 ISSN:2302-8149
e-ISSN:2540-9719

Enkripsi dan Dekripsi Suara Menggunakan Metode *AES* 128b dengan *Secret Key*

Voice Encryption and Decryption Using AES 128b Method with Secret Key

Fajar Nugraha, Toni Arifin*
Teknik Informatika, Fakultas Teknik Informasi, ARS University
Jl. Sekolah Internasional No.1-2 Antapani Bandung Jawa Barat Indonesia
*e-mail: toni.arifin@ars.ac.id

Abstrak

Mengirim atau memperdagangkan informasi adalah sesuatu yang biasa terjadi di ranah inovasi data. Salah satu data yang biasa dilakukan pertukaran adalah suara. Suara biasanya digunakan untuk berkomunikasi. Informasi yang dikirimkan sesekali seringkali berisi informasi yang penting dan secara mengejutkan sangat pribadi dan harus tetap berhati-hati. Untuk menjaga keamanan informasi, mungkin dapat diselesaikan dengan menggunakan kriptografi. Salah satu teknik kriptografi adalah *Advanced Encryption Standard* atau biasa disebut AES. Terdapat 3 jenis AES yaitu: AES- 128, AES-192 dan AES-256. Pengiriman data melalui wireless kadang terdapat noise, sehingga data yang dikirimkan tidak sama dengan yang diterima. Untuk mengatasi hal tersebut dapat dilakukan dengan *Forward Error Correction* (FEC) yaitu metode yang mampu mengoreksi *error* dari informasi yang ditransmisikan. Untuk mengenkripsi informasi dari *audio* pada penelitian ini ditambahkan dan dicontrol oleh *Secret key Controller* dan *Interleaver* lain harus ditambahkan ke output dikendalikan oleh *Secret key Controller*. Penelitian ini bertujuan untuk melakukan kriptografi pada suara guna mengikuti keamanan informasi dengan memanfaatkan prosedur kriptografi Advanced Encryption Standard (AES) dengan parameter uji yaitu waktu, ukuran file dan nilai SNRnya. Hasil pada penelitian ini didapatkan enkripsi yang baik dengan rata-rata filter sebesar 400Hz.

Kata Kunci : AES, Enkripsi Suara, Dekripsi Suara

Abstract

Sending or exchanging data is something that often happens in the world of information technology. One of the data that is usually exchanged is voice. Voice is usually used to communicate. The data sent is sometimes important and even very confidential and must be kept safe. To maintain data security, it can be done using cryptography. One of the cryptographic techniques is the Advanced Encryption Standard or commonly called AES. There are three types of AES, they are AES-128, AES-192, and AES-256. Sending data via wireless sometimes there is noise, so the data sent is not the same as what is received. To overcome this, it can be done by forwarding Error Correction (FEC), which is a method that can correct errors from the transmitted information. To encrypt the information from the audio in this study added and controlled by the Secret key Controller and another Interleaver must be added to the output controlled by the Secret key Controller. This study aims to perform cryptography on voice to maintain data security by using the Advanced Encryption Standard (AES) cryptographic technique with test parameters namely time, file size, and SNR value. The results in this study obtained good encryption with an average filter of 400Hz.

Keywords : *AES, Voice Encryption, Voice Decryption*

1. Pendahuluan

Teknologi informasi sering dilibatkan dalam berbagai macam keperluan salah satunya yaitu pengiriman atau pertukaran informasi dan data [1]. Pengiriman atau pertukaran informasi salah satunya yaitu menggunakan media suara. Pada proses pengiriman suara yang berisi informasi penting tentunya perlu dijaga keamanannya dikarenakan informasi tersebut tidak bisa sembarangan diterima dan diketahui oleh orang yang tidak memiliki kepentingan. Upaya dalam menjaga keamanan informasi salah satunya dengan menyembunyikan informasi tersebut dengan teknik *cryptography* [2]. Teknik dalam *cryptography* yang dapat membantu menyembunyikan informasi adalah enkripsi. Enkripsi dapat menyembunyikan informasi sehingga ketika terdapat orang yang tidak berkepentingan mencoba mencuri akses tersebut, yang muncul bukanlah informasi sebenarnya melainkan informasi yang sudah dimodifikasi [3]. Informasi yang telah dimodifikasi atau dilakukan enkripsi selanjutnya akan dilakukan proses dekripsi ketika diterima oleh orang yang berkepentingan. Permasalahan pada proses dekripsi salah satunya yaitu terjadinya kerusakan data atau *noise* [4]. Penelitian sebelumnya pernah melakukan enkripsi dan dekripsi suara menggunakan Steganografi [5]. penelitian lain menggunakan *hybrid* dan menggunakan *voice recognition* tetapi masih menghasilkan noise pada proses dekripsinya. Metode yang diterapkan dalam penelitian ini yaitu metode *Advanced Encryption Standard* (AES) dimana metode ini sudah pernah dilakukan dalam proses enkripsi text tanpa menghasilkan *noise. Penelitian sebelumnya pernah juga menerapkan metode AES dalam enkripsi suara tetapi menggunakan 256 bit dan menggunakan Matlab* [6] *maka pada penelitian ini diterapkan AES menggunakan 128 Bit dan menggunakan bahasa pemrograman python.*

