Steganography in Audio Using RC5 and Rijndeal Algorithms

Asst. Teach. ISRAA S.AHMED

University of Information Technology and Communication

Computer Department, Informatics Institute for Postgraduate Studies

Baghdad- Iraq

Abstract

In this paper, method of steganography in Audio is presented to hide secret information in audio file. Keeping out date of sight in audio is a difficult task due to the extremely high sensitivity of the Auditory System. The current work deals with embedding 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. Transformation the audio file from time to frequency domain is achieved in the first phase utilizing 1-level linear wavelet decomposition technique and only high frequency is used for hiding secreted message. The text message encrypted using RC5 algorithm then encrypt the result with Rijndeal 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, RC5 algorithm, Rijndeal algorithm, LSB algorithm, Wavelet transform.

الإخفاء في الصوت باستخدام خوارزميتي RC5 و Rijndeal

الخلاصة

في هذا البحث جرى عرض اثنان من الطرائق المقترحة للإخفاء البيانات السرية في ملفات صوتية أن الإخفاء في الصوت هو بالغ الدقة, لأن النظام السمعي للإنسان حساس جدا. الطريقة المقترحة هي إخفاء رسالة نصية مشفرة في ملف صوتي من نوع (Wav) في المجال الترددي. تضمنت الطريقة المقترحة مرحلتين هما: مرحلة الإخفاء ومرحلة فك الإخفاء 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 لإخفاء الرسالة فيه. الرسالة النصية تم تشفيرها باستخدام خوارزمية (RC5) ومن ثم تشفر المسج الناتج باستخدام خوارزمية Rijndeal. 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 بأحجام مختلفة واظهرت نجاحها في اخفاء واعادة الرسالة النصية وباستخدام معادلة نسبة الضوضاء في الملف الصوتي (PSNR).

الكلمات المفتاحية:- الاخفاء في الصوت، خوارزمية RC5، خوارزمية Rijndeal،خوارزمية البت الاقل اهمية، التحويل الموجي.

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 data; such as those related to legal and medical records, credits, financial transactions, audio mails are also require to be protected from outsiders. Cryptography, or writing in codes, is a method to hide data digitally in order to maintain integrity, confidentiality and authenticity of transmitted data [1].

The term steganography has Greek origin; with Steganos, meaning hidden and graphy meaning writing. This term will therefore, refers to secret writing. It is the mixing of science and art skills to cover the presence of information and making them difficult to detect. Classified data are encoded to reformulate them and print them in a secret manner. Coupled with present communication techniques, steganography is employed to transmit secret exchanges [2].

The principle aim of steganography is to safely send; difficult to uncover, information files and to ensure drawing attention to the transmitted secret data [3].

In the field of Steganography, copyrighting audio files is made to safeguard the rights artists work. Phase & spread spectrum coding, echo hiding and least significant bit insertion, are utilized to protect the audio file data. The greatest problem facing all above techniques is the extremely sensitive human auditory system (HAS); in which a successful information covering is very hard to reach [4].

Wavelet Analysis

The wavelet transform (WT) has attracted great attention when compressing an image or processing a signal becomes the ultimate goal. WT is a zero average value limited duration waveform in which signal is segmented into scaled and shifted replica of the original. Low-frequency is used to represent the signal identity, while the high-frequency is employed to save nuance. When the high tone of our talking is removed, our voice will

slightly differ from the original, but can be understood. If, on the other hand, the low frequency tone is omitted, our spoken words will come out too fast. Wavelet transformations applied can bring back all missed parts of the original audio signal. Low tone signal is the approximated original while the high frequency one will provide the detailed signal. Because of its low energy, detail of the first level coefficients is not as important as that of the next level. The audio signal decomposition on wavelet transform is conveyed in Figure (1), [5].

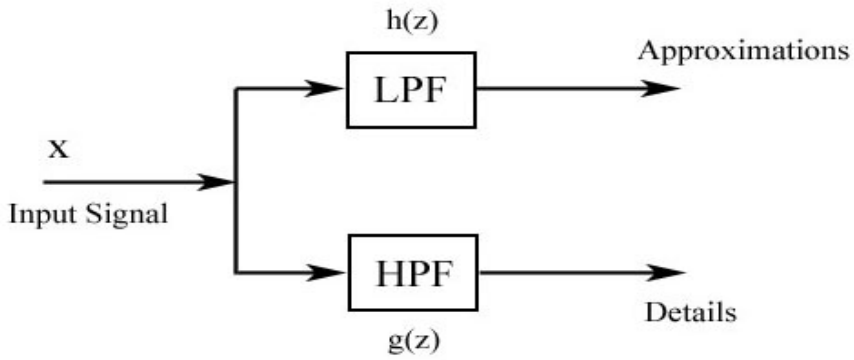

Fig. (1) Signal Decomposition

RC5

RC5 block cipher is a candidate to replace Data Encryption Standard (DES). RC5 encryption use data-dependent rotation operation to prevent differential and linear cryptanalysis [6]. RC5 is suitable and flexible for software and hardware implementation because having a variation value of block size, key length and number of rounds. RC5 have three parameters:

