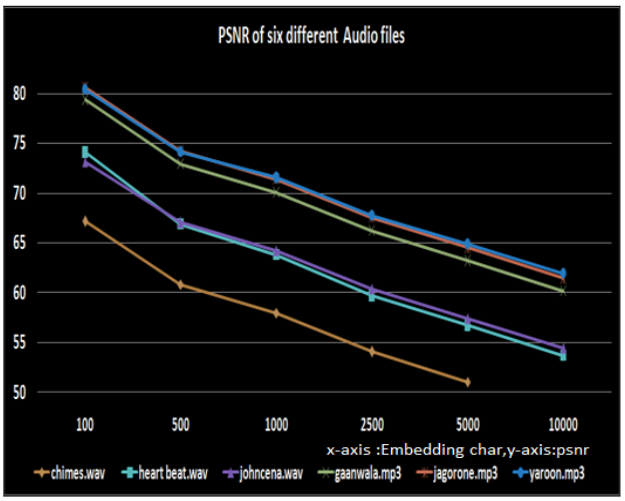


Figure 11: PSNR Plot of different audio files.

### 6.2 Similarity Measure of the Cover Audio and Stego Audio through Correlation

The most familiar measure of dependence between two quantities is the Pearson product-moment correlation coefficient [17-20], or"Pearson's correlation." It is obtained by dividing the covariance of the two variables by the product of their standard deviations. Karl Pearson developed the coeffcient from a similar but slightly different idea by Francis Galton. The Pearson correlation is +1 in the case of a perfect positive (increasing) linear relationship (correlation), -1 in the case of a perfect decreasing (negative) linear relationship (anti correlation) , and some value between -1 and 1in all other cases, indicating the degree of linear dependence between the variables.As it approaches zero there is less of a relationship (closer to uncorrelated). The closer the coefficient is to either -1 or 1, the stronger the correlation between the variables. If the variables are independent, Pearson's correlation coefficient is 0, but the converse is not true because the correlation coefficient detects only linear dependencies between two variables. If there is a series of n measurements of X and Y written as $x_i$ and $y_i$ where i = 1, 2 …., n then the sample correlation coefficient can be used in Pearson correlation r between X and Y. The sample correlation coefficient is written as

$$r_{xy} = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{(n-1)s_x s_y}$$

Where $\bar{x}$ and $\bar{y}$ are the sample means of X and Y, $s_x$ and $s_y$ are the sample standard deviations of X and Y.

| Secret Message Size(in char) | Cover Audio | Correlation-Coefficient |
|---|---|---|
| 100 | Chimes.wav | 1.000 |
| 500 | Chimes.wav | 0.9999 |
| 1000 | Chimes.wav | 0.9994 |
| 2500 | Chimes.wav | 0.9980 |
| 5000 | Chimes.wav | 0.9976 |
| 8000 | Chimes.wav | 0.9970 |
| 10000 | heartbit.wav | 0.9951 |
| 10000 | gaanwala.mp3 | 0.9950 |

Figure 12: Similarity Measure of the Cover and Stego through Correlation

Figure 13-17 shows the signal structure of the audio file chimes.wav at different embedding rate.

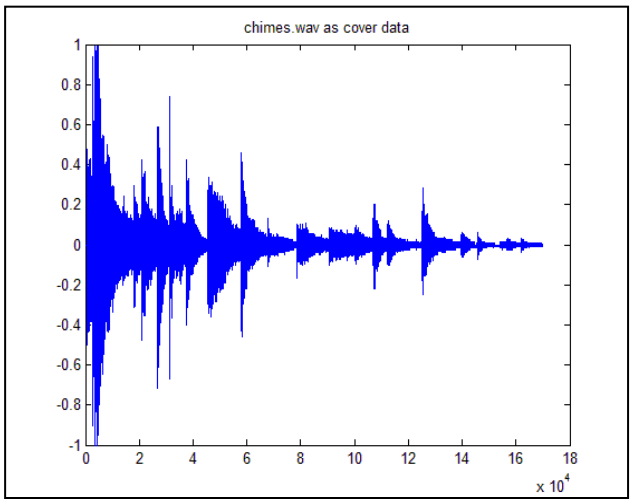


Figure 13: Signal plotting of the cover audio chimes.wav.

