Management of Information System Journal
Vol 3, No 2, Maret 2025, Hal. 38 - 45
ISSN: 2964-9455 (media online)
DOI: 10.47065/mis.v2i3. 1942
https://journal.fkpt.org/index.php/MIS

Pengamanan File Teks Dengan Algoritma Enkripsi Pohlig-Hellman Dan Steganografi Ezstego Pada File Audio

Herwansyah

[1]Fakultas Ilmu Komputer dan Teknologi Informasi, Program Studi Teknik Informatika, Universitas Budi Darma Medan, Medan, Indonesia
Email: [1]herwansyah@gmail.com

Abstrak- Pada kriptografi proses enkripsi dilakukan dengan cara merubah data tersebut ke dalam bentuk data yang lain yang tidak dapat dimengerti dan dipahami maknanya. Namun dengan bentuk lainnya data tersebut dapat menimbulkan kecurigaan, maka setelah data tersebut dienkripsi, perlu adanya melakukan penyembunyian data kedalam sebuah objek tanpa merubah bentuk objek tersebut dengan teknik steganografi. Proses dengan *double* pengamanan file teks dilakukan dengan teknik kriptografi menggunakan algoritma *Pohlig-Hellman* yang kemudian hasil enkripsi berupa *chipertext* disisipkan kembali kedalam objek audio menggunakan algoritma Ezstego. Dari hasil analisa, karakter *chipertext* yang telah di enkripsi menggunakan algoritma *Pohlig-Hellman*, dapat disisipkan dengan akurat kedalam objek audio tanpa memrubah bentuk audio tersebut menggunakan algoritma Ezstego.

Kata Kunci: *kriptografi, steganografi, teks, Pohlig-Hellman, Ezstego*

Abstract- In cryptography, the encryption process is carried out by changing the data into another form of data that cannot be understood and its meaning can be understood. However, with other forms of data, this can raise suspicion, so after the data is encrypted, it is necessary to hide the data into an object without changing the object's shape using steganography techniques. The process of double securing text files is done by using cryptographic techniques using the Pohlig-Hellman algorithm, then the encryption results in the form of ciphertext are inserted back into the audio object using the Ezstego algorithm. From the analysis, the ciphertext characters that have been encrypted using the Pohlig-Hellman algorithm can be accurately inserted into the audio object without changing the audio form using the Ezstego algorithm.

Keywords: *cryptography, steganography, text, Pohlig-Hellman, Ezstego*

1. PENDAHULUAN

Berbagi informasi adalah salah satu hal yang sering diterapkan oleh setiap manusia. Informasi yang kerap dibagikan umumnya terkandung kedalam bentuk karakter teks untuk dibaca dan dipahami maknanya. Akan tetapi disamping informasi yang dimiliki semakin rahasia, maka terdapat juga berbagai kalangan yang ingin mencuri informasi tersebut sebelum sampai kepada pihak yang menerima. Proses pencurian informasi data bisa terjadi dikarenakan data yang disimpan sangat mudah diakses. Sehingga penyimpanan data yang dilakukan didalam media *stroge* rawan terhadap pengaksesan oleh orang-orang yang tidak memiliki wewenang [1]. Saat ini berbagai macam teknik digunakan untuk melindungi informasi, karena data informasi yang dikirim kepada penerima harus tetap rahasia dan terjaga keaslianya atau tidak termodifikasi.

Teknik yang dapat diandalkan adalah teknik kriptografi. Kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data serta otentikasi. Kriptografi memelurkan algoritma untuk melakukan proses enkripsi, salah satu Algoritma *pohlig hellman.*. Konsep enkripsi pada algoritma *Pohlig-Hellman* hampir sama dengan algoritma RSA [2]. Algoritma *Pohlig-Hellman* lebih sederhana dibandingkan dengan algoritma RSA karena hanya menggunakan satu bilangan prima sebagai kunci privat, sedangkan untuk algoritma RSA menggunakan dua bilangan prima untuk pembangkitan kunci publik [3]. Pada kriptografi proses enkripsi dilakukan dengan cara merubah data tersebut ke dalam bentuk data yang lain yang tidak dapat dimengerti dan dipahami maknanya. Namun dengan bentuk lainnya data tersebut dapat menimbulkan kecurigaan, maka setelah data tersebut dienkripsi, perlu adanya melakukan penyembunyian data kedalam sebuah objek tanpa merubah bentuk objek tersebut dengan teknik steganografi.

