Terbit pada laman web jurnal : **http://ojsamik.amikmitragama.ac.id**

JURNAL JARINGAN SISTEM INFORMASI ROBOTIK (JSR)
Vol. 8 No. 1 TAHUN 2024 E - ISSN : 2579-373X

TEKNIK STEGANOGRAFI *DISCRETE COSINE TRANSFORM* DAN ALGORITMA RSA UNTUK MENYISIPKAN PESAN PADA AUDIO

Abdul Halim Hasugian[1], Ibnu Rusydi[2], Puja Apriani[3]
[1,3] Program Studi Ilmu Komputer, Universitas Islam Negeri Sumatera Utara, Medan, Indonesia
[2] Fakultas Teknik dan Ilmu Komputer, Universitas Dharmawangsa, Medan, Indonesia
Email: [1]abdulhalimhasugian@uinsu.ac.id, [2]ibnurusydi@dharmawangsa.ac.id, [3]pujaapriani5@gmail.com

Abstrak

Transmisi informasi menjadi lebih umum, yang dapat membahayakan keaslian dan integritas pesan. Pesan yang sangat pribadi atau sensitif seringkali diinginkan oleh individu. Untuk melindungi pesan pribadi dan sensitif, diperlukan sistem keamanan data. sehingga mereka yang berhak menerimanya dapat melakukannya. Salah satunya melalui penggunaan metode yang dikenal dengan kriptografi dan steganografi, yang dimana pesan tersebut dienkripsi terlebih dahulu menjadi karakter yang tidak bermakna kemudian disisipkan pada wadah penampung. Metode Kriptografi yang digunakan ialah Algoritma RSA. Kesulitan mengubah bilangan besar menjadi faktor prima untuk mendapatkan keamanan pada algoritma RSA terletak pada kunci publik dan private. Namun, Algoritma Kriptografi ini memiliki kelemahan dalam penerapannya yaitu mudah menimbulkan konflik karena pesan diubah atau diacak menjadi bentuk yang tidak bermakna. Untuk menghindari kekurangan dari algoritma kriptografi yang digunakan, keberadaan pesan perlu disembunyikan untuk menjaga kerahasiaan pesan. Maka, penulis menggunakan pendekatan steganografi dan kriptografi. Metode Steganografi yang digunakan adalah metode transformasi yang bekerja dengan melakukan transformasi audio kemudian dilakukan modifikasi terhadap koefisien DCT sesuai dengan bit pesan yang disisipkan. Pesan yang disembunyikan ialah pesan teks biasa yang disisipkan pada audio (*.wav) diimplementasikan dengan bantuan Microsoft Visual Studio 2012. Sistem penanaman dengan teknik DCT menghasilkan suara Stegano yang tidak terlalu mempengaruhi kualitas suara, hanya naik 1kb untuk size audio dibawah 2mb dan menghasilkan proses pemulihan pesan sebagai pesan secara efektif dikembalikan seperti semula.

Kata Kunci: Audio Wav, DCT, Kriptografi, RSA, Steganografi

Abstract

Information transmission is becoming more common, which can compromise the authenticity and integrity of messages. Highly personal or sensitive messages are often desired by individuals. To protect private and sensitive messages, a data security system is required. so that those who deserve it can do so. One of them is through the use of methods known as cryptography and steganography, in which the message is first encrypted into meaningless characters and then pasted into a container. The cryptographic method used is the RSA Algorithm. The difficulty of changing large numbers into prime factors to get security in the RSA algorithm lies in the public and private keys. However, this Cryptographic Algorithm has weaknesses in its application, namely it is easy to cause conflicts because messages are changed or scrambled into meaningless forms. To avoid the drawbacks of the cryptographic algorithm used, the existence of the message needs to be hidden to maintain the confidentiality of the message. As a result, the authors use a steganographic and cryptographic approach. The steganography method used is a transformation method that works by transforming the audio and then modifying the DCT coefficients according to the inserted message bits. The hidden messages are plain text messages embedded in audio (*.wav) implemented with the help of Microsoft Visual Studio 2012. The embedding system with the DCT technique produces Stegano sound which doesn't really affect the sound quality, only increases 1kb for audio sizes below 2mb and produces the process message recovery as the message is effectively restored to the way it was.

Keywords: Audio Wav; Cryptography; DCT ; RSA; Steganography

1. PENDAHULUAN

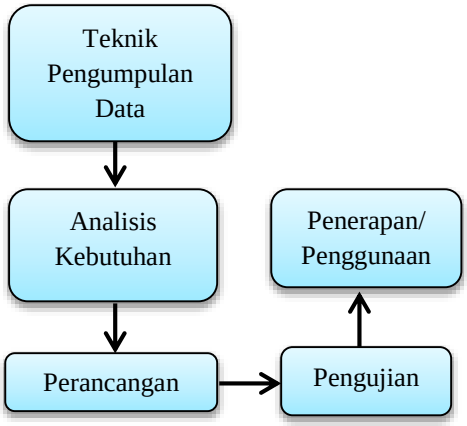
Seiring dengan perkembangan dan kemajuan teknologi komunikasi digital yang pesat saat ini, tidak menutup kemungkinan bahwa tindak kejahatan digital pun dapat ikut bertambah dan berkembang. Semua kebutuhan sehari-hari dapat dilakukan hanya dengan perangkat pintar dan koneksi internet. Semua hal dapat dilakukan mulai dari mencari informasi, media sosial, pembelajaran *online* hingga kebutuhan ekonomi [1]. Pencurian maupun penyadapan informasi merupakan sebuah isu keamanan yang harus diperhatikan. Data dapat diakses dengan mudah jika mereka tidak memanfaatkan teknologi keamanan khusus oleh oknum yang tidak bertanggung jawab. Media komunikasi dianggap dapat diakses oleh pihak atau individu manapun karena dapat digunakan untuk mengirimkan data atau informasi melalui jaringan publik seperti internet atau jaringan lokal. dengan maksud untuk mencuri, menyadap, atau memodifikasi data[2].