- ***w*:** Word size in bit. Each word consist of $u = (w/8)$ byte. Allowable w value are 16, 32, and 64. RC5 algorithm process two words in encryption and decryption, so that size of the block are $2w$ bits.
- ***r*:** The value of r determines the number of rounds used and S table size. S is the expanded key table that has $t = 2(r+1)$ words.
- ***b*:** This parameter determines the number of bytes in array of secret key $K(K[0], K[1], ..., K[b-1])$.

RC5 use three basic operation, i.e. addition modulo 2*w*, exclusive-or, and word rotation. Similarly with others block ciphers, RC5 algorithm perform key expansion session before encryption or decryption process. Figure (2) shows the steps of RC5 algorithm [7].

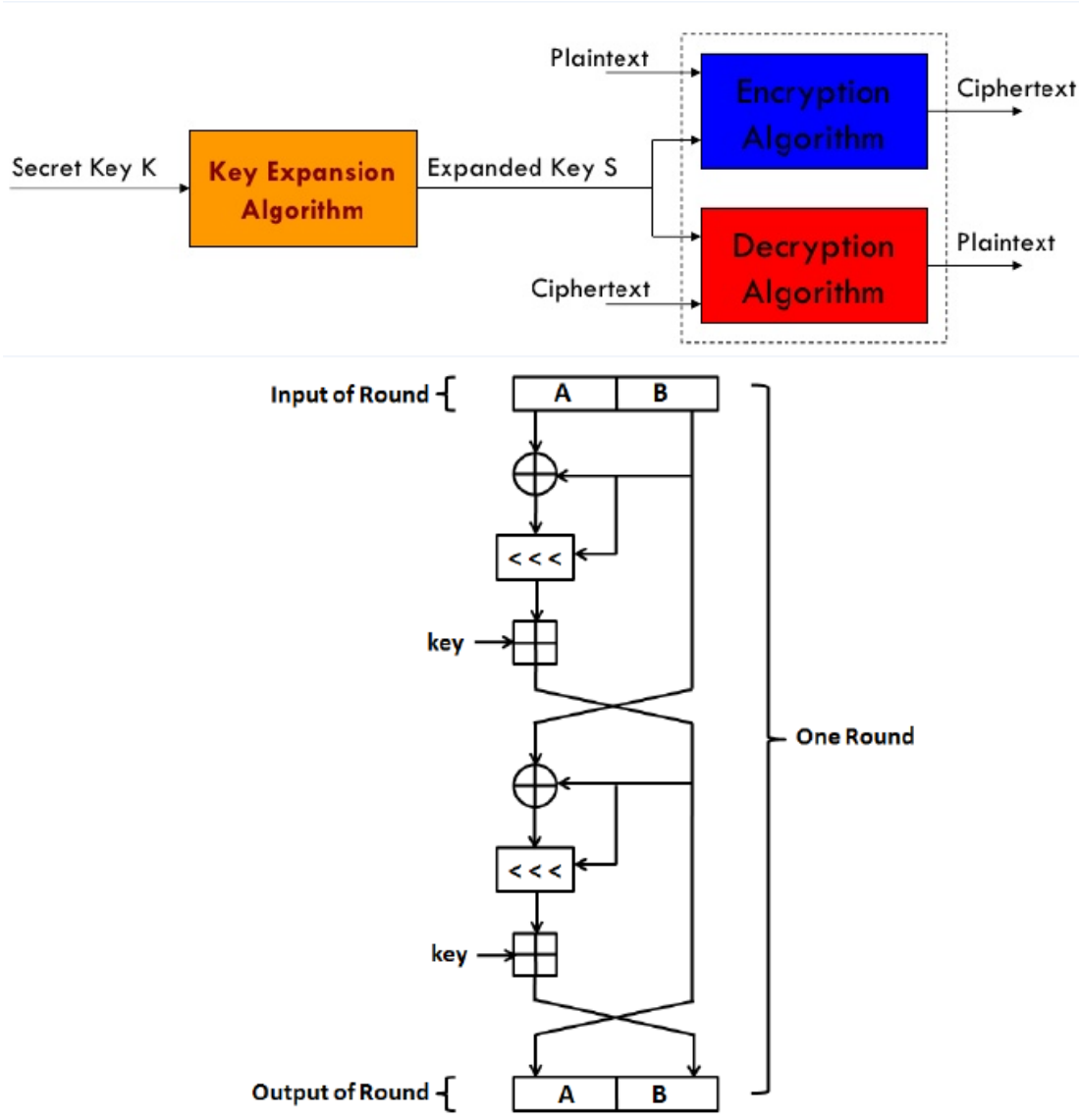

Fig. (2) The Structure of RC5

RIJNDAEL ALGORITHM

