LEAST SIGNIFICANT INVERSE BIT (LSIB) PADA STEGANOGRAFI HEADER MP3

Ibnu Utomo Wahyu Mulyono[1], Ajib Susanto[2], Christy Atika Sari[3], Eko Hari Rachmawanto[4], De Rosal Ign. Moses Setiadi[5], Stefano Felix Pranata[6], Castaka Agus Sugianto[7]

[1,2,3,4,5,6]*Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro*

Jl. Imam Bonjol No 207 Semarang, 50131

[7]*Program Studi Teknik Informatika, Politeknik TEDC Bandung*

Jl. Politeknik - Pesantren Km 2, Cibabat, Cimahi, 40513

E-mail : ibnu.utomo.wm@dsn.dinus.ac.id[1], ajib.susanto@dsn.dinus.ac.id[2], atika.sari@dsn.dinus.ac.id[3], eko.hari@dsn.dinus.ac.id[4], moses@dsn.dinus.ac.id[5], stefanofelixpranata@gmail.com[6], castaka@poltektedc.ac.id[7]

Abstrak

Keamanan dari pengiriman informasi menjadi sebuah masalah penting yang perlu di tindak lanjuti, khususnya penyembunyian pesan dalam media tertentu. File MP3 adalah salah satu media yang sangat populer digunakan, namun ternyata jarang dimanfaatkan dalam steganografi. Algoritma Inverse Bit dapat meningkatkan MSE dan PSNR dari cover. LSB adalah algoritma yang sederhana, selain itu juga sudah diterapkan pada bit yang tidak digunakan pada header MP3. Dalam penelitian ini, Inverse Bit akan digabungkan dengan LSB pada header MP3. Inverse bit LSB ditentukan dari nilai bit kedua terakhir dan ketiga terakhir cover dibandingkan dengan citra stego, yang didapat dari menerapkan LSB standar, sehingga akan muncul pola 01, 10, 00, dan 11. Pada penelitian ini akan dilakukan pada 50 citra dan MP3 berdurasi antara 2 sampai 4 menit. Pada proses penyisipan pesan memerlukan waktu antara 3 hingga 40 detik dan pada pengambilan pesan memerlukan 2 hingga 20 detik. Nilai MSE yang didapat pada seluruh file hasil embedding adalah 0, sedangkan PSNR bernilai infiinitif. Nilai infinitive dapat diartikan bahwa file hasil steganografi dapat diproses dengan baik. Nilai BER hasil ekstraksi mendekati 0.

***Kata Kunci*:** Steganografi, MP3, LSB, Inverse Bit, PSNR, BER

I. PENDAHULUAN

Luasnya penggunaan internet menyediakan kenyamanan untuk melakukan pengiriman data dalam jumlah besar melalui jaringan [1]. Penggunaan internet hari demi hari meningkat dan pengiriman informasi penting melalui internet juga meningkat. Pengiriman pesan melalui internet memiliki beberapa masalah seperti keamanan informasi dan pelanggaran hak cipta [2]. File audio dapat digunakan untuk menyembunyikan informasi seperti layaknya file gambar [3]. Steganografi audio dapat dilakukan pada file MP3. Umumnya metode LSB digunakan untuk menyisipkan pesan pada tiap audio sample pada file. Pada file MP3, penyisipan pesan dengan LSB dapat dilakukan pada bit yang tidak digunakan pada header untuk kapasitas yang lebih dan meningkatkan ketahanan pesan [4]. Salah satu pentingnya menyembunyikan data pada file audio adalah umumnya keberadaan dari sinyal audio sebagai informasi pada masyarakat.