Salah satu cara untuk menaklukkan apa yang terjadi di atas adalah dengan menyandikan atau menyamarkan pesan misteri dengan kunci menjadi kode yang sulit dibaca dengan menggunakan strategi kriptografi. Ada berbagai macam teknik yang dapat digunakan dalam aktivitas keamanan pesan karena bidang kriptografi. RSA adalah salah satunya. Teknik enkripsi yang dikenal sebagai algoritma RSA menggunakan kunci publik dan kunci pribadi untuk proses enkripsi dan dekripsi[3]. Kesulitan algoritma RSA dalam memfaktorkan bilangan menjadi faktor primanya, khususnya n ke p dan q, dan ketahanannya terhadap berbagai bentuk serangan, khususnya serangan *brute force*, adalah yang membedakannya dari algoritma Kriptografi lainnya. Kriptografi di sisi lain, hanya digunakan untuk menyembunyikan pesan rahasia sehingga tidak ada yang bisa melihatnya. Kelemahannya adalah karakter pesan menjadi lebih mudah untuk tidak dipercaya, semakin tidak berarti. Orang yang memiliki kecurigaan ini dapat mencoba mendekripsi data[4]. Berdasarkan masalah tersebut maka dibutuhkan suatu metode untuk menyembunyikan pesan rahasia.

Salah satu nya adalah dengan menggunakan teknik Steganografi. Steganografi bertujuan untuk menyisipkan pesan rahasia ke dalam pesan lain sedemikian rupa sehingga orang lain tidak menyadari keberadaannya. Dalam hal ini, pesan asli akan disembunyikan atau diselipkan pada media pembawa sehingga perubahan yang terjadi pada media pembawa tidak dapat diketahui[5]. Steganografi biasanya dilakukan dengan media digital, yang dapat disematkan pesan atau media *cover-object* berupa teks, gambar, audio, atau video. Dengan kata lain, data berupa teks dapat disembunyikan kedalam sebuah citra digital. DCT(*Discrete Cosine Transform*), adalah salah satu teknik steganografi. Sebuah sinyal dapat dipecah menjadi komponen frekuensi dasarnya menggunakan *Discrete Cosine Transform* (DCT). Steganografi menggunakan DCT pertamatama dilakukan dengan mengubah audio kemudian mengubah koefisien DCT sesuai dengan bit pesan yang telah disisipkan. DCT merupakan teknik yang efektif karena menghasilkan audio yang terkompres, sehingga tidak menandakan adanya pesan rahasia di dalamnya, dan kokoh terhadap manipulasi pada stego *object* dibanding metode Steganografi yang lain seperti LSB yang memiliki kapasitas pesan yang disisipkan terbatas dan sensitif terhadap *filtering*. Penggunaan citra dan video sebagai media penyisipan pesan sudah banyak dianalisa dan dikembangkan baik dalam Kriptografi maupun Steganografi , sedangkan penggunaan media arsip audio relatif jarang terkhusus untuk metode DCT dengan format (*.wav)[6]. Maka dari itu penelitian ini menggunakan wadah penampung audio.

Pada penelitian sebelumnya (Yudha et., all, 2019) [7], mereka mempresentasikan kombinasikan algoritma RSA yang digunakan untuk mengenkripsi pesan rahasia dan teknik LSB digunakan untuk menyembunyikan pesan terenkripsi dengan tujuan untuk menghasilkan Stego *file* yang lebih aman dan lebih baik secara kualitas. Kemudian (Purwanto & T, 2018) mempresentasikan Implementasi pada sistem yang dibangun dilakukan dengan menggabungkan penerapan metode algoritma Kriptografi El-Gamal dalam menyandikan pesan pada penerapan metode Steganografi citra dalam menyembunyikan pesan tersandi yang dihasilkan kedalam sebuah citra warna (RGB) dalam domain *Discrete Cosine Transform* dengan teknik penyisipan Least Significant Bit. .

2. METODOLOGI PENELITIAN



Gambar 1. Bagan Prosedur Penelitian

kerangka kerja pada penelitian ini bertujuan untuk menguraikan tahapan-tahapan kegiatan yang dilakukan agar sesuai dengan tujuan yang telah ditentukan.

