Audio Steganography Using Two LSB Modification and RSA For Security Data Transmission

Bambang Harjito, Beni Sulistyarso, and Esti Suryani
Department of Informatics, Universitas Sebelas Maret, Surakarta, Indonesia.
estisuryani@staff.uns.ac.id

***Abstract*—Data security is the practice of keeping data protected from unauthorized access and it is one of the important keys to communication and transmission. In order to achieve to ensure privacy while protecting data. The security must be guaranteed. Cryptography is a method of providing security for data information in a particular form so that only those for whom it is intended can read and process it. While steganography is a method to secure data by hiding the message in another media. Many researches have already been done to develop a design involving both these methods, however these design does not resist to message attack and reduced capacity. In this paper, we purpose of using two-bit LSB is to increase the space for hidden message, and RSA to give one more security layer. The result shows that the steganography using two LSB modification and RSA is successfully achieved to protect data. The stego audio is robust to noise and crop attack, but it does not suffer on resampling. To evaluate the stego audio, we perform Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and Bit Error Rate (BER). The result show MSE, PSNR, and BER sequentially is 9.08875, 34.2775 db, and 17.995%.**

***Index Terms*—Data Security; Least Significant Bit Modification; RSA; Steganography.**

I. INTRODUCTION

The advanced of public technological development has led to a rapid increase in information data security that must be fulfilled in communicating. Information data can be publicly distributed. These data can be retrieved from individuals and agencies that remain a very important asset and need to be properly managed in order to benefit as great as possible with the likelihood of low risk [1]. There are two ways commonly used to secure information data, namely cryptography and steganography. Cryptography is a study of encoding message so that this message can not be read by others people who do not have a key. Steganography is the art of secret communication by hiding messages on seemingly innocuous objects [2]. Steganography and cryptography have various methods, one of them is a Least Significant Bit (LSB) and RSA. LSB and RSA have their advantages respectively. LSB is known as a simple, fast method and has a large enough insertion capacity, however it has weaknesses namely easily detected in messages [3]. This weakness can be covered by adding RSA methods. The combination of steganographic and cryptographic methods can form multiple layers of protection that can result in better security solutions for information sharing [4].

The challenge of this combination is that how to hide messages in the media to avoid its existence. The various media can be used and audio media is the most challenging media. This is because the human hearing system (HAS) has a dynamic range that can listen, so that humans become very sensitive to sound changes [5]. There are many researches which have been done to study involving cryptography and steganography. In 2012, Samir Kumar modified the LSB by using two LSB bits layers to insert messages [6]. In this study, he obtained greater message capacity, however he did not increase the resistance of messages to attacks. In 2013, Dyah Ayu modified the LSB applied to the image media [7]. Her research obtained stego files that survive the crop and noise attacks, however, the capacity of the message can be accommodated to be reduced using replication and RSA. In the Year 2015, Raviraj B. Vyavahare, Amit J. Bajaj, Hitesh P. Fuse and Pravin K Patil devised a system design involving steganography and cryptography in data transmission [4]. From the research, the data transmission protection system design is better and safer with steganography and cryptography.The purpose of this paper is to combine steganography and cryptography methods to be able to run optimally on audio media. The method used in this research is LSB modification using 2 bits of LSB and RSA. Then tested by measuring Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and Bit Error Rate (BER).

II. PROPOSE LSB BIT MODIFICATION AND RSA

In this section, we give general audio steganography for secure data transmission using LSB bit modification and RSA. This generally can be seen in Figure 1.

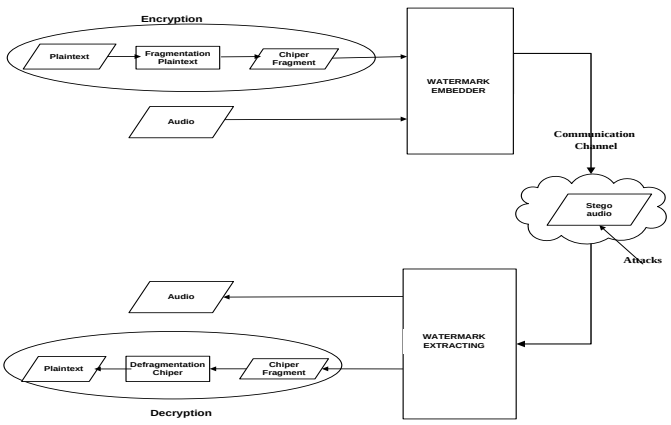


Figure 1**:** LSB bit modification and RSA for secure data transmission

A. Message fragmentation

Message Fragmentation is the process of breaking message into small or separate parts. This message is divided into 100 parts smaller message. This message sharing serves to simplify the storage process. The range of 100 fragments starts from fragment 0 to 99, so it takes 2 bytes to store the character. The following algorithm 1 for message fragmentation [7]:

Algorithm 1
Input: Message
Output: Fragment message
Process:

1. Initiation of variable number of fragments, i.e. 100.
2. Calculate the length of the text message
3. Divide the message into 100 fragments
4. If result = 0, then break the message character to 100 fragments
5. If the result is ≠ 0, then fragment 0 - 98 = fragment of the message with the size according to the quotient, while fragment 99 = message fragment with size fit for the remainder.

In addition to message security, fragment fragments are encrypted with RSA algorithms.

B. Message Encryption Fragments with RSA

The embedding process used LSB is easily recognized by attacker, to anticipate and to secure this, it needs RSA. Even though the message was successfully extracted from LSB audio, however the extracted message is still in the form of RSA cipher. Here is an RSA encryption algorithm. The following algorithm 2 for RSA encryption Fragment message.

Algorithm 2
Input: 100 Fragment message
Output: 100 Cipher message
Process:

1. Read 100 Fragment message
2. Change Fragment message into decimal form
   Compute *Cipher* using RSA encryption.
3. Merge 100 Fragment-based on numbering.

Disadvantages of RSA method, there is a change in the size of messages to be embedded in the audio frame. The size of the message in the form of a cipher is relatively larger than the original message. To reduce the effect is modified on the LSB process.

C. Modified LSB Method

Embed Cipher Fragment - Embedding message is the process of retrieving and inserting data to the audio file so that an audio stegofiles is obtained. The algorithm used to embed the message can be seen in algorithm 3:

Algorithm 3
Input : audio file, *cipher*, key
Output : audio *stegofile*
Process :

1. Change Fragment message into decimal form
2. Convert each audio frame to binary bit.
3. Calculate multiple duplicate messages
4. Take a 1-bit message.
5. Change 4th LSB to the 1st-bit message.
   - If 1st bit 4th LSB change form 0 to 1
     Case 1: If the 3rd bit and 5th bit are 1 and 1, then replace all the bits in the right bit to 4 to 0.
     Case 2: If the 3rd bit and 5th bit are 1 and 0, then replace all the bits in the right bit to 4 to 0.
     Case 3: If the 3rd bit and 5th bit are 0 and 1, then replace all the bits in the right bit to 4 to 1 and change the bit to the left of bit 4 to 0
     Case 4: If the 3rd bit and 5th bit are 0 and 0, replace all the bits in the right of the 4th bit to 1, and change the bit to the left of the 4th bit from 0 to 1 until the value 1 is found. Stop.
   - If the 4th LSB bit changes from 1 to 0
     Case 1: If the 3rd bit and 5th bit are 0 and 0, then replace all the bits in the right bit to 4 to 1.
     Case 2: If the 3rd bit and the 5th bit are 0 and 1, then replace all the bits in the right bit to 4 to 1.
     Case 3: If the 3rd bit and 5th bit are 1 and 0, then replace all the bits in the right bit to 4 with the value 0 and all the bits on the left of the 4th bit to 1.
     Case 4: If the 3rd bit and 5th bit are 1 and 1, then replace all the bits in the right of the 4th bit with the value 0, and replace the bit to the left of bit to 4 from 1 to 0 until it finds a value of 0. If value 0 is found Process stopped.
6. If the 4th LSB bit is the same as the original audio bit, there is no modification of bit insertion.
7. Take the next 1-bit message
8. Replace the last LSB bit with the second message bit.
9. The process is repeated until all messages are processed in LSB.
10. After all messages are processed, repeat Process as duplicated.

Extract Cipher Fragment - The extract process of the Fragment message is the process of retrieving the data that is inserted on the stegofile so that the message can be revealed again. The extract message algorithm can be seen in the following algorithm 4:

Algorithm 4
Input: audio stegofile, key *text*
Output: Message
Process:

1. Split each frame of audio
2. Take the 4th and 1st bits of the LSB from the audio frame
3. Find the key byte of the byte of the audio frame
4. Find the fragment number, fragment size and cipher fragment before entering the RSA decryption process.
5. Merge all message fragments into a unified message

Cipher Fragment Decryption with RSA - RSA decryption is used to recover the chiper fragments that have been found in the LSB extract process. The RSA decryption process uses the private key searched at the time of key generation. This key is transmitted in a secure path so it is only known by the recipient of the message. The RSA decryption process can be seen in the following algorithm 5:

Algorithm 5
Input: Fragment *Cipher*
Output: Fragment message
Process:

1. Take Fragmentchiper according to fragment number
2. Decrypt Fragmentchiper by using RSA key
3. Change the message into ASCII form
4. Save the message according to the order of fragments.

