Keamanan Informasi Menggunakan *Steganografi 3LSB* dengan Modifikasi Jarak *Byte* pada Audio

Ilham Akbar*[1], Khoerul Anwar[2], Samsul Arifin[3]
[1,2,3,] Teknologi Informasi, STMIK PPKIA Pradnya Paramita, Malang, Indonesia
Korespodensi author: ilhamakbarki@gmail.com

Info Artikel

Diajukan: 20 Februari 2020
Diterima: 12 Maret 2020
Diterbitkan: 19 Maret 2020

Keywords:
Security; cryptography; Steganography; 2LSB; 3LSB
Kata Kunci:
Keamanan;kriptografi; Steganografi; 2LSB; 3LSB

Abstract

Information security and data confidentiality are very important when exchanging information through communication networks. This is done with the aim of securing data from people who are not responsible. The techniques used to secure information today are cryptography and steganography. One of the methods often used in steganography is the Least Significant Bit (LSB), and this method can be improved by adding binary values which are replaced with modern ones (3LSB). The experiments carried out were the success rate of the insertion, extraction, capacity change, and quality change of the stego audio sound. The results of 20 experiments obtained a success percentage of 100% in the process of encoding and decoding information. The capacity of information on the media also increased by 2.21% from the conventional method (2LSB), And the sound quality of the resulting modern stego audio is not too different from conventional methods. So it can be concluded that using modern methods can increase the capacity and does not really change the sound quality of conventional methods

Abstrak

Keamanan informasi dan kerahasiaan data sangat penting dalam pertukaran informasi melalui jaringan komunikasi. Hal ini dilakukan dengan tujuan untuk mengamankan data dari pihak yang tidak bertanggung jawab. Teknik yang digunakan untuk mengamankan informasi saat ini adalah kriptografi dan steganografi. Salah satu metode yang sering digunakan dalam steganografi adalah Least Significant Bit (LSB), dan metode ini dapat diperbaiki dengan menambahkan nilai biner yang diganti dengan nilai modern (3LSB). Eksperimen yang dilakukan adalah tingkat keberhasilan penyisipan, ekstraksi, perubahan kapasitas, dan perubahan kualitas suara audio stego. Hasil dari 20 percobaan diperoleh persentase keberhasilan sebesar 100% pada proses pengkodean dan penguraian informasi. Kapasitas informasi pada media juga meningkat sebesar 2,21% dari metode konvensional (2LSB). Dan kualitas suara audio stego modern yang dihasilkan tidak jauh berbeda dengan cara konvensional. Jadi dapat disimpulkan bahwa penggunaan metode modern dapat meningkatkan kapasitas dan tidak terlalu mengubah kualitas suara dibandingkan metode konvensional

Cara mensitasi artikel:
Akbar I, Anwar, K., Arifin, S., & Arifin S (2020). Keamanan Informasi Menggunakan *Steganografi 3LSB* dengan Modifikasi Jarak *Byte* pada Audio. Jurnal Teknologi Informasi: Teori, Konsep, dan Implementasi (JTI-TKI), 11(1), 22-27. https://doi.org/10.36382/jti-tki.v11i1.492

PENDAHULUAN

Pada zaman perkembangan teknologi seperti saat ini, salah satu pertukaran data yang paling besar adalah melalui jaringan Internet, dimana setiap orang dapat mengirim dan menerima Data berupa Text, Gambar, Audio atau Video secara bebas tanpa dibatasi jarak dan waktu. Hal ini juga mempengaruhi perkembangan kejahatan yang memanfaatkan teknologi Informasi, dimana orang yang tidak bertanggung jawab dapat dengan mudah mengakses informasi pribadi atau informasi yang bersifat privasi, akibatnya kejahatan ini dapat merugikan orang lain, Oleh karena itu kemanan sangat dibutuhkan untuk melindungi pertukaran informasi yang ditrasmisikan melalui jaringan komunikasi seperti jaringan Internet.

