Steganography in Audio Using Wavelet and DES

*Rasha H. Ali**

Received 25, May, 2014
Accepted 10, August, 2014

Abstract

In this paper, method of steganography in Audio is introduced for hiding secret data in audio media file (WAV). Hiding in audio becomes a challenging discipline, since the Human Auditory System is extremely sensitive. The proposed method is to embed the secret text message in frequency domain of audio file. The proposed method contained two stages: the first embedding phase and the second extraction phase. In embedding phase the audio file transformed from time domain to frequency domain using 1-level linear wavelet decomposition technique and only high frequency is used for hiding secreted message. The text message encrypted using Data Encryption Standard (DES) algorithm. Finally; the Least Significant bit (LSB) algorithm used to hide secret message in high frequency. The proposed approach tested in different sizes of audio file and showed the success of hiding according to (PSNR) equation.

Keywords: Steganography in Audio, Secret message, DES algorithm, LSB algorithm, Wavelet transform.

Introduction:

In present, information security is very important in digital communication. As the internet and multimedia technology increasing, a need of secure algorithm is required to protect the authenticated and authorized multimedia contents such as, image, audio and video etc. Sensitive information like medical and legal records, credit ratings, Business transactions, Voice mails are also require to be protected from outsiders. Cryptography is a technique to hide the information in digital communication which preserves integrity, confidentiality and authenticity of multimedia and text information [1].

The word steganography comes from the Greek Steganos, which means covered or secret and –graphy means writing or drawing. Therefore, steganography means, literally, covered writing. Steganography is the art and science of hiding information such that its presence cannot be detected and a communication is happening. Secret information is encoding in a manner such that the very existence of the information is concealed. Paired with existing communication methods, steganography can be used to carry out hidden exchanges [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 [3].

Steganography is often used to copyright audio file to protect the rights of music artists. Techniques like least significant bit insertion, phase coding, spread spectrum coding, and echo hiding can be used to protect the content of audio file. The biggest challenge face all these methods is the sensitivity of human auditory system (HAS), it is so sensitive, such that

*Department of Computer- College of Education for Women- University of Baghdad.
E-mail: rashaha2003@yahoo.com

people can often pick up randomly added small noise, and this making hard to success-fully hide data within audio data [4].

Wavelet Analysis

The wavelet transform (WT) has gained widespread acceptance in signal processing and image compression. Wavelet transform is the breaking up of a signal into shifted and scaled versions of the original (or mother) wavelet. A wavelet is a waveform of effectively limited duration that has an average value of zero. For signals; identity of the signal is given by the low-frequency component. The high-frequency content only imparts save our or nuance. In human voice, if high frequency components are removed, the voice sounds different, but still it can be understood. If low frequency components are removed, signal sounds gabble. On applying wavelet transformations on audio signal, approximation and detail components of audio can be obtained. The approximations are low-frequency components of the signal and details are high-frequency components. The first level detail coefficients have less importance in comparison with detail coefficients of next levels and approximation coefficients because of their low energy level. Figure (1) shows the decomposition of audio signal on wavelet transform [5].

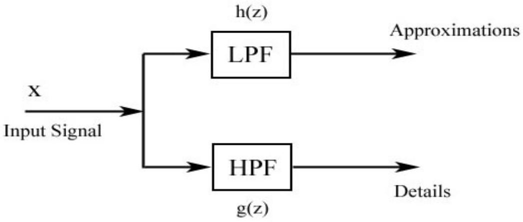

Fig. (1) Signal Decomposition

Data Encryption Standard (DES) :

The Data Encryption Standard algorithm (DES) is the most widely used symmetric encryption algorithm in the world so far. DES was quickly adopted for non-digital media. The banking industry, adopted DES as a banking standard. Standards for the banking industry are set by the American National Standards Institute.

DES is a symmetric block cipher designed to encrypt and decrypt blocks of data consisting of 64 bits under control of a 56 bit key. Each 8th bit of the 64-bit key is used for parity checking and otherwise ignored. Decrypting must be done by using the same key as for encryption [6].

An initial permutation (IP) used in this algorithm, the 64-bit plaintext is split into two 32 bit input (L0 & R 0). DES consists of 16 rounds. In each round a function, ‘f’ is performed in which the data is combined with a 48-bit permutation of the key. After the 16the iteration, the right (R 16) and left (L16) halves are concatenated and an inverse permutation (IP-1) completes the encryption process [7]. The figure for the entire DES encryption is shown in figure (2).