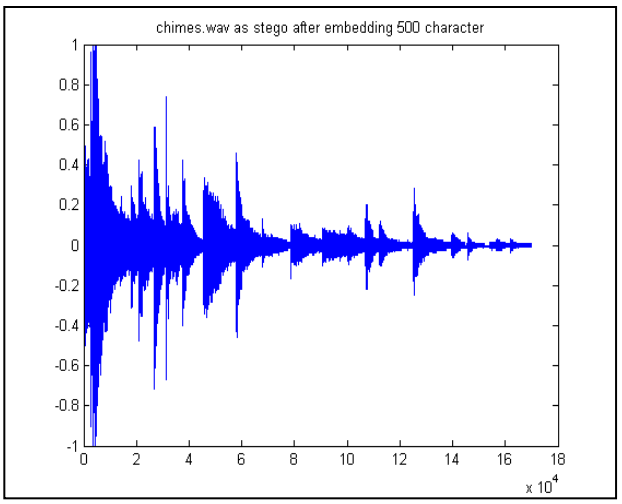


Figure 14: Signal plotting of the chimes.wav after embedding 500 char.

### 6.3 Comparison of M4M with other Audio Steganography Methods

- No previous work focuses on keeping the increasing size of the embedding capacity and similarity between cover audio and stego audio generated based on different message sizes.
- The human ear is very sensitive and can often detect even the slightest bit of noise introduced into a sound file and most of the existing methods do not come much closer to making the introduced noise inaudible.

Proposed M4M method in Audio steganography has been designed keeping in mind to overcome the above mentioned short comings.

- Embedding capacity has been increased by mapping of two bits at a time instead of one.
- Similarity measure between cover audio and stego audio has been inducted here through correlation method and this method is capable of producingstego audio with minimum or zero degradation.

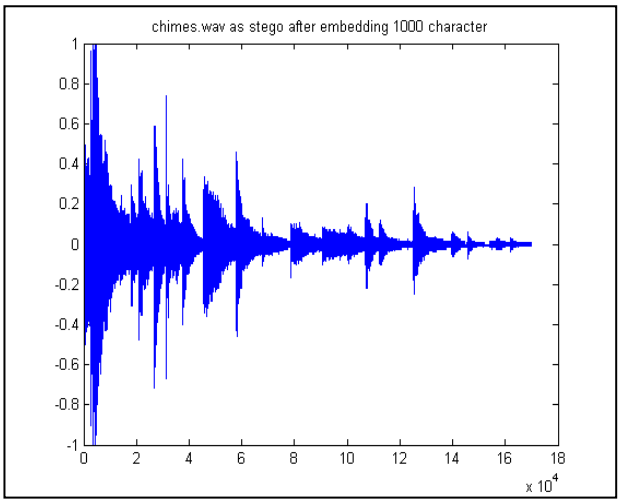


Figure 15: Signal plotting of the Chimes.wav after embedding 1000 char.

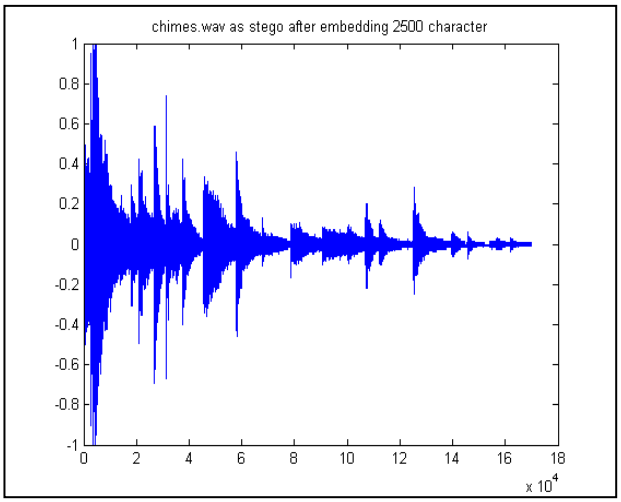


Figure 16: Signal plotting of the Chimes.wav after embedding 2500 char.

