

STEGANOGRAFI PENGAMANAN DATA TEKS MENGUNAKAN AUDIO WAV DENGAN METODE LSB

STEGANOGRAPHY TEXT DATA SECURITY USING AUDIO WAV WITH LSB METHOD

Deny Adhar ¹ Andrian Syahputra ² Raden Aris Sugianto ³ Rini Oktari Batubara ⁴ Andi Sanjaya ⁵
Ahmad Sabir ⁶

*Fakultas Teknik dan Ilmu Komputer*¹²³⁴⁵,

*Fakultas Psikologi*⁶

*Universitas Potensi Utama*¹²⁴

*Universitas Muhammadiyah Sumatera Utara*³

*Universitas Nusa Mandiri*⁵

*Universitas Mercu Buana*⁶

adhardeny@gmail.com, andriansyahputra4@gmail.com, ra.sugianto@umsu.ac.id,
rini.admmedan@gmail.com, andi.sj7@gmail.com, ahmad.sabir@mercubuana.ac.id

Abstrak

Maraknya kasus pencurian data digital ini mulai menyedot perhatian publik termasuk para pegiat ilmu forensika digital yang tergerak untuk menemukan cara untuk mengamankan data digital dengan efisien dan cepat dari pihak-pihak yang tidak bertanggung jawab, salah satunya dengan menggunakan teknik steganografi. Metode ini akan di terapkan pada data teks yang akan dimasukkan kedalam media audio berformat wav. Salah satu cara untuk mengatasi situasi tersebut dengan menggunakan Steganografi, karena teknik ini dapat menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui. Steganografi dapat menyamarkan pesan ke dalam suatu media tanpa orang lain menyadari bahwa media tersebut telah disisipi suatu pesan, karena hasil keluaran steganografi berupa data yang memiliki bentuk persepsi yang sama dengan data aslinya apabila dilihat menggunakan indera manusia. Banyak metode yang ditemukan untuk melakukan audio steganografi, salah satunya dengan menggunakan algoritma Least Significant Bit (LSB)

Kata kunci: Steganografi, Least Significant Bit (LSB), Keamanan data teks

Abstrak

The rise of cases of digital data theft has begun to attract public attention, including digital forensic science activists who are moved to find ways to secure digital data efficiently and quickly from irresponsible parties, one of which is by using steganography techniques. This method will be applied to text data that will be entered into wav format audio media. One way to overcome this situation is to use Steganography, because this technique can hide a secret message in another message so that the existence of the secret message cannot be known. Steganography can disguise messages into a medium without other people realizing that the media has been inserted a message, because the output of steganography is in the form of data that has the same form of perception as the original data when viewed using the human senses. Many methods have been found to perform audio steganography, one of which is by using the Least Significant Bit (LSB) algorithm.