Steganografi bertujuan untuk menyembunyikan pesan sehingga hanya pengirim dan penerima pesan yang mengetahui keberadaan dari informasi yang dikirimkan [11]. Teknik ini dapat dikombinasikan dengan teknik lain misalnya watermarking [12] atau kriptografi [13] [14]. Steganografi dapat dilakukan pada banyak media misalnya

teks [15], gambar, audio dan video, dimana menyisipkan file gambar seperti dilakukan oleh [11], misalnya gambar penyakit menggunakan salah satu teknik pengembangan dari LSB yaitu End Of File [16] lebih mudah dibandingkan file audio maupun video. Dalam makalah ini akan dilakukan uji performa steganografi pada media audio yaitu file MP3, disisi lain penelitian yang telah banyak dilakukan pada steganografi audio biasanya menggunakan file wav. Metodologi steganografi dapat di bedakan menjadi reversible dan irreversible bedasarkan kemampuan mengembalikan cover dari stego pada tahap ekstraksi. Teknik reversible dilakukan untuk mendapatkan data yang dibenamkan dan media pembawa dari stego. Teknik ini dilakukan ketika cover dan data yang dibenamkan sangat penting, sedangkan teknik irreversible berfokus pada pengambilan pesan dari stego.

Praktek Steganografi mengasumsikan bahwa cover yang digunakan untuk menyembunyikan pesan seharusnya tidak meningkatkan kecurigaan pada lawan. Faktanya ketersediaan dan popularitas dari file audio menyebabkan mereka layak untuk membawa pesan tersembunyi [5]. Tidak seperti sistem visual manusia, sistem auditori manusia lebih sensitif, meteode LSB langsung dapat menyebabkan masalah seperti timbulnya suara mendesis jika pesan yang disisipkan memiliki amplitudo nol atau mendekati nol yang menyatakan tidak adanya suara. Pada penelitian Mohammed Abdul Majeed dan Rossilawati Sulaiman pada tahun 2015, metode LSB dikembangkat dengan Inverse Bit. Metode LSB Inverse Bit adalah metode untuk membalik nilai bit pada cover [6]. Pembalikan nilai bit dilakukan setelah metode LSB standard selesai dilakukan untuk mengurangi jumlah bit yang berubah pada cover. Keamanan pesan yang disisipkan pada cover juga meningkat untuk memperkuat kelemahan dari LSB. Pada penelitian oleh Neha Gupta dengan cara memodifikasi LSB dengan Discrete Wavelet Transform, pesan disisipkan kedalam tepi objek gambar supaya perubahan semakin tidak terlihat [7].

II. METODOLOGI PENELITIAN

1. Penelitian Terkait

Menurut penelitian yang dilakukan oleh Muhammad Asad [8], telah dilakukan teknik modifikasi LSB konvensional untuk steganografi audio agar lebih aman terhadap steganalisis. Rata-rata, teknik tersebut menyematkan satu bit pesan rahasia per empat sampel pesan host. Tingkat embedding maksimum adalah satu bit pesan rahasia per sampel pesan host sementara tingkat embedding minimum adalah satu bit pesan rahasia per delapan sampel pesan host. Perintah buruk untuk memastikan pesan rahasia benar-benar tertanam, contoh pesan host seharusnya. Improvisasi dilakukan dengan mengkombinasikan Advanced Encryption Standard (AES) dengan panjang kunci 256 bit digunakan untuk mengamankan pesan rahasia jika teknik steganografi pecah. Teknik yang diusulkan telah diuji keberhasilannya pada file .wav pada frekuensi sampling 8000 sampel /detik dengan masing-masing sampel yang dalam 8 bit.

Tabel 1. State of the Art

Tahun	Nama Peneliti	Algoritma			Media (audio file)			
		LSB	Inverse Bit	DWT	AES	Wav	Au	Mp3
2011	Muhammad Asad, dkk [8]	v			v	v	v	v
2013	Mohammed Salem Atoum, dkk [9]	v						v
2014	Neha Gupta dan Nidhi Sharma [7]	v		v				v
2016	Biswajita Datta [10]	v				v		
2019	Usulan pada paper ini	v	v			v		

Pada penelitian yang dilakukan oleh Gupta [7], percobaan membuktikan adanya peningkatan ketahanan, keamanan dengan menggunakan konsep DWT (Discrete Wavelet Transform) dan LSB (Least Significant Bit) mengajukan metode baru Audio Steganography. Penekanannya adalah pada skema yang diusulkan untuk