Saat ini untuk mengamankan sebuah informasi dibagi menjadi Kriptografi dan *Steganografi*[1][2], Kriptografi adalah mengubah informasi bermakna menjadi informasi yang tidak bermakna, sedangkan *steganografi* adalah teknik menyembunyikan informasi[3] kedalam suatu media atau wadah pembawa informasi. [4]

Kemanan informasi yang dengan menggunakan metode Kriptografi dapat diketahui dengan mudah oleh orang lain karena data yang dihasilkan dari proses Kriptografi dapat dilihat dengan jelas dari struktur datanya, berbeda sekali dengan menggunakan metode steganografi ini, dimana proses pengamanan data yang dilakukan oleh metode ini disembunyikan atau disisipkan [5] pada media berupa file gambar atau Audio, hasilnya data yang diamankan sangat sulit dibedakan oleh manusia, karena didalam sebuah media tersebut tenyata terdapat sebuah data/informasi yang tersembunyi.

Salah satu metode yang digunakan pada *Steganografi* adalah *Least Significant Bit* (*LSB*)[6]. Metode *LSB* melakukan penyisipan[7]pesan dengan mengganti *bit* terakhir dalam sebuah *byte* media pembawa pesan. Dengan mempelajari Jurnal dari Astuti, E. S., Prihadmantyo, B., &

Apriyani, M. E. Dengan judul "Implementasi Algoritma Kriptografi *Rc4* [8]Dan Metode *Steganografi* Audio *2lsb* Pada Sistem Keamanan Informasi", Pada penelitian tersebut penulis menggunakan metode *steganografi 2LSB* dan memodifikasi jarak *byte* sebesar 5 *byte* dan setelah melakukan percobaan sebanyak 3 kali dengan menyisipkan *plaintext*, didapatkan hasil bahwa berhasil menyimpan dan mengembalikan pesan rahasia, dan kualitas suara dari *stego* audio bagus dengan nilai lebih dari 30 db.

Metode *LSB* [9] ini bergantung pada ukuran *file* media pembawanya dimana jika *file* media memiliki ukuran yang besar maka pesan yang dapat disisipkan [10] akan memiliki ukuran yang besar juga, hal ini mempengaruhi data yang simpan pada *hardisk* penyimpanan (*drive*) atau data yang dikirim melalui jaringan dimana jika *file* tersebut besar maka akan terlalu banyak membuang-buang *resource* atau dapat dikatakan kurang efisiensi pada penyimpanan data, maka daya tampung ini sangat diperlukan untuk dikembangkan [11][12]lagi karena kita mengetahui bahwa saat ini kita dibatasi oleh *drive* yang dapat kita pakai ataupun limit penggunaan data (*Bandwidth*) yang disediakan oleh jaringan.

Pada metode *2LSB*, 2 *bit* pada akhir dari tiap 8 *bit* data *file* media diganti dengan 2 *bit* data *plaintext* dari informasi yang akan disembunyikan[13]. Metode ini dapat digunakanan, akan tetapi daya tampung informasi yang akan disembunyikan dapat dimaksimalkan [2]lagi, dengan cara meningkatkan *byte* penampungan informasi sebanyak 3 *bit* atau dikenal dengan metode *3LSB* [14].

Penelitian ini bertujuan untuk menerapkan metode *3LSB* pada *file* media dan membandingkan efektifitasnya dalam menyembu-nyikan informasi dengan metode *2LSB*. Permasalahannya adalah bagaimana meningkatkan kapasitas nilai daya tampung informasi yang akan disembunyikan,

METODE PENELITIAN

Metode steganografi adalah sebuah cara pengamanan data dengan menyisipkan sebuah pesan pada media, media yang dapat digunakan dalam metode ini sangatlah beraneka ragam, seperti video, gambar, atau audio. Media yang digunakan dalam metode ini menggunakan media audio berformat WAV, metode ini memecah byte dari *chippertext* pesan rahasia dan menyisipkannya pada file media audio tersebut [15]. Salah satu metode yang sering digunakan untuk menyisipkan byte adalah *Least Significant Bit* (LSB) [16], karena proses penyisipannya mengubah bit terakhir dari byte media audio, seperti penelitian yang dilakukan oleh [17], mereka berhasil mengembangkan metode LSB ini menjadi 2LSB, hasil dari penelitian ini adalah media untuk menyimpan pesan rahasia lebih besar dari metode 1LSB, dan kualitas dari audio lebih dari 30 dB, sehingga tidak menimbulkan noise.