Figure (3) portrays Rijndael cipher algorithm which runs a number of transformations on a file of data for a given protocol key. This same key turns the other way round the transformations employed during decryption. Despite its limited 128-bit data blocks, the AES specification was chosen as the Advanced Encryption Standard (AES) in 2001 by the National Institute of Standards and Technology (NIST), [8].

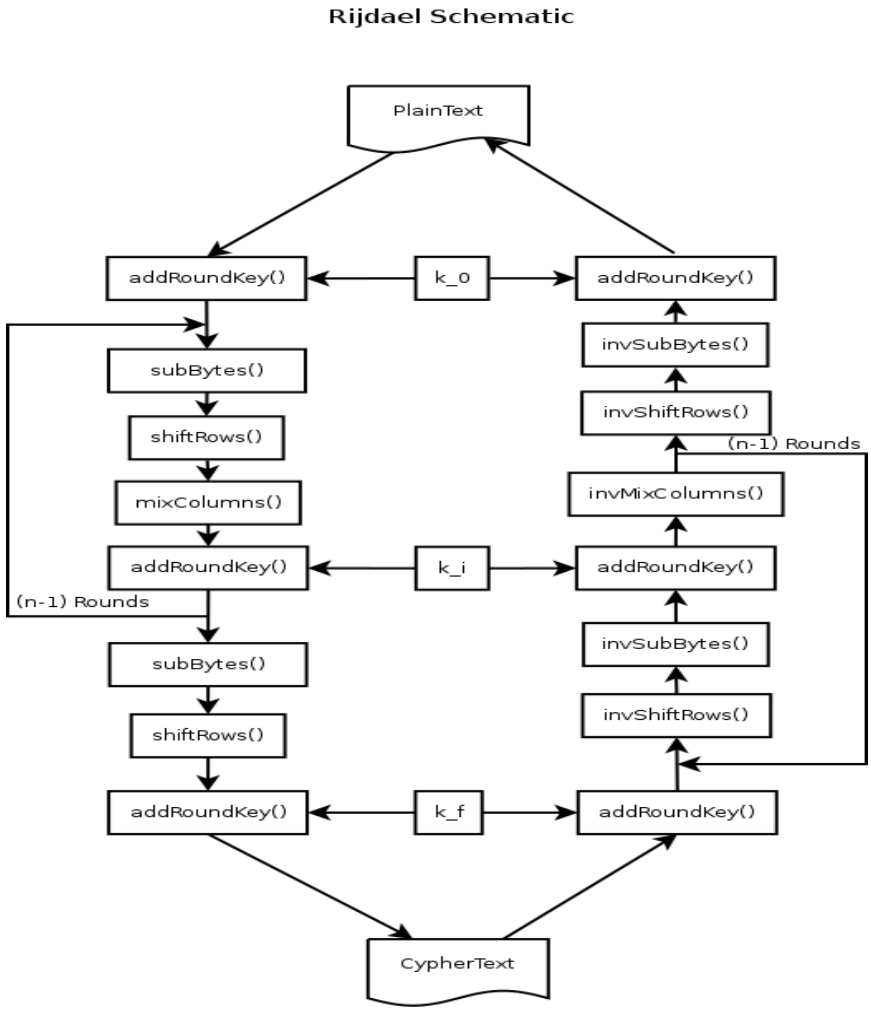

Fig. (3) The structure of Rijndeal Algorithm

The Proposed System

In this paper, a method for hiding secret text message encrypted by using RC5 then encrypted the produced message using Rijndeal for more secure, then embedding in frequency domain of audio. This method contains two phases, the embedding and extraction, as shown in figure(4).

