Analisis Kualitas Suara Stego Audio Penyisipan Informasi Tersembunyi dengan Metode *Least Significant Bit*

Agitiya Dwi Hendrata[1], Agus Prihanto[2]

[1,2]Jurusan Teknik Informatika/Teknik Informatika, Universitas Negeri Surabaya
[1]agitiyahendrata16051204029@mhs.unesa.ac.id
[2]agusprihanto@unesa.ac.id

***Abstrak*—Keamanan data telah menjadi kebutuhan dalam komunikasi pada era yang sudah serba digital. Teknik mengamankan data dapat dilakukan pada lintasan komunikasi data maupun dari data yang dikirimkan. Saat ini telah banyak berkembang teknik yang dapat digunakan untuk mengamankan data yang dikirimkan, salah satunya adalah teknik steganografi. Steganografi merupakan teknik mengamankan data dengan cara menyisipkan pesan utama kedalam sebuah media. Sehingga, pengirim dan penerima akan tampak seperti berkirim file biasa. Kelebihan teknik steganografi dibandingkan dengan teknik mengamankan data lainnya, seperti enkripsi dan *watermarking* adalah, pihak selain pengirim dan penerima kemungkinan besar tidak menyadari bahwa terdapat pesan rahasia di dalam suatu file yang dikirimkan. Teknik steganografi dapat dilakukan pada semua jenis media pembawa (*audio, video,* dan *audio video*) dengan berbagai jenis pesan rahasia (*text, audio, video,* dan *audio video*). Teknik steganografi yang diterapkan pada media pembawa berupa audio dinilai lebih sulit karena *Human Auditory System* dianggap sebagai indera yang paling peka pada manusia. Sehingga pada penerapannya, dibutuhkan algoritma yang dapat menghasilkan perbedaan paling kecil pada file hasil steganografi. Algoritma *Least Significant Bit* (LSB) dianggap sebagai algoritma yang paling sederhana dan mudah dalam penerapannya. Steganografi dengan LSB ini dilakukan dengan mengganti bit paling kanan (2^0) dari media pembawa dengan bit pesan rahasia. Perubahan pada bit yang dinilai kurang signifikan akan membuat hasil steganografi tidak jauh berbeda dengan file asli. Pada penelitian ini, dibangun sebuah sistem yang menerapkan algoritma LSB untuk menyisipkan pesan rahasia bertipe *txt* kedalam file audio WAV. Melalui pengamatan nilai PSNR dan MSE setelah menyisipkan pesan berukuran 50% dari kapasitas maksimal menghasilkan audio dengan rata-rata nilai PSNR sebesar 56.3571 dB dan rata-rata nilai MSE sebesar 0.15044, sedangkan rata-rata nilai PSNR setelah penyisipan pesan dengan ukuran maksimal adalah 53.2277 dB dan rata-rata nilai MSE sebesar 0.3092. Penyisipan pesan kedalam audio tidak banyak mempengaruhi kualitas signal audio, dibuktikan dengan perbandingan grafik signal audio asli dengan grafik signal audio hasil stego-audio yang hamir serupa.**

***Kata Kunci* — Steganografi, Audio, WAV, LSB, PSNR, MSE**

I. PENDAHULUAN

Di era yang sudah serba digital ini, teknologi telah masuk hampir ke seluruh bidang kehidupan manusia. Peran teknologi yang membantu dan mempermudah pekerjaan manusia membuatnya menjadi hal yang paling diandalkan. Agar suatu teknologi tetap digunakan di zaman yang serba berkemajuan ini, dibutuhkan kepercayaan pengguna. Selain dari sisi fitur, hal lain yang menjadi pertimbangan pengguna dalam memilih teknologi adalah sisi keamanan data.

Dalam sistem komunikasi modern, menyembunyikan data merupakan salah satu teknik penyelesaian untuk masalah keamanan data [1]. Teknik mengamankan data di internet menjadi disiplin ilmu yang digemari para peneliti karena keamanan data harus dapat diterapkan untuk semua jenis file baik audio, visual, maupun audio visual. Pada [2], menyembunyikan informasi pada media gambar berwarna 24-bit. Dengan model warna RGB menggunakan masing-masing 8 bit untuk merah, hijau dan biru untuk merepresentasikan sebuah piksel. Dengan memodifikasi Algoritma LSB, penelitian ini berhasil menggunakan posisi acak dari biner RGB yang merepresentasikan warna citra untuk menyembunyikan pesan ke dalam citra. Hasilnya, melalui uji PSNR dan MSE teknik yang diusulkan memiliki kinerja yang lebih baik dari sisi *invisibility* dan *robustness* dibandingkan dengan LSB biasa. Pada penelitian lain [3], mengenalkan metode yang disebut "*StegIbiza*" untuk menyembunyikan pesan rahasia pada layanan *streaming* musik mengunakan tempo sebagai media untuk menutupi. Teknik pada penelitian ini adalah dengan memanipulasi *Beats per Minute* (BPM) pada file musik. Metode ini menggunakan kode morse pada proses *pre-encode* pesan rahasia. Hasilnya, penerima yang dituju dapat menyadari perubahan halus pada BPM kemudian merekonstruksi pesan dalam kode morse menjadi karakter ASCII dengan menganalisis tempo yang sama.