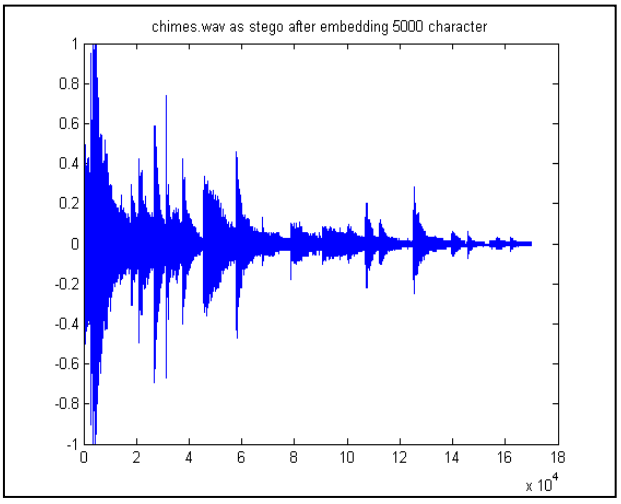


Figure 17: Signal plotting of the Chimes.wav after embedding 5000 char.

## 7 CONCLUSION

In this paper authors have introduced a new and efficient method of imperceptible audio data hiding of wav or mp3 format. Comparison has been shown with some other existing methods also. From the experimental results in can be seen that the embedding capacity of the proposed method is better compared to the other methods because this method can map each two bit of the secret message in the embedding positions instead of one of those existing methods.From the similarity measure point of view the proposed method can be considered as best by producing stego audio with minimum or zero degradation in terms of audio quality as well as the size of the audio.Figure [13-17] shows the signal level of the audio chimes.wav as a cover and at various embedding rate. Also as the message bits are not directly embedded,steganalysis may be able to find out the embedded bits but can not be able to extract the original message bits.Besides PSNR value of the proposed method for various size of the secret message is very good. This system is to provide a good, efficient method for hiding the data from vernal able effect of hostile eavesdropping, theft, wiretapping etc.Although this method has been designed for wav and mp3 format but this method can be extended for any type of audio file format.

## REFERENCES

[1] Gustavus J. Simmons, The Prisoners' Problem and the Subliminal Channel, Proceedings of CRYPTO ,83(1984) 51-57.

[2] RJ Anderson, Stretching the Limits of Steganography, Information Hiding, Springer Lecture Notes in Computer Science, 1174 (1996) 39-48.

[3] Scott. Craver, On Public-key Steganography in the Presence of an Active Warden, Proceedings of 2nd International Workshop on Information Hiding., (1998) 355-368.

[4] Ross J. Anderson. and Fabien A.P.Petitcolas,On the limits of steganography, IEEE Journal on Selected Areas in Communications (J-SAC), Special Issue on Copyright and Privacy Protection,16(1998) 474-481.

[5] N.F.Johnson. and S. Jajodia, Steganography: seeing the unseen, in IEEE Computer, 16(1998) 26-34.

[6] T Mrkel., JHP Eloff and MS Olivier, An Overview of Image Steganography, in Proceedings of the fifth annual Information Security South Africa Conference, (2005).

[7] Souvik Bhattacharyya and Gautam Sanyal, Study of Secure Steganography model, in Proceedings of International Conference on Advanced Computing and CommunicationTechnologies,(2008).

[8] Souvik Bhattacharyya and Gautam Sanyal, Implementation and Design of an Image based Steganographic model, in Proceedings of IEEE International Advance Computing Conference,(2009).

[9] Souvik Bhattacharyya and Gautam Sanyal,An Image based Steganography model for promoting Global Cyber Security, in Proceedings of International Conference on Systemics, Cybernetics and Informatics,(2009).