Steganografi (*steganography*) adalah ilmu dan seni menyembunyikan pesan rahasia (*hiding message*) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia. Algoritma *Ezstego* adalah salah satu algoritma yang dapat diandalkan dalam mewujudkan teknik steganografi. Algoritma *Eztstego* adalah algoritma steganografi yang menyisipkan bit-bit pesan dengan metode penyisipan pada bit karakter terakhir kedalam sebuah objek yang akan menampung pesan. Algoritma *Eztego* tidak menggunakan kunci dalam proses penyisipan pesan sehingga siapapun yang mengetahui algoritmanya dapat mengekstraksi pesan [4]. Oleh sebab itu pada penelitian ini algoritma *Ezstego* dalam proses penyisipan dan ekstraksi pesan dimodifikasi menggunakan kunci (*stego-key*).

Adapun dalam penelitian ini objek yang digunakan untuk menampung data enkripsi teks menggunakan algoritma *Pohlig-Hellman* adalah objek berupa *file audio.* Hasil enkripsi berupa *chipertext* akan di sembunyikan dengan steganografi kedalam *file audio* sehingga menambahkan keamanan data yang akan dikirim. Penelitian yang dilakukan oleh Sari menyatakan bahwa algoritma *Pohlig-Hellman* dapat mengamankan data teks dengan dengan tingkat kerahasiaan yang terjaga dikarenakan proses dekripsi dilakukan dengan kunci yang diperoleh dari iterasi algoritms Pohlig-Helman.

Management of Information System Journal
Vol 3, No 2, Maret 2025, Hal. 38 - 45
ISSN: 2964-9455 (media online)
DOI: 10.47065/mis.v2i3. 1942
https://journal.fkpt.org/index.php/MIS

2. METODOLOGI

2.1 Kriptografi

Kriptografiberasal dari bahasa Yunani, *crypto* dan *graphia*.*Crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan) [5].Kriptografi adalah sebuah teknik penyandian pesan yang dilakukan agar pesan dapat dikirim dan diterima dengan aman.Kriptografi bertujuan untuk menjaga kerahasian data dan informasi agar tidak disalah gunakan oleh pihak yang tidak sah[6].

2.2 Steganografi

Kata Steganografi *(steganography)* berasal dari bahasa Yunani yang terdiri dari kata *steganos* yang artinya tersembunyi dan *graphien* yang artinya menulis, sehingga bisa diartikan sebagai tulisan yang tersembunyi. Dapat disimpulkan bahwa, Steganografi adalah ilmu yang mempelajari teknik pengembangan pesan rahasia di dalam pesan yang lainnya, sedemikian rupa sehingga orang lain tidak akan tahu bahwa terdapat pesan rahasia di dalam pesan yang mereka baca [7]. Dalam melakukan penyisipan pesan baik itu pada pesan teks, gambar, suara dan *video* dibutuhkan masukan berupa *file digital* yang akan disisipkan pesan, pesan yang akan disisipkan (*message*), dan kunci (*key*).