2.1 Alat dan Bahan penelitian

Bahan yang di ambil untuk penelitian ini adalah 4 file audio dengan format (*.Wav). Perangkat keras dan perangkat lunak adalah alat yang digunakan dalam sistem untuk mendukung proses desain :

1. *Processor : Intel®Pentium® CPU B970 @ 2.30GHz*
2. RAM : 2.00 GB
3. *Operating System Windows 10 Pro 64 bit*
4. *Microsoft Visual Studio 2012*

2.2 Teknik Pengumpulan Data

a. Penelitian Kepustakaan
   Suatu kegiatan penelitian yang dikenal dengan penelitian kepustakaan melibatkan pengumpulan data dan informasi dari berbagai sumber, antara lain buku, hasil penelitian terdahulu yang dapat diperbandingkan, artikel dan jurnal online, dan sebagainya.
b. Studi Literatur
   Merupakan rangkaian kegiatan yang melibatkan membaca dan mencatat, mengolah bahan penelitian, dan mengumpulkan data dari perpustakaan. Ini juga melibatkan pengumpulan sejumlah buku dan jurnal yang terkait dengan masalah dan tujuan penelitian[8].

2.3 Analisis Kebutuhan

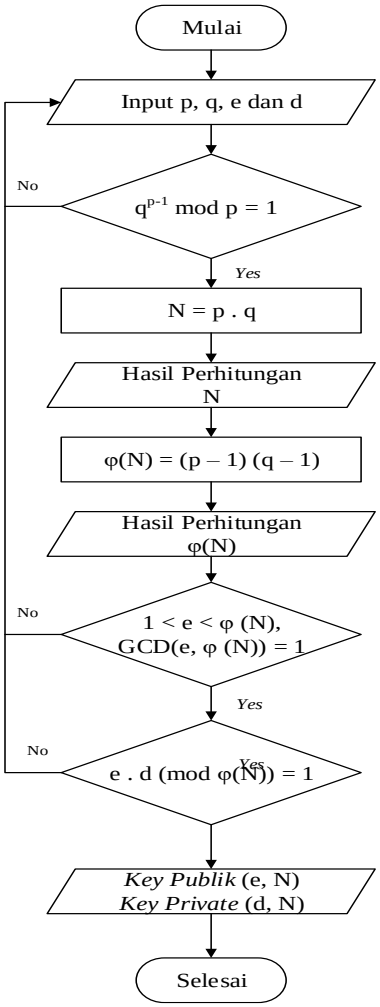
Analisa kebutuhan adalah suatu langkah awal untuk menentukan gambaran perangkat yg akan dihasilkan. Pada tahap ini, dirancang program penyisipan pesan rahasia dengan menggunakan aplikasi *Microsoft Visual Studio 2012*. Dalam perancangan sistem Kriptografi dan Steganografi audio ini, dibutuhkan *file* audio (*.wav) yang akan digunakan sebagai penampung pesan dan juga pesan teks sebagai pesan rahasia yang disisipkan pada.

2.4 Perancangan

Tujuan perancangan adalah untuk memberikan gambaran tentang sistem yang sedang dibangun. Menggunakan flowchart, pemodelan program ini akan dirancang.

2.5 Algoritma Rivest Shamir Adleman(RSA)

Metode kriptografi yang dikenal sebagai RSA memanfaatkan dua bilangan prima. Kunci Publik, yang digunakan untuk mengenkripsi teks biasa, dan Kunci Pribadi, yang digunakan untuk mendekripsi teks sandi, dapat diturunkan dari dua bilangan prima ini. Ada tiga proses dalam algoritma RSA: pembuatan kunci, proses enkripsi, dan proses dekripsi. Oleh karena itu, kekuatan algoritma RSA meningkat seiring dengan besarnya bilangan yang difaktorkan. Proses enkripsi dan dekripsi algoritma RSA didasarkan pada proses matematika, terutama bilangan prima dan aritmatika modulo, dua bilangan prima terbesar adalah p dan q, di mana p q Prosedur matematis dilakukan untuk menghasilkan kunci rahasia yang hanya dapat digunakan oleh pengirim dan penerima pesan untuk dekripsi[9]. Berikut *flowchart* pembangkit kunci untuk memperoleh kuncik publik dan *private* dalam kriptografi RSA :



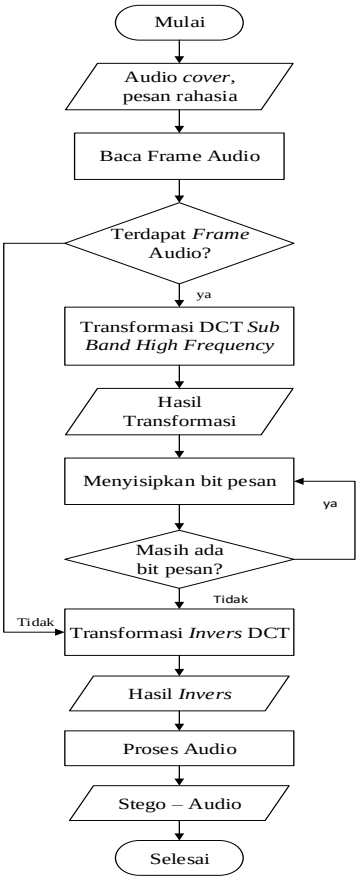
Gambar 2. *Flowchart Generate Key*

1. Pembangkit Kunci : menunjukkan alur pembuatan kunci RSA yang akan digunakan untuk enkripsi dan dekripsi. Empat bilangan bulat yang membentuk input adalah p, q, e, dan d. Nilai prima dari dua input pertama, p dan q, akan dicari. Lanjutkan menghitung nilai N jika benar, kemudian dilanjut dengan menghitung φ(N). Selanjutnya membangkitkan kunci public padabilangan e jika e relatif prima terhadap φ(N), Jika benar maka dilanjut menghitung menghitung nilai d, yang dimana proses ini untuk membangkitkan kunci private. Sehingga proses-proses yang sudah dilalui sebelumnya menghasilkan kunci public (e, N) dan kunci Private (d, N).

