A Review of Secret Message Hiding Algorithm in Audio File

Sumit Thakur[1], Prof. Piyush Singh[2]
[1](Computer Science Engineering, RKDF Bhopal, India)
[2](Computer Science Engineering, RKDF Bhopal, India)

ABSTRACT

Flood of multimedia contents in the structure of transmitted data rapid growth of Internet users and the increasing range of data types emphasize the security problem. The data Encryption system is used for hiding data by supervised trained dictionary. It involves concealing the secret text inside the cheating text. Then cheating text is hiding in Audio file. If the cheating text is intercepted, the secret text may still be undetected. There are many reasons to hide data but most important is to prevent unauthorized persons from becoming aware of the existence of a message. Hidden message is information that is not immediately noticeable, and that must be discovered or uncovered and interpreted before it can be known. We propose a novel approach for generating cheating text and hiding cheating text in audio file this high capacity audio algorithm based on the wavelet packet transform with adaptive hiding in least significant bits. The adaptive hiding is determined depend on the cover signal strength and bits block matching between message and cover signals.

Keywords: *Steganalysis, Data Hiding data, audio hiding wavelet packet transform, least significant bit. adaptive hiding*

1. INTRODUCTION

The Internet has revolutionized the modern world and the numerous Internet based applications that get introduced these days add to the high levels of comfort and connectivity in every aspects of human life. The expansion of data transmission through Internet made the process of improving data protection inevitable. The broadband Internet access has enabled a bigger flow of audio content through this network. When the data protection is based only on our system, it's often related to LSB technique. The Difference between the original images and the one with data embedded in still evident. This difference tends to be decreased, because of the signal for cryptanalyst's and hackers. There have been some improvements by altering the modified (embedded) picture with a substitution matrix [1, 2]. The unwanted effect is increased the complexity of computational system. Strengthening the proposed solutions with an existing cryptographic algorithm Advanced Encryption Standard can partially improve this unwanted effect. Because AES has a *K* level security from the aspect of cryptography they offered increase in security of data transfer with the combination of the AES algorithm and steganography [1, 2], The process of receiving the message and the removal of the protection is, however, equally important. Looking at the complexity and implementation, this processes are considered symmetric. Audio hiding file system is a useful means for transmitting convert battlefield information via and innocuous cover audio signal. Audio is an important communication way for people, and therefore is a convenient medium secure communications. In order to discriminate stegno audios from clear normal ones, that embed random data into a (possibly) stegno audio file by using a certain steganography tool. It was found that the variation in some statistical features of audio file is significantly different between clear audio files and stegno ones which already contain hidden messages embedded by the same tool. In this paper, that can detect the existence of hidden messages, and also identify the tools used to hide them.

IJERT

The other Peer-to-Peer (P2P) audio services provide vast opportunities for covert communications by slightly altering the binary sequence of the audio signal with existing system tools, after converting communication channels may be relatively easy to establish. Moreover, the inherent redundancy in the audio signal and its transient the unpredictable characteristics imply a high hidden capacity [3]. This is further aided by the fact that the human ear is insensitive to small distortions in the audio signal. Information hiding in digital documents provides a means for overcoming those problems. Depending on what information in which form is hidden in the audio, one can distinguish at least two types of data hiding schemes: non-robust, undetectable data hiding, and robust audio watermarking. In the first case, a digital audio serves as a container for a secret message. In the second application, robust audio watermarking, a short message (a watermark) is embedded in the audio in a robust manner. By robustness we mean the ability to survive common audio processing operations, such as lossy compression, filtering, noise adding, geometrical transformations, etc. Such robust watermark can be obviously used for copyright protection, fraud detection (verification of audio integrity), authentication, etc. At this point we emphasize that cryptographic authentication protocols cannot solve all the issues related to authentication.

Here we also encrypt textual data in cipher text because of many researchers have made a great effort on developing cryptosystems, which is difficult and complicated to reverse from the cipher text into the original data. However, cipher text usually seems meaningless as it is encrypted. When a hacker intercepts this meaningless data [4], he knows that it has been encrypted. In other words, as soon as he gets the encrypted data, he knows that he had obtained an important message. There is an old saying "Trying to cover up a misdeed, one only makes it more conspicuous". Therefore, a better approach to protect the message may suggest us to choose a different technique for concealing Data Hiding and Encrypting Scheme.

