Hiding Encrypted Data in Audio Wave File

Firas Ali Sabir
University of Baghdad/ College of Engineering

ABSTRACT
Today at a time of globalization in which the whole planet become look like a small village and transport information through it with a push button in keyboard and at a time of huge evaluation in the digital world and for the millions of users to international net and some application importance, let us to use both cryptography and steganography as a means to protect the information from hacking and interlopers. Combinations of steganography and cryptography have been made in this paper to increase the level of security and to make the system more complex to be defeated by attackers. This paper presents a method of ciphering and hiding information into a cover of audio wave file. In the first step, the text is converted to its equivalent ASCII code. Text is scrambled using DES (Data Encryption Standard) technique according to secret key then the cipher text is embedded inside a cover audio wave file using time and frequency domain. The modeled system builds of a secret key steganographic system, which embeds certain text after scrambling into random positions inside audio wave file and the other technique used in this paper to analyze the cover audio into its frequency components is wavelet transform using Haar filter as a basis function. Tests were carried out to evaluate the performance of the modeled algorithm and results in successful hiding. From the simulation results on the time domain, it is noticed that value of Signal to Noise Ratio (SNR) will decrease as the number of bits in the audio wave file to be replaced by the message increase and noticed that the value of SNR in frequency domain is higher than in time domain, so hiding in frequency domain is better than hiding in time domain.

Keywords
Steganography, Hiding, Cryptography, Data Encryption Standard, Time Domain, Frequency Domain.

1. INTRODUCTION
Security issue is the main requirement for every system or protocol, which deals with information. There are two basic ideas to keep something as a secret:

1. The object could be changed by rules to a form that is not recognized, except for people who know these rules and everything about it such that they can obtain the original object; this is called **Cryptography** [1].
2. The object can be hidden at a secret place such that nobody will find this object except people who are familiar with the secret sender, the methodology concerned with this kind of information security is called **Steganography** [2].

This paper combines the cryptography and steganography to get a high level of security and to prevent the attackers from detecting the existence of the hidden message. In the first stage, the proposed system uses a technique of cryptography to encrypt the text by using DES (Data Encryption Standard) [3] algorithm with a secret key produced from the Gold Code algorithm [4]. The cipher text is embedded in the audio wave file by using the steganographic techniques which are Substitution technique (Least Significant Bits (LSB) technique) and Wavelet Transform. The remainder of this paper is organized as follows: Section 2 brief some review related work. Section 3 illustrates the proposed system. The testing parameters and analysis of the results will be analyzed in section 4. Finally section 5 provides the conclusions.

2. RELATED WORKS
Several researches in the field of data hiding are developed. Mohammed Majeed proposed a system for hiding audio in audio using Discrete Cosine Transform (DCT). The research is designed and implemented steganography system that provides six hiding methods with different hiding rates for hiding data into audio signal by using DCT. These methods could be classified according to the accuracy of secret data reconstruction (lossy and lossless), and to the domain for both secret and cover data during the hiding process (time and frequency) [5]. Poulami Dutta et al. proposed efficient method for hiding the data from hackers and sent to the destination in a safe manner. The proposed system does not change the size of the file even after encoding and also suitable for any type of audio file format [6]. Kriti Saroha and Pradeep Kumar Singh presented a new steganographic using Least Significant Bit (LSB) method for embedding an image in an audio file [7]. Pushpa Aigal and Pramod Vasambekar proposed an efficient audio steganography system, in which the LSB technique is used to get high data hiding capacity and low perceptibility [8].

3. THE PROPOSED SYSTEM
The proposed system consists of two main steps. In the first step the message is encrypted using Data Encryption Standard (DES). DES designed to encipher and decipher blocks of data consisting of 64-bits under control of 64-bits key. The strength of its secrecy depends on the key used for encryption and decryption. DES is asymmetric key algorithm (use the same key at sender and receiver). For more secrecy it not used directly but it considered as initial value to the random generator. So the date entered in this sequence: day, month and year. Then it converted to its equivalent binary representation

$$Y_4\ Y_3\ Y_2\ Y_1\ M_4\ M_3\ M_2\ M_1\ D_5\ D_4\ D_3\ D_2\ D_1$$

The mechanism used to generate random 64-bit key is the used of two linear feedback shift registers (gold code generator).The first LFSR of six flip flops while the second one consists of seven flip flops. Fig. 1 shows the key generation of proposed system.

