Jurnal Teknik Informatika (JUTIF)
Vol. 5, No. 6, December 2024, pp. 1529-1537
DOI: https://doi.org/10.52436/1.jutif.2024.5.6.1793
p-ISSN: 2723-3863
e-ISSN: 2723-3871

IMPLEMENTATION OF LSB AND PLAYFAIR METHODS TO SECURE TEXT FILES INTO WAV AUDIO FILES

Arief Al Akbar[1], Muhammad Taufiq Sumadi[*2], Faldi[3]

[1,2,3]Informatics Engineering, Faculty of Science and Technology, Universitas Muhammadiyah Kalimantan Timur, Indonesia
Email: [2]mts653@umkt.ac.id

(Article received: January 26, 2024; Revision: April 06, 2024; published: December 29, 2024)

Abstract

In the rapidly evolving digital communication era, the demand for information security is escalating. Three main security techniques are required: cryptography, watermarking, and steganography. Despite cryptography and watermarking having detectability weaknesses, steganography emerges as a more reliable choice as it can conceal messages across various media without arousing suspicion. This article discusses the utilization of steganography, particularly the Least Significant Bit (LSB) technique, for embedding messages within audio wave files as the medium. In this research, the author combines steganography with encryption using the Playfair Cipher algorithm to enhance overall data confidentiality. Implementation results demonstrate that the combination of LSB and Playfair methods effectively conceals messages without compromising audio quality. Evaluation of stego quality using PSNR indicates that audio quality remains high after embedding secret messages, with PSNR exceeding 40 dB. Despite successful message extraction during decoding, the message content remains protected and requires decryption to be read. In conclusion, the use of steganography in audio wave files with a combination of Playfair Cipher encryption and LSB methods proves to be an effective approach in preserving privacy and data confidentiality during transmission.

Keywords: *Encryption, Least Significant Bit (LSB), Playfair Cipher, Steganography.*

IMPLEMENTASI METODE LSB DAN *PLAYFAIR* UNTUK MENGAMANKAN *FILE* TEKS KE DALAM *FILE* AUDIO WAV

Abstrak

Dalam era komunikasi digital yang semakin berkembang, permintaan akan keamanan informasi semakin meningkat. Tiga teknik keamanan utama yang diperlukan adalah kriptografi, *watermarking*, dan steganografi. Meskipun kriptografi dan *watermarking* memiliki kelemahan terdeteksi, steganografi menjadi pilihan yang lebih andal karena mampu menyembunyikan pesan dalam berbagai media tanpa menimbulkan kecurigaan. Artikel ini membahas penggunaan steganografi, khususnya teknik *Least Significant Bit* (LSB), untuk penyisipan pesan dalam *file* audio wave sebagai media. Dalam penelitian ini, penulis menggabungkan steganografi dengan enkripsi menggunakan algoritma *Playfair Cipher* untuk meningkatkan kerahasiaan data secara keseluruhan. Hasil implementasi menunjukkan bahwa kombinasi metode LSB dan *Playfair* mampu menyembunyikan pesan dengan baik tanpa merusak kualitas audio. Evaluasi kualitas stego menggunakan PSNR menunjukkan bahwa kualitas audio tetap tinggi setelah proses penyisipan pesan rahasia, dengan PSNR di atas 40 dB. Meskipun pesan berhasil diekstrak selama proses decoding, isi pesan tetap terlindungi dan memerlukan dekripsi untuk dibaca. Kesimpulannya, penggunaan steganografi dalam audio wave dengan kombinasi enkripsi *Playfair Cipher* dan metode LSB merupakan pendekatan yang efektif untuk menjaga privasi dan kerahasiaan data selama proses transmisi.

Kata kunci: *Encryption, Least Significant Bit (LSB), Playfair Cipher, Steganography.*

1. PENDAHULUAN

Perkembangan komunikasi digital melalui Internet telah meningkatkan permintaan akan tiga teknik keamanan: kriptografi, *watermarking*, dan steganografi. Dalam kriptografi konten pesan diubah dari teks biasa menjadi teks terenkripsi (*ciphertext*), sementara *watermarking* menyembunyikan pesan dan mencakup informasi seperti hak cipta dan kepemilikan. Namun, metode ini jarang digunakan karena pesan rahasia dapat terdeteksi. Disisi lain,

steganografi menyembunyikan pesan dalam berbagai media seperti gambar, audio, dan video. Pendekatan ini menghindari kecurigaan, mencegah pihak yang tidak berwenang mengetahui isi pesan. Oleh karena itu, steganografi dianggap sebagai teknik yang dapat diandalkan untuk menjaga privasi dan kerahasiaan data selama proses transmisi[1].

Steganografi adalah sistem keamanan yang telah berkembang dari kebutuhan aspek perlindungan data tambahan. Meskipun mirip dengan kriptografi, steganografi memerlukan pendekatan yang lebih luas daripada hanya penggunaan kriptografi[2]. Oleh karena itu, penggunaan steganografi yang digabungkan dengan enkripsi dapat meningkatkan kerahasiaan keseluruhan data sehingga menyulitkan akses ke data asli dengan mengubahnya menjadi format yang tidak dapat digunakan. Dengan menyembunyikan pesan dalam berbagai media seperti gambar, audio, dan video, steganografi menjaga kerahasiaan pesan tanpa terdeteksi[3], [4].

Salah satu bentuk steganografi yang umum digunakan adalah teknik *Least Significant Bit* (LSB). Pemilihan metode ini didasarkan pada kesederhanaan algoritma yang digunakan dan kebutuhan sumber daya yang minimal. Prinsip dasar dari teknik ini adalah mengubah nilai bit paling tidak signifikan atau 1 bit terakhir dari sampel audio dengan menggunakan bit dari pesan yang akan disisipkan[5]. Prosedur steganografi menggunakan 1 bit terakhir, dengan contoh angka biner yang menunjukkan *file* sampul yang akan diisi dengan pesan, yang ditunjukkan pada gambar 1.

