SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM

TNC TRANSACTIONS ON NETWORKS AND COMMUNICATIONS

VOLUME 5, NO. 6
ISSN: 2054 -7420

Whisper: A High Capacity File Encrypting and Hiding Method in an Audio File.

[1]Mohammed Aldarwbi, [2]Talal Al-Kharobi
[1,2] Computer Engineering, King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia
m.aldarwbi@gmail.com; talalkh@kfupm.edu.sa

ABSTRACT

The advance of internet and multimedia allows for tremendous transferring of digital media data and the percentage of time that users spend in online activity and exchanging important information is increasing day by day. Besides that, the simplicity in editing and transmitting the files, makes them vulnerable for stealing or disrupting. Therefore, it is of utmost importance to find an effective way for sending the sensitive information without being noticed by the eavesdroppers or hackers. Cryptography and Steganography are considered the main protection techniques used against eavesdroppers or hackers. Securing the transmission of the sensitive information over the internet and the publicly available media is essential. Intercepting the transmitted information over internet in any form - text, data, voice, image or video should be denied or at least made it harder by encrypting them or hiding them within any cover media. The need for an innovative approach to secure the personal information is increasing dramatically especially by the organizations and governments as they exchange a highly sensitive information. In this work, beside using the most common used encryption methods for encrypting the hidden file and the key, a novel idea for hiding the required information is proposed. Unlike the proposed approaches in the literature, **Whisper** hide two bytes at a time. **Whisper** finds the unheard samples and hide two bytes in them where each byte is placed in a different channel.

Keywords: Steganography, File Encryption, File hiding, Audio Steganography.

1 Introduction

Due to huge amount of information exchange in digital world, it is necessary to secure the information. So, the communication made must be secret. The need for secured communication introduces the concept of steganography. Steganography is an art of hiding the transmitted secret information over internet to provide data confidentiality. The secret information may be text, image and audio file. But there are different steganographic techniques available. In this paper we focus on digital audio steganography which is an efficient way to hide data as audio files are one of the most filetypes used over internet and it provide a higher hiding capacity.

Along with the increase of internet development, new types of threats are emerged. The transmitted documents over internet could be manipulated or intercepted by the attackers. Thus, sending a sensitive piece of information to the other parity over the internet is not secure any more. The emerging security

DOI: 10.14738/tnc.56.3766
Publication Date: 09th November 2017
URL: http://dx.doi.org/10.14738/tnc.56.3766

and privacy issues make it necessary to find an appropriate way to protect the sent sensitive information. Due to the aforementioned reasons the field of steganography got a new lease of life. Steganography, a Greek word which means secret writing, is the art of science in which secret message is hiding in different files types such as image, audio, text, or video. One of Steganography types is using audio file type as stego-medium. In audio steganography system, secret messages are hidden in a digital sound. Hiding the secret message in digital audio is more difficult than hiding it in other media, such as digital images or videos. The hidden message is embedded within the audio file either by inserting it to the original in the form of signal noise or by slightly altering the binary sequence of a sound file.

Figure. 1: Steganography System.

It is easy to use any encryption method to protect the transmitted information, but if the hacker noticed an encrypted information is transmitted they may destroy it in its way and make it useless. Encryption is a solution for protecting the information but sometimes we need to transmit data without being noticed. So that, steganography is best way to hide the required data within any media file type. Steganography gives the open environment systems the required privacy of information. In [1], an audio steganography method is proposed along with encryption.

In this paper a new approach for hiding information within an audio file is presented. Audio files are one of the most transmitted file type in the internet so we choose it hide in it. Audio steganography provides the user the ability to conceal information within audio files and transfer across the internet it to the other users. The hidden information is encrypted first using AES algorithm and the key of AES is encrypted using the public-key of the receiver.

2 Related Work

Hiding secret information in digital audio file is much more difficult than hiding it in other media, such as digital images. In the literature the secret message is hidden by altering the binary sequence of a audio file. The exist approaches are either powerful techniques that utilize a powerful signal processing methods to hide the secret message or simple techniques that insert the information in form of noise or echo. All the proposed technique in the literature hide the secret message bit by bit. The successful hiding technique must adhere the following rules:

- The hidden message should be undetectable.
- The stego file should display no properties that flag it as a suspicious.
- The added data should maintain the integrity of the cover file.
- The retrieval of the concealed message should be guaranteed and easy by the receiving parity.

2.1 Audio Steganography

The existing audio steganography methods can be classified into the following.