Testing - In this section, testing of LSB method in this research is divided into two parts, that are:

1. Stegofile quality test
   This test is intended to assess the quality of audio generated after the process embedding message. To assess the audio, Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Bit Error Rate (BER) are used
2. Testing message resilience against attack
   This test is aimed at measuring message resistance against multiple attacks on audio files, cropping, noise, and resampling.

III. Results and Discussion

In this paper, we used 8 Audio files of type wav and .au. These files are anderson.au, boygeorge.au, chcomb.au, radio_opening .au, elvis_riverside.wav, anthrax.wav,strokin.wav, welcome.wav. These audio files can be seen in Figure 2.

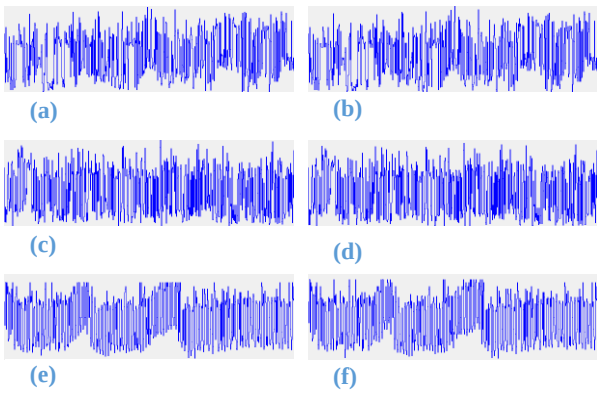
The file will be a medium for storing messages contained in the message.txt file. The content of the message.txt is a character with a post" AUDIO STEGANOGRAFI MENGGUNAKAN TWO LEAST SIGNIFICANT BIT MODIFICATION DAN RSA UNTUK KEAMANAN DATA TRANSMISI"

The result of the embedding test is an audio file that has been inserted message (stego audio). Preview waveform audio and audio stego can be seen in Figure 2.

Figure 3 is a sample waveform view of an audio file before and after embedding a message using a modified LSB. To extract the message, the audio stego is taken by 4th and 1st LSB bits. The bit is then rearranged to search for Fragment messages stored in the LSB.

From audio stego welcome.wav in Figure 3 can be found all Fragment message with number of 100 fragments. Fragment-Fragment can be seen in Table 1.

Fragment is founded at Table 1 then combine to one so that "AUDIO STEGANOGRAFI MENGGUNAKAN TWO LEAST SIGNIFICANT BIT MODIFICATION DAN RSA UNTUK KEAMANAN DATA TRANSMISI". The output that of the decryption can be seen in Figure 4.



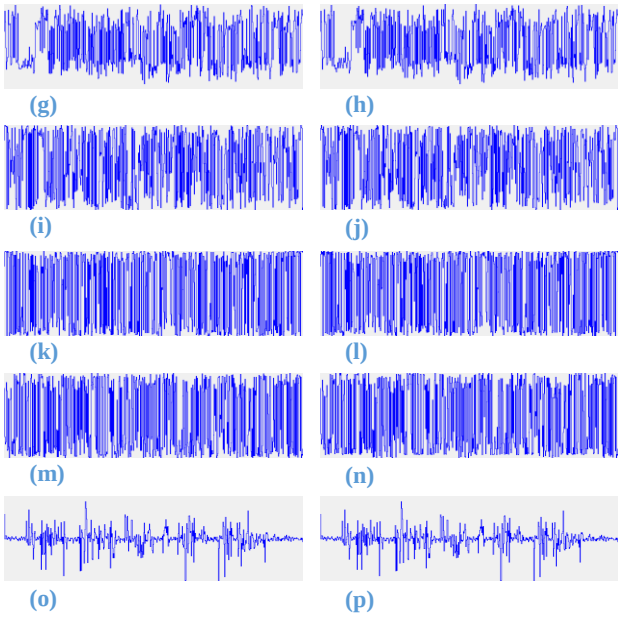


Figure 2: Waveform Audio (a) anderson.au (b) stego anderson.au (c) boygeorge.au (d) stego boygeorge.au (e) chcomb.au (f) stego chcomb.au (g) radio_opening.au (h) stego radio_opening.au (i) elvis_riverside.wav (j) stego elvis_riverside.wav (k) gang_anthrax.wav (l) stego gang_anthrax.wav (m) strokin.wav (n) stego strokin.wav (o) welcome.wav (p)stego welcome.wav