2. Tinjauan Pustaka

(Kriptografi) adalah ilmu dan keahlian menyimpan pesan, informasi, atau data dengan aman dan berencana untuk menjaga kerahasiaan data yang terkandung dalam informasi sehingga data tidak dapat diketahui oleh pihak yang tidak disetujui [7]. Sesuai dengan klasifikasi informasi, kriptografi mengubah informasi yang jelas (plaintext) menjadi ciphertext yang tidak dapat dikenali. Cipherteks ini kemudian dikirim oleh pengirim kepada penerima (*collector*). Setelah muncul di kolektor, ciphertext diubah lagi menjadi plaintext dengan tujuan agar cenderung diterima lagi. Jalannya perubahan dari plaintext ke ciphertext adalah siklus Encipherment (enkripsi), setelah itu akan ditransformasikan ciphertext kembali menjadi plaintext yang merupakan proses unscrambling (decoding). Untuk mengacak dan mengacak informasi, kriptografi menggunakan perhitungan (gambar) dan (kunci).[8]. Proses enkripsi dan penguraian ditangani oleh suatu tempat di sekitar satu kunci kriptografi. Selanjutnya keamanan pesan bergantung pada kunci atau kunci yang digunakan, dan bukan bergantung pada perkiraan dimanfaatkan. Sehingga perhitungan yang digunakan dapat diedarkan dan dianalisis, dan hal-hal yang menggunakan perkiraan tersebut dapat dibuat secara efektif [9]. Penelitian terdahulu perlu dijadikan acuan dalam penelitian ini, yaitu penelitian yang melakukan perhitungan AES (*Advanced Encryption Standard*) 256 siklus untuk mengacak dan mengacak dokumen perekam suara dan *Huffman Coding Algorithm* sebagai tekanan dokumen untuk mengurangi hasil rekaman enkripsi sehingga memori yang digunakan tidak terlalu besar. Hasilnya ialah perbedaan ukuran file enkripsi dan kompresi, sementara waktu interaksi enkripsi lebih lama dari proses penggambaran, biasa memakan waktu 18 detik untuk enkripsi dan 5 detik untuk dekripsi. Penelitian lain yang dijadikan acuan adalah penelitian dengan Strategi steganografi digunakan untuk menyembunyikan pesan yang bersifat misteri di media gambar yang terkomputerisasi. Apalagi untuk menambah kekuatan dalam menjaga kerahasiaan pesan, harus dibarengi dengan pemanfaatan perhitungan enkripsi. [10]. Mengingat studi penelitian masa lalu, ada kesamaan dan kontras dalam eksplorasi dipimpin. Persamaannya terletak pada strategi yang digunakan, baik memanfaatkan strategi kunci AES maupun menguji proses enkripsi dan decoding. Perbedaannya terletak pada panjang kunci yang digunakan dalam motede AES dan algoritma steganografi [11]. Pada penelitian kali inipun

melakukan perhitungan kualitas dari sebuah sinyal yang terganggu oleh derau. Secara luas digunakan untuk kerangka korespondensi. Sebuah media korespondensi sinyal data akan mengalami banyak hambatan atau (clamor), sehingga dapat merusak sinyal data dan akan mengalami keributan. penururan kualitasnya. Maka dari itu ditentukan nilai *Signal Noise to Ratio (SNR)* untuk menghitung estimasi nilai SNR berdasarkan nilai RMS tersebut dalam satuan desibel (dB) [12]. Lalu pada penelitian inijuga dilakukan proses *filtering* yang digunakan untuk mengeliminasi tentang frekuensi dari sinyal original. Umumnya filtering ini dirancang dalam rangkaian pasif yang diidentifikasikan oleh *cut frequency* [13] ada 2 jenis proses filtering ini yaitu low-pass filtering dan high-pass filtering. Dua jenis filter inilah yang paling penting, yang memungkinan frekuensi di bawah cut-recurrency pass, dengan demikian frekuensi di atas pengulangan irisan menurun secara dinamis ke tempat mereka sekarang tidak penting. Sedangkan *high-pass filtering* melakukan cara kerja yang sebaliknya dengan melewatkan frekuensi tinggi. *High-pass filtering* ini digunakan untuk menghilangkan getaran dengan frekuensi rendah, misalnya, yang diciptakan oleh langkah seniman yang direkam oleh penerima, atau getaran fondasi dari pendinginan. Sementara itu, pengayakan low-pass digunakan untuk membunuh keributan atau keributan berulang tinggi [14]. *Tools* pendukung yang menunjang pada penelitian kali ini yaitu Bahasa pemrograman python yang salah satu pemrograman komputer yang popular dan sering digunakan dalam melakukan perhitungan. Bahkan deklarasi suatu variabel dapat dilakukan secara langsung tanpa menyebutkan tipe datanya [15]. Pada Tabel 1 di bawah ini menjelaskan beberapa tinjauan jurnal yang dipakai sebagai acuan dalam penelitian kali ini, yaitu:

Tabel 1. Kesimpulan Tinjauan Jurnal

No	Judul	Peneliti	Hasil	Perbedaan	Persamaan
1.	Implementasi Algoritma *AES*-256B Dan Kompresi Pada Aplikasi *Voice Recorder*	Selvia Rahmawati, (2018)	Hasil yang didapat adalah kontras dalam enkripsi dan tekanan ukuran dokumen. Waktu proses enkripsi lebih lama daripada unscrambling.	Menggunakan 256 bit	Enkripsi *audio* Dan metode yang dipilih
2.	*Steganografi Dengan AES Pada Media Suara Berbasis Internet*	Rifki Indra Perwira , (2020)	Hasil yand didapat yaitu menyisipkan pesan di bit terakhir dari wadah.	Algoritma Steganografi	*AES* dan enkripsi suara
3.	Keamanan rekaman suara menggunakan kriptografi yippee rijndael dengan proses enkripsi dan penguraian	Kristin D R Sianipar, Septri Wanti Sihaan, Marina Siregar, Indra Gunawan (2018)	Dengan Algoritma Kriptografi Rijndael, proses enkripsi dan dekode pada arsip padat akan mempermudah klien untuk mengikuti legitimasi dokumen mereka. Kemudian, pada saat itu, juga perlu mengingat frasa rahasia yang kami buat selama siklus enkripsi.	Metode yang digunakan berbeda	Sama-sama mengenkripsi suara

 ISSN:2302-8149
e-ISSN:2540-9719

4.	Voice Recognition untuk Sistem Keamanan PC Menggunakan Metode MFCC dan DTW	Destian Tri Handoko, Patmi Kasih (2018)	Eksekusi secara damai dengan ketepatan 86% dengan jumlah 10 mempersiapkan informasi. Jika tingkat pencapaian seseorang (tidak memiliki otoritas) yang dapat membuka kerangka keamanan, maka, pada saat itu, kerangka kerja yang perlu ditingkatkan masih jauh dari efektif. Sebaliknya, jika tingkat pencapaian seseorang (tidak memiliki otoritas) yang dapat membuka kerangka keamanan yang dibuat dengan suara yang tidak sah itu sedikit, maka, pada saat itu, kerangka tersebut mendekati kemajuan. Kerangka kerja yang dibuat dapat dijalankan pada kerangka kerja Windows 8.1 64-siklus dengan spesifikasi RAM 3 GB dan prosesor tengah ganda.	Berbeda metode	Sama-sama melakukan enkripsi suara

3. Metode Penelitian

Penelitian ini terdiri dari tahapan, metode pengumpulan data, rancangan pengujian, dan perangkat penelitian.

3.1. Tahapan Penelitian

Tahapan pertama yang dilakukan ialah dengan studi literatur dengan mencari berbagai sumber atau materi yang mendukung dalam penelitian serta mengidentifikasi masalah yang mungkin sering terjadi dalam proses pertukaran informasi melalui media suara seperti keamanan, noise serta hal semacamnya dan mencari solusi yang salah satunya dengan proses enkripsi,dekripsi serta filtering.

3.2. Metode Pengumpulan Data

Pada tahapan kedua adalah pengumpulan data dengan studi pustaka pencarian data melalui sumber terkait seperti internet, jurnal, artikel yang serupa yang akan digunakan sebagai bahan referensi untuk menguji pada proses penelitian enkripsi dan dekripsi

 ISSN:2302-8149
e-ISSN:2540-9719

3.3. Rancangan Pengujian

Pada tahapan ketiga adalah skenario utnuk pembuatan serta menjalankan aplikasi enkripsi dan dekripsi suara beserta memfilter dari *noise*, menghitung waktu pengerjaan, serta nilai SNR dari data *voice* yang sudah dikumpulkan yang nanti hasil akhirnya akan dibandingkan seberapa besar tingkat keberhasilan kombinasi algoritma kriptografi AES dengan *secret key* dan *filter* suara berdasarkan parameter pengujian waktu dan ukuran file yang telah difilter sebelum proses enkripsi dekripsi dengan sesudah proses enkripsi dekripsi