2.3 File Audio

Audio adalah suara atau bunyi yang dihasilkan oleh getaran suatu benda, agar dapat tertangkap oleh telinga manusia getaran tersebut harus kuat minimal 20 kali/detik. Suara yaitu suatu getaran yang dihasilkan oleh gesekan , pantulan dan lain-lain, antara benda-banda. Sedangkan gelombang yaitu suatu getaran yang terdiri dari Amplitudo dan juga waktu. Suara dibangun oleh periode, Apabila Tidak Berarti itu bukanlah Suara [8]. Definisi *audio* yang lainnya adalah merupakan salah satu elemen yang penting, karena ikut berperan dalam membangun sebuah sistem Komunikasi dalam bentuk suara, ialah suatu sinyal elektrik yang akan membawa unsur-unsur bunyi didalamnya. *Audio* itu terbentuk melalui beberapa tahap, diantaranya: tahap pengambilan atau penangkapan suara, sambungan transmisi yang membawa bunyi, *amplifier* [8].

2.4 Algoritma Pohlig-Ellman

Pada awalnya algoritma *pohlig hellman* ditemukan oleh Roland Silver, namun untuk pertama kalinya diterbitkan oleh Stephen Pohlig dan Martin Hellman. Algoritma *pohlig hellman* dipatenkan di Amerika Serikat dan Kanada. Konsep enkripsi pada Algoritma Pohlig-Hellman hampir sama dengan algoritma RSA. Pada dasarnya algoritma ini adalah salah satu algoritma asimetris karena menggunakan kunci yang berbeda untuk enkripsi dan dekripsi [9].
Dalam algoritma *Pohlig Hellman* tidak menggunakan konsep kunci publik karena kuncinya dapat digunakan pada saat enkripsi dan dekripsi sehingga harus terjaga kerahasiaannya. Sama seperti algoritma lainnya seperti algoritma RSA dimana dapat melakukan enkripsi dan dekripsi dalam dihitung dengan rumus:
$C = Pe \bmod n$ (untuk melakukan enkripsi) …….. (1)
$P = Cd \bmod n$ (untuk melakukan dekripsi)….. …… (2)

2.5 Algoritma Ezstego

Algoritma *EzStego* menyisipkan bit-bit pesan pada bit LSB dari indeks palet. Akibat penyisipan tersebut, indeks palet dapat bertambah satu, tetap, atau berkurang satu. Oleh karena indeks palet merupakan *pointer* ke palet warna, maka indeks yang baru (setelah penyisipan LSB) menunjuk ke warna berikutnya atau ke warna sebelumnya di palet yang tentu saja secara *visual* berbeda signifikan. Hal ini tentu menimbulkan degradasi warna yang membuat citra stego berbeda jauh dengan citra *cover*. Untuk meminimalkan degradasi warna, maka langkah pertama di dalam algoritma *EzStego* adalah mengurutkan warna-warna di dalam palet sedemikian sehingga perbedaan dua warna yang bertetangga adalah minimal. Perbedaan dua warna dapat dihitung dengan rumus jarak *Euclidean*. Misalkan warna 1 dinyatakan sebagai vektor ($R1$, $G1$, $B1$) dan warna 2 dinyatakan sebagai ($R2$, $G2$, dan $B2$) [4].

3. HASIL DAN PEMBAHASAN

Metode yang digunakan dalam pembahasan ini adalah sebuah algoritma kriptografi asimetri yaitu algoritma *Pohlig-Hellman.* Algoritma *Pohlig-Hellman* melakukan enkripsi dan dekripsi dengan 2 kunci yang berbeda. Kunci yang digunakan untuk enkripsi adalah kunci publik sedangkan kunci yang digunakan utnuk dekripsi adalah kunci *private*. Pembentukan kunci ini ditentukan oleh 3 bilangan yaitu satu bilangan prima, bilangan e dan bilangan d. Bilangan tersebut adalah bilangan prima yang acak. Setelah proses pembentukan kunci, hal selanjutnya adalah porses enkripsi. Proses enkripsi algoritma *Pohlig-Hellman* dilakukan dengan Modulus nilai *plaintext* dengan kunci private yang dudapat, sehingga menghasilkan *chipertext.*
Hasil *chipertext* enkripsi *Pohlig-Hellman* kemudian dilanjutkan dengan pengamanan teknik steganografi. Steganografi dapat menyembunyikan bit-bit karakter *chipertext* hasil enkripsi kedalam sebuah objek tanpa merubah bentuk objek

