Echo hiding method for video file message security

C Rahmad¹*, I Muhiqqin², T S Patma², R Ariyanto¹ and N Muna²

¹ Department of Information Technology, State Polytechnic of Malang, Malang, Indonesia
² Department of Electrical Engineering, State Polytechnic of Malang, Malang, Indonesia

*cahya.rahmad@polinema.ac.id

Abstract. Sending secret message need an algorithm that can protect message to receiver without knowing by other and keep the originality of message. Previous research, encoding secret message in video inserted in frame while audio secret message inserted in bit audio. it makes it easier for someone to detect the presence of a message. In this paper, try to encode the secret message at video file to encode in audio. Audio separated from video in order to encode secret message in audio. Echo Hiding method used in encode secret message to audio process. Testing use Bit Error Rate (BER) method to analysis modification in audio and Normalized Correlation (NC) analysis authentic the secret message. Based on the experiment, the results obtained were NC values (0.98-1) and BER values (0-3.12). based on the results obtained by the method we can insert messages better than the previous method with the addition of noise elimination in audio.

1. Introduction
The internet makes it easy for someone to send messages and disseminate digital products in the form of text files, image files, audio files, and videos. Each file is confidential and public. For public files there is no concern because everyone can access it, but it is different from confidential files not everyone can access it. But there are parties who have no interest in trying to access and abuse. Therefore, a technique is needed to overcome this problem. Steganography is an art or science that is used to hide secret messages into a media so that the existence of a secret message is not known other than the intended person, so that other people will not be aware of the existence of the secret message [1]. Media to hide various messages, in previous research the hiding of messages in video media was included in each video frame, in the image media inserted in the bits of each pixel, and on the audio media included in each audio bit [2]. This habit makes it easier for someone to detect the presence of messages in each media. This research tries to hide messages in video media included in every audio bit rather than in the video frame [3]. There are three methods of insertion in audio media, namely low bit encoding, spread spectrum, and echo data hiding [4]. Of the three methods in message insertion on audio media, echo hiding techniques have the advantage that the file generated from the insertion process has a size that is not too different from the size of the original audio file, and is more robust in inserting messages in audio [5]. But has disadvantages, with changes in the contents of the audio file creating noise in the audio file. To reduce the noise, e tried to remove noise before the data encoding process.
2. Proposed method
The main purpose of steganography is to communicate safely in a fully undetectable way [6]. In steganography itself there are two main parts that are most important, namely the encoding and decoding process, in this paper the encoding and decoding process is explained as follows.

2.1. Encoding

![Figure 1. Stage encoding.](image)

The stages of the encoding process are shown in figure 1. The first stage of file separation, obtains audio files, images from video files and echo audio signals, the process steps are as follow.

- Insert media files into video forms, then separate images and audio
- The audio file that is produced has the extension wav. Because the wav file is not compressed, so there is no sampling of the lost audio signal [7].
- Remove audio noise by separating noise and signals with a band pass filter. With a maximum frequency divided by 2 or called the nyquist frequency of a frequency of 48000 Hz, which means that the maximum frequency is 24000 Hz and centered to 0 Hz, with the left range 0 to -24000hz and the right range 0 to 24000 Hz, band pass filters are placed between 700 to 12000Hz, with \( n = 7 \) to start. And normalize the nyquist frequency to 1, while the others are between 0 and 1.
- Making echo audio because echo data hiding performs k message insertion in digital sound by adding echo to the signal [8]. Echo is formed by summing the incoming signal with a delayed signal that has been attenuated by equation (1) where the delta value is given by equation (2). Echo is made in different parameters, namely amplitude, delay rate, and offset. The offset parameter is varied to represent binary messages that are hidden. The first offset value represents binary 1 with delay \( \delta_1 \) seconds and the second offset value represents binary 0 with delay \( \delta_0 \) seconds [9].

\[
h_0[n] = \delta[n] + \frac{a}{2} \delta[n - d_0] + \frac{\alpha}{2} \delta[n + d_0]. \tag{1}
\]

\[
\delta[n] = \begin{cases} 
1, & \text{if } n = 0 \\
0, & \text{if } n \neq 0
\end{cases} \tag{2}
\]

\( n \) is an inserted audio signal, \( \delta[n] \) is a valuable signal 1 when \( n = 0 \) and valuable 0 when \( n \neq 0 \), \( d_0 \) to delay creating bits 0, \( d_1 \) and \( \alpha \) to delay creating bits 1.
The audio signal is then normalized by changing the audio file sampling value according to the characteristics of the 16-bit audio, because the message insertion in 16-bit audio is better than 8 bits [10], so that the sampling value is processed from the range -1 input value and 1 double data type to unit 16 which has a range of 0 to 65,535.

