Journal of Theoretical and Applied Information Technology
15th June 2019. Vol.97. No 11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IMPROVING AUDIO FILES SECURITY BY USING RIVEST SHAMIR ADLEMAN ALGORITHM AND MODIFIED LEAST SIGNIFICANT BIT ON THE RED CHANNEL METHOD

[1]DIAN RACHMAWATI,[2]FEBRIYANA PRATIWI, [3]SRI MELVANI HARDI

[1,2,3]Departemen Ilmu Komputer, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Sumatera Utara, Jl. Universitas No. 9-A, Kampus USU, Medan 20155, Indonesia

E-mail: [1]dian.rachmawati@usu.ac.id

ABSTRACT

The audio is digital media that is widely used in the message exchange as it is easy to use and can be accessed anywhere. The security aspect is very important if the audio to be delivered contain secret information. Using cryptography, message content can be hidden so that the delivery of a message to a recipient can be more secure. The security of RSA (Rivest Shamir Adleman) lies in the difficulty of resolving the private key. This is because looking for prime factors of large integers is not easy. With a longer bit key, it becomes more difficult to solve. In practice, these cryptographic algorithms have a weakness that easily raises suspicions because of the character of the message changed or scrambled into another form that is not meaningful. So that the confidentiality of the message needs to be made safer, concealment of messages to address the cryptographic algorithms that are used, the author combines the cryptographic method with a method of steganography. MLSB method (Modified Least Significant Bit) on the Red Channel is an improvement over the method of LSB, in which the only one selected color channel to store the information. The bit that is used is the last bit of the red channel value is binary. The results showed that the combination of the two algorithms is successfully done and the possibility of knowing the existence of an audio message in the picture is very small.
Keywords: Ri*vest Shamir Adleman, Modified Least Significant Bit, Audio, Cryptography*

1. INTRODUCTION

One of the digital media that can be used in the delivery of messages in the form of auditive symbols is audio. Audio media is used because it is easy to use and followed by ease of accessing. In sending messages via audio media and when it arrives in the recipient of the message, the information must remain confidential and authentic or unmodified. Therefore required cryptographic techniques to maintain the security of data contained in the audio file.

Cryptography is the study of mathematical techniques related to information security aspects such as confidentiality, data integrity, and authentication [7]. The most popular cryptographic algorithm is the RSA (Rivest Shamir Adleman) algorithm [1]. RSA algorithm consists of an encryption algorithm and a decryption algorithm. In cryptography, the character of the conveyed message is changed or randomized into another meaningless form so that because of its imprecision the message in cryptography is easy to arouse suspicion. So after the file is encrypted, we need to hide the file into another file so that non-interested parties are not suspicious in viewing the file. This step is often referred to as steganography.

Steganography is the science and art of hiding messages so that the existence of messages is undetectable by the human senses. Steganography is the term used to describe the hiding of data in images to avoid detection by attackers [2]. A simple and easy-to-implement steganography method is the LSB (Least Significant Bit) method. Least Significant Bit steganography is one such technique in which least significant bit of pixels of the image is replaced with data bits [3]. The LSB technique is one of the simplest ways of implanting the message [8]. Each pixel in a 1 by 3-byte image consists of pixel segments, for example, Red, Green, Blue. In this method will be inserted messages that have been converted to binary to the far right bit of the pixel segment [4]. By using the binary insertion pattern in the rightmost bit of the Red Green and Blue channel, the insertion concept with the LSB method is very predictable. Because of these

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

weaknesses, a technique is needed to camouflage the shortcomings of the LSB. Therefore, in this study, the research is only using the Red channel in its insertion.

Many steganographic systems incorporate steganographic methods with cryptographic methods to gain more security. Cryptography aims to hide the message content and steganography aimed at hiding the existence of the message. The goal of steganography is to hide the secret message from a third party[5]. The advantage of steganography over cryptography is that its messages do not attract other people's attention. The core message is retained, only in its delivery obscured or hidden in various ways. So only the legitimate recipient can know the core message.

2. LITERATURE REVIEW

2.1 Digital Audio

Digital audio is a digital version of the analog sound. Analog voice converter to digital sound requires a tool called Analog to Digital Converter (ADC). The ADC will change the amplitude of the analog wave into the time interval (sample) to produce a digital representation of the sound. Understanding the ADC's performance has an important role to read in the future communication trends.[11]

Digital audio is the presentation of the original sound. In other words, digital audio is a sound sample. Digital recording quality is calculated when the sample is taken, the number of samples taken or calculated in kilohertz or one thousand samples per second). The three most frequently used samples in multimedia are CD quality 44.1 kHz, 22.05 kHz and 11,025 kHz with sample sizes of 8 bits and 16 bits. The 8-bit sample size provides 256 units of description of dynamic distance or amplitude (the sound level at one time). The size file of digital audio depends on the sampling rate, the resolution and the channel (Stereo or Mono).

2.2 AMR Audio File

AMR (Adaptive Multi-Rate) is a compressed audio file, this file has AMR extension, and is very small. This file is kept secret from an encoder that adjusts the processing and streaming capabilities of the MCU / CPU so that the resulting file has a bit-rate that matches the MCU / CPU / Processor used. This file is usually more embedded on a mobile device (Embedded File) and can be transformed in the form of an MP3 file.