Berdasarkan beberapa artikel pendahuluan tersebut memungkinkan bahwa metode 2LSB ini dapat dikembangkan lagi menjadi 3LSB. Oleh karena itu pada penelirian ini dikembangkan dari 2LSB menjadi 3LSB dengan tujuan mendapat daya tampung dari metode ini lebih besar dari metode sebelumnya dan tidak mengurangi kualitas dari Audio.

A. Solusi

Metode yang di terapkan dalam penelitian ini adalah metode 3LSB, metode ini mengambil 1 byte dari pesan dan membaginya mejadi 3 bagian, yaitu 2 bit, 3 bit, dan 3 bit, lalu menyisipkan 3 bagian tersebut pada byte media audio dan ditambah jarak penyisipan antar byte agar tidak mendapatkan noise yang besar dari Audio hasil dari metode steganografi 3LSB. Proses pada metode ini digambarkan secara umum sebagai berikut:

01100010 0000011 00010110 0000110 01000100 00000001

Deretan biner diatas adalah biner dari media audio, dan akan disipkan biner dari pesan rahasia berikut ini 01100100**.** Deret biner pesan rahasia tersebut dibagi menjadi 3 bagian yaitu: 01, 100**,** dan 100 lalu disisipkan pada deret biner media audio dengan ditambahkan jarak, maka hasil dari penyisipan metode tersebut sebagi berikut:

01100001 0000011 00010100 0000110 01000100 00000001

Hasil dari penyisipan menggunakan metode 3LSB dengan menambah jarak 1 *byte*, berbeda jika menggunakan metode 2LSB, proses pembagian biner pesan rahasia dibagi menjadi 4 bagian, yaitu 01, 10, 01, dan 00, maka dapat ditarik rumus cepat untuk menghitung besar dari daya tampung pesan rahasia menggunakan Persamaan 1.

$$\boldsymbol{daya\ tampung} = \frac{\boldsymbol{byte\ media}}{\boldsymbol{n}} \quad (1)$$

Nilai n adalah nilai pembagi dari media, jika menggunakan 3LSB maka pembaginya adalah 3, sedangkan jika menggunakan 2LSB maka pembaginya adalah 4, dapat dipastikan bahwa daya tampung 3LSB lebih besar dari 2LSB. Dan untuk melihat perbandingan kualitas audio dapat dilakukan dengan cara membandingkan 2 metode tersebut dengan menggunakan metode *Peak Signal to Noise Ratio* (PSNR) dan melihat hasil angka desibel dari kedua audio tersebut, serta ditambah dengan melihat grafik dari frekuensi audio kita dapat melihat seberapa besar perbedaan antara metode 2LSB dan 3LSB.

B. Eksperimen

Eksperimen yang akan dilakukan dalam penelitian ini adalah : Menganalisa besar media, besar pesan rahasia, dan besar daya tampung media. Menerapkan Proses enkripsi menggunakan metode *AES*. Menerapkan metode *stegano grafi* 2*LSB* dan 3*LSB* terhadap informasi yang sudah di enkripsi. Membandingkan besar daya tampung media antara metode 2*LSB* dan 3*LSB*. Membandingkan kualitas

suara berdasarkan metode *PSNR* dengan melihat nilai desibel antara metode 2*LSB* dan 3*LSB*. Mengambil data daya tampung dari perbandingan 2 *file* media yang berbeda yaitu "alone.wav" dan "starwars.wav".

1) Menghitung kapasitas penyimpanan

Kapasitas penyisipan pesan rahasia pada dasarnya mengikuti ekstensi dari *file* audio media yang akan disisipi. Setiap *file* ekstensi memiliki panjang *header* yang berbeda-beda, *Byte header* adalah bagian paling penting dari *file*, jika terdapat perubahan *byte* pada deretan *byte* header ini, maka *file* audio tersebut akan rusak. Oleh karena itu *file* yang akan disisipkan berada pada deretan *byte* data. Skema deretan *byte* pada *file* berformat *wav* adalah 45 *byte header* yang berada pada *index* 0 sampai 44, dan sisanya adalah deretan *byte* data.

