**ANALISIS KOMBINASI KRIPTOGRAFI DAN STEGANOGRAFI AUDIO DALAM MENGAMANKAN INFORMASI**

**Disusun dan diajukan oleh:**

WIRA SATYA TRI ALMI

D121181324

****

PROGRAM STUDI SARJANA TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS HASANUDDIN

GOWA

2023

**LEMBAR PENGESAHAN**

**ANALISIS KOMBINASI KRIPTOGRAFI DAN STEGANOGRAFI AUDIO DALAM MENGAMANKAN INFORMASI**

Disusun dan diajukan oleh

**Nama Mahasiswa**

**D121181324**

Telah dipertahankan di hadapan Panitia Ujian yang dibentuk dalam rangka Penyelesaian Studi Program Sarjana Program Studi Teknik Informatika

Fakultas Teknik Universitas Hasanuddin

Pada tanggal …………………

dan dinyatakan telah memenuhi syarat kelulusan

Menyetujui,

|  |  |
| --- | --- |
| Pembimbing Utama, | Pembimbing Pendamping, |
| Dr. Eng. Ady Wahyudi Paundu, S.T., M.T.  NIP.197503132009121003 | Mukarramah Yusuf, B.Sc., M.Sc., Ph.D |

**ABSTRAK**

**DAFTAR ISI**

**DAFTAR GAMBAR**

**DAFTAR LAMPIRAN**

**KATA PENGANTAR**

# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

Perkembangan dunia digital saat ini membuat lalu lintas pengiriman data elektronik semakin ramai dan sensitif. Seiring dengan perkembangan tersebut, kejahatan teknologi komunikasi dan informasi juga turut berkembang. Dengan adanya pencurian data maka aspek keamanan dalam pertukaran informasi serta penyimpanan data dianggap penting, karena suatu komunikasi data jarak jauh, belum tentu memiliki jalur transmisi yang aman dari penyadapan, serta penyimpanan data belum tentu aman dari pencurian sehingga keamanan informasi menjadi bagian penting dalam dunia informasi (Putri, Kartikadewi, & Rosyid, 2020) . Seringkali seseorang yang hendak mengirim pesan kepada orang lain, tidak ingin orang yang tidak berwenang mengetahui pesan tersebut. Pesan yang berisi sesuatu bersifat rahasia yang ditujukan untuk kalangan terbatas. Salah satu upaya untuk mengantisipasi pesan agar tidak sampai kepada orang yang tidak berwenang dapat dilakukan menyembunyikan pesan pada suatu media yang dapat ditelusuri oleh setiap orang. Data yang disembunyikan berupa data teks, gambar, audio, dan video (Minarni & Redha, 2020). Terdapat teknik yang digunakan untuk mengamankan dan menjaga kerahasiaan data, yaitu kriptografi dan steganografi. Algoritma kriptografi merupakan salah satu metode pengamanan data yang bertujuan digunakan untuk menjaga kerahasiaan data, keaslian data serta originalitas. Sedangkan, Steganografi adalah menyembunyikan informasi kedalam sebuah media, biasa berupa media gambar, suara ataupun video. Dengan demikian, dapat disimpulkan bahwa kriptografi fokus pada bagaimana melindungi isi informasi agar tetap aman (secure) dan steganografi fokus bagaimana agar isi informasi tersebut tidak terlihat keberadaannya (Laia, 2020) .

Untuk menangani keamanan pertukaran informasi yang sifatnya rahasia maka dikembangkanlah metode pengamanan data pada audio menggunakan algoritma AES (Advanced Encryption Standard) dan Algoritma F5 dimana metode yang mampu menjaga sifat-sifat histogram DCT dengan baik, cukup unggul dalam kapasitas supaya data pesan rahasia tersebut tidak dapat dibajak oleh orang lain. Algoritma F5 bekerja dengan menyisipkan bit pesan kedalam bit koefisien DCT hasil kuantisasi yang telah dipermutasi (Sianturi & Hutagaol, 2019).

## 1.2 Rumusan masalah

1. Bagaimana menyembunyikan sebuah pesan teks terkompresi ke dalam media cover yang berupa berkas audio dengan metode F5 ?