2.3 Cryptography

Cryptographic techniques used in encrypting messages are done by hiding or coding the original message. Furthermore, the sender of the message will encode the initial message into codes that can only be read by the recipient of the message. This process is called Encryption. The recipient of the message then returns the codes that have been received into the original message using the key sent by the sender of the message. This process is called Decryption. Cryptography is divided into two, namely symmetrical and asymmetrical. Symmetric cryptography has the same key in the encryption and decryption process, so the security of this key symmetry system lies in the secrecy of the key. Examples of symmetrical algorithms are Permutation Cipher, Substitute Cipher, Hill Cipher, OTP, RC6, Twofish, Magenta, FEAL, SAFER, LOCI, CAST, Rijndael (AES), Blowfish, GOST, A5, Kasumi, DES (Data Encryption Standard) and IDEA (International Data Encryption Algorithm). Asymmetric cryptography has two keys in the process of encryption and decryption, where the encryption key is public (public key), and the decryption key is confidential (private key). Examples of well-known asymmetrical algorithms are RSA (Rivest Shamir Adleman), ECC (Elliptic Curve Cryptography and ElGamal). The encryption and decryption process is shown in figure 1.

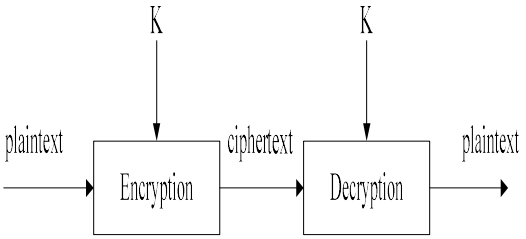


Figure 1.The Illustration Of Cryptography

2.4 Digital Image

In general, digital image processing shows the processing of two-dimensional images using a computer. In a broader context, digital image processing refers to the processing of every two-dimensional data. The digital image is an array that contains real and complex values that are represented by a certain row of bits.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2.5 Steganography

Steganography is a technique to hide secret messages in a media that can be seen by others so that no one knows or realizes that there is a secret message except the recipient of the message. In general, steganographic messages appear in various formats such as text, images, videos, audio, and other messages. This visible message is cover media.

To measure resistance to steganography, a measuring instrument is needed to be used as a parameter. The measuring instrument is Peak Signal to Noise Ratio (PSNR). PSNR is a comparison between the maximum value of the signal as measured by the amount of noise that affects the signal. To determine the PSNR, it must first be determined the mean square error (MSE). The steganography process is shown in figure 2.

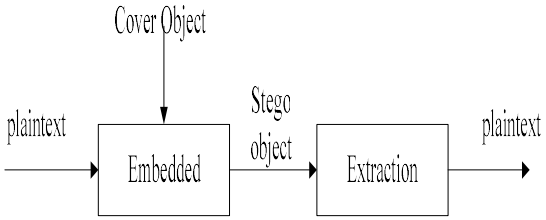


Figure 2. The Illustration Of Steganography

2.6 Least Significant Bit

Least significant bits are part of the binary data base (base two) which has the least significant value. Its location is the far right of the row of bits. While the most significant bit is the opposite, namely the most meaningful / largest number and is located next to the far left. ``LSB is a binary data insertion method that works by replacing the last bit of each pixel value cover with the secret message bits. Before inserting a secret message into the cover, of course, both must be converted into binary forms so that the insertion process can be done. In each byte of the image pixel, there is the least significant bit (Least Significant). The 24-bit bitmap file, then each pixel (dot) in the image consists of three red, green and blue (RGB) arrangements, each of which is composed of 8-bit numbers (bytes) from 0 to 255 or with binary formats 00000000 to 11111111 [10].
Least significant bits are often used for the purpose of inserting data into another digital media, one of which uses the Least significant bit as a concealment method is audio steganography.

3. METHOD

This research uses the RSA algorithm for encoding and decoding messages and the MLSB on the Red Channel method for the process of concealing the existence of messages, including the process of embedding and extraction of audio messages in an image.

3.1 Rivest Shamir Algorithm

Encryption is a method that can be used in data security. Data encryption cannot be read because the plaintext (original text) has been converted to unreadable text or called ciphertext. There are many cryptographic algorithms that can be used, based on the nature of the key divided into two, namely symmetric which only uses one secret and asymmetric key (public key algorithm) that uses the public key and secret key.
The RSA algorithm was made by three researchers from MIT (Massachusetts Institute of Technology) in 1976, namely Ron Rivest, Adi Shamir, and Leonard Adleman.

RSA algorithm security lies in the difficulty of factoring large numbers into prime factors. The factoring is done to obtain the private key. During the factoring of large numbers into prime factors have not found an effective algorithm, so long as it is also RSA algorithm security is guaranteed. The length of keys in bits can be set, with the longer the bits, the more difficult to solve because of the difficulty of factoring the two very large numbers, but also longer in the decryption process.

In making the code in the RSA algorithm has a way of working to create the public key and private key [9].

1. Generation of two prime numbers (integer) p and q, where $p \neq q$.
2. Calculate the value of $N = p \bullet q$, $(p \neq q)$; the number N is a security parameter, where the longer the value of N it is more difficult to solve.
3. Calculate $\varphi(N) = (p - 1)(q - 1)$.
4. Generate random key e with the condition:
   - $1 < e < \varphi(N$
   - gcd $(e, \varphi(N)) = 1$ e relatively prime.
5. Calculate the value of d with the condition:

- $e \bullet d \equiv 1 \pmod{\varphi(N)}$ or $e \bullet d \pmod{\varphi(N)} = 1$
- By trying the value d = 1,2,3,4, .. n to satisfy the equation.

Journal of Theoretical and Applied Information Technology
15th June 2019. Vol.97. No 11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

• e •d (mod φ (N)) = 1 The result of the algorithm is to obtain the public key (e, N) and private key (d, N).

