IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p-ISSN: 2278-8735
PP 18-22
www.iosrjournals.org

Audio Watermarking Of Images Using LSB Technique

S.Anitha[1], Dr.C.Jeyalakshmi[2]
[1](PG Scholar, Department Of ECE, K.Ramakrishnan College Of Engineering, India)
[2](Assistant Professor, Department Of ECE, K.Ramakrishnan College Of Engineering, India)

Abstract: *In audio watermarking algorithm image is embedded into an audio signal. In this paper we propose least significant bit based audio watermarking method which can embed two images into an audio signal without compromising the robustness against common attacks. First we have to separate the LSB and MSB bits, then the image should be read as binary and finally embed the image binary into the audio signal in place of LSB. Compared with the existing audio watermarking methods, the proposed one is especially robust against noise addition. It is experimentally proved by adding noise to the input audio signal. Moreover the new audio watermarking method is computationally efficient.*

Index Terms: *Audio watermarking, Least Significant Bit, Most Significant Bit, Embedding, Extraction.*

I. Introduction

Watermarking found initially in plain paper and subsequently in paper bills for several centuries. During the last 15 years, the field of digital watermarking was evolving rapidly and currently used for many different applications such as authentication of documents, as well as for secure communication [1]. Consequently, watermarking techniques are occurred in pictures, movies and audios to solve this problem. An audio watermarking is also an interesting research topic. In order to protect an audio media from copying, watermark should be embedded into an original audio without any effect to the quality of original audio. Only the owner can recover this watermarking. Recently, there are several techniques which can be used to embed the watermark into an original audio file. This paper describes a new idea to improve the robust of image watermark embedded into audio signal [2].

Digital watermarking is the act of embedding a message (i.e. an image, song, and video). Its concept is similar to steganography; they both hide a data inside a digital media. However, the difference between them is their goal. Watermarking hides a data related to the actual content of the digital signal where both data and digital signal are important, while steganography has no relation between digital signal and data. The audio signal used as a cover to hide the data i.e. the data is mainly important only. The watermarking system consists of a watermark embedded and a watermark extraction [1].

The watermark embedded part hides the watermark image onto the audio file. The watermark extraction part extracts the watermark image which has been embedded into the audio file during the first stage [1].

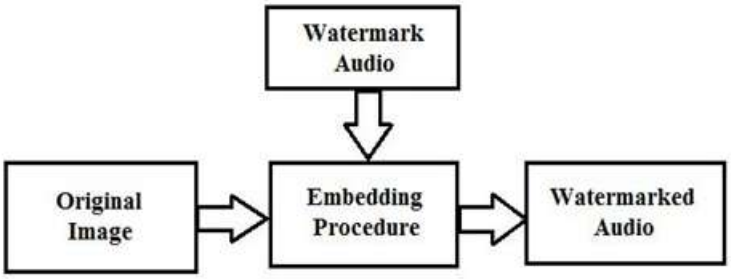

Fig.1 Embedding process of watermarking

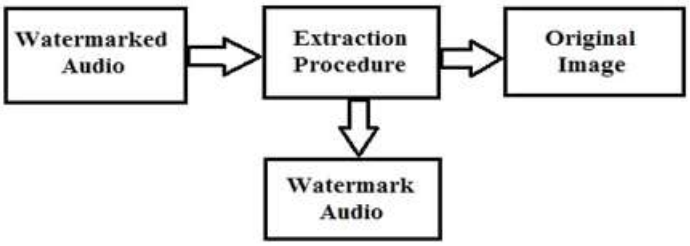

Fig.2 Extraction Process of watermarking

The embedding message may be text data, activation password, key number, authentication key or an image. According to the type of embedding message (image), watermarking techniques can be classified [1].

Watermarking requires two main functions, embedding (hiding) the watermarks with the information and extraction this information. The process of embedding watermark is done at the source end as shown in Fig.1, while the process of extracting the watermark from the watermarked image by reversing the embedding algorithm as shown in Fig.2 [1].

