Sound Conveyors for Stealthy Data Transmission

D. M. S. Eranga, Hesiri. D. Weerasinghe

Abstract—**Hiding messages for countless security purposes have become highly fascinating subject on now a day. Encryption facilitates the data hiding. With the express development of the technology, people tend to figure out a method which is not only capable in hiding a message, but also capable in hiding the survival of the message. The present-day study is conducted in order to hide information in an Audio file. Generally steganography advantages are not use among industry and learners even though it is extensively discussing area in present information world. The major aim of this implementation is to hide any kind of information except video files in an audio file and retrieve the hidden information when necessary. This system is called DeepAudio v1.0. The system supports AES 256 bit key encryption and tolerates both wave and MP3 files as carrier. The sub aims of this work were the creation of a free, openly available and bugs free software tool with additional features which are new to the area.**

Index Terms—**Encryption, Steganography, wave, MP3, AES**

I. Introduction

With the rapid development of information and communication technologies are constantly increasing demands to achieve maximum safety and reliability in these areas. This is a current and highly debated issue and there is evidence the fact that such a situation will persist. Currently, there are a number of methods and disciplines dealing with provision of information and communication systems. During the 'information age', [1] Information have become very important as the also implies some way to protect the information. Of course, protection, or secrecy of the information is not new. Ancient Greece People, who first mentioned of attempts of classification of important messages that could affect the course of war. The importance of confidentiality of sensitive information in the military sector has persisted to this day, but it is very important in other areas, mainly due to the rapid development and expansion of information technology and computer networks. Sometimes we do not need the information to protect confidentiality, but just on the contrary, we want to be free to expand while maintaining our proof of authorship. These programs most frequently used image file formats like cover (sometimes called as carrier).

II. Aims and Objectives

Steganography of audio signals is more challenging compared to the steganography of images or video sequences, due to wider energetic range of the Human auditory system in comparison with Human visual system [2]. Only a few algorithms are developed to embed a message to an Audio files. The surviving systems require a considerable time to embed a small message. Furthermore, we have studied that the local people/authorities do not have awareness of Steganography, even though it is widely discussing topic in modern information world. Prominent goal was to create a software tool for hiding valuable files within an audio file. Therefore, it was necessary to revise the proposed program should extract the concealed data directly from the audio. This process is collaborated to following ordered objectives. Enhance cryptographic security of hidden data (Confidentiality) together with passwords (Authentication) and Increase data rate of the embedded data. Furthermore, assure exactness of decrypted data (Integrity) as well as assure unapparent perceptual transparency of audio file (Cover object) and the object containing secret messages. Finally, send audio files to another location or party through any common network.

III. Literature Review

Steganography can be defined as “The art of hiding and transmitting data through apparently innocuous transporters in an effort to cover the existence of the data”. Steganography is Greek origin word which means "hidden writing”. The word can divide in to two parts, Steganos and Graphic. Stegnos means "Secret" or "covered". And graphic means "Writing". The book called "Steganographia" which wrote by Johannes Trithemius in 1499 was the first book covered the techniques of Steganography [3].

In General, the basics of Steganography uses by many operating systems to hide files and folders. In Windows OS imply we can hide a folder or a file in another folder by using Hidden Directories or in UNIX hiding directories. In networks, Covert channels are used for transfer valuable data in apparently usual network traffic. Furthermore, encryption software called Truecript is also using steganography for the additional security of hidden data [4]. With that they have given the ability of hiding a hidden truecript volume or a hidden operating system, within the main outer truecrypt volume by using different passwords. With this nobody can easily find the existence of hidden data volume or the hidden operating system even though he knows that’s a truecript volume and has the password of outer volume. There are two prominent steganography types exist [5] which called Pure and Secret key steganography. Pure steganography hides valuable information inside the carrier file without an additional shield while secret key Steganography hides valuable information inside the carrier files with an additional shield (Password). Cryptography and Steganography seems to