Teknik pengamanan data bertujuan untuk melindungi data yang dikirimkan dari akses pengguna yang tidak sah, seperti menyalin, menyebar luaskan dan bahkan mengubah data yang asli. Data-data yang dikirimkan melalui internet diamankan dengan berbagai teknik, seperti kriptografi, steganografi dan *watermarking* [4]. Kriptografi digunakan untuk mengenkripsi atau melindungi pesan rahasia. Pesan rahasia ini diacak sehingga tidak berarti apa-apa bagi orang lain. Meskipun demikian, teknik kriptografi memungkinkan pihak ketiga mengetahui terdapat pesan rahasia meskipun tidak dapat membaca pesan tersebut. Teknik pengamanan data lainnya adalah *watermarking,* teknik ini umumnya digunakan untuk melindungi hak cipta dan otentikasi file digital [5]. Pada [6] menggunakan teknik *watermarking* yang di kombinasikan dengan *Convolutional Neural Network* (CNN) dan *Discrete Wavelett Transform* (DWT). DWT digunakan untuk menguraikan citra menjadi beberapa *sub-band* yang berbeda. Kemudian dipilih piksel pada frekuensi tinggi dan rendah pada sub-band untuk digunakan sebagai masukan dan keluaran yang diinginkan, untuk melatih CNN. Peletakkan watermark dan proses ekstrai dilakukan sepenuhnya oleh CNN. Melalui uji PSNR, NC, dan SSIM, metode yang diujikan ini memiliki

keunggulan dari sisi *invisibility* dan *robustness* dibandingkan dengan metode lain.

Enkripsi pada kriptografi dan *watermarking* memungkinkan pihak lain mengetahui keberadaan pesan rahasia sehingga menarik penyadap dengan mudah. Untuk mengatasi permasalahan ini, teknik steganografi digunakan untuk menyembunyikan pesan rahasia kedalam media video, audio maupun gambar, sehingga tidak ada yang menyadari keberadaan pesan rahasia ini selain pengirim dan penerima [4].

Saat ini, steganografi digunakan untuk menyembunyikan pesan rahasia melalui media digital. Steganografi dapat digunakan untuk menyembunyikan berbagai jenis tipe pesan (text, gambar, audio, dan video) [7] pesan digital (text file) lebih banyak digunakan secara luas di internet [8]. Pada [9] memodifikasi algoritma LSB untuk menyembunyikan pesan *text* kedalam *file audio* sehingga lebih aman dari *steganalysis*. Algoritma yang diusulkan menggunakan *Simulated annealing* sebagai teknik optimasi. Penelitian ini berhasil menyembunyikan bit pesan kedalam bit yang lebih tinggi dari media pembawa dan mengubah bit lain untuk meminimalkan kesalahan. Dari uji objektif, algoritma ini berhasil meningkatkan kapasitas pesan rahasia namun tidak terlalu mempengaruhi SNR dibandingkan dengan algortima LSB biasa. Hasil stego audio yang terbentuk melalui algoritma optimasi ini tidak dapat dibedakan dari *file audio* yang asli. Dari sisi penerima, data telemetri dapat diekstrak dari pesan stego dengan baik.

Teknik steganografi dapat diterapkan pada beberapa tipe media yang berbeda seperti *text, audio,* dan *video*. *file audio* dan *video* dianggap sebagai media yang baik pada teknik steganografi karena banyaknya redundansi. Penerapan steganografi pada *file audio* dianggap lebih rumit dibandingkan pada file video. Hal ini dikarenakan kemampuan pendengaran manusia (*Human Auditory System)* lebih peka daripada kemampuan pengelihatan manusia (*Human Visual System)* [8]. Telinga manusia sangatlah peka dan dan sering kali dapat merasakan *noise* dalam *file audio* [10].