Cryptographic authentication deals with authenticating the sender of the message over insecure channels. However, once the message (audio) is decrypted, the audio is unprotected and can be copied and further distributed. Unlike classical paintings that can be studied for authenticity using sophisticated experimental techniques, a digital artwork is just a collection of bits. A visible signature in the corner of the audio can be easily replaced or removed with advanced audio processing software packages, such as Photo-Shop. Additional information in the audio file header can be erased or changed as well. In other words, any attempt to authenticate the digital audio file by appending information will fail. The embedded information will be transparent to the human ear, but it should be detectable using a sophisticated algorithm provided a secret key is available [5] and [6] and [7].

2. LITERATURE SURVEY

This paper presents [8] a double layered secure data transfer technique is used Cryptography and Audio Steganography for mobile network. Firstly, the characters of chipper text data are converted to bit values and are encrypted by XOR operation using a Symmetric key. They using a secret key-box, it is again scrambled and then divided into 2bit blocks. These blocks from MSB are replaced by the Left Significant two bits of each byte of cover audio bit stream. they used trick for this steganography method hides behind logic of selecting the next byte of the cover audio. And additive method with a key constraint is used as the proposed algorithm. After replacing by the secret bit blocks, the byte of the cover audio is divided into two nibbles and added overlooking the carry and is converted to decimal values. The second and third bits are taken together and the decimal value is considered as key constraint. Both the values are added and next byte is chose after counting that numbers of byte positions. The technique presented this paper has overcome many of the limitations like selection of chipper text size and cover audio format, noise removal etc. that helps the user to transfer data through mobile network in a more secured and efficient way.

In the previous methods, mainly the wav files were used. Also the chipper text file size was limited. But, in our proposed algorithm, not only wav or mp3 can be used but also any kind of audio file can be used. The main advantage in this audio steganography technique is that it is very hard to find out the interferences when we hear the stego audio file. Not only the used steganography technique, but also a strong cryptography technique that is used here makes this double-layered method a hard breakable one. So, according to the previous studies and proposed method provides an efficient technique for the users who want to send secret data over wireless network concealing from the eavesdroppers.

In this paper Confused Document Encrypting Scheme [9] is a technique for data hiding. It involves concealing the secret text inside the cheating text. If the cheating text is intercepted, the secret text may still be undetected. This study focuses on reducing the amount of data transmission in delivering confused documents. They can use any article on the internet as a cheating text. The sender only needs to transmit the encrypted Uniform Resource Locator (URL), and then the receiver can follow the URL and download the cheating text. This avoids transmitting large amounts of cheating text, which is a major drawback of traditional confused document encrypting schemes. In this paper, they proposed a new approach which can improve existing confused document encrypting schemes by reducing their transmission overhead, and thus make it suitable for wireless environment with low data rate.

To reduce the overhead of cheating text transmission, the sender only need to send an encrypted URL, and the receiver can follow the URL to get the cheating text. This method greatly reduces transmission requirements. For example, the sender can only send a 60-byte URL, and the receiver can obtain a cheating text as large as 30,000-40,000 bytes from that. This is very useful in wireless environment with low data rate. Even a mobile phone using GPRS can easily apply this approach to send out a secret message.

This study certainly reduces the transmission overhead, and reduces bandwidth consumption to make this method suitable for mobile environment due to. For Chinese text in Big5 code, this method demonstrates good performance with 50% overhead reduction. It would be interesting to investigate its behavior by applying this method on other languages with difference character sets.

In this research paper, 2011, Haider Ismael Shahadi et. al.[10], they propose a new high capacity audio steganography algorithm based on the wavelet packet transform with adaptive hiding in least significant bits.

IJERT

The results show that message can be embedded up to 42 % of the total size of the cover audio signal with at least of 50 dB signal to noise ratio.