Watermarking techniques can be classified as Text Watermarking, Image Watermarking, Audio Watermarking, and Video Watermarking. In other manner, the watermarks can be divided into three different types they are given as visible watermark, Invisible-Robust watermark and Invisible-Fragile watermark [3].

In this Frequency domain watermarking method the values of selected frequencies can be altered, it is similar to the spatial domain watermarking. Because high frequencies will be lost by compression or scaling, the watermark signal is applied to lower frequencies, or better yet, applied adaptively to frequencies containing important elements of the original picture [3].

In this Spread Spectrum technique can be used for both spatial domain and frequency domain. The spread spectrum method has the advantage that the watermark extraction is possible without using the original unmarked image [3].

Techniques in spatial domain class generally share the following characteristics. The watermark is applied in the pixel domain. No transforms are applied to the host signal during watermark embedding. Combination with the host signal is based on simple operations, in the pixel domain. The watermark can be detected by correlating the expected pattern with the received signal [3].

Spatial domain watermarking is performed by modifying values of pixel color samples of a video frame.

The most common algorithm using spatial domain watermarking is LSB [6].

The process of watermarking begins when the encoder inserts watermark into audio, producing watermarked audio. The decoder extracts and validates the presence of watermarked input or unmarked input. If the watermark is visible, the decoder is not needed. Otherwise, the decoder may or may not require a copy of decoder to do this job [6].

The decoder is so designed to process both marked as well as unmarked image. Finally, the decoder needs to correlate the extracted watermark with original image and compare the result to a predefined threshold that sets the degree of similarity accepted as a match. If the correlation matches the threshold value, then watermark is detected i.e. original image belong to the user otherwise the data does not belong to the user [6].

The audio watermarking is similar to the concept of watermarking physical objects with the difference that the watermarking technique is used for digital content instead of physical objects. In audio watermarking a secret information or image is embedded in another image in an imperceptible manner. This secret information or image is called watermark and it contains some metadata, like security or copyright information about the main data/image [6].

The watermark embedded inserts a watermark onto the audio file and the watermark detector detects the presence of watermark information/image. Sometime a watermark key is also used during the process of embedding and detecting watermarks [6].

The watermark key has a one-to-one relation with watermark information. The watermark key is private and known to only intended users and it ensures that only desirable set of users can detect the watermark [6].

II. LSB Algorithm

The most common method of watermark embedding is to embed the watermark into the least significant-bits of the cover object. Although it can survive transformations like cropping, any addition of undesirable noise or lossy compression but a more sophisticated attack that could simply set the LSB bits of each pixel to one can fully defeat the Watermark with negligible impact on the cover object. Security of the watermark would be enhanced greatly as the Watermark could now be no longer is easily viewable to the hackers or any other unintended user. Although this algorithm is still vulnerable to replacing the LSB's with a constant value [8].

There are many algorithms available for audio watermarking. The simplest algorithm is Least Significant Bit (LSB) Insertion, 4in which each 8-bit pixel's least significant bit is overwritten with a bit from the watermark. Given the extraordinarily high channel capacity of using the entire cover for transmission in this method, a smaller object may be embedded multiple times. In an audio file, information can be inserted directly into every bit of audio information or the more busy areas of an audio file can be calculated so as to hide such messages in less perceptible parts of an audio. The methods were based on the pixel value's Least Significant Bit (LSB) modifications [6].

This LSB algorithm uses spatial domain technique. In this technique watermark is applied in pixel province. During watermark embedding no transforms are applied to the host signal. In the pixel domain the combination with the host domain is based on easy operations. The watermark can be detected by correlating the anticipated model with the received signal. This technique is performed by changing values of pixel color samples of a video frame [7].

The LSB stands for Least Significant Bit. It is the byte or octet in that position of a multi byte number which has the least potential value. The Least Significant Bit gives the unit value and it shows the bit position in a binary integer. It determines whether the number is odd or even. The LSB is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digit further to the right [7].