Management of Information System Journal
Vol 3, No 2, Maret 2025, Hal. 38 - 45
ISSN: 2964-9455 (media online)
DOI: 10.47065/mis.v2i3. 1942
https://journal.fkpt.org/index.php/MIS

tersebut. Algoritma yang digunakan adalah algoritma *Ezstego*. *Ezstego* menyisipkan pesan bit-bit *chipertext* dengan menukar bit terakhir nilai objek dengan bit *chipertext*. Sedangkan objek yang digunakan adalah sebuah file audio. Hal pertama yang dilakukan adalah membaca setiap nilai hexadesimal *plain* audio, kemudian merubah setiap nilai dari file audio kedalam bentuk biner. Biner file audio terdiri dari beberapa oktet, dimana 1 oktet terdiri dari 8 bit. Proses *Ezstego* mennukar bit kedalam pada file audio biner dengan setiap bit-bit *chipertext*, sehingga menghasilkan audio stegano.

3.1 Contoh Penerapan Algoritma Pohlig Hellman

Algoritma Pohlig_hellman adalah algoritma asimetri, dimana kunci untuk enkripsi dan dekripsi menggunakan kunci yang berbeda. Kunci yang berbeda ini disebut dengan *public key* dan *private key*. *Public key* digunakan untuk proses enkripsi, sedangkan *private key* digunakan utnuk melakukan dekripsi. Adapun proses pertama adalah membangkitan kunci publik dan kunci *private*.

1. Pembangkitan kunci publik dan *private*

Adapun proses membangkitan kunci pertama terlebih menentukan pilihan bilangan prima secara acak.

a. Menentukan nilai p

Pada pembahasan ini bilangan prima (p) adalah 403.

b. Menetukan nilai totien p

Proses selanjutnya menhitung nilai totien p dengan rumus:
p = p-1 sehingga nilai totient p = 403 -1 = 402.

c. Menentukan e

Selanjutnya adalah menentukan nilai e dengan syarat e > 1 dan GCD (p mod e) = 1
Nilai e yang akan diambil adalah 7. Sebagai bukti dilakukan tes sebagai berikut:
402 mod 7 = 3
7 mod 3 = 1
sehingga nilai e=7 dapat digunakan.

d. Tentukan nilai d

Selanjutnya adalah menentukan nilai f dengan rumus d = (d*e) mod p=1
Ditentukan nilai d=103 Sebagai bukti dilakukan tes sebagai berikut :
d = (103 * 7) Mod 402
= 721 Mod 402
= 1

Dengan demikian didapatkan kunci publik dan kunci *private* sebagai berikut :
Kunci Publik = (p, e) = (403, 7)
Kunci Private = (p, f) = (403, 103)

2. Enkripsi Algoritma *Pohlig-Hellman*

Setalah didapatkan kunci publik dan *private* proses selanjutnya adalah melakukan enkripsi *plaintext* dengan menggunakan kunci publik. Adapun *plaintext* yang akan di enkripsi adalah "**HERWANSYAH**". Rubah karakter kedalam nilai desimal menggunakan tabel ASCII. Sehingga :

H = 72
E = 69
R = 82
W = 87
A = 65
N = 78
S = 83
Y = 89
A = 65
H = 72

Adapun rumus enkripsi *Pohlig-Hellman* adalah : **Chiper = (Plain^e) Mod p**

Chiper1 = 72^7 Mod 403
= 10030613004288 Mod 403
= 175

Chiper2 = 69^7 Mod 403
= 446353252589 Mod 403
= 62

Chiper3 = 82^7 Mod 403
= 24928547056768 Mod 403
= 173

Chiper4 = 87^7 Mod 403
= 37725479487783 Mod 403

Management of Information System Journal
Vol 3, No 2, Maret 2025, Hal. 38 - 45
ISSN: 2964-9455 (media online)
DOI: 10.47065/mis.v2i3. 1942
https://journal.fkpt.org/index.php/MIS

