ADAPTIVE METHOD OF INFORMATION HIDING IN AUDIO BY USING LFSR AND LSB ENCODING

Hayder I. Hendi

ABSTRACT

Steganography is the practice of encoding secret information in indiscernible way. Audio Steganography is a technique used to transmit hidden information by modifying an audio signal in an imperceptible manner. It is mainly required for increasing security in transferring and archiving of audio files. Steganography complements rather than replaces encryption by adding another layer of security- it is much more difficult to decrypt a message if it is not known that there is a message. The basic idea of the paper is hide information in cover audio by using linear feedback shift registers LFSR with the Least Significant Bit (LSB) coding to hide data for it and the proposed method hiding data in audio signals using LFSR to select any LSB of audio signals. this proposed method has more security than classical methods because the analysis didn't know any vector used for hide data and proposed method has low noise audio signals than classical method because less number of LSB used for hide data ,the proposed method was applied on two experimental for hiding data and extracting the embedded data in audio signals and applied the noise tests mean squared error (MSE) and Signal-to-noise ratio (SNR) and peak signal-to-noise ratio (PSNR) on it .

Keywords

Information Hiding, Audio Steganography, linear feedback shift registers LFSR, Least Significant Bit (LSB),

I. INTRODUCTION

Any data can be represented as digital data. With the advancement of the technologies and the internet, storage and communication via digital data has gained a lot of significance .As a direct consequence, the need for data security in digital communications, copyright protection of digitized properties and secure communication has also gained equal importance.

The term steganography is the technique of embedding secret information in a communication channel in such a manner that the very existence of the information is concealed .

The aim is to embed and deliver secret messages in digital data without any suspiciousness. The secret message might be a caption, a plain text, another image, a control signal, or any data that can be represented in bit stream form. The secret message may be compressed and encrypted before the embedding begins.

Steganography techniques have been successfully applied on text files, images, audio and video files. Although, steganography in audio is a field not much explored. It is because of the fact that embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images [5].

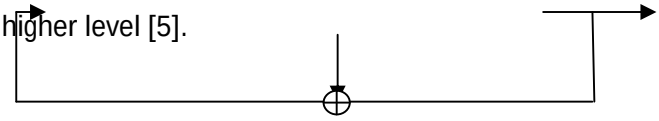
Among the methods of Steganography, the most common one is to use images for applying steganography. Image steganography has been explored extensively with various steganographic schemes. Since nowadays, audio files are available everywhere and moreover; today's technology allows the copying and redistribution of audio files over the Internet at a very low or almost no cost. So it is necessary to have methods that confines access to these audio files and also for its security [3]

Audio Steganography, or information hiding in audio signals, is gaining widespread importance for secure communication of information such as covert battlefield data and banking transactions via open audio channels.

A Steganography system, in general, is expected to meet three key requirements, namely, imperceptibility of embedding, correct recovery of embedded information, and large payload. Some degradation in the perceptual quality of the stego-signal from that of the original host signal may be acceptable. Practical audio embedding systems, however, face hard challenges in fulfilling all three requirements due to the large power and dynamic range of hearing, and the large range of audible frequency of the human auditory system [5].

The techniques include the Least Significant Bit substitution (LSB) and echo hiding techniques, among many others [1]. LSB embeds information in the least significant bits of the audio sample values by overwriting the original bits [1]

Audio Steganography relies on the imperfection of the human auditory system. In several audio steganography techniques, the secret message is embedded in the frequency range which is in either higher or lower than the frequency range which can be audible to the human ears. Several other Audio steganography techniques take advantage of the psychoacoustic masking phenomenon of the human auditory system [HAS]. Frequency masking occurs when human ear cannot perceive frequencies at lower power level if these frequencies are present in the vicinity frequencies at higher level [5].



The mean squared error (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. [4]

Signal-to-noise ratio (SNR) is a measure used in science and engineering that compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power. [4]

The peak signal-to-noise ratio (PSNR) is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation .[4]

2. LINEAR FEEDBACK SHIFT REGISTERS (LFSR)

=Linear Feedback Shift Registers sequence through ($2^n - 1$) states, where n is the number

of registers in the LFSR. At each clock edge, the contents of the registers are shifted right by one position and feedback from predefined registers or taps to the left most register through an Exclusive-NOR (XNOR) or an Exclusive-OR (XOR) gate, a value of all "1"s is illegal in the case Of a XNOR feedback, a count of all "0"s is illegal for an XOR feedback, This state is illegal because the counter would remain locked-up in this state.