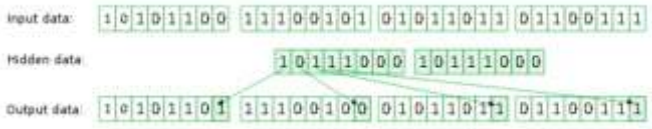
menyembunyikan gambar dalam audio dan perbandingannya dengan metode penyisipan Bit Least Significant Bit yang sederhana untuk menyembunyikan data dalam audio. Dalam hal ini pesan berupa gambar yang disisipkan ke dalam file audio, dimana ukuran file pesan yaitu 1 KB sedangkan file induk yaitu 2,5 MB dengan hasil nilai PSNR yaitu 37.0733 dB. Kekurangan dari penelitian ini yaitu data yang digunakan belum beragam.

Pada penelitian lain yang dilakukan oleh Data, dkk [10] telah dilakukan percobaan dengan menanamkan tiga bit dalam sampel dan mempertimbangkan representasi 6 bit ASCII sebagai gantinya 7 membantu meningkatkan kapasitas, pemilihan piksel acak non-berturut-turut meningkatkan ketidaksempurnaan media stego serta ketahanan. Ketangguhan teknik ini juga dicapai dengan memilih beberapa LSB Layers secara acak untuk embedding. Disini dua tingkat keacakan diperkenalkan satu dengan melakukan permutasi untuk memilih tiga dari lima lokasi LSB dan kemudian dengan memilih pengaturan secara acak. Hal ini membuat para penyusup bekerja lebih keras untuk mendapatkan pesan rahasia saat transit.

Berbeda dengan beberapa penelitian diatas menggunakan LSB atau mengkombinasikan LSB dengan DWT maupun AES yang disisipkan pada bagian body file sehingga payload yang dioperasikan sangat kecil dan terdapat perbedaan anatara file asli dengan file hasil steganografi. Pada karya ilmiah ini, kami mengimplementasikan LSB untuk memenuhi aspek ketidaknampakan dan perbedaan tempat penyisipan yaitu pada bagian header file. Hal ini dimaksudkan supaya gambar yang digunakan sebagai pesan dapat tertampung dengan baik.

2. Least Significant Bit (LSB)

Pada teknik steganografi, nilai Least Significant Bit dari cover digunakan untuk menyembunyikan pesan. LSB paling sederhana [17] yaitu dengan melakukan subtitusi terhadap nilai LSB dengan nilai pesan yang perlu disembunyikan. Metode ini merubah nilai data dengan sangat kecil. Pada penelitian ini LSB akan digunakan pada file MP3 sebagai cover pesan.



Gambar 1. Model Embedding menggunakan LSB

3. Struktur file MP3

File MP3 adalah bagian dari MPEG yaitu MPEG Versi 1 Layer 3 yang masih aktif dan menjadi standard yang popular [15]. Sebuah file audio MPEG terdiri dari bagian yang lebih kecil disebut dengan frame. Secara umum frame bersifat independen. Setiap frame memiliki header dan informasi audio sendiri. Tidak ada file header. Oleh sebab itu, file MPEG dapat dipotong di bagian manapun dan dimainkan dengan benar. Ketika ingin membaca informasi tentang file MPEG, biasaya cukup untuk menemukan frame pertama, baca headernya dan asumsikan bahwa frame lain juga memiliki header yang sama. Frame header terdapat pada 4 byte pertama pada frame. Sebelas bit pertama selalu bernilai 1 dan mereka disebut dengan “frame sync”. Kemudian pencarian dapat dilakukan. Frame mungkin memiliki pengecekan CRC yang panjangnya 16 bit dan jika ada akan mengikuti frame header. Setelah CRC terdapat data audio. Terdapat 3 bagian header yang tidak diperlukan untuk decoding yaitu private bit, original bit, dan copyright bit. Header file MPEG dapat digambarkan dengan notasi [16]: AAAAAAAA AABBCCD EEEEFFGH IIJJKLMM

