KINETIK, Vol. 4, No. 1, February 2019, Pp. 63-74
ISSN : 2503-2259
E-ISSN : 2503-2267

Encryption of Text Message on Audio Steganography Using Combination Vigenere Cipher and LSB (Least Significant Bit)

Ibnu Utomo Wahyu Mulyono*[1], Ajib Susanto[2], Tiara Anggraeny[3], Christy Atika Sari[4]
[1,2,3,4]Universitas Dian Nuswantoro/Departement of Informatics Engineering
ibnu.utomo@dsn.dinus.ac.id[*1], ajib.susanto@dsn.dinus.ac.id[2], tiara.anggraeny15@gmail.com[3], atika.sari@dsn.dinus.ac.id[4]

Abstract

*The growing information technology is very rapidly, the more evolving crime techniques to find information that is confidential. The Internet is one of the main media in disseminating information. The use of security on the internet still needs to be developed. Based on these problems, the type of research undertaken in the writing of this final task is the type of experimental research by developing methods that have been done by previous researchers to hide secret data that is inserted into the audio * .wav so that the security and confidentiality of data can be guaranteed. data security can be done with various methods, including cryptography and steganography. Cryptography is a technique for encrypting messages and steganography is a message concealment technique. This insertion type uses binary ASCII character code. In the cryptographic process, using the Vigenere Cipher algorithm and in the steganography, process using the algorithm (LSB) Least Significant Bits. The merger of the two techniques resulted in a better new digital image security system and increased the value of MSE, PSNR and Execution time. Then the test results in the evaluation using BER and histogram analysis. Good audio quality has a minimum value of 30 dB PSNR. In the embedding process using combinations of vigenere and LSB methods, Audio 15 is the best audio compared to other audio. Audio 15 has a smaller MSE (0.001656) value and a larger PSNR (124.138499) value than any other audio when embeded messages *.txt file with character 4096.*

Keywords: *Cryptography, Vigenere Cipher, Steganography, LSB, WAV*

1. Introduction

In the dissemination of private and confidential information it is usually more likely to experience attacks from third parties, so the security of sending data or confidential information should be further enhanced. As technology develops, researchers conduct research to solve security problems. Data security can be done with various methods, including cryptography and steganography. Both of these methods is the method of approach to ensure the confidentiality of information. Cryptography is the study of keeping the security of a data or message, then transformed from a readable form (plaintext) into an unreadable form (cipher text) using a certain key in order to remain secure and unintelligible by others [1]. Cryptography has two main concepts, namely encryption and decryption. Encryption is the process of encoding plaintext into cipher text by converting the message into a disguised code, so as not to be recognized directly. The description is the process of returning cipher text to plaintext. Encryption and decryption processes require a key as a parameter used for transformation. The result of cryptography is a different form of the original message/information and has random/irregular features. The result of cryptography process can make suspicions about what information is contained therein [2]. One of the famous classical cryptographic algorithms, easy to understand and implemented is Vigenere Cipher. According to Caesar Cipher, Vigenere Cipher is a science in the form of a polyalphabetic substitution by adding a key to the message to become a safer cipher [1].

Steganography is the art and science of secret writing (hide in plain sight) and the technique has been used hundreds of years. Today, in the digital age it is easy to access to any form of data such as audio, video, images and text so easily vulnerable to many threats [1]. Steganography consists of steganography objects and secret messages. Commonly used steganography objects and the message such as images, audio and video. At present, a combination of steganography and cryptography methods is also used to ensure data confidentiality and to improve information security [1]. Steganography has two processes: encoding and decoding process. Encoding is the

Mulyono, I., Susanto, A., Anggraeny, T., & Sari, C. (2018). Encryption of Text Message on Audio Steganography Using Combination Vigenere Cipher and LSB (Least Significant Bit). Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 4(1). doi:http://dx.doi.org/10.22219/kinetik.v4i1.701
Receive September 13, 2018; Revise November 01, 2018; Accepted November 10, 2018

process of embedding the message into the container. This research uses file audio as a container. Decoding is the process of message extraction from audio steganography. The decoding and encoding process requires a secret key for the process of embedding message and extraction message so, only eligible parties can insert and extract messages [3].