Keywords : Steganography, Least Significant Bit (LSB), Text data security

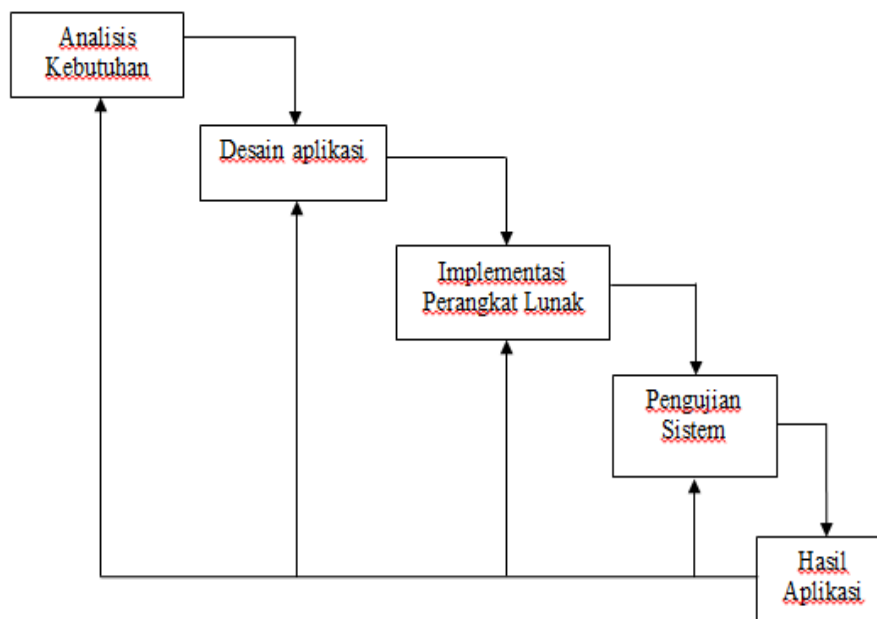
I. PENDAHULUAN

Melindungi informasi termasuk dokumen multimedia merupakan suatu kebutuhan utama dalam era keterbukaan informasi seperti saat ini. Konten multimedia dalam berbagai bentuk seperti teks, gambar, audio, dan video mudah sekali menyebar. Seiring dengan semakin meluasnya penggunaan jaringan internet, pengiriman informasi semakin rentan terhadap penyadapan yang dapat mengubah autentifikasi dan integritas data. Seringkali seseorang yang hendak mengirim pesan kepada orang lain, tidak ingin isi pesan tersebut diketahui oleh orang lain. Biasanya isi pesan tersebut bersifat sangat rahasia atau pribadi, yang hanya boleh diketahui antara pihak pengirim dan pihak penerima pesan. Oleh karena itu, diperlukan suatu sistem pengamanan data yang dapat melindungi pesan yang bersifat pribadi dan rahasia agar sampai ke tangan orang yang berhak menerima pesan tersebut.

Maraknya kasus pencurian data digital ini mulai menyedot perhatian publik termasuk para pegiat ilmu forensika digital yang tergerak untuk menemukan cara untuk mengamankan data digital dengan efisien dan cepat dari pihak-pihak yang tidak bertanggung jawab, salah satunya dengan menggunakan teknik steganografi. Salah satu cara untuk mengatasi situasi tersebut dengan menggunakan Steganografi, karena teknik ini dapat menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui. Steganografi dapat menyamarkan pesan ke dalam suatu media tanpa orang lain menyadari bahwa media tersebut telah disisipi suatu pesan, karena hasil keluaran steganografi berupa data yang memiliki bentuk persepsi yang sama dengan data aslinya apabila dilihat menggunakan indera manusia. Banyak metode yang ditemukan untuk melakukan audio steganografi, salah satunya dengan menggunakan algoritma *Least Significant Bit* (LSB). Algoritma *Least Significant Bit* menjadi metode yang paling populer dalam audio steganografi. Karena algoritma ini bekerja dengan cara memodifikasi bit-bit terakhir dalam beberapa *byte* file audio untuk menyembunyikan urutan *byte* yang mengandung data rahasia. LSB merupakan teknik yang paling simpel dan efektif jika dibandingkan dengan metode lainnya dan tidak menyebabkan perubahan kualitas yang signifikan terhadap audio file yang menjadi cover object tersebut

II. METODE PENELITIAN

Analisis kebutuhan sistem. Perancangan waterfall tersebut dapat dilihat pada gambar 1.



Gambar 1. Diagram Waterfall

A. Metode Least Significant Bit

Metode LSB Mengubah bit *LSB* hanya mengubah nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya → tidak berpengaruh terhadap persepsi visual/auditori. Untuk memperkuat teknik penyembunyian data, bit-bit data rahasia tidak digunakan mengganti byte-byte yang berurutan, namun dipilih susunan byte secara acak. Pembangkit bilangan acak-semu (PRNG: pseudo-random number generator) digunakan untuk membangkitkan bilangan acak. Umpan (seed) untuk bilangan acak berlaku sebagai kunci (stego-key). Misalnya jika terdapat 50 byte dan 6 bit data yang akan disembunyikan, maka byte yang diganti bit LSB-nya dipilih secara acak, misalkan byte nomor 36, 5, 21, 10, 18, 49.

