An Advanced Approach for Implementation of Audio Steganography: Modified LSB Algorithm

Dr. Nanhay Singh
Associate Professor
Department of Computer Science & Engineering
Ambedkar Institute of Advanced Communication Technologies & Research, Delhi

Ayush Singhal
UG Student
Department of Computer Science & Engineering
Ambedkar Institute of Advanced Communication Technologies & Research, Delhi

Mohit Singh Bora
UG Student
Department of Computer Science & Engineering
Ambedkar Institute of Advanced Communication Technologies & Research, Delhi

Abstract

Steganography is a branch of information security which deals with transmission of message without being detected. Message, to be send, is embedded in a cover file. Different types of digital can be used as cover object, we used (.WAV) audio as our cover file in the research work. The objective of steganography is to shield the fact that the message exists in the transmission medium. Many algorithms have so far derived for this purpose can be categorized in terms of their embedding technique, time and space complexity. LSB is the acronym of 'Least Significant Bit', is one of the algorithm that is considered as the easiest in way of hiding information in a digital media, also it has good efficiency. It perform its task by embedding secret message in the least significant bits of each data sample of audio file. Ease of cracking this algorithm makes it more prone to visual and statistical attacks. Keeping this in mind few improvisation are being done on LSB algorithm that reduces the ease of cracking message. Modified version of LSB algorithm which we call as 'MODIFIED LSB ALGORITHM' uses the pseudo-random number generator to spread the secret message over the cover in a random manner. This algorithm will be more immune to statistical attacks without affecting its efficiency significantly.

Keywords: Audio steganography, LSB algorithm, Modified LSB Algorithm, MSE, PSNR

I. INTRODUCTION

Steganography is a widely used approach for hiding information in digital media. Steganography played a vital role throughout history. A variety of ways was used for sending secret information covertly, which includes usage of imperceptible ink to write instructions on a section of the paper which was unlikely to be recognized by naked eye. A liquid solution comprising of different ingredients such as vinegar was used to hide the message because of their ability to darken when heated at a specified temperature. In early Greek civilization, secret messengers used to prune their head so that the message can be scribbled on their head, but they had to wait ample amount of time to regrow their hair so that message can be sent. After which the messenger was sent to deliver the message and the message was extracted by the receiver. In the present context of digital steganography, steganography alone is not sufficient, it is augmented by cryptography to ensure data security. In this scheme, original message data is first encrypted and then inserted, into redundant data that is part of a particular file format such as a WAV audio file which is used in our research work. We will briefly discuss audio steganography and digital audio.

A. Audio Steganography

Audio Steganography is a technique of embedding secret messages into a digital audio file. Audio Steganography can be implemented in different audio file formats such as WAV, AU, and MP3. One of the key prospect of audio steganography is to make sure that the modification in data samples of audio file is not perceivable to human ear, to achieve it, the properties of human auditory system (HAS) are exploited in this process[1]. Audio steganography is challenging to perform than image based steganography because HAS is more responsive than naked human eye.

B. Digital Audio

Analog audio signal is continuous in nature whereas digital audio signal is discrete in nature. Now, to convert an analog signal to a digital signal the process of 'sampling' is performed. Sampling is performed at a specified rate which we call as the sampling

frequency. Any digital data is stored in the binary form that means in the form of 0's and 1's, same is the case with digital audio. A digital audio file may contain some redundant sequence, we can exploit this redundancy to embed our secret message bits but making sure that the changes are not perceivable to the human ear. Modulation procedure is used to store audio data in the digital domain. The raw audio signal needs to be sampled at Nyquist rate, according to which for lossless digitization, the sampling rate should be at least twice the maximum frequency present in the audio signal. Prevailing wave file format is used for storing PCM data. To store audio bit streams, different organizations came up with a different format. In case of Microsoft, Waveform Audio File Format was used. It is the fundamental format used by Windows systems for natural and uncompressed audio file. Therefore, Wav audio file is used to carry out our research work. [1]