Data is hidden within audio files using the bits that represent sounds which are not audible to human ears. Wave (.wav) audio file type was selected to be used as a cover file for the purpose of hiding data. Advantages of this type of file include high data redundancy which allows higher data capacity to be hidden in the file which makes it suitable to apply LSB that depends on redundancy for hiding data. The high data redundancy came from the fact that wave file format is not subjected to any type of compression. In addition, wave files can exist in a 16-bit sample audio file so it achieves the requirement that introduces for providing high data hiding capacity. [3]. The header is located in the first 44 bytes of the audio file and the next bit contains the data. The insertion of a message inserted in the data (body) is not inserted in the header [4]. In this research use of audio files and the use of LSB technique for steganography. LSB is the simplest substitution algorithm to hide messages. The advantages of using the steganography technique called “Least Significant Bit (LSB)”. One of its main advantages is the huge amount of data that could be embedded within audio files using this methodology. Through their paper, they concentrate mainly on the amount of data and the ability to increase the bit depth within multimedia files. They depend in their choice on that combining LSB methodology with audio files of amplitude resolution of 16 bits per sample achieves the required large amount of data size hiding. They say “Data hiding in the least significant bits of audio samples in the time domain is one of the simplest algorithms with very high data rate of additional information”[3]. The result of the steganography process will look the same (in plain sight) with the message before the secret message is inserted. Cryptography focuses on protecting the content of information to keep it secret. In cryptographic methods, the messages that have been embedded by secret messages are very different from the messages before they are embedded.

M.Baritha Begum and Y.Venkataramani [5] propose a new text-based text compression technique for ASCII text to get good performance on varius document size the dictionary-based compression bits are hidden to the LSB audio signal bit and to calculate the signal at the noise rasio (SNR). Audio Steganography is done for various compression algorithms with dictionary-based compression. Audio Steganography based dictionary compression produces a better signal to noise ratio (SNR). Audio Steganography based dictionary compression produces a better signal to noise ratio.

According to Anu Binny and Maddulety Koilakuntla [2], explains that in the proposed method each audio sample is converted into bits and then embedded text data in the embedding process, first the message character is converted to its equivalent binary. By using the proposed algorithm based on LSB, the system capacity increases steganography to hide text. The performance of the proposed algorithm is calculated using SNR values for various input audio.

Based on research by Ratul Chowdhury, Debnath Bhattacharyya, Samir Kumar Bandyopadhyay and Tai-hoon kim [4], proposed a new approach in which the duel encryption methodology has been implemented. In the first level encryption pattern matching algorithms have been used to encrypt text messages in terms of their position value. In the second level, the conventional LSB method has been used to embed position values on the cover file. Such duel encryption methods will ensure data security efficiently. The performance of the proposed method is evaluated in terms of mean square error (MSE) and signal to noise ratio (SNR). Comparison is done by conventional LSB method. The results of experiments and comparisons show that the algorithm created by the authors is very efficient in terms of encryption and size of text capacity.

Based on the explanation that has been described in the background above, then taken a problem Statement are to implement embedded in an encrypted *.txt file message used a vigenere cipher algorithm in a wav audio file with LSB (Least Significant Bits) Method and The variation in the size of the audio and the size of the text messages contained in the audio file, as well as the execution time and sound quality generated by the audio file that has been embedded a secret message.

2. Research Method

2.1 Cryptography

Cryptography comes from Greek: “cryptos” means “secret”, while “graphein” means “writing”, so Cryptography means “secret writing”. Cryptography is a science and art to maintain

the confidentiality of the message by encoding it into a form that can't be understood its meaning [6]. Cryptography has existed and used since centuries ago known as classic cryptography, which works in alphabetic character mode. With the help of digital computing technology, cryptographic algorithms have developed in a modern way. Modern cryptography uses the same idea as classical cryptography but does not operate in alphabetic character mode as in classical cryptographic algorithms. Modern cryptography operates in bit mode, which means all data and information (key, plaintext, and ciphertext) are expressed in binary, 0 and 1.

One of the classic algorithm techniques with numerical substitution techniques that is easy to understand and implement is Vigenere Cipher. Vigenère Cipher was made by Blaise de Vigenère in the 16th century, Vigenere is a method of encoding alphabetical text using Caesar's row of passwords based on a series of letters on a keyword. The Vigenère algorithm can be expressed mathematically, using summation and modulus operation:

Encryption algorithm as shown Equation 1.

$$Ci \equiv (Pi + Ki) \, mod \, 26 \quad (1)$$

Decryption algorithm seen in Equation 2.

$$Ci \equiv (Pi + Ki) \, mod \, 26 \quad (2)$$

Where:
Ci = the decimal value of i-ciphertext character,
Pi = the decimal value of i-plaintext character,
Ki = the decimal value of i-key character (assuming the decimal number of characters
A = 0, B = 1 .., Z = 25).