It analogous to the least significant digit of a decimal integer, which is the digit in the ones position. If the number changes even slightly then the least significant bits have the useful property of changing rapidly. It is easy to understand and simple implement [7].

III. Proposed Work

In an audio watermark processing, information can be embedded directly into every bit of audio signal. In computing, the Least Significant Bit is defined as the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The LSB is sometimes referred to as the right -most bit, due to the convention in the positional notation of writing less significant digit further to the right. lt is analogous to the least significant digit of a decimal integer, which is the digit in the ones (right-most) position . The most common and earliest method of a watermark is to insert the watermark information into the least significant bits of the cover object (audio). An example of the less predictable or less perceptible is Least Significant Bit insertion.

This part shows how this works for an 8-bit gray-scale image and the possible effects of modifying such an image. The principle of embedding is truly simple and effective. By using an 8-bit jpeg image in gray-scale, we add bit information to the least significant bits of each pixel (byte), in every 8-bit pixel. In a gray-scale image, each pixel is equivalent to 1 byte i.e. 8 bits. lt can represent 256 gray colors vary from black to white i.e. from 0 to 255. The principle of encoding uses the Least Significant Bit of each of these bytes, the bit on the far right side. For example, only the least significant bit of each pixel will be used for embedding (insertion) information.

Security of the watermark would be enhanced greatly as the Watermark could now be no longer is easily viewable to the hackers or any other unintended user. Although this algorithm is still vulnerable to replacing the LSB's with a constant value.

EMBEDDING PROCESS

The following algorithm describes the enveloping process of message image into audio signal.
Input: Message Image
Output: Watermarked Audio Signal.

Step 1: Read the audio file you want to use for embedding.
Step 2: Read the message image you want to hide in the audio signal.
Step 3: Conversion of message image into double.
Step 4: Rounding of values after operation (message/256).
Step 5: Conversion into uint8 values.
Step 6: Determine the size of audio signal used for embedding.
Step 7: Determine the size of message object to embed.
Step 8: Set the MSB or 8st bit of cover object (ii,jj) to the value of the MSB of watermark (ii,jj).
Step 9: Write to file the two images.
Step 10: Display watermarked image.

Fig.3 shows the audio signal. In this audio signal the two images have to be hidden.

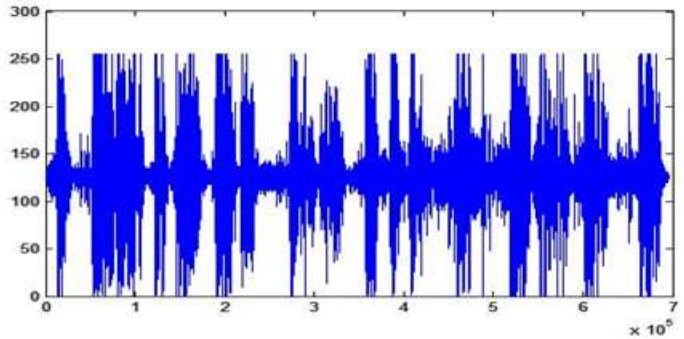

Fig.3 Audio Signal

(a) **(b)**

Fig.4 (a) and (b) are the embedded images

Fig.4 shows the two secret images that are hidden into the audio signal. These two images are in the jpeg format. The dimension of these images is 50x50.

The above two images are embedded into the host audio signal using the least significant bit technique. This least significant bit technique is based on the spatial domain technique.

Fig.5 shows the two images embedded host audio signal with the noise addition. There is slight difference between the original host audio signal and image embedded host audio signal.