The encryption process is performed using a public key. Plaintext is organized into blocks with procedures:

1. The recipient's public key (e) and mod N.
2. Plaintext is expressed with blocks m1, m2,…, mx until each block represents the value [0, N-1].
3. Each block n1 is encrypted into a block with the formula: $c_i = p_i^e \bmod N$

The decryption process is done by using the private key. Where messages that have been encrypted will be restored just like the original message. Each ciphertext block will be decrypted by the formula: $p_i = c_i^d \bmod N$

3.2 Modified Least Significant Bit on the Red Channel

To improve the effectiveness and safety of the LSB method, it is necessary to modify the method. The MLSB Red Channel is a modification of the LSB algorithm, where only one color channel is selected to store information. The bit used is the last bit of the binary value of the selected color channel which is red.

Steps for embedding the secret audio:

1. Input the cover image and file cipher.
2. Previously cipher files whose contents in decimal were first converted to hexadecimal, where the hexadecimal here is not the hexadecimal value of the previous decimal value, but the fractional form of the decimal value.
3. Convert the value of the cipher file into the binary array.
4. Embed the value of the secret binary array into R (red channel) of the cover image's pixel. A pixel can contain just 1 bit of the secret binary array's value.
5. Do step 3 until all the secret binary array's value have been embedded.

Steps for extraction the secret audio:

1. Input the right pair of the stego image and the key (the length of the message).
2. Get MLSB's value from the stego image's pixel that is chosen from the red channel, to get the binary array value of the cipher file.
3. Convert the cipher file's binary array value into the byte.

The architecture of the system was shown in figure 3 :

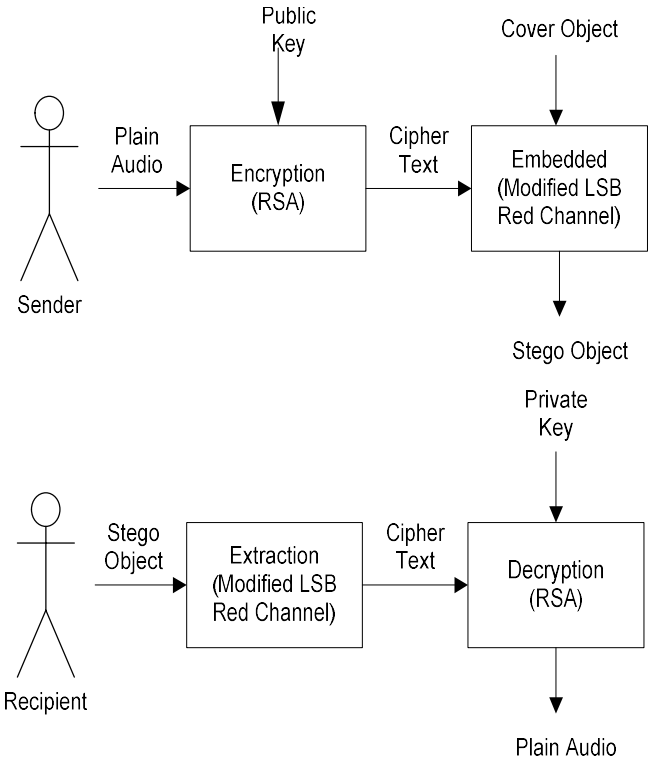


Figure 3. The Architecture Of The System

Example:

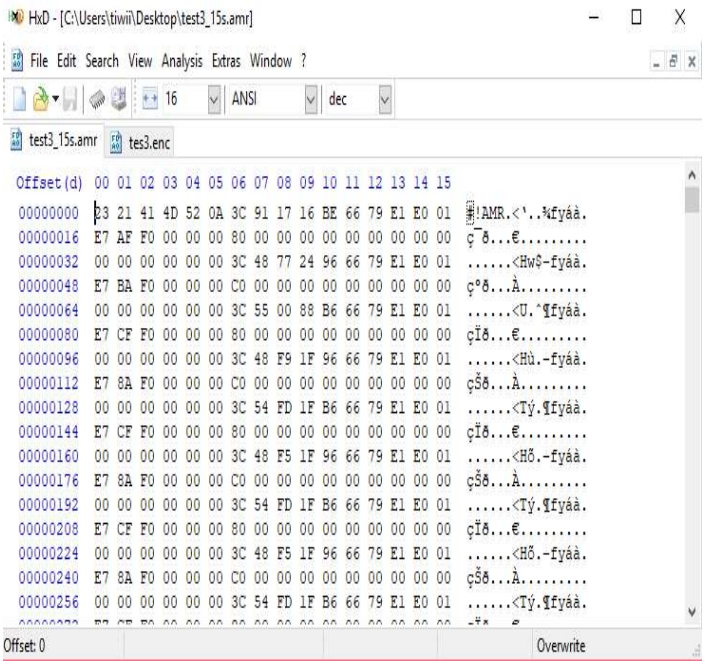


Figure 4. The Hexadecimal Value On AMR Audio Files Before Encrypted (Plaintext)

Journal of Theoretical and Applied Information Technology
15th June 2019. Vol.97. No 11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Generate the key :

- p = 79 and q = 29
- N = p•q = 79 x 29 = 2291
- φ (N) = (p - 1) (q - 1)
  = (79-1) (29-1)
  = 2184.
- e = 29
  gcd (e, φ (N)) = 1
  gcd (29,2184) = 1 (complied)
- d = 1205
  e • d (mod φ (N)) = 1
  29 • 1205 (mod 2184) = 1
  34945 (mod 2184) = 1 (complied)
- Public key (29, 2291) and private key (1205, 2291).