If the decryption is negative, then the value is added to the number 26 to get plaintext [6]. The key found on the Vigenere cypher has a certain length. The length of the key may be shorter or equal to the length of the plaintext. If the key find length is less than the length of the plaintext, then the key will be repeated periodically until the key length is equal to the length of the plaintext [7]. So it will produce the ciphertext of the substitution process between plaintext and key as follow in Figure 1.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Figure 1. Alphabeth Indexs

2.2 Steganography

The term steganography comes from two Greek words "steganos" and "graphy". "steganos" which means closed or secret and "graphy" which means writing or drawing. Steganography is a hidden or secret writing. In general, steganography is the process of hiding the communication media, which can be text, sound or image to another medium. During World War II, steganography was used to conceal text of messages in other messages [8]. The steganography technique consists of two different media. One medium serves as a medium of information (secret message) and other media serves as the bearer of such information (media container). In Steganography there are several terms, namely:

1. Hidden text or embedded message is Message or information is hidden.
2. Covertext or cover-object is message used to hide embedded messages.
3. Stegotext or stego-object is messages that already contain embedded messages. In digital steganography, either hidden text or cover text can be text, audio, images, or video.
4. Steganography Technique is the purpose of steganography techniques is to hide the existence of messages.

One of steganography algorithm is LSB (Least Significant Bit). The LSB method is the simplest and easiest method of steganography to implement. This method uses digital audio as cover text [9]. In the order of bits in a byte (1 byte = 8 bits), Figure 2, there are the least significant bits (MSB) and least significant bits (LSBs). For example, byte of 01111011, bit number 0 (first, underlined) is bit MSB, and bit number 1 (last, underlined) is bit LSB. The LSB bit only changes the byte value one higher or one lower than the previous value. So that only a few significant of the bits are changed then visually invisible to humans [2].

Examples before adding bits are:

10100001 00101010 10101110 10101110 00100011
00110010 11001011 11001000 10101010 10100011

The secret message (which has been converted to binary system) eg:'1010111010', then every bit of the message replaces the LSB position to be (underlined):

10100001 00101010 10101111 10101110 00100011
00110011 11001011 11001000 10101011 10100010

In this case, only four bits need to be changed. On average, only half of the bits in audio need to be modified to hide secret messages using the maximum cover size. The resulting change made on the least significant bit is too small to be recognized by the human eye, so the message is effectively hidden [8].

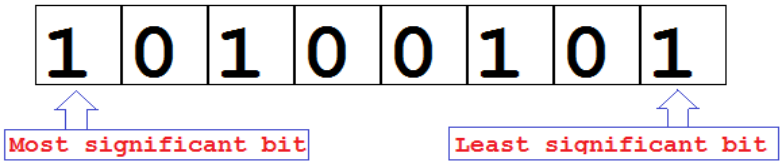

Figure 2. MSB and LSB

3. Results and Discussion

The data used in this study there are 15 * .wav audio as a container or audio cover and 3 *.txt file as a message to be inserted into the audio cover. Table 1 is an Audio cover that is used as a research object taken from a website on the internet with links: https://freesound.org/.

Table 1. Audio Cover

File Name	Duration	Size	Bit rate
Dolphin.wav	00:06	1,04 MB	1411
mark1111111__beat-120bpm-05	00.07	1,26 MB	1411
Donkey.wav	00:08	1,36 MB	1411
fullmetaljedi__low-dirty-loop2.wav	00:09	3,51 MB	3072
luckylittleraven__harp-tinkly-riff-2.wav	00:11	1,88 MB	1411
savina2000__giro-guitar-ableton.wav	00:13	2,26 mb	1411
zagi2__rocker.wav	00:16	2,69 MB	1411
bleepingcreepers__subnautica-twisty-bridges-biome-music.wav	00:20	3,76 MB	1536
jimmyfisher__dr0000-0634.wav	00:30	5,04 MB	1411
luckylittleraven__harp-wild-run-down-long.wav	00:31	5,36 MB	1411
setuniman__preoccupied-1q21.wav	00:34	5,87 MB	1411
klavo1985__club-synth-by-kk-demo-final.wav	00:51	4,35 MB	705
toiletrolltube__hellocatfood-b6b7-o.wav	01:00	10,1 MB	1411
neolein__spring-theme	01:03	5,35 MB	705
gis-sweden__electronic-minute-no-26-affordance	01:41	18,6 MB	1536

Table 2 is the message * .txt file hidden in audio cover in the research process:

*Table 2. Message *.txt*

Text Name	Character	Size
4096character.txt	212 = 4096	4,00 KB
8192character.txt	213 = 8192	8,00 KB
16384character.txt	214 = 16384	16,0 KB
32768character.txt	215 = 32768	32,0 KB
65536character.txt	216 = 65536	64,00 KB

This research is implemented by simulation using Matlab application. In this section, we will describe the audio cover used, the * .txt file of messages embedded in the embedding and extraction process. Cryptographic simulation using Vigenere Cipher method and steganography simulation using LSB (Least Significant Bit) method.