II. RELATED WORK

Many theories and algorithms have been proposed in the field of steganography, few of them are listed here. In the year 2009, 'A Modulo Based LSB Steganography Method' was proposed that combines samples of least significant bits by using modulo operator to form the value which is compared to the part of the secret message [2]. Later in 2010, 'An audio steganography by a low-bit coding method with wave files' proposed two approached for steganography. The lowest bit coding which was nothing but LSB algorithm and the variable low bit coding to increase the embedded capacity [3]. In the year 2011, 'A view on latest audio steganography techniques' presented different domains in digital audio steganography, which include temporal domain, transform domain, encoder domain. Comparison and evaluation for the reviewed techniques were also presented in the paper [4]. Asad, Gilani proposed different ways to improve the regular LSB algorithm. One of the way is arbitrary assigning bit number used for embedding classified message while the second way is arbitrary allocating sample number containing next classified message bit [5]. Another method which was proposed is presented in paper 'Implementation of Direct Sequence Spread Spectrum Steganography on Audio Data' that emphasized on embedded Messages will be transmitted like noise wave in audio files. A key is used to embed messages into noise, this key is used to generate pseudo-noise wave [6]. Ghazanfari, Ghaemmaghami, Khosravi published paper on 'LSB++: An Improvement to LSB+ Steganography' proposed modification of LSB+ algorithm which decreases the degree of modifications made to the characteristics of the cover image by simply identifying sensitive pixels affecting the signal characteristics [7]. Another method in the same year was proposed was 'Enhanced LSB technique for Audio Steganography' to reduce the aftermath on carrier file, in initial phase steno file is sampled at specified rate and then pertinent bits are modified, modified bit would be LSB [8]. Research paper 'An Improved Inverted LSB Image Steganography' proposed two schemes to improve image quality by bit reversal approach in which LSBs of few pixels of carrier image are reversed if they appear with a specified arrangement of bits of the pixels [9]. Another research paper, 'DWT and LSB based steganography' was published in 2014, that described a procedure by which image is embedded into the audio file by using discrete transformation [10]. 'A New Audio Steganography Scheme based on Location Selection with Enhanced Security' highlighted a new technique in which individual secret message bit is inserted into the selected coefficient of a carrier file. The position for embedding secret message bit was based upon the upper three MSB (Most Significant Bit) [11].

III. PROPOSED WORK

As mentioned above, LSB algorithm is common and easy that makes it prone to visual and statistical attacks. Considering these factors few modifications have been proposed and the name given to this version of LSB is "MODIFIED LSB ALGORITHM" which have better security without affecting its efficiency significantly. The Complexity of existing algorithm would be improved by embedding message at random bit position. But the message will not be embedded directly at that position, LSB would be taken as reference bit. If chosen bit position comes out to be LSB then the message will be embedded in reverse order.

IV. TECHNICAL APPROACH FOR AUDIO STEGANOGRAPHY

In this context, LSB with pseudo-random generator is implemented. MATLAB inbuilt pseudo-random number generator is used for this purpose and seed to this is taken as the key of steganography. Now secret bits are embedded to chosen bit position of audio data samples.

Now to maintain key synchronization at both ends of the communication we used two MATLAB functions namely:

1) rng(seed) – seeds the random number generator using the non-negative integer so that randi(seed) produces a predictable sequence of numbers.
2) randi(seed) – returns an integer containing pseudorandom integer value drawn from the discrete uniform distribution on the interval [1, seed].

A. Embedding Algorithm:

Input: Secret message file, Carrier audio (.wav) file, Seed value.
Procedure:

1) Step1: Read secret message text file and carrier audio file.

2) Step2: Convert message file text into bytes stream.
3) Step3: Enter seed value.
4) Step4: Generate a pseudo random number N using seed value. (N = randi(seed)).
5) Step5: To determine the bit position where the message will be embedded, mod N by 8.
   Chosen bit position n = N%8.
6) Step6: Embed message length in first few data samples at chosen bit position. (We used first 20 data samples in our experiment).
7) Step7: for i = 1 to message length

```
{
  If (n == 0)
 {   If message bit == 1
      Then LSB = 0;
     Else
        LSB= 1 ;}
  Else   // if 8<n<0
{   If message bit == bit at nth position
          Then LSB = 0;
    Else
    LSB = 1;
  } };
End
```

Output: Stenographic audio (.wav) file.