Encription process:

Cipher(P_1) = 35^{29} mod 2291
= 59975418370462576427266132086515426635742 1875 mod 2291
= 1311

Cipher(P_2) = 33^{29} mod 2291
= 10886900568230179568421170544636998209774 2753 mod 2291
= 1019

Cipher(P_3) = 65^{29} mod 2291
= 37539401358852377310116580942975915968418121 3890625 mod 2291
= 732

Table 1. Cipher file to be embedded

C_i	Decimal	Hexadecimal	Binary
C_1	$1311_{(10)}$	$13_{(16)}$, $11_{(16)}$, $FF_{(16)}$	$00010011_{(2)}$, $00010001_{(2)}$, $11111111_{(2)}$
C_2	$1019_{(10)}$	$10_{(16)}$, $19_{(16)}$, $FF_{(16)}$	$00010000_{(2)}$, $00011001_{(2)}$, $11111111_{(2)}$
C_3	$732_{(10)}$	$07_{(16)}$, $32_{(16)}$, $FF_{(16)}$	$00000111_{(2)}$, $00110010_{(2)}$, $11111111_{(2)}$

Embedding process:

Table 2. Embedding Process Into Cover Image 9x8 Pixels

	0	1	2	3	4	5	6	7	8
	R=11010110	R=10111100	R=11011110	R=11111111	R=11111111	R=11100010	R=11101101	R=11101000	R=11111010
0	G=220	G=242	G=235	G=231	G=240	G=240	G=237	G=217	G=210
	B=229	B=233	B=247	B=231	B=193	B=217	B=237	B=243	B=228
	R=10101101	R=10000010	R=10111101	R=11111111	R=11111111	R=11000101	R=11011011	R=11011100	R=11111000
1	G=182	G=230	G=215	G=204	G=229	G=224	G=219	G=197	G=190
	B=202	B=213	B=238	B=204	B=147	B=180	B=219	B=237	B=216
	R=10000100	R=01001001	R=10011101	R=11111111	R=11111111	R=10101001	R=11001001	R=10111011	R=11110101
2	G=11	G=219	G=195	G=153	G=216	G=209	G=201	G=144	G=161
	B=176	B=195	B=230	B=153	B=93	B=142	B=201	B=220	B=199
	R=00110011	R=00100111	R=01011011	R=11111111	R=11111111	R=01110000	R=10100101	R=10010000	R=11110010
3	G=63	G=199	G=155	G=101	G=206	G=173	G=165	G=92	G=130
	B=80	B=172	B=213	B=101	B=51	B=71	B=165	B=204	B=181
	R=00101000	R=00100100	R=00101110	R=11111111	R=11111010	R=01010100	R=01111100	R=10000000	R=11110000
4	G=42	G=182	G=117	G=63	G=190	G=130	G=124	G=57	G=108
	B=53	B=158	B=182	B=63	B=0	B=53	B=124	B=181	B=168
	R=00011010	R=00011100	R=00101010	R=11111111	R=11101010	R=01001101	R=01101111	R=01101110	R=11101100
5	G=32	G=140	G=108	G=9	G=178	G=119	G=111	G=49	G=70
	B=40	B=121	B=168	B=9	B=0	B=49	B=111	B=155	B=145
	R=00011000	R=00010101	R=00011111	R=10011110	R=10011110	R=00111000	R=01010010	R=01010101	R=11011000
6	G=23	G=105	G=78	G=0	G=143	G=87	G=82	G=38	G=22
	B=2	B=91	B=121	B=0	B=0	B=35	B=82	B=120	B=110
	R=00000000	R=00001011	R=00000000	R=01100000	R=01110100	R=00011011	R=00110000	R=00111000	R=10000101
7	G=0	G=55	G=25	G=0	G=88	G=41	G=48	G=25	G=13
	B=0	B=48	B=50	B=0	B=0	B=17	B=48	B=79	B=67

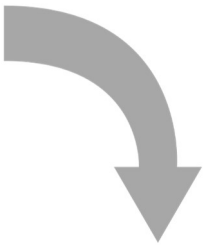
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Embedding
↓

	0	1	2	3	4	5	6	7	8
0	R=11010110 G=220 B=229	R=10111100 G=242 B=233	R=11011110 G=235 B=247	R=11111111 G=231 B=231	R=11111110 G=240 B=193	R=11100010 G=240 B=217	R=11101101 G=237 B=237	R=11101001 G=217 B=243	R=11111010 G=210 B=228
1	R=10101100 G=182 B=202	R=10000010 G=230 B=213	R=10111101 G=215 B=238	R=11111110 G=204 B=204	R=11111110 G=229 B=147	R=11000100 G=224 B=180	R=11011011 G=219 B=219	R=11011101 G=197 B=237	R=11111001 G=190 B=216
2	R=10000101 G=11 B=176	R=01001001 G=219 B=195	R=10011101 G=195 B=230	R=11111111 G=153 B=153	R=11111111 G=216 B=93	R=10101001 G=209 B=142	R=11001000 G=201 B=201	R=10111010 G=144 B=220	R=11110100 G=161 B=199
3	R=00110011 G=63 B=80	R=00100110 G=199 B=172	R=01011010 G=155 B=213	R=11111110 G=101 B=101	R=11111110 G=206 B=51	R=01110000 G=173 B=71	R=10100100 G=165 B=165	R=10010000 G=92 B=204	R=11110011 G=130 B=181
4	R=00101001 G=42 B=53	R=00100100 G=182 B=158	R=00101110 G=117 B=182	R=11111111 G=63 B=63	R=11111011 G=190 B=0	R=01010101 G=130 B=53	R=01111101 G=124 B=124	R=10000001 G=57 B=181	R=11110001 G=108 B=168
5	R=00011011 G=32 B=40	R=00011101 G=140 B=121	R=00101011 G=108 B=168	R=11111110 G=9 B=9	R=11101010 G=178 B=0	R=01001100 G=119 B=49	R=01101110 G=111 B=111	R=01101110 G=49 B=155	R=11101101 G=70 B=145
6	R=00011001 G=23 B=2	R=00010101 G=105 B=91	R=00011110 G=78 B=121	R=10011110 G=0 B=0	R=10011111 G=143 B=0	R=00111001 G=87 B=35	R=01010010 G=82 B=82	R=01010100 G=38 B=120	R=11011001 G=22 B=110
7	R=00000000 G=0 B=0	R=00001011 G=55 B=48	R=00000001 G=25 B=50	R=01100001 G=0 B=0	R=01110101 G=88 B=0	R=00011011 G=41 B=17	R=00110001 G=48 B=48	R=00111001 G=25 B=79	R=10000101 G=13 B=67

