

USULAN TUGAS AKHIR

1. IDENTITAS PENGUSUL

NAMA : Muhammad Bagus Andra
NRP : 5111100086
DOSEN WALI : Prof. Ir. Handayani Tjandrasa, M.Sc.,Ph.D.
DOSEN PEMBIMBING : 1. Tohari Ahmad, S.Kom.,MIT.,Ph.D.
2.

2. JUDUL TUGAS AKHIR

“Reversible Multi-Layer Steganography pada Audio Menggunakan Metode Reduced Difference Expansion”

3. LATAR BELAKANG

Berkembangnya teknologi jaringan terutama *internet* memberikan dampak besar pada distribusi dan pengiriman berkas *digital*. Ada kalanya berkas *digital* yang dikirimkan bersifat rahasia atau *confidential* seperti, data catatan kesehatan dan pesan militer, sehingga harus dipastikan isi dari berkas hanya diketahui oleh pihak yang berhak. Salah satu metode yang dapat digunakan untuk menjaga kerahasiaan adalah steganografi.

Steganografi sendiri adalah sebuah praktik mengubah data secara tidak terdeteksi untuk menyisipkan sebuah pesan [1]. Secara umum sistem steganografi terdiri dari dua komponen yaitu *Embedder* dan *Detector*. Bagian *Embedder* akan mempunyai dua buah masukan yaitu data rahasia atau biasa disebut *Secret Message* atau *Payload*, dan *Cover* yaitu data yang akan digunakan sebagai media untuk menyisipkan pesan rahasia. Kedua masukan ini kemudian diproses menghasilkan *Embedded Data