Jurnal: Elektrika Borneo (JEB)
Vol. 6, No. 2, Oktober 2020, hlm. 48-53 p-ISSN: 2443-0986

PERANCANGAN ENKRIPSI KEAMANAN DATA MENGGUNAKAN METODE LEAST SIGNIFICANT BIT DENGAN TEKNIK MODIFIKASI RANDOM DATA ENCRYPT ALGORITHM UNTUK AUDIO STEGANOGRAPHY

Tengku Musri[1], Awang Pradana[2]

[1]*Politeknik Negeri Bengkalis, Bengkalis, Riau, Indonesia*
[2]*Universitas Borneo Tarakan,Tarakan,Kalimantan Utara, Indonesia*

[1]musri@polbeng.ac.id
[2]awang.prada@borneo.ac.id

Abstract—Technological developments in the field of delivery media are growing very rapidly, as well as the data security side of the media to be conveyed.There are many ways to protect very important or confidential data that will be conveyed without any third person knowing what the confidential data contains.By applying the field of steganography as a technique that is commonly used where the concealment of secret messages on the carrier media is very difficult or cannot be known by third parties. However, from the steganalysis side, it can easily solve secret messages that have entered the steganography category without any additional encryption or filters. Without additional filters or encryption, this steganographic technique is not sufficient to fulfill the security of the secret message. Therefore, this study will implement an encryption which in previous studies using encryption algorithms DES (Data Encrypt Standard). In the DES encryption method, the function of addition or evolution of DES encryption is applied, namely RDEA (Random Data Encrypt Algorithm). This research also expects maximum results so that it is not easily threatened from brute force attacks or from the threat of steganalysis even though there has been a decrease or increase in the capacity of the audio file.

Keywords—Least Significant Bit, RDEA Modification, Encryption, Data Security, Audio Stegranography

Intisari—Perkembangan teknologi pada bidang media penyampaian berkembang sangat luar biasa pesat, begitu juga dengan sisi pengamanan data pada media yang akan disampaikan. Banyak cara untuk melindungi data yang sangat penting atau rahasia yang akan di sampaikan tanpa ada orang ketiga yang mengetahui apa isi data rahasia tersebut. Dengan menerapkan Bidang ilmu dari steganografi sebagai teknik yang biasa digunakan dimana penyembunyian pesan rahasia pada media *carrier* sehingga sangat sulit atau tidak dapat diketahui oleh pihak ketiga. Akan tetapi dari pihak steganalisis dapat dengan mudah memecahkan pesan rahasia yang telah masuk ke kategori steganografi tanpa adanya enkripsi ataupun filter-filter tambahan. Tanpa adanya filter tambahan atau enkripsi teknik steganografi ini belum cukup untuk memenuhi keamanan dari pesan rahasia tersebut. Oleh karena itu pada penelitian ini akan menerapkan suatu enkripsi dimana pada penelitian sebelumnya menggunakan algoritma enkripsi DES (Data Encrypt Standard). Pada metode enkripsi DES akan diterapkan fungsi penambahan atau evolusi dari enkripsi DES yaitu RDEA (Random Data Encrypt Algorithm). Penelitian ini juga mengharapkan hasil yang maksimal agar tidak mudah terancam dari serangan brute force attack maupun dari ancaman steganalisis meskipun telah terjadi penurunan ataupun kenaikan kapasitas dari file audio tersebut.

Kata Kunci—Least Significant Bit, Modifikasi RDEA, Enkripsi, Keamanan Data, Audio Stegranography

I. PENDAHULUAN

Steganografi adalah teknik dari data yang telah tersisipkan atau tersembunyi pada suatu media tertentu. Asal dari kata steganografi sendiri diambil dari Bahasa yunani yaitu "stegos" yang berarti "tertutup" dan "grafia" yang berarti "menulis" oleh karena itu dapat diartikan sebagai penulisan secara tersembunyi. Tujuan utama mengapa adanya teknik steganografi ini adalah menyembunyikan pesan rahasia dan tidak dapat diketahui oleh pihak ketiga, sehingga pihak pertama sebagai pengirim dan pihak kedua sebagai penerima dapat saling menyampaikan pesan ataupun sebaliknya[1]. Pesan yang akan digunakan sebagai media carier bisa berbentuk gambar, audio, video, file teks dan begitu juga dengan pesan yang tersembunyi.