LFSR counters are very fast since they use no carry signals, used as pseudo-random bit stream generators. They are important building blocks in the implementation of encryption and decryption algorithms. [2]

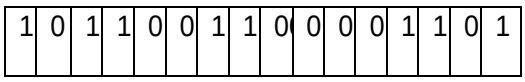


Fig (1) Linear Feedback Shift Registers

3. PROPOSED EMBEDDING METHOD

This proposed method use Hidden data in the LSBs of the audio Signals. Also used the LFSR a selector of any LSB used to hide data, there are two advantages of proposed method.

First more secure because the hidden data does not use all audio signal that given more difficult to analysis.

Second low noise in audio signals because used limit number LSB for hide data in it.

The proposed hidden method consists of the Following steps:

1- Let a sound data *S (M)*, such that *M* is the number sound vectors. Each vector had size *L=32 bits* in this work and LSB of vector use hide data .
2- Text files T (N) such N is number of bits of text file.
3- LFSR has 16 bits with high period initial value of LFSR.
4- J=0
5- For *I=0 to m-1* do
6- C is output of clock LFSR
7- If (c=0) and (j=N) then go to 11
8- LSB(S(I))=T(j)
9- J=j+1
10- Next i

And flow chart of algorithm see figure (1)

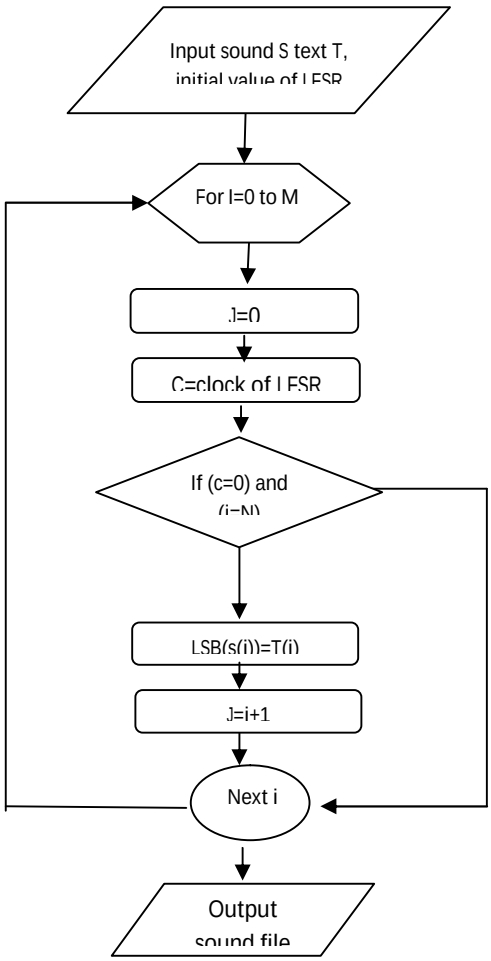


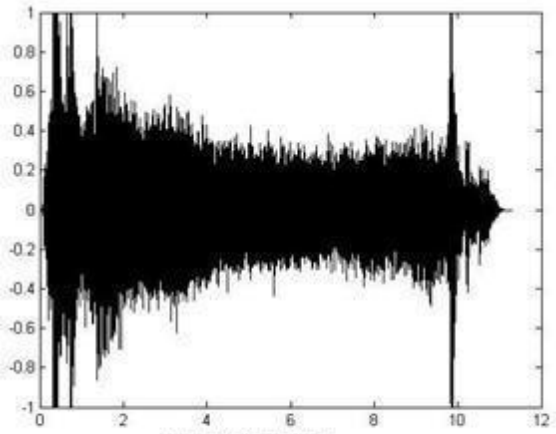
Fig (2) flow chart of embedding method

In this method applied sound files (.wav), Many tests are performed to ensure the success of hidden method and measure the noise in audio signals such that mean squared error (MSE) and Signal-to-noise ratio (SNR) and peak signal-to-noise ratio (PSNR).

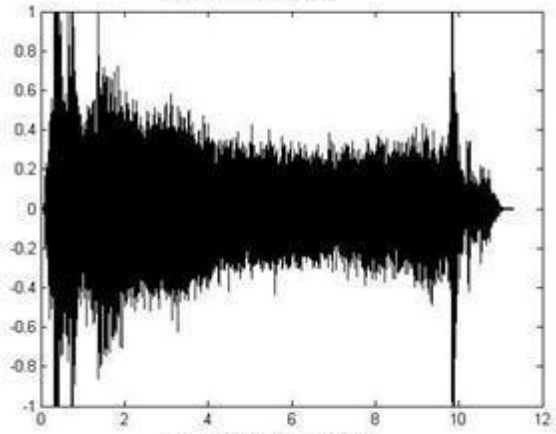
4. IMPLEMATATOIN

This proposed method implemented in (MATLAB 2008 a) and proposed method applied two e sound files (.wav). The proposed method used hidden data and relative the embedded data in audio signals without loss in hidden data.