01001100	01001001	01010011	01010100	01001110	01000110
01001111	01100001				

Gambar 1. Biner media cover

Angka biner tersebut menampung huruf '**U**' yang nilai binernya (**01010101**), mengalami modifikasi yang ditunjukkan pada gambar 2.

01001100	01001001	0101001**0**	0101010**1**	01001110	0100011**1**
0100111**0**	01100001				

Gambar 2. Biner yang dimodifikasi

Menjaga keamanan informasi termasuk dokumen multimedia menjadi sangat penting dalam era informasi yang terbuka seperti sekarang ini. Berbagai konten multimedia seperti gambar, audio, dan video dengan mudah tersebar luas. Seiring dengan pertumbuhan penggunaan internet yang semakin merata, pengiriman informasi menjadi semakin rentan terhadap penyadapan yang dapat mengancam keaslian dan keselamatan data[6]. Oleh karena itu, dalam penelitian ini file audio dipilih sebagai media atau wadah untuk menyembunyikan data atau pesan. Pemilihan audio didasarkan pada peran pentingnya dalam transmisi sinyal saat ini, di mana audio memainkan peran penting dalam penyampaian informasi[7].

Penulis menggunakan audio berformat wave sebagai media penyisipan data, sebuah format yang dikembangkan oleh Microsoft. Format wave dirancang untuk menyimpan informasi properti, di mana suara direkam dan dikuantisasi langsung ke dalam bentuk digital. Format audio wave adalah jenis format yang tidak terkompresi. Karena siftanya yang tidak terkompresi, maka tidak ada kehilangan kualitas saat merekam atau menyimpan audio dalam format ini[8], [9].

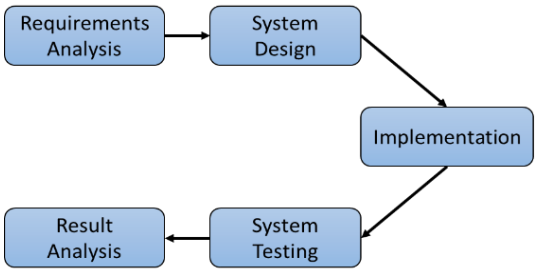
Keamanan dokumen teks adalah perhatian yang sangat penting, terutama ketika dokumen tersebut berisi informasi rahasia. Secara alami, pemilik dokumen tidak ingin informasi di dalamnya diketahui atau diubah oleh pihak yang tidak berwenang[10]. Oleh karena itu, untuk meningkatkan tingkat kerahasiaan, penulis menggunakan kriptografi dengan menerapkan algoritma *Playfair Cipher* sebagai metode untuk mengenkripsi teks. Algoritma kriptografi yang digunakan untuk menyembunyikan pesan dari pihak yang tidak berwenang melibatkan dua konsep utama, yaitu enkripsi dan dekripsi[11], [12]. *Playfair Cipher* membuat sulit bagi pihak yang tidak berwenang untuk membaca atau *decipher* karena menggunakan aturan subsitusi huruf berdasarkan lokasinya dalam matriks[13], [14].

Dalam penelitian ini, penulis merancang sebuah sistem yang dapat mengamankan pesan dengan mengenkripsi pesan menggunakan metode *Playfair Cipher*[15]. Kemudian menyisipkan pesan ke dalam audio format wave menggunakan algoritma LSB *Substiotion*[16]. Dengan menggunakan metode ini, pesan yang dikirim akan tetap terjaga kerahasiaannya.

2. METODE PENELITIAN

2.1. Metode Penelitian

Penelitian ini mencakup beberapa tahap, yakni analisis kebutuhan, desain sistem, implementasi, pengujian sistem, dan analisis hasil. Pada Gambar 3, terdapat alur untuk penelitian ini.



Gambar 3. Metode penelitian

2.1.1. Analisis Kebutuhan

Pada tahap analisis kebutuhan, dipertimbangkan perangkat untuk menerapkan keamanan file teks pada audio menggunakan metode LSB *Substitution* dan *Playfair Cipher*. Berikut adalah tabel 1 dan 2 yang berisi *hardware* dan *software* yang digunakan dalam penelitian ini:

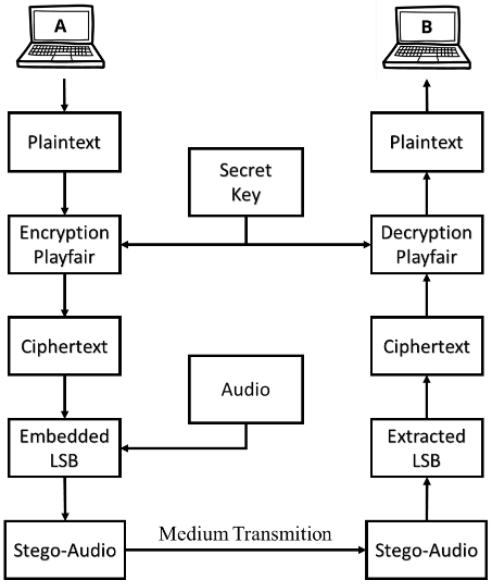
Tabel 1. *Hardware*

Nama	Spesifikasi
Laptop ASUS X540NA	*Intel Celeron N3350, RAM 4GB, SSD 256GB + HDD 320GB, Windows 10*

Tabel 2. *Software*

Nama	Deskripsi
Text File	Format *file* *.txt
Audio File	Format *file* *.wav
Python	*Python 3*
Pycharm Community Edition	Versi 2023.2.5

2.1.2. Desain Sistem



Gambar 4. Desain sistem

Alur penelitian berdasarkan desain sistem pada gambar 4 di atas melibatkan beberapa langkah:

1. Enkripsi *plaintext* dengan kunci "Arief Al Akbar" pada matriks kunci Playfair 16 X 16, menghasilkan *ciphertext*. Pada gambar 5 dan 6 berikut terdapat matriks kunci *Playfair* berdasarkan ASCII *value*.