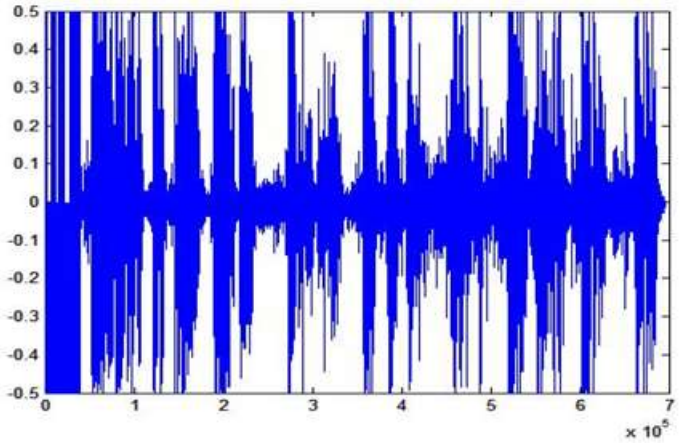

Fig.5 image embedded audio signal

EXTRACTION PROCESS

The following algorithm describes how the original message image is retrieved from the audio signal

Input: The Audio File
Output: Original message image

Step 1: Read the watermarked audio signal to be used for recovering.
Step 2: Determining size of audio signal.
Step 3: Use the LSB of audio signal to recover watermark.
Step 4: Scaling the recovered watermark by converting the image into double.
Step 5: Scaling and displaying the recovered image.

Noise Addition:

The noise is added to the host audio signal where the secret images are hidden. The robustness of the audio signal is determined by the addition of the noise. Fig.6 (a) and (b) shows the output images that are watermarked into the host audio signal using the Least Significant Bit technique.

(a)

(b)

Fig.6 (a) and (b) are the retrieved images

Even though the noise is added to the audio signal during the embedding process of images, the output images are not affected by the noise addition. During the extraction process two images are retrieved properly.

IV. Conclusion

This paper proposed two images watermarked into the audio signal using the Least Significant Bit technique. In watermarking two processes are done namely Embedding and Extraction. During the embedded process the two secret images are hidden into the host audio signal. And the noise is also added to the host audio signal. In the extraction process the host audio signal is converted into the decimal and the secret images are retrieved.

The advantage of LSB embedding is well reliant on its simplicity as many techniques use such methods. There are many weaknesses when robustness, tamper resistance and other security issues are measured. LSB encoding is sensitive to any kind of filtering or manipulation of the image. Scaling, rotation, cropping, addition of noise or lossy compression to the image is very likely to destroy the message. The major advantages of LSB algorithm are (1) it is rapid and easy to implement, (2) it works very well with the gray-scale image. Therefore using the proposed algorithm the results has been achieved.

Reference

[1]. Moustafa M.Kurdi, Imad A.Elzein and Akram M.Zeki **"**Least Significant Bit (LSB) and Random Right Circular Shift (RRCF) in Digital Watermarking**"**, IEEE transaction 2016.

[2]. Sarawut Kaengin, Surapan Airphaiboon and Somsanouk pathoumvanh **"**New technique for embedding watermark image into an audio signal**"**, IEEE 2009.

[3]. Rajni Goyal and Naresh Kumar **"**LSB based digital watermarking technique**"**, international journal of application or innovation in engineering and management, vol 3, issue 9, September 2014.

[4]. Santhoshi Bhatt, Arghya Ray, Avishake Ghosh and Ananya Ray, **"** Image Steganography and Visible Watermarking Using LSB Extraction Technique**"**, IEEE sponsored 9th International Conference on Intelligent Systems and Control,2015.

[5]. Yong Xiang, Iynkaran Natgunanathan, Yue Rong and Song Guo, **"**Spread Spectrum Based High Embedding Capacity Watermarking Method for Audio Signals**"**, IEEE transaction august 31,2015.

[6]. Patil V.A and S.S.Tamboli, **"**Image Watermarking Using Least Significant Bit (LSB) Algorithm**"**, International Journal Of Trend in Research and Development, vol 3(3),ISSN:2394-9333,May-Jun 2016.

[7]. Preeti Gaur and Neeraj Manglani, **"**Image watermarking using LSB Technique**"**, International Journal of Engg research and general science, volume3, issue 3, May-June, 2015.

[8]. Puneet Kr Sharma and Rajni, **"**Analysis of Image Watermarking Using Least Significant Bit Algorithm **"**, International Journal of Information Science and techniques, vol 2, July 2012.