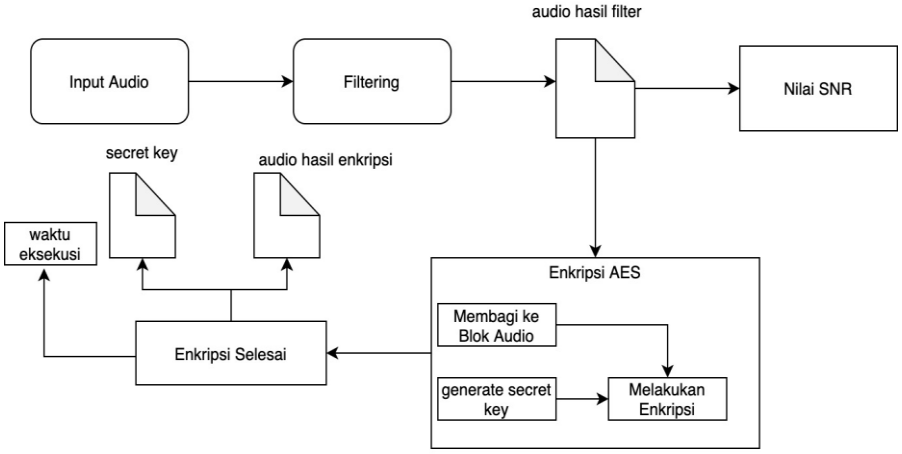
3.4. Perangkat Penelitian

Pada tahapan terakhir ialah perangkat digunakan dalam ulasan ini adalah Prosesor Intel Core™ i5-6200 CPU @2.30GHz 2.80GHz, RAM 4GB, Hardisk 1000GB, Sistem Operasi Windows 10, Bahasa Pemrograman *Python*.

4. Hasil dan Pembahasan

4.1. Konsep Alur Enkripsi dan Dekripsi

Metode pengujian yang digunakan adalah metode AES-128b, berikut alur gambaran proses enkripsi dan penguraian yang ditunjukan pada Gambar 1 dan 2.

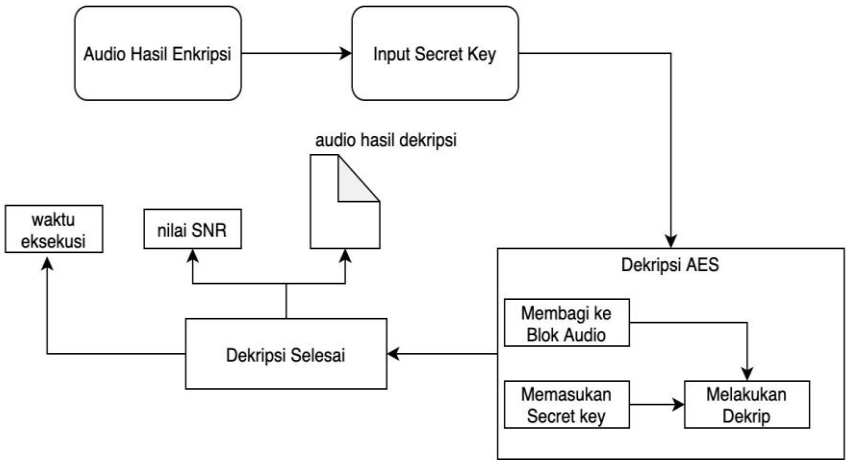


Gambar 1. Proses Enkripsi

Langkah – langkah proses enkripsi dijelaskan pada *Gambar 1* sebagai berikut:

1) User pengirim menentukan voice yang akan dienkripsi, voice disini merupakan audio dengan ukuran 8bit dari berbagai bentuk pengumpulan data yaitu dengan *audacity*
2) Setelah diinput, *audio* tersebut dilakukan filtering guna memunculkan grafik nilai *filter*
3) Muncul nilai SNR sebagai ukuran seberapa kualitas informasi audio tersebut terjaga tanpa noise
4) Dilakukan pembuatan *secret key* dan enkripsi menggunakan metode AES, nantinya akan digunakan oleh penerima untuk mengembalikan *audio* menjadi audio asli
5) Muncul *audio* sinyal dalam bentuk grafik untuk melihat hasil dari enkripsi
6) Menyimpan file *audio* Terenkripsi untuk membuktikan bahwa audio asli telah selesai proses enkripsi dan tidak dapat diputar

ISSN:2302-8149
e-ISSN:2540-9719



Gambar 2. Proses Dekripsi

Langkah – langkah proses dekripsi dijelaskan pada Gambar 2 sebagai berikut:

1) Penerima menerima *secret key* dan *audio* yang masih berekstens wav. dan sudah dienkripsi oleh pengirim
2) User penerima memasukkan *secret key* berupa file text untuk proses dekripsi
3) *Audio* mengalami proses dekripsi menggunakan metode AES 128 bit
4) Setelah proses dekripsi selesai, maka muncul nilai SNR dari *file audio* hasil dekripsi dengan bentuk grafik
5) *Output* hasil dekripsi adalah *audio* dapat diputar kembali yang nantiknya akan dibandingkan dengan *audio* asli