Konsep *stego audio* yang baik harus memenuhi tiga kriteria berikut: 1. *Inaudibility of distortion* (Perceptual Transparency): *file audio* yang telah disisipi pesan tidak dapat diketahui perbedaannya dibandingkan dengan *file audio* asli. Informasi yang disisipkan harus disamarkan tanpa mempengaruhi *intuitive nature* dari suara asli. 2. *Robustness*: diukur melalui kapasitas dari pesan yang dimasukkan kedalam *file audio* apakah tahan terhadap serangan yang disengaja maupun tidak disengaja. Serangan yang tidak disengaja seperti *re-inspecting, re-quantization,* dll. Sedangkan serangan yang disengaja lebih mengarah ke *re-sizing, re-scaling*, dll. 3. *Data Rate (Capacity)*: besarnya pesan yang dapat disembunyikan tanpa memperlihatkan perubahan berarti pada file asli [10]. Penelitian terkait penerapan steganografi pada *file audio* telah dilakukan pada [5]. Penelitian ini menggabungkan teknik LSB dengan *modified phase coding*. Kelemahan utama dari teknik LSB diatasi menggunakan *modified phase coding* untuk meningkatkan ketahanan dari LSB. Penelitian ini menggunakan Matlab 2013a dan memanfaatkan beberapa *file audio* untuk menyembunyikan berbagai pesan rahasia. Pesan rahasia yang digunakan pada penelitian ini berupa *file text, audio* atau gambar hitam putih. Melalui uji SNR dan PSNR, teknik yang diusulkan berhasil menyembunyikan pesan rahasia kedalam *file audio* lebih baik daripada penggunaan teknik LSB dengan *phase coding* secara terpisah.

Least significant bit (LSB) dianggap sebagai teknik paling sederhana dan cepat untuk memasukkan pesan kedalam file audio dan menyediakan kapasistas pesan rahasia yang lebih tinggi [7] [10]. Dalam pendekatan LSB, tiap bit yang mempunyai nilai paling kecil pada deret *file audio* diganti dengan deret biner pesan rahasia. Dalam kode LSB, rata-rata transmisi data yang paling baik adalah 1 kbps pada 1 kHz. Pada beberapa penerapan LSB, dua digit biner yang nilanya paling kecil diganti dengan dua bit data lain. Hal ini dapat menambah informasi yang dapat disembunyikan namun juga meningkatkan *noise* pada *file audio* tersebut [10]. Penelitian [11] berhasil merancang perangkat lunak stego audio mp3 menggunakan *Visual Basic* 6.0. Perangkat lunak yang dirancang mengizinkan pengguna untuk memilih sendiri file audio yang digunakan untuk menyembunyikan pesan dan juga pesan yang ingin disampaikan secara rahasia. Metode LSB yang digunakan berhasil menyisipkan pesan bertipe *text* kedalam file *mp3* tanpa menunjukkan perubahan yang besar pada ukuran file hasil stego audio. Pada penelitian lain [1], menggunakan metode LSB untuk menyembunyikan pesan pada file audio bertipe *WAV*. Proses stego audio yang diterapkan menggunakan Matlab 7.10 diukur kinerjanya menggunakan pendekatan *Mean Opinion Score* (MOS) pendekatan ini dilakukan dengan meminta 20 orang untuk membedakan file WAV yang telah disisipi pesan dan file WAV asli. File audio dikelompokkan berdasarkan jumlah bit per sample dan jumlah channel. Melalui pendekatan MOS ini, didapatkan nilai untuk Stego-8k-s1(menggunakan media lagu,sampled at fs=8khz) mendapatkan nilai 4.6. Stego-16k-m1 (menggunakan media suara pria, sampled at fs=16khz) nilai 4.8. Stego-44.1k-s1 (menggunakan media lagu, sampled at fs=44.1khz) nilai 4.8. Stego-48k-f1 (menggunakan suara wanita, sampled at fs=48khz) mendapatkan nilai 5.

Penelitian ini fokus pada penerapan metode LSB untuk melakukan stego audio pada file WAV. Pesan *text* akan disisipkan pada file audio dengan berbagai ukuran. Kualitas audio hasil stego audio akan diukur menggunakan perhitungan PSNR dan pengamatan signal audio hasil stego-audio.

II. METODOLOGI PENELITIAN

Pada penelitian ini, sistem dirancang menggunakan Bahasa Matlab. *Dataset* suara yang digunakan sebagai media penyisipan pesan didapatkan dari *https://www2.cs.uic.edu/~i101/SoundFiles/*. Perangkat lunak yang dirancang dapat menyembunyikan file *text* kedalam *audio* bertipe *WAV* dan dapat mengekstrak pesan rahasia yang telah disisipkan tanpa menghilangkan informasi yang disisipkan.