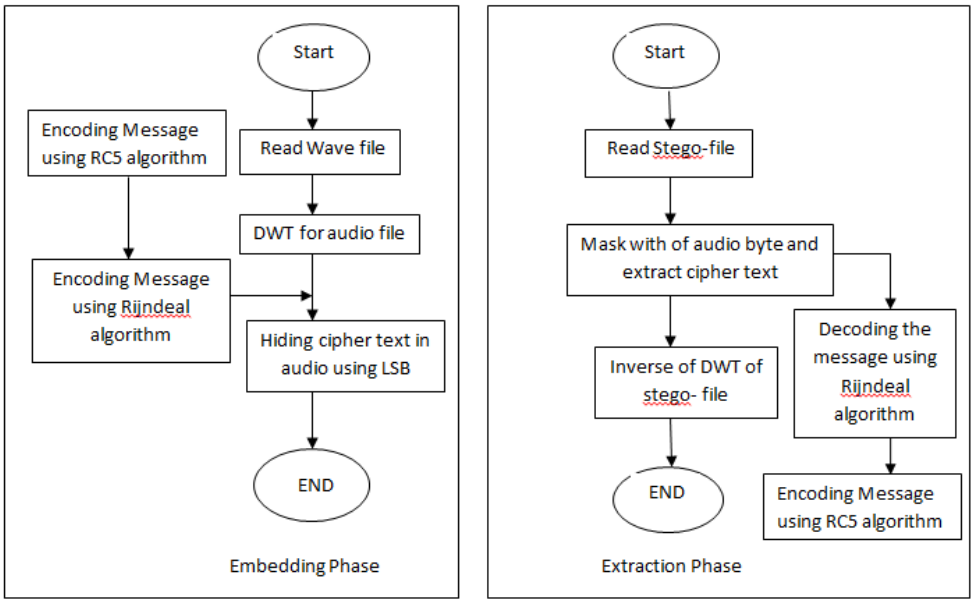

Fig. (4) The Proposed System

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 RC5 and Rijndeal algorithms.

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 are11024sample/sec, the number of channel is one(mono), and the number of bits in each sample is8 bits.

Secondly; The digital signal transformed into frequency domain to hide a secret text message on it. The use of frequency domain instead of spatial domain, adds more robustness to the hiding process. The simple and

fast wavelet Haar transformation filter is chosen to treat data by working out the sums and differences of the adjoining 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 [9].

Finally; The encrypted text message will be hidden in Audio, After encryption the text message using RC5 and Rijndeal methods, 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 was considered for hiding the secret message by using the LSB (Least Significant Bit) algorithm; after bits embedding.

2. Extraction Phase

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

Experimental 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,

Word:- computer department
Key:- university
Output RC5 :-PUcnHH5V3Nyls0IECg+0rsPweY7MH0X6
Output Rijndeal 128:-
o3byum8yqVBtmxz9ihQwU9e1wDXUyaGo++qGMDCrB4E=

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

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 (2.wav) has getter the high PSNR(89.70) then (3.wav) lastly (1.Wav).

Table(1) The values of PSNR

The audio file	Size of audio	Number of channel	Sampling rate	PSNR
1.Wav	307740byte	1	22050	55.87
2.Wav	1207220 byte	1	22050	89.70
3.Wav	807596 byte	1	22050	60.43

Conclusion

In this paper, proposed method for hiding secret text message in audio file has been applied. Encryption and Decryption techniques by RC5 and Rijndeal methods 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. 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.

Reference

[1]-BidyutSaha, KunalKabi and Arun,2013,"Digital Image Encryption using ECC and DESwith Chaotic Key Generator",IJERT, 2 (11):1-10.

[2]- M. Ramkumar& A.N. Akansu, 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, Vol. 1525: pp. 273-289.

[4]- Cummins Jonathan, Patrick Diskin, Samuel Lau and Robert Parlett, 2010, "Steganography and Watermarking",School of Computer Science, The University of Birmingham, 2(11):5.

[5]- Michael Weeks,2011,"Digital Signal Processing Using MATLAB and Wavelets", Pearson publications,ISBN – 81-297-0272-X 2(13) :15-16.

[6]- M. Y. Rhee, "Internet Security: Cryptographic Principles, Algorithms, and Protocol", John Wiley & Sons, West Sussex, 2003.

[7]- R. Rivest, " The RC5 encryption algorithm", in Lecture Notes in Computer Science 1008, edited by B. Preneel , Springer-Verlag, Berlin, 1995, pp. 86-96.

[8]- Ali.K, Mahmod. R, "A Faster Version of Rijndael Cryptographic Algorithm Using Cyclic Shift and Bit Wise Operations", International Journal of Cryptology Research 1(2), 2009, pp.215-223.

[9]-Steinbuch, M Van de Molengraft and M.J.G, 2005, "Wavelet Theory and Applications", A Literature Study, Eindhoven University of Technology, 53(7):53.