4.2. Teknologi yang Digunakan

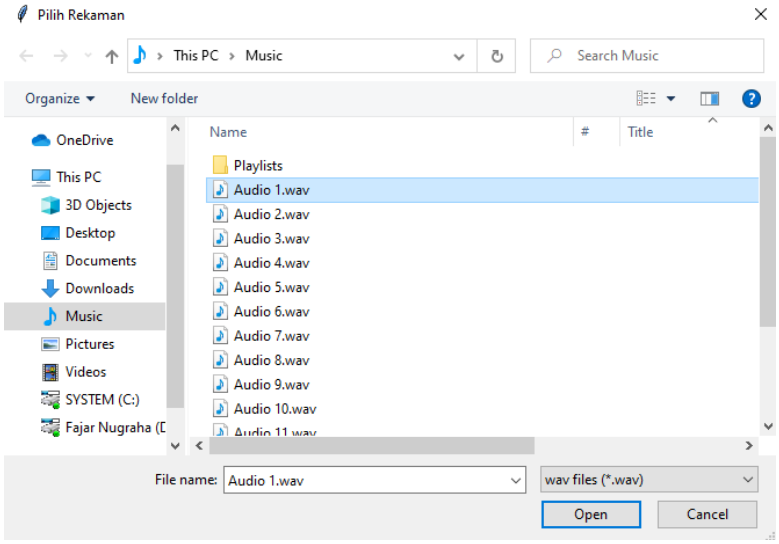
Inovasi yang digunakan dalam ulasan ini, menggunakan bahasa pemrograman Python dengan beberapa *library* yang mendukung untuk proses enkripsi dan dekripsi. *Library* ini sebagai berikut:

1) *Pycryptodome*
   i. *Pycyptodome* digunakan untuk menunjang kode yang berhubungan dengan proses enkripsi dan dekripsi dengan motode AES. Dalam *python* untuk menginstall *library* ini bisa digunakan dengan perintah pip atau perintah *conda*. *Library* ini merupakan paketan dari library *cryptography*.
2) *Scipy*
   i. *SciPy* merupakan library untuk menunjang urusan dan proses aritmatika atau perhitungan. *Library* ini merupakan paketan dari *library numpy*
3) *Matplotlib*
   i. *Matplotlib* merupakan *library python* yang membantu dalam melakukan visualisasi data dengan grafik atau gambar yang berbentuk 3D maupun 2D. *Matplotlib* juga merupakan paketan dari library *numpy*
4) *Tkinter*
   i. *Tkinter* merupakan Python standar UI grafis yang digunakan untuk membuat tampilan aplikasi dengan bagian-bagian dalam modul Tkinter seperti Tombol, Kotak Teks, Label, Bingkai, Jendela yang

4.3. Implementasi

Berdasarkan data sampel *audio* yang akan diuji proses enkripsi, dekripsi, serta *filtering* berjumlah 16 sampel dengan format wav 8bit yang ditunjukan pada Gambar 3.