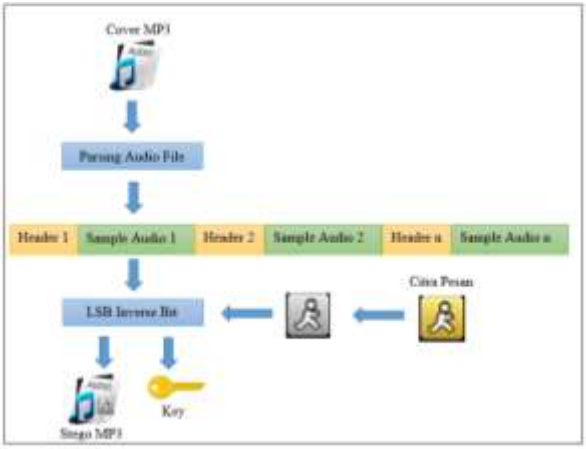
Tabel 2. Bagian dari header MP3

Kode	Panjang (byte)	Posisi (byte)	Deskripsi

A	11	(0-10)	Frame sync, semua bit bernilai 1.
B	2	(11-12)	ID versi audio MPEG.
C	2	(13-14)	Deskripsi Layer
D	1	(15)	Bit perlindungan CRC
E	4	(16-19)	Indeks Bitrate
F	2	(20-21)	Indeks sampling rate frequency (nilai dalam Hz)
G	1	(22)	Padding bit
H	1	(23)	Private bit.
I	2	(24-25)	Mode Channel
J	2	(26-27)	Mode penggabungan (Hanya jika Joint stereo)
K	1	(28)	Hak Cipta
L	1	(29)	Original Bit
M	2	(30-31)	Emphasis

4. Metode yang diusulkan

Secara umum, metode yang diusulkan dalam penelitian ini terdiri dari dua proses utama, yaitu proses untuk merahasiakan pesan dan proses untuk pengambilan pesan.



Gambar 2. Proses penyisipan pesan

Operasi untuk membalik nilai bit terakhir dari tiap pixel pada cover bedasarkan nilai pesan rahasia. Metode standar LSB ini dilakukan ketika setiap bit pesan sudah di sisipkan dalam cover. Teknik inverse ditentukan dari nilai bit kedua terakhir dan ketiga terakhir cover dibandingkan dengan citra stego, yang didapat dari menerapkan LSB standar. Tahap metode ini adalah:

1. Hitung pola kemunculan pola bit 00, 01, 10, dan 11 dalam citra cover.
2. Terapkan metode LSB standar untuk mendapat citra stego.

3. Hitung pola kemunculan pola di bit kedua terakhir dan ketiga terakhir dari citra stego, hasil dari pola ini akan digunakan sebagai metode inverse.
4. Bandingkan jumlah bit dari pola citra cover dan citra stego yang berubah.
5. Inverse bit LSB yang jumlah pixel yang berubah lebih banyak dari jumlah pixel yang tidak berubah
6. Simpan status perubahan pesan yang di inverse nilai pixelnya.

Contoh tahap demi tahap proses: Pesan : 1011 dengan Cover : 10001100 (A), 10101101 (B), 10101011 (C), dan 10101101 (D), adalah :

1. Jumlah kemunculan p, Pola bit kedua dan bit ketiga terakhir adalah

Tabel 2. Frekuensi kemunculan pola

Pola	Kemunculan	Kode
00	0	-
01	1	C
10	3	A, B, D
11	0	-

2. Terapkan metode LSB standar

   Stego : 10001101 (A), 10101100 (B), 10101011 (C), dan 10101101 (D)

   Hitung kemunculan pola pada citra stego

Tabel 3 Frekuensi perubahan pada pola

Pola	Kemunculan	Berubah
00	0	0
01	1	0
10	3	2
11	0	0

3. Bandingkan jumlah bit pola citra cover dan citra stego

Tabel 4 Persentase perubahan pada pola

Pola	Kemunculan	Berubah	Perubahan
00	0	0	0%
01	1	0	0%
10	3	2	66,6%
11	0	0	0%

4. Inverse bit LSB yang jumlah pixel yang berubah lebih banyak dari jumlah pixel yang tidak berubah

   Stego : 10001101 (A), 10101100 (B), 10101011 (C), dan 10101101 (D)

   Stego : 10001100 (A), 10101101 (B), 10101011 (C), dan 10101100 (D)

5. Status perubahan 0010

Diakhir hanya terdapat satu pixel pada citra stego yang berbeda dari citra awal, dan kualitas citra stego meningkat [9].