Tabel 1. Tabel ASCII

Binary	Oct	Dec	Hex	Glyph	Binary	Oct	Dec	Hex	Glyph	Binary	Oct	Dec	Hex	Glyph
010 0000	040	32	20	SP	100 0000	100	64	40	@	110 0000	140	96	60	`
010 0001	041	33	21	!	100 0001	101	65	41	A	110 0001	141	97	61	a
010 0010	042	34	22	"	100 0010	102	66	42	B	110 0010	142	98	62	b
010 0011	043	35	23	#	100 0011	103	67	43	C	110 0011	143	99	63	c
010 0100	044	36	24	\$	100 0100	104	68	44	D	110 0100	144	100	64	d
010 0101	045	37	25	%	100 0101	105	69	45	E	110 0101	145	101	65	e
010 0110	046	38	26	&	100 0110	106	70	46	F	110 0110	146	102	66	f
010 0111	047	39	27	'	100 0111	107	71	47	G	110 0111	147	103	67	g
010 1000	050	40	28	(	100 1000	110	72	48	H	110 1000	150	104	68	h
010 1001	051	41	29	)	100 1001	111	73	49	I	110 1001	151	105	69	i
010 1010	052	42	2A	*	100 1010	112	74	4A	J	110 1010	152	106	6A	j
010 1011	053	43	2B	+	100 1011	113	75	4B	K	110 1011	153	107	6B	k
010 1100	054	44	2C	,	100 1100	114	76	4C	L	110 1100	154	108	6C	l
010 1101	055	45	2D	-	100 1101	115	77	4D	M	110 1101	155	109	6D	m
010 1110	056	46	2E	.	100 1110	116	78	4E	N	110 1110	156	110	6E	n
010 1111	057	47	2F	/	100 1111	117	79	4F	O	110 1111	157	111	6F	o
011 0000	060	48	30	0	101 0000	120	80	50	P	111 0000	160	112	70	p
011 0001	061	49	31	1	101 0001	121	81	51	Q	111 0001	161	113	71	q
011 0010	062	50	32	2	101 0010	122	82	52	R	111 0010	162	114	72	r
011 0011	063	51	33	3	101 0011	123	83	53	S	111 0011	163	115	73	s
011 0100	064	52	34	4	101 0100	124	84	54	T	111 0100	164	116	74	t
011 0101	065	53	35	5	101 0101	125	85	55	U	111 0101	165	117	75	u
011 0110	066	54	36	6	101 0110	126	86	56	V	111 0110	166	118	76	v
011 0111	067	55	37	7	101 0111	127	87	57	W	111 0111	167	119	77	w
011 1000	070	56	38	8	101 1000	130	88	58	X	111 1000	170	120	78	x
011 1001	071	57	39	9	101 1001	131	89	59	Y	111 1001	171	121	79	y
011 1010	072	58	3A	:	101 1010	132	90	5A	Z	111 1010	172	122	7A	z
011 1011	073	59	3B	;	101 1011	133	91	5B	[	111 1011	173	123	7B	{
011 1100	074	60	3C	<	101 1100	134	92	5C	\	111 1100	174	124	7C	
011 1101	075	61	3D	=	101 1101	135	93	5D	]	111 1101	175	125	7D	}
011 1110	076	62	3E	>	101 1110	136	94	5E	^	111 1110	176	126	7E	~
011 1111	077	63	3F	?	101 1111	137	95	5F	_					

B. Peak Signal to Noise Ratio

PSNR adalah sebuah istilah dalam bidang teknik yang menyatakan perbandingan antara kekuatan sinyal maksimum yang mungkin dari suatu sinyal digital dengan kekuatan derau yang mempengaruhi kebenaran sinyal tersebut. Sama halnya dengan SNR hanya saja penggunaan PSNR digunakan pada suatu citra. Nilai PSNR dikatakan memiliki kemiripan yang tinggi jika nilai PSNR lebih besar atau sama dengan 40dB [8]. Perhitungan PSNR dilakukan dengan menghitung nilai MSE pertama kali. Mean Square Error (MSE) dihitung untuk seluruh pixel dalam citra. (Mohammad Iqbal Maulana, dkk : 2018)