3.1 Encryption Process

The encryption of messages *.txt files using vigenere cipher method and embedding in audio wav using Least Significant Bit (LSB). The process of embedding text secret in this research seen Figure 3.

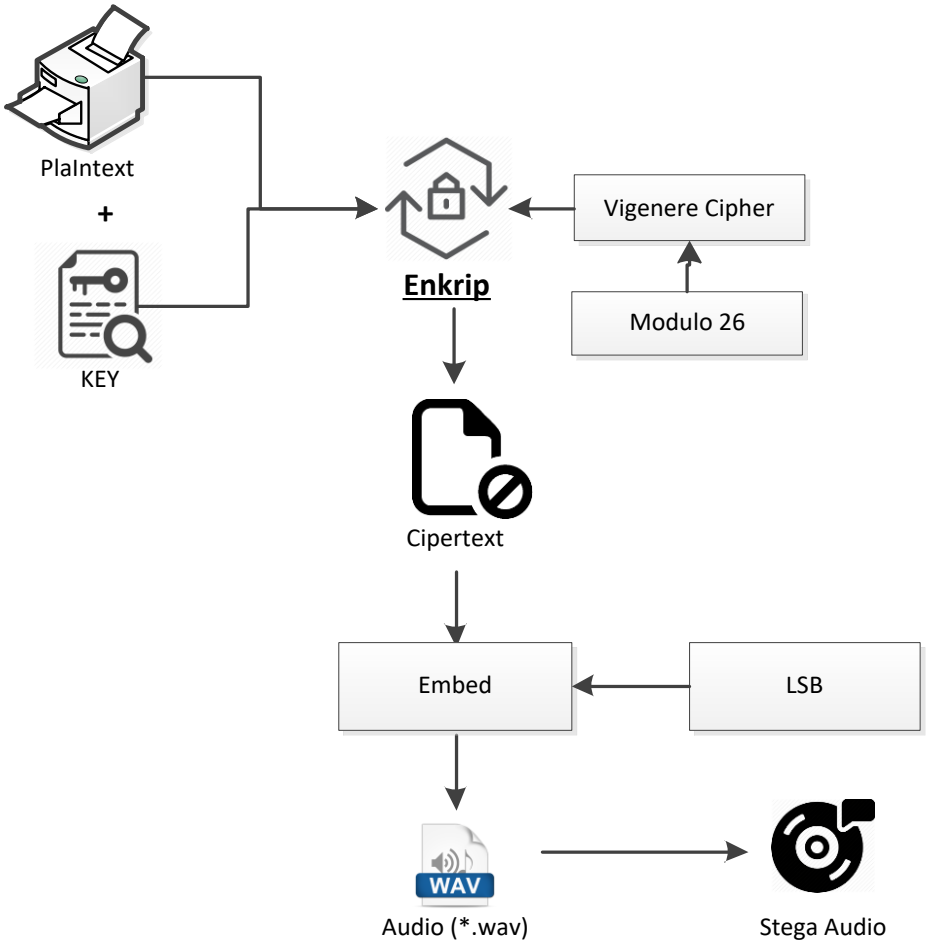

Figure 3. Proposed Embedding Process

Based on Figure 3, the process of inserting a secret text file using a combination of Vigenere Cipher and Least Significant Bit (LB) algorithms will be explained as follows in Table 3:

1. The first step of the plaintext input is a *.txt file. In this report, I use the plaintext example: ENCRYPTION OF TEXT and use the key: TIARA ANGGRAENY.
2. Then plaintext and key for encrypting using vigenere cipher algorithm with substitution method using modulo 26.