Pada penelitian ini penyisipan dilakukan dengan memberikan *space* kosong sebanyak 5 *byte* dari header, sehingga penyisipan dimulai dari *index* ke 50.

$$\boldsymbol{daya\ tampung = byte\ media - byte\ header - byte\ stegano - 5} \quad (2)$$

Header Steganografi membutuhkan 165 *byte*, untuk menyimpan data metode yang digunakan dalam proses *encrypt*, Setelah daya tampung media diketahui, selanjutnya dapat dihitung *byte* yang dapat disisipi dengan rumus persamaan 3.

$$\boldsymbol{Maksimal\ penyisipan = \frac{Daya\ tampung}{(jarak + 1)xmetode}} \quad (3)$$

Jarak disini adalah nilai *space* kosong antar *byte* saat penyisipan, sedangkan untuk nilai metode berbeda sesuai dengan metode apa yang digunakan, jika menggunakan metode 2*LSB* maka nilainya 4, dan nilainya 3 saat menggunakan metode 3*LSB*. Nilai tersebut didapat dari pembagian *byte* saat proses penyisipan, 1 *byte* sama dengan 8 *bit*, untuk metode 2*LSB* maka diambil 2 *bit* tiap penyisipan, jadi 1 *byte* itu akan habis jika sudah terambil sebanyak 4 kali, sedangkan untuk 3*LSB* diambil sebanyak 3 *bit* tiap penyisipan, maka akan habis jika sudah terambil sebanyak 3 kali.

2) Menghitung kapasistas PSNR

Pengukuran *noise* pada *stego* audio dilakukan menggunakan perhitungan untuk *Peak Signal to Noise Ratio* (*PSNR*), pengukuran *PSNR* ini memakai rumus persamaan 2.

$$PNSR = 10.log_{10}\left(\frac{p_1^2}{p_1^2 + p_0^2 - 2P_1P_2}\right) \quad (4)$$

Dimana P1 adalah kekuatan sinyal audio setelah disisipkan pesan dan P0 adalah kekuatan sinyal audio awal. Contoh perhitungan *PSNR* adalah sebagai berikut:

$P_0 = 56.65$
$P_1 = 54.25$
$PNSR = 10.log_{10}\left(\frac{54.25^2}{54.25^2 + 56.65^2 - 2\ x\ 54.25x56.65}\right)$
$PNSR = 10.log_{10}(510.9484)$
$PNSR = 27.08377$

Dari contoh perhitungan *PSNR*, didapatkan hasil dari perubahan suara setelah disisipi pesan sebesar 27.08377 *dB*

HASIL DAN PEMBAHASAN

Data yang akan diamankan adalah "HALO SAYA ILHAM AKBAR" menggunakan metode steganografi 3LSB dengan jarak antar byte adalah 2 byte, dan kunci kriptografi "123456", setelah dilakukan proses Analisa didapat hasil seperti gambar berikut:Font Teks untuk Seluruh Isi Dokumen.

Gambar 1 Hasil analisa aplikasi

Gambar 1 adalah hasil dari Analisa dari aplikasi, data yang dihasilkan adalah : *Byte* media: **4546052 *byte*** adalah besar *byte* dari media penampung. *Byte* pesan: **21 *byte*** adalah besar *byte* dari data yang akan kita amankan. *Byte Ciphertext* sebesar: **44 *byte*** adalah besar *byte* dari pesan rahasia setelah dilakukan proses *encrypt* dengan menggunakan metode kriptografi *AES*. Jarak *Byte* sebesar: **2 *byte*** adalah jarak antar *byte* penyisipan pada file media penampung. Kunci *Encrypt*: **123456** adalah kunci kriptografi *AES* untuk lebih meng-amankan data. Tipe *Encrypt*: **3*LSB*** adalah metode *steganografi* yang digunakan untuk melakukan proses pengamanan data. Daya Tampung Media: **505088 *byte*** adalah daya tampung yang dapat kita pakai pada *file* media ini, didapat dari perhitungan *byte* media, jarak antar *byte*, dan metode *steganografi* yang digunakan. Persentase daya tampung sebesar: **11,11%** adalah persentase perbandingan dari daya tampung media dibandingkan dengan besar dari media penampung.