2.6 Steganografi

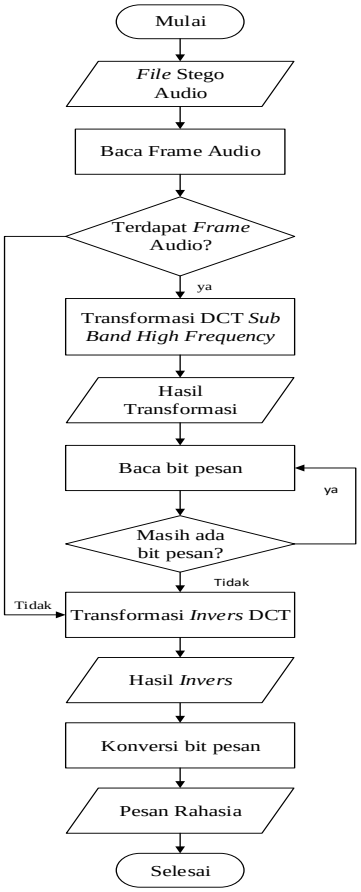
Steganografi adalah ilmu dan seni melampirkan pesan rahasia di dalam pesan lain untuk mencegah penemuannya. Steganografi mencegah munculnya kecurigaan terkait wadah media atau pesan yang dikirim. Pesan primitif didelegasikan sebagai sinyal pembawa yang dapat berupa teks, audio, gambar, video, dll., sedangkan pesan sekunder (tersembunyi) adalah ditetapkan sebagai pesan yang dimuat[10]. *Discrete Cosine Transform* (DCT) merupakan salah satu metode untuk berpindah dari domain koordinat ke domain

frekuensi. Metode DCT menggunakan fungsi gelombang kosinus diskrit untuk mengganti koefisien DCT pada audio asli dengan koefisien baru[11]. Berikut *Flowchart* penyisipan pesan yang akan di enkripsi :



Gambar 3. *Flowchart* Penyisipan

2. Penyisipan DCT : *Embedding* pada penelitian ini diawali dengan memasukkan audio cover dan pesan rahasia, kemudian membaca frame dari audio yang telah dipilih, jika tidak terdapat *frame* audio maka langsung dilakukan invers DCT, jika terdapat *frame* audio maka dilakukan transformasi DCT menyisipkan bit pesan ke dalam setiap *frame* yang berhasil dibaca menggunakan pita frekuensi tinggi hingga semua bit pesan dimasukkan. Jika masih ada bit pesan yang ingin disisipkan makan kembali pada proses menyisipkan bit pesan, jika bit pesan yang disisipkan sudah sesuai maka dilanjutkan dengan melakukan transformasi *invers* DCT. Kemudian proses audio hingga menjadi Stego-audio[12].



Gambar 4. *Flowchart* Ekstraksi

3. Ekstraksi : Tahap pertama memasukkan *file* stego audio, kemudian membaca *frame* audio, jika tidak terdapat frame audio maka dilanjutkan dengan transformasi *invers* DCT, jika terapat *frame* audio maka dilanjutkan dengan transformasi DCT lalu membaca bit-bit pesan. Jika ada bit pesan yang ingin disisipkan lagi maka kembali pada proses menyisipkan bit pesan, jika tidak ada bit pesan yang ingin maka dilanjutkan dengan mentransformasi *invers* DCT, lalu mengkonversi bit pesan sehingga menampilkan pesan rahasia. *Flowchart* Ekstraksi merupakan bagian dari Kriptografi untuk mendekripsikan suatu pesan yang sudah di ekstrak saat disisipkan pesan.

2.7 Pengujian dan Penerapan

Pengujian kotak hitam, atau pengujian sistem, dilakukan secara bertahap. Pengujian *black box* digunakan untuk mengetahui apakah setiap fungsi program dapat berfungsi dengan baik. Pengujian dilakukan pada 4 *file* audio berbeda berformat Wav. Sedangkan Penerapan pada penelitian ini dilakukan dengan mengenkripsi dan mendekripsi suatu kunci/pesan yang dimana pesan tersebut akan disisipkan pada media digital audio berjenis (*.wav) dan *output* yang dihasilkan adalah audio yang sudah disisipi pesan. Penelitian ini menyisipkan pesan secara manual dengan di ketik oleh pengguna[13].