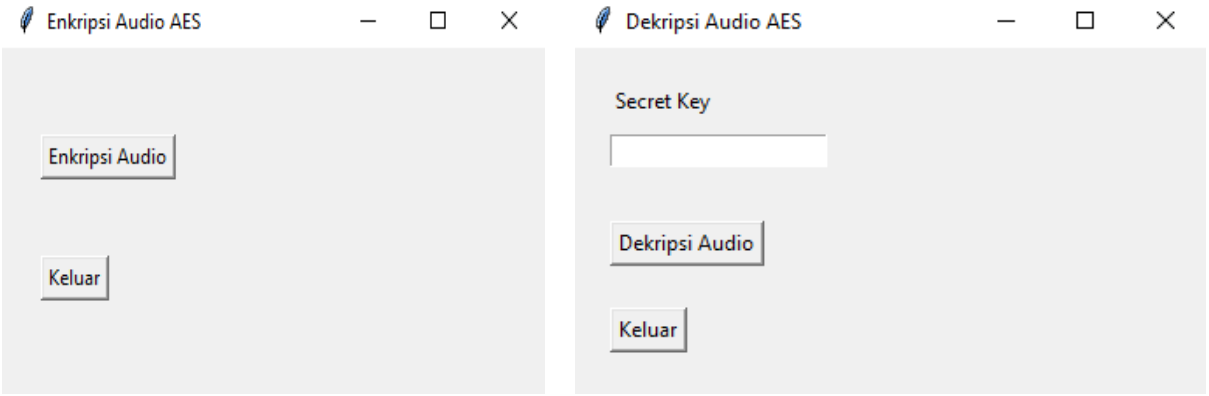
 ISSN:2302-8149
e-ISSN:2540-9719



Gambar 3. Dataset Sampel Audio

4.4. Hasil Pengujian

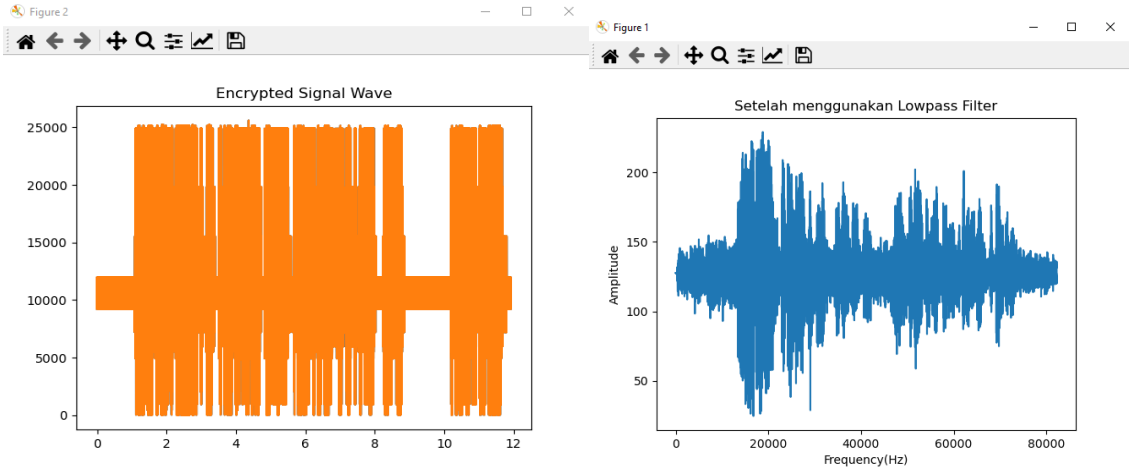
Untuk melihat hasil dari aplikasi serta metode yang digunakan pada peneitian ini, dimulai dari input sampel *audio* yang akan dilakukan proses enkripsi dan dekripsi dengan terlebih dahulu input di proses enkripsi lalu setelah proses enkripsi selesai maka berlanjut ke proses dekripsi yang dijelaskan pada Gambar 4 hingga Gambar 6 serta dari Tabel 2 hingga Tabel 5.



Gambar 4. *Grafik User Interface* Proses Enkripsi dan Dekripsi

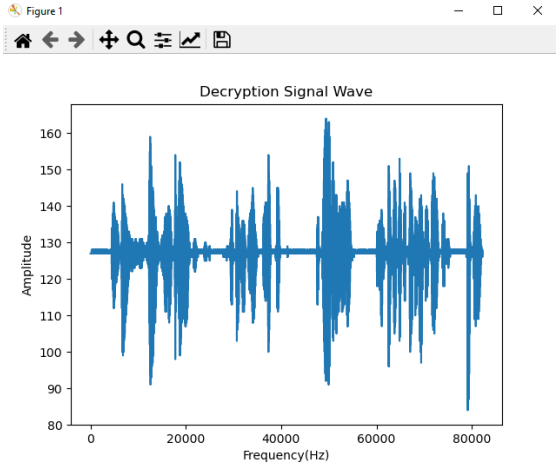
Pada gambar diatas menunjukan halaman *grafik user interface* yang berfungsi untuk memulai proses enkripsi dan dekripsi dengan memasukkan contoh datases yang akan dipilih untuk melakukan proses enkripsi, lalu dilanjutkan ke halaman selanjutnya dengan memasukkan *secret key* serta memilih *file* yang sudah dienkripsi terlebih dahulu untuk memulai kembali proses dekripsi.

 ISSN:2302-8149
e-ISSN:2540-9719



Gambar 5. *Signal Audio* Setelah di Enkripsi dan *Filtering*

Setelah melalui proses enkripsi, maka akan muncul tampilan grafik *signal audio* setelah enkripsi serta filtering untuk melihat seberapa bagus kualitas *audio* setelah melakukan proses enkripsi yang dijelaskan pada Gambar 5.



Gambar 6. *Signal Audio* Setelah di Dekripsi

Setelah proses enkripsi dan filtering selesai maka dilannjutkan dengan proses dekripsi yang didahului dengan menginput secret key lalu dilanjutkan dengan proses dekripsi dan outputnya berupa grafik signal *audio* setelah dekripsi yang dijelaskan pada Gambar 6.

Pada tabel ini dijelaskan hasil dari perhitungan *(Signal Nose to Ratio)* untuk mengukur seberapa bagus kualitas *audio* setelah melalui proses enkripsi dan dekripsi dalam satuan desibel *(dB)* yang ditujukan pada Tabel 2 dan 3.