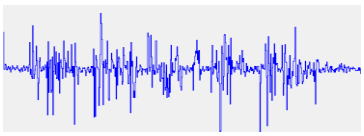


Figure 3: Preview waveform stego audio welcome.wav

Table 1
Extract Fragment message

Fragment	Chiper Fragment	RSA Decryption (ASCII)	Plaintext
0	0615	65	A
1	0869	85	U
2	0660	68	D
3	1784	73	I
4	1936	79	O
..	..	..	..
93	0660	68	D
94	0615	65	A
95	0692	84	T
96	0615	65	A
97	1184	32	(SPASI)
98	0692	84	T
99	2126 0615 3189 0784 3077 1784 0784 1784	82 65 78 83 77 73 83 73	RANSMI SI

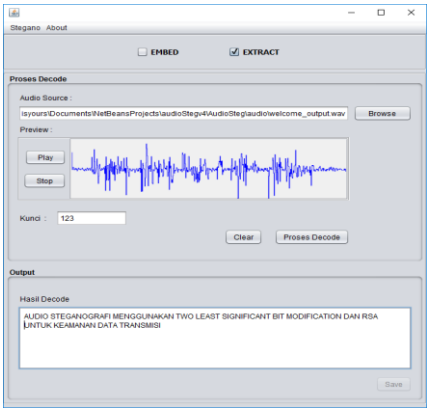


Figure 4: Display extract messages

Testing results from Process embed message on audio file can be measured by calculating the value of MSE and PSNR. The following results from the measurements of MSE and PSNR can be seen in Table 2.

Table 2
Calculation of MSE and PSNR

No	Audio	MSE	PSNR(db)	BER(%)
1	anderson.au	16,628	29,868	23,049
2	boygeorge.au	4,697	35,358	15,388
3	chcomb.au	13,005	30,935	18,172
4	radio_opening .au	5,313	34,822	12.29
5	elvis_riverside.wav	0,344	46,714	16,395
4	gang_anthrax.wav	14,288	30,526	25,912
7	strookin.wav	13,614	30,736	23,754
8	welcome.wav	4,821	35,245	8,997
	Mean	9.08875	34.2775	17.995

The result of the calculation of 8 stego audio samples obtained the average value of MSE, PSNR, and BER sequentially 9.08875, 34.2775 db, and 17.995%.

The next test is to test the attack on the audio stego file. The test is done by cropping, noise, and resampling. Table 3 is a test result of cropping attacks on audio stego. From testing the cropping message attacks can be extracted even though the audio experiences some crop variations. The next test is a noise attack. The result of noise attack test on stego audio can be seen in Table 4.

Table 1
Test attack cropping

No	Audio	Cropping (%)								
		10	20	30	40	50	60	70	80	90
1	anderson.au	✓	✓	✓	✓	✓	✓	✓	✓	×
2	boygeorge.au	✓	✓	✓	✓	✓	✓	✓	✓	✓
3	chcomb.au	✓	✓	✓	✓	✓	✓	×	×	×
4	radio_opening .au	✓	✓	✓	✓	✓	✓	✓	✓	✓
5	elvis_riverside .wav	✓	✓	✓	✓	✓	✓	✓	✓	✓
4	gang_anthrax. wav	✓	✓	✓	✓	✓	✓	✓	✓	✓
7	strookin.wav	✓	✓	✓	✓	✓	✓	✓	✓	✓
8	welcome.wav	✓	✓	✓	✓	✓	✓	✓	✓	✓

Table 2
Noise Attack Test

No	Audio	Noise (%)								
		10	20	30	40	50	60	70	80	90
1	anderson.au	✓	✓	✓	✓	✓	✓	✓	✓	×
2	boygeorge.au	✓	✓	✓	✓	✓	✓	✓	✓	✓
3	chcomb.au	✓	✓	✓	✓	✓	×	×	×	×
4	radio_opening .au	✓	✓	✓	✓	✓	✓	✓	✓	✓
5	elvis_riverside .wav	✓	✓	✓	✓	✓	✓	✓	✓	✓
4	gang_anthrax. wav	✓	✓	✓	✓	✓	✓	✓	✓	✓
7	strookin.wav	✓	✓	✓	✓	✓	✓	✓	✓	✓
8	welcome.wav	✓	✓	✓	✓	✓	✓	✓	✓	✓

Table 4 shows the message can still be extracted again despite having variations of noise added. The next test is to resampling the audio stego. Resampling test results can be seen in Table 5.