Dalam teknik penyisipan steganografi biasanya sering dikaitkan dengan ilmu dari kriptografi. Teknik dari kriptografi sendiri merupakan cara mempelajari sesuatu yang tersembunyi pada media, sehingga pesan yang akan tersisipkan tersebut tidak mudah untuk diketahui oleh pihak ketiga[2]. Kriptografi mempunyai dua bagian yang penting, yaitu enkripsi dan dekripsi. Enkripsi adalah proses penerapan encoding pada sebuah pesan, dimana proses tersebut akan mentransformasikan pesan asli atau plain text menjadi output biasa disebut sebagai chipertext. Dekripsi adalah fungsi untuk mentransformasikan *ciphertext* kembali menjadi *plaintext*[3]. Aspek-aspek keamanan dalam kriptografi merupakan penambahan yang diusulkan pada penelitian ini. Tekait dengan tujuan apa saja aspek-aspek keamanan pada kriptografi sebagai berikut[4]. a) *Authentication* (otentikasi), yaitu pada penerima pesan dapat memastikan keaslian pengirimanya sedangkan otentikasi dari sisi penyerang tidak dapat berpura-pura menjadi penerima ataupun pengirim pesan. b) *Confidentiality* (kerahasiaan) yaitu layanan yang ditujukan untuk menjaga pesan tidak dapat dibaca oleh

pihak yang tidak terkait. c) *Integrity* (data integritas) yaitu pada penerima pesan harus dapat memeriksa apakah pesan ini telah dimodifikasi atau tidak, pada saat pesan dalam proses pengiriman, dan. d) Non-*repudiation* (peyangkalan) yaitu pengirim pesan tidak dapat mengelak bahwa dia yang telah mengirimkan pesan sedangkan pada penerima juga tidak dapat menyangkal bahwa dia telah menerima pesan rahisa tersebut.

Dalam hal penelitian tentang teknik enkripsi yang berkembang dengan melibatkan fungsi-fungsi matematis dengan penambahan pada input yang disebut dengan kunci atau *key*, agar tidak mudah di deksripsi seandainya algoritma enkripsinya diketahui. Secara umum dikenal dua macam metode enkripsi, yaitu simetris dan asimetris. Enkripsi simetris sebuah *key* yang sama digunakan baik untuk mengenkrip maupun mendekripsi data. Sedangkan enkripsi asimetris, proses enkripsi dan dekripsi masing-masing menggunakan *key* yang berbeda, namun kedua *key* tersebut saling berpautan secara matematis.

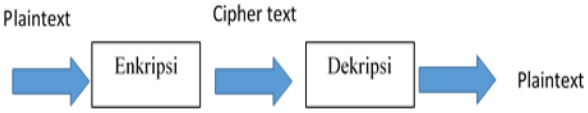
Penelitian ini menggunakan file audio sebagai *cover* dan teks sebagai pesan yang akan disisipkan, mengapa menggunakan file audio? Karena salah satu dari media carrier yang baik untuk steganografi dan juga mempunyai tingkat redudansi yang baik. Steganografi pada umumnya dapat memenuhi tiga persyaratan utama, yaitu imperceptibility, perolehan data yang tepat setelah dilakukannya teknik embedding dan kapasitas yang tidak terlalu melebihi ambang batas. Steganografi audio pada penelitian ini menggunakan teknik dari LSB (least Significant Bits) merupakan teknik paling sederhana yang biasa digunakan. Didalam teknik ini, LSB menyembunyikan sedikit data pada sample audio, kepentingan LSB pada saat penggabungan sangat kecil. Namun LSB sendiri akan memberikan noise pada audio sehingga akan sangat mudah di ketahui bahwa audio ini telah disisipkan teknik dari steganografi[5]. Apabila noise meningkat dari ambang batas yang ditentukan maka akan sangat mudah terdeteksi menggunakan teknik steganalysis, maka otomatis teknik tersebut gagal, dengan adanya teknik enkripsi dapat membantu agar media carrier sebagai audio ini tidak mudah untuk dicurigai.

Maka dari itu, pada penelitian ini akan mengusulkan adanya teknik dari enkripsi RDEA (R*andom Data Encrypt Algoritm*[6]. dengan beberapa modifikasi dalam alur algoritma yang dikembangkan dari enkripsi DES (*Data Encrypt Standard*). Adapun struktur alur penjelasan pada penelitian ini sebagai berikut. Bagian II akan memberikan penjelasan tentang permasalahan pada algoritmanya. Bagian III adalah rancangan metodelogi yang akan diusulkan. Bgaian IV skenario proses. Bagian V merupakan referensi dari penulisan penelitian ini.