Manuscript received August 23, 2016
D. M. S. Eranga, Statistics and Computer Science, University of Kelaniya, Kelaniya, Sri Lanka
Hesiri D. Weerasinghe, Statistics and Computer Science, University of Kelaniya, Kelaniya, Sri Lanka

be a similar to each other. Both techniques are used in information Security and symmetric and asymmetric keys for embedding and extracting as well. However, Cryptography mainly Concerns on Protect information Steganography concerns on concealing the existence of hidden information. Cryptography can be noticed by third party and it is a common technology. Moreover, most Cryptography algorithms are known by all, but Steganography is less known Technology and algorithms are developing.

IV. Theory and Methodology

Prominent logics of this research based on specific theories in computer science as well as statistics.

A. Sampling Rate

Capture audio covering the entire 20–20,000 Hz range of human hearing, such as when recording music or many types of acoustic events, audio waveforms are typically sampled at 44.1 kHz, 48 kHz, 88.2 kHz, or 96 kHz. The approximately double-rate condition is a consequence of the Nyquist theorem. Sampling rates higher than about 50 kHz to 60 kHz cannot supply more usable information for human listeners [6].

B. Advance Encryption Standard

AES is not a Feistel cipher. It works in parallel over the whole input block. It performs in an efficient way both in hardware and software through a variety of platforms. Symmetric or secret-key ciphers use the same key for both encryption and decryption, so receiver must know same key to decrypt the message. Block size is 128 bit (but also 192 or 256 bit). Key length can be 128, 192, or 256 bit. Number of rounds is 10, 12 or 14. Key scheduling is 44, 52 or 60 sub keys of having length = 32 bit [7].

C. Java Libraries

JAVA libraries played a tremendous role inside this research. Specific libraries such as bouncy castle as well as default libraries, to provide a one tire of security and also some other libraries to process an audio files [8].

D. Simple Random Sampling

Statistics use to process the survey and analyze the information retrieve from the survey. Basic statistic theories are used for prepare survey document, select sample and analyze. Sample selected in such a way that every possible sample of the same size equally likely to be chosen to archive randomness, random number method is used [9]. Sample Size to estimate population proportion can be mentioned as follows.

N=Population Size, n=Sample size, P=probability of success, Q=probability of failure, B=bound of the error of estimation.

$$n = \frac{NPQ}{(N-1)D+PQ}$$

V. Proposed Way-outs

Resolutions include different approaches, but each style performs under same generic architecture. Common architecture for hiding information is to encrypt the secret message (let say message) and then encode to the cover object. Retrieval process is to decode the hidden information and decrypt to original message. Original qualities of audio file remains after the process of encode and decode. So, the audio file performs as it is [10].

A. LSB Encoding

The system has developed on the top of three distinct logics. According to the selected logic and options, the system will present the maximum size of data which can be hidden before execute the process. First approach belongs to least significant bit (LSB) technique and the system which uses LSB technique called Method I. Though the Method I is complex process it is flexible. In the first place, the systems copies audio file to buffer and the same time calculates the size of the message and write that value inside 4 byte using 8 bit right shift [11]. Skip the audio header and then write the message type next to the audio header. Then, reads the message and encrypts using AES 256 with given key. Then, start to write the encrypted message inside the audio from last used position. If user requires compress to escalation the size of the message then change the LSB in each byte. Otherwise, skip the first 8 bit and change LSB in next 8bit until the end of the message. The system changes bits from left and right channels from each sample. It causes to reduce the noise inside the audio while modifications. At the end of the process, encoded audio is written in given location same as original audio file.

Retrieve process requires encoded audio and the secret key which used to encode the message. Read the size and other information of hidden data retrieves correct bits from audio byte stream. Use left shifting and calculates message size from retrieved bytes. Then decrypts the extracted message and save the document in given location. Users are able to remove the message from audio after extracted, if it is required. The process of encode or message removal, does not affect to the audio file.