= 87
Chiper5 = 65^7 Mod 403
= 4902227890625 Mod 403
= 234
Chiper6 = 78^7 Mod 403
= 17565568854912 Mod 403
= 39
Chiper7 = 83^7 Mod 403
= 27136050989627 Mod 403
= 73
Chiper8 = 89^7 Mod 403
= 44231334895529 Mod 403
= 15
Chiper9 = 65^7 Mod 403
= 4902227890625 Mod 403
= 234
Chiper10 = 72^7 Mod 403
= 10030613004288 Mod 403
= 175

Gabungkan hasil enkripsi *chiper* sehingga menjadi nilai *chipertext* **"175, 62, 173, 87, 234, 39, 73, 15, 234, 175.** Kemudian rubah nilai chipertext kedalam karakter dengan tabel ASCII sehingga menghasilkan *chipertext* seperti pada tabel di bawah ini :

Tabel 1 *Chipertext*

Nilai Desimal Chipertext	Karakter Chipertext
175	¯
62	>
173	
87	W
234	ê
39	'
73	I
15	SI
234	Ê
175	¯

Berdasarkan tabel karakter *chipertext* didapatkan *chipertext* hasil enkripsi algoritma *Pohlig Hellman* adalah " ¯> **Wê'ISIê¯** ". *Chipertext* tersebut kemudian disembunyikan menggunakan agoritma *Ezstego* kedalam objek audio.

3.1 Contoh Penerapan Algoritma Ezstego

Proses selanjutnya adalah melakukan penyembunyian data hasil enkripsi algoritma *Pohlig-hellman* kedalam objek audio menggunakan algoritma *Ezstego*. Adapun nilai hexa dan biner sampel audio sebanyak 96 byte dapat dilihat pada tabel di bawah ini :

Tabel 2 Nilai Biner Audio Sampel

No	Audio Objek			No	Audio Objek		
	Hexa	Des	Biner		Hexa	Des	Biner
1	49	73	01001001	25	B2	178	10110010
2	6C	108	01101100	26	6D	109	01101101
3	6D	109	01101101	27	A9	169	10101001
4	75	117	01110101	28	6C	108	01101100
5	20	32	00100000	29	98	152	10011000
6	4B	75	01001011	30	7A	122	01111010
7	6F	111	01101111	31	A4	164	10100100
8	6D	109	01101101	32	78	120	01111000
9	70	112	01110000	33	99	153	10011001
10	75	117	01110101	34	A1	161	10100001

Management of Information System Journal
Vol 3, No 2, Maret 2025, Hal. 38 - 45
ISSN: 2964-9455 (media online)
DOI: 10.47065/mis.v2i3. 1942
https://journal.fkpt.org/index.php/MIS

11	74	116	01110100	35	7B	123	01111011
12	65	101	01100101	36	A7	167	10100111
13	72	114	01110010	37	98	152	10011000
14	50	80	01010000	38	B1	177	10110001
15	61	97	01100001	39	A7	167	10100111
16	B1	177	10110001	40	9D	157	10011101
17	A9	169	10101001	41	95	149	10010101
18	B4	180	10110100	42	89	137	10001001
19	85	133	10000101	43	BE	190	10111110
20	80	128	10000000	44	70	112	01110000
21	A9	169	10101001	45	96	150	10010110
22	B3	179	10110011	46	78	120	01111000
23	BE	190	10111110	47	BD	189	10111101
24	A4	164	10100100	48	B1	177	10110001
		….		….	….	….	….