II. LANDASAN TEORI

Steganografi merupakan teknik yang paling sering digunakan untuk mengamankan data, tetapi bukan berarti tidak mudah untuk dipecahkan[7]. Steganalisis merupakan teknik yang menganalisa apakah media carrier tersebut memiliki pesan rahasia atau tidak. Dengan adanya tambahan pada teknik steganografi dapat menyulitkan bagi steganalisis untuk memecahkan pesan rahasia tersebut.

Kriptografi biasanya sering dikaitkan dengan teknik steganografi. Secara umum, kriptografi merupakan teknik pengamanan informasi yang dilakukan dengan cara mengolah informasi awal atau biasa yang disebut dengan *plaintext* suatu kunci tertentu sehingga menghasilkan suatu informasi biasa disebut dengan *ciphertext* yang tidak dapat dibaca secara langsung[7]. *Ciphertext* dapat kembali menjadi informasi awal atau disebut dengan *plaintext* melalui proses dekripsi. Urutan proses melakukan kriptografi pada umumnya dapat dilihat pada gambar 1.



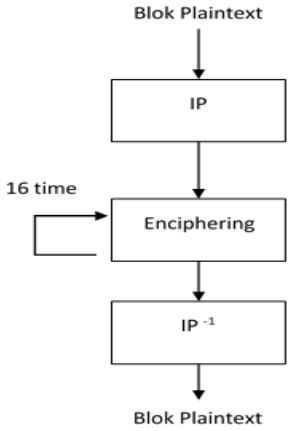
Gambar 1. Proses Kriptografi

Kriptografi menggunakan algoritma DES dianggap kurang aman dalam melakukan enkripsi hal ini dikarenakan panjang ukuran bit yang digunakan terlalu kecil. Pada bulan januari 1999, distribute.net dan *Electronic Frontier Foundation* bekerjasama untuk memecahkan kunci algoritma DES hanya dalam waktu 22 jam 15 menit dan masih banyak lagi yang melakukan analisis macam-macam kelemahan pada cipher DES, oleh karena itu kami mengajukan suatu algoritma baru yang merupakan implementasi dari algoritma DES yaitu Random Data Encrypt Algorithm (RDEA), dimana pada saat pesan rahasia sebelum di *enhanced* akan di enkripsi terlebih dahulu menggunakan RDEA tersebut[8].
Pada algoritma simetris terdapat beberapa macam aplikasi yang bisa digunakan untuk meng-enkripsi ataupun dekripsi salah satunya yang digunakan pada penelitian ini yaitu : Data Encryption Standard (DES) dan Random Data Encryption Algorithm (RDEA)[4][9].

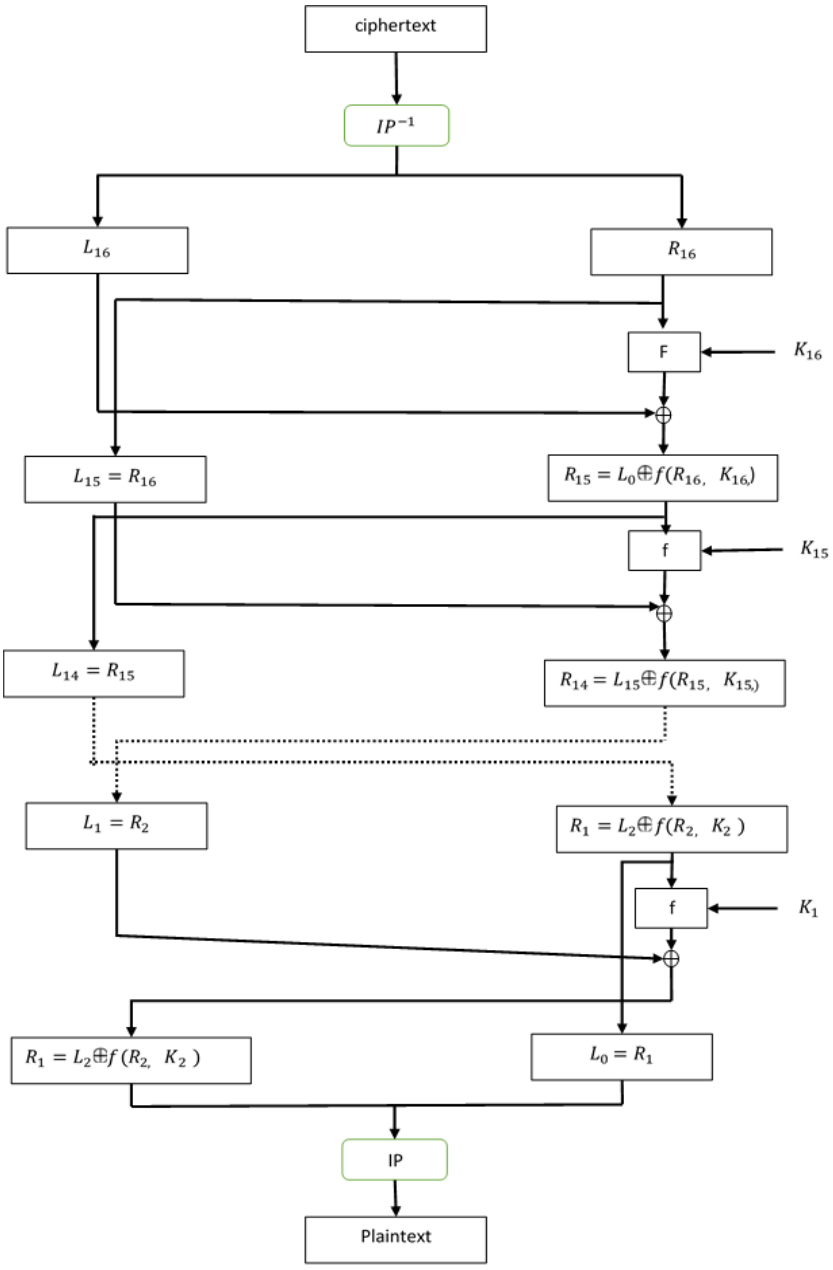
A. *Data Encryption Standard* (DES)

