International Journal of Information System & Technology
Akreditasi No. 36/E/KPT/2019 | Vol. 3, No. 2, (2020), pp.290-294

Application of Steganography to Audio Files with Least Significant Bit (LSB) Process and Vigenere Cipher Encryption

Heri Santoso
Universitas Islam Negeri Sumatera Utara Medan, Indonesia

herisantoso@uinsu.ac.id

Abstract

*Current technological developments, making the information very important, then the need arises in sending information that contains secrets. To solve this information security problem, the method that can be used is cryptography to encode messages using the Vigenere Cipher algorithm and steganography to hide messages using the Least Significant bit (LSB) method. This steganography application is able to insert text messages in files that have the format * .txt, * .docx, and * .pdf, but the size of the amount of text does not exceed the cover capacity of the audio file and can extract the text that has been inserted again. This application is also capable of encrypting and decrypting text files in * .txt, * .docx and * .pdf formats. Tests conducted on the audio size, audio that has a large bit rate will have a large capacity.*

Keywords: *Steganography, Cryptography, Least Significant Bits, Vigenere Cipher*

1. Introduction

Current technological developments make the information very important. Some even say that the world community is now in an "information-based society." It is very important the value of information that helps the information to be conveyed is not accepted by the intended recipient but falls in the hands of others. Therefore, the need arises in sending information that contains confidentiality and privacy without being noticed by the person not being addressed, only between the sender of the message and the recipient of the message. This makes people who do not have power over the files who want to see the contents of the files, and then a criminal threat appears for the security of the confidential information. To solve this information security problem, the methods that can be used are cryptography and steganography. Cryptography was chosen because it can maintain the confidentiality of messages by pairing them into a form that no longer functions. One of the encryption algorithms in the text that is in cryptography is the vigenere code, which is an encryption technique in classical cryptography. The encryption technique chosen because it has advantages over Caesarean cipher and other monoalphabetic ciphers is that they are not too vulnerable to a coding method called frequency analysis. Meanwhile, steganography was chosen because it can accommodate messages or secret information so that other people are not aware of the hidden messages. Steganography can be implemented in digital files, media that can be used as a messenger in the form of multimedia files, one of which is audio. One of the methods in steganography is the Least Significant Bit (LSB). This method can store text at the lowest bit of each byte of the audio file. The advantages of this method are fast, easy and the comparison between the original file and the stego file is almost the same so that it doesn't really affect the quality of the audio file. The purpose of this research is to implement the vigenere algorithm for storing messages and the Least Significant Bit (LSB) method for filling messages into audio files.

ISSN : 2580-7250

2. Research Methodology

Steganography is the art of covering messages in digital media in such a way that other people do not know there is a message in the media. In the field of information security, steganography is used to cover sensitive data when encryption is not feasible or at the same time as encryption [1]. Even if the encryption has been broken (deciphered), the message or sensitive data remains invisible [2].

Audio Steganography is a technique for injecting hidden messages into audio media. The method of inserting hidden messages into the steganography system is effectively achieved by defining the audio medium of the message carrier, i.e., the redundant bits that can be changed without losing the credibility of the audio media itself [3-4]. Various techniques can be used to apply steganography to audio files. Here are some of the methods that can be used:

a) It's a replacement bit. This approach is widely used in digital steganography techniques, i.e., to substitute sections of data bits with hidden data inserted. In this approach, the benefit gained is that the size of the message inserted is comparatively large, but it has an effect on the outcome of poor quality audio with a lot of noise.
b) The second approach used is the phase-out of the input signal. The idea used is to replace the initial phase of each section, starting with the phase that has been done in such a way and reflects the secret message. The process from the beginning of each segment is rendered in such a way that each segment always has a relationship that results in sound quality is preserved. This technique produces a much better performance than the first approach but is compensated for by the difficulty of its implementation.
c) The third method is the continuum of distribution. With this process, the message is encoded and distributed through any possible frequency spectrum. It would also be very difficult for those who want to overcome it unless they have access to the data or can recreate random signals used to disperse messages across a variety of frequencies.
d) The last approach that is sometimes used is to cover a message using an echo technique. The technique of disguising a message into a signal producing an echo. Then the message is hidden by changing the three parameters in the echo, namely the initial amplitude, the attenuation frequency, and the offset. With the echo offset and the original signal, the echo will be mixed with the original signal since the human hearing system can not distinguish the echo and the original signal.