1. Least Significant Bit

Metode LSB digunakan untuk menanamkan bit dari pesan rahasia pada bit yang kurang signifikan dari file audio [5]. Keuntungan dari penerapan teknik LSB adalah kompleksitas

komputasi dari algoritma ini lebih rendah dibandingkan dengan teknik lain dan juga *noise* yang dihasilkan dari teknik ini relatif rendah bahkan tidak terdeteksi oleh indera. Namun, pada penerapannya, metode ini memiliki kelemahan pada sisi ketahanan terhadap serangan dan kemudahan dalam mengekstrak dan menghancurkan pesan yang telah disisipkan pada *file*.

Langkah utama pada stego-audio menggunakan teknik LSB ini dilakukan dengan mengganti bit paling kanan (2^0) dari *file original audio* dengan pesan rahasia yang sebelumnya telah di konversi menjadi deret biner berukuran sama dengan audio sample. Proses ini dilakukan berulang-ulang hingga semua karakter pada pesan rahasia telah disisipkan kedalam *file audio*.

Pseudo code untuk proses *embedding* pesan rahasia kedalam media penyisipan dapat dilihat pada Gambar 1

```
    embedding text file to audio file process

1   f_oriaudio ← media penyisipan
2   f_oriaudio_bin ← binary string(f_oriaudio)
3   textmssg ← pesan rahasia
4   textmssg_bin ← binary string (textmssg)
5   mssg_length ← length(textmssg_bin)
6   for (i=1 to mssg_length)
7   {
8         text_str(i) ← f_oriaudio_bin(i)
9   }
10  f_stegoaudio ← bin2dec(f_oriaudio_bin)
11  f_stegoaudio.wav ← f_stegoaudio
```

Gambar 1 *Pseudo code embedding process*

Hasil stego audio menggunakan metode LSB diukur berdasarkan nilai *Peak Signal to Ratio (PSNR).* PSNR sering digunakan untuk mengukur kualitas stego-audio dengan membandingkan perubahan bit antar kedua audio [12].

PSNR dapat dihitung dengan menemukan *nilai Mean Square Error* (MSE) terlebih dahulu. MSE dapat dihitung menggunakan persamaan (1) [13]:

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(x_i - y_i)^2 \quad (1)$$

MSE mewakilkan perbedaan antara audio asli dengan audio hasil stego-audio. Semakin mirip kedua audio, maka semakin kecil pula nilai MSE [14]. Setelah nilai MSE didapatkan, PSNR dapat dihitung dengan persamaan (2):

$$PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right) \quad (2)$$

Dimana:
x = original audio signal
y = stego audio signal
N = jumlah signal sample
R = nilai puncak signal

Nilai puncak signal merupakan nilai maksimal yang memungkinkan dari signal audio, ketika file audio direpresentasikan kedalam persamaan linear B bit per sample, maka nilai puncaknya adalah 2^B-1. PSNR adalah perbandingan dari nilai puncak signal audio dengan nilai MSE. Ketika kedua file yang sama dibandingkan, akan menghasilkan nilai MSE=0, sehingga nilai PSNR menunjukkan nilai tak hingga. Untuk itu, semakin kecil nilai MSE semakin tinggi PSNR dari audio tersebut. Semakin tinggi nilai PSNR, semakin kecil *noise* dari audio tersebut, sehingga kualitas audio semakin baik [15].

2. Encoding

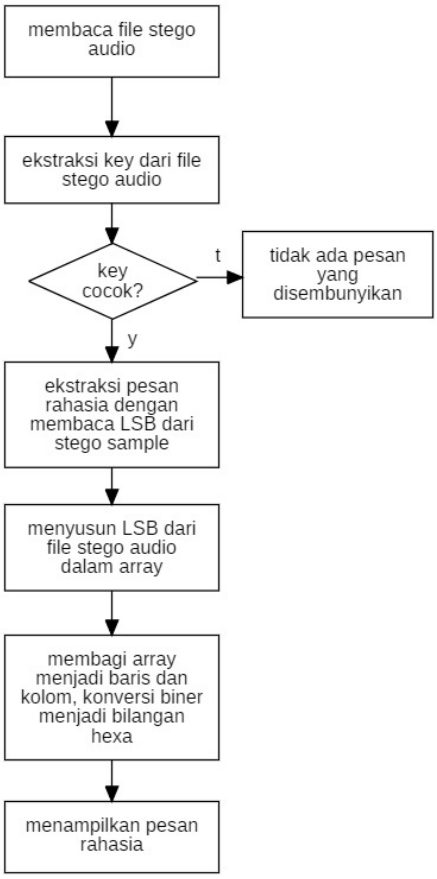
Encoding adalah proses menempatkan urutan karakter tertentu (huruf, angka, tanda baca, dan simbol tertentu) ke dalam format khusus untuk transmisi yang efisien [11]. *Encoding* pada penelitian ini meliputi proses mengubah pesan yang akan disisipkan menjadi baris kode, menentukan *key* dan audio sample kemudian dilanjutkan dengan proses menggantikan LSB pada file audio WAV dengan bit-bit pesan rahasia. Setelah semua bit dari pesan berhasil disisipkan, file audio hasil stego audio akan terbentuk. Proses *encoding* pada penelitian ini dapat dilihat pada Gambar. 2