III. HASIL DAN PEMBAHASAN

Data audio yang digunakan bebas royalti dan diambil dari http://bensound.com dengan lisensi dari Creative Commons. Audio sebagai media cover penyisipan pesan seperti pada Gambar 3, sednagkan data citra yang digunakan diambil dari all-free-download.com dibawah lisensi dari Creative Commons Attribution-Share Alike 3.0 Unported License. Pengujian dilakukan dengan menghitung nilai MSE (Mean Square Error), PSNR (Peak Signal to Noise Ratio) dan BER (Bit Error Ratio) cover audio dengan stego audio, begitu juga dengan pesan yang disisipkan dan pesan yang di ekstrak. Pengujian ini dilakukan agar dapat mengetahui kualitas stego-audio bila dibandingkan dengan cover aslinya dan kualitas pesan yang disisipkan dengan pesan yang diekstrak. Semakin rendah nilai MSE dan semakin tinggi nilai PSNR berarti semakin bagus kualitas audio dan citra.

Tabel 5. Cover Audio

No	Nama File	Durasi	No	Nama File	Durasi
1	bendsound-dubstep.mp3	2:04	6	bendsound-epic.mp3	2:58
2	bendsound-cute.mp3	3:14	7	bendsound-funnysong.mp3	3:07
3	bendsound-littleidea.mp3	2:49	8	bendsound-happiness.mp3	4:21
4	bendsound-acousticbreeze.mp3	2:37	9	bendsound-goinghigher.mp3	4:04
5	bendsound-buddy.mp3	2:02	10	bendsound-betterdays.mp3	2:33

Aim Apple Bebo Blogger Brightkite Delicious Designfloat Designmoo Deviantart Digg

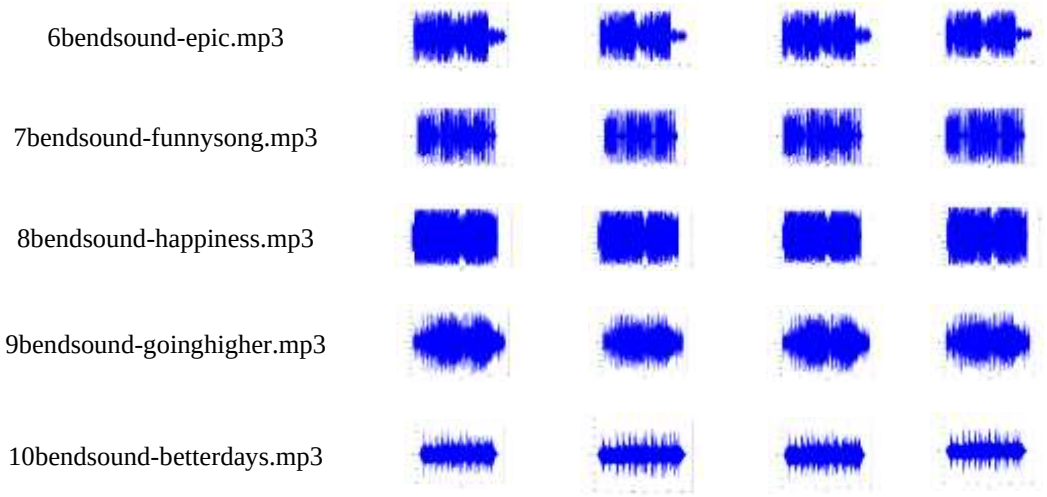
Gambar 3. Gambar Pesan yang akan disisipkan

Tabel 6. Header dan Kapasitas Cover

Cover	Header	Jumlah	Kapasitas bit	Kapasitas pixel
1	FFFD1062	1282	3846	480
2	FFFD1062	2045	6135	766
3	FFFD1062	1657	4971	621
4	FFFD1022	619	1857	232
5	FFFD1022	340	1020	127
6	FFFD1062	1749	5247	655
7	FFFD1062	1572	4716	589
8	FFFD7002	1023	3069	383
9	FFFD1062	1637	4911	613
10	FFFD1062	1021	3063	382

