Image Steganography In Securing Sound File Using Arithmetic Coding Algorithm, Triple Data Encryption Standard (3DES) and Modified Least Significant Bit (MLSB)

A B Nasution1*, S Efendi1, and S Suwilo2
1Faculty of Computer Science and Information Technology Universitas Sumatera Utara, Medan, Indonesia
2Department of Mathematics, Universitas Sumatera Utara, Medan, Indonesia

E-mail : *buyung.cool@gmail.com

Abstract. The amount of data inserted in the form of audio samples that use 8 bits with LSB algorithm, affect the value of PSNR which resulted in changes in image quality of the insertion (fidelity). So in this research will be inserted audio samples using 5 bits with MLSB algorithm to reduce the number of data insertion where previously the audio sample will be compressed with Arithmetic Coding algorithm to reduce file size. In this research will also be encryption using Triple DES algorithm to better secure audio samples. The result of this research is the value of PSNR more than 50dB so it can be concluded that the image quality is still good because the value of PSNR has exceeded 40dB.

1. Introduction
Delivery of data or messages from one place to another is plagued with confidential issues. Many ways can be done to hide data or messages to be sent. The first by using cryptographic techniques, namely by encoding data/messages by using a particular algorithm. Another technique with steganography techniques is the art of hiding the existence of the message so as not to attract attention to secret messages, then third parties or illegal people can’t detect the message [1]. Steganography secures data with an insertion object in the form of audio, images and video and is considered to be a complement from cryptography [2]. In general, digital audio files have a size (size) larger than the text file. So to reduce its size can be done by way of compression. Audio files with WAV format have uncompressed data so that all audio samples are stored all on the hard drive (not coding). Moreover, the concealment of audio files has its own challenges because human hearing is more sensitive than vision [3].

Least Significant Bit algorithm can be used to hide data to cover like image, audio or video. However, LSB requires 8 bits of data to store 1 byte of data [4]. This method is simple method and easy to implement steganography concept [5]. The amount of data inserted in the form of audio samples that use 8 bits with LSB algorithm. The impact is a low PSNR value and resulted alteration of image quality from the insertion result. [6]. In Kauls research in 2013 has used Wavelet Transform and LSB (Least Significant Bit) methods. The results of this study indicate that the value of Peak Signal to Noise Ratio (PSNR) decreases as the number of votes increases so that there is a change in image quality of the insertion result [7]. So in this research will be inserted audio samples using 5 bits with MLSB algorithm to reduce the number of data insertion where previously the audio sample will...
be compressed with Arithmetic Coding algorithm to reduce file size. In this research will also be encryption using Triple DES algorithm to better secure audio samples.

2. Audio Files
Wav file format (Waveform audio format) is one format used to store sound in the frequency range 20 Hz to 20 kHz. File with wave format using pulse code modulation (PCM) method to store analog voice into digital data on the computer. PCM is one way of representing analog data in the digital form where the analog signal data is sampled at each interval of a certain period and then converted into a value on a digital system [8].

![Figure 1. Analog Waves Turned into Digital Waves [9].](image)

3. Arithmetic Coding Algorithm
Compression with Arithmetic Coding algorithm is by replacing one row of input symbols with a floating point number. The output of the encoding Arithmetic Coding is a number smaller than the number 1 and greater or equal to 0 [10]. To generate the output number, each symbol to be encoded is assigned a set of probability values. Once the probability of each character is known, each symbol / character will be given a certain range whose value is between 0 and 1 [11]. For example, suppose that in the audio sample "00 3e 1f 00 9a 00 1f 9a 00 3e 00 1f 00 3e 1f" will be encoded, we will get a probability table like Table 1.

| Character | Frequency | Probability  | Range        |
|-----------|-----------|--------------|--------------|
| 00        | 6         | 6/15=0.4     | 0 ≤ 00 <0.4  |
| 1f        | 4         | 4/15=0.3     | 0.4 ≤ 1f <0.7|
| 9a        | 2         | 2/15=0.1     | 0.7 ≤ 9a <0.8|
| 3e        | 3         | 3/15=0.2     | 0.8 ≤ 3e <1.0|

One thing to note from this table is that each character covers the mentioned range, except for a high number. Thus, the symbol "3e" actually has a range from 0.8 to 0.9999 ... Furthermore, to perform the encoding process, the following algorithm is used.

1. Set low = 0.0
2. Set high = 1.0
3. While do
4. Take the input symbol.
5. CR = high – low.
6. High = low + CR*high_range
7. Low = low + CR*low_range
8. End while
9. Print low
Here "low" is the output of the arithmetic coding process.

4. Triple Data Encryption Standard
Triple Data Encryption Standard (3DES) is a development algorithm of DES (Data Encryption Standard) algorithm. Basically, the algorithm used the same, only in 3DES developed by performing
encryption with DES algorithm implementation three times [12]. 3DES has three 168-bit keys (three 56-bit keys from DES). In the 3DES algorithm is divided into three stages, each stage is an implementation of the DES algorithm. The first stage, the inputted plaintext is operated with the first external key (K1) and performs the encryption process using the DES algorithm. So as to produce the first pre ciphertext. The second stage, the first pre-ciphertext generated in the first stage, is then operated with a second external key (K2) and performs the encryption or decryption process (depending on the way the encryption is used) using the DES algorithm. So as to produce a second pre ciphertext. The final stage, the second pre ciphertext generated in the second stage, is operated with the third external key (K3) and performs the encryption process using the DES algorithm, resulting in ciphertext (C).