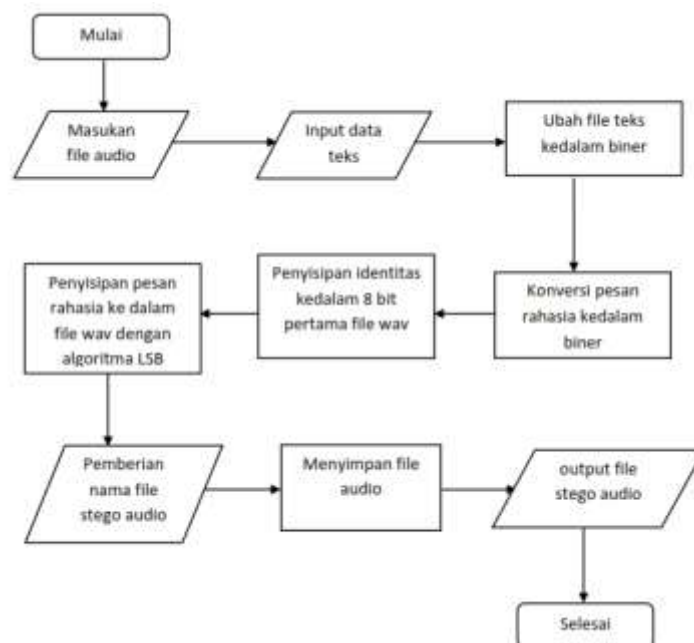
$$MSE = \frac{\sum_{i=1, j=1}^{i=n, j=m} (f(i, j) - F(i, j))^2}{M \times N}$$

$$PSNR = 10 \times \log_{10} \left(\frac{255^2}{MSE} \right)$$

Gambar 2. Rumus MSE dan PSNR

C. FLOW CHART

1. Flow chart Enkripsi

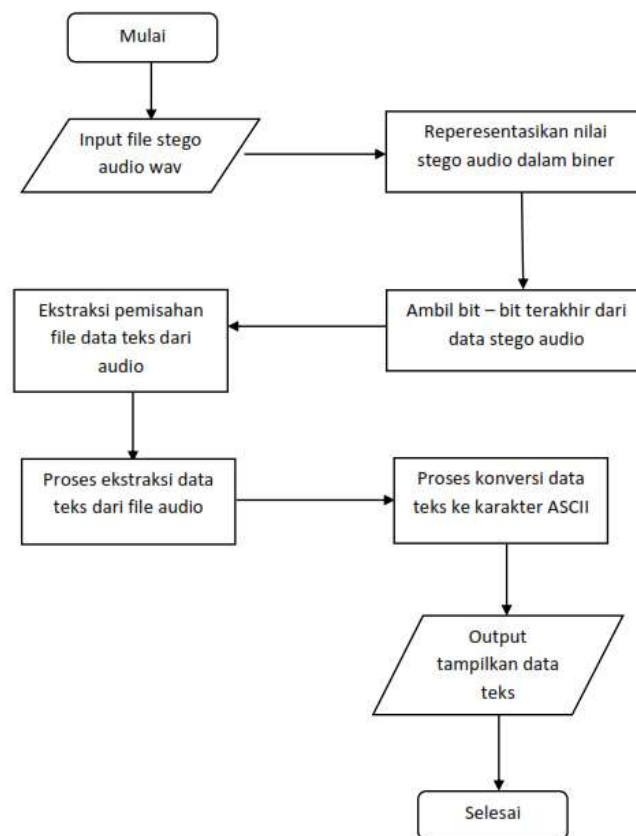


Gambar 3. Flowchart Enkripsi

Keterangan dari *Flowchart Enkripsi* di atas adalah ;

- Pertama masukan file audio wav
- Selanjutnya input data teks.
- Lalu ubah file data teks kedalam biner.
- Lalu dilakukan sebuah penyisipan identitas kedalam 8 bit pertama file wav.
- Setelah itu dilakukan penyisipan pesan rahasia kedalam file wav dengan menggunakan algoritma LSB.
- Selanjutnya pemberian nama file stego audio.
- Dan proses penyimpanan file audio.
- Output hasilnya berbentuk file stego audio.
- Selesai.

2. Flowchart Dekripsi



Gambar 4. Flowchart Dekripsi

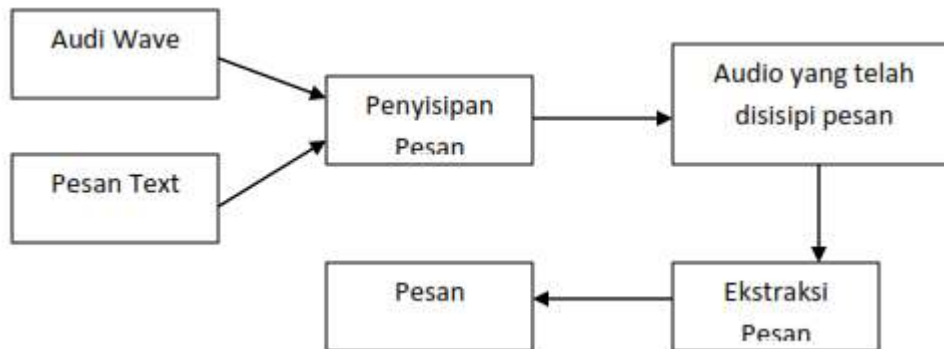
Keterangan dari *Flowchart Dekripsi* di atas adalah ;