Merupakan suatu blok cipher yang mempunyai serangkaian panjang bit dan mengubah plaintext melalui serangkaian operasi rumit ke bit string ciphertext yang sama dengan panjang bitnya. DES menggunakan kunci yang menyesuaikan dari sisi transformasi biasanya ukuran blok pada DES sendiri adalah 64 bit. Sehingga dapat dilakukan oleh orang-orang yang mengetahui kunci yang digunakan untuk mengenkripsi, dari 64 bit hanya 56 bit panjang kunci yang efektif di antaranya yang terpakai oleh algoritma, sisanya delapan bit tersebut digunakan hanya untuk memeriksa paritas. Simulasi pada DES secara global dapat dilihat Pada gambar 2. DES merupakan algoritma yang beroperasi pada ukuran 64 bit *ciphertext* dengan menggunakan 56 bit kunci internal dan kunci eksternal sebagai pembuat yang panjangnya 64 bit, dan gambar 3. Menunjukan skema dasar dari proses enkripsi algoritma DES, blok *plaintext* dipermutasi dengan matriks permutasi awal (*initial permutation*), kemudian hasil dari permutasi awal di *ecnchipering* sebanyak 16 kali atau 16 putaran[4][10]. Setiap putaran menggunakan kunci internal yang berbeda. Hasil dari *enchipering* kemudian dipermutsi dengan matriks

permutasi balikan (*invers initial permutation*) menjadi blok *ciphertext*.



Gambar 2. Skema proses algoritma DES



Gambar 3. Skema Dasar Algoritma DES

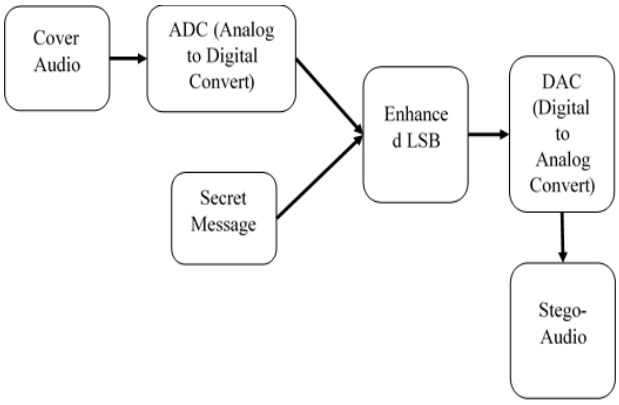
B. *Random Data Encrypt Algorithm* (RDEA)

Merupakan implementasi evolusi dari algoritma DES, fitur yang membedakan antara RDEA dan DES yaitu penggunaan pseudo acak pada kunci cipher di dalam algoritma enkripsi dan membuat pembentukan protokol baru pada kunci cipher yang tertanam dalam teks cipher. Teknik dari RDEA ini mengubah secret *key* yang ada pada setiap blok yaitu pada secret *key* yang memiliki panjang 128 *byte* sampai dengan 256 *byte* atau bisa tergantung dengan sistem memori yang tersedia[8], sehingga dapat menghasilkan jumlah maksimum cipher *key*. Secret *key* dipilih secara acak sehingga akan menambah kompleksitas dari serangan *brute force attack*.