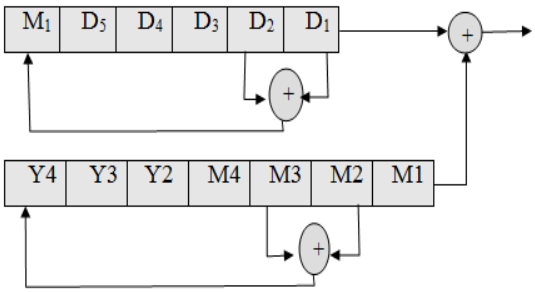

Fig 1: Key Generation used in DES.

The second step performs the hiding process. LSB substitution technique is used for hiding in time domain and wavelet transform in frequency domain. The hiding process uses the LSFR to generate the positions inside cover in which text is to be hide, this algorithm used 16 bit shift register as shown in the Fig. 2 and then take the initial states of registers and convert to decimal which perform the number of the selected position which used to hide.

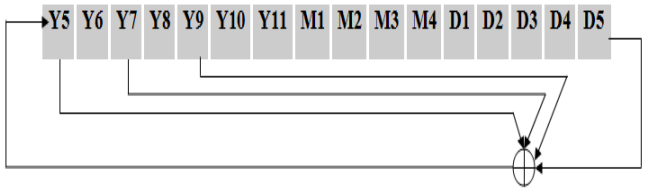

Fig 2: Random Positions Generation for Hiding.

The initial value that will result from twelve bits giving from the input date after converting to binary form as showing below:

Initial value=Y(5) Y(6) Y(7) Y(8) Y(9) Y(10) M(1) M(2) M(3) M(4) D(4) D(5)

This initial value is incremented by 50 to give the first position and the other positions are giving by the following equation:

Position (i) =initial value + 50*i ... (1)

Where (i) is the number of position (second, third… twelve).
The LSB steganography model steps that occurred at the sender side are described below:

1. Encrypt the entered secret message using DES.
2. Convert the encrypted message to binary form.
3. Read the cover audio wave file and convert it to binary form.
4. Entered date key used to choose the positions in the audio wave file to hide the encrypted message inside it, these positions must be as random as possible so the gold code is used.
5. Replace the least significant bit of each cover position by the bit of the encrypted secret message avoiding silent region.
6. For frequency domain, the audio wave file is converted to frequency domain using Haar filter for this transformation process and then the above procedure from step 1 are repeated.

To extract the encrypted message from the cover audio wave file at the receiver side, the following steps are applied:

1. Read the cover audio wave file and convert it to binary form.
2. The same entered date key that used at the sender side is used to discover the positions in the audio wave file that the encrypted message hidden inside it.
3. Decrypted the secret message to obtain the original message using DES algorithm.
4. For frequency domain, the audio wave file is converted to frequency domain using Haar filter for this transformation process and then the above procedure from step 1are repeated.

4. RESULTS AND PERFORMANCE ANALYSIS

The measurement criteria used to evaluate the performance of the proposed hiding system is SNR which calculated by applying the following equation:

$$SNR = 10 \times \log_{10}\left(\frac{\sum_{i=1}^{N} f(i)^2}{\sum_{i=1}^{N}\left(f(i)-g(i)\right)^2}\right) \quad \text{... (2)}$$

Where:

N is the size of the audio

f : represent the samples with index number i in the original audio

g : represent the samples with index number i in the stego audio

The *SNR* is often measured in logarithmic scale and the unit of measurement is called decibel (dB). Some of text files and audio files like speech, music and song were used as test samples to study the performance of the suggested system. The specifications of the tested text files (the text to be hiding) and the tested audio files (the cover) are shown in Table1 and Table 2 respectively.

Table 1. The tested text samples.

Name	Size (char)	Data Type
Text1	50	Text
Text2	500	Text
Text3	1500	Text

Table 2. The tested audio samples.

Name	Size (KB)	Type	Length	Behavior	Nature
Song	21.973	Mono	2 Min :07 Sec	Song	Low Pitch
Music	14.815	Stereo	42 Sec	Music	High Pitch
Speech	4.60	Mono	1 Min:15 Sec	Speech	-

The test strategy is to check the error between the original audio (cover without secret data, the encryption data) and the stego audio (cover containing the secret data). The two hiding methods, substitution technique and wavelet transform with Haar wavelet transform are used for testing. The SNR values when hiding **one**, **two**, **four**, **six** and **eight** bits of the encryption message in one position of **song** audio cover using substitution technique in time domain and wavelet transform technique in frequency domain are shown in Fig. 3 and Fig. 4 respectively. Fig. 5 and Fig. 6 show the values of SNR when hiding **one**, **two**, **four**, **six** and **eight** bits of the encrypted message in one position of **music** audio cover using substitution technique in time domain and wavelet transform technique in frequency domain while Fig. 7 and Fig. 8 show the SNR values when hiding in **speech** audio cover.