A	r	i	e	f	space	l	k
b	a	\x00	\x01	\x02	\x03	\x04	\x05
\x06	\x07	\x08	\t	\n	\x0b	\x0c	\r
\x0e	\x0f	\x10	\x11	\x12	\x13	\x14	\x15
\x16	\x17	\x18	\x19	\x1a	\x1b	\x1c	\x1d
\x1e	\x1f	!	"	#	$	%	&
'	(	)	*	+	,	-	.
/	0	1	2	3	4	5	6
7	8	9	:	;	<	=	>
?	@	B	C	D	E	F	G
H	I	J	K	L	M	N	O
P	Q	R	S	T	U	V	W
X	Y	Z	[	\	]	^	_
`	c	d	g	h	j	m	n
o	p	q	s	t	u	v	w
x	y	z	{	|	}	~	\x7f

Gambar 5. Matriks *Playfair* ASCII *value* 1

\x80	\x81	\x82	\x83	\x84	\x85	\x86	\x87
\x88	\x89	\x8a	\x8b	\x8c	\x8d	\x8e	\x8f
\x90	\x91	\x92	\x93	\x94	\x95	\x96	\x97
\x98	\x99	\x9a	\x9b	\x9c	\x9d	\x9e	\x9f
\xa0	¡	¢	£	¤	¥	¦	§
¨	©	ª	«	¬	\xad	®	¯
°	±	²	³	´	µ	¶	·
¸	¹	º	»	¼	½	¾	¿
À	Á	Â	Ã	Ä	Å	Æ	Ç
È	É	Ê	Ë	Ì	Í	Î	Ï
Ð	Ñ	Ò	Ó	Ô	Õ	Ö	×
Ø	Ù	Ú	Û	Ü	Ý	Þ	ß
à	á	â	ã	ä	å	æ	ç
è	é	ê	ë	ì	í	î	ï
ð	ñ	ò	ó	ô	õ	ö	÷
ø	ù	ú	û	ü	ý	þ	ÿ

Gambar 6. Matriks *Playfair* ASCII *value* 2

2. Menyisipkan *ciphertext* ke dalam audio dengan mengganti *least significant bit* dari *byte* data audio, dan menghasilkan file stego.
3. Proses ekstraksi mengambil stego-audio dan mengonversinya menjadi string 8-bit, menghasilkan *ciphertext*.
4. Dekripsi *ciphertext* menjadi *plaintext* dengan menggunakan kunci yang sama seperti pada tahap enkripsi, menghasilkan pesan rahasia (*plaintext*).

2.1.3. Implementasi

Tahap awal dari implementasi adalah merancang sistem yang akan dijalankan. Proses ini mencakup pemilihan bahasa pemrograman, dalam hal ini *Python*, untuk mengembangkan program yang dapat melakukan enkripsi-dekripsi serta penyisipan-ektraksi pesan dalam audio.

Metode yang diterapkan untuk enkripsi-deksripsi dan penyisipan-ekstraksi pesan dalam audio telah ditentukan. Dalam hal ini, metode yang dipilih adalah LSB (*Least Significant Bit*) untuk penyisipan-ekstraksi pesan dalam audio, dan *Playfair Cipher* untuk enkripsi-dekripsi pesan sebelum disisipkan ke dalam audio..

2.1.4. Pengujian Sistem

Tahap awal dari pengujian ini adalah menyiapkan data yang akan digunakan, termasuk pemilihan pesan teks yang akan dienkripsi menggunakan algoritma *Playfair Cipher* serta pemilihan audio yang akan digunakan sebagai media penutup untuk menyisipkan pesan. Pesan teks tersebut kemudian dipilih dan dienkripsi menggunakan algoritma *Playfair Cipher* dengan menggunakan kunci yang telah ditentukan, dalam hal ini kunci yang digunakan adalah "Arief Al Akbar". Pesan teks yang telah dienkripsi kemudian disisipkan ke dalam audio *cover* menggunakan metode LSB *Substitution*, di mana proses ini melibatkan

penggantian bit-bit terakhir dari sampel audio dengan bit-bit pesan yang telah dienkripsi.

Audio yang telah dimodifikasi dengan penyisipan pesan tersebut kemudian disebut audio-stego. Tahap berikutnya melibatkan ekstraksi pesan dari audio-stego dengan menggunakan teknik yang sesuai, yaitu ekstraksi menggunakan metode LSB *Substitution* yang terbalik. Pesan yang berhasil diekstraksi dari audio-stego kemudian didekripsi menggunakan algoritma yang sesuai, yaitu *Playfair Cipher* dengan menggunakan kunci yang sama seperti yang digunakan ada tahap enkripsi.

2.1.5. Analisis Hasil

Tahap pertama adalah menyiapkan sampel uji yang terdiri dari audio *cover* dan audio stego yang telah dimodifikasi dengan penyisipan pesan. Sampel uji ini digunakan untuk melakukan evaluasi terhadap kualitas audio serta kemampuan penyimpanan pesan di dalam audio.