Table 3
Test Resampling Attack

No	Audio	Resampling (Hz)					
		8000	11025	16000	22050	37800	44100
1	anderson.au	✓	×	×	×	×	×
2	boygeorge.au	✓	×	×	×	×	×
3	chcomb.au	✓	×	×	×	×	×
4	radio_opening .au	✓	×	×	×	×	×
5	elvis_riverside. wav	×	✓	×	×	×	×
4	gang_anthrax. wav	×	✓	×	×	×	×
7	strookin.wav	×	✓	×	×	×	×
8	welcome.wav	×	✓	×	×	×	×

In the resampling attack test, there is a complete audio change, so that the LSB data also changed. From table 5 it can be seen that messages can be extracted back when the audio is rebuilt with the same sample rate.

IV. CONCLUSION

Implementation of Two Least Significant Bit and RSA Methods have been successfully implemented. Messages can be hidden into audio and it can be extracted again. The MSE, PSNR, and BER values of the 8 consecutive audio stego samples were 9.08875, 34.2775 db, and 17.995%. The value of MSE, PSNR and BER indicates the resulting audio stego is quite good, although some audio causes noise because BER is large enough. The resulting audio stego is able to withstand crop and noise attacks, but messages are lost when a thorough attack like resampling. In the next research can be studied more LSB bit effect on the quality of the resulting audio. So it can be done the development of LSB modification method to make audio stego more robust against other audio attacks.

REFERENCES

[1] KOMINFO RI, Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik, Jakarta, 2011.

[2] S. H. Monalisa, "Steganografi Pada File Citra Untuk Pengamanan Data Menggunakan Metode Spead Spectrum," *Pelita Informatika Budi Darma*, pp. 75-79, 2014.

[3] A. Prihanto and S. S. Wahyuningsih, "Penyembunyian dan Pengacakan Data Text Menggunakan Steganografi dan Kriptografi Triple DES Pada Image," 2009.

[4] R. B. Vyavahare, A. J. Bajaj, H. P. Fuse and P. K. Patil, "Study of Secure Data Transmission Using Audio File," *International Journal of Advanced Research in Computer and Communication Engineering* , pp. 146-149, 2015.

[5] B. G. B. Prof. Samir Kumar, "LSB Modification and Phase Encoding Technique of Audio Steganography Revisited," *International Journal of Advanced Research in Computer and Communication Engineering*, pp. 1-4, 2012.

[6] D. A. Listiyoningsih. *Modifikasi Least Significant Bit Untuk meningkatkan Ketahanan Pesan terhadap Cropping dan Noise*. Surakarta, 2014.

[7] E. Cole, Hidden *In Plain Sight: Stegaography and the Art of Cover Communication*. United States: Wiley Publishing, 2003.

[8] D. S. B. P. P. B. Sheetal A. Kulkarni, "An Optimized and Secure Audio Steganography for Hiding Secret Information - Review," *Journal of Electronics and Communication Engineering*, pp. 12-16, 2013.

[9] M. I. Khan, I. H. Sarker, K. Deb and H. Furhad, "A NEW Audio Watermarking Method Based on Discrete Cosine Transform With a Gray Image," *International Journal of Computer Science & Information Technology (IJCSIT)* , pp. 119-128, 2012.

[10] S. V. Asyani and T. Rahajoeningroem, "Transceiver Audio Wireless One Point to Multipoint untuk Laboratorium Bahasa," *TELEKONTRAN*, pp. 62-73, 2014.

[11] N. N. Alfiah, "Digitalisasi Koleksi Audio Dengan Aplikasi Software Magix Audio Cleaning Lab Dalam Pustaka Pandang Dengar (Audio Visual) di UPT PerpustakaanInstitut Seni Indonesia Surakarta,", Surakarta, 2010, [Unpublished].

[12] J. Filipus, "Perbandingan Digital Steganografi Pada Media Image, Audio, Video dan Teks serta Kekuatannya Terhadap Steganalisis," 2010.

[13] M. M. A. Azim and X. Jiang. *Wireless Sensor Multimedia Networks*, Boca raton: CRC Press, 2015.