Gambar 2 Alur proses *Encoding*

Pesan *text* diubah menjadi bilangan biner dengan panjang 8 bit sebelum disisipkan kedalam audio. File audio yang telah dipilih sebagai media pembawa kemudian dikonversikan menjadi deret biner dan dipecah dengan panjang 8 bit. Pesan *text* disisipkan pada file audio dengan mengganti bit paling kanan (2^0) dari file audio.

3. Decoding

Agar pesan yang disisipkan dapat dimengerti penerima, perlu adanya proses *decoding.* Pada proses *decoding*, penerima harus memiliki *key* yang sama dengan *key* yang digunakan pengirim ketika menyisipkan pesan rahasia kedalam file audio. Alur pada proses *decoding* dapat dilihat pada Gambar 3



Gambar 3 Alur proses *decoding*

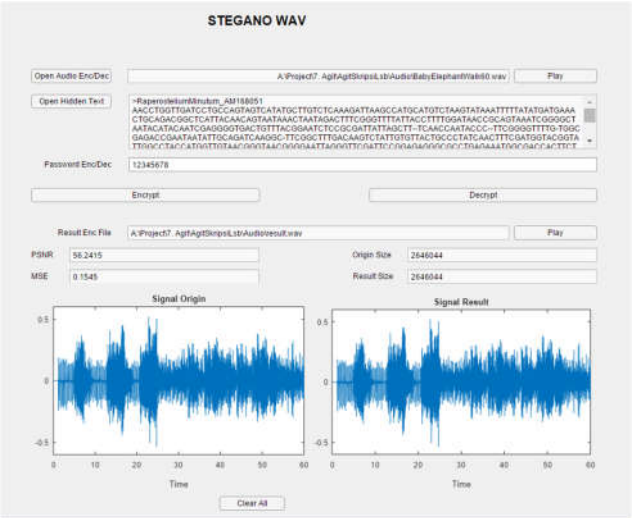
III. HASIL DAN PEMBAHASAN

Pada penelitian ini kualitas audio hasil proses stego-audio dinilai berdasarkan parameter *Mean Squared Error* (MSE) dan *Peak Signal to Ratio (PSNR)*. Pengujian dilakukan pada 6 *file audio WAV* dengan durasi 60 *second* yang disisipi pesan bertipe txt. Ukuran maksimal dari pesan yang dapat disisipkan kedalam audio adalah 1/16 ukuran *array* dari *bit* audio yang digunakan sebagai media penyisipan. Perhitungan ini didasarkan pada teknik LSB yang digunakan. Pada LSB yang digunakan pada penelitian ini, letak bit yang akan disisipkan pesan adalah satu bit terakhir dari panjang 16 bit audio. Pengujian dilakukan secara bertahap, yaitu 1) Menguji PSNR dan MSE pada audio yang telah disisipi pesan berukuran 50% dari kapasitas maksimal. 2) Menguji PSNR dan MSE pada audio hasil stego-audio yang telah disisipi pesan dengan ukuran mencapai kapasistas maksimum. 3) Pengamatan terhadap signal audio hasil stego-audio.