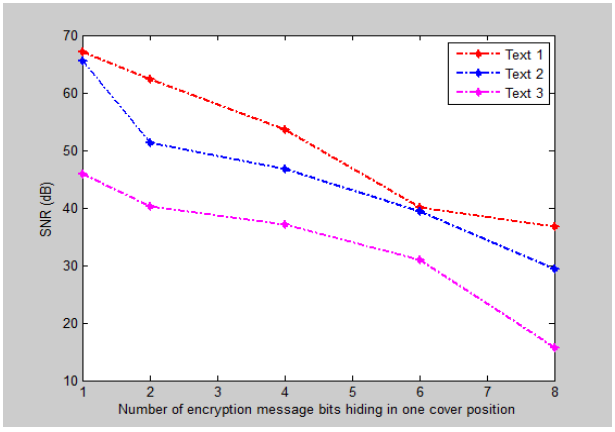

Fig 3: SNR Values of Hiding in Song Audio Cover in Time Domain.

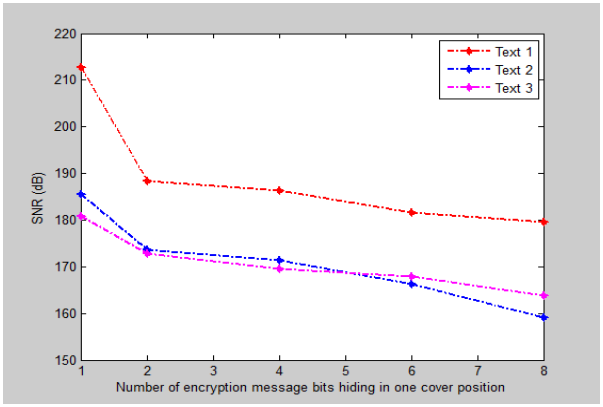

Fig 4: SNR Values of Hiding in Song Audio Cover in Frequency Domain

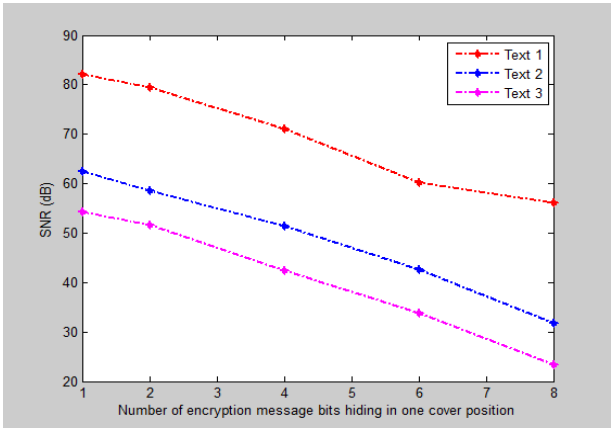

Fig 5: SNR Values of Hiding in Music Audio Cover in Time Domain.

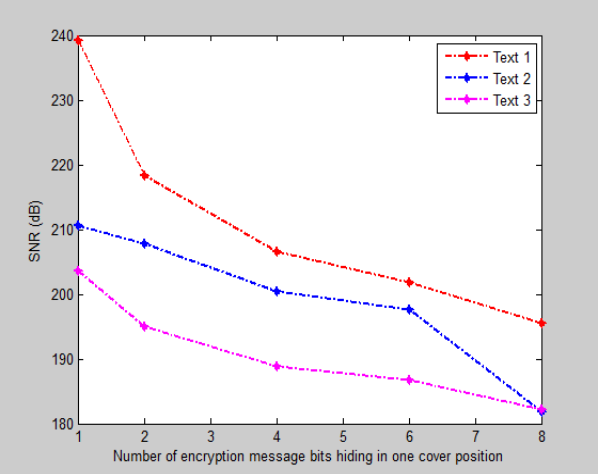

Fig 6: SNR Values of Hiding in Music Audio Cover in Frequency Domain.