Analisis dilakukan untuk menilai seberapa efektif penyimpanan pesan dalam audio, dengan memastikan bahwa pesan yang disisipkan dalam audio stego dapat diekstraksi kembali tanpa mengganggu kualitas audio secara signifikan. Selain itu, analisis juga dilakukan untuk mengukur dampak modifikasi, yakni penyisipan pesan, terhadap kualitas audio *cover*. Proses ini melibatkan identifikasi perubahan dalam sinyal audio, seperti distorsi atau penurunan kualitas audio yang disebabkan oleh proses penyisipan pesan.

Evaluasi terhadap kualitas audio dilakukan dengan menghitung dan membandingkan nilai PSNR (*Peak Signal-to-Noise Ratio*) antara audio *cover* dan audio stego. PSNR berperan sebagai parameter untuk mengukur seberapa baik kualitas audio stego dibandingkan dengan audio *cover*, di mana nilai PSNR yang lebih tinggi menunjukkan kualitas audio yang lebih baik. Kriteria PSNR dapat dilihat pada tabel 3 berikut[17]:

Tabel 3. Kriteria PSNR

Rasio (dB)	Kualitas
60	*Excellent*, tanpa *noise*
50	*Good*, minim *noise*, kualitas audio bagus
40	*Reasonable*, terdapat *noise*, audio masih dapat digunakan
30	*Poor*, banyak *noise*
20	*Unusable*

Nilai PSNR dihitung dengan membagi perbedaan antara audio *cover* dan audio stego dengan *Mean Squared Error* (MSE)[18].

PSNR didefinisikan sebagai berikut:

$$PSNR = 20log_{10}\left(\frac{(L-1)}{MSE}\right) \quad (1)$$

L = Jumlah tingkat intensitas maksimum

MSE didefinisikan sebagai berikut:

$$MSE = \frac{1}{n}\sum_{i=0}^{n-1}(O-S)^2 \quad (2)$$

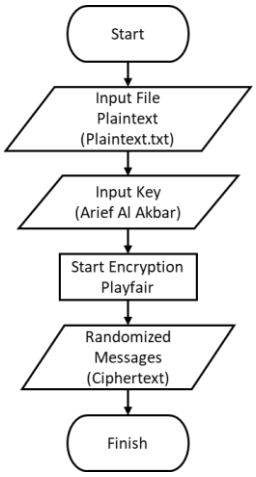
n = Jumlah *frame data*
O = Nilai *cover audio*
S = Nilai *stego audio*.

3. HASIL DAN PEMBAHASAN

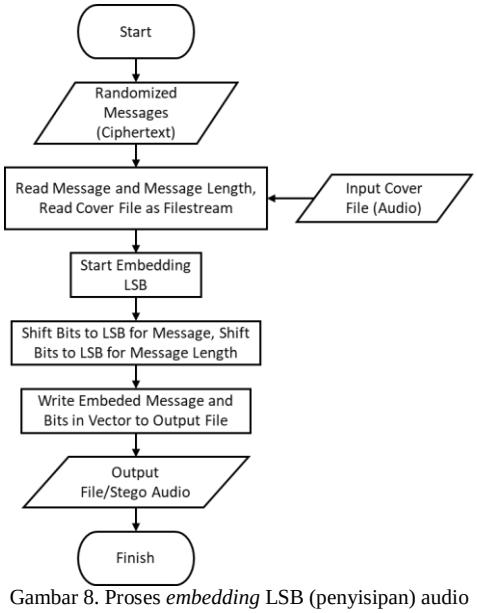
Bagian ini membahas hasil penerapan steganografi LSB (*Least Signifcant Bit*), untuk menyisipkan pesan dalam file audio wave dan algoritma *Playfair Cipher* untuk mengenkripsi pesan.

3.1. Implementasi

Pada tahap ini, membahas perancangan sistem yang digunakan untuk mengamankan data teks atau pesan dalam audio. Sistem ini terdiri dari dua proses utama, yaitu *encoding* dan *decoding*. Rancangan sistem ini kemudian diimplementasikan dan dijalankan menggunakan *Jupyter Notebook* dengan bahasa pemrograman *Python 3*.

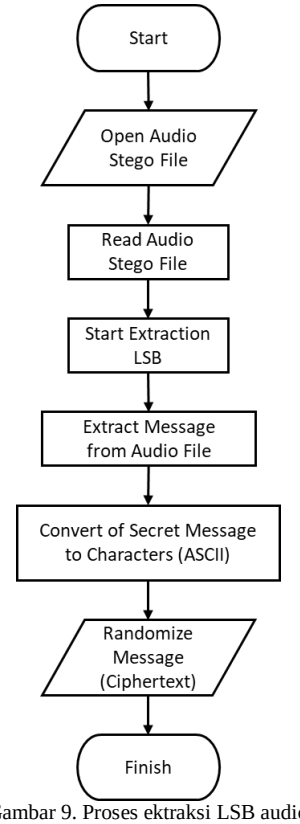


Gambar 7. Proses enkripsi *Playfair*

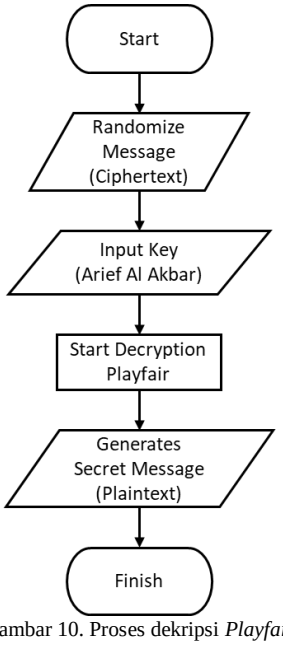


Gambar 8. Proses *embedding* LSB (penyisipan) audio

Gambar 7 dan 8 menunjukkan rancangan sistem untuk proses *encoding*. Proses ini dimulai dengan enkripsi menggunakan algoritma Playfair, seperti yang ditunjukkan pada Gambar 7, dan dilanjutkan dengan proses embedding LSB atau penyisipan pesan dalam audio wave, seperti yang ditunjukkan pada Gambar 8.