B. Injection Encoding

Injection is a quite simple method which directly injects the message into the carrier file [12]. The payload and carrier message are directly fed into the specially designed stegosystem encoder. Wherever, the proposed system refers this technique called as method II. Each audio file consists of header and body, which include summarized details about the audio and data respectively [13]. This technique inserts the summarized message information according to the message in the middle of header and body, and then attaches the secret message or file. Method II is simple process but it is very powerful and much quicker than the previous technique. The system copies audio bits to buffer and calculates the size of the message or file. Write header and then add six bytes, which represents the size of the message, type of the message and compression details of the message. Then, writes the rest of the audio into buffer. Then reads the message and encrypts using AES 256 with given key. If user requires compressing the message then it process before encrypt. Write the encrypted and compressed message at the end of the buffer. Finally, writes the entire encoded audio in user given location.

Retrieval process of Method II skips the header bytes of audio file and read next six bytes. Then, points to the end of the audio file and retrieves the hidden message. Next, decrypts the message using encoded secret key and decompress. Finally the document is saved as in user given location. Users are able to remove the message when necessary. Removal of the hidden message does not affect to the audio file and also during encode, decode or removal process, audio file can be listen.

C. *MP3 Encoding*

Mp3 file format consists of packets and each packet includes header and data [14]. Then reads the message and encrypts using AES 256 with given key. Skip the header and write the size of the message in data field, which belongs to first packet. Then, writes the type of the message in the same packet and start to write the message in data field in each packet using LSB technique. There is a constant skip value between two modification packets to protect the original quality of mp3 file. Higher the number of skip better for the audio sounds. Finally encoded mp3 file write in user given location. Because of the size limitation, small file or message is allowed regarding to the size of the mp3 audio file and also maximum message size should 1/16 (6.25%) from its mp3 carrier. Otherwise, system might not perform the user request and raises a message to the user.

Retrieve process is vice versa process of encode. Check first packet and read the encrypted message size, then read the message bits in data field according to pre-defined skip value. Decrypts the extracted bits using encoded secret key and save the bits according to the type of the message file. Inside this process, message compression does not prompt to the user but system does itself. However, the protection of the original quality of the mp3 file is the extremely difficult mission.

D. *Send and Receive Encoded File*

The System also facilitates that send audio files to target location in LAN environment. It is specially design for sender and receiver who use DeepAudio v1.0. Users who intend to send the encoded audio to target receivers are able to use the system and also each encoded audio file is treated as normal audio file inside the system. Sender should enter the receiver's IP address and connection does not success until receiver accepts the file transfer request. For each sender and receiver have single connection via random socket. Furthermore, more than one processes are allowed simultaneously without having size restrictions and file transferring fragment is independent from encode and decode processes.

VI. TESTING

Following test results based on 25.4 MB audio (wave) file along with same size of text, document and pdf document formats. Test cycle has been completed 60 times per one single message size and 20 times per each document format. However, the consequences have been displayed as an average time for above three types of document formats according to the above proposed technique.

TABLE I

Average time required for both encode and decode according to proposed way-outs.

	Method I (LSB)		Method II (Injection)	
Message (kb)	Encode time (s)	Decode time (s)	Encode time(s)	Decode time (s)
2.2	0.01	1.29	0.10	0.10
20.1	0.10	8.61	0.13	0.11
46	0.18	12.44	0.20	0.12
59.6	0.20	15.83	0.22	0.13
110	0.34	33.96	0.30	0.18
207.5	0.42	71.76	0.36	0.20
240	0.44	82.07	0.41	0.22
1,047.8	0.50	306.54	0.58	0.29
2,095.8	1.1	682.32	0.91	0.35

MP3 encode perform low when compare with method I and method II. Furthermore, it takes approximately same amount of time for both encode and decode processes due to the small size of the hidden message. However, exactness of original message and message after retrieve have been tested Using open source software called Winmerge version 2.14.0. WinMerge is a freeware, differencing and integration tool for Windows. This software can compare both folders and files, giving differences in a text format that is easy to comprehend and handle [15].