The first experimental has size 974 Kbyte and 11second and second experimental has size 947 Kbyte and 11 second such that fig (2) and fig (3).

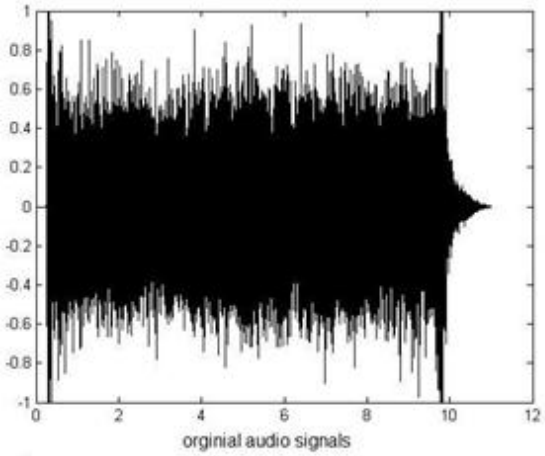


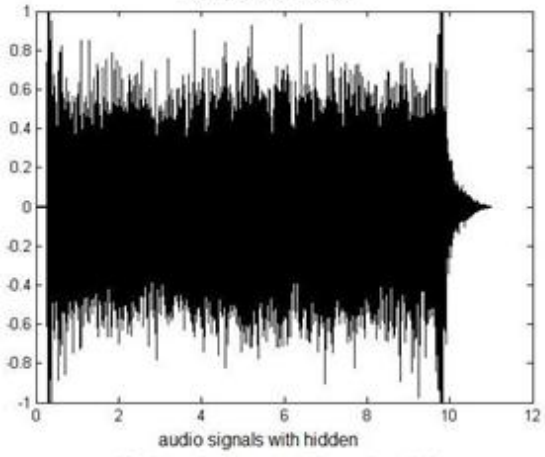
orginial audio signals



audio signals with hidden

fig(3) audio signals of Expermental 1





fig(4) audio signals of Experimental 2

The proposed method applied on two experimental for hide data and relative embedded data in audio signals. The first experimental has 3 Kbyte and embedded data in second experimental is 2.9 Kbyte.

Also applied noise tests mean squared error (MSE) and Signal-to-noise ratio (SNR) and peak signal-to-noise ratio (PSNR) on the original audio signals and result audio signals of hidden and compared with classical method for two experimental and the result given in table below:-

NAME	METHOD	MSE	PSNR	SNR
Experiment 1	classical	0.064	158.4595	732.3502
	Proposed method	0.055	158.8053	845.9817
Experime	classical	0.064	158.27	740.10

nt 2			26	48
	Proposed method	0.020	160.4531	2.3966e3

Table (1) the noise tes

The result classical method audio signal has little comparison the original audio signals.

5. CONCLUSION

It is adaptive method and efficient method for embedding messages in audio signals and extracting the embedded data from stego-audio signals without lossless. The data is embedded into cover audio signals more secure that classical method because using LFSR the choose audio vector embedded data into or not, and low noise in audio signals that improved by noise in table above will see MSE and PSNR in proposed method is low that classical methods and SNR in proposed method high than in classical method.

The proposed method is difficult for hidden analysis because difficult found the embedded data in audio signals.

but hide data in proposed method is less than classical methods .

REFERENCES

[1] Ali Al-Haj," DWT–Based Audio Watermarking", The International Arab Journal of Information Technology, Vol. 8, No. 3,pp .326-333,July 2011

[2] Maria George, "Linear Feedback Shift Registers in Virtex Devices",XAPP210 ,http://www.xilinx.com,2007

[3] H.B.Kekre "Information Hiding in Audio Signals", International Journal of Computer Applications Vol. 7– No.9 ,pp 14-19, October 2010.

[4] Huynh-Thu, "Scope of validity of PSNR in image/video quality assessment". Electronics Letters 44 (13) pp. 800–801. 2008

[5] Shafi K, "A Novel Audio Steganography Scheme using Amplitude Differencing", IEEE Xplore, Vol. 10, pp. 163-167, 2010.