3. HASIL DAN PEMBAHASAN

3.1 Analisis Data

Teknik steganografi membutuhkan objek untuk menyisipkan pesan teks ke dalam audio; dalam penelitian ini, audio dalam format wav digunakan sebagai data objek. Sample *.wav adalah nama audio yang digunakan, seperti yang bisa dilihat di bawah ini :

Gambar 5. Audio Sampel

Pada gambar 5 diatas terdapat contoh audio sampel berformat *.wav yang akan digunakan sebagai wadah untuk menyisipkan pesan teks. Sebuah objek audio yang akan berfungsi sebagai media penyimpanan nilai pesan teks yang mengandung karakter diperoleh berdasarkan gambar. Mengenkripsi pesan teks terlebih dahulu memastikan bahwa hanya pengirim dan penerima pesan yang dapat menguraikan isinya sebelum memasukkannya. Pesan teks yang terdiri dari karakter, simbol, dan angka merupakan pesan yang dapat dienkripsi. Teks yang mengandung karakter "PUJA UINSU" merupakan sebagian contoh data teks yang akan diselipkan pada saat proses aplikasi manual.

3.2 Representasi Data

Selanjutnya untuk proses penyisipan dengan metode DCT, *File* teks di enkripsi secara manual terlebih dahulu kemudian dilanjutkan dengan *file* audio sample yang akan di ekstraksi terlebih dahulu nilainya.

1. Data Teks Sampel

Tabel 1. Perhitungan Proses Enkripsi

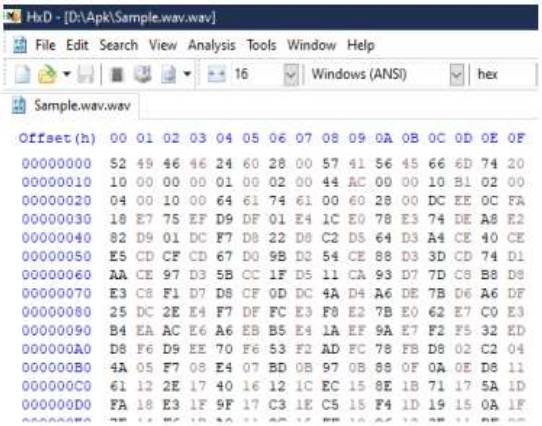
No	Plainteks(P)	N	E	C = $\mathbf{P}_i^e$ mod N
1	P= 80	1073	673	80
2	U = 85	1073	673	85
3	J = 74	1073	673	74
4	A = 65	1073	673	761
5	U = 85	1073	673	85
6	I = 73	1073	673	73
7	N = 78	1073	673	252
8	S = 83	1073	673	460
9	U = 85	1073	673	85

Tabel 2. Biner Karakter

No	Karakter	Desimal	Biner	Jumlah Bit
1	P	80	01010000	8
2	U	85	01010101	8
3	J	74	01001010	8
4	A	65	01000001	8
5	U	85	01010101	8
6	I	73	01001001	8
7	N	78	01001110	8
8	S	83	01010011	8
9	U	85	01010101	8
Total Bit				72 Bit

2. Data Audio Sampel

penelitian ini memanfaatkan aplikasi *HxD Hex Editor* yang secara otomatis dapat mengubah audio wav menjadi bilangan hexa untuk perhitungan manual. Cukup masukkan audio wav ke dalam aplikasi, dan nilai hexa dari audio wav akan muncul.



Gambar 6. Nilai Hexa Audio Sampel

Contoh nilai 72 byte diambil dalam bentuk heksagonal dan diubah menjadi bentuk biner sesuai dengan tabel di bawah ini, yang didasarkan pada Gambar 6 :

Tabel 3. Nilai Biner Audio Sampel

No	Audio Objek		
	Hexa	Des	Biner
1	52	82	01010010
2	49	73	01001001
3	46	70	01000110
4	46	70	01000110
5	24	36	00100100
6	60	96	01100000
7	28	40	00101000
8	00	00	00000000

.....Sambungan Seterusnya sampai 72 bit

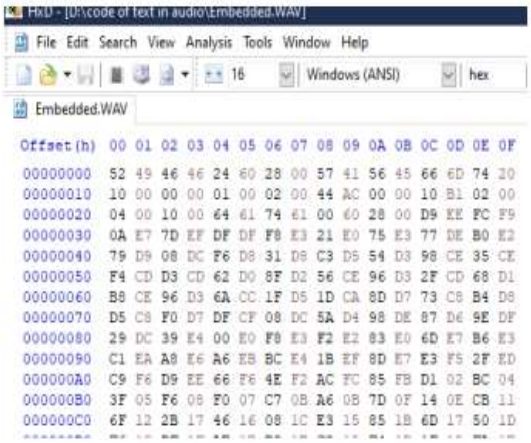
64	E2	226	11100010
65	82	130	10000010
66	D9	217	11011001
67	01	01	00000001
68	DC	220	11011100
69	F7	247	11110111
70	D8	216	11011000
71	22	34	00100010
72	D8	216	11011000

Berdasarkan tabel 3 diatas, didapat nilai biner dari audio sampel yang akan dijadikan objek *placeholder* pada teks karakter“PUJAUINSU”

3.3 Hasil Analisis Data

1. Proses Penyisipan DCT

Langkah selanjutnya adalah menggunakan metode *Discrete Cosine Transform* untuk melakukan proses penyisipan setelah menemukan nilai biner sampul audio dan nilai enkripsi teks karakter. Pada proses penyisipan Steganografi membutuhkan sebuah kunci Publik pada saat enkripsi yang berbentuk *.txt sebagai pembatas untuk ekstraksi bit biner dari audio wav di titik awal dan akhir.