Table 3. Result of Encryption Process

Encryption plaintext + key	Encryption Process (Pi + Ki) mod 26	Result ciphertext	Ciphertext (Ci)
(E + T) mod 26	(4 + 19) mod 26	23 mod 26	X
(N + I) mod 26	(13 + 8) mod 26	21 mod 26	V
(C + A) mod 26	(2 + 0) mod 26	2 mod 26	C
(R + R) mod 26	(17+17) mod 26	34 mod 26	I
(Y + A) mod 26	(24 + 0) mod 26	24 mod 26	Y
(P + A) mod 26	(15 + 0) mod 26	15 mod 26	P
(T + N) mod 26	(19+13) mod 26	32 mod 26	G
(I + G) mod 26	(8 + 6) mod 26	14 mod 26	O
(O + G) mod 26	(14 + 6) mod 26	20 mod 26	U
(N + R) mod 26	(13+17) mod 26	30 mod 26	E
(O + A) mod 26	(14 + 0) mod 26	14 mod 26	O
(F + E) mod 26	(5 + 4) mod 26	9 mod 26	J
(T + N) mod 26	(19+13) mod 26	32 mod 26	G
(E + Y) mod 26	(4 + 24) mod 26	28 mod 26	C
(X + T) mod 26	(23+19) mod 26	42 mod 26	Q
(T + I) mod 26	(19 + 8) mod 26	27 mod 26	B

3. After doing the calculation using the vigenere cipher formula it will produce ciphertext or random message, where this ciphertext is a message that has been encrypted using vigenere cipher method. Here is a ciphertext or random message generated from the encryption process: "XYCIYPGOUEOJGCQB". The Ciphertext next will be embedding into audio cover using Least Significant Bit (LSB) method. Before embedding the ciphertext will be converted into binary form as shown Table 4.

Table 4. Converting Ciphertext to Binary

Ciphertext	ASCII	Binary
X	88	01011000
V	86	01010110
C	67	01000011
I	73	01001001
Y	89	01011001
P	80	01010000
G	71	01000111
O	79	01001111
U	85	01010101
E	69	01000101
O	79	01001111
J	74	01001010
G	71	01000111
C	67	01000011
Q	81	01010001
B	66	01000010
X	88	01011000

4. Then the binary result is picked up one bit at the back to serve as a message to be embedded into the cover audio.

3.2 Embedding Process

The embedding process of ciphertext on cover audio using Least Significant Bit (LSB) method, in Least Significant Bit (LSB) contains a binary number arrangement is show in Table 5.

Table 5. Embedding Process of LSB

Cover Audio	Message	Steganography Audio
0000000000000000	0	0000000000000000
1111111111000001	0	1111111111000000
0000000001111101	1	0000000001111101
0000000000000000	1	0000000000000001
1111111110000011	1	1111111110000011
1111111111000001	0	1111111111000000
0000000000000000	1	0000000000000001
1111111111000001	1	1111111111000001
0000000001111101	1	0000000001111101
0000000000111111	1	0000000000111111
1111111110000011	1	1111111110000011
1111111111000001	0	1111111111000000
0000000000111111	1	0000000000111111
0000000000111111	1	0000000000111111
0000000001111101	1	0000000001111101
0000000000000000	0	0000000000000000

3.3 Extraction Process

The extracting process steganography audio in this research seen Figure 4.

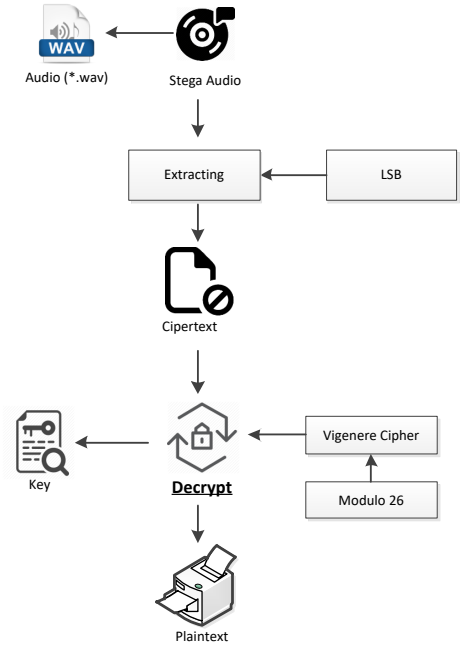

Figure 4. Extracting Process

Based on the Figure 4, the process of Extracting Stego Audio is the same as the process of embedding using the Least Significant Bit (LSB) method. Before retrieving the message, audio is parsed again to separate headers and audio samples. Then the message of each bit in the audio header that has been embed key will be taken and rearranged into the *.txt. At this stage, the plaintext in the form of *.txt file inserted in the stego audio is still not visible because the plaintext is still encrypted and still integral to the stego audio, therefore it takes a decryption process to display the plaintext contained in the stego audio. The results of the Least Significant Bit (LSB) process on the steganography audio cover did not change significantly. So, the audio that has been embedded with ciphertext will has small changed when compared with the original audio cover, as seen Table 6.

