Hiding Image in Audio using DWT and LSB

Neha Gupta
Department of Computer Engineering,
The Technological Institute of Textile & Sciences,
Bhiwani
Haryana, India

Nidhi Sharma
Assistant professor in Department of Computer Engineering
The Technological Institute of textile & Sciences,
Bhiwani
Haryana, India

ABSTRACT
The issue of important information hiding preoccupied the minds of many people especially in business, military and political fields due to the secrecy of their information. Thus, there were always secret means and methods that were pursued to send such information. Later on the spread of internet, information can be sent easily and quickly .Still, at the same time the sent data was easily intercepted and uncovered by hackers. Researchers and scientists have made a lot of research work to solve this problem and to find an effective method for image hiding .The proposed system aims to provide improved robustness, security by using the concept of DWT (Discrete Wavelet Transform) and LSB (Least Significant Bit) proposed a new method of Audio Steganography. The emphasize will be on the proposed scheme of image hiding in audio and its comparison with simple Least Significant Bit insertion method for data hiding in audio.

KEYWORD
DWT, LSB, PSNR, AUDIO STEGANOGRAPHY

1. INTRODUCTION
Steganography has evolved into the practice of hiding a message within a larger one in such a way that others cannot discern the presence or contents of the hidden message. In present day, steganography has evolved into a digital strategy of hiding a file in some form of multimedia, such as an image, an audio file (like a .wav or mp3) or even a video file [1]. Stenographic systems can be divided into two categories. In which one is very existence of the message is kept secret and other non-stenographic Systems, in which the existence of the message need not be secret [2].The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. That is not to keep others from knowing the hidden information. Also it is to keep others from thinking that the Information even exists. Steganography is of three types Audio, Image and Video. Through image steganography is the more famous of the two, audio steganography is at present more secure due to the fact that the hackers do not suspect the presence of a hidden message in an audio file.

2. AUDIO STEGANOGRAPHY
Secret information is encoded in a manner such that the very existence of the information is concealed. Main goal of steganography is to communicate securely in a completely undetectable manner [3] and to avoid drawing suspicion to the transmission of a hidden data [4]. It is not only prevents others from knowing the hidden information, simply it also prevents others from thinking that the information even exists. Although a steganography method causes someone to suspect there is secret information in a carrier medium, then the method has failed [5, 6]. The methods that embeds data in sound files use the properties of the Human Auditory System (HAS). The HAS perceives the additive random noise and also the perturbations in a sound file can also be detected. But there are some "holes" we can exploit. As the HAS have a large dynamic range, that has a fairly small differential range. Therefore, loud sounds tend to mask out quiet sounds. So there are also some distortions that are so common that the HAS ignores them. The digital sound is obtained from the analog sound by converting it to digital domain. And this process implies two sub processes: sampling and quantization.

When developing a data-hiding method for audio, a first consideration is the likely environments the sound signal will travel between encoding and decoding. So there are two main areas of modification. Firstly, the storage environment, or digital representation of the signal that will be used, and second the transmission pathway the signal might travel [7, 8]. In order to conceal secret messages successfully, there is a variety of methods for embedding information in digital audio has been introduced. All 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.]. Literally meaning "covered writing", it includes a wide range of secret communication methods like invisible inks, microdots, character arrangement, digital signatures, covert channels, spread spectrum etc. that conceal the very existence of message.

The basic model of Audio steganography consists of Carrier (Audio file), Message and Password. The carrier is also known as a cover-file, which conceals the secret information. While the HAS a large dynamic range, so it often has a fairly small differential range. Therefore, loud sounds tend to mask out quiet sounds. There are some environmental distortions so common as to be ignored by the listener in most cases. There are two concepts to consider before choosing an encoding technique for audio. All they are the digital format of the audio and the transmission medium of the audio.

There are three main digital audio formats typically in use.

These are Sample Quantization, Temporal Sampling Rate and Perceptual Sampling.

1. Sample Quantization which is a 16-bit linear sampling architecture used by popular audio formats such as .WAV and .AIFF.

2. Temporal Sampling uses selectable frequencies (8 kHz, 9.6 kHz, 10 kHz, 12 kHz, 16 kHz, 22.05 kHz and 44.1 kHz.) to sample the audio. Sampling rate puts an upper bound on the usable portion of the frequency range. Generally, the higher sampling rate is higher usable data space gets.

3. Perceptual Sampling format changes the statistics of the audio drastically by encoding only the parts the listener perceives, thus maintaining the sound but changing the signal. And this format is used by the most popular digital audio on the Internet today in ISO MPEG (MP3).