Gambar 7. Sampel Audio Steganografi

Tabel 4. Proses Penyisipan Teks

No	C	Nilai Audio Cover			Nilai Bit Karakter
		Hex	Des	Biner	
1	80	52	82	01010010	0
2		49	73	01001001	1
3		46	70	01000110	0
4		46	70	01000110	0
5		24	36	00100100	0
6		60	96	01100000	0
7		28	40	00101000	0
8		00	00	00000000	0

Lanjutan Samping nilai bit karakter……

Nilai Audio Stegano		
Hex	Des	Biner
52	82	01010010
49	73	01001001
46	70	01000110
46	70	01000110
24	36	00100100
60	96	01100000
28	40	00101000
00	00	00000000

……..Sambungan Seterusnya

69	F7	247	11110111	0	D8	216	11011000
70	D8	216	11011000	1	31	49	00110001
71	22	34	00100010	0	D8	216	11011000
72	D8	216	11011000	1	C3	195	11000011

2. Proses Ekstraksi DCT

Diperlukan metode ekstraksi untuk mengambil data penyisipan teks terenkripsi pada objek audio wav setelah proses penyisipan. Tujuan dari proses ekstraksi adalah untuk menemukan teks yang tersembunyi atau disisipkan dalam audio wav. Pada proses ekstraksi kunci yang digunakan adalah kunci *private* yang disimpan dalam format *.txt yang di dapatkan pada saat awal pembangkitan kunci.

Tabel 5. Proses Ekstraksi Teks

No	Nilai Audio Stegano			Bit Data Teks	Cipher
	Hex	Des	Biner		
1	52	82	01010010	0	80
2	49	73	01001001	1	
3	46	70	01000110	0	
4	46	70	01000110	0	
5	24	36	00100100	0	
6	60	96	01100000	0	
7	28	40	00101000	0	
8	00	00	00000000	0	

……..Sambungan Seterusnya

69	D8	216	11011000	0	
70	31	49	00110001	1	
71	D8	216	11011000	0	
72	C3	195	11000011	1	

Sistem kemudian akan mengembalikan teks asli dengan mendekripsi hasil ekstraksi setelah dilakukan. Tabel di bawah memberikan ilustrasi tentang bagaimana deskripsi ini :

Tabel 6. Perhitungan Proses Dekripsi

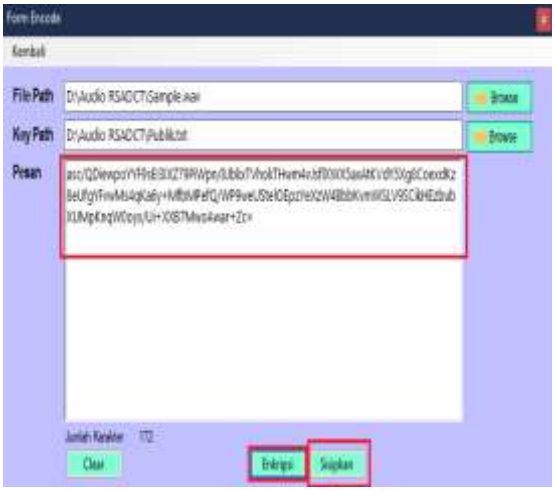
No	Cipher (C)	N	D	P = C_i^d mod N
1	80	1073	337	80
2	85	1073	337	85
3	74	1073	337	74
4	761	1073	337	65
5	85	1073	337	85
6	73	1073	337	73
7	252	1073	337	78
8	460	1073	337	83
9	85	1073	337	85

3.4 Hasil Pengujian

Sesuai dengan desain dan perhitungan manual yang dibuat dalam mengenkripksi, menyisipkan, mengekstraksi dan dekripsi pesan teks pada audio wav menggunakan Metode Kriptografi RSA dan Steganografi DCT, Kemudian terapkan aplikasi perangkat lunak. Proses implementasi aplikasi ini meliputi langkah-langkah berikut: pembangkitan kunci, mengenkripksi, menyisipkan, mengekstraksi dan mendeksripsi kan kembali pesan asli. Penerapan dalam aplikasi adalah sebagai berikut :

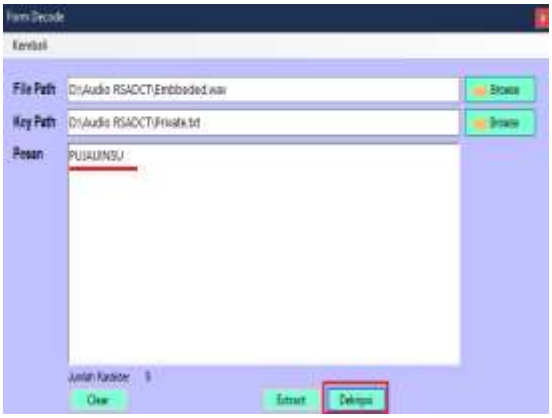
Gambar 8. Tampilan *Generate Key*

Pada gambar 8 diatas, adalah tampilan saat mengambil kunci publik dan privat, kemudian masing-masing kunci disimpan.