The second stage of the secret message is used. Messages in the form of text characters are stored in the .txt format, before the change process, the number of characters in the message is calculated first, the character used is 1 character, namely the letter ‘i’, then changes the character in binary ASCII, with binary values 01101001. The binary word is then formed into 2 signals with binary value 1 and signal with binary value 0 as shown in figure 2.

![Figure 2. Mixer signal.](image)

The third stage is the process of inserting confidential data. At each binary offset value 1 or 0 and binary signals 1 and 0 are inserted with the equation (3).

\[
C_w(t) = Co(t) + \alpha_k \cdot Co(t - \Delta t_k), k = 0,1.
\]  

(3)

\(Co\) is an original sound signal, \(\alpha_k\) is a multiplier / amplifier each bit, \(t\) is a message signal, \(\Delta t_k\) is the delay of each bit. Then combine the modified parts of the sound signal to get the full signal sound. The signal is then combined with the image.

2.2. Decoding

![Figure 3. Stage decoding.](image)

The decoding process are illustrated in Fig 3. The first step is to separate the stegano audio from the video image in the wav format. File reading continued with data normalization. The normalization process is the same as the normalization process in encoding. divide the length of the audio signal into \(n\) equal lengths where \(n\) is the number of steganography bits.

The second stage transforms the audio signal into the frequency domain by performing FFT (Fast Fourier Transform) with equation (4) in each section. And amplifies the frequency signal by squaring the audio signal in the frequency domain.

\[
X(k) = \sum_{n=0}^{N-1} x(n) \sin \left(\frac{2\pi kn}{N}\right) - j \sum_{n=0}^{N-1} x(n) \cos \left(\frac{2\pi kn}{N}\right)
\]  

(4)
The third step looks for the logarithmic value of each audio signal in the frequency domain and returns the sound signal into the time domain with IFFT (Inverse Fast Fourier Transform) with equation (5).

\[
X(n) = \sum_{n=0}^{N-1} x(k) \sin\left(\frac{2\pi kn}{N}\right) - j\sum_{n=0}^{N-1} x(k) \cos\left(\frac{2\pi kn}{N}\right)
\] (5)

Compare the bit time interval 0 \(\Delta t_0\) with the time range used for bit insertion 1 \(\Delta t_1\). If value \(\Delta t_0\) greater than \(\Delta t_1\) then the bit inserted in that section is 0 bits, and vice versa if \(\Delta t_1\) greater than \(\Delta t_0\) then the inserted bit is 1.

The fourth stage is merging. Combine the bits obtained to produce a complete message.

3. Results and discussion
The following discussion tries to hide the message on the audio by increasing the noise removal process before the echo creation process besides placing the hiding differently, with the following test

3.1. Dataset
To evaluate the performance of the proposed algorithm. Tests were carried out on 14 video files with mp4 data rate format of 122kbps to 681kbps with frame rate of 14.30 frames/second to 30.00 frames/second. with audio characters as shown in table 1.

| File | Bitrate | Channels | Sample Rate | length |
|------|---------|----------|-------------|--------|
| Video 1 | 70kbps | 1(mono) | 44.100kHz | 0:00:29 |
| Video 2 | 96kbps | 2(stereo) | 44.100kHz | 0:00:58 |
| Video 3 | 98kbps | 1(mono) | 44.100kHz | 0:00:34 |
| Video 4 | 98kbps | 1(mono) | 44.100kHz | 0:00:30 |
| Video 5 | 110kbps | 1(mono) | 44.100kHz | 0:00:26 |
| Video 6 | 104kbps | 1(mono) | 44.100 kHz | 0:00:40 |
| Video 7 | 101kbps | 1(mono) | 44.100kHz | 0:00:30 |
| Video 8 | 100kbps | 1(mono) | 44.100kHz | 0:00:29 |
| Video 9 | 102 kbps | 1(mono) | 44.100kHz | 0:00:31 |
| Video 10 | 98kbps | 1(mono) | 44.100 kHz | 0:00:29 |
| Video 11 | 114kbps | 1(mono) | 44.100 kHz | 0:00:31 |
| Video 12 | 100kbps | 1(mono) | 44.100kHz | 0:00:30 |
| Video 13 | 96kbps | 2(stereo) | 44.100kHz | 0:00:28 |
| Video 14 | 96kbps | 2(stereo) | 44.100kHz | 0:00:30 |

