Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 5, May 2016, pg.76 – 80

Secured Way of Ciphering Text Using Audio Steganography

O.SIVA[1], M.HIRANMAYE[2], M.CHANDU JAGAN SEKHAR[3]

[1]Department of CSE, VITS College of Engineering, Sontyam, Visakhapatnam, India

[2]Department of CSE, VITS College of Engineering, Sontyam, Visakhapatnam, India

[3]Department of CSE, VITS College of Engineering, Sontyam, Visakhapatnam, India

sivaommi2012@gmail.com, Hiranmayemoola@gmail.com, mchandujagansekhar@gmail.com

Abstract- It is a method akin to covert channels, and invisible inks, which add another step in security. A message in cipher text may arouse suspicion while an invisible message will not. Digital steganography use a host data or message, known as a "container" or "cover" to hide another data or message in it. The conventional way of protecting information was to use a standard symmetric or asymmetric key system in encryption. Steganography can also be used to place a hidden "trademark" in images, music, and software, a technique referred to as watermarking. Steganography, if however used along with cryptography, for example, if a message is encrypted using triple DES (EDE) which requires a 112 bit key then the message has become quite secure as far as cryptanalytic attack are concerned. Now, if this cipher text is embedded in an image, video, voice, etc., it is even more secure. If an encrypted message is intercepted, the interceptor knows the text is an encrypted message. With steganography, the interceptor may not know the object contains a massage. When performing data hiding on audio, one must exploit the weakness of the Human Auditory System (HAS), while at the same time being aware of the extreme sensitivity of the human auditory system.

I. INTRODUCTION

A process which ensure the privacy of the communication between two parties, various new methods are being developed. Cryptography is like a tool, it can do as well as it programmed to do. Also, there are various different techniques that can implemented to attain a certain level of security. Here we implement a technique for data hiding in audio images, known as Audio file STEGANOGRAPHY. However, steganography alone is not able to provide a sufficiently high enough level of security. In order to improve the security of our technique, we will also be incorporating encryption of the data to be hidden.

II. OBJECTIVE

A technique of hiding the message in the audio file in such a way, that there would be no perceivable changes in the audio file after the message insertion. At the same time, if the message that is to be hidden were encrypted, the level of security would be raised to quite a satisfactory level. Now, even if the hidden message were to be discovered, the person trying to get the message would only be able to lay his hands on the encrypted message with no way of being able to decrypt it.

III. MODULE DESCRIPTION

In this paper there are two modules to implement. First is embedding for hiding the data in Audio and second is extraction for retrieval of data from that Audio.

EMBEDDING

1. Selecting File

The File is selected for ciphering the text.

Hide and Seek uses the Least Significant Bit of each pixel to encode characters, pixels per character and spreads the data.

2. Selecting the Audio File

Here the WAV is selected for encrypt the original file. There are a large number of steganographic methods that most of us are familiar with (especially if you watch a lot of spy movies!), ranging from invisible ink and microdots to secreting a hidden message in the second letter of each word of a large body of text and spread spectrum radio communication. With computers and networks, there are many other ways of hiding information

3. Entering Password

For security purpose, the password is entered.

4. Embedding the Data into Audio

The data to be encrypted is embedded into the Audio File.

For Others, It is an Audio file. But it carries the data file.

cover_medium + hidden_data + stego_key = stego_medium

In this context, the *cover_medium* is the file in which we will hide the *hidden_data*, which may also be encrypted using the *stego_key*. The cover_medium (and, thus, the stego_medium) are typically image or audio files. In this article, I will focus on image files and will, therefore, refer to the *cover_image* and *stego_image*.

5.1.2 EXTARCTING

1. Selecting the input Audio File

Here Audio File is selected for getting the original Message.

2. Entering the output file Name

Here the user should mention the path to be stored.

3. Entering the password for security

Here the original password should be entered to get the original message.

4. Extracting the data from the Audio File

Here the Original Message is extracted from the audio File.

IV. IMPLEMENTATION

Audio File Format

In order to demonstrate the use of steganography techniques combined with encryption, the AU format used on Sun and NeXT machines was chosen as the host audio file. Sun AU format is well documented elsewhere and java Sound API provides convenient way to handle formatted audio data. Formatted audio data refers to sound in any of a number of standard formats. The java Sound API distinguishes between data formats and file formats. A data format tells you how to interpret a series of bytes of "raw" sampled audio data, such as samples that have already been read from sound file, or samples that have been captured from the microphone input. You might need to know, for example, how many bits constitute one sample (the representation of the shortest instant of sound), and similarly you might need to know the sound's sample rate (how fast the samples are supposed to follow one another). When setting up for playback or capture, you specify the data format of the sound you are capturing or playing.