III. METODE PENELITIAN

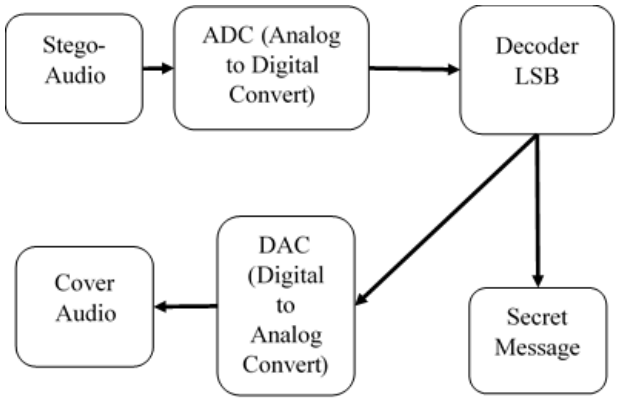
LSB merupakan teknik paling sederhana untuk melakukan penyisipan pada *cover* audio yang menghasilkan stegano audio dan mempunyai kapasitas yang tinggi. Pada teknik ini merupakan proses dimana pesan rahasia akan disisipkan pada *cover* audio yang dapat menyebabkan kebisingan atau *noise* yang sangat mudah terdeteksi apabila melewati ambang batas kapasitasnya[1]. Ini disebabkan oleh meningkatnya jumlah bit yang telah tersisipkan. Apabila kebisingan melewati ambang batas maka akan mudah terdeteksi oleh teknik steganalisis dan menyatakan bahwa *cover* audio ini adalah hasil dari stegano audio. Pada penelitian metode LSB sebelumnya dijelaskan bahwa menggunakan sample bit secara berlebih dapat meningkatkan kapasitas dan mengurangi transparasi begitu juga sebaliknya.

Gambar 4. Merupakan proses dimana teknik penggabungan pada metode LSB tanpa menggunakan fitur penambahan. Dari *cover* audio yang berbentuk analog diubah ke bentuk digital melewati proses ADC (*Analog-to-Digital Converter*). Setelah itu, proses LSB pada *cover* audio yang berbentuk digital akan digabungkan dengan pesan rahasia. Untuk menghasilkan stego audio, Hasil dari penggabungan akan diubah lagi menjadi sinyal analog melewati proses DAC (*Digital-to-Analog*).



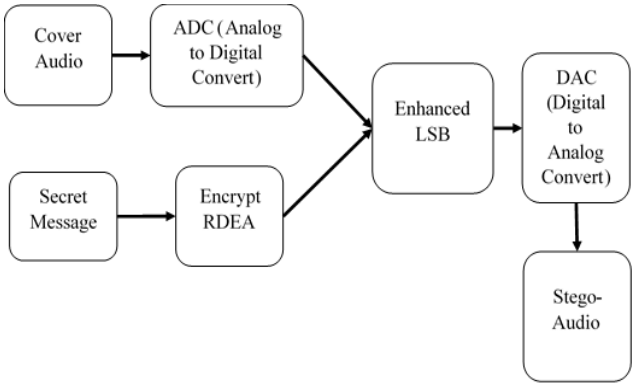
Gambar 4. Proses Penggabungan Steganografi Audio

Gambar 5. Merupakan alur dari proses dari teknik decoder. Hasil stegano audio yang berbentuk analog diubah menjadi bentuk digital melewati proses DAC, kemudian pada proses LSBs decoder akan mendapatkan data berupa *cover* audio dan pesan rahasia yang sebelumnya sudah disisipkan.



Gambar 5. Proses *Decoder* steganografi audio

Pada metodelogi penelitian sebelumnya telah diusulkan *cover* audio telah melewati proses sebelum penggabungan dilakukan yaitu pada proses ADC dimana frekuensi dari *cover* audio bernilai 8000 sampel/detik dan mengandung jumlah 8 bit per masing-masing sampel. Selain itu penelitian sebelumnya juga menggunakan enkripsi AES 256 untuk mengenkripsi data dari pesan rahasia yang akan disisipkan. Pada penelitian ini akan berimprovisasi pada bagian enkripsi kriptografi data di pesan rahasia dengan menggunakan algoritma dari RDEA, yang mana algoritma ini merupakan pengembangan dari algoritma DES. Gambar 6. Menampilkan alur penerapan pada stegano audio yang menggunakan enkripsi algoritma dari RDEA.