A. *Noise*

While editing the audio files, noise inside the audio file becomes the prominent fact and the noise increases according to the edited portion in particular audio file [16]. Noise inside an audio file increases according to the size of hidden text/document, but this will only affects Method I because, Method II does not edit inner part of the audio. However, the noise change hard to detect using software, because it is negligible and the system has restricted the size of hidden data, which is maximum of 1/8 from its carrier for Method I to minimize the noise increment as well.

VII. PERFORMANCE

Survey was conducted to measure the system performance among professionals to identifying the quality of the system which satisfies the expectation among IT Professionals and acceptance of the system availability in the internet are two prominent areas which have had been considered.

TABLE II

Summarized results based on the survey.

Subject	Quality of the program		
	Yes	No	No Idea
Exactness of secret message before and after the process	96.21%	2.13%	1.66%
Exactness of audio before and after the process	86.31%	12.68%	1.01%
Availability in the internet	89.59%	6.03%	4.38%

When considered the Exactness of secret message before and after the process, there are 96.21% accepting that the

retrieved message exactly same to its original message. Approximately 2.13% of them believe that there are some conflict between the original document and extracted copy. Furthermore, 86.31% believe that the program protect the freshness of the carrier, while 12.68% have complains about the matchlessness. According to the subjects about originality, 1.66% and 1.01% do not have an idea about the existence respectively.

Availability of the system in the internet was one of the most important areas to evaluate the system. It represents the essential of software which related to researched area. There are 89.59% accepted that the quality of the program was good and like to see available in the internet. At the same time 6.03% were implied negative impression.

VIII. Discussion

The current study was done in order to hide a message in an audio. The importance of hiding in an audio is sheltered because it less susceptible. It can be reduce the man in the middle attack. The main technique is to change the LSB value of the carrier file. In order to do that, the audio is separated into a set of byte values and message as well. The LSB value in carrier file is changed in each byte according to the message bytes, so that the LSB carries the hidden message. In addition to use injection technique to hide text messages in an audio file. It gives accurate and decent security for data hiding. It also provides cryptography way out to secure data in an audio file. Suppose that someone could separate message bytes from original audio file. If that person need to read the secrete message first of all he should break the AES encryption because hidden message was encrypted from AES-256. However, the system assures the original quality of the carrier after encoded and exactness of the hidden information after retrieve.

IX. Conclusion

The main objective of this research is to hide a message or file in an audio transporter. The system was evaluated for its main functionalities such as hiding the existence of the message and extracting the message correctly. The results show that the system performs well in hiding the message file and extracting the message from the carrier file. LSB technique is implemented by changing the LSB of the audio file according to the text message file. The message is converted into the byte code and embedding to the carrier file. Message size is written in audio file header. With this technique, size difference between original and encoded audio file cannot be monitored. Injection technique is very accurate and provides more capacity to the encoded message. It allows hiding larger messages into audio file without having limitations.

Both approaches use compression technique which defines into three levels such as Low, Medium and High. Medium is the default compression level. It permits users to hide more information and also guarantees the quality of the message. Although it uses Advance Encryption standard cryptography to protect the message, the message is less traceable. Let say someone could divide the message from audio but he need to break encryption also to see the hidden message. Moreover, the system supports two tire protection using cryptographic associations. This application affords send and receives technique to enhance the user interaction. It can be used to transmit any audio from one computer to another computer. Providing a User manual to users will have enhanced the interaction with this application and make it to use easier as much as possible. It has been tested and handled all the exceptions and display to the user using simple messages. The coupling of the Cryptography and Steganography make very high degree of security and a number of programs available software tools, implementing just such combined information security.