![3DES Algorithm](image)

**Figure 2. 3DES Algorithm.**

5. Modified Least Significant Bit

Modified Least Significant Bit (MLS B) or modification of the LSB algorithm is used to encode an identity into a file. MLSB uses the manipulation of several levels of insert bits before encoding the message. Modify messages with MLSB algorithm where message bits that should have 1 character have an 8 bit ASCII code will be modified to 5 bits. Each message character will be treated with their 8-bit ASCII code, and then the code will be converted to 5-bit code using the MLSB technique. [13]

In this algorithm characters and numbers are represented in 5 bits which will then be inserted into the original file by technique LSB [14].

6. Fidelity Measurements

Measurement of steganography fidelity can be calculated by calculating the value of MSE (Mean Squared Error) and PSNR (Peak Signal to Noise Ratio). PSNR is the ratio between the maximum values of the image as measured by the magnitude of noise affecting the image. PSNR is usually measured in decibels. PSNR is used to determine the quality (validation) file processing. To determine PSNR, we must first determine the mean value of the square of the error (MSE - Mean Square Error). The smaller the MSE the better. The larger the PSNR parameter means the more similar it is to the original image. The image with the value of PSNR> 40 dB can be said to have good quality [15].

MSE and PSNR can be calculated by equations (1.1) and (1.2). In equation (2.1), I(i, j) is the image sample value at position (i, j), I' is the value of the image sample value inserted at positions (i, j). X and Y are image file sizes. In equation (2.2), m is the maximum sample value that may be possessed by audio [16].

\[
MSE = \frac{1}{XY} \sum_x \sum_y [I(x,y) - I'(x,y)]^2
\]

\[
PSNR = 10 \log \frac{m^2}{MSE}
\]
7. Proposed Method
The proposed method can be seen as in Figure 2.

![Figure 2. Proposed Method.]

In Figure 2 is a general description of the audio insertion step into the image. The first step is to do audio and image where the audio input format. Wav and image format .jpg. Then the program will read the audio and the input image to get the data. The next audio data will be compressed using Arithmetic Coding algorithm. The compressed audio is then encrypted with 3DES to obtain ciphertext. The obtained ciphertext is then inserted into the image file with the MLSB algorithm. The image that has been inserted audio then calculated the value of PSNR to obtain optimization results. Furthermore, the image that has been inserted audio and PSNR value is displayed.

8. Result and Discussion
This research has 3 performance that is performance arithmetic coding algorithm, 3DES and MLSB. The performance result of arithmetic coding algorithm can be seen in table 2.

### Table 2. Performance of Arithmetic Coding Algorithm.

| File Audio  | File Size | Size After Compress | Ratio   | Time   |
|-------------|-----------|----------------------|---------|--------|
| Flute.wav   | 48 KB     | 47 KB                | 11.09%  | 0.033 s|
| Baby.wav    | 117 KB    | 107 KB               | 8.65%   | 0.045 s|
| SMS.wav     | 246 KB    | 236 KB               | 4.41%   | 0.075 s|
| Police.wav  | 356 KB    | 341 KB               | 4.29%   | 0.097 s|
| Bird.wav    | 471 KB    | 436 KB               | 1.56%   | 0.110 s|

In table 2 shows that the highest ratio value of 11.09% with time 0.033s and the lowest ratio value of 1.56% with time of 0.110s. So it can be collected that the bigger the audio file size the smaller the ratio. However, the larger the audio file size, the greater the time it takes. The result of the compressed audio file will be the encryption and shown in table 3.

### Table 3. Performance of 3DES.

| File Audio  | File Size | Size After Encryption | Time |
|-------------|-----------|-----------------------|------|
| Kom_Flute.wav | 47 KB   | 47 KB            | 1 s  |
| Kom_Baby.wav  | 107 KB  | 107 KB           | 1 s  |
| Kom_SMS.wav   | 236 KB  | 236 KB           | 2 s  |
| Kom_Police.wav | 341 KB | 341 KB           | 2 s  |
| Kom_Birds.wav | 436 KB | 436 KB          | 2 s  |
Table 3 shows that the highest time is 2s and the lowest is 1s. In this table also shows that the file size has no effect in the encryption process. Then the encrypted file will be inserted, the insertion result is shown in table 4.