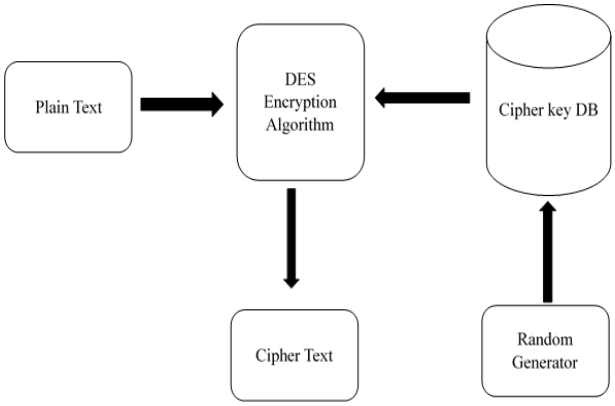
Gambar 6. Konsep yang diusulkan Steganografi menggunakan algoritma enkripsi RDEA

IV. HASIL DAN PEMBAHASAN

Skenario alur penerapan steganografi yang diusulkan sebagai berikut. Data *cover audio* yang berbentuk analog akan diubah ke bentuk digital melewati proses ADC (*Analog-to-Digital Converter*). Setelah itu, proses LSB pada *cover* audio yang berbentuk digital akan digabungkan dengan pesan rahasia. Pada alur pesan rahasia dimana proses sebelum menggabungkan dengan data *cover*, akan memasuki tahap proses dari enkripsi RDEA Untuk menghasilkan stego audio, Hasil dari penggabungan akan diubah lagi menjadi sinyal analog

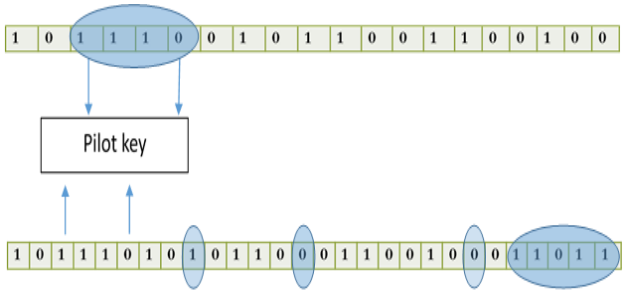
melewati proses DAC (*Digital-to-Analog*). Dalam kasus algoritma steganografi *break*, menggunakan algoritma tambahan pada pesan rahasia yang ter-enkripsi akan membuat pesan rahasia tidak mudah dipecahkan oleh penyusup yang melakukan steganalisis[1].

Pada gambar 7. Akan dijelaskan bagaimana cara kerja dari algoritma enkripsi RDEA. Pesan rahasia yang akan di enkripsi disini bernama *plain text*, dari *plaintext* ini akan di dapatkan dua data yaitu *cipher key* dan *cipher text.* proses dari *cipher key* digunakan untuk menyisipkan beberapa bit ke dalam *plaintext*, *cipher key* ini dihasilkan dari *random generator* yang kemudian akan disimpan ke *cipher key DB*. Dari *cipher key DB* akan memberikan jumlah bit tertentu pada *plaintext* yang akan disisipkan melalui enkripsi algoritma DES. Setelah penggabungan dari algoritma tersebut maka menghasilkan *cipher text*, yang mana cipher text ini merupakan bentuk dari pesan rahasia yang telah digabungkan dengan bit tertentu.



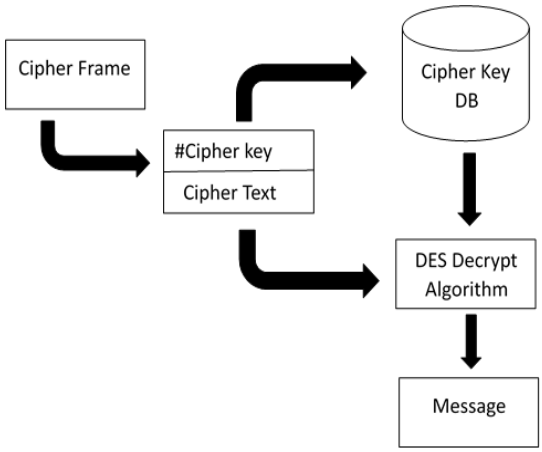
Gambar 7. Konsep enkripsi dari algoritma RDEA

Bagaimana cara kerja penggabungan enkripsi dari RDEA ini dapat dilihat pada contoh gambar 8. Contoh tersebut diambil dari penelitian *v. hassler* dimana susunan bit acak yang dihasilkan oleh *cipherkey db* akan disisipkan pada *plaintext*[8]. Contoh masukkan *plaintext* yaitu 1011 1001 0110 0110 0100 dan data *cipherkey* yang dihasilkan dari *random generator* adalah 1001 1011. Simulasi tugas dari DES dengan menyisipkan secara acak *pilot key* sebgai patokan untuk menyisipkan bit yang telah dihasilkan oleh *random generator*.