DeepAudio v1.0 provide more features, security and speed rather than the other surviving systems. DeepAudio v1.0 allows considerable percentage of security and performance guarantee System and it will be major competitor with other surviving systems. It provides security, considerable message capacity, robustness and greater speed.

The survey results represent that more than 89% employees who work in IT environment accept this application and wish to available in the internet in future. Finally the consequence of this research achieved all the goals and go beyond expected targets.

Acknowledgment

We would like to show our gratitude to the Academic staff of Statistics and Computer Science Department, university of Kelaniya and private and government companies for sharing their pearls of wisdom with us during the course of this research.

References

[1] Castells, M., The Information Age, *Cambridge (Mass.); Oxford: Wiley-Blackwell*, Volumes 1-3, 1999.

[2] Neil F. Johnson, Zoran Duric and Sushil Jajodia, Information Hiding, Springer US, 2001.

[3] G. J. Simmons, The prisoners' problem and the subliminal channel, *Advances in Cryptology. Proc. of Crypto 83*, 1984, pp.51-67.

[4] Walter Bender, Daniel Gruhl, Norishige Morimoto, Anthony Lu, Techniques for Data Hiding, *IBM Systems Journal*, vol.35, no. 3 and 4, 1996, p. 313-336.

[5] Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay and Sugata Sanyal, Steganography and Steganalysis: Different Approaches, *International Journal of Computers, Information Technology and Engineering (IJCITAE), Serial Publications*, *Vol. 2, No 1,* June, 2008.

[6] Shannon, C. E., Communication in the presence of noise, *Proc. Institute of Radio Engineers*, *vol. 37, no.* 1, 1949, pp. 10–21.

[7] (2016), prezi.com, [Online]. Available: https://prezi.com/eiieebohsjet/rijndael-alogithm/

[8] (2015), How Classes are Found - Oracle Corporation. [Online]. Available:*http://docs.oracle.com/javase/6/docs/technotes/tools/findingclasses.html*

[9] ALAN AGRESTI, *Categorical Data Analysis* (2nd edition ,John Wiley & Sons, Gainesville, Florida ,2002).

[10] Fatiha Djebbar et al, A view on latest audio steganography techniques, *IEEE international conference on innovations in information and technology*, 2011.

[11] N. Cvejic, T. Seppiinen, Increasing the capacity of LSB-based audio steganography, *IEEE Workshop on Multimedia Signal processing*, 2002, pp. 336 -338.

[12] D. M. S. Eranga, Hesiri D. Weerasinghe, Audio transporters for unrevealed communication, in IEEE Xplore, 2015, p.267.

[13] (2015), WAVE and AVI Codec Registries – RFC 236, Microsoft Corporation (June 1998), [Online]. Available: http://tools.ietf.org/html/rfc2361

[14] (2015), MP3, [Online]. https://en.wikipedia.org/wiki/MP3.
[15] (2015), winmerge, [Online]. Available: http://winmerge.org/
[16] Rothwell, Dan J. In the Company of Others: *An Introduction to Communication* (New York: McGraw Hill, 2004).

D**. M. S. Eranga**[1] was born in Sri Lanka. He has completed his BSc(special) degree in computer science from University of Kelaniya, Sri Lanka. His research interest includes computer networking, network security and cyber security, cloud computing and quality assurance. Mr. Eranga is currently working as a temporary demonstrator in department of statistics and computer science in University of Kelaniya, Sri Lanka.

Hesiri D. Weerasinghe[2] was born in Sri Lanka. He has completed his B.Sc. degree in University of Kelaniya, Sri Lanka. Furthermore, he has finished his M.Sc. and PhD in University of Oakland, USA majority in computer network and security. His research Interests are Network Security and Privacy, Secure cloud computing, VANET & MANET security, Elliptic Curve Cryptography (ECC). Dr. Weerasinghe is working as a senior lecturer in department of statistics and computer science in University of Kelaniya, Sri Lanka.