The following four main stages are repeated to hide each secret message segment in one cover segment:

a. Cover Signal Decomposition and Preparing Stage

Each segment of the input audio cover signal is decomposed using L-levels of Haar DWPT to obtain 2^L signals one represents the approximation coefficients signal and the others represent details coefficients signals. Each one of the produced signal has length of $Z/2^L$samples. They select 2^L-2 from the details signal starting from the highest frequency component for embedding of the secret message.

b. Key Generating and Secret Message Embedding Stage

The preprocessed message segment (MP) that has size of M_xN and the matrix of embedding positions contents that has size W_xM are fed to the bits block matching process. In the bits block matching process, the bits blocks of MP and EPC matrix are compared to compute matching between each bits block (row) of MP and whole blocks (rows) of EPC to obtain the blocks matching matrix BM which has size of M_xW.

c. Stego-Key Embedding Stage

Because of the arbitrary distribution of the message blocks in embedding process in the previous section, the recovery algorithm of the proposed scheme will need stego key and message size to extract the message blocks from the stego-signal. Therefore, the stego-key with the message size will embed in the lowest frequency details signal ($D_2{}^{L}$ -1). They choose this signal to embed the stego-key because it has maximum power between all other details signals and that make the stego-key more resistance against distortion or lost.

3. PROPOSED TECHNIQUE

In this paper text documents are considering, where each document consists of an ordered list of sentences [11], and each sentence consists of an ordered list of words. each word treat as contained in the text as a Scrt_text associated with its tag Document, including *noun* (n.), *verb* (v.). For example, the word “are” contained in the text is depicted by (v.), where (v) is the Scrt_text of “are”. Without loss of generality, here we create a dictionary and simplified the tag document for denoting a generalized word. The generalization relation between two words having the same tag document, which is a partial relation such that:

let w_1 = (Scrt_text $_1$|doc$_1$) and w_2 = (Scrt_text $_2$|doc$_2$),
We have that w_1 _ w_2 implies Scrt_text$_1$ = Scrt_text$_2$ A *vocabulary*, denoted as V = {w_1,w_2, . . . ,w_n}, is a collection of a limited number of distinct words.

A *phrase* is an ordered list of words, denoted as
s = w_1w_2 ……..w_k.

A phrase can also contain generalized words. Within context of mining [12, 13], sequence patterns a word is an *item* and a phrase is a *sequence*.

A *sentence* is a *grammatical complete* phrase, denoted as s#. A *document* is a set of sentences. Paper not concentrates in the order of the context of sequence data mining though the document which is logically an ordered list of sentences. Moreover, in the same context, a document can be generalized to be a set of phrases.

Data-1“The actors in this film are all also very good. This is a good film without big budget sets. Very good sound, picture, and seats.”

Example-1 Data-1 contains 3 sentences. If paper considers only the nouns, verb, contained in the data, Data-1 corresponds to a document Doc1

After apply cheating text algorithm:-

“the actresses in this film are all also very bad. this is a bad film without small budget sets. very bad sound, picture, and seats.”

On the other hand, importing the tags document into the data model it makes possible to focus on specific part of text [14], such as for building text class descriptors by nouns.

3.1 Encryption

Step 1: Use the cheating text to generate the Index of Words (IOW). In this type dictionary, each row stores a noun word and verb word, all word index of its occurrence in the cheating text [11].

Step 2: Using the IOW and the plaintext, paper can obtain a plaintext file. For each Word in plaintext, we look up the corresponding row in dictionary and choose a word from the row. The randomness here is significant, because it can improve the degree of safety.

Step 3: Encrypt the plaintext file with the public-key cryptography with any ciphering algorithm can be used, such as the International Data Encryption. After generation of cheating text hiding data inside Audio files the technique usually used is low bit encoding which is somewhat similar to LSB that is generally used in Images. Spread Spectrum is another method used to conceal information inside of an audio file. This method works by adding random data to the signal the information is conceal inside a carrier and spread across the frequency spectrum. The thing that makes this method of concealing information inside of audio files better than other methods is that it can actually improve the sound of the audio inside an audio file. There are some major audio hide algorithms are available like Low-bit encoding, Phase encoding, Spread spectrum coding and Echo data hiding.