2.1.1 Least significant bit(LSB):

It is one of earliest methods used in steganography. This method is used to hide information not only in audio file but in any other file type. It is used in many published work in the literature such as [2–6]. The LSB in some bytes of the cover file is replaced by a sequence of bits containing the hidden message. LSB main advantage is the low complexity of the algorithm either in hiding the information or in extracting them. It considers an effective technique where the substitution of the least significant bit does not cause significant quality degradation. Because of the very deterministic way in embedding the hidden data, an attacker can remove the entire LSB plane and extract the uncovered message.As shown in the figure(2), the message hi is converted into ascii h=01101000,i=01101001 and placed at the least bit of the original message.

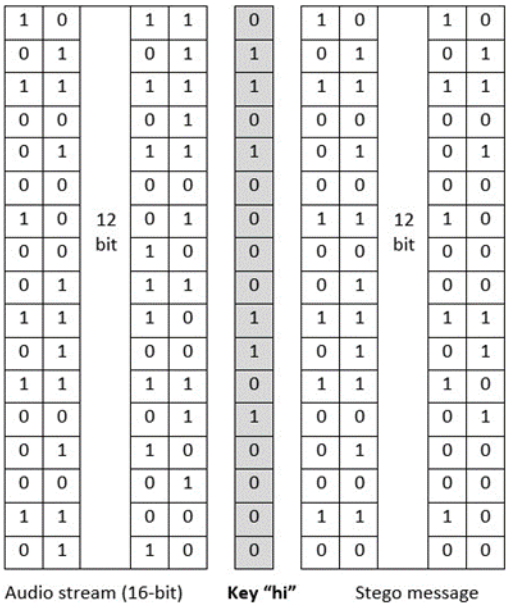


Figure 2: LSB example.

2.1.2 Parity bit Coding:

This method breaks the signal down into a totally separated samples called sample regions and decode the parity bit of each sample with a bit from the secret message [7]. The parity bit is used to hide the data on it only if it matches the secret bit to be encoded otherwise it flips to use the least significant bit. It provides more choice to the sender for encoding the secret message and the signal can be changed in a more unobtrusive manner. This method share the same disadvantage with LSB which is that the coding is not robust in nature.

2.1.3 Echo data hiding:

The resonance added to the host audio is called echo. Using the same term, echo hiding is done by representing the secret information as a resonance and add it to the cover audio file. This method solve the issue of sensitivity of the Human Auditory System (HAS) towards the additive nose [8]. The delay between watermarked message and the original audio file is small enough to not be perceived by the HAS as an added echo. Both the watermarked data and the original audio share the same statistical and perceptual characteristics. Technically, by varying the three main parameters of the echo: offset, initial

amplitude, and decay rate, the data is then hidden and not audible. Echo hiding drawback that restrict its related application domains is the limitation of induced echo size. Only one bit of the data could be encoded when only one echo is produced from the original signal. Dividing the original message down into blocks precedes the decoding process then the divided encoded blocks are concatenated together to create the final signal.

2.1.4 Hiding in Silence Intervals:

This method of hiding information is mainly focus on speech signals not any type of audio files. It identifies the number of samples in each silence intervals of speech and change them to hide information [9]. The speech samples will not be interpreted as silence intervals and vice-versa. Usually, using this method of hiding they ignore the first and last added intervals in data hiding and retrieval for no apparent reason. It has two main shortcomings, it hide only one bit in a single silence interval , and it cannot hide one or two bits individually they hide group of bits as a block instead. To hide a group of bits as a single block it is required to find a set of neighboring silence sample intervals.

2.1.5 Spread spectrum:

Spread spectrum hiding method encodes the watermarked message as a binary sequence which sounds like nose and only using the correct key the receiver can recognize the hidden message [10]. To hide the required information in MP3 and WAV signals spread spectrum apply the conventional direct sequence spread spectrum (DSSS) technique.

2.1.6 Tone insertion:

It relies into frequency masking property. Audio masking is the effect by which a low but audible tone becomes inaudible in the presence of another louder audible tones [11].the presence of a stronger tone is used to mask a weak pure tone. This property of inaudibility is used in different ways to embed information. The faint tone will not be perceptible, if it lies in the critical band of a louder tone. "By inserting tones at known frequencies and at low power level, concealed embedding and correct data extraction are achieved. The hidden information is imperceptible if a listener is unable to distinguish between the cover- and the stego-audio signal" [11]. This method can resist to attacks such as bit truncation and low-pass filtering.