The most common steganography method for image file types is the least significant bit (LSB). This method hides the data by replacing the least meaningful data bits in the cover with secret data bits. In the arrangement of bits in a byte (1 byte = 8 bits), there are bits that mean the most significant bit (MSB) and the least significant bit means the least significant bit (LSB) [5].

The Vigenere cipher is perhaps the best example of a manual compound-alphabet cipher. This algorithm was published by the French diplomat (cryptologist) Blaise de Vigenere in the 16th century, although Giovan Batista Balaso first described it in 1553, as written in his book La Cifra del Sig. Giovan Batista Belaso [6]. The Vigenere Cipher was published in 1586, but the algorithm was only widely known 200 years later, which the inventor of the cipher called the vigenere cipher. The Vigenere cipher is well known for being easy to understand and implement. Ciphers use vigenere squares to perform encryption [7].

The column from the left of the block represents the key letters, while the top row represents the plaintext letters. Each line in the square represents the letters of the ciphertext obtained with the Caesar cipher, in which the number of paintex shifts is determined by the

numeric value of the key letter (i.e., a = 0, b = 1, c = 2,… .., z = 25) [8]. For example, the key letter c (= 2) states that the plaintext letters are shifted two letters to the right (from the alphabetical order) so that the ciphertext letters on line c are:

C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	P	W	X	Y	Z	A	B

The vigenere squares were used to obtain the ciphertext using the specified jars. If the key length is longer than the plaintext length, then the key is repeated using it (periodic system). If the key length is m, then the period is said to be m.

An overview of the system is defined in the design of this system. The goal of the design is to better guide the detailed system, namely to provide a simple and complete design that will later be used for the development of the system. This segment explains how the current flow of the software is a flowchart. There are two processes in the manual framework that are currently ongoing, namely the message insertion process and the message separation process.

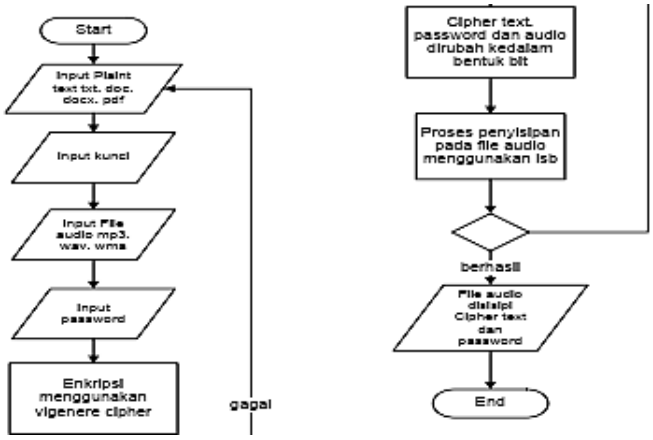

Figure1. Insertion flowchart (embedded)

The following is the reason for Figure 1:

a) Input of plaintext in * .txt, * .docx or. * Format PDF.
b) Encryption input key.
c) Audio input that has * .mp3, * .wav, * .wma, * .amr, * .aac, * .ape, * .flac, * .mp2, and * .wv.
d) Login input for insertion
e) Encryption so that you get the ciphertext you want to insert.
f) Change text and audio to bits, then use the least important bit (etc.) to make the insertion operation.
g) If the insertion process is successful, the audio file inserted with the message will be saved; if it fails, repeat step 1 to the completion of the message.

The following is the reason for Figure 2:

a) Enter the audio file that has been inserted with the post.
b) The audio file is converted to bits, then checked whether or not the file contains a hidden message, and then separated by taking the last bits in the file.
c) If the separation process is efficient, the ciphertext will be given.
d) Input key to get back the plain text.