The secret message used is the .txt file that reads "pesan rahasia" test by calculating the BER (Bit error rate) with the equation (6) and NC (Normalized Correlation) with equation (7).

\[
BER(w, w') = \frac{100}{N} \cdot \sum_{n=1}^{N} XOR(w(n), w(n))
\] (6)

\[
NC = \frac{\sum_{n=1}^{N} w(n)w'(n)}{\sqrt{\sum_{n=1}^{N}(w(n))^2} \cdot \sum_{n=1}^{N}(w'(n))^2}
\] (7)

\(w\) is the desired bit, \(w'\) is the bit taken, with amplitude echo 0.002

3.2. Trial results of message insertion
From table 2, compared to the previous method [2], with the proposed method. The results obtained from 14 trials, the proposed method can be able to insert and re-extract the secret message and cause a slight change in the audio better than the previous method by removing audio noise before the encoding process results in a better 0.08 result from the previous method.
Table 2. Test results.

| File   | The previous application | Proposed Algorithm |
|--------|--------------------------|---------------------|
|        | BER | NC | BER | NC |
| Video 1| 0   | 1  | 0   | 1  |
| Video 2| 0   | 1  | 0   | 1  |
| Video 3| 0   | 1  | 0   | 1  |
| Video 4| 3.12| 0.96| 2.08| 0.97|
| Video 5| 0   | 1  | 0   | 1  |
| Video 6| 0   | 1  | 0   | 1  |
| Video 7| 3.12| 0.96| 3.12| 0.96|
| Video 8| 1.04| 0.98| 0   | 1  |
| Video 9| 0   | 1  | 0   | 1  |
| Video 10| 0  | 1  | 0   | 1  |
| Video 11| 0 | 1  | 0   | 1  |
| Video 12| 0  | 1  | 0   | 1  |
| Video 13| 3.12| 0.9 | 3.12| 0.96|
| Video 14| 2.08| 0.97| 1.04| 0.98|

4. Conclusion

In this paper, we present a message insertion algorithm with audio steganography algorithm. By adding noise deletion and inserting messages on media with different locations to avoid suspicion of the inserted message, the results of being stripped from the test using the BER method, method are better 0.222 but in the NC-007 method.

Acknowledgment

The authors would like to thank State Polytechnic of Malang for supporting this research.

References

[1] Syawal M F, Fikriansyah D C and Luhur N A U B 2016 Implementasi Teknik Steganografi Menggunakan Algoritma Vigenere Cipher Dan Metode LSB Jurnal TICom 4(3)
[2] Tekeli K and Asliyan R 2017 A Comparison Of Echo Hiding Methods ISRES 1 397
[3] Ria G 2010 Studi Perbandingan Steganografi pada Audio, Video dan Gambar (Bandung: Institut Teknologi Bandung)
[4] Prima P 2011 Studi dan Analisis Teknik-Teknik Steganografi Dalam Media Audio (Bandung: Institut Teknologi Bandung)
[5] Xie C, Cheng Y and Wu F 2010 A New Detection Scheme for Echo Hiding (China: University of Science & Technology of China Hefei)
[6] Jayaram P, Ranganatha H R and Anupama H S 2011 Information Hiding Using Audio Steganography-A Survey IJMA 3
[7] Fiqar T P and Ahmad T 2017 Peningkatan Kapasitas Penyisipan Audio Data Hiding Berbasiskan Modifikasi Metode Least Significant Digit JNTETI 6 2301–4156
[8] Primbadi T, Shiddiqi A M and Pratomo B A 2012 Aplikasi Chat dengan Steganografi pada Audio Menggunakan Metode Echo Data Hiding Jurnal Teknik Pomits 1 1–6
[9] Kim H J and Choi Y H 2003 A Novel Echo-Hiding Scheme With Backward and Forward Kernels IEEE Trans. On Circuits and Systems for Video 13 1051–8215
[10] Rana M and Tanwar R 2014 Genetic Algorithm in Audio Steganography IJETT 13 2231–5381