1. Proses Decrypt Steganografi

Decrypt Steganografi melakukan proses decrypt aplikasi melalui beberapa tahap proses, tahapan proses *decrypt* adalah: Pengecekan file adalah proses aplikasi untuk melakukan pengecekan file wav apakah file yang masukkan adalah hasil dari proses steganografi atau bukan, jika file tersebut hasil dari steganografi maka akan dilanjutkan pada tahap berikutnya, jika bukan maka proses akan terhenti. Proses analisa file adalah proses aplikasi untuk membaca jenis metode apa yang digunakan saat encrypt steganografi, dalam tahap ini yang dibaca adalah

jarak antar byte dan metode 2LSB atau 3LSB steganografi. Proses *decrypt steganografi* adalah proses aplikasi untuk mengambil *biner* yang telah disisipkan pada deretan byte pada media, sesuai dengan metode dan jarak yang telah dianalisa pada tahap sebelumnya.

Proses *decrypt* kriptografi adalah proses aplikasi untuk mengubah deretan byte array *chipper text* dari hasil *encrypt* kriptografi AES menjadi deretan *byte array* plain text menggunakan key *decrypt* yang diinputkan oleh pengguna, Proses *decrypt* kriptografi adalah proses aplikasi untuk mengubah deretan *byte array chipper text* dari hasil *encrypt* kriptografi AES menjadi deretan *byte array plain text* menggunakan *key decrypt* yang diinput oleh penggunan, jika *key decrypt* yang dimasukkan pengguna sesuai dengan kunci yang dimasukkan saat proses *encrypt* steganografi, maka akan keluar hasil *decrypt* steganografi sesuai dengan pesan rahasia yang diinputkan pengguna, dan jika key *decrypt* salah maka *byte array chipper text* tidak berhasil di *decrypt* menjadi plain *text*. Proses menampilkan hasil adalah proses aplikasi untuk menampilkan hasil *decrypt* pada memo text.

2. Perbandingan daya tampung

Setelah melakukan beberapa proses analisa dengan menggunakan data yang sama seperti Gambar 2, dengan menggunakan beberapa metode serta jarak antar *byte*, maka dapat dibuat sebuah tabel untuk melihat perbedaan antara metode 2*LSB* dan 3*LSB*, seperti berikut:

Tabel 1. Perbandingan daya tampung

Jarak	Konvensional 2LSB	Diusulkan 3LSB	Δ Perubahan
0	25,00%	33.33%	8.33%
1	12.50%	16.67%	4.17%
2	8.33%	11.11%	2.78%
3	6.25%	8.33%	2.08%
4	5.00%	6.67%	1.67%
5	4.17%	5.56%	1.39%
6	3.57%	4.76%	1.19%
7	3.12%	4.17%	1.05%
8	2.78%	3.70%	0.92%
9	2.50%	3.33%	0.83%
10	2.27%	3.03%	0.76%

Berdasarkan Tabel 1 dapat dilihat perbedaan daya tampung antara metode *steganografi* 2*LSB* dan 3*LSB*, pada metode 3*LSB* daya tampung yang dihasilkan lebih besar dari metode 2*LSB* sebesar 2.21% diambil dari rata-rata persentase perubahan.

Berikut ini adalah analisa dari perbandingan ukuran *file* media dengan ukuran yang *file* yang berbeda:

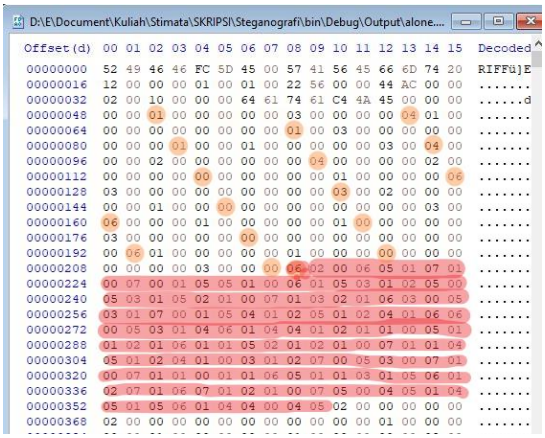
Tabel 2 Perbandingan ukuran media

Jarak	Ukuran *Byte* Media	
	4.546.052 *byte*	2.646.044 *byte*
0	1515274 *byte*	881943 *byte*
1	757634 *byte*	440972 *byte*
2	505088 *byte*	350532 *byte*
3	378815 *byte*	293981 *byte*
4	303051 *byte*	176389 *byte*
5	252542 *byte*	146990 *byte*
6	216463 *byte*	125992 *byte*
7	189405 *byte*	110243 *byte*
8	168359 *byte*	97994 *byte*
9	151523 *byte*	88194 *byte*
10	137748 *byte*	80177 *byte*

Dari tabel 2 tabel perbandingan ukuran media didapatkan hasil bahwa untuk persentase daya tampung ternyata sama meskipun ukuran media berbeda-beda, akan tetapi berbeda pada ukuran yang dapat disisipkan yaitu semakin besar ukuran *file* media maka semakin besar juga ukuran *byte* yang dapat disisipkan.