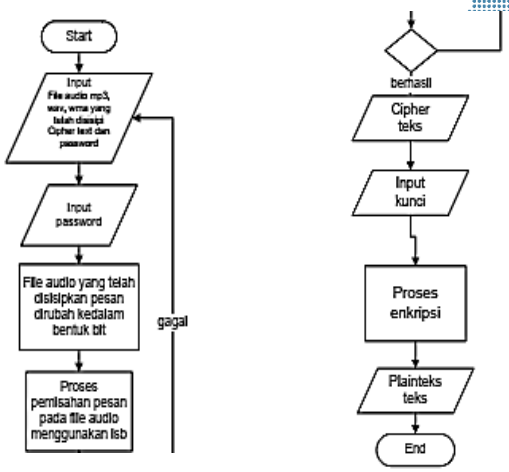

Figure 2. Flowchart of separation (extraction)

3. Results and Discussion

In order to assess the success of the application to be made, an application trial will be performed. The aim of the insertion and extraction test is to test the success of the insertion and extraction of messages and to test the success of the decryption and extraction of messages.

Table 1. Insertion and extraction testing

No.	Audio info				File info		Process	
	Name	Format	Size (byte)	Capacity (character)	Name	amount character	Insertion	Extraction
1	See you again	mp3	2497861	187212	Message1	10	Success	Success
					Message2	100	Success	Success
					Message3	1000	Success	Success
2	Shake it off	wav	1230718	28819	Message1	10	Success	Success
					Message2	100	Success	Success
					Message3	1000	Success	Success
3	All About That Bass	wma	1127156	15874	Message1	10	Success	Success
					Message2	100	Success	Success
					Message3	1000	Success	Success
4	Al-baqarah	Amr	1008038	984	Message1	10	Success	Success
					Message2	100	Success	Success
					Message3	1000	Failed	Failed
5	Ibadallah	Aac	1171028	21358	Message1	10	Success	Success
					Message2	100	Success	Success
					Message3	1000	Success	Success
6	One more time	Ape	1064376	8027	Message1	10	Success	Success
					Message2	100	Success	Success
					Message3	1000	Success	Success
7	Jodoh pasti bertemu	Flac	1025002	3105	Message1	10	Success	Success
					Message2	100	Success	Success
					Message3	1000	Success	Success
8	Papatong	mp2	1008117	994	Message1	10	Success	Success
					Message2	100	Success	Success
					Message3	1000	Failed	Failed
9	Pacar lima langkah	wv	1032547	4048	Message1	10	Success	Success
					Message2	100	Success	Success
					Message3	1000	Success	Success

4. Conclusion

The Vigenere cipher algorithm can secure data by encrypting and decrypting text files in * .txt, * .docx and * .pdf formats. The least significant bit method is capable of hiding text messages in * .txt, * .docx, and * .pdf formats, but the size of the amount of text does not exceed the capacity of the audio file. The results of the insertion with the least significant bit method are as follows:

a) The size (size) of the original audio with Stego-Audio does not change even though it has undergone a steganography process with messages stored in it.
b) After the audio that has been inserted with the message is played, the audio format is * .mp3, * .wma, * .ape, * .wav.

Reference

[1] Arius, Doni. (2009). Keamanan Multimedia. Andi. Yogyakarta
[2] Benington W., (2012). Pengantar Multimedia <URL :https://www.academia .edu/8289612/Pengantar_Multimedia>
[3] Cahyadi, Tri, (2012). “Implementasi Steganografi LSB dengan enkripsi vigenere chipher pada citra jpeg”. Jurnal Teknologi Informasi dan Komunikasi, 1.
[4] Hartanto, Bayu Putra, (2014). Implementasi Steganografi Metode Least Significant Bit (Lsb) Untuk Pengamanan Pesan Teks Dengan Media Image Dan Audio Menggunakan Enkripsi Blowfish . Tugas Akhir, Jurusan Teknik Informatika, Universitas Islam negeri Sunan Gunung Djati Bandung.
[5] Kalangi, Jeff Andre. (2010). “Pembuatan Aplikasi Steganografi pada file audio MP3 dengan metode parity coding”. Jurnal Ilmiah Universitas Komputer, 1.
[6] Munir. (2012). Multimedia. Alfabeta. Bandung
[7] Munir, Rinaldi. (2006). Kriptografi. Informatika. Yogyakarta
[8] Pressman, Roger. (2002). Rekayasa Perangkat Lunak. Andi. Yogyakarta.

Authors

1st Author
Heri Santoso
Universitas Islam Negeri Sumatera Utara Medan, Indonesia