Gambar 9. Proses ektraksi LSB audio



Gambar 10. Proses dekripsi *Playfair*

Sementara itu, gambar 9 dan 10 menggambarkan rancangan sistem untuk proses *decoding*. Proses ini dimulai dengan ekstraksi LSB audio untuk mendapatkan pesan yang terenkripsi dari audio, seperti yang ditunjukkan pada Gambar 9, dan dilanjutkan dengan proses dekripsi menggunakan algoritma *Playfair* untuk mendapatkan pesan atau teks asli, seperti yang ditunjukkan pada Gambar 10.

3.2. Pengujian Sistem

Bagian ini membahas hasil uji coba pada file teks dan sampel audio. Aspek yang disorot termasuk langkah-langkah *encoding-decoding*, perbandingan antara *audio cover* dan *audio stego*, serta analisis audio melalui perhitungan nilai PSNR untuk mengevaluasi dampak penyisipan pesan terhadap kualitas audio. Sebelum itu berikut adalah data yang akan digunakan yang terdiri dari pesan teks dan audio dengan format wave. Sampel pesan teks teradapat pada tabel 4 dan sampel audio terdapat pada tabel 5:

Tabel 4. *File* Teks

***File* Teks**	**Panjang Pesan (*Char*)**	**Ukuran (*bytes*)**
Plaintext1.txt	778	773
Plaintext2.txt	1.038	1.031
Plaintext3.txt	1.556	1.546
Plaintext4.txt	3.110	3.093
Plaintext5.txt	6.224	6.185

Tabel 5. *File* audio yang digunakan sebagai *cover audio*

***File* Audio**	**Durasi (*s*)**	**Ukuran (*bytes*)**	**Panjang Frame**
Chinese.wav	24	389.442	398.398
British.wav	40	640.044	640.000
American.wav	53	850.744	857.468
French.wav	79	1.275.156	1.275.112
Hindi.wav	68	2.187.896	2.187.852

3.2.1. Proses *Encoding*

Tabel 6. Hasil proses *encoding*

Audio	***Message***		***Length Bit* (*bits*)**
	***Length Message* (*Char*)**	***Length Ciphertext* (*Char*)**	
Chinese.wav	773	778	6.224
	1.031	1.038	8.304
	1.546	1.556	12.448
	3.093	3.110	24.880
	6.185	6.224	49.792
British.wav	773	778	6.224
	1.031	1.038	8.304
	1.546	1.556	12.448
	3.093	3.110	24.880
	6.185	6.224	49.792
American.wav	773	778	6.224
	1.031	1.038	8.304
	1.546	1.556	12.448
	3.093	3.110	24.880
	6.185	6.224	49.792
French.wav	773	778	6.224
	1.031	1.038	8.304
	1.546	1.556	12.448
	3.093	3.110	24.880
	6.185	6.224	49.792
Hindi.wav	773	778	6.224
	1.031	1.038	8.304
	1.546	1.556	12.448
	3.093	3.110	24.880
	6.185	6.224	49.792

Tabel 7. Nilai PSNR *stego audio*

Stego Audio	PSNR (dB)
Chinese_Stego.wav	51,68
	51,88
	52,26
	53,69
	60,23
British_Stego.wav	51,47
	51,58
	51,80
	52,55
	54,58
American_Stego.wav	51,39
	51,47
	51,63
	52,15
	53.43
French_Stego.wav	51,32
	51,37
	51,48
	51.81
	52,56
Hindi_Stego.wav	51,25
	51,28
	51,34
	51,52
	51,92

Tabel 6 dan 7 di atas menampilkan hasil pengujian proses *encoding*, termasuk enkripsi dan embedding, pada beberapa file audio dengan variasi panjang pesan. Tabel juga mencantumkan nilai PSNR untuk setiap stego audio yang dihasilkan. Panjang pesan yang disisipkan berkisar antara 773 hingga 6.185 karakter, sedangkan panjang pesan yang dienkripsi (*ciphertext*) memiliki perbedaan yang sangat kecil, yaitu 778 hingga 6.224 karakter. Penambahan karakter pada *ciphertext* terjadi karena pasangan huruf yang sama dan huruf padding. Sebagai contoh, jumlah huruf ganjil pada *plaintext* menyebabkan penambahan karakter tertentu untuk membentuk pasangan huruf. Analisis embedding dengan panjang bit pesan 6.224 hingga 49.792 bit pada file audio Chinese.wav menunjukkan rata-rata PSNR sebesar 53,95 dB. Pada file audio British.wav, stego memiliki rata-rata PSNR sebesar 52,40 dB. File audio American.wav menghasilkan stego dengan rata-rata PSNR 52,01 dB, sementara French.wav dan Hindi.wav menghasilkan stego dengan rata-rata PSNR masing-masing sebesar 51,71 dB dan 51,46 dB.