1. Pengujian PSNR dan MSE stego-audio dengan ukuran pesan 50% dari kapasitas maksimal

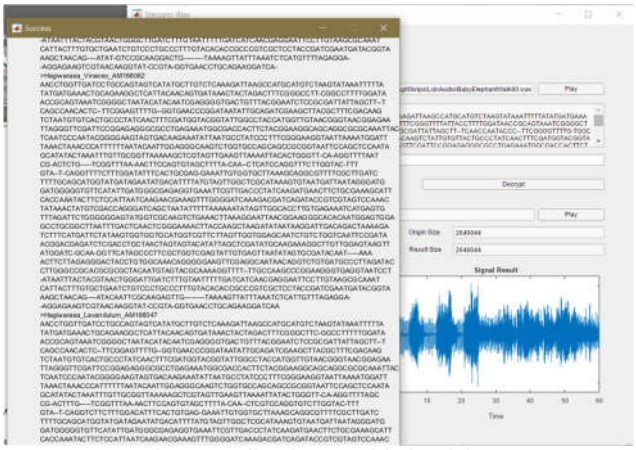
Pengujian ini dilakukan setelah menyisipkan pesan rahasia kedalam audio menggunakan teknik LSB. Pengujian dilakukan untuk mengetahui kualitas audio hasil stego-audio melalui nilai PSNR dan MSE. Ukuran pesan yang disisipkan pada pengujian ini adalah 50% dari kapasitas maksimal pesan yang dapat disisipkan, dimana besaran nilai 50% dari kapasitas maksimal diperoleh angka 50 KB. File pesan yang disisipkan didapat dari *https://ars.els-cdn.com/content/image/1-s2.0-S1434461017300925-mmc9.txt*

Teknik LSB berhasil digunakan untuk menyisipkan dan mengekstrak file pesan dari audio. Gambar 4 merupakan tampilan sistem ketika proses penyisipan pesan kedalam audio.



Gambar 4 Tampilan sistem ketika proses *encoding*

Sistem berhasil menampilkan nilai PSNR dan MSE dari audio yang diproses beserta dengan perbandingan signal dari kedua audio. Gambar 5 adalah tampilan sistem ketika berhasil melakukan ekstraksi pesan dari file audio.



Gambar 5 Tampilan sistem setelah ekstraksi pesan

Ketika menu *decrypt* dijalankan, sistem akan memproses audio hasil stego-audio kemudian menampilkan pesan tersembunyi yang sama persis dengan pesan yang disisipkan kedalam audio melalui proses *encoding*.

Melalui sistem yang dibangun, nilai MSE dan PSNR dari audio yang telah disisipi pesan berhasil didapatkan. Nilai MSE dan PSNR dari masing-masing audio hasil stego-audio yang telah disisipi 50% dari kapasitas maksimal pesan dapat dilihat pada tabel I

TABEL I
NILAI PSNR DAN MSE SETELAH PENYISIPAN 50% KAPASISTAS MAKSIMAL

Audio File	MSE	PSNR
Babyelephantwalk60.Wav	0.15051	56.3551
Cantinaband60.Wav	0.15053	56.3545
Fanfare60.Wav	0.15075	56.3482
Imperialmarch60.Wav	0.15017	56.3650
Pinkpanther60.Wav	0.15023	56.3634
Starwars60.Wav	0.15045	56.3569

Semua audio yang diujikan menunjukkan nilai PSNR diatas 50 dB. Rata-rata nilai PSNR dari audio yang telah melalui proses stego-audio menggunakan pesan yang ukurannya mencapai 50% dari kapasitas maksimal adalah 56.3571 *dB* dengan rata-rata nilai MSE sebesar 0.15044.

2. *Pengujian PSNR dan MSE stego-audio dengan ukuran pesan mencapai kapasitas maksimal*

Pada pengujian ini, audio yang diamati nilai PSNR dan MSE nya merupakan audio hasil stego-audio menggunakan pesan dengan ukuran maksimal. File pesan yang digunakan adalah file *txt* berukuran 100 *KB,* yang didapat dari *https://ars.els-cdn.com/content/image/1-s2.0-S1871678417305101-mmc3.txt*.
Pengujian ini dilakukan untuk mengamati kualitas audio hasil stego-audio ketika pesan yang disisipkan mencapai batas maksimal pesan yang dapat disisipkan.

Hasil pengamatan parameter MSE dan PSNR file audio hasil stego-audio yang telah disisipi pesan dengan kapasitas maksimal dapat dilihat pada tabel II

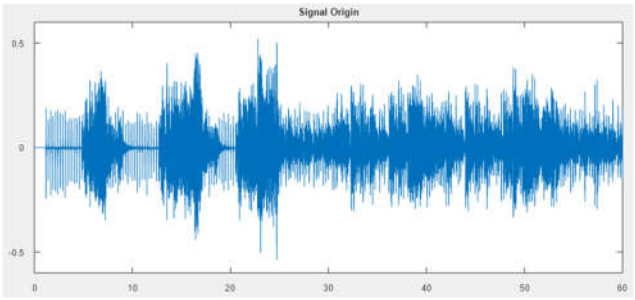
TABEL II
NILAI PSNR DAN MSE AUDIO SETELAH DISISIPI PESAN DENGAN UKURAN MAKSIMAL

Audio File	MSE	PSNR
Babyelephantwalk60.Wav	0.30925	53.2277
Cantinaband60.Wav	0.30938	53.2259
Fanfare60.Wav	0.30910	53.2298
Imperialmarch60.Wav	0.30926	53.2276
Pinkpanther30.Wav	0.30934	53.2265
Starwars60.Wav	0.30918	53.2287