Based on the results of the previous insertion, the change in the red value was not significant so that it would not be returned by the human eye.

	0	1	2	3	4	5	6	7	8
0	R=214 G=220 B=229	R=188 G=242 B=233	R=222 G=235 B=247	R=255 G=231 B=231	R=255 G=240 B=193	R=226 G=240 B=217	R=237 G=237 B=237	R=232 G=217 B=243	R=250 G=210 B=228
1	R=173 G=182 B=202	R=130 G=230 B=213	R=189 G=215 B=238	R=255 G=204 B=204	R=255 G=229 B=147	R=197 G=224 B=180	R=219 G=219 B=219	R=220 G=197 B=237	R=248 G=190 B=216
2	R=132 G=151 B=176	R=73 G=219 B=195	R=157 G=195 B=230	R=255 G=153 B=153	R=255 G=216 B=93	R=169 G=209 B=142	R=201 G=201 B=201	R=187 G=144 B=220	R=245 G=161 B=199
3	R=51 G=63 B=80	R=39 G=199 B=172	R=91 G=155 B=213	R=255 G=101 B=101	R=255 G=206 B=51	R=112 G=173 B=71	R=165 G=165 B=165	R=156 G=92 B=204	R=242 G=130 B=181
4	R=34 G=42 B=53	R=36 G=182 B=158	R=46 G=117 B=182	R=255 G=63 B=63	R=250 G=190 B=0	R=84 G=130 B=53	R=124 G=124 B=124	R=128 G=57 B=181	R=240 G=108 B=168
5	R=26 G=32 B=40	R=28 G=140 B=121	R=42 G=108 B=168	R=255 G=9 B=9	R=234 G=178 B=0	R=77 G=119 B=49	R=111 G=111 B=111	R=110 G=49 B=155	R=236 G=70 B=145
6	R=24 G=23 B=2	R=21 G=105 B=91	R=31 G=78 B=121	R=158 G=0 B=0	R=188 G=143 B=0	R=56 G=87 B=35	R=82 G=82 B=82	R=85 G=38 B=120	R=216 G=22 B=110
7	R=0 G=0 B=0	R=11 G=55 B=48	R=0 G=25 B=50	R=96 G=0 B=0	R=116 G=88 B=0	R=27 G=41 B=17	R=48 G=48 B=48	R=56 G=25 B=79	R=133 G=13 B=67



Journal of Theoretical and Applied Information Technology
15th June 2019. Vol.97. No 11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

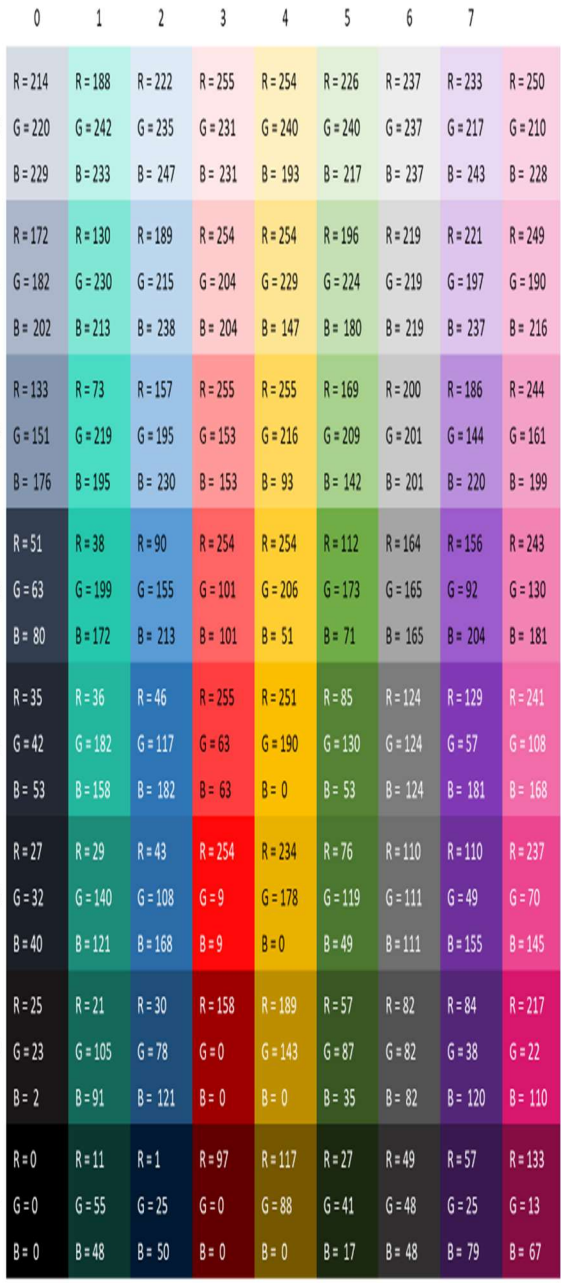


Figure 5. The Embedding Process

Extraction process:

Table 3. Extraction Process From Stego Image 9x8 Pixels

	0	1	2	3	4	5	6	7	8
0	R=11010110 G=220 B=229	R=10111100 G=242 B=233	R=11011110 G=235 B=247	R=11111111 G=231 B=231	R=11111110 G=240 B=193	R=11100010 G=240 B=217	R=11101101 G=237 B=237	R=11101001 G=217 B=243	R=11111010 G=210 B=228
1	R=10101100 G=182 B=202	R=10000010 G=230 B=213	R=10111101 G=215 B=238	R=11111110 G=204 B=204	R=11111110 G=229 B=147	R=11000100 G=224 B=180	R=11011011 G=219 B=219	R=11011101 G=197 B=237	R=11111001 G=190 B=216
2	R=10000101 G=11 B=176	R=01001001 G=219 B=195	R=10011101 G=195 B=230	R=11111111 G=153 B=153	R=11111111 G=216 B=93	R=10101001 G=209 B=142	R=11001000 G=201 B=201	R=10111010 G=144 B=220	R=11110100 G=161 B=199
3	R=00110011 G=63 B=80	R=00100110 G=199 B=172	R=01011010 G=155 B=213	R=11111110 G=101 B=101	R=11111110 G=206 B=51	R=01110000 G=173 B=71	R=10100100 G=165 B=165	R=10010000 G=92 B=204	R=11110011 G=130 B=181
4	R=00101001 G=42 B=53	R=00100100 G=182 B=158	R=00101110 G=117 B=182	R=11111111 G=63 B=63	R=11111011 G=190 B=0	R=01010101 G=130 B=53	R=01111101 G=124 B=124	R=10000001 G=57 B=181	R=11110001 G=108 B=168
5	R=00011011 G=32 B=40	R=00011101 G=140 B=121	R=00101011 G=108 B=168	R=11111110 G=9 B=9	R=11101010 G=178 B=0	R=01001100 G=119 B=49	R=01101110 G=111 B=111	R=01101110 G=49 B=155	R=11101101 G=70 B=145
6	R=00011001 G=23 B=2	R=00010101 G=105 B=91	R=00011110 G=78 B=121	R=10011110 G=0 B=0	R=10011111 G=143 B=0	R=00111001 G=87 B=35	R=01010010 G=82 B=82	R=01010100 G=38 B=120	R=11011001 G=22 B=110
7	R=00000000 G=0 B=0	R=00001011 G=55 B=48	R=00000001 G=25 B=50	R=01100001 G=0 B=0	R=01110101 G=88 B=0	R=00011011 G=41 B=17	R=00110001 G=48 B=48	R=00111001 G=25 B=79	R=10000101 G=13 B=67

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Extraction

↓

	0	1	2	3	4	5	6	7	8
0	R=11010112 G=220 B=229	R=10111102 G=242 B=233	R=11011112 G=235 B=247	R=11111112 G=231 B=231	R=11111112 G=240 B=193	R=11100012 G=240 B=217	R=11100102 G=237 B=237	R=11101002 G=217 B=243	R=11111012 G=210 B=228
1	R=10101102 G=182 B=202	R=10000012 G=230 B=213	R=10111102 G=215 B=238	R=11111112 G=204 B=204	R=11111112 G=229 B=147	R=11000102 G=224 B=180	R=11011012 G=219 B=219	R=11011102 G=197 B=237	R=11111002 G=190 B=216
2	R=10000102 G=11 B=176	R=01001002 G=219 B=195	R=10011102 G=195 B=230	R=11111112 G=153 B=153	R=11111112 G=216 B=93	R=10101002 G=209 B=142	R=11001002 G=201 B=201	R=10111012 G=144 B=220	R=11110102 G=161 B=199
3	R=00110012 G=63 B=80	R=00100112 G=199 B=172	R=01011012 G=155 B=213	R=11111112 G=101 B=101	R=11111112 G=206 B=51	R=01110002 G=173 B=71	R=10100102 G=165 B=165	R=10010002 G=92 B=204	R=11110012 G=130 B=181
4	R=00101002 G=42 B=53	R=00100102 G=182 B=158	R=00101112 G=117 B=182	R=11111112 G=63 B=63	R=11111012 G=190 B=0	R=01010102 G=130 B=53	R=01111102 G=124 B=124	R=10000002 G=57 B=181	R=11110002 G=108 B=168
5	R=00011012 G=32 B=40	R=00011102 G=140 B=121	R=00101012 G=108 B=168	R=11111112 G=9 B=9	R=11100102 G=178 B=0	R=01001102 G=119 B=49	R=01101112 G=111 B=111	R=01101112 G=49 B=155	R=11101102 G=70 B=145
6	R=00011002 G=23 B=2	R=00010102 G=105 B=91	R=00011112 G=78 B=121	R=10011112 G=0 B=0	R=10011112 G=143 B=0	R=00111002 G=87 B=35	R=01010012 G=82 B=82	R=01010102 G=38 B=120	R=11011002 G=22 B=110
7	R=00000002 G=0 B=0	R=00001012 G=55 B=48	R=00000002 G=25 B=50	R=01100002 G=0 B=0	R=01110102 G=88 B=0	R=00011012 G=41 B=17	R=00110002 G=48 B=48	R=00111002 G=25 B=79	R=10000102 G=13 B=67

Extraction process do by taking the last bits of the stego image the message is 00010011 (2) = 13 (16), 0001001 (2) = 11 (16), 11111111 (2) = FF (16), 00010000 (2) = 10 (16), 00011001 (2) = 19 (16), 11111111 (2) = FF (16), 00000111 (2) = 32 (16), 00110010 (2) = 32 (16), 11111111 (2) = FF (16) which when converted to decimal form becomes 1311 (10), 1019 (10) and 732 (10) which is the cipher file and also the remaining pixels of the first stage of the cover image.