3.2.2. Proses *Decoding*

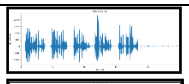
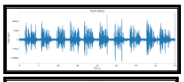
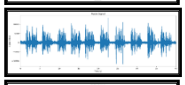
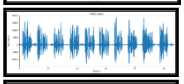
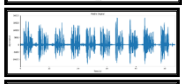
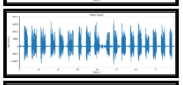
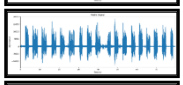
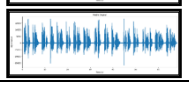
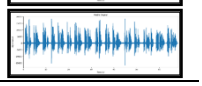
Tabel 8. Hasil proses *decoding*

Audio	*Length Hiddentext* (*Char*)	*Length Message* (*Char*)
Chinese_Stego.wav	778	773
	1.038	1.031
	1.556	1.546
	3.110	3.093
	6.224	6.185
British_Stego.wav	778	773
	1.038	1.031
	1.556	1.546
	3.110	3.093
	6.224	6.185
American_Stego.wav	778	773
	1.038	1.031
	1.556	1.546
	3.110	3.093
	6.224	6.185
French_Stego.wav	778	773
	1.038	1.031
	1.556	1.546
	3.110	3.093
	6.224	6.185
Hindi_Stego.wav	778	773
	1.038	1.031
	1.556	1.546
	3.110	3.093
	6.224	6.185

Tabel 8 di atas menampilkan hasil dari proses decoding, menunjukkan panjang pesan yang berhasil diekstrak (*length hiddentext*) dan panjang pesan asli (*length message*). *Length hiddentext* adalah panjang pesan yang diperoleh dari file audio stego setelah ekstraksi, berisi karakter acak (*ciphertext*), sedangkan *length message* adalah panjang pesan yang diperoleh dari proses dekripsi, memuat pesan asli (*plaintext*). Panjang pesan yang diekstrak sesuai dengan panjang karakter sebelum penyisipan, dan panjang pesan yang didekripsi sesuai dengan panjang pesan asli.

3.2.3. Perbandingan Audio

Tabel 9. Perbandingan audio

Audio	*Cover Audio*	*Stego Audio*
Chinese.wav		
British.wav		
American.wav		
French.wav		
Hindi.wav		

Tabel 9 di atas menyajikan perbandingan periodogram antara sinyal audio asli (cover audio) dan audio yang telah dimodifikasi (stego audio) untuk beberapa file audio. Periodogram digunakan untuk menganalisis frekuensi pada sinyal audio. Sinyal stego audio yang diuji mengandung pesan sepanjang 6.224 karakter. Perbandingan periodogram menunjukkan perubahan yang minim, menandakan keberhasilan proses penyisipan pesan pada data audio digital tanpa menimbulkan kecurigaan terhadap audio tersebut. Modifikasi pada berkas audio tidak memengaruhi struktur dasar frame audio, menunjukkan bahwa proses steganografi atau modifikasi tidak mengubah struktur file dari segi jumlah data frame.

3.3. Hasil Analisis

Hasil uji coba penyandian yang diperlihatkan dalam tabel 6 dan 7 mencakup proses enkripsi dan

penyisipan yang dilakukan pada 5 berkas audio dengan variasi panjang pesan yang disisipkan. Uji coba ini menunjukkan bahwa panjang pesan terenkripsi (*ciphertext*) pada *Playfair Cipher* memiliki perbedaan yang sangat kecil dibandingkan dengan panjang pesan asli. Hal ini disebabkan oleh beberapa faktor, seperti keberadaan pasangan huruf yang sama pada proses enkripsi dan penambahan huruf *padding* untuk memastikan pembentukan pasangan huruf pada *Playfair Cipher*. Selain itu, proses penyisipan pada berkas audio menunjukkan variasi panjang bit yang digunakan untuk menyembunyikan pesan, dengan nilai PSNR yang berbeda pada setiap berkas audio. Hal ini menunjukkan bahwa teknik steganografi audio menggunakan LSB dan *Playfair* dapat melindungi pesan dengan baik tanpa memberikan dampak yang signifikan pada kualitas audio.

Hasil pengujian proses *decoding* yang tercatat dalam tabel 8 menampilkan panjang pesan yang berhasil diekstrak (*length hiddentext*) dari file audio stego setelah mengalami proses ekstraksi, serta panjang pesan asli (*length message*) yang berhasil dipulihkan melalui proses dekripsi. Dalam uji coba ini, proses *decoding* sukses menghasilkan dua panjang pesan yang berbeda. Panjang *hiddentext* merupakan panjang pesan yang berhasil diekstrak dari file audio stego, tetapi masih berbentuk karakter acak akibat dari proses enkripsi atau penyembunyian pesan sebelumnya. Panjang pesan menunjukkan panjang pesan asli yang berhasil dikembalikan setelah melalui proses dekripsi. Ini menunjukkan bahwa meskipun panjang pesan berhasil diekstrak dari file audio stego, namun isi pesan tersebut tidak dapat dibaca atau dimengerti tanpa melalui proses dekripsi. Dengan demikian, keberhasilan proses *decoding* pada tahap ini terutama dinilai berdasarkan panjang pesan yang sesuai dengan pesan asli yang diharapkan.

Ada beberapa aspek yang terkait dengan berkas audio, khususnya dalam konteks modifikasi yang dilakukan terhadap berkas audio, seperti struktur data *frame* audio dan perbandingan periodogram. Seperti terlihat dalam tabel 9, perbandingan audio menunjukkan bahwa modifikasi yang diterapkan pada berkas audio, seperti proses steganografi atau penyisipan pesan, tidak mengubah struktur dasar berkas audio dalam hal jumlah *frame*. Selain itu, tidak ada perubahan yang signifikan pada karakteristik frekuensi sinyal audio dalam perbandingan periodogram antara berkas audio asli dan berkas audio stego. Ini mengindikasikan bahwa modifikasi yang diterapkan berhasil dilakukan tanpa menyebabkan perubahan mencolok atau mencurigakan pada karakteristik sinyal audio secara keseluruhan.