Tabel 2. Hasil Enkripsi

No	Nama *File*	Keterangan	SNR
1	Audio 1.wav	Berhasil	29.95181745280945
2	Audio 2.wav	Berhasil	38.14440237115774
3	Audio 3.wav	Berhasil	24.39163409756477
4	Audio 4.wav	Berhasil	38.50825612582019
5	Audio 5.wav	Berhasil	25.08072113886705
6	Audio 6.wav	Berhasil	28.698060751166093
7	Audio 7.wav	Berhasil	29.5183727075138

 ISSN:2302-8149
e-ISSN:2540-9719

8	Audio 8.wav	Berhasil	39.094543882015536
9	Audio 9.wav	Berhasil	26.671929289013345
10	Audio 10.wav	Berhasil	22.472502745826443
11	Audio 11.wav	Berhasil	24.37778234219003
12	Audio 12.wav	Berhasil	28.926625499266535
13	Audio 13.wav	Berhasil	26.732919906896395
14	Audio 14.wav	Berhasil	27.654913200235693
15	Audio 15.wav	Berhasil	37.41601762061276
16	Audio 16.wav	Berhasil	29.593369334701826

Tabel 3. Hasil Proses Dekripsi

No	Nama *File*	Keterangan	SNR Setelah Dekripsi
1	Audio 1.wav	Berhasil	29.488389571514443
2	Audio 2.wav	Berhasil	38.10335007234403
3	Audio 3.wav	Berhasil	24.3556510855776
4	Audio 4.wav	Berhasil	39.93069449401566
5	Audio 5.wav	Berhasil	25.0456974923313053
6	Audio 6.wav	Berhasil	28.6531793495131
7	Audio 7.wav	Berhasil	29.47266473424332
8	Audio 8.wav	Berhasil	38.96579034678871
9	Audio 9.wav	Berhasil	26.635573485538554
10	Audio 10.wav	Berhasil	22.438966205043336
11	Audio 11.wav	Berhasil	24.348265966755775
12	Audio 12.wav	Berhasil	28.88797712740007
13	Audio 13.wav	Berhasil	26.698342811501274
14	Audio 14.wav	Berhasil	27.614075728234027
15	Audio 15.wav	Berhasil	37.36915192309403
16	Audio 16.wav	Berhasil	29.552575092923497

Pada tabel dibawah ini dijelaskan catatan perolehan waktu *audio* selama proses enkripsi dan dekripsi berlangsung yang dihitung dalam satuan menit dan detik yang ditunjukan pada Tabel 4.

Tabel 4. Pengujian Waktu Proses Enkripsi dan Dekripsi

No	Nama *File*	Waktu Enkripsi	Waktu Dekripsi
1	Audio 1.wav	0 menit 12 detik	0 menit 7 detik
2	Audio 2.wav	0 menit 20 detik	0 menit 4 detik
3	Audio 3.wav	0 menit 5 detik	0 menit 6 detik
4	Audio 4.wav	0 menit 4 detik	0 menit 9 detik
5	Audio 5.wav	0 menit 6 detik	0 menit 13 detik
6	Audio 6.wav	0 menit 6 detik	0 menit 7 detik
7	Audio 7.wav	0 menit 5 detik	0 menit 8 detik
8	Audio 8.wav	0 menit 5 detik	0 menit 6 detik
9	Audio 9.wav	0 menit 10 detik	0 menit 5 detik
10	Audio 10.wav	0 menit 5 detik	0 menit 4 detik
11	Audio 11.wav	0 menit 5 detik	0 menit 5 detik
12	Audio 12.wav	0 menit 4 detik	0 menit 5 detik
13	Audio 13.wav	0 menit 17 detik	0 menit 16 detik
14	Audio 14.wav	0 menit 5 detik	0 menit 6 detik
15	Audio 15.wav	0 menit 3 detik	0 menit 6 detik
16	Audio 16.wav	0 menit 5 detik	0 menit 5 detik

Pada tabel dibawah ini dijelaskan perubahan ukuran file pada saat sebelum proses berlangsung/*original* sampai sesudah proses enkripsi dan dekripsi selesai dilakukan yang dihitung dalam satuan (kb) yang dijelaskan pada Tabel 5.

Tabel 5. Pengujian Ukuran File Setelah Proses Enkripsi dan Dekripsi

No	Nama *File*	Ukuran Asli (kB)	Ukuran Setelah Enkripsi (kB)	Ukuran Setelah Dekripsi (kB)
1	Audio 1.wav	160	80,3	80,3
2	Audio 2.wav	156	78,3	78,3
3	Audio 3.wav	162	81,4	81,4
4	Audio 4.wav	161	80,8	80,8
5	Audio 5.wav	189	94,5	94,5
6	Audio 6.wav	169	84,7	84,7
7	Audio 7.wav	153	76,7	76,7
8	Audio 8.wav	296	148	148
9	Audio 9.wav	160	80,3	80,3
10	Audio 10.wav	189	94,8	94,8
11	Audio 11.wav	195	97,9	97,9
12	Audio 12.wav	226	113	113
13	Audio 13.wav	181	90,6	90,6
14	Audio 14.wav	206	103	103
15	Audio 15.wav	171	85,5	85,5
16	Audio 16.wav	186	91,3	91,3