Tabel 7. Gelombang Frekuensi Audio sebelum dan sesudah penyisipan

Cover	Cover Audio		Stego Audio	
	Channel 1	Channel 2	Channel 1	Channel 2
1bendsound-dubstep.mp3				
2bendsound-cute.mp3				
3bendsound-littleidea.mp3				
4bendsound-acousticbreeze.mp3				
5bendsound-buddy.mp3				



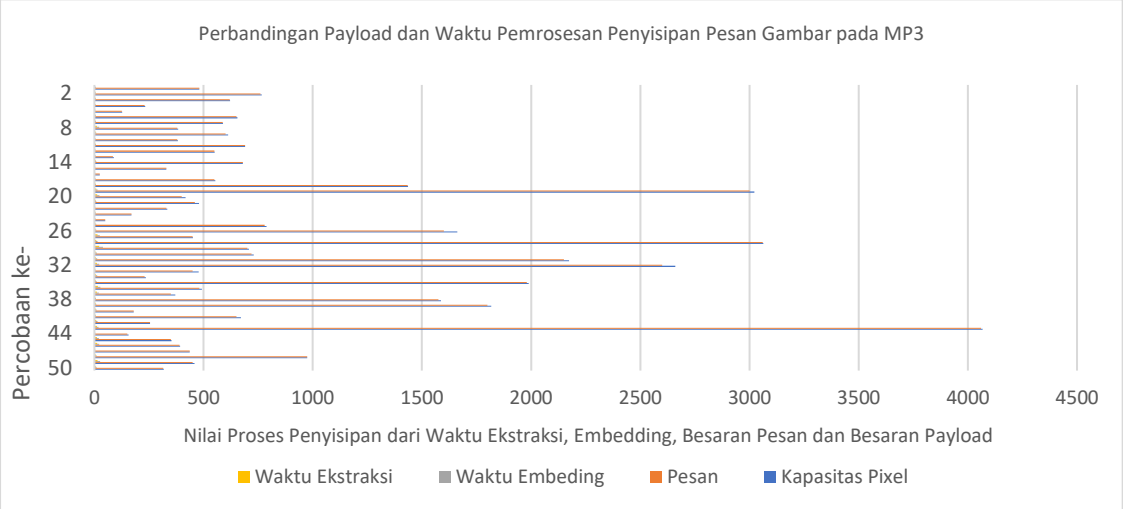
Tabel 7 merupakan hasil embedding atau penyisipan pesan menggunakan LSB inverse bit. Dapat dilihat pada Channel 1 dan Channel 2 yang telah diuji coba pada 10 buah data audio. Gelombang frekuensi audio tampak tidak berubah setelah dilakukan penyisipan. Berarti metode penyisipan pada bit yang tidak digunakan pada header tidak akan merubah suara pada cover. Di bawah ini merupakan percobaan yang telah dilakukan untuk menguji dta MP3 dengan menghitung nilai MSE, PSNR dan BER. Nilai MSE dan PSNR dihitung pada setiap cover dan stego, nilai MSE 0 dan PSNR Inf berarti suara tidak mengalami perubahan, BER menunjukan adanya perubahan bit pada stego karena penyisipan pesan seperti tampak pada Tabel 8 berikut.