Decrytion process:

$P_1 = 1311^{1205} \bmod 2291 = 35$

$P_2 = 1019^{1205} \bmod 2291 = 33$

$P_3 = 732^{1205} \bmod 2291 = 65$

So the plaintext returns from the audio file is P_1=35, P_2=33 dan P_3=65.

4. RESULTS AND DISCUSSIONS

The experiments were performed on Windows 8.1 Notebook with Intel Inside processor, 64-bit architecture, and 4096MB RAM. The Integrated Development Environment (IDE) used for coding is Microsoft Visual Studio 2017 and the programming language used is C#. Images are very popular target media used in the field of steganography, in this research image uses as the cover image[6]. The results of the experiments by using the application shown in figure 10, each set are presented in Tables 4, 5, 6,7, 8, 9 and 10 as follows.

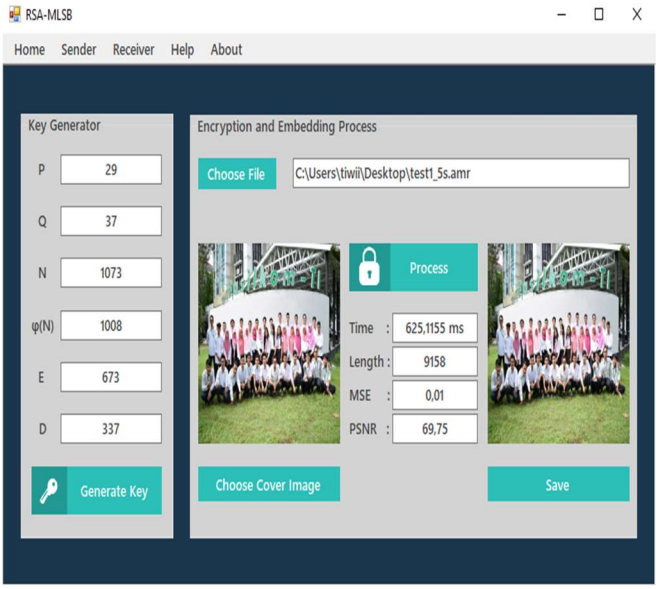


Figure 6. The Application Of Cryptostego

Journal of Theoretical and Applied Information Technology
15th June 2019. Vol.97. No 11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 4. Calculation Of Encryption Process

Index of message's length (i)	Plaintext (P) Audio	N	e	$C = P_i^e mod N$
0	35	1073	673	905
1	33	1073	673	932
2	65	1073	673	761
3	77	1073	673	744
4	82	1073	673	82
. . .	. . .	. . .	. . .	. . .
25313	58	1073	673	580
25314	96	1073	673	183
25315	3	1073	673	670
25316	64	1073	673	64
25317	80	1073	673	80

Table 5. Calculation Of Embedding Process

c	Hexadecimal	Binary	Pixel of cover image	R_{cover}	R_{stego}
$905_{(10)}$	$09_{(16)}$	00001001	(0,0), (1,0), (2,0), (3,0), (4,0), (5,0), (6,0), (7,0)	38, 36, 45, 55, 53, 57, 68, 68	38, 36, 44, 54, 53, 56, 68, 69
	$05_{(16)}$	00000101	(8,0), (9,0), (10,0), (11,0), (12,0), (13,0), (14,0), (15,0)	64, 75, 71, 67, 73, 80, 81, 65	64, 74, 70, 66, 72, 81, 80, 65
	$FF_{(16)}$	11111111	(16,0), (17,0), (18,0), (19,0), (20,0), (21,0), (22,0), (23,0)	50, 60, 75, 70, 49, 46, 59, 66	51, 61, 75, 71, 49, 47, 59, 67
. . .	. . .	. . .	. . .	. . .	. . .
$80_{(10)}$	$80_{(16)}$	10000000	* to not exceed the limit of the number of pixel covers		