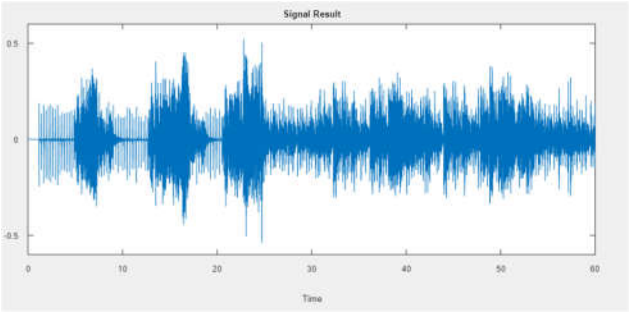
Semua audio yang diujikan menunjukkan kualitas yang baik, dengan nilai PSNR diatas 50 *dB*. Rata-rata nilai PSNR audio yang telah disisipi pesan rahasia yang ukurannya mencapai ukuran maksimal dari ukuran pesan yang dapat disisipkan adalah 53.2277 *dB* dengan rata-rata nilai MSE sebesar 0.3092.

3. *Perbandingan signal audio asli dengan hasil stego-audio.*

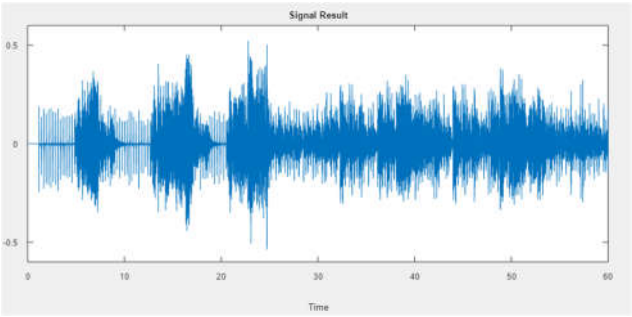
Pada pengujian ini, signal audio asli dibandingkan dengan signal audio hasil stego-audio pada pengujian 1 dan 2 melalui pengelihatan mata manusia. Gambar 6 merupakan signal asli dari audio "Babyelephantwalk.WAV" sedangkan gambar 7 adalah tampilan signal dari "Babyelephantwalk.WAV" ketika disisipi pesan berukuran 50% dari kapasitas maksimal, dan Gambar 8 merupakan tampilan signal "Babyelephantwalk.WAV" setelah disisipi pesan dengan ukuran maksimal.



Gambar 6 Signal asli "Babyelephantwalk60.WAV"



Gambar 7 Signal "Babyelephantwalk60.WAV" dengan 50% dari isi pesan



Gambar 8 Signal "Babyelephantwalk60.WAV" setelah disisipi keseluruhan isi pesan

Signal dari audio yang telah melalui proses stego-audio tidak menunjukkan perubahan signifikan, baik yang telah disisipi pesan berukuran 50% dari kapasitas maksimal maupun pesan dengan ukuran maksimal. Hal ini menunjukkan bahwa penyisipan pesan kedalam audio tidak banyak memengaruhi kualitas signal audio, dibuktikan dengan grafik signal antara audio asli dengan audio hasil stego-audio yang hampir serupa yang didukung dengan nilai rata-rata PSNR yang berada diatas 50 *dB*.

IV. KESIMPULAN

Berdasarkan hasil pengujian yang telah dilakukan pada penerapan teknik *Least Significant Bit* untuk menyisipkan pesan rahasia kedalam file audio diperoleh kesimpulan sebagai berikut:

1. Sistem yang dibangun berhasil melakukan proses *encoding* pesan rahasia kedalam audio dan proses *decoding* untuk mengekstrak pesan rahasia dari dalam audio.
2. Pada pengujian penyisipan pesan berukuran 50% dari kapasitas maksimum diperoleh PSNR sebesar 56.3571 *dB* dengan rata-rata nilai MSE sebesar 0.15044 sedangkan pada pengujian penyisipan pesan berukuran 100% dari kapasitas maksimum diperoleh PSNR sebesar sebesar 53.2277 *dB* dengan rata-rata nilai MSE sebesar 0.3092.
3. Pada pengujian perbandingan grafik signal audio asli dengan signal audio stego diperoleh hasil bahwa secara kasat mata memiliki grafik signal yang hampir serupa. Hal ini menunjukkan bahwa setelah dilakukan penyisipan kulitas signal tidak banyak mengalami perubahan juga didukung dengan rata-rata nilai PSNR dari audio yang diujikan masih berada diatas 50 dB.