3. Perbandingan Byte Stego Audio

Pada deretan *byte* media terdapat blok-blok yang akan disisipkan *header* dari *steganografi* dan deretan *byte* yang akan disisipkan pesan rahasia, Blok yang berwarna hijau adalah blok yang akan disisipkan *header*, sedangkan yang berwarna biru adalah blok yang akan disisipkan *byte* dari pesan.



Gambar 2 Hexadecimal byte stego audio

Gambar 3 adalah gambar *hexa-decimal byte* dari media audio setelah dilakukan proses *steganografi*, blok dengan warna oranye adalah blok *header* untuk *steganografi* dan blok warna merah adalah deretan *byte* dari isi pesan rahasia.

Blok *header* seperti Gambar 3, teknik penyisipan *steganografi* dimulai dari *index byte* ke 50 karena blok *index* 0 sampai dengan 45 adalah *index header* dari *file* media *wav*, jika terdapat perubahan pada blok tersebut maka akan merusak *file* media, dan 5 *index byte* setelahnya adalah *space* kosong untuk penyisipan data rahasia.

Blok warna merah pada Gambar 3 adalah blok pesan rahasia, Pada blok ini *byte array* dari *chipper text* akan disisipkan, teknik penyisipan ini dimulai dari *index* awal ke 206 dan selanjutnya diisi sesuai dengan jarak antar penyisipan *byte*, pada percobaan ini menggunakan jarak penyisipan 0 *byte*, maka tidak ada *space* kosong antara *byte* satu dengan yang lainnya.

4. Perbandingan frekuensi metode 2LSB dan 3LSB

Perbandingan frekuensi antara metode 2*LSB* dan 3*LSB* dapat dilihat menggunakan aplikasi *audacity*, Grafik sampel frekuensi dari detik ke 1.6690 sampai 1.67 atau 2 gelombang frekuensi suara yang diambil dari aplikasi *audacity*.

Perhitungan yang dilakukan disini adalah mencari nilai perubahan yang terjadi pada frekuensi suara pada 2 metode tersebut, nilai frekuensi pada *audacity* antara 1 sampai -1,

Berdasarkan dua perbedaan frekuensi diatas dapat ditarik sebuah tabel kesimpulan dari perbedaan antara 2 metode tersebut seperti ditunjukkan pada Tabel 3.

Tabel 3 Perbedaan frekuensi

Detik	2*LSB*	3*LSB*	Δ Perubahan
1.6690	-0.15	-0.19	0.04
1.66908	-0.12	-0.13	0.01
1.66911	-0.08	-0.09	0.01
1.66916	-0.06	-0.04	0.02
1.66921	-0.01	-0.01	0
1.66925	0.01	0.01	0
1.66929	0.04	0.035	0.05
1.66935	0.05	0.01	0.04
1.66938	-0.015	-0.015	0
1.66944	-0.06	-0.04	0.02
1.66948	-0.05	-0.01	0.04
1.66952	-0.01	-0.015	0.05
1.66958	-0.015	-0.02	0.05
1.66961	-0.012	-0.013	0.01
1.66966	0.04	0.04	0
1.66970	0.1	0.07	0.06
1.66974	0.16	0.15	0.01
1.66980	0.19	0.2	0.01
1.66985	0.193	0.22	0.027
1.66988	0.14	0.13	0.01
1.66990	0.06	0.08	0.02
1.66998	0.04	0.01	0.03
1.67	0.01	0.02	0.01
Rata – Rata perubahan			0.022478261

Dari tabel 3 tentang perbedaan frekuensi metode 2*LSB* dan 3*LSB*, dapat ditarik data perubahan frekuensi sekitar 0 sampai 0.05 dan rata-rata dari detik 1.6690 sampai 1.67 adalah 0.022478261 frekuensi, dari tabel tersebut dapat dilihat perubahan frekuensi yang dihasilkan pada 3*LSB* tidak terlalu besar, sehingga pengaruh terhadap nada suara tidak akan terlalu berbeda dengan metode 2*LSB*.