2. Bagaimana membangun sistem steganografi audio menggunakan algoritma F5

## 1.3 Tujuan Penelitian

1. Melakukan analisis kualitas pada audio dengan menggunakan metode SNR dari audio asal dan audio yang disisipi informasi

2. Membangun sistem steganografi audio menggunakan algoritma F5

## 1.4 Manfaat Penelitian

1. Memberikan informasi tentang teknik steganografi yang dapat menyembunyikan pesan pada audio.

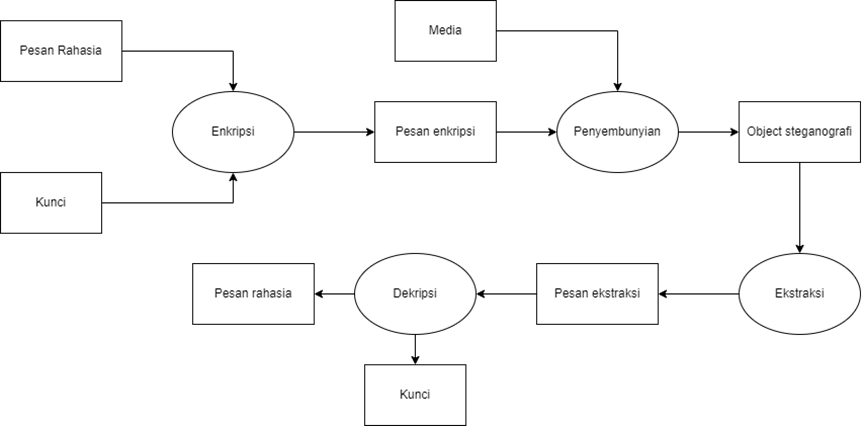
2. Membantu masyarakat untuk melindungi pesannya dalam audio agar pesannya hanya dapat dibaca oleh penerima yang dituju.

## 1.5 Ruang Lingkup

1. Analisis yang akan dilakukan terhadap sistem hanya berkaitan dengan kualitas audio.

2. Algoritma yang digunakan AES (Advanced Encryption Standard) dan F5.

**8.** **Usulan Sistem**

****

Gambar 1. Skema kriptografi dan Steganografi

1. Enkripsi (AES)

Input dan output dari algoritma AES terdiri dari urutan data sebesar 128 bit. Urutan data yang sudah terbentuk dalam satu kelompok 128 bit tersebut disebut juga sebagai blok data atau plaintext yang nantinya akan dienkripsi menjadi ciphertext. Cipher key dari AES terdiri dari key dengan panjang 128 bit, 192 bit, atau 256 bit.

Perbedaan panjang kunci akan mempengaruhi jumlah round yang akan diimplementasikan pada algoritma AES ini. Berikut ini adalah Tabel 1 yang memperlihatkan jumlah round/putaran (Nr) yang harus diimplementasikan pada masing-masing panjang kunci.

Jumlah round/putaran (Nr)

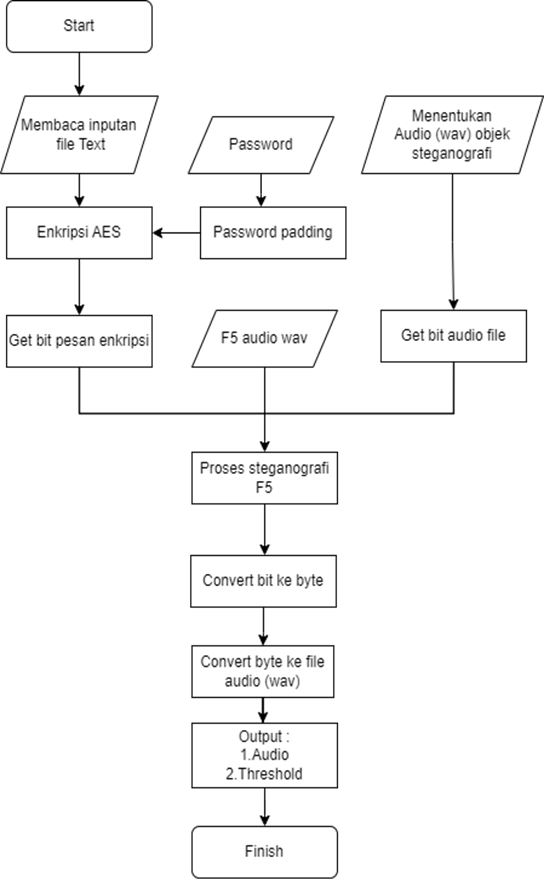
|  |  |  |  |
| --- | --- | --- | --- |
| Tipe | Jumlah Key (Nk) | Besar Blok (Nb) | Jumlah Round (Nr) |
| AES-128 | 4 | 4 | 10 |
| AES-192 | 6 | 4 | 12 |
| AES-256 | 8 | 4 | 14 |