Gambar 9. Tampilan Enkripsi & Sisip Pesan

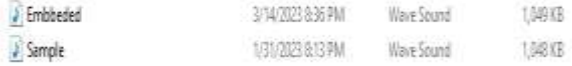
Gambar 9 menunjukkan tampilan saat memilih *file* audio dengan format *.wav, kemudian mengambil kunci publik yang telah disimpan, lalu ketik pesan yang ingin disisipkan kemudian klik enkripsi dan sisipkan.



Gambar 10. Tampilan Pesan Dekripsi

Pada gambar 10, klik *browser* untuk mengambil file audio yang sudah disisipkan pesan, kemudian pilih kunci publik yang sudah disimpan lalu klik ekstrakuntuk menampilkan pesan yang di enkripsi kemudian klik dekripsi untuk menampilkan pesan teks asli.

Berikut perbandingan ukuran audio wav sebelum dan sesudah ditambahkan pesan :



Gambar 11. Perbedaan Sebelum dan Sesudah disisipi Pesan

Berdasarkan gambar diatas, terdapat sedikit perbedaan audio wav pada saat sebelum dan sesudah disisipkan, terlihat bahwa saat disisipkan pesan ukuran audio Stegano naik 1kb. Tidak signifikan, yang berarti tidak

terlalu banyak perubahan pada audio tersebut. Aplikasi Spektrum dapat digunakan untuk menguji frekuensi suara audio sebelum dan sesudah memasukkan pesan teks, seperti yang ditunjukkan pada gambar :

Gambar 12. Spektrum sesudah dan sebelum disisip pesan

Tabel 7. Hasil Pengujian Penyisipan

Nama File		Ukuran Data		Keterangan
Audio *Cover*	Audio Stegano	Audio *Cover*	Audio Stegano	
Sample .wav	Embbeded.wa v	1048kb	1049kb	Berubah
Sample 1.wav	Embbeded1.w av	2585kb	2585kb	Tidak Berubah
Sample 2.wav	Embbeded2.w av	2203kb	2203kb	Tidak Berubah
Sample 4.wav	Embbeded3.w av	3304kb	3304kb	Tidak Berubah

Berdasarkan Tabel 7 diatas, audio Stegano yang disisipkan pesan teks mengalami sedikit perubahan pada ukuran audio wav 1 mb sedangkan pada ukuran audio 2 mb keatas tidak mengalami perubahan ukuran sekalipun disisipkan pesan teks. Berikut adalah hasil dari pengujian proses ekstraksi :

Tabel 8. Hasil Pengujian Ekstraksi – Dekripsi

Nama File		Pesan Teks	Keterangan
Audio *Cover*	Audio Stegano		
Sample.wav	Embbeded.wav	PUJAUINSU	Berhasil
Sample1.wav	Embbeded1.wav	Kitabisa1	Berhasil
Sample2.wav	Embbeded2.wav	@Kominfo1-6	Berhasil
Sample4.wav	Embbeded3.wav	Cobateslagi.	Berhasil

Berdasarkan pada tabel 8 diatas, pesan teks berhasil diekstraksi dan didekripsikan kembali ke pesan teks asli nya.

Tabel 9. Pengujian *Blackbox*

Pengujian	Target Pengujian	Pengamatan	Kesimpulan
Tombol *Generate* Kunci	Menampilkan kunci publik dan *privatte* pada masing-masing *textbox*	Berhasil menampilkan kunci dan menyimpan masing-masing kunci publik dan *private* yang telah diperoleh	Pengujian Berhasil (Valid)
Tombol *Browse*	Menampilkan *file explorer*, menampilkan nama *file*, dan menampilkan lokasi audio yang dipilih, serta memilih kunci publik untuk enkripsi dan kunci private untuk proses dekripsi	Berhasil mengambil Audio wav, kunci publik kemudian mengetik pesan dan kunci private untuk mengekstraksi	Pengujian Berhasil (Valid)
Tombol Enkripsi	Menampilkan karakter pesan yang sudah dienkripsi menjadi karakter yang tidak dipahami	Berhasil mengenkripsi dan menampilkan karakter yang tidak bermakna	Pengujian Berhasil (Valid)
Tombol Sisipkan	Menampilkan *file explorer* untuk membuat nama *file* dan menyimpan audio Stegano	Berhasil menyimpan *file* audio Stegano yang sudah tersisipi pesan	Pengujian Berhasil (Valid)
Tombol *Extract*	Menampilkan hasil ekstraksi pesan yang sudah dienkripsi	Berhasil menampilkan pesan yang terenkripsi	Pengujian Berhasil (Valid)
Tombol Dekripsi	Menampilkan pesan yang sudah terekstrak	Berhasil mengembalikan pesan teks asli	Pengujian Berhasil (Valid)

4. KESIMPULAN

Berdasarkan hasil analisis, perancangan dan pengujian sistem dengan menggunakan metode Kriptografi RSA

dan Steganografi DCT untuk melindungi pesan teks yang tersembunyi pada audio wav, maka dapat disimpulkan bahwa :