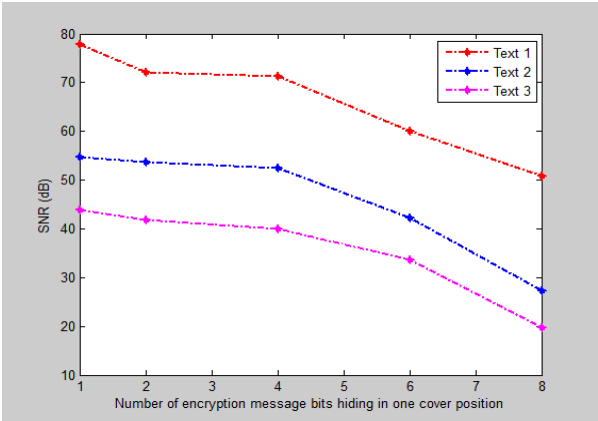

Fig 7: SNR Values of Hiding in Speech Audio Cover in Time Domain.

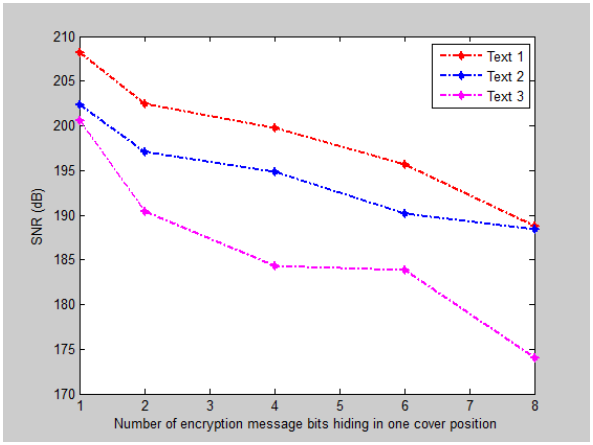

Fig 8: SNR Values of Hiding in Speech Audio Cover in Frequency Domain.

From the obtained results, it is clear that SNR in frequency domain is higher than in time domain. Therefore, hiding in frequency domain is better than hiding in time domain since in time domain it is unknown whether the position that is chosen from the random number generation algorithm may carry important information about the audio wave file or detailed information, but in frequency domain the audio wave is converted to detail and approximation region, so it is possible to choose the region which carry additional (detailed) information which is less noticeable if it is changed, so hiding in frequency domain is better than hiding in time domain. Also it is noticed that SNR will decrease when the number of bits in audio cover to be replaced by the secret message increase, SNR of hiding eight bits of secret message inside one position audio cover is less than SNR when hiding one bit. Finally when the size of the message to be hidden increases then the SNR decreases for the same type of method of hiding such as hiding one bit, SNR of hiding Text1 inside the cover is larger than SNR of hiding Text2 and SNR of hiding Text2 is larger than SNR of hiding Text3, this due to the large size of Text3 (1500 characters).

5. CONCLUSTION

The system in this paper provides a comparable level of security since it combine the steganography and cryptography techniques which makes the system more complex to be defeated by attackers. The embedding technique increase the imperceptibility property because it based on replacing each secret bit with one of the host coefficient bit (the host coefficient bit may be the same as secret bit). The proposed system with wavelet transform technique is better than hiding with substitution technique.

6. REFERENCES

[1] D. E. R. Denning, "Cryptography and Data Security", Addison-Wesly Publishing Company, 1983.

[2] S. Katzenbeisser and F. A. Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House, ISBN 1580530354, USA, 2000.

[3] W. Stallings, "Network Security Essentials: Applications and Standards", Fifth Edition, Prentice Hall, March, 2013.

[4] ALTERA, "Gold Code Generator Reference Design Application Note 295", VER.10, March, 2003.

[5] M. Majeed, "Hiding Audio in Audio Using DCT", M.Sc. Thesis, Computer Science Dept., College of Science, Al-Nahrain University, Baghdad, Iraq, 2004.

[6] P. Dutta, D. Bhattacharyya and T. Kim, "Data Hiding in Audio Signal: A Review", International Journal of Database Theory and Application, Vol. 2, No. 2, June, 2009.

[7] K. Saroha and P. K. Singh, "A Variant of LSB Steganography for Hiding Images in Audio", International Journal of Computer Applications, Vol. 11, No. 6, December, 2010.

[8] P. Aigal and P. Vasambekar, "Hiding Data in Wave Files", International Conference in Recent Trends in Information Technology and Computer Science (ICRTITCS), 2012.