Transmission medium (path the audio takes from sender to receiver) must also be considered when encoding secret messages in audio.

The four transmission mediums are as:

1. Digital end-to-end environment*:* If a sound file is copied directly from machine to machine but never modified, so it will go through this environment. Therefore, the sampling will be exactly the same between the encoder and decoder. A very little constraint put on data hiding in this environment.

2. **Increased/decreased resampling environment***:* In this environment, a signal is resampled to a higher or lowers sampling rate, simply remains digital throughout. Though the absolute magnitude and phase of most of the signal are preserved, temporal characteristics of the signal are changed.

3. Analog transmission and resampling*:* This occurs played on a relatively clean analog line when a signal is converted to an analog state and resampled. The absolute signal magnitude, temporal sampling rate sample quantization and are not preserved. Generally, phase will be preserved.

4. ''Over the air'' environment*:* This occurs when the signal is "played into the air" and "resampled with a microphone". Possible unknown nonlinear modifications of the signal will be subjected causing phase changes, drifting of different frequency components, echoes, amplitude changes etc.

Transmission environment and signal representation both need to be considered when choosing a data-hiding method.

Methods of Audio Data Hiding

Now we need to consider some methods of audio data hiding.

1. In **low-bit encoding data** is embedded by replacing the Least Significant Bit (LSB) of each sampling point by a coded binary string. This results in a large amount of data that can be encoded in a single audio file. For example if the ideal noiseless channel capacity is I Kbps then the bit rate will be 8 Kbps given an 8 kHz sampled sequence. While the simplest way to hide data in the audio files, low-bit encoding scheme can be destroyed by the channel noise and re-sampling.

2. Phase coding when it can be used has proven to be most effective coding techniques in terms of signal to noise ratio. In this method the phase of the original audio signal is replaced with the reference phase of the data to be hidden. It is discovered that a channel capacity of approximately 8 bps can be achieved by allocating 128 frequency slots per bit with a little background noise.

3. LSB MATCHING

Least Significant Bit (LSB) algorithm has a larger amount of capacity than other embedding techniques and it is recognized now, due to many advantages such as the algorithm is simple, the embedded velocity is fast and so on. It is vulnerable to even a slight image manipulation. Compared with the hidden algorithm based on transform domain, the advantage of LSB algorithm is unparalleled. So LSB algorithm still occupies an important position in information hiding. The common steganography software in internet uses LSB algorithm or LSB derivative algorithm [9]. However, steganography is not the same as cryptography. The cryptography hides the contents of a secret message from malicious people, than steganography even conceals the existence of the message [10].

4. PROPOSED WORK

For hiding the image in audio we consider the concept of least significant bit by using DWT and generate an algorithm. LSB is the most simple and a straight forward approach to embed or hide a message into a cover-audio. The message is embedded with sequence-mapping technique in the bit of a cover-audio. Although LSB hides the message in such way that the humans do not perceive it, it is still possible for the opponent to retrieve the message due to the simplicity of the technique. Therefore, malicious people can easily try to extract the message from the beginning of the audio if they are suspicious that there exists secret information that was embedded in the audio.

For hiding, firstly we have to read the audio signal and convert it into binary form. Then embed an image file and also convert it into binary bits. Now apply the DWT (Discrete wavelet transforms) on audio files for taking the higher frequency. And generate a random key. We take 8x8 blocks for each 16 bits data and store the image bits into the last 3bits of the audio file.

For extracting, in this system using the reverse steps for the proposed Method for getting encrypted image and then decrypted for getting the original image in which hiding in the audio file. Now for retrieval read the audio signal and convert signals into binary form. We are taking the higher frequency bits of DWT. We can take 8x8 blocks for each 16 bits data, then taking the last 3 bits data and convert it into original form.

STEPS OF DATA HIDING*:*

1. Read the cover audio signal and convert it into sequence of binary bits.
2. Read the Image to be embedded. Convert it into a sequence of binary bits say msg.
3. Apply DWT on audio file.
4. Take higher frequency component as data
5. Generate a random key using the random key generator.
6. Segment binary audio into 8x8 sub blocks each with 16 bits
7. Initiate textpos = 1;
8. For i= 1:length(Data)
9. Data(i,12:16) = msg (textpos,textpos+3);
10. Textpos = textpos+4;
11. End
12. Generate audio file from Data.