Table 6. Extractig of LSB

Steganography Audio	Message	Steganography Audio	Message
0000000000000000	0	0000000001111101	1
1111111111000000	0	0000000000111111	1
0000000001111101	1	1111111110000011	1
0000000000000001	1	1111111111000000	0
1111111110000011	1	0000000000111111	1
1111111111000000	0	0000000000111111	1
0000000000000001	1	0000000001111101	1
1111111111000001	1	0000000000000000	0

3.4 Decryption Process

From the encryption calculation process that has been described above produces ciphertext: “XVCIYPGOUEOJGCQB” which is embeded on the audio cover. Here is the calculation of the decryption process vigenere cipher method.

Table 7. Decryption Process of Vigenere

Decryption Ciphertext - Key	Decrption Process (Ci - Ki) mod 26	Result Plaintext	Plaintext (Pi)
(X-T) mod 26	(23-19) mod 26	4 mod 26	E
(V-I) mod 26	(24-8) mod 26	16 mod 26	N
(C-A) mod 26	(2-0) mod 26	2 mod 26	C
(I-R) mod 26	(8-17) mod 26	-9 mod 26	R
(Y-A) mod 26	(24-0) mod 26	24 mod 26	Y
(P-A) mod 26	(15-0) mod 26	15 mod 26	P
(G-N) mod 26	(6-13) mod 26	-7 mod 26	T
(O-G) mod 26	(14-6) mod 26	8 mod 26	I
(U-G) mod 26	(20-6) mod 26	14 mod 26	O
(E-R) mod 26	(4-17) mod 26	-13 mod 26	N
(O-A) mod 26	(14-0) mod 26	14 mod 26	O
(J-E) mod 26	(9-4) mod 26	5 mod 26	F
(G-N) mod 26	(6-13) mod 26	-7 mod 26	T
(C-Y) mod 26	(2-24) mod 26	-22 mod 26	E
(Q-T) mod 26	(16-19) mod 26	-3 mod 26	X
(B-I) mod 26	(1-8) mod 26	-7 mod 26	T

Based on Table 7, the ciphertext has been decrypted using the Vigenere cipher method and using the same key as the encryption process generates the plaintext or the original message as follows: “ENCRYPTION OF TEXT”. This test is performed to determine the quality of steganography audio compared with the original cover. In this study, test the quality of audio steganography and original cover using MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio), and also execution time. MSE is the average mean squared value between the original audio (audio cover) and the audio of the embedding (stego audio). PSNR is the ratio between the maximum value of a signal as measured by the magnitude of the noise affecting the signal. PSNR is usually measured in decibels (dB). Those values are used to determine the audio quality of the cover before and after the message is inserted. The lower the MSE value and the higher the PSNR value means the better the audio and image quality. Here are the values of MSE and PSNR for 45 test data.

Based on test results in Table 8, Audio 15 is the best audio compared to other audio. So, the author gives a different color mark. Good audio quality has a minimum value of 30 dB PSNR [10]. Audio 15 has a smaller MSE value and a larger PSNR value than any other audio.

Based on test results Figure 5 and Figure 6 in Table 9 and Table 10, Audio 15 is the best audio compared to other audio. So, the author gives a different color mark. Good audio quality has a minimum value of PSNR 30 dB. Audio 15 has a smaller MSE (0.001656) value and a larger PSNR (124.138499 dB) value than any other audio when inserted messages *.txt file with character 4096.

Table 8. Result fo MSE, PSNR and BER

Audio	Embedding message file*.txt in 16384 Character			
	MSE	PSNR (dB)	Time (s)	BER (%)
Audio 1	0.116797	105.655142	0.329098	24.425592
Audio 2	0.083007	107.138296	0.354223	24.425592
Audio 3	0.089764	106.798462	0.317113	24.425592
Audio 4	0.034668	110.930140	0.398338	24.425592
Audio 5	0.064575	108.228849	0.323223	24.425592
Audio 6	0.053958	109.008876	0.337654	24.425592
Audio 7	0.045510	109.748443	0.344580	24.425592
Audio 8	0.032611	111.195788	0.572668	24.425592
Audio 9	0.024339	112.466438	0.427146	24.425592
Audio 10	0.022744	112.760879	0.422298	24.425592
Audio 11	0.020862	113.135880	0.451624	24.425592
Audio 12	0.028116	111.839980	0.391826	24.425592
Audio 13	0.012079	115.509003	0.590439	24.481437
Audio 14	0.022809	112.748460	0.465579	24.425592
Audio 15	0.006580	118.147070	0.898750	24.425592
Avg	0,043895	111,0208	0,441637	24,42932