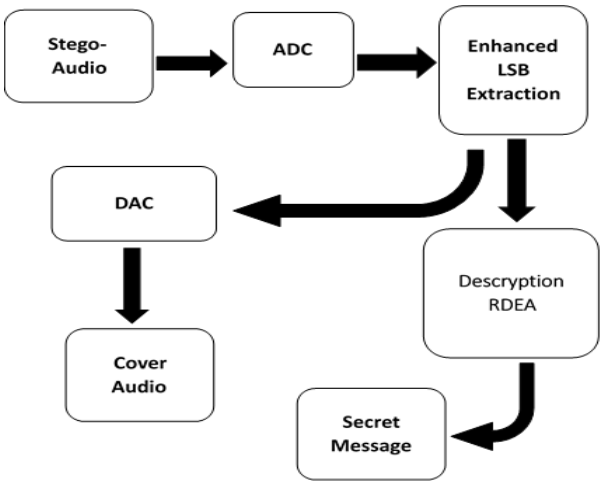
Gambar 8. Penyisipan secara acak pada enkripsi RDEA

Konsep selanjutnya bagaimana cara dekripsi menggunakan algoritma RDEA, pada penelitian *v.hassler* sudah memaparkan bagaimana cara men-dekripsikan dari hasil *ciphertext*.



Gambar 9. Konsep deskripsi alur pada RDEA

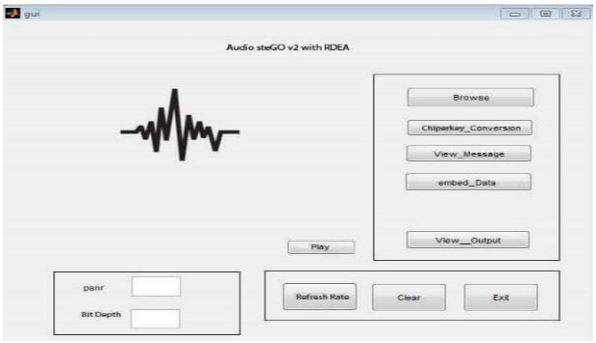
Gambar diatas menjelaskan *cipher frame* adalah *ciphertext*, dimana akan mendapatkan dua data yaitu *cipher key dan cipher text*. Dari *cipher key* akan disamakan dengan kunci dari *cipher key db* dimana kunci yang telah ditetapkan sama dengan kunci yang telah di set oleh *ciphertext*. Kemudian menggunakan algoritma DES akan melakukan proses *descryption* dan menghasilkan pesan rahasia yang sebelumnya telah di *encrypt*.



Gambar 10. Konsep *extraction* stegano audio

Gambar 10. Konsep proses dari ekstrasi stegano audio. Dari data stego audio kemudian memasuki proses dimana data tersebut akan diubah bentuk menjadi digital, melaui proses ADC (*analog – to – digital*) setelah mendapatkan data berbentuk digital maka data tersebut akan di proses pada LSB *extraction* kemudian didapatkan data media carrier dan data pesan rahasia yang telah di enkripsi. Untuk mendapatkan *cover* audio, data media *carrier* akan diubah menjadi analog dimana proses tersebut melewati DAC (*digital-to-analog*). Untuk mendapatkan pesan rahasia yang asli maka akan dilakukan proses deskripsi dimana data pada *ciphetext* akan diproses melalui deskripsi RDEA.

Pada gambar 11 memperlihatkan *Graphic User Interface* (GUI) rancangan aplikasi dari proses steganografi, dirancangan sedemikan rupa sehingga mudah digunakan.



Gambar 11. Rancangan (GUI) main menu

Tabel I
Hasil pengujian terhadap file audio dengan ekstensi .wav

No.	Data *Carrier*		Random Data Enrypt (*key*) dan pesan	Stegoaudio lsb dan RDEA (Kb)
	File Cover Audio	Kapasitas (Kb)		
1.	Jason Shaw - Snappy	992	10011011	1.320
2.	Jason Shaw - Jenny's Theme	895	10101011	1.237
3.	Jason Shaw - Morning	2.401	01101110	2.622

Hasil pengujian pada penelitian ini dilakukan dengan menggunakan device laptop HP AMD A4 5300 dan dengan menggunakan pemrograman Matlab 2010a, pada pengujian ini dilakukan dengan menggunakan 3 dataset *cover* audio[11],dengan file format WAV. Pada Tabel 1. diperlihatkan hasil eksperimen yang telah dilakukan, kemudian terlihat bahwa penggunaan least significant bit dan melalui proses deskripsi RDEA lebih cenderung mendukung pada format "WAV" dari beberapa penelitian serta dataset yang paling banyak digunakan, karena file wav ini terdiri dari format standar audio yang tak menyematkan representasi digital(uncomppressed) dalam pengertian yaitu pada suara asli[12].