Tabel Lanjutan 2 Nilai Biner Audio Sampel

No	Audio Objek			No	Audio Objek		
	Hexa	Des	Biner		Hexa	Des	Biner
7 9	A9	169	10101001	88	6D	109	1101101
80	B1	177	10110001	89	96	150	10010110
81	9D	157	10011101	90	78	120	1111000
82	79	121	1111001	91	9D	157	10011101
83	B4	180	10110100	92	89	137	10001001
84	C0	192	11000000	93	78	120	1111000
85	A8	168	10101000	94	B4	180	10110100
86	B1	177	10110001	95	B1	177	10110001
87	66	102	01100110	96	A7	167	10100111

Adapun *chipertext* yang akan disisipkan sebagai berikut :
¯> **Wê'ISIê**¯
Chipertext di atas, dikonversikan kedalam bentuk biner seperti pada tabel di bawah ini:

Tabel 3. Biner *Chipertext*

No	Chipertext	Nilai Desimal	Biner
1	¯	175	10101111
2	>	62	00111110
3		173	10101101
4	W	87	01010111
5	ê	234	11101010
6	'	39	00100111
7	IS	73	01001001
8	I	15	00001111
9	ê	234	11101010
10	¯	175	10101111

Berdasarkan pada tabel di atas, nilai biner *chipertext* sudah didapatkan. Selanjutnya adalah proses penyisipan nilai biner menggunakan algoritma *Ezstego*. Algoritma *Eztego* menyisipkan setiap nilai bit biner *chipertext* dengan menukarkan nilai bit akhir (bit ke 8) nilai biner audio sampel. Sebelum dilakukan penyisipan bit terlebih dahulu

Management of Information System Journal
Vol 3, No 2, Maret 2025, Hal. 38 - 45
ISSN: 2964-9455 (media online)
DOI: 10.47065/mis.v2i3. 1942
https://journal.fkpt.org/index.php/MIS

meyiapkan kunci stegano *Eztego* sebagai penanda awal proses penyisipan dan penambahan *string* karakter sebagai penanda akhir proses penyisipan.

1. Menyiapkan Kunci Stegano *Ezstego*

Kunci stegano *Ezstego* diperlukan sebagai penanda awal penyisipan biner *chipertext* dimulai, sedangkan penanda akhir sebagai proses pemberhantian penyisipan yang berfungsi untuk proses ektraksi. Adapun kunci yang digunakan untuk keperluan hitungan manual adalah string "IRWAN" dan penanda akhir adalah sebuah karakter #. Untuk mendapatkan nilai 8 bit kunci penanda awal dilakukan XOR nilai biner setiap karakter kunci seperti di bawah ini :

Tabel 4 Nilai Biner Kunci

Karakter	Nilai Desimal	Nilai Biner
I	73	01001001
R	82	01010010
W	87	01010111
A	65	01000001
N	78	01001110

Lakukan XOR untuk setiap nilai kunci seperti berikut :

I = 01001001
R = 01010010
_____ XOR
00011011
W = 01010111
_____XOR
01001100
A = 01000001
_____XOR
00001101
N = 01001110
_____XOR
01000011

Berdasarkan hasil XOR didapati nilai kunci stegano *Ezstego* penanda awal adalah **01000011** dan nilai penanda akhir penyisipan biner *chipertext* adalah # dalam biner **00100011.** Gabungkan kunci *Ezstego*, biner *chipertext* dan penanda akhir menjadi satu bagian seperti di bawah ini :

0101011010101111001111101010110101010111111010100010011101001001000011111110101010101111**00100011**

2. Proses Penyisipan Bit Ke-8 *Ezstego*

Penyisipkan dilakukan pada bit ke-8 nilai biner audio sampel dengan menukarkan atau memindahkan nilai bit pertama *chipertext* dengan nilai bit ke-8 byte pertama audio sampel. Keseluruhan nilai biner *chipertext* dan nilai penanda awal serta akhir disisipkan menggunakan algoritma *Ezstego* pada bit ke 8 setiap nilai biner sampel audio. Jumlah keseluruhan nilai yang bit yang akan disisipkan adalah sebanyak 96 bit. Adapun proses penyisipan atau perpindahan nilai biner *chipertext* dapat dilihat pada tabel di bawah ini :