Tone insertion suggests a pair of tones frequencies f0 and f1 o embed one bit in an audio. The two frequencies power level (f0 & f1) is set to a known power ratio of each audio frame pi where: i = 1; :::n and n is the frame number.

2.1.7 Amplitude coding:

According to [12], S¸"HAS characteristics depend more on the frequency values as it is more sensitive to amplitude components. Following their stated principle they pro-ˇ posed an algorithm that embeds data in the speech spectrum while controlling the distortion of the cover-medium and ensuring the hidden-data security". The payload (hidden information) could be encrypted, compressed or even groups of data (parameters of speech recognition ,MP3, LPC, AMR, CELP, etc).

2.2 Encryption

In this work we use two well known encryption methods which are Advanced Encryption Standard (AES) and RSA. AES is used to encrypt the hidden file and RSA is used to encrypt the key of AES.

According to Wikipedia "AES is a symmetric-key block cipher algorithm and U.S. government standard for secure and classified data encryption and decryption". The algorithm was developed by two Belgian cryptographer Joan Daemen and Vincent Rijmen in [13]. AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits.

Public key algorithm can be defined as a steganography system that uses a public key and a private key to secure the communication between the parties [14]. Private-key has a direct mathematical relationship. Public key is used during the encoding process and private key can decipher the message. Figure (3), illustrate how public-key algorithm works.

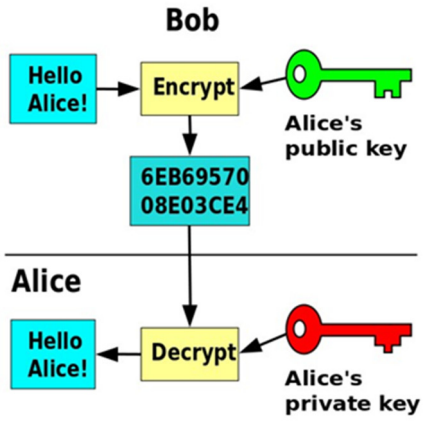


Figure. 3: Public-key cryptography.

3 Proposed Work

Audio files are one of the most transmitted file type over the internet so we choose it hide in it. Audio steganography provides the user the ability to conceal information within audio files and transfer across the internet it to the other users. Actually, hiding information in an audio file should be unnoticeable and the file size should be the same. To do so, we propose a novel idea to hid information in an audio file without being noticed.

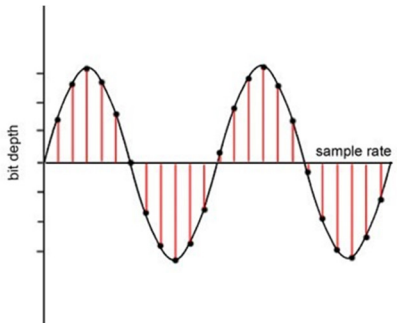


Figure 4: Sample rate.

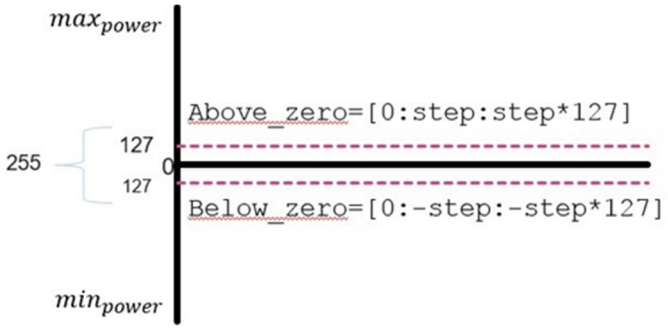
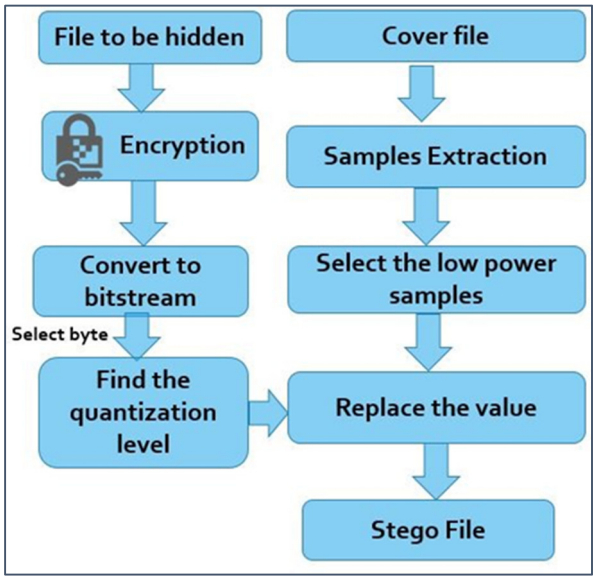