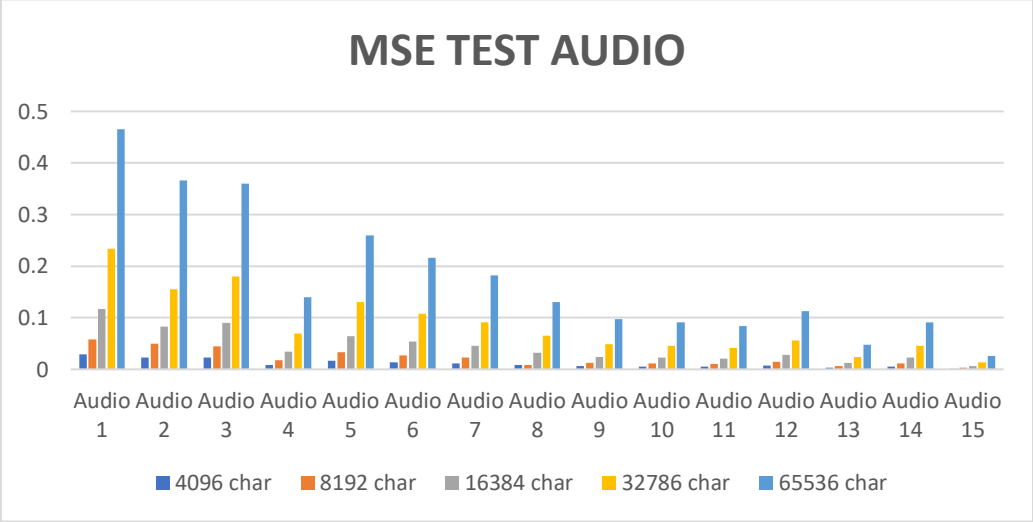

Figure 5. Evaluation of Audio Result using MSE

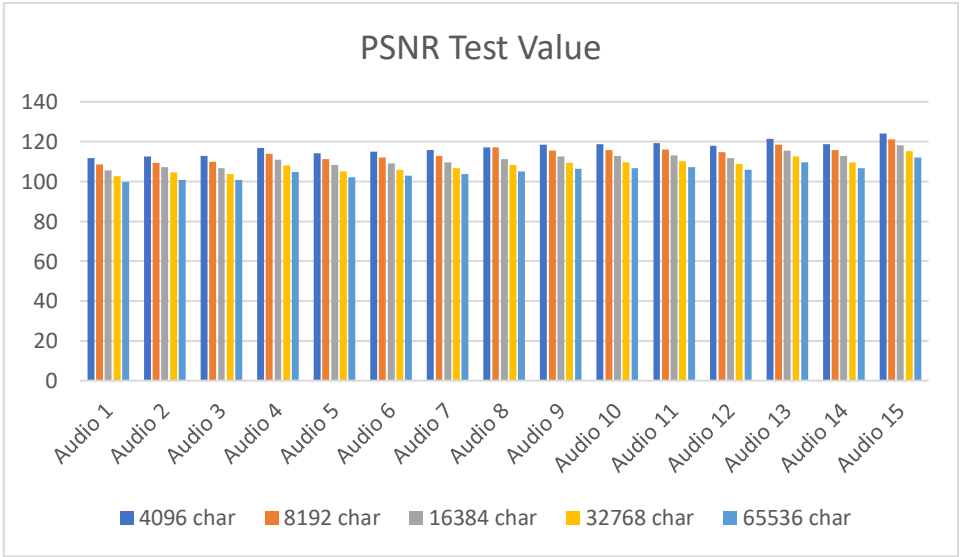

Figure 6. Evaluation of Audio Result using PSNR

Table 9. MSE Test Audio

Audio	4096 char	8192 char	16384 char	32786 char	65536 char
Audio 1	0.029212	0.058153	0.116797	0.233658	0.465891
Audio 2	0.023136	0.050064	0.083007	0.154897	0.365757
Audio 3	0.022563	0.044773	0.089764	0.179957	0.36037
Audio 4	0.008635	0.017345	0.034668	0.069695	0.139321
Audio 5	0.016261	0.032965	0.064575	0.130139	0.259744
Audio 6	0.013641	0.026883	0.053958	0.107958	0.215852
Audio 7	0.011392	0.02266	0.04551	0.090851	0.182345
Audio 8	0.008211	0.008211	0.032611	0.065205	0.130476
Audio 9	0.006036	0.012106	0.024339	0.048617	0.09723
Audio 10	0.005759	0.011402	0.022744	0.04558	0.091085
Audio 11	0.005227	0.010491	0.020862	0.041691	0.083435
Audio 12	0.007049	0.014079	0.028116	0.056278	0.11235
Audio 13	0.003033	0.006044	0.012079	0.024077	0.048157
Audio 14	0.005788	0.01151	0.022809	0.045821	0.091415
Audio 15	0.001656	0.003287	0.00658	0.013157	0.026199