B. Extraction Algorithm:

Input: Stenographic audio (.wav) file, Seed value.
Procedure:

1) Step1: Read Stenographic audio (.wav) file.
2) Step2: Enter seed value.
3) Step3: Generate a pseudo random number N using seed value. (N = randi(seed)).
4) Step4: To determine the bit position where the message is embedded, mod N by 8.
5) Chosen bit position n = N%8.
6) Step5: Extract the message length from first few data samples. (We used first 20 data samples in our experiment).
7) Step6: for i = 1 to message length

```
{ If (n == 0)
{
If LSB == 1
          Then message bit = 0;
   Else
          Message bit = 1;
  }
Else   // if 8<n<0
{
  If LSB == 0;
    Then message bit = bit at nth position
 Else
   Message bit = complement of bit at nth position;
  } };
End
```

Output: Secret message.

V. EXPERIMENTAL WORK

The tool which have been used for implementing Modified LSB algorithm on carrier audio file is MATLAB R2013a. The carrier audio file which is used has the following technical specifications: Filename: 'C: \Program Files\MATLAB\R2013a\bin\carrier.wav', it is an 'Uncompressed' audio file of size 143 KB. The count of channels in our audio file is 1, it represents a stream of audio information in our audio file. The sampling rate which signifies number of samples of audio carried per second is 8192 Hz. The number of bits per sample (bps) corresponds to the resolution of each sample, our steno file contains 16 bps. The count of samples in carrier audio file is 73113 and its duration is 8.9249 seconds.

Link to audio file:
file:https://drive.google.com/file/d/0B3szr0sucPsBMDFFczRfNllqZGM/view?usp=sharing.

Secret message text which is used in our experimental work is of size 2 KB, but the message of greater size can also be embedded, each byte of carrier file can contain 1 bit of the secret message. MODIFIED LSB algorithm is enforced on sample carrier file. We compared initial carrier file with LSB stenographic file and MLSB stenographic file on the basis of three basic specifications- Amplitude of audio signal, PSNR (peak signal to noise ratio) and MSE (mean squared error). As we discussed above that the properties of the human auditory system (HAS) are exploited in the process of audio Steganography, in company with this it is vital that when any statistical analysis in performed upon the stenographic audio signal it do not show abrupt change in its characteristics. So, we selected these parameters as they will help us to compare both original carrier and steno-file effectively as they focus on different aspects of the audio signal.

A. Amplitude:

Amplitude graph of the audio file will enable us to understand the relative distribution of audio data samples with respect to time. Data samples with greater value will exert greater atmospheric pressure in comparison to one with smaller sample value. Sampling rate plays a vital role in the plot of amplitude vs. time, as it determines the frequency at which samples will be picked from the raw audio file.

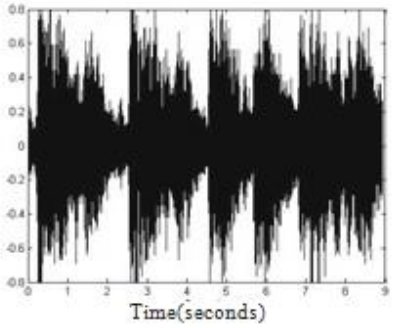

Fig.2. waveform of carrier file.