2. Steganografi (F5)

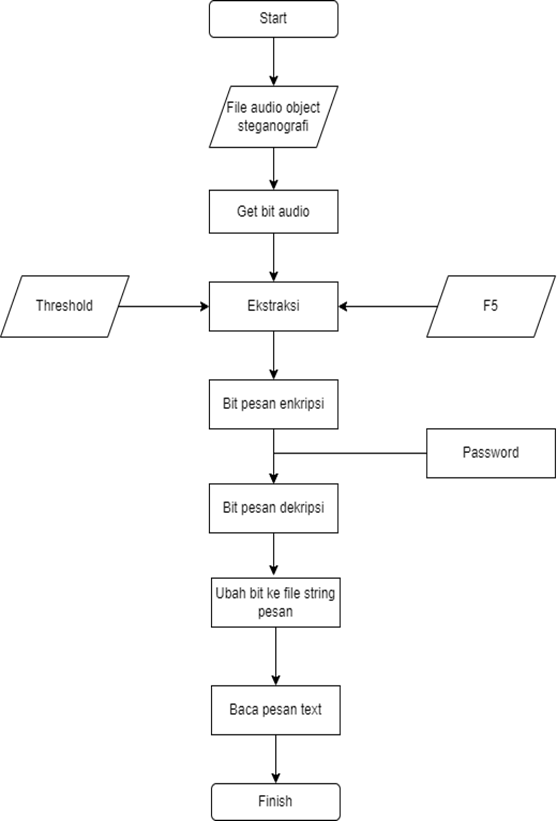
F5 merupakan sebuah metode/algoritma yang diajukan oleh Andreas Westfeld dari Techniche Universitas Desden, Institute for System Architecture, Jerman. F5 merupakan perbaikan dari algoritma F3 dan F4. Algoritma ini tidak menggunakan LSB, namun ia menghitung penyebaran byte-byte dari steganogram citra (dalam hal ini berformat JPEG) baik positif maupun negatif, namun bukan 0. Menyisipkan (embeddin) bit dari pesan rahasia ke beberapa byte tersebut dengan kompresi XOR(Exlusive Or), lalu mengurangi nilai (decrement) byte tersebut, baik yang disisipi oleh bit dari pesan rahasia maupun tidak.

3. Ekstraksi Pesan

Pesan enkripsi yang telah tersembunyi dalam media audio akan diekstraksi. Ekstraksi dilakukan dengan cara menentukan threshold atau batas dari pesan yang disembunyikan. Threshold merupakan jumlah bit pesan yang di enkripsi. Setelah kita mengetahui threshold dan jumlah bit maka kita dapat melakukan ekstraksi pesan sesuai region yang dibagi di dalam media audio.



**Gambar 2.** Skema Penyembunyian



**Gambar 3.** Skema Ekstraksi

Penjelasan Sistem :

Pesan yang digunakan adalah text dimana akan di enkripsi lebih dahulu dengan menggunakan metode AES. Hasil enkripsi selanjutnya akan disembunyikan ke media audio menggunakan metode F5. Output dari proses ini adalah file audio yang menjadi objek stegano dan threshold. Threshold merupakan panjang bit pesan yang di enkripsi untuk digunakan pada proses ekstraksi pada proses selanjutnya.