3.1.1.1 Low-bit Encoding

Low-bit encoding [15], the binary version of the secret data message is substituted with the least significant bit (LSB) of each sample of the audio cover file. Though this method is simple and can be used to embed larger messages, the method cannot protect the hidden message

IJERT

from small modifications that can arise as a result of format conversion or lossy compression.

Phase Coding

Phase coding is based on the fact that the phase components of sound are not as perceptible to the human ear as noise [16]. Message bits are encoded as phase shifts in the phase spectrum of a digital signal.

This leads to inaudible encoding in terms of the Signal-to-Perceived Noise Ratio (SPNR) and the secret message gets camouflaged in the audio signal, not detectable by the Steganalysis methods based on SPNR.

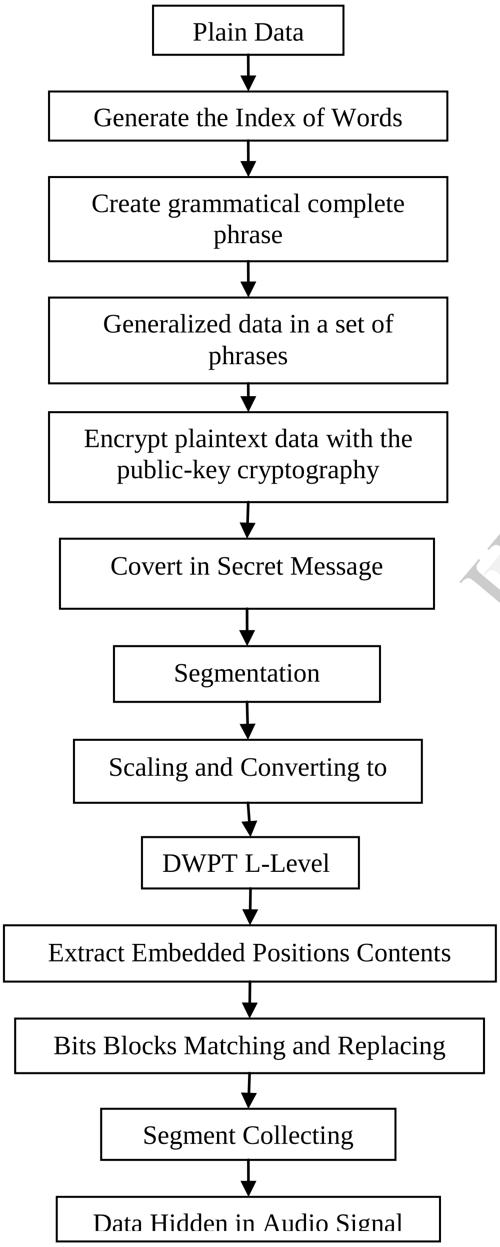
Plain Data
Generate the Index of Words
Create grammatical complete phrase
Generalized data in a set of phrases
Encrypt plaintext data with the public-key cryptography
Covert in Secret Message
Segmentation
Scaling and Converting to
DWPT L-Level
Extract Embedded Positions Contents
Bits Blocks Matching and Replacing
Segment Collecting
Data Hidden in Audio Signal

Fig. 1. Proposed Embedding algorithm

The receiver is mandated to know the message length in order to use DFT and extract the embedded message from the cover signal. A characteristic feature of phase coding is the low data transmission rate owing to the fact that the secret message is encoded only in the first segment of the audio signal. On the contrary, an increase in the length of the segment would have a ripple effect by altering the phase relations between the frequency components of the segment; thereby making detection easier.

4. CONCLUSION

In this research paper proposed algorithm first we taken plain data than convert it in cheating data after hiding data in audio signal to hide data. There are many reasons to hide data in audio signal but important is to prevent unauthorized persons from becoming aware of the existence of a message. The arbitrary results of the block matching generate an arbitrary key for embedding process, and cheating data increasing the security of massage information in the proposed algorithm. Audio data hiding can also be used in corporate world. Hiding data can also be used in the non-commercial field to hide information that keep data private. Terrorists can also use data hiding to keep their communications secret and to coordinate attacks. Another advantage for the proposed algorithm is the reconstruction of the actual secret messages does not require the original cover audio signal and therefore, the cover signal can be any recorded audio by the hiding side. And implemented using a Matlab tools.