5. Kesimpulan

Pada penelitian kali ini untuk pengujian proses enkripsi dan dekripsi suara menggunakan metode AES 128 bit dinyatakan berhasil dengan menyembunyikan informasi suara serta menghilangkan *noise.* Pada saat proses berlangsung mengalami penurunan serta peningnkatan kualitas suara berdasarkan hasil perhitungan SNR yang dinyatakan dalam satuan Hz, lalu juga mengalami perubahan pada ukuran *file* sampel *audio* baik dari sebelum proses enkripsi dan dekripsi berlangsung hingga setelah proses enkripsi dan dekripsi selesai,namun semua perubahan itu tidak menunjukan grafik yang berubah dengan signifikan. Serta menorehkan waktu tercepat selama prosses enkripsi sekitar 3 detik.

Referensi

[1] E. A. Wibowo, "Penggunaan Teknologi E-Commerce dalam Proses Bisnis," *Equilibiria*, vol. 1, no. 1, pp. 95–108, 2016, [Online]. Available: http://journal.unrika.ac.id/index.php/equi/article/view/222.
[2] R. Munir, "Slide Kuliah Pengantar Kriptografi," *J. Ilmu Komput. dan Inform.*, 2019.
[3] W. Steven, V. Afriyandi, and K. M. Suryaningrum, "Implementasi Algoritma Ez Stego Untuk Menyembunyikan Pesan Terenkripsi Dengan Playfair Cipher Pada Gambar GIF," vol. 5, no. 2, 2019.
[4] M. Natsir, "Kemajuan Prototipe Sistem Kriptografi untuk Enkripsi dan Dekripsi Data Kantor," Jurnal, vol. 6, hlm. 2089–5615, 2016.
[5] I. J. Kusuma, "Investigation of Steganography Techniques on MP3 Audio Using Parity Coding and Cipher Transposition Encryption Methods," *J. Elektron. Sist. Inf. dan Komput. p. ISSN 2477-5290 e. ISSN 2502-2148*, vol. 3, no. 2, 2017, [Online]. Available: http://www.jesik.web.id/index.php/jesik/article/download/65/44%0A.
[6] S. Rahmawati, I. Taufik, and G. Sandi, "Execution of AES (Advanced Encryption Standard) 256 Bit Algorithm and Compression Using the Huffman Algorithm in Voice Recorder Applications,"

Proceedings-Seminar Nas. Technology. Electrical Engineering UIN Sunan Gunung Djati Bandung, hlm. 91–99, 2018.

[7] H. Patricia, "Teknik Keamanan Data Menggunakan Kriptografi dengan Algoritma Vigenere Cipher dan Steganografi dengan Metode End of File (EoF)," *Progr. Stud. Tek. Inform. Fak. Ilmu Komput. Univ. Dian Nuswantoro*, pp. 1–7, 2018.

[8] J. Caesar, "Bagian II KRIPTOGRAFI Alasan dan Sejarah Kriptografi Pengertian Kriptografi (Pendahuluan Kriptografi) Istilah-istilah yang Digunakan Notasi Matematis," no. 1, pp. 1–14, 2018.

[9] I. Febriana and G. A. S, "Use of Cryptographic Techniques in Sms Android Security," JOIST (Journal of Educ. Inf. Commun. Technol., vol. 1, no. 1, pp. 29–36, 2017.

[10] P. D. S. Kunjung Wahyudi, "Aplikasi kriptografi untuk pesan perdagangan menggunakan steganografi dan prosedur yippee AES," *Pros. Semin. Nas. Teknoin*, no. January 2011, pp. 67–72, 2018.

[11] A. J. Dedi Darwis, Wamiliana Wamiliana, "Proses Pengamanan Data Menggunakan Kombinasi Metode Kriptografi Data Encryption Standard dan Steganografi End Of File," 2017.

[12] K. Khairunnisa, N. Nurkamilia, and Z. Zuraidah, "Analisis Signal-To-Noise Ratio Pada Sinyal Audio Dengan Teknik Konvolusi," *J. ELTIKOM*, vol. 2, no. 2, pp. 78–86, 2018, doi: 10.31961/eltikom.v2i2.84.

[13] I. Hadi, "Rancang bangun filter portable," *J. Teliska*, vol. 4, no. 3, pp. 61–67, 2012.

[14] D. Almanda, E. Dermawan, D. Ery, Syawaluddin, and I. R. Anwar, "Investigasi Desain Filter Teredam Lintas Tinggi untuk Beban FL-4 pada PL-LB/2 Berdasarkan ETAP," *J. Teknol.*, vol. 10, no. 2, pp. 161–166, 2018.

[15] H. Herwanto, "Diagnosis Faktual Pemahaman Bahasa Pemrograman Pemetaan Sebagai Acuan Penelitian Mahasiswa," Nuansa Inform., vol. 13, no. 2, p. 33, 2019, doi: 10.25134/nuansa.v13i2.1950.