Encryption method used

We chose a Password Based Encryption scheme based on RSA Laboratories PKCS # 5 v2.0 standard

Since a password is not directly applicable as a key to any conventional cryptosystem, however, some processing of the password is required to perform cryptographic operations with it. Moreover, as passwords are often

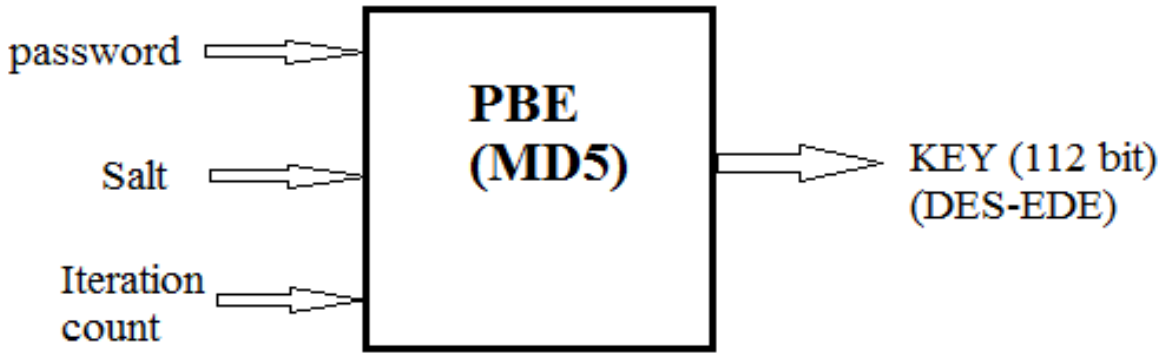

Figure 5.2 Key Derivation Function (KDF) in PBE

Chosen from a relatively small space, special care is required in the processing to defend against search attacks. A general approach to password-based cryptography, for the protection of password tables, is to combine a password with a salt to produce a key. The salt can be viewed as index into a large set of keys derived from the password, and need not be kept secret. Although it may be possible for an opponent to construct a table of possible passwords (a so-called "dictionary attack"), constructing a table of possible keys will be difficult, since there will be many possible keys for each password. An opponent will thus be limited to searching through passwords separately for each salt.

PBKDF1 Algorithm

PBKDF1 (P,S,c,dkLen)

Options : Hash underlying hash function

Input : P password, an octet string

S salt, an eight-octet string

c interaction count, a positive integer

dkLen intended length in octets of derived key, a positive integer

at most 16 for MD5 and 20 for SHA-1

Output: DK derived key, a dkLen-octet string

Steps:

1. If dkLen > 16 for MD2 and MD5, or dkLen > 20 for SHA-1, output "derived key too long" and stop.
2. Apply the underlying hash function Hash c iterations to the concatenation of the password P and the salt S, then extract the first dkLen octets to produce a derived key DK:

T1 - Hash (P\\S),

T2 - Hash(T1),

. . .

Tc - Hash (Tc - 1),

DK - Tc <0..dkLen - 1)

3. Output the derived key DK

V. CONCLUSION

In this paper we have introduced a robust method of imperceptible audio data hiding. Thus we conclude that audio data hiding techniques can be used for number of purposes other than covert communication or deniable data storage, information tracing and finger printing, tamper detection. As the sky is not limit so is not for the development. Man is now pushing away its own boundaries to make every thought possible. So similarly these operations described above can be further modified as it is in the world of Information Technology.

REFERENCES

[1] Bender W., Gruhl D., Morimoto N., "Techniques for data hiding", IBM systems journal, Vol 35, Nos 3&4, 1996

[2] Java Sound API-http://java.sun.com/products/java-media/sound/

[3]PKCS #5: Password-based Encryption Standard. Version 2.0. RSA Laboratories. March 1999.

[4] Java TM Cryptography Extension (JCE)-http://java.sun.com/products/jce

[5] Declan McCullagh. "Bin Laden: Steganography Master?". Wired News Feb. 2001(http://www.wired.com/news/politics/0,1283,41658,00.html)