STEPS FOR DATA RETRIEVAL*:*

1. Read the stego audio signal.
2. Convert it into a sequence of binary bits.
3. Segment binary audio into 8x8 sub blocks each with 16 bits.
4. Initiate tpos=1;
5. For i=1:length(Data)
6. .msg(pos,pos+3)= Data(i,12:16);
7. Pos=pos+4;

8. End
9. The msg is the original message

RANDOM KEY GENERATION ALGORITHM:

1. Take two initial values, say 0, 1.
2. An initial "carry bit", say 0.
3. Repeat Step 4 until required number of Digits
4. The new digit can be calculated as

We take each element the sum of the previous two. If we take this sequence mod 10, we have an example of a lagged-Fibonacci sequence with lags r=2 and s=1 and binary operation$v\Delta\, w - v + w\, mod 10$:

0,1,2,2,3,5,8,3,1,4,5,9,4,3,7,……

The information description of the sequence is $x_n = x_{n-2} + x_{n-1} mod 10$, but to formally describe it and define and establish its period we need the finite set X of 1×2 vectors $x = (x_1, x_2)$ with elements reduced residues of 10 and the iterating function *f* defined by $f(x_1, x_2) = (x_2, x_1 + x_2 mod\ m)$. Since *f* has an inverse , for any initial vector $x \in X$ the sequence

$$x\ , f(x), f^2(x), f^3(x), \ldots\ldots$$

It is strictly periodic. Depending on the initial vector$x$, there is a longest cycle of period 60 and shorter cycles of periods 1, 3,4,12 and 20. Each period is the least common multiple (LCM) of the periods of moduli 2 and 5.

Now consider add with carry version of this generator. We assign two initial values, say 0, 1 and an initial "carry bit", say 0. Then each new digit is the sum of the previous two digits plus the carry bit. The result is taken mod 10 and the next carry bit set to 1 or 0 according to whether or not the sum exceeds 10. Using a superscript to indicate the carry bit, the sequence of digits becomes

$$0, 1^0, 1^0, 2^0, 3^0, 5^0, 8^0, 3^1, 2^1, 6^0, 8^0, 4^1, 3^1, 8^0, 4^1, 3^1, 8^1, 1^0, 0^1, 2^1, \ldots\ldots$$

Formally, as before, we have a sequence of iterates $x, f(x), f^2(x), \ldots.$ but now our $x's$ come from the set X of 1×3 vectors $x = (x_1, x_2, c)$ with x_1, x_2 reduced residues of 10 and c the "carry bit", 0 or 1. Then the iterating function *f* is

$$f(x_1, \ldots\ldots, x_r, c) =$$

$$(x_2, x_1 + c, 0) \qquad if\ x_1 + x_2 + c < 10$$

$$(x_2, x_1 + x_2 + c - 10, 1) \qquad if\ x_1 + x_2 + c \geq 10$$

For initial vectors $x = (x_1, x_2, 0)$ with

$$f(x_1, \ldots\ldots, x_r, c) = \begin{cases} (x_2, \ldots., x_r, x_{r+1-s} + x_1 + c, 0) & if\ x_{r+1-s} + x_1 + c < b \\ (x_2, \ldots., x_r, x_{r+1-s} + x_1 + c - b, 1) & if\ x_{r+1-s} + x_1 + c \geq b. \end{cases}$$

Where b is base (here b=10).

ADD WITH-CARRY GENERATORS

We introduce add-with-carry generators with a simple example. Consider the classical Fibonacci sequence. 0,1,1,2,3,5,8,13,21,34,55,89,…., $x_1 < x_2 or\ x = (x_1, x_2, 1)$ with $x_1 > x_2$ the sequence of iterates$x, f(x), f^2(x)$… is strictly periodic with period 108. If the initial vector x is not of those two types and not (0, 0, 0) or (9, 9, 9) then the sequence beginning with $f(x)$ is strictly periodic with period 108, but the "seed" vector x may not reappear in the sequence. We develop rules for finding the period and assigning seed vectors for add-with-carry generators below.