5. Perhitungan kualitas suara

Pada saat proses penyisipan data terhadap file media audio maka akan menghasilkan file audio yang memiliki *noise*, *noise* tersebut dihasilkan dari adanya perubahan nilai *byte* yang terjadi pada *file* media.

Noise yang terjadi pada audio ini dapat diukur dengan menggunakan *Peak Signal to Noise Ratio* (PSNR) dengan menghitung nilai-nilai kekuatan *signal stego* audio yang didapat dari hasil *record* aplikasi *Spectrum Plus SC*, Berikut ini adalah tabel perbandingan hasil uji coba perhitungan yang dilakukan pada *stego* audio 2*LSB* dan 3*LSB* ditunjukkan pada Tabel 4.

Tabel 4 Perbandingan nilai PSNR

Jarak	Metode		Δ Perubahan
	Konvensional (2LSB)	Modern (3LSB)	
0	63.63151465	61.87586618	1.755648469
1	60.27111237	59.73526764	0.535844729
2	59.20086165	58.64711687	0.553744773
3	59.34338535	58.56220099	0.78118436
4	58.18765172	57.75748039	0.430171325
5	56.72732399	56.70312654	0.024197451
6	57.52180733	57.15193683	0.369870498
7	56.23034404	56.22809907	0.002244966
8	57.04078216	56.70408223	0.336699935
9	55.85497282	55.86309478	0.008121956
10	56.66478712	56.34951916	0.315267959
Rata-rata	58.24314029	57.77979915	0.464817856

Dari tabel 4 perbandingan nilai PSNR, nilai-nilai perubahan yang terjadi pada metode modern (3*LSB*) dari jarak penyisipan 0 sampai 10 tidak mengalami perubahan nilai desibel *(db)* yang signifikan terhadap nilai *db* pada metode konvensional (2*LSB*), dan dengan mendapat nilai rata-rata perubahan desibel sebesar 0.464817856 *dB* maka kualitas suara pada metode modern tidak terlalu jauh berbeda dengan metode konvensional.

6. Hasil Perhitungan

Hasil dari pengujian yang telah dilakukan terhadap *stego* audio oleh aplikasi *steganografi* sebagai berikut: Persentase daya tampung sebesar 0,76% sampai 8,33% dan nilai rata-rata perubahan sebesar 2,21%. Perubahan frekuensi yang terjadi pada metode modern tidak terlalu besar antara 0 sampai 0.05, dan rata-rata dari perubahan sebesar 0.022478261. Nilai desibel perubahan yang terjadi pada metode modern tidak terlalu besar yaitu 0.464817856 *dB*, dan perubahan kualitas suara juga tidak terlalu jauh berbeda dengan metode konvensional, dari nilai rata-rata desibel keseluruhan pada metode modern sebesar 57.77979915 *dB.* Daya tampung yang dapat disisipkan berbanding lurus dengan ukuran *byte* media, jika semakin besar ukuran *file* media maka semakin besar juga ukuran *byte* yang dapat disisipkan.

KESIMPULAN

Pesan yang disisipkan pada file media dapat kembali 100% seperti semula, hasil ini didapat dari 20 kali percobaan menyimpan pesan "HALO SAYA ILHAM AKBAR" pada file media audio wav sebesar 4,33MB. Rata-rata kenaikan daya tampung terhadap jarak penyisipan sebesar 2.21%. Perubahan gelombang suara sebesar 0.022478261 dari metode konvensional, akibatnya perubahan kualitas suara tidak akan telalu beda jauh. Rata-rata nilai desibel yang didapatkan sebesar 57.77979915 dB, sehingga noise pada stego audio ini tidak dapat didengar oleh telinga manusia, dan perubahan desibel pada metode modern sebesar 0.464817856 dB dari metode konvensional.

REFERENSI

[1.] R. Maulana, "Steganografi Berbasis Citra Menggunakan Prosesor ARM7TDMI dan Algoritma LSB," J. ElekFormatika, vol. 1, no. 1, pp. 0–7, 2019.