Beberapa aspek terkait pengujian kualitas audio stego setelah melalui proses *embedding* menggunakan PSNR (*Peak Signal-to-Noise Ratio*) adalah penting untuk diperhatikan. PSNR digunakan sebagai parameter evaluasi untuk menilai kualitas audio yang telah mengalami *embedding*, dengan tujuan menunjukkan sejauh mana audio stego yang dihasilkan mampu menyimpan pesan rahasia tanpa memberikan dampak signifikan pada kualitas audio asli. Kriteria yang diinginkan untuk nilai PSNR adalah di atas 40 dB, dan semakin tinggi nilai PSNR, semakin baik kualitas audio stego yang dihasilkan. Pada tabel 7, hasil pengujian menunjukkan bahwa kualitas audio stego berada dalam kriteria baik, dengan rentang nilai antara 51.25 hingga 60.23 dB. Contohnya, sampel Chinese.wav memiliki nilai PSNR tertinggi (60.23 dB) dengan panjang pesan yang disisipkan sebanyak 6.224 karakter, menunjukkan bahwa audio stego dari sampel tersebut memiliki kualitas yang sangat baik. Di sisi lain, sampel Hindi.wav memiliki nilai PSNR terendah (51.25 dB) dengan panjang pesan yang disisipkan sebanyak 778 karakter, menunjukkan kualitas yang sedikit lebih rendah namun masih berada dalam kriteria baik. Hasil pengujian ini menyiratkan bahwa audio stego yang dihasilkan memiliki kualitas yang memadai, yang ditandai oleh nilai PSNR yang tinggi. Dengan demikian, proses *embedding* berhasil mengintegrasikan pesan rahasia tanpa signifikan mengurangi kualitas audio, dan tanpa menimbulkan kecurigaan terhadap keberadaan pesan tersembunyi dalam audio tersebut.

4. DISKUSI

Penelitian-penelitian terdahulu yang terkait dengan dilakukannya penelitian ini adalah:

1. Penelitian pertama, mengamankan data teks di dalam sinyal audio dengan menerapkan teknik steganografi LSB. Peneliti menyisipkan pesan rahasia menggunakan metode LSB ke dalam file audio berformat WAV. Implementasi teknik LSB menunjukkan bahwa data teks dapat diamankan secara efektif, dan file audio WAV dapat diputar tanpa mengalami perubahan yang dapat terdeteksi[6].
2. Penelitian kedua, melakukan pendekatan dengan memanfaatkan algoritma genetika dengan kunci keamanan simetris K-Bit. Sebuah pesan tersembunyi dimasukkan ke dalam klip audio. Hasilnya menunjukkan bahwa metode ini dapat menyisipkan lebih banyak bit pesan dengan menggunakan jumlah sampel yang lebih kecil, sehingga meningkatkan kapasitas penyisipan dan tingkat keamanan[19].
3. Penelitian ketiga, melakukan penelitian terkait pemetaan data dan substitusi LSB dengan menggunakan pembangkitan kunci RSS. Penelitian ini mengusulkan suatu metode pembangkitan kunci dalam steganografi yang memanfaatkan komunikasi nirkabel dan RSS. Uji coba dilakukan pada kondisi statis dan dinamis, dan hasilnya menunjukkan kemampuan untuk menyisipkan sejumlah besar bit pesan[2].

Namun, penelitian ini menggunakan dua pendekatan, yaitu metode LSB (*Least Significant Bit*) dan Playfair Cipher. LSB digunakan untuk menyisipkan pesan rahasia ke dalam audio, sementara *Playfair Cipher* bertanggung jawab atas enkripsi pesan. Dengan penggunaan algoritma kriptografi, maka keamanan pesan rahasia meningkat. Pesan dienkripsi terlebih dahulu menggunakan metode *Playfair* sehingga tidak dapat dibaca atau dimengerti. Setelah proses enkripsi, hasilnya disisipkan ke dalam audio menggunakan metode LSB. Melalui metode LSB, nilai bit terakhir pada audio digantikan dengan bit pada pesan tanpa mengurangi kualitas audio secara signifikan. Sehingga, file audio tetap dapat didengarkan dengan pesan rahasia di dalamnya.

5. KESIMPULAN

Berdasarkan hasil implementasi Metode LSB dan *Playfair* untuk mengenkripsi dan menyembunyikan pesan rahasia pada sinyal audio, dapat disimpulkan bahwa, Hasil steganografi audio dengan metode *Playfair* dan LSB menunjukkan kemampuan untuk menyembunyikan pesan tanpa memberikan dampak yang signifikan pada kualitas audio berdasarkan perbandingan sinyal dari audio *cover* dan audio stego. Modifikasi pada file audio tidak secara signifikan mengubah struktur dasar atau karakteristik frekuensi sinyal audio.

Pada proses *decoding*, meskipun panjang pesan yang disembunyikan berhasil diekstrak, isi pesan masih bersifat acak dan memerlukan proses dekripsi untuk mendapatkan kembali pesan aslinya. Evaluasi kualitas stego menggunakan PSNR menunjukkan bahwa kualitas audio hasil steganografi baik, dengan nilai PSNR di atas 40 dB, berkisar antara 51.25 hingga 60.23 dB. Hal ini menegaskan bahwa proses penyisipan pesan rahasia dapat dilakukan tanpa mengurangi secara signifikan kualitas audio.

Berdasarkan hasil penelitian, terdapat beberapa saran untuk pengembangan lebih lanjut. Pertama, disarankan untuk melakukan pengujian pada berbagai jenis *file* audio lainnya. Selain itu, disarankan juga untuk mengembangkan metode steganografi audio dengan menerapkan algoritma kriptografi yang berbeda.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Prodi Teknik Informatika, Fakultas Sains dan Teknologi, Universitas Muhammadiyah Kalimantan Timur atas dukungan dan fasilitasnya untuk melaksanakan penelitian ini.

DAFTAR PUSTAKA

[1] D. Tan, Y. Lu, X. Yan, and X. Wang, "A simple review of audio steganography," *Proc. 2019 IEEE 3rd Inf. Technol. Networking, Electron. Autom. Control Conf. ITNEC 2019*, no. Itnec, pp. 1409–1413, 2019, doi: 10.1109/ITNEC.2019.8729476.

[2] M. T. SUMADI, A. SUDARSONO, and M. YULIANA, "Steganography Based on Data Mapping and LSB Substitution With RSS Key Generation," *ELKOMIKA J. Tek. Energi Elektr. Tek. Telekomun. Tek. Elektron.*, vol. 10, no. 1, p. 1, 2022, doi: 10.26760/elkomika.v10i1.1.

[3] R. Indrayani, "Human perception evaluation toward end of file steganography method's implementation using multimedia file (image, audio, and video)," *2019 4th Int. Conf. Inf. Technol. Inf. Syst. Electr. Eng. ICITISEE 2019*, vol. 6, pp. 200–204, 2019, doi: 10.1109/ICITISEE48480.2019.9003759.

[4] M. Anusha, K. N. Bhanu, and D. Divyashree, "Secured Communication of Text and Audio using Image Steganography," *Proc. Int. Conf. Electron. Sustain. Commun. Syst. ICESC 2020*, no. Icesc, pp. 284–288, 2020, doi: 10.1109/ICESC48915.2020.9155715.

[5] K. Bansal, A. Agrawal, and N. Bansal, "A Survey on Steganography using Least Significant bit (LSB) Embedding Approach," no. Icoei, pp. 64–69, 2020.

[6] D. Adhar, A. Syahputra, R. A. Sugianto, R. Oktari Batubara, A. Sanjaya, and A. Sabir, "Steganografi Pengamanan Data Teks Menggunakan Audio Wav Dengan Metode LSB," *CSRID J.*, vol. 13, no. 3A, pp. 211–220, 2021.

[7] R. Indrayani, "Modified LSB on Audio Steganography using WAV Format," *2020 3rd Int. Conf. Inf. Commun. Technol. ICOIACT 2020*, pp. 466–470, 2020, doi: 10.1109/ICOIACT50329.2020.9332132.

[8] R. Hussein and W. Alexan, "Secure Message Embedding in Audio," *2nd Int. Conf. Comput. Appl. Inf. Secur. ICCAIS 2019*, pp. 1–6, 2019, doi: 10.1109/CAIS.2019.8769505.

[9] F. C. Venna, "Implementasi Steganografi Audio pada File Wav dengan metode Redundant Pattern Encoding (RPE) Berbasis Sndroid," *Repository.Uinjkt.Ac.Id*, 2019, [Online]. Available: http://repository.uinjkt.ac.id/dspace/handle/123456789/47958

[10] S. D. Surbakti, "Implementasi Algoritma Playfair Cipher pada Penyandian Data," *J. Tek. Inform. Unika St. Thomas*, vol. 4, no. 2, pp. 166–123, 2019, [Online]. Available: https://core.ac.uk/download/pdf/267031349.pdf

[11] S. Khasanah and T. Sutabri, "Analisis Pencegahan Pencurian Data Melalui Aplikasi Whatsapp Menggunakan Metode

Kriptografi," *J. Sain dan Tek.*, vol. 5, no. 2, pp. 145–153, 2023.

[12] M. Bertaccini, *Cryptography Algorithms: A guide to algorithms in blockchain, quantum cryptography, zero-knowledge protocols, and homomorphic encryption*. Packt Publishing, 2022. [Online]. Available: https://books.google.co.id/books?id=t1taEAAAQBAJ

[13] Muhammad Pristiwanto, "Perancangan Aplikasi Enkripsi Kata Menggunakan Algoritma Playfair Cipher Berbasis Web," *J. Comput. Sci. Inf. Syst. Progr. Stud. Sist. Informasi, Fak. Sains Teknol. Univ. Labuhanbatu Vol. 2, Nomor 4, Novemb. 2021, Pages. 176-185 e-ISSN 2747-2221*, vol. 5, no. 3, pp. 248–253, 2021.

[14] G. Lasry, *A Methodology for the Cryptanalysis of Classical Ciphers with Search Metaheuristics*. kassel University Press, 2018. [Online]. Available: https://books.google.co.id/books?id=YI9NDwAAQBAJ

[15] R. M. Marzan and A. M. Sison, "An enhanced key security of playfair cipher algorithm," *ACM Int. Conf. Proceeding Ser.*, vol. Part F147956, no. February 2019, pp. 457–461, 2019, doi: 10.1145/3316615.3316689.

[16] E. W. Abood *et al.*, "Audio steganography with enhanced LSB method for securing encrypted text with bit cycling," *Bull. Electr. Eng. Informatics*, vol. 11, no. 1, pp. 185–194, 2022, doi: 10.11591/eei.v11i1.3279.

[17] A. D. Hendrata and A. Prihanto, "Analisis Kualitas Suara Stego Audio Penyisipan Informasi Tersembunyi dengan Metode Least Significant Bit," *J. Informatics Comput. Sci.*, vol. 2, no. 03, pp. 178–184, 2021, doi: 10.26740/jinacs.v2n03.p178-184.

[18] Prudhvi Raj Budumuru, G Prasanna Kumar, and B Elisha Raju, "Hiding an Image in an Audio File using LSB Audio Technique," *Int. Conf. Comput. Commun. Informatics*, pp. 5–8, 2021.

[19] J. Mohajon, "An Improved Approach in Audio Steganography Using Genetic Algorithm with K-bit Symmetric Security Key," *Nucl. Phys.*, vol. 13, no. 1, pp. 104–116, 2018.