As with lagged-Fibonacci sequences, a whole class of such generators can be created by altering the lags from the values *r*=2 and *s*=1 used in the previous example. The general add-with-carry generator has a base *b*, lags *r* and *s* with *r*>*s*, a seed vector $x = x_1, x_2, \ldots., x_r, c$ with elements "digits" of the base *b* . Then the generated sequence is $x, f(x), f^2(x), f^3(x), \ldots$ with

$f(x_1, \ldots\ldots, x_r, c)$=

$$(x_2, \ldots., x_r, x_{r+1-s} + x_1 + c, 0) \qquad if\ x_{r+1-s} + x_1 + c < b$$
$$(x_2, \ldots., x_r, x_{r+1-s} + x_1 + c - b, 1) \qquad if\ x_{r+1-s} + x_1 + c \geq b.$$

With appropriately chosen base *b*, lags r and s and seed vector$x$, the generated sequence $x, f(x), f^2(x), \ldots..$ will be periodic with period$b^r + b^k - 2$. These generators have extremely long periods. For example, when *b* is near 2^{32} each base-*b* "digit" is a computer word, and with r=1 and k=0 so, then periods of some 2^{640} are attainable at the cost of only r memory locations and simple computer arithmetic.(The add-with-carry instruction is basic to all CPU instruction sets.)

5. RESULTS

Peak signal-to-noise ratio (PSNR) is most commonly used to measure the quality of reconstruction of Loss compression example: for image compression. A signal in this case is the original data, and the noise is the error introduced by compression.

In Table1 we take same size of audio files with different size of image size (jpeg) and get different PSNR values. And in Table2 we used the concept of different size of audio files with same size and get the results (PSNR values).

Table1:

MP3 File Size	Image(.jpeg) Size	PSNR Value
2.5 MB	2KB	36.9988
2.5 MB	1KB	37.0176
2.5 MB	1KB	37.0733
2.5 MB	1KB	37.0186
2.5 MB	1KB	36.9905

Table2:

MP3 File Size	Image(.jpeg) Size	PSNR Value
2.33MB	1KB	36.6810
2.5 MB	1KB	36.9905
350 KB	1KB	20.5

The audio file before and after hiding the image into the audio file sounds same. It means there is no audible difference in audio file before and after hiding the data in to file.

6. CONCLUSION

The main aim is to come up with a technique to hide the data in audio file in such a way there are no perceivable changes in the audio file after the message insertion. Also, if the message that is to hidden was also encrypted then the level of security would be hidden was also encrypted then the level of security would be further raised to a more satisfactory level. The person who got the message would only have the encrypted form of the message with no way of decrypting it so the hidden messages were to be discovered. Proposed scheme has been discussed in this paper for embedding image in cover audio file. Emphasis is on proposed scheme from simple LSB based data hiding in audio, and their robustness in term of steganolysis. Proposed method is better by using the concept of DWT (Discrete Wavelet Transform) and LSB technique. By taking the higher frequency from DWT and using in LSB (Least Significant Bit) we get the PSNR values.

7. ACKNOWLEDGEMENT

The work on this paper was done by Neha Gupta Student of Master of Technology, Department of Computer Engineering Under the guidance of Ms. Nidhi Sharma Assistant Professor in Computer Engineering, The Technological Institute Of textile & Sciences, Bhiwani

8. REFERENCE

[1] Jain a kit, " Steganography: A solution for data hiding", Guru Nanak Dev Engineering College, Ludhiana.

[2] mazleena s., mohd r. k., muhalim m. a., and subariah i., " information hiding using steganography", universiti teknologi malaysia, 2003.

[3]NedeljkoCvejic, TapioSeppben "Increasing the capacity of LSB-based audio Steganography" FIN-90014 University of Oulu, Finland, 2002.

[4]SajadShirali-Shahreza M.T. Manzuri-Shalmani "High capacity error free wavelet domain speech steganography" ICASSP 2008

[5]Neil F.Johnson , Z.Duric and S.Jajodia. "Information Hiding Steganography and Watermarking-Attacks and Countermeasures", Kluwer Academic Publishers, 2001

[6]Min Wu, Bede Liu. "Multimedia Data Hiding", Springer-Verlag New York, 2003.

[7] W. Bender, D. Gruhl , N. Morimoto , A. Lu : Techniques for data hiding, IBM SYSTEMS JOURNAL, VOL 35, NOS 3&4, 1996.

[8] R.Anderson, F.Petitcolas: On the limits of the steganography, IEEE Journal Selected Areas in Communications, VOL .16, NO. 4, MAY 1998.

[9] Neil F. Johnson the Steganography Tools Available from: http://www.jjtc.com /Security /stegtools.htm 2005.

[10] M. M Amin, M. Salleh, S. Ibrahim, M.R.K atmin, and M.Z.I. Shamsuddin "Information Hiding using Steganography" 4* National Conference on Telecommunication Technology Proceedings, Shah Alma, Malaysia, 2003.