[2.] S. Saidah, N. Ibrahim, And M. H. Widianto, "Pengamanan Pesan pada Steganografi Citra dengan Teknik Penyisipan Spread Spectrum," ELKOMIKA J. Tek. Energi Elektr.

Tek. Telekomun. Tek. Elektron., vol. 7, no. 3, p. 544, 2019, doi: 10.26760/elkomika.v7i3.544.

[3.] A. Ardiansyah and M. Kurniasih, "Penyembunyian Pesan Rahasia Pada Citra Digital Dengan Teknik Steganograpi Menggunakan Metode Least Significant Bit," Respati, vol. 13, no. 3, pp. 96–101, 2018, doi: 10.35842/jtir.v13i3.258.

[4.] E. S. Astuti, B. Prihadmantyo Dan M. E. Apriyani, Implementasi Algorit-Ma Kriptografi Rc4 Dan Metode Steganografi Audio 2lsb Pada Sistem Keamanan Informasi, Pp. 81-87, 2017.

[5.] Y. Salim, "Implementasi Teknik Steganografi Menggunakan Algoritma Transposisi Columnar," Respati, vol. 14, no. 2, pp. 102–107, 2019, doi: 10.35842/jtir.v14i2.294.

[6.] A. E. Minarno, "Analisa Perbandingan Lsb Steganografi Antara Shifting Dan Random Color," J. Repos., vol. 3, no. 2, pp. 2–5, 2021, doi: 10.22219/repositor.v3i2.1202.

[7.] N. Nurmaesah, T. Lestari, and A. Retno Mariana, "Aplikasi Steganografi Untuk Menyisipkan Pesan Dalam Media Image," Technol. Accept. Model, vol. 8, no. 1, pp. 13–17, 2017.

[8.] O. Soleh, F. Alfiah, and B. Yusuf, "Perancangan Aplikasi Steganografi Dengan Teknik LSB dan AlgoritmaRC4 & Base64 Encoding," Technomedia J., vol. 3, no. 1, pp. 1–15, 2018, doi: 10.33050/tmj.v3i1.493.

[9.] Z. Hasibuan, Perancangan Aplika-Si Steganografi Dengan Me-Tode Least Significant Bit (Lsb) Untuk Data Terenkripsi Dari Algoritma Hill Cipher, P. 5, 2014.

[10.] S. Sembiring, Perancangan Aplikasi Steganografi Untuk Menyisipkan Pesan Teks Pada Gambar Dengan Metode End Of File, 2013.

[11.] S. Hotlan Sitorus, U. Ristian, J. Rekayasa Sistem Komputer, and F. H. MIPA Universitas Tanjungpura Jalan Hadari Nawawi Pontianak, "Perbandingan Steganografi Metode Least Significant Bit+3 (Lsb+3) Dengan Most Significant Bit (Msb)," Coding J. Komput. dan Apl., vol. 08, no. 01, pp. 77–85, 2020.

[12.] E. S. Astuti, M. E. Apriyani, and M. R. Qulyubi, "Pengembangan Sistem Keamanan Informasi Menggunakan Metode Kriptografi 3Des Dan Steganografi Random Byte Position Encoding Pada Audio," J. Inform. Polinema, vol. 4, no. 2, p. 109, 2018, doi: 10.33795/jip.v4i2.154.

[13.] B. K. S Y, D. Puspitaningrum Dan F. F. Coastera, Perancangan Dan Pembuatan Aplikasi Stegano-Grafi Pesan Teks Pada Audio Digital Dengan Metode Least Significant Bit, Pp. 288-289, 2017.

[14.] Jatrya, S. H. Sitorus Dan U. Ristian, "Perbandingan Steganografi Metode Least Significant Bit+3 (Lsb+3) Dengan Most Significant Bit (Msb)," Pp. 78-79, 2020.

[15.] A. F. Marisman Dan A. Hidayati, "The Development Of A Crypto-Graphy Application With Caesar Cipher And Advance Encryption Standard(Aes) For Text File," Pp. 214-216, 2015.

[16.] T. I. Widyawan, Pengamanan Pesan Steganografi Dengan Metode Lsb Berlapis Enkripsi, P. 17, 2018.

[17.] M. M. A. Syaifullah, R. Dan D. S. B. Utomo, Implementasi Steganografi Pesan Text Ke Dalam Audio Dengan Metode Spread Spectrum, P. 8, 2018.