Tabel 8 Key Inverse, MSE, PSNR dan PSNR hasil percobaan

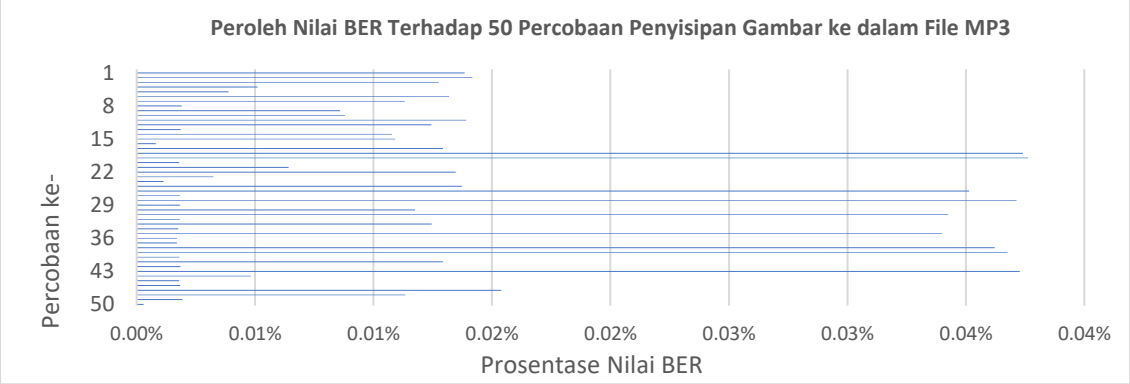
Percobaan ke	Key Inverse Bit	MSE	PSNR	BER
1	5FFFFFFFFFFFFFFFBFBFFFFFFFFFFFFF7FFFFFFFFBFFFFFFF3F7EFFFBFFFF08	0	Inf	0.01384621%
2	F5FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFEFFFFFFFFFFFFFFFFFFFF08	0	Inf	0.01416759%
3	06CFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF08	0	Inf	0.01275740%
4	000CFFFFFF77FFFFDE7FEFFAE78ED5F47FBDDE4EDB77FB953E479688F6E8FF08	0	Inf	0.00510594%
5	0008DF7F84F7FDD3BB4CF3AF5BA97EDBD5CB7F87B17F77AD4ECFF9EF77B2EF08	0	Inf	0.00387409%
6	004EFFFFFFFFFFFFFFFFFDFFFFFFFFFFDFFDFFFFFBFFE67FBD7F7D97FBCF708	0	Inf	0.01317988%
7	DCFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFDFFBFFFF08	0	Inf	0.01131690%

8	FFFFFFFFFFFFD9C74FBF77F95DDCF5EFD75FBDE72798F467FB6FFFFF35000008	0	Inf	0.00190164%
9	14FFFFFFFFFFFFFFFFFFFFFFF7FFFFFFFFFFFFFFFFDFFFFFFFFFFFFFFFF08	0	Inf	0.00858783%
10	DFEFFFFFFFF43E2C01C3C6B0206298024040008000000000080000000008508	0	Inf	0.00878724%

Citra yang diambil dari stego audio dibandingkan dengan citra yang disisipkan untuk mengetahui apakah citra yang diambil sama dengan citra yang disisipkan. Nilai MSE 0 dan PSNR Inf menunjukan bahwa citra tidak mengalami perubahan. Pada Gambar 4 diketahui bahwa terdapat 50 data percobaan yang telah dilakukan dengan hasil nilai BER tertinggi yaitu pada data ke 43, dimana nilai payload dan pesan yang disisipkan dalam kapasitas yang besar. Sedangkan untuk seluruh data yang digunakan dalam percobaan, nilai MSE bernilai 0, PSNR bernilai Inf. BER dapat dilihat pada Gambar 5.



Gambar 4. Perbandingan Payload dengan Waktu Pemrosesan



Gambar 5. Gambar Pesan yang akan disisipkan

IV. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan oleh penulis, maka dapat disimpulkan bahwa proses steganografi telah berhail dilakukan dan mendapat hasil yang baik. Kapasitas penyimpanan pada header MP3 sangat bervariasi bergantung pada file MP3 yang digunakan. Kapasitasnya berkisar antara 195 bit sampai 32550 bit pesan. Setelah dilakukan penyisipan, stego audio memiliki MSE 0 dan PSNR tidak terhingga, yang berarti audio tidak berubah setelah disisipi pesan. Pada proses penyisipan pesan memerlukan waktu antara 3 hingga 40 detik dan pada pengambilan pesan memerlukan 2 hingga 20 detik. Steganografi dengan LSB inverse bit terbukti dapat memenuhi aspek imperceptibility sesuai Tabel. 7 dan aspek payload yang ditunjukkan pada Gambar 5. LSB inverse bit terbukti dapat digunakan untuk melakukan penyisipan pesan pada pesan dan kapasitas piksel dengan ukuran sama

VI. REFERENSI

[1] D. R. I. M. Setiadi, E. H. Rachmawanto, and C. Sari, "Secure Image Steganography Algorithm Based on DCT with OTP Encryption," *J. Appl. Intell. Syst.*, vol. 2, no. 1, pp. 1–11, 2017.