Function of DES[7]

The function of the DES algorithm is made up of four operations:

- The 32-bit right half of the plaintext R0 is expanded to 48-bits with expansion box.
- 48 bit plaintext is XORed with a 48-bit sub-key, K1.
- The result passes into 8 S-Boxes. Each S-Box transforms 6 bit input to 4 bit output.
- Finally, a permutation is performed; the output of the result is XORed with the initial left half L0, to obtain the new right half R1. The original right half, R 0, becomes the new left half L1. The whole process iterates for 16 times and operates with 16 different keys (K 1, K2, K3… K16).

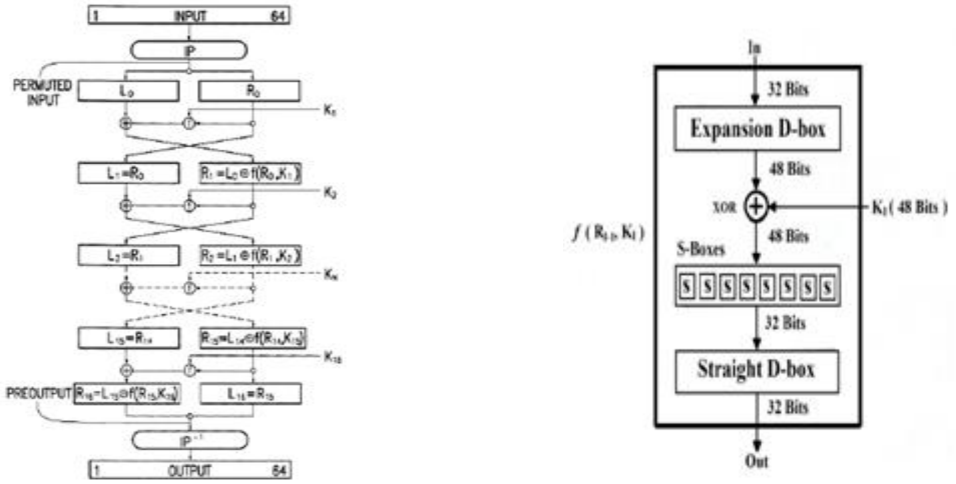

Fig. (2) DES Encryption Process

The Proposed System

In this paper, a method for hiding secret text message encrypted by using DES then embedding in frequency domain of audio. This method contains two phases, the embedding and extraction, as shown in figure (3).

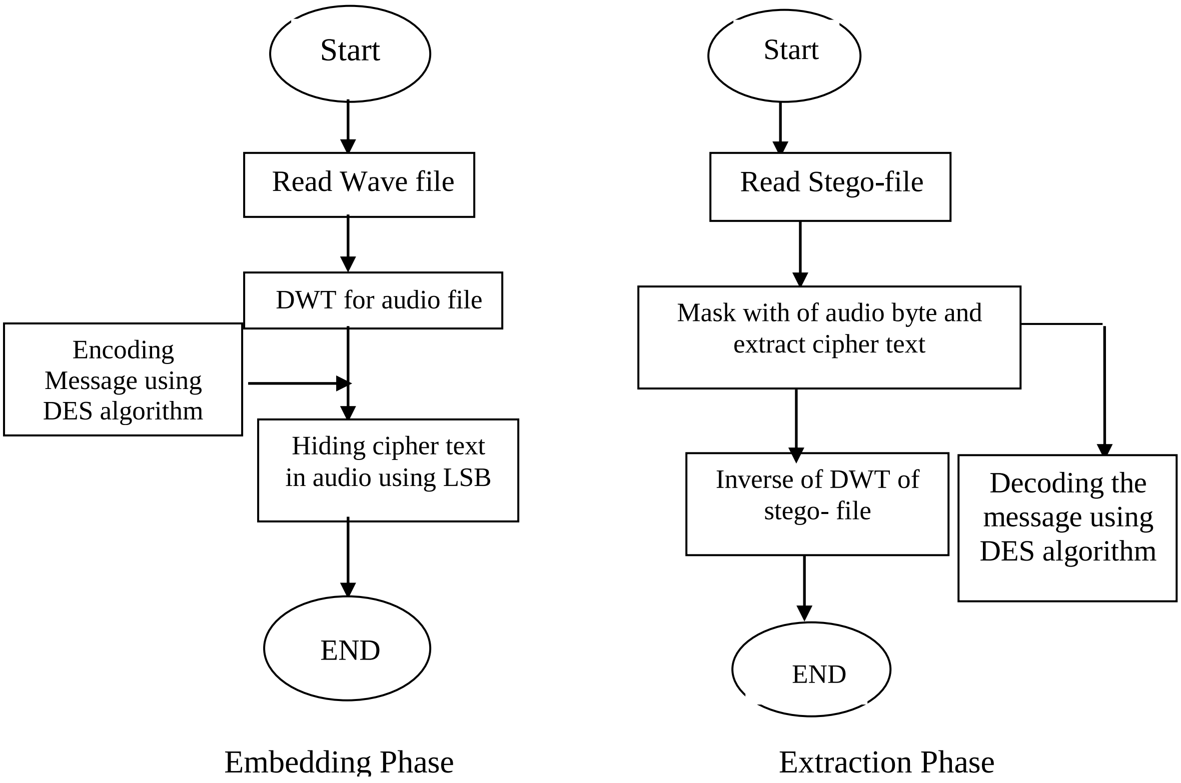
Start
Read Wave file
DWT for audio file
Encoding Message using DES algorithm
Hiding cipher text in audio using LSB
END
Start
Read Stego-file
Mask with of audio byte and extract cipher text
Inverse of DWT of stego- file
Decoding the message using DES algorithm
END
Embedding Phase
Extraction Phase