### Table 4. Performance of MLSB.

| File Audio       | File Size | File Image | File Size After Inserted | MSE  | PSNR (dB) |
|------------------|-----------|------------|--------------------------|------|-----------|
| Kom_Flute.wav.3des | 47 KB     | Beach.jpg  | 49 KB                    | 92 KB| 4.480     | 58.382   |
| Kom_Baby.wav.3des | 107 KB    | Palm.jpg   | 127 KB                   | 223 KB| 1.159     | 52.475   |
| Kom_SMS.wav.3des  | 236 KB    | Tree.jpg   | 179 KB                   | 396 KB| 6.749     | 60.162   |
| Kom_Police.wav.3des | 341 KB  | Pond.jpg   | 504 KB                   | 845 KB| 1.159     | 52.475   |
| Kom_Birds.wav.3des | 436 KB    | Mountain.jpg | 530 KB               | 992 KB| 3.411     | 57.198   |

In Table 4 it shows that the size of the inserted image file rises close to the number of audio file sizes plus the image file size, it indicates that the audio is inserted into the image file. In the table also shows that the PSNR value is more than 50dB with the lowest PSNR value of 52.475 and the highest PSNR value is 60.162 so it can be concluded that the picture quality is very good because the PSNR value is greater than 35dB.

### 9. Conclusion

The conclusion in this research are as follows.

1. In the process of arithmetic coding algorithm, the larger the audio file size the higher the time. However, inversely proportional to the ratio, the larger the audio file size the lower the ration value. This can be seen in Table 2 where the smallest audio file size has a high ratio of 11.09% with the lowest time of 0.033s. While the largest audio file size has the lowest ratio of 1.56% with the highest time of 0.110s.
2. In the 3DES process, the time required for encryption is 1s to 2s and in this process the size of the audio file does not change in size.
3. In the MLSB process, the PSNR value is more than 50dB with the lowest PSNR value of 52.475 and the highest PSNR value is 60.162 so it can be concluded that the picture quality is very good because the PSNR value is greater than 40dB.

Future work, the expected testing process can be done by testing the reliability of the insertion algorithm (robustness) with the addition of noise into the image steganography and extraction of audio data again.

### References

[1] Dilawar, A. 2014. Image Steganography: For Hiding Audio Messages Within Grayscale Images Using LSB, DCT And AES Algorithm. Thesis. International Islamic University, Sector H-10: Islamabad

[2] Kumar A. & Pooja, K. 2010. Steganography- A Data Hiding Technique. International Research of Computer Aplication. pp. 19.23

[3] Cvejic. N. 2004. Algorithms for Audio Watermarking and Steganography. Linier Networks and Systems (Book Style). pp. 123-135

[4] Rachmawati, D., Amalia, A. and Surya, J. 2016. Combination of Huffman Coding Compression Algorithm and Least Significant Bit for Image Hiding. International Conference on Computing and Applied Informatics. pp. 1-4

[5] Kekre, H.B., Athawale, A. & Halarnkar, P.N. 2008. Increased Capacity of Information Hiding in LSB’S Method for Text and Image. International Journal of Computer, Electrical, Automation, Control and Information Engineering. pp. 1497-1500
[6] Por, L.Y., Beh, D., Ang, T.F. & Ong, S.Y. 2013. An Enhanced Mechanism for Image Steganography Using Sequential Colour Cycle Algorithm. *The International Arab Journal of Information Technology*. pp. 51-60

[7] Kaul, N. and Bajaj, N. 2013. Audio in Image Steganography based on Wavelet Transform. *International Journal of Computer Application*. pp. 7-10

[8] Husain, M.P. & Rafat, K.F. 2016. Enhanced Audio LSB Steganography for Secure Communication. *International Journal of Advanced Computer Science and Applications*. pp. 340-347

[9] Kumar, S., Barnali, B. & Banik, G. 2012. LSB Modification and Phase Encoding Technique of Audio Steganography Revisited. *International Journal of Advanced Research in Computer and Communication Engineering*. pp. 1-4

[10] Habib, A. & Chowdhury, D. 2015. An Efficient Compression Technique Using Arithmetic Coding. *Journal of Scientific Research & Reports 4 (1)*, pp. 60-67

[11] Sentilkumar, M. & Mathivanan, V. 2016. Analysis of Data Compression Techniques using Huffman Coding and Arithmetic Coding. *International Journal of Advanced Research in Computer Science and Software Engineering*. pp. 930-936

[12] Kumar, P. & Rajaanadan, N.S. 2016. Data Encryption and Decryption Using By Triple DES Performance Efficiency Analysis of Crypto System. *International Journal of Innovative Research in Computer and Communication Engineering*. pp. 4030-4040

[13] Shreya, M.S. & Khumar, S. 2013. Separable Reversible Data Hiding In Encrypted Image Using Modified Least Significant Bit and Virtual Embedding. *International Journal of Science and Research*. pp. 3099-3106

[14] Zaher, M.A. 2011. Modified Least Significant Bit (MLSB). *Computer and Information Science*. pp. 60-67

[15] Laskar, S.A. & Hamachandran, K. 2012. High Capacity Data Hiding Using LSB Steganography and Encryption. *International Journal of Database Management System*. pp. 57-68

[16] Prasetyo, B. 2013. Kombinasi Steganografi Bit Matching dan Kriptografi DES untuk Pengamanan Data. *Thesis*. Universitas Diponegoro : Semarang