Table 10. PSNR Test Value

Audio	4096 char	8192 char	16384 char	32768 char	65536 char
Audio 1	111.67385	108.683731	105.655142	102.64366	99.646624
Audio 2	112.68651	109.334196	107.138296	104.429025	100.697543
Audio 3	112.795543	109.819346	106.798462	103.777773	100.761983
Audio 4	116.966739	113.93779	110.93014	107.897438	104.889285
Audio 5	114.218081	111.148913	108.228849	105.185393	102.184009
Audio 6	114.981106	112.034695	109.008876	105.996919	102.987904
Audio 7	115.763572	112.776825	109.748443	106.746193	103.720533
Audio 8	117.185608	117.185608	111.195788	108.186668	105.17416
Audio 9	118.522315	115.499388	112.466438	109.46157	106.451456
Audio 10	118.725734	115.759593	112.760879	109.741768	106.735007
Audio 11	119.146755	116.12137	113.13588	110.129063	107.115973
Audio 12	117.848216	114.843722	111.83998	108.826062	105.823746
Audio 13	121.510137	118.516344	115.509003	112.513394	109.502892
Audio 14	118.704193	115.718541	112.74846	109.71878	106.719276
Audio 15	124.138499	121.160878	118.14707	115.137748	112.146545

4. Conclusion

Based on the research result, it can be concluded that the purpose of this research is to improve the audio quality of wav on crypto-stegano digital audio security system with the implementation of vigenere and LSB combination method has been reached, this can be proved by the following conclusion:

1. Application of insertion of encrypted messages with vigenere cipher algorithm in wav audio file with LSB (Least Significant Beat) method has been successfully applied
2. In the embedding process using combinations of vigenere and LSB methods, Audio 15 is the best audio compared to other audio. Good audio quality has a minimum value of 30 dB PSNR [1]. Audio 15 has a smaller MSE (0.001656) value and a larger PSNR (124.138499) value than any other audio when embeded messages *.txt file with character 4096.

References

[1] N. Kaur and S. Behal, *"Audio Steganography Techniques-A Survey,"* Journal of Engineering Research and Application, *Vol. 4, No. 6, Pp.* 94–100, 2014.
[2] A. Binny and M. Koilakuntla, *"Hiding Secret Information Using LSB Based Audio Steganography,"* in 2014 International Conference on Soft Computing and Machine Intelligence, Pp. 56–59, 2014.
[3] H. K. Qattous, *"Hiding Encrypted Data into Audio File,"* Vol. 17, No. 6, Pp. 162–170, 2017.
[4] R. Chowdhury, D. Bhattacharyya, S. K. Bandyopadhyay, and T. Kim, *"A View on LSB Based Audio Steganography,"* Vol. 10, No. 2, Pp. 51–62, 2016.
[5] M. Baritha Begum and Y. Venkataramani, *"LSB Based Audio Steganography Based On Text Compression,"* Procedia Engineering, Vol. 30, Pp. 703–710, 2012.
[6] A. Kriptografi, V. Dan, M. Fairuzabadi, and M. Kom, *"Steganografi Menggunakan Metode Least Significant Bit dengan Kombinasi Algoritma Kriptografi Vigenère dan Rc4,"* Vol. 5, No. September, Pp. 1–17, 2010.
[7] R. Damara Ardy, O. R. Indriani, C. A. Sari, D. R. I. M. Setiadi, and E. H. Rachmawanto, *"Digital Image Signature Using Triple Protection Cryptosystem (RSA, Vigenere, and MD5),"* in Proceeding of 2017 International Conference on Smart Cities, Automation and Intelligent Computing Systems, ICON-SONICS 2017, 2018, Vol. 2018–Januari.
[8] C. Science and M. Studies, *"Inside Audio and Video Media,"* No. C, Pp. 46–59, 2014.
[9] E. H. Rachmawanto, R. S. Amin, D. R. I. M. Setiadi, and C. A. Sari, *"A performance Analysis StegoCrypt Algorithm based on LSB-AES 128 bit in Various Image Size,"* in International Seminar on Application for Technology of Information and Communication, October 2017.
[10] Z. Fitri, *"Audio Digital Watermarking Untuk Melindungi Data Multimedia," TECHSI*, vol. 6, No. 1, Pp. 190–208, 2015.