Figure 5: The selected quantized levels

The analogy signal is taken in order and converted into digital form by dividing the signal into samples which is called sample rate as shown in figure (4). Bit-depth or bit-resolution is the number of bits that are used to store each sample digitally. The common used bit-depth are 16-bit,24-bit, and 32-bit. We assume that the bit-depth of the cover file is at least 24-bit. To store the value of the sample value is converted into a quantization level. The total number of quantization levels based on the bit-depth which equal 24bit−depth. From this huge number of samples, we pick only those samples that there level of power is low (ie: from 24bit−depth quantization level we pick only 256 level which are near to zero as shown in figure (5)). Each step between the quantized levels is computed using equation (1).

$$step = \frac{max_{power} - min_{power}}{numberoflevels} \quad (1)$$

In each sample there are two channels of sound, therefore we could store two bytes at a time. Beside hiding the information in unheard samples, the hidden file and its information is encrypted. Figure (6) shows how our approach hide the information and figure (7) shows the recovery process. Hiding process is divided into two sub processes each of which goes through many steps. The first sub-process is to read the cover file, extract its samples, and select the low power ones. The second sub-process is responsible for reading the file to be hidden, encrypting it (will be explained later), and convert it into bitstream. Once the two sub processes achieve their task the process of converting the encrypted bit stream into quantized levels is started. The recovery process starts by reading the stego file, extract its samples, select the low power ones, reconstruct the original value from the quantized value, collect the reconstructed values as a file, and finally decrypt it.



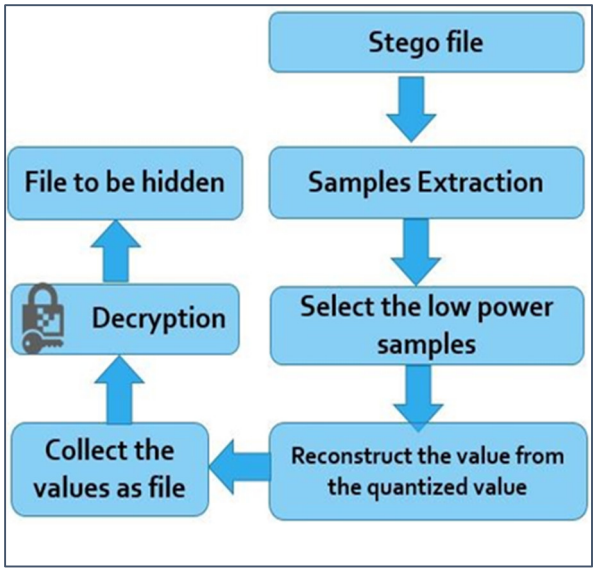


Figure. 6: File hiding.

Figure. 7: File recovery.

The encryption process is presented in figure (8), not only the content is encrypted but also the type of the file is also encrypted to provide more security. As it is presented in the figure AES is used and its key is encrypted using RSA algorithm. The reason behind using RSA is eliminate the possibility of intercepting

the key. The key is encrypted using the public-key of the receiver. Only the receiver can decipher the key and decrypt the received information as shown in figure (9).

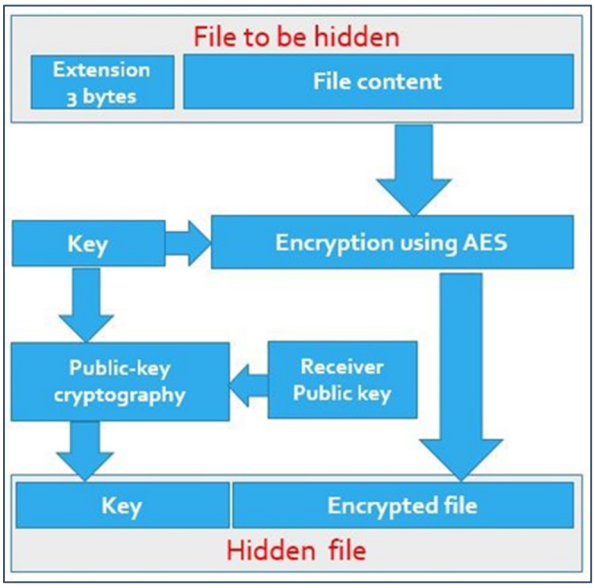


Figure. 8: File encryption.