Fig. (3) The Proposed System

1. Embedding phase

The embedding phase contains, loading the wav file, transform the audio file into the frequency domain using Wavelet transform, and ciphering text message by using DES.

A. Load Wave file

Firstly, the wave file content is loaded; it consists of header and data section. Header contains information about the audio file attributes (like, sample rate, no. of channels, bits per channel ...etc), while the data section holds the values of audio samples within the wave. In this paper the number of samples are 11024 sample/sec, the number of channel is one (mono), and the number of bits in each sample is 8 bits.

B. Wavelet Transform

Wavelet transform was used as a cover to hide secret text message in frequency domain. The use of frequency domain instead of spatial domain, adds more robustness to the hiding process. Haar filter is selected for wavelet transform. The Haar Wavelet is a simplest and the fast wavelet transformation, which operates on data by calculating the sums and the differences of the adjacent elements. Only one wavelet pass is applied; which leads to two sub bands (i.e., low and high). High frequency coefficients are treated as the host for the secret bit, while the low coefficients are kept unchanged [8].

C. Encryption text Message

The encrypted text message will be hidden in Audio, encrypt by Data Encryption Standard (DES) method. At beginning converting the message into ASCII code, making the 64 bits blocks of the message, generating an encryption key, and performing permutations and logical operations to bit pattern the following steps shows the process of DES algorithm.

After encryption the text message using DES method, the message convert it into ASCII code, and transform the audio file form time domain to frequency domain by Haar wavelet transform. We take the high frequency coefficient for hiding the secret message by using the LSB (Least Significant Bit) algorithm. And after bits embedding, the audio file transformed back to spatial domain using inverse Wavelet transform.

2 Extraction Phase

The Extraction Phase contains, decrypt the hidden message, and take the inverse of wavelet transform.

2.1 Decrypt the Message

Decryption is simply the inverse of encryption, following the same steps as mentioned in 4.1, but reversing the order in which the sub keys are applied.

Results:

The performance of the proposed method was using Wave files (with specifications: PCM, mono, 8 bits/sample, 11024 sample/ sec. Peak Signal to noise ratio (PSNR) of the stego cover audio objects was used for calculating the noise, as shown in equation (1).For example, the word (GoGoogle) wanted to secret using DES.

Key: - 1100101 0100100 1001001 0011101 0110101 0101011 1101100 0011010

Input bit string: 11100010 11110110 10000010 11100110 11100110 10010110 10100110 11001110

Output bit string: 10011111 11110010 10000000 10000001 01011011 00101001 00000011 00101111

Output character string: UOU AO

$$\text{PSNR} = 10\log\frac{255^2}{\frac{1}{n}\sum_{i=1}^{n-1}(s'i-si)} \quad \ldots\ldots (1)$$

n is the number of cover audio samples.
si is the original *ith* audio sample.
s'i is the value of *ith* stego sample.