[10] Arko Kundu, Kaushik Chakraborty and Souvik Bhattacharyya,Data Hiding in Images Using Mod 16 Method, in In the Proceedings of ETECE 2011,(2011)

[11] W. Bender. and D. Gruhl, Steganography: Techniques for data hiding, in IBM SYSTEMS JOURNAL, 35(1996).

[12] Fabien A. P. Pettitcolas, Ross J. Anderson, and Markus G. Kuhn, Information Hiding-A Survey, in Proceedings of the IEEE, 87(1999).

[13] Nedeljko Cvejic and Tapio Seppben, Increasing the capacity of LSB-based audio steganography, in IEEE 2002, (2002).

[14] Samir Kumar Bandyopadhyay, Debnath Bhattacharyya, Poulami Das, Debashis Ganguly and Swarnendu Mukherjee,A tutorial review on Steganography, in In the Proceedings of International Conference on Contemporary Computing, (2008).

[15] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal,A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier, in Journal of Global Research in Computer Science (JGRCS) VOL 2, NO 4 (2011),APRIL-2011.

[16] Natarajan Meghanathan and Lopamudra Nayak, Steganalysis Algorithms for Detecting the Hidden Information in Image, Audio and Video Cover Media, in at International Journal of Network Security & Its Application (IJNSA), Vol.2, No.1, January 2010.

[17] S. Dowdy and S. Wearden. Statistics for research. Wiley. ISBN 0471086029, page 230, 1983.

[18] M. A. Jaro. Advances in record linking methodology as applied to the 1985 census of tampa florida. Journal of the American Statistical Society. 84:414–420, 1989.

[19] M. A. Jaro. Probabilistic linkage of large public health data file. Statistics in Medicine 14 (5-7)., pages 491–498, 1995.

[20] W. E. Winkler. The state of record linkage and current research problems. Statistics of Income Division, Internal Revenue Service Publication R99/04., 1999.

**Souvik Bhattacharyya** has received his B.E. degree in Computer Science and Technology from B.E. College, Shibpur, India, presently known as Bengal Engineering and Science University (BESU) and M.Tech degree in Computer Science and Engineering from National Institute of Technology, Durgapur, India. Currently he is working as an Assistant Professor in Computer Science and Engineering Department at University Institute of Technology, The University of Burdwan. He has a good no of research publication in his credit. His areas of interest are Natural Language Processing, Network Security and Image Processing.

**Arko Kundu** has received his B.E. degree in Computer Science and Engineering from University Institute of Technology, The University of Burdwan.Currently he is pursuing his M.E. degree in Computer

Science and Technology from B.E. College, Shibpur, India, presently known as Bengal Engineering and Science University (BESU).His areas of interest are Network Security, Image Processing and Quantum Computing

**Kaushik Chakrborty** has received his B.E. degree in Computer Science and Engineering from University Institute of Technology, The University of Burdwan. He is working as a Software Engineer at Tavant Technologies (HQ Santa Clara, California), Bangaluru, India. His areas of interest are Web Technology and RDBMS.

**Gautam Sanyal** has received his B.E and M.Tech degree from National Institute of Technology (NIT), Durgapur, India. He has received Ph.D (Engg.) from Jadavpur University, Kolkata, India, in the area of Robot Vision. He possesses an experience of more than 25 years in the field of teaching and research. He has published nearly 50 papers in International and National Journals / Conferences. Two Ph.Ds (Engg) have already been awarded under his guidance. At present he is guiding six Ph.Ds scholars in the field of Steganography, Cellular Network, High Performance Computing and Computer Vision. He has guided over 10 PG and 100 UG thesis. His research interests include Natural Language Processing, Stochastic modeling of network traffic, High Performance Computing, Computer Vision. He is presently working as a Professor in the department of Computer Science and Engineering and also holding the post of Dean (Students' Welfare) at National Institute of Technology, Durgapur, India.