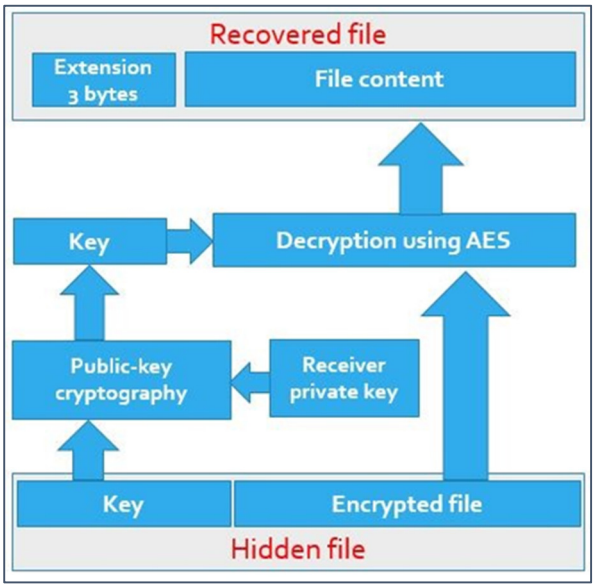


Figure. 9: File decryption.

4 Conclusion

The proposed work, **Whisper**, focusses on hiding any sensitive file in an audio file. Audio file is chosen as a cover file due to its enormous usage over internet and it provide a higher hiding capacity. Whisper choose the low power samples a place to hide the content of the file. The file is protected not only by hiding it but also by encrypting its content and its information using AES algorithm and AES encryption key is encrypted using RSA algorithm.

REFERENCES

[1] Shaikh, K. Solanki, V. Uttekar, and N. Vishwakarma, "Audio steganography and security using cryptography," Int. J. Emer. Technol. Adv Eng., ISO, vol. 9001, 2008.

[2] R. Priyanka, K. R. Vrushabh, P. K. Komal, S. M. Pingle, and S. R. Mahesh, "Audio steganography using lsb," International Journal of Electronics, Communication and Soft Computing Science & Engineering (IJECSCSE), vol. 2, p. 90, 2012.

[3] N. Cvejic and T. Seppanen, "Increasing the capacity of lsb-based audio steganography," in Multimedia Signal Processing, 2002 IEEE Workshop on. IEEE, 2002, pp. 336–338.

[4] G. Nehru and P. Dhar, "A detailed look of audio steganography techniques using lsb and genetic algorithm approach," IJCSI International Journal of Computer Science

[5] P. Jayaram, H. Ranganatha, and H. Anupama, "Information hiding using audio steganography–a survey," The International Journal of Multimedia & Its Applications (IJMA) Vol, vol. 3, pp. 86–96, 2011.

[6] R. Garg and V. Laxmi, "Various audio steganography techniques for audio signals."

[7] S. K. Bandyopadhyay, D. Bhattacharyya, D. Ganguly, S. Mukherjee, and P. Das, "A tutorial review on steganography," in International conference on contemporary computing, vol. 101, 2008, pp. 105–114.

[8] W. Bender, D. Gruhl, and N. Morimoto, "Method and apparatus for echo data hiding in audio signals," Apr. 6 1999, uS Patent 5,893,067.

[9] S. Shirali-Shahreza and M. Shirali-Shahreza, "Steganography in silence intervals of speech," in Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP'08 International Conference on. IEEE, 2008, pp. 605–607.

[10] H. Matsuoka, "Spread spectrum audio steganography using sub-band phase shifting," in Intelligent Information Hiding and Multimedia Signal Processing, 2006. IIH-MSP'06. International Conference on. IEEE, 2006, pp. 3–6.

[11] K. Gopalan and S. Wenndt, "Audio steganography for covert data transmission by imperceptible tone insertion," in Proc. The IASTED International Conference on Communication Systems And Applications (CSA 2004), Banff, Canada, 2004.

[12] F. Djebbar, B. Ayad, K. A. Meraim, and H. Hamam, "Comparative study of digital audio steganography techniques," EURASIP Journal on Audio, Speech, and Music Processing, vol. 2012, no. 1, p. 25, 2012.

[13] J. Daemen and V. Rijmen, The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media, 2013.

[14] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.