The secret message was embedding in three audio files of different sizes. Table (1) shows; the (b.wav) has getter the high PSNR (99.21) then (a.wav) lastly (c.Wav).

Table (1) The values of PSNR

The audio file	Size of audio	Number of channel	Sampling rate	The time	PSNR
a.Wav	1207220byte	2	22050	0.27	50.69
b.Wav	5554948byte	2	22050	1.2	99.21
c.Wav	595462byte	1	22050	0.27	45.66

Conclusion:

In this paper, proposed method for hiding secret text message in audio file has been applied. Encryption and Decryption techniques by DES have been used to make the security system robust, With Compression with the other methods that has been used another method for cryptography. Also using Wavelet in steganography of text in audio has made high hiding capacity and transparency with compression with other methods which used DES in time domain.

The result showed when the size of audio file is large; the PSNR value is high with regard of fixed the number of bits for secreted massage. The number of bits in secured message must be less than the half of the size audio file.

Reference:

1. Bidyut S; Kunal K. and Arun, 2013. Digital Image Encryption using ECC and DES with Chaotic Key Generator, IJERT, 2 (11):1-10.
2. Ramkumar, M. and Akansu, A. N. 2010. Some Design Issues for Robust Data hiding Systems, IEEE, 2(12):1528-1532.
3. Johnson N. F. and Jajodia S. 1998. Steganalysis of Images Created Using Current Steganography Software, in Proceeding for the Second Information Hiding Workshop, Portland Oregon, USA, 1525: 273-289.
4. Cummins J.; Patrick D.; Samuel L. and Robert P., 2010. Steganography and Watermarking, School of Computer Science, The University of Birmingham, 2(11):5.
5. Michael W., 2011. Digital Signal Processing Using MATLAB and Wavelets, Pearson publications, ISBN–81-297-0272-X 2(13):15-16.
6. ANSI3. 106, 1983. American National Standard for Information Systems-Data Encryption Algorithm-Modes of Operation, American National Standards Institute, 25:6.
7. Grabbe, J. O. 1992. The DES Algorithm Illustrated, Laissez Faire City Times, 2(28):12-15.
8. Steinbuch, M. Van de Molengraft and M.J.G, 2005. Wavelet Theory and Applications, a Literature Study, Eindhoven University of Technology, 53(7):53.

الاخفاء في الصوت باستخدام التحويل المويجي ومعيار تشفير البيانات

رشا حسين علي

علوم الحاسبات، قسم علوم الحاسبات- كلية التربية للبنات- جامعة بغداد

الخلاصة:

في هذا البحث جرى عرض اثنتان من الطرائق الجديدة لأخفاء البيانات السرية في ملفات صوتية أن الأخفاء في الصوت هو بالغ الدقة, لأن النظام السمعي للأنسان حساس جدا. الطريقة المقترحة هي اخفاء رسالة نصية مشفرة في ملف صوتي من نوع (Wav) في المجال الترددي. تضمنت الطريقة المقترحة مرحلتين هما: مرحلة الاخفاء ومرحلة فك الاخفاء او الاستخلاص. في مرحلة الاخفاء تم تحويل الملف الصوتي من المجال الزمن الى المجال الترددي باستخدام تحويل الموجة من النوع البسيط ذات المستوى الواحد ثم نختار القيم ذات الترددات العالية لاخفاء الرسالة فيه. الرسالة النصية تم تشفيرها باستخدام خورازمية (DES). واخيرا تم اخفاء الرسالة النصية المشفرة في قيم الترددات العالية للملف الصوتي باستخدام خوارزمية (البت الاقل الاهمية). الطريقة المقترحة اختبرت على عدد من ملفات صوتية باحجام مختلفة واظهرت نجاحها في اخفاء واعادة الرسالة النصية وباستخدام معادلة نسبة الضوضاء في الملف الصوتي (PSNR).

الكلمات المفتاحية:- الاخفاء في الصوت، رسالة مشفرة، خوارزمية معيارتشفيرالبيانات، خوارزمية البت الاقل اهمية، التحويل المويجي.