1. Sistem aplikasi yang dibangun mampu mengombinasikan Kriptografi RSA dengan Steganografi DCT, Pesan teks dapat dilindungi dengan Steganografi pada audio wav dan mampu dikembalikan seperti semula
2. Sistem aplikasi yang dibangun mampu melakukan pengamanan berupa enkripsi, penyisipan, ekstraksi dan dekripsi pesan rahasia pada file audio dengan baik, sehingga tidak mengubah makna dan informasi yang ada di dalamnya
3. Berdasarkan pengujian diketahui penambahan 1kb ukuran file audio Stegano terjadi ketika size audio cover berukuran 1mb, yang awalnya ukurannya 1048kb setelah disisipkan pesan menjadi 1049kb, setelah dilakukan pengujian untuk audio size 2mb keatas tidak ada perubahan kapasitas sama sekali pada audio setelah disisipkan pesan dan kualitas suara sebelum dan sesudah disisipkan pesan tidak ada perubahan. Pesan yang disisipkan pada audio tidak mempengaruhi output.

5. REFERENCES

[1] I. Rusydi, Z. Agustiana, and W. Satria, "Sosialisasi Dalam Mengantisipasi Kejahatan Internet Di Era Internet of Think Dan Revolusi Industri 4.0," *RESWARA J. Pengabdi. Kpd. Masy.*, vol. 1, no. 2, pp. 129–135, 2020, doi: 10.46576/rjpkm.v1i2.581.

[2] N. Siregar and A. Usman, "Penerapan Algoritma Kriptografi Hybrid Subtitusi dan Transposisi Spiral Dalam Mengamankan Data Teks," vol. 6341, no. April, pp. 81–90, 2021.

[3] S. Nada, "Pada Pengamanan File Teks," vol. XVI, no. Januari ISSN:2301-9425, pp. 55–60, 2017.

[4] A. Harbani and M. A. Fahreza, "Aplikasi Keamanan Data Gambar Menggunakan Algoritma RSA (Rivest Shamir Adleman) Berbasis Desktop," *Teknois J. Ilm. Teknol. Inf. dan Sains*, vol. 9, no. 1, pp. 1–9, 2019, doi: 10.36350/jbs.v9i1.1.

[5] F. Sidik, wamiliana wamiliana, and F. Eka Febriansyah, "Perbandingan Metode Adaptive Minimum Error Least Significant Bit Replacement (Amelsbr) Dan Discrete Cosine Transform (Dct) Untuk Steganografi Citra Digital," *J. Komputasi*, vol. 6, no. 1, pp. 43–53, 2018, doi: 10.23960/komputasi.v6i1.1563.

[6] A. S. Pratama and I. M. Suartana, "Analisis Kualitas Stego Video dalam Penyisipan Data Memanfaatkan Metode DCT-DWT," *J. Inf. Eng. Educ. Technol.*, vol. 5, no. 1, pp. 13–18, 2021, doi: 10.26740/jieet.v5n1.p13-18.

[7] D. P. Yudha, K. A. Baihaqi, and B. I. Hasbi, "Penyisipan Pesan Rahasia Pada Citra Gambar Dengan Teknik Steganografi Dan Algoritma Asimetris Enkripsi Rivest Shamir Adleman (Rsa)," *Techno Xplore J. Ilmu Komput. dan Teknol. Inf.*, vol. 4, no. 1, pp. 1–6, 2019, doi: 10.36805/technoxplore.v4i1.538.

[8] B. Kuniadi, D. Puspitaningrum, and F. F. Coastera, "Perancangan Dan Pembuatan Aplikasi Steganografi Pesan Teks Pada Audio Digital Dengan Metode Least Significant Bit," *J. Rekursif*, vol. 5, no. 3, pp. 285–297, 2017.

[9] J. K. Azhar and S. Yuliany, "Implementasi Algoritma RSA (Rivest , Shamir dan Adleman) Untuk Enkripsi dan Dekripsi File .pdf," no. December, 2019.

[10] P. Pristiwanto and Abdul Halim Hasugian, "Steganography Formation by utilizing Enhanced Least Significant Bit Algorithm," *J. Info Sains Inform. dan Sains*, vol. 11, no. 1, pp. 19–22, 2021, doi: 10.54209/infosains.v11i1.38.

[11] M. K. Ridwan, W. F. Pattipeilohy, and S. Sanwani, "Aplikasi Keamanan Document Digital Menggunakan Algoritma Steganografi Discrete Cosine Transform (Dct) Pada Perusahan Alat Berat," *JITK (Jurnal Ilmu Pengetah. dan Teknol. Komputer)*, vol. 5, no. 2, pp. 177–182, 2020, doi: 10.33480/jitk.v5i2.1033.

[12] E. W. Purwanto and S. S. S. T, "Algoritma Kriptografi El-Gamal Untuk Pengamanan Pesan Pada Steganografi Citra Domain Discrete Cosine Transform Dengan Teknik Penyisipan Least Significant Bit," *e-Proceeding Eng.*, vol. 5, no. 1, pp. 116–123, 2018.

[13] A. Malvi and P. Painem, "Pengamanan File Gambar pada Media Video dengan Kriptografi Algoritma RSA dan Steganografi Algoritma End of File (EOF)," *Inform. J. Ilmu Komput.*, vol. 16, no. 2, p. 67, 2020, doi: 10.52958/iftk.v16i2.1860.