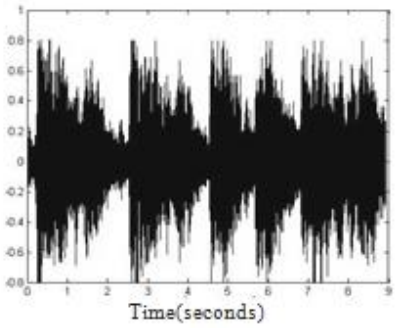

Fig.3. waveform of steno-LSB file

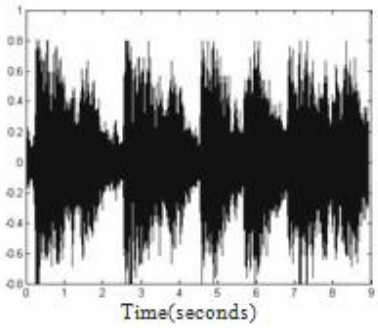

Fig. 4 waveform of steno-MLSB file

From the graph presented above where mean value is set to 0 we can observe the variation of sampled data values with time. In fig.2, we can see distribution of carrier file, in fig.3, we see distribution by LSB algorithm whereas in fig.4, we see distribution by MLSB algorithm. Our aim behind this graph is to compare the plot of sampled data values of original as well as steno-file. Carrier file acted as a base file for comparison with LSB steno-file and MLSB steno-file. Based on keen observation we can state that the variation of LSB and MLSB steno-file are similar which is comparable to that of original file. So, a listener will not be able to perceive any change among the original file and steno-file.

B. MSE (mean squared error):

In statistical term, the mean squared error (MSE) of an audio file measures the average of the squares of the "errors", in our case it measures the difference between the original file and steno-file. A lower value of MSE is desired as it represents lesser introduced error. If we are provided with a noise-free $n_1 * n_2$ matrix of audio data samples *M* and its noisy counterpart *M'*, then its mse is defined by: [12]

$$\text{mse} = \frac{1}{n_1 * n_2} \sum_{x=0}^{n_1-1} \sum_{y=0}^{n_2-1} [M(x,y) - M'(x,y)]^2 \quad (1)$$

In our sample file n_1 = 73113 (16 bit data samples) and n_2 = 1 (as number of channels is = 1).

C. PSNR (Peak Signal To Noise Ratio):

This parameter is frequently used to obtain a numerical value to determine the quality of restoration of “lossy” compression, for example, audio file compression. The signalling wave in the present scenario is the initial audio data samples, and the noise represents the error introduced after the secret message is embedded in carrier audio file. When we compare this parameter, PSNR is a resemblance to human consciousness towards reconstructed signal. In laymen term, a greater value of PSNR commonly demonstrates that the reorganization of our signal is of better quality.
The PSNR (in dB) is defined as: [12]

$$PSNR = 10 * log_{10}(max\text{^}2/mse) \quad (2)$$

Here, max is the maximum possible data sample value of the audio file. In our sample file, its value is 65335 as 16-bit data samples are used.

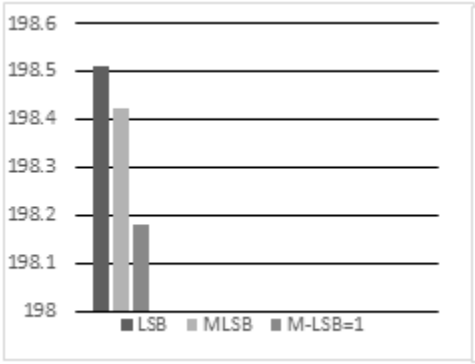

Fig. 5: PSNR (Peak Signal To Noise Ratio)

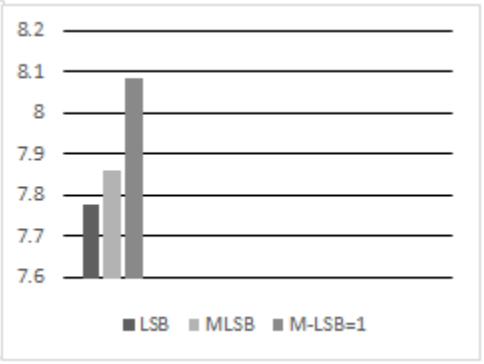

Fig. 6: MSE E^-6(Mean Square Error)

Here LSB represents result of least significant bit algorithm, MLSB represents result of Modified LSB algorithm and M-LSB=1 represents result of MLSB algorithm when chosen bit position is LSB because when chosen bit position is LSB then our message is embedded in opposite sequence.

D. MSE:

X-axis – represents the algorithm used for steganography.
Y-axis – represents the value of MSE (e^-6).
An MSE of value 0, represents that both the files, in present scenario original carrier file and steno-file are equivalent, but it is not factual as far as spatial domain is concerned, because certain amount of bits needs to be altered to covertly embed secret message in cover file. From fig.6, the MSE value observed for LSB is 7.7786 e^-6, for MLSB it is 7.8592 e^-6, and for MLSB=1 it is 8.0821 e^-6. From this data, it can be inferred that LSB algorithm introduced least amount of change followed by MLSB but this change is acceptable as it will decrease the ease of cracking message significantly.