Setelah di enkripsi dan disembunyikan pesan harus didapatkan kembali dari objek media steganografi. Objek steganografi diekstraksi menggunakan metode F5 untuk mendapatkan pesan yang telah di enkripsi. Setelah didapatkan pesan enkripsi maka akan dilakukan proses dekripsi menggunakan metode AES.

4. Analisis Hasil Laporan

Pada tahap ini, audio yang telah disisipkan pesan kemudian dianalisis untuk mencari tahu apakah ada perubahan kualitas pada data audio yang signifikan dengan cara:

Membandingkan kualitas sebelum dan sesudah pesan disisipkan pada dengan parameter pendengaran manusia.

Mengvaluasi kinerja teknik dengan menggunakan metode SNR

# BAB II

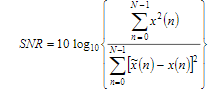
# TINJAUAN PUSTAKA

## 2.1 Audio

Audio adalah suara atau bunyi yang dihasilkan dari getaran suatu benda. Dibutuhkan getaran minimal 20 kali/detik, agar audio dapat didengar oleh telinga manusia. Sinyal audio dibagi menjadi dua macam, yaitu analog dan digital (). audio analog memproduksi variasi suara dengan membuat atau membaca variasi sinyal listrik. Sedangkan audio digital memproduksi suara dengan mengambil sampel tekanan suara atau level sinyal pada rate tertentu dan mengubahnya menjadi angka ().

2.1.1 Kualitas Audio

Dasar yang paling penting pada audio steganografi adalah penyisipan data tidak boleh mengubah kualitas suara dari sinyal audio yang digunakan sebagai cover. Jadi data rahasia yang disisipkan tidak boleh terdeteksi oleh pendengar. Performa ini sangat penting pada aplikasi proteksi hak cipta. Parameter yang digunakan dalam menentukan kualitas audio yang telah disisipkan data adalah SNR (*signal to noise ratio*). Persamaan untuk menghitung SNR adalah sebagai berikut:



Keterangan: *x(n)* adalah sinyal audio cover dari panjang sample *N* dan *x(n)* adalah sinyal data yang disisipkan.

2.1.2 Bit Rate

Tujuan dari bit rate adalah untuk menghitung banyaknya data rahasia yang mungkin disisipkan ke sinya *audio cover* per satuan waktu. Beberapa aplikasi *steganography*, seperti penyisipan nomor serial dan pengidentifikasian hak cipta membutuhkan hanya sedikit data yang disisipkan pada sinya *audio cover* (Riko Arlando Saragih 2006).

## Daftar Pustaka

[1] Laia, R. (2020). Implementasi Algoritma Aes 256 Bit Dan Lsb Untik Pengamanan Dan Penyisipan Pesan Teks Pada File Audio. *Pelita Informatika: Informasi dan Informatika*, *8*(4), 467-469.

[2] Minarni, M., & Redha, R. (2020). IMPLEMENTASI LEAST SIGNIFICANT BIT (LSB) DAN ALGORITMA VIGENERE CIPHER PADA AUDIO STEGANOGRAFI. *Jurnal Sains dan Teknologi: Jurnal Keilmuan dan Aplikasi Teknologi Industri*, *20*(2), 168-174.

[3] Peling, I. B. A., & Sastra, N. P. (2018). Enhanced Audio Steganografi dengan Algoritma Advanced Encryption Standard Untuk Pengamanan Data Pada File Audio. *Majalah Ilmiah Teknologi Elektro*, *17*(1), 66-71.

[4] Putri, A. E., Kartikadewi, A., & Rosyid, L. A. (2021). Implementasi Kriptografi dengan Algoritma Advanced Encryption Standard (AES) 128 Bit dan Steganografi menggunakan Metode End of File (EOF) Berbasis Java Desktop pada Dinas Pendidikan Kabupaten Tangerang. *Appl. Inf. Syst. Manag*, *3*(2), 69-78.

[5] Sianturi, T. N., & Hutagaol, R. G. (2019, February). Penyisipan Pesan Rahasia Kedalam Audio Menggunakan Algoritma F5. In *Seminar Nasional Teknologi Komputer & Sains (SAINTEKS)* (Vol. 1, No. 1).