V. KESIMPULAN

Banyak cara untuk meningkatkan hasil dari stego audio yang baik maka dipastikan bahwa LSB modifikasi memiliki jumlah fitur tambahan agar tidak mudah di analisis oleh sekelompok oknum yang tidak bertanggung jawab. Cara mengetahui apakah teknik penggabungan tersebut sudah cukup untuk mengamankan suatu pesan rahasia pada *cover* audio, yaitu dengan melakukan beberapa parameter perhitungan atau penilaian terhadap data yang telah menjadi stego audio. Berdasarkan analisa dari konsep deskripsi RDEA dapat ditarik kesimpulan bahwa hasil dari proses steganografi tidak menunjukan perubahan data carrier yang signifikan baik sebelum dan sesudah proses dari steganografi tersebut. Kemudian merupakan hal yang penting dalam memilih data *carrier* dalam hal ini yaitu audio, meskipun mengalami penurunan atau kenaikan dalam kapasitas audio secara kasat pendengaran manusia tidak dapat di deteksi atau sangat kecil kemungkinan untuk di curigai. Peneliti mengharapkan hasil yang maksimal agar tidak mudah terancam dari serangan brute force attack maupun dari ancaman steganalisis.

REFERENSI

[1] M. Asad, J. Gilani, and A. Khalid, "An Enhanced Least Significant Bit Modification Technique for Audio Steganography," *Univ. Eng. Technol. Taxila*, pp. 143–147, 2011.

[2] M. Baritha Begum and Y. Venkataramani, "LSB Based Audio Steganography Based On Text Compression," *Procedia Eng.*, vol. 30, no. 2011, pp. 703–710, 2012, doi: 10.1016/j.proeng.2012.01.917.

[3] A. Bhattacharya and S. Banerjee, "Reversible Data Encryption Algorithm," *CSE Dep. Herit. Inst. Technol. / Kolkata*, pp. 40–43, 2012.

[4] C. Liu, J. Ji, and Z. Liu, "Implementation of DES Encryption Arithmetic based on FPGA," *AASRI Procedia*, vol. 5, pp. 209–213, 2013, doi: 10.1016/j.aasri.2013.10.080.

[5] V. F. Ramadhani and B. Hidayat, "STEGANALISIS UNTUK FILE AUDIO BERFORMAT MP3 DENGAN METODE LEAST SIGNIFICANT BIT (LSB) PADA KLASIFIKASI PRINCIPAL COMPONENT ANALYSIS (PCA)," pp. 1–6, 2017.

[6] K. Gopalan, "Audio steganography using bit modification," *2003 Int. Conf. Multimed. Expo. ICME '03. Proc. (Cat. No.03TH8698)*, pp. I–629, 2003, doi: 10.1109/ICME.2003.1220996.

[7] A. Budi and A. Chicali, "ANALISIS PERBANDINGAN ALGORITMA KRIPTOGRAFI METODE DATA ENCRYPTION STANDARD DENGAN METODE ADVANCED ENCRYPTION SYSTEM (STUDI KASUS PADA PT. ONE STANDARD GROUP PTE LTD)," *J. Inform. dan Bisnis*, vol. 8, 2019.

[8] E. Algorithm, "FUndtim Data," *Twenty Second Natl. Radio Sci. Conf.*, no. Nrsc, 2005.

[9] K. Gopalan, "Audio Steganography by Cepstrum Modification," *Dep. Electr. Comput. Eng. Purdue Univ. Calumet*, vol. 4323, no. 3, pp. 481–484, 2005.

[10] R. Sridevi, "EFFICIENT METHOD OF AUDIO STEGANOGRAPHY BY MODIFIED LSB ALGORITHM AND STRONG ENCRYPTION," *Sch. Inf. Technol. JNTUH, Hyderabad*, 2009.

[11] L. D. P. W. E. and T. Bertin-Mahieux, "Dataset Audio." http://millionsongdataset.com/pages/additional-datasets/index.html.

[12] I. Kurniawan, "Implementasi dan Studi Perbandingan Steganografi pada File Audio WAVE Menggunakan Teknik Low-Bit Encoding dengan Teknik End Of File," *J. Informatics Technol.*, vol. 2, no. 3, pp. 0–11, 2013.