- a. Pertama input file stego audio.
- b. Kemudian reperesentasikan nilai stego audio dalam biner
- c. Lalu ambil bit – bit terakhir dari data stego audio.
- d. Ekstraksi pemisahan file data teks dari audio.
- e. Selanjutnya proses ekstraksi data teks dari file audio.
- f. Proses konversi data teks ke karakter ASCII.
- g. Output akan menampilkan tampilan data teks.
- h. Selesai

III. HASIL DAN PEMBAHASAN

A. Blok Diagram Sistem

Pada sistem steganografi terdiri dari beberapa langkah yang dapat digambarkan menjadi blok diagram dengan model seperti Gambar berikut :



Gambar 5. Diagram Blok Sistem Secara Keseluruhan

Fungsi masing-masing bagian dalam diagram blok ini adalah sebagai berikut :

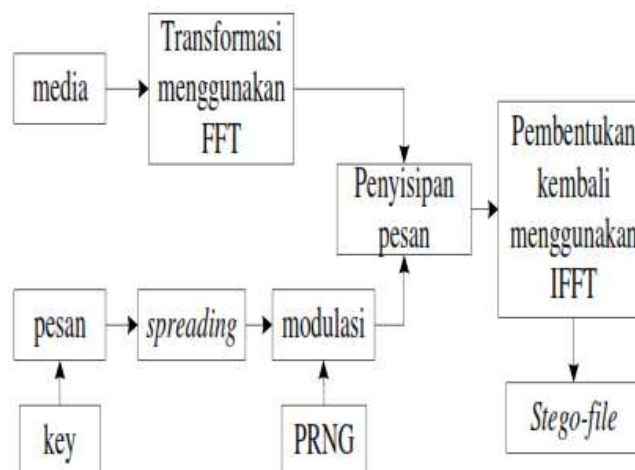
1. Pesan dan audio penampung pesan digunakan sebagai input sistem.
2. Melakukan processing penyisipan pesan kedalam audio.
3. Proses penyisipan pesan menghasilkan stego-object.
4. Melakukan proses ekstraksi pesan dari stego-image.

B. Perancangan Perangkat Lunak

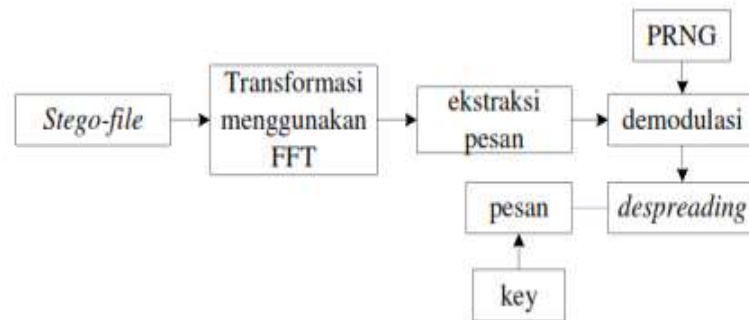
Pada bagian perancangan ini perangkat lunak yang akan dibuat menggunakan bahasa pemrograman Microsoft Visual Studio C#.NET 2012 dan sistem yang digunakan untuk membangun perangkat lunak ini dirancang dengan spesifikasi mampu melakukan hal-hal berikut :

1. Pesan dan Audio penampung pesan digunakan sebagai input sistem.
2. Melakukan proses penyisipan pesan kedalam audio.
3. Proses penyisipan pesan menghasilkan stego-object.
4. Melakukan proses ekstraksi pesan dari stego-object.

Sedangkan untuk detail desain aplikasi secara umum akan ditunjukkan pada gambar 6 dan 7.



Gambar 6. Rancangan Umum Proses Penyisipan Pesan.