IJERT

5. REFERENCES

[1]. A. Brazil, Path Relinking and Aes Cryptography in Color Image Steganography, M. Sc. Dissertation, Computer Institut, UFF (avaiable at http://www.ic.uff.br/PosGraduacao/lista_dissertacao.php?ano=2008

[2]. A L Brazil, A Sanchez, A Conci, N Behlilovic « An Hybrid of Genetic and Path Relinking Algorithms for Steganography" , , Proceedings of 53st International Symposium ELMAR 2011, pp. 285, Zadar, Croatia.

[3]. Er. Niranjan Singh and Dr. Bhupendra Verma, "Quality and Distortion Evaluation of Audio Signal by Spectrum" *International Journal of Computer Science and Security (IJCSS)*, Volume (6) : Issue (1), PP 629-636, 2012.

[4]. F. Cayre, O. Devillers, F. Schmitt, and H. Maıˆtre, "Watermarking Triangle Meshes for Authentication and Integrity," INRIA Research Report RR-5223, June 2004..

[5]. Masoud Nosrati, Ronak Karimi and Mehdi Hariri, "An introduction to steganography methods", *World Applied Programming, Vol (1), No (3), August 2011*, pp.191-195.

[6]. Mohammed Salem Atoum, Mamoun Suleiman Al Rababaa, Dr. Subariah Ibrahim, Osamah Abdulgader Ahmed, "A Steganography Method

Based on Hiding secrete data in MPEG/Audio Layer III", *IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.5*, May 2011, pp 184-188.

[7]. M. L. Mat Kiah1, B. B. Zaidan, A. A. Zaidan, A. Mohammed Ahmed1 and Sameer Hasan Al-bakri, "A review of audio based steganography and digital watermarking", *International Journal of the Physical Sciences Vol. 6(16),* 18 August, 2011, pp. 3837-3850.

[8]. Saswati Ghosh, Debashis De and Debdatta Kandar," A Double Layered Additive Space Sequenced Audio Steganography Technique for Mobile Network", *2012 International Conference on Radar, Communication and Computing (ICRCC),SKP Engineering College, Tiruvannamalai, TN., India. 21 - 22 December, 2012. pp.29-33.* 978-1-4673-2758-9/12/$31.00 ©2012 IEEE.

[9]. Tzu-Jung Yao and Quincy Wu, On the Study of Overhead Reduction for Confused Document Encrypting Schemes, MelT 2010, 201 0 IEEE.

[10]. Haider Ismael Shahadi, Razali Jidin, "High Capacity and Inaudibility Audio Steganography Scheme", *7th International Conference on Information Assurance and Security (IAS),* IEEE 2011.

[11]. H. Schmid. Probabilistic Part-of-Speech tagging using decision trees. In NeMLaP, 1994.

[12]. R. Agrawal and R. Srikant. Mining sequential patterns. In ICDE, pages 3–14, 1995.

[13]. S. Jaillet, A. Laurent, and M. Teisseire. Sequential patterns for text categorization. Intelligent Data Analysis Journal, 10(3):199–214, 2006

[14]. R Weis and S Lucks, ―Cryptographic Hash Functions-Recent Results on Cryptanalysis and their Implications on System Security, 5th System Administration and Network Engineering Conference, pp 15-19, 2006.

[15]. R. Sridevi, A. Damodaram and S.V.L. Narasimham, "Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key with Enhanced Security," *Journal of Theoretical and Applied Information Technology*, vol. 5, no. 6, pp. 768 – 771, June *2009*.

[16]. W. Bender, D. Gruhl and N. Morimoto, "Techniques for Data Hiding," *IBM Systems Journal*, vol. 35, no. 3, pp. 313 – 336 ,1996.

IJERT