Table 6. Cover image and stego image

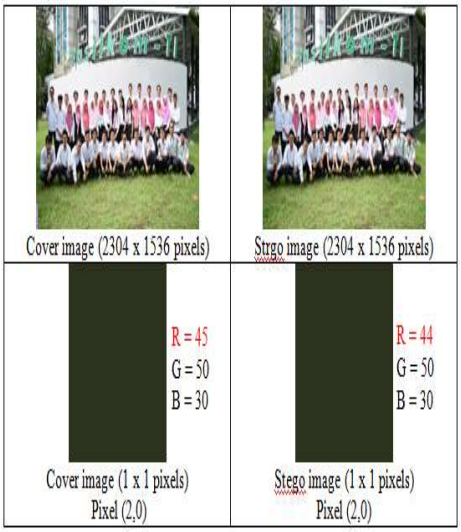


Table 7. Calculation Of Extraction Process

Pixel of stego image	R_{stego}	Bit cipher	Cipher	
(0,0)	$00111000_{(2)}$	0	$09_{(16)}$	$905_{(10)}$
(1,0)	$00110110_{(2)}$	0		
(2,0)	$01000100_{(2)}$	0		
(3,0)	$01010100_{(2)}$	0		
(4,0)	$01010011_{(2)}$	1		
(5,0)	$01010110_{(2)}$	0		
(6,0)	$01101000_{(2)}$	0		
(7,0)	$01101001_{(2)}$	1		
(8,0)	$01100100_{(2)}$	0	$05_{(16)}$	
(9,0)	$01110100_{(2)}$	0		
(10,0)	$01110000_{(2)}$	0		
(11,0)	$01100110_{(2)}$	0		
(12,0)	$01110010_{(2)}$	0		
(13,0)	$10000001_{(2)}$	1		
(14,0)	$10000000_{(2)}$	0		
(15,0)	$01100101_{(2)}$	1		
(16,0)	$01010001_{(2)}$	1	$FF_{(16)}$	
(17,0)	$01100001_{(2)}$	1		
(18,0)	$01110101_{(2)}$	1		
(19,0)	$01110001_{(2)}$	1		
(20,0)	$01001001_{(2)}$	1		
(21,0)	$01000111_{(2)}$	1		
(22,0)	$01011001_{(2)}$	1		
(23,0)	$01100111_{(2)}$	1		
. . .	. . .	. . .	. . .	. . .

* Until the number of long messages (key length)

Table 8. Calculation Of Decryption Process

Early audio duration	: 15 seconds
Initial audio size	: 24.7 KB
Image pixel	: 2304 x 1536 pixels
Cover image size	: 5.21 MB
Stego image size	: 8.34 MB
Message length	: 25318
MSE	: 0.02

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

PSNR : 65,32
Final audio duration : 15 seconds
Final audio size : 24.7 KB

Index of The Length Message(i)	Cipher (C)	N	d	$P = C_i^d \bmod N$
0	905	1073	337	35
1	932	1073	337	33
2	761	1073	337	65
3	744	1073	337	77
4	82	1073	337	82
. . .	. . .	. . .	. . .	. . .
25313	580	1073	337	58
25314	183	1073	337	96
25315	670	1073	337	3
25316	64	1073	337	64
25317	80	1073	337	80

Table 9. Running Time Of Encryption – Embedding Process

Encryption - Embedding		
Audio Duration (*sec*)	Running Time (*ms*)	Running Time' Average (*ms*)
5	703,2033	647,5014
	625,1155	
	614,1855	
10	1604,1564	1412,5413
	1421,9444	
	1211,5233`	
15	2092,7603	2040,8832
	2062,0995	
	1967,7899	

Table 10. Running Time Of Extraction – Decryption Process

Extraction - Decryption		
Audio Duration (*sec*)	Running Time (*ms*)	Running Time' Average (*ms*)
5	712,6601	671,3417
	679,2348	
	622,1302	
10	1477,0028	1316,2835
	1281,1855	
	1190,6623	
15	1878,7655	1913,3545
	1906,1564	
	1955,1416	

4. CONCLUSION

Based on table 8 the conclusion of this research, combining RSA algorithm with MLSB Red Channel method can perform the security process in the form of encryption, embedding, extraction, and decryption which shows that the audio file of the process and the original audio file is the same. This conclusion is equal with the result of the prior research by entitled Audio Steganography with Least Significant Bit (LSB) Methods for Message Encrypted with Twofish Algorithm[12]. Therefore although the prior research using the original LSB and this research using the Modified LSB, the Modified LSB can extract the original audio file.

The larger the audio size, the longer it takes for the process. Based on the results of MSE and PSNR testing, a non-significant change in the cover image with stego image shows that the use of RSA algorithm and MLSB Red Channel method is relatively safe and simple for the security of audio files.

REFERENCES

[1] Dian Rachmawati and Yeni Rosalin Munthe 2018. Phys.: Conf. Ser. 1090 012062
[2]M. Juneja and P. S. Sandhu, "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption," 2009 International Conference on Advances in Recent Technologies in Communication and Computing, Kottayam, Kerala, 2009,pp. 302-305.doi: 10.1109/ARTCom.2009.228
[3] V. Verma, Poonam and R. Chawla, "An enhanced Least Significant Bit steganography method using midpoint circle approach," 2014 International Conference on Communication and Signal Processing, Melmaruvathur, 2014, pp.105-108.doi: 10.1109/ICCSP.2014.6949808
[4] D. Rachmawati and M. A. Budiman, "New approach toward data hiding by using affine cipher and least significant bit algorithm," 2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT), KutaBali,2017,pp.1-6.doi:10.1109/CAIPT.2017.8320737
[5] Chua Teck Jian et al 2017 IOP Conf Ser.: Mater, Sci. Eng. 226012084
[6] M.D Anitha Devi and K B ShivaKumar 2017 IOP Conf. Ser.: Mater. Sci. Eng. 225 012070
[7] Kumar, A. 2013. A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique. ISSN: 2277 128X
[8] Rahmani, Vahid & Mostafa, M.P. 2017. High Hiding Capacity Steganography Method

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Based On Pixel Indicator Technique. DOI: 10.1109/CFIS.2017.8003673. ISBN: 978-1-5090-4008-7.

[9] Saurabh, J. 2012. Audio Steganography using RPrime RSA and GA Based LSB Algorithm to Enhance Security. ISSN: 2319-7064.

[10] Gutub, Adnan, et al. 2008. Pixel indicator high capacity technique for RGB image based Steganography. WoSPA 2008–5th IEEE International Workshop on Signal Processing and its Applications.

[11] J.H. Reed, Software Radio: A Modern Approach to Radio Engineering. Upper Saddle River, NJ: Pearson Education, Inc., 2002.

[12] Maryam, 2013, Audio Steganography with Least Significant Bit (LSB) Methods for Message Encrypted with Twofish Algorithm , Skripsi, Universitas Sebelas Maret