E. PSNR:

X-axis – represents the algorithm used for steganography.
Y-axis – represents the value of PSNR (in decibels).
It defines the ratio between the maximal conceivable power of a signal and the power of pernicious noise that influence the nature of its representation. PSNR is inversely proportional to MSE which means PSNR value of infinity signifies that both the signals are identical. From fig.5, the PSNR value observed for LSB is 198.5115 dB, for MLSB it is 198.4225 dB, and for MLSB=1 it is 198.1789 dB. From this data, it can be inferred that LSB and MLSB exhibit a similar value of PSNR which means the quality of steno-file generated from proposed algorithm is similar to that of steno-file generated by LSB algorithm.

VI. RESULT ANALYSIS

The output steno-file is correct and audible. If we compare amplitude graph of steno-file after LSB and MLSB algorithm, there is no such discrepancy found among the two algorithms. From PSNR (peak signal to noise ratio) and MSE (mean squared error) graph we can conclude that the distortion caused by LSB algorithm is comparable to that of MLSB algorithm. Since bit position is chosen randomly at run time and secret message bits are not embedded directly instead relative to other available bits MLSB algorithm would be more secure in comparison to LSB algorithm.

A. Advantages: (MLSB):

1) Simple to implement.
2) Embedding capacity similar to that of LSB algorithm. (one bit of secret message per byte of data)
3) Usage of Random number generators.
4) Usage of more than one bit from each byte of data sample value.
5) More resistive towards cracking in comparison to LSB algorithm as message sequence is embedded relative to other available bits, it will ensure that original message sequence is available nowhere in the transmission medium.

VII. CONCLUSION AND FUTURE SCOPE

We have provided an advanced approach for audio steganography using Modified LSB algorithm. In further research, we are going to use more advance schemes like steganography with some hybrid cryptographic algorithm for enhancing the data

security. The most important use of stenographic techniques lies in the domain of digital watermarking. Authors, publishers, distributors are keen to secure or look after their propriety works to counter illegitimate distribution and this technique will furnish an approach of tracking the proprietor of their content.

REFERENCES

[1] Prof. Samir Kumar, BandyopadhyayBarnali, Gupta Banik, 2012, "LSB Modification and Phase Encoding Technique of Audio Steganography Revisited",'Introduction', Vol. 1, pp. 1.
[2] Dr. V. Vijayalakshmi, Dr. G. Zayaraz, and V. Nagaraj, 2009, "A modulo Based LSB Steganography Method",'Introduction', pp. 1.
[3] Masahiro Wakiyama, Yasunobu Hidaka, Koichi Nozaki, 2010, "An audio steganography by a low-bit coding method with wave files", pp. 530.
[4] Fatiha Djebbar, Beghdad Ayad, Habib Hamam and Karim Abed-Meraim, 2011, "A view on latest audio steganography techniques", pp. 409.
[5] Muhammad Asad, Junaid Gilani, Adnan Khalid, 2011, "An Enhanced Least Significant Bit Modification Technique for Audio Steganography", pp.143.
[6] Rizky M. Nugraha, 2011, "Implementation of Direct Sequence Spread Spectrum Steganography on Audio Data".
[7] Kazem Ghazanfari, Shahrokh Ghaemmaghami, Saeed R. Khosravi, 2011, "LSB++: An Improvement to LSB+ Steganography", pp.364.
[8] Harish Kumar, Anuradha, 2012, "Enhanced LSB technique for Audio Steganography".
[9] Nadeem Akhtar, Shahbaaz Khan, Pragati Johri, 2014, "An Improved Inverted LSB Image Steganography", pp.749.
[10] Neha Gupta, Nidhi sharma, 2014, "Dwt and LSB based steganography", pp.428.
[11] Pratik Pathak, arup kumar, amitava nag, 2014, "A New Audio Steganography Scheme based on Location Selection with Enhanced Security", pp.1.
[12] David, Salomon, 2007 "Data Compression: The Complete Reference. Springer", pp.281.