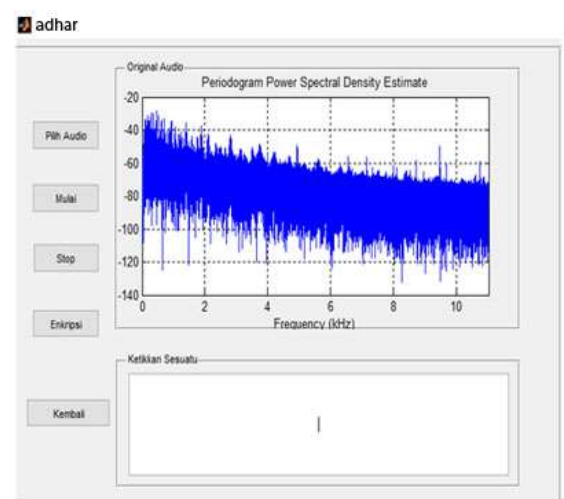
Gambar 7. Rancangan Umum Proses Ekstraksi Pesan

C. Tampilan Aplikasi

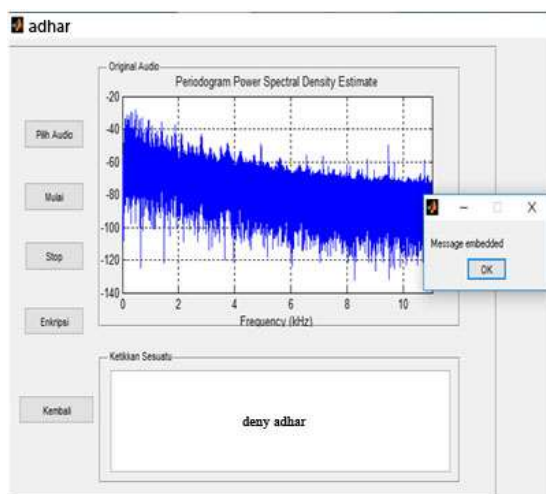
Berikut ini adalah tampilan Menu Utama



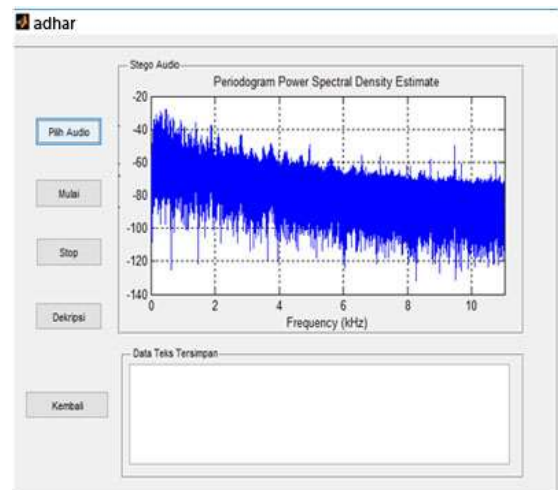
Gambar 8. Tampilan Halaman Menu Utama



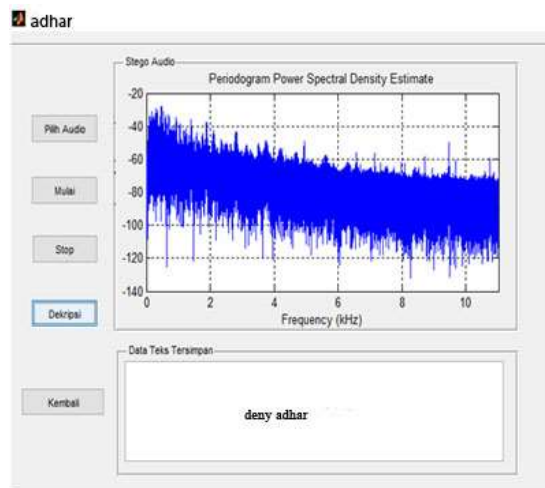
Gambar 9. Tampilan Visualisasi Sinyal Audio



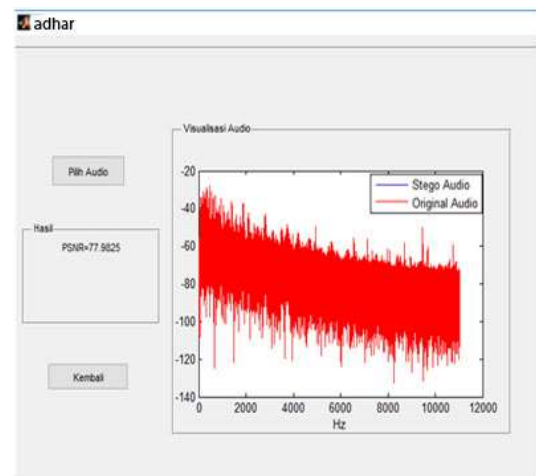
Gambar 10. Tampilan Proses Enkripsi



Gambar 11. Tampilan Visualisasi Sinyal Stego Audio



Gambar 12. Tampilan Sukses Dekripsi



Gambar 13. Tampilan Hasil Proses PSNR

D. Pengujian Perangkat Lunak

Tabel 2. Hasil Pengujian Perangkat Lunak.