UCAPAN TERIMA KASIH

Terimakasih kepada Tuhan Yang Maha Segalanya, yang telah memberikan kesempatan terlaksananya penelitian ini. Kepada para dosen Jurusan Teknik Informatika Unesa yang telah memberikan bimbingan dan ilmu yang bermanfaat. Juga teman-teman jurusan Teknik Informatika yang selalu memberikan dukungan dalam segala kesempatan. Tak lupa untuk kedua orang tua atas kasih sayang dan segala harapan besar yang selalu dipanjatkan kepada Tuhan.

REFERENSI

[1] B. D. J. Dan M. R. Dixit, "Performance Improving Lsb Audio Steganography Technique," *International Journal Of Advance Research In Computer Science And Management Studies,* Vol. 1 (4), Pp. 67-75, 2013.

[2] U. A. M. E. Ali, M. Sohrawordi Dan M. P. Uddin, "A Robust And Secured Image Steganography Using Lsb And Random Bit Substitution," *American Journal Of Engineering Research (Ajer),* Vol. 8 (2), Pp. 39-44, 2019.

[3] S. K. Szczypiorski, "New Method For Information Hiding In Club Music," Dalam *2nd International Conference On Frontiers Of Signal Processing*, 2016.

[4] B. Sharmila, "Effective Audio Steganography Based On Lsbmr Algorithm," *International Journal Of Research In Engineering, Science And Management,* Vol. 3 (4), Pp. 37-40, 2020.

[5] A. M. Meligy Dan M. M. N. A. F. T. Eid, "A Hybrid Technique For Enhancing The Efficiency Of Audio Steganography," *International Journal Of Image, Graphics And Signal Processing,* Pp. 36-42, 2016.

[6] N. C. Sy, H. H. Kha Dan N. M. Hoang, "An Efficient Robust Blind Watermarking Method Based On Convolution Neural Networks In Wavelet Transform Domain," *International Journal Of Machine Learning And Computing,* Vol. 10 (5), Pp. 675-684, 2020.

[7] A. A. Hosny, W. A. Murtada Dan Mohamed I. Youssef, "Improving Lsb Audio Steganography Using Simulated Annealing For Satellite Telemetry," Dalam *14th International Computer Engineering Conference (Icenco)*, 2018.

[8] J. Hashim, A. Hameed, M. J. Abbas, M. Awais, H. A. Qazi Dan S. Abbas, "Lsb Modification Based Audio Steganography Using Advanced Encryption Standard (Aes-256) Technique," Dalam *12th International Conference On Mathematics, Actuarial Science, Computer Science And Statistics (Macs)*, 2018.

[9] K.P.Adhiya Dan S. A. Patil, "Hiding Text In Audio Using LSB Based Steganography," *Information And Knowledge Management,* Vol. 2 (3), Pp. 8-14, 2012.

[10] S. Mishra, V. K. Yadav Dan M. C. Trivedi, "Audio Steganography Techniques: A Survey," Dalam *Advances In Computer And Computational Sciences*, Singapore, Springer Nature Singapore Pte Ltd, 2018, Pp. 581-589.

[11] A. R. Lubis, M. S. Lidya Dan M. A. Budiman, "Perancangan Perangkat Lunak Steganografi Audio Mp3 Menggunakan Metode Least Significant Bit (Lsb) Dengan Visual Basic 6.0," *Jurnal Dunia Teknologi Informasi,* Vol. 1 (1), Pp. 63-68, 2012.

[12] M. E. Mustakma, "Audio Steganografi Dengan Algoritma Lsb Untuk Pengamanan Data Digital," Yogyakarta, 2018.

[13] A. K. G. Satish Bhalshankar, "Audio Steganography: Lsb Technique Using A Pyramid Structure And Range Of Bytes," *International Journal Of Advanced Computer Research (Ijacr),* Vol. 5 (20), Pp. 233-248, 2015.

[14] A. Koyun Dan H. B. Macit, "Generating A Stego-Audio Data Using Lsb Technique And Robustness Test," *Journal Of Engineering Sciences And Design,* Vol. 6 (1), Pp. 87-92, 2018.

[15] D. Salomon Dan G. Motta, Handbook Of Data Compression Fifth Edition, London: Springer-Verlag London Limited, 2010.