[2] M. a. Faizal, H. B. Rahmalan, E. H. Rachmawanto, and C. A. Sari, "Impact Analysis for Securing Image Data using Hybrid SLT and DCT," *Int. J. Futur. Comput. Commun.*, vol. 1, no. 3, pp. 309–311, 2012.

[3] L. Umaroh, C. A. Sari, Y. P. Astuti, and E. H. Rachmawanto, "A robust image watermarking using hybrid DCT and SLT," in *2016 International Seminar on Application for Technology of Information and Communication (ISemantic)*, 2016, pp. 312–316.

[4] M. Bazyar and R. Sudirman, "A Recent Review of MP3 Based Steganography Methods," *Int. J. Secur. Its Appl.*, vol. 8, no. 6, pp. 405–414, Nov. 2014.

[5] M. Tayel, A. Gamal, and H. Shawky, "A proposed implementation method of an audio steganography technique," in *2016 18th International Conference on Advanced Communication Technology (ICACT)*, 2016, no. 3, pp. 180–184.

[6] M. A. Majeed and R. Sulaiman, "An improved LSB image steganography technique using bit-inverse in 24 bit colour image," *J. Theor. Appl. Inf. Technol.*, vol. 80, no. 2, pp. 342–348, 2015.

[7] N. Gupta and N. Sharma, "Dwt and Lsb based Audio Steganography," in *2014 International Conference on Reliability Optimization and Information Technology (ICROIT)*, 2014, pp. 428–431.

[8] M. Asad, J. Gilani, and A. Khalid, "An enhanced least significant bit modification technique for audio steganography," in *International Conference on Computer Networks and Information Technology*, 2011, pp. 143–147.

[9] M. S. Atoum, S. Ibrahimn, G. Sulong, A. Zeki, and A. Abubakar, "Exploring the Challenges of MP3 Audio Steganography," in *2013 International Conference on Advanced Computer Science Applications and Technologies*, 2013, pp. 156–161.

[10] B. Datta, P. K. Pal, and S. K. Bandyopadhyay, "Multi-bit Data Hiding in Randomly Chosen LSB Layers of an Audio," in *2016 International Conference on Information Technology (ICIT)*, 2016, no. July, pp. 283–287.

[11] E. H. Rachmawanto and C. A. Sari, "Steganografi Pengamanan Data Gambar Penyakit dengan Hybrid SLT-DCT," in *SEMANTIK 2013*, 2013, vol. 2013, no. November, pp. 96–101.

[12] C. A. Sari, S. D.R.I.M., and E. H. Rachamwanto, "Robust and Imperceptible Image Watermarking by DC Coefficients Using Singular Value Decomposition," in *4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI 2017)*, 2017.

[13] E. H. Rachmawanto and C. A. Sari, "KEAMANAN FILE MENGGUNAKAN TEKNIK KRIPTOGRAFI," *Techno.COM*, vol. 14, no. 4, pp. 329–335, 2015.

[14] C. A. Sari, E. H. Rachmawanto, D. W. Utomo, and R. R. Sani, "Penyembunyian Data Untuk Seluruh Ekstensi File Menggunakan Kriptografi Vernam Cipher dan Bit Shiffting," *J. Appl. Intell. Syst.*, vol. 1, no. 3, pp. 179–190, 2016.

[15] S. Roy and M. Manasmita, "A novel approach to format based text steganography," in *Proceedings of the 2011 International Conference on Communication, Computing & Security - ICCCS '11*, 2011, pp. 511–516.

[16] C. A. Sari and E. H. Rachmawanto, "Gabungan Algoritma Vernam Chiper Dan End of File," *Techno.COM*, vol. 13, no. 3, pp. 150–157, 2014.