Nama Audio	Size (bytes)	Sisip Pesan	Ekstraksi
Buih Jadi Permadani	20	berhasil	Berhasil
Mencari Alasan	30	berhasil	Berhasil
rindu	35	berhasil	Berhasil
Bring me to Life	46	berhasil	berhasil

Tabel 3. Hasil Pengujian Tingkat Keberhasilan Memainkan Audio Hasil Penyisipan.

Nama Audio yang disisipkan pesan	Hasil Play Audio
Buih Jadi Permadani	Berhasil
Mencari Alasan	Berhasil
rindu	Berhasil
Bring me to Life	Berhasil

Dari hasil pengujian, terbukti bahwa perangkat lunak yang sudah dibuat telah berhasil menjalankan proses penyisipan dan ekstraksi pesan dengan baik. Semua pesan berhasil disisipkan dan diekstraksi dengan baik.

E. Pengujian Kinerja Perangkat Lunak

Pengujian dilakukan dengan cara melihat seberapa lama waktu yang dibutuhkan untuk melakukan proses penyisipan dan juga proses ekstraksi pesan. Pengujian dilakukan dengan menggunakan ukuran pesan serta berkas audio yang berbeda-beda. Hasil pengujian dapat dilihat pada Tabel 4, 5 dan 6.

Tabel 4. Hasil Pengujian Waktu Proses Penyisipan pesan

No	Size	Nama Audio	Pesan	Waktu Proses (detik)
1	4.45 MB	Buih Jadi Permadani	Deny	27:02
2	10.2 MB	Mencari Alasan	adhar	32:06
3	12.5 MB	rindu	testing	37:04
4	17.4 MB	Bring me to life	Deny Adhar	42:06

Tabel 5. Hasil Pengujian Waktu Proses Ekstraksi

No	Size	Nama Audio	Pesan	Waktu Proses (detik)
1	4.45 MB	Buih Jadi Permadani	Deny	12:05
2	10.2 MB	Mencari Alasan	adhar	17:06
3	12.5 MB	rindu	testing	21:04
4	17.4 MB	Bring me to life	Deny Adhar	25:06

Tabel 5. Hasil Pengujian Kualitas Audio berdasar PSNR

No	Size	Durasi	Size Pesan (byte)	PSNR (dB)
1	10.2 MB	01:00 menit	20	41.75
2	10.2 MB	01:00 menit	30	40.55
3	10.2 MB	01:00 menit	35	40.06
4	10.2 MB	01:00 menit	46	38.02

IV. KESIMPULAN

Kesimpulan sebagai berikut :

- Dengan penerapan teknik steganografi menggunakan metode least significant bit dapat membantu untuk mengamankan data teks kedalam audio wav.
- Setelah menggunakan teknik steganografi terjadinya perubahan nama file audio setelah dienkripsi, kualitas dari kedua audio sebelum di enkripsi dan sesudah di enkripsi tidak mengalami perubahan, untuku kuran file audio sedikit mengalami perubahan pada ukuran audio.
- File audio yang sudah di enkripsi dapat didengarkan dengan baik seperti file audio asli.
- Nilai hasil dari audio akan dihitung menggunakan system rumus psnr setelah kedua audio dimasukan.