Tabel 5. Proses Penyisipan Bit Chiper

No	Audio Objek			Bit Chiper	Audio Stegano		
	Hex	Des	Biner		Hex	Des	Biner
1	49	73	01001001	0	48	72	01001000
2	6C	108	01101100	1	6D	109	01101101
3	6D	109	01101101	0	6C	108	01101100
4	75	117	01110101	1	75	117	01110101
5	20	32	00100000	0	20	32	00100000
6	4B	75	01001011	1	4B	75	01001011
7	6F	111	01101111	1	6F	111	01101111
8	6D	109	01101101	0	6C	108	01101100
9	70	112	01110000	1	71	113	01110001

Management of Information System Journal
Vol 3, No 2, Maret 2025, Hal. 38 - 45
ISSN: 2964-9455 (media online)
DOI: 10.47065/mis.v2i3. 1942
https://journal.fkpt.org/index.php/MIS

10	75	117	01110101	0	74	116	01110100
11	74	116	01110100	1	75	117	01110101
12	65	101	01100101	0	64	100	01100100
13	72	114	01110010	1	73	115	01110011
14	50	80	01010000	1	51	81	01010001
15	61	97	01100001	1	61	97	01100001
16	B1	177	10110001	1	B1	177	10110001
17	A9	169	10101001	0	A8	168	10101000
18	B4	180	10110100	0	B4	180	10110100
19	85	133	10000101	1	85	133	10000101
20	80	128	10000000	1	81	129	10000001
21	A9	169	10101001	1	A9	169	10101001
		….			….	….	….

Proses yang sama dilakukan hingga penyisipan bit terakhir sepeti pada tabel lanjutan 5 di bawah ini :

Tabel Lanjutan 5 Proses Penyisipan Bit Chiper

No	Audio Objek			Bit Chiper	Audio Stegano		
	Hex	Des	Biner		Hex	Des	Biner
79	A9	169	10101001	1	A9	169	10101001
80	B1	177	10110001	0	B0	176	10110000
81	9D	157	10011101	1	9D	157	10011101
82	79	121	01111001	0	78	120	01111000
83	B4	180	10110100	1	B5	181	10110101
84	C0	192	11000000	0	C0	192	11000000
85	A8	168	10101000	1	A9	169	10101001
86	B1	177	10110001	1	B1	177	10110001
87	66	102	01100110	1	67	103	01100111
88	6D	109	01101101	1	6D	109	01101101
89	96	150	10010110	0	96	150	10010110
90	78	120	01111000	0	78	120	01111000
91	9D	157	10011101	1	9D	157	10011101
92	89	137	10001001	0	88	136	10001000
93	78	120	01111000	0	78	120	01111000
94	B4	180	10110100	0	B4	180	10110100
95	B1	177	10110001	1	B1	177	10110001
96	A7	167	10100111	1	A7	167	10100111

Berdasarkan pada proses penyisipan biner *chipertext*, nilai desimal atau hexadesimal audio sampel mengalami perubahan pengurangan dan penambahan nilai sebanyak 1 nilai. Adapun nilai keseluruhan audio sampel yang telah disisipkan dengan biner *chipertext* menggunakan algoritma *Ezstego* dapat dilihat pada tabel di bawah ini :

Tabel 6. Audio Stegano

No	Audio Objek			No	Audio Stegano		
	Hex	Des	Biner		Hex	Des	Biner
1	48	72	01001000	13	73	115	01110011

Management of Information System Journal
Vol 3, No 2, Maret 2025, Hal. 38 - 45
ISSN: 2964-9455 (media online)
DOI: 10.47065/mis.v2i3. 1942
https://journal.fkpt.org/index.php/MIS

2	6D	109	01101101	14	51	81	01010001
3	6C	108	01101100	15	61	97	01100001
4	75	117	01110101	16	B1	177	10110001
5	20	32	00100000	17	A8	168	10101000
6	4B	75	01001011	18	B4	180	10110100
7	6F	111	01101111	19	85	133	10000101
8	6C	108	01101100	20	81	129	10000001
9	71	113	01110001	21	A9	169	10101001
10	74	116	01110100	22	B3	179	10110011
11	75	117	01110101	23	BF	191	10111111
12	64	100	01100100	24	A4	164	10100100
....	....	....	....	....	....	....	....
79	A9	169	10101001	88	6D	109	01101101
80	B0	176	10110000	89	96	150	10010110
81	9D	157	10011101	90	78	120	01111000
82	78	120	01111000	91	9D	157	10011101
83	B5	181	10110101	92	88	136	10001000
84	C0	192	11000000	93	78	120	01111000
85	A9	169	10101001	94	B4	180	10110100
86	B1	177	10110001	95	B1	177	10110001
87	67	103	01100111	96	A7	167	10100111

4. KESIMPULAN

Hasil enkripsi berupa *chipertext* dapat diminalisir kecurigaanya dengan berhasil disembunyikan kedalam objek audio menggunakan teknik steganografi. Proses *Embedding* dan Enkripsi serta Ekstraksi dan Dekripsi berhasil dilakukan dengan baik pada file teks dengan objek file audio menggunakan algoritma *Pohlig-Hellman* dan *Ezstego*. Proses enkripsi dan dekripsi menggunakan algoritma *Pohlig-Hellman* rentan terhadap kriptoanalisis, hal ini karenakan proses enkripsi dan dekripsi yang begitu sederhana. File audio yang telah disisipkan karakter *chipertext* mengalami perubahan ukuran. Ukuran audio stegano menjadi lebih besar dari audio awal.

REFERENSI

[1]. R.Munir, "Analisa Keamanan Enkripsi Citra Digital Menggunakan Kombinasi
[2]. Dua *Chaos Map* dan Penerapan Teknik Selektif", Juti, vol. 10, pp89-95, 2012
[3]. R.N. Sari, , "Penggunaan Algoritma Kriptografi Pohlig-Hellman Dalam
[4]. Mengamankan Data", Seminar Nasional Informatika, pp.240-245, 2015
[5]. A. Simarmata, "Rancangan Model Algoritma Pohlig-Hellman dengan Menggunakan Multiple-key Berdasarkan Algoritma RSA Multiple-key", Seminar Nasional Aplikasi Teknologi informasi", pp.21-27, 2013
[6]. R.Munir, "Eksperimen Steganalisis dengan Metode *Visual Attack* pada Citra Hasil *EzStego* Berformat GIF", SNATI, pp.8-14, 2016
[7]. Wira (2017,Sep.27). Pengamanan dan Keamanan [online]. Available : https://wiratamabakti.com/2017/09/27/pengamanan-dan-keamanan/
[8]. E.R. Agustina and A. Kurniati, "Pemanfaatan Kriptografi Dalam Mewujudkan Keamanan Informasi Pada *e-Voting* di Indonesia", Seminar Nasional Informatika, pp.22-28, 2009
[9]. Sumberpengertian (2019,Feb.18). Pengertian Teks Menurut Para Ahli [online] Available : http://www.sumberpengertian.co/pengertian-teks-menurut-para-ahli
[10]. S.Rohayah et al, "Aplikasi Steganografi Untuk Penyisipan Pesan", Jurnal Informatika, vol. 9, pp.976-981, 2015
[11]. Sora, (2019,Feb.18). Pengertian Audio dan Media Audio Secara Lengkap [online]. Available: http://www.pengertianku.net/2014/11/pengertian-audio-dan-media-audio-secara-lengkap.html
[12]. A.Simarmata, "Rancangan Model Algoritma *Pohlig-Hellman* dengan Mengguakan *Multiple-key* Berdasarkan Algoritma RSA *Multiple-key*", Sminar Nasional Aplikasi Teknologi Informasi, pp.21-27, 2013