V. SARAN

Dalam perancangan Steganografi Pengamanan Data Teks Menggunakan Audio Wav Dengan Metode LSB, penulis sadar bahwa masih banyak kekurangan yang harus disempurnakan sehingga mencapai titik kesempurnaan. Penulis menyarankan untuk pengembangan Steganografi Pengamanan Data Teks Menggunakan Audio Wav Dengan Metode LSB ini sebagai berikut:

- a. Membuat aplikasi agar bias menggunakan audio berekstensi lain seperti mp3, aac, wma dan lain – lain dalam mengamankan data.
- b. Selain menyimpan data teks dikembangkan juga untuk menyisipkan gambar kedalam audio.
- c. Steganografi memiliki tingkat keamanan yang sangat baik selain menggunakan metode least significant bit, untuk mengembangkan aplikasi ini dapat menggunakan metode low bit codingI dalam teknik steganografi untuk menyisipkan pesan gambar kedalam audio wav.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Potensi Utama yang telah membantu penulis dalam menyelesaikan penelitian ini.

DAFTAR PUSTAKA

- [1] N. Q. Fitriyah and Y. Y. Prayudi, "Implementasi Steganografi Audio File Wav Dengan Metode Discrete Cosine Transform (Dct)," *Pros. SENSEI 2017*, vol. 1, no. 1, 2017.
- [2] M. I. Ukkas, R. Andrea, and A. B. P. Anggen, "Teknik Pengamanan Data Dengan Steganografi Metode End Of File (EOF) Dan Kriptografi Vernam Cipher," *Sebatik*, vol. 17, no. 1, pp. 20–26, 2017.
- [3] A. E. Setiawan, A. Pasaribu, and A. E. Setiawan, "Penerapan Steganografi Pada Citra Digital Menggunakan Metode Least Significant Bit (LSB) Kombinasi RC4 Berbasis Mobile Android," *Aisyah J. Informatics Electr. Eng.*, vol. 2, no. 1, pp. 18–28, 2020.
- [4] I. Santiko, "Implementasi Model Steganografi Dalam Mengelola Kerahasiaan Informasi Dengan Metode LSB (Least Significant Bit)."
- [5] L. B. Handoko and C. Umam, "PENYEMBUNYIAN PESAN MENGGUNAKAN STEGANOGRAFI DENGAN METODE LSB DAN ENKRIPSI KRITOGRAFI," 2019.
- [6] A. Hafiz, "Steganografi Berbasis Citra Digital Untuk Menyembunyikan Data Menggunakan Metode Least Significant Bit (LSB)," *J. Cendikia*, vol. 17, no. 1 April, pp. 194–198, 2019.
- [7] A. Lingga, "ANALISA IMPLEMENTASI APLIKASI KEAMANAN FILE AUDIO WAV DENGAN MENERAPKAN ALGORITMA BEAUFORT CIPHER DAN ROOT 13," *Pelita Inform. Inf. dan Inform.*, vol. 8, no. 1, pp. 372–379, 2019.
- [8] S. Saifuddin, A. R. Mido, and E. I. H. Ujianto, "Perancangan Aplikasi Steganografi Menggunakan Metode Discrete Cosine Transformation berbasis Android," *Progresif J. Ilm. Komput.*, vol. 16, no. 1, pp. 25–36, 2020.
- [9] A. Atina, "Aplikasi Matlab pada Teknologi Pencitraan Medis," *J. Penelit. Fis. dan Ter.*, vol. 1, no. 1, pp. 28–34, 2019.
- [10] M. A. R. H. Wahab, "IMPLEMENTASI MEKANISME KEAMANAN DATA DALAM BENTUK STEGANOGRAFI DENGAN METODE LEAST SIGNIFICANT BIT (LSB) PADA FILE AUDIO WAV," *JURISTEK*, vol. 5, no. 2, pp. 202–211, 2018.
- [11] A. M. A. Rizki, N. Ismail, and R. Mardiaty, "Integrasi Kriptografi Algoritma MARS dan Steganografi Metode Least Significant Bit (LSB) dengan Media File Berekstensi*. wav," *TELKA-Telekomunikasi, Elektron. Komputasi dan Kontrol*, vol. 3, no. 1, pp. 57–67, 2017.
- [12] A. Samsudin, A. Haryoko, and A. Nugroho, "STEGANOGRAPHY PADA FILE AUDIO MP3 UNTUK MENGAMANKAN DATA MENGGUNAKAN METODE LEAST SIGNIFICANT BIT (LSB)," *Pros. SNasPPM*, vol. 3, no. 1, pp. 335–340, 2018.
- [13] J. Manurung, "MENYEMBUNYIKAN FILE TEKS PADA COVER AUDIO WAV DENGAN MENGGUNAKAN METODE LSB," *J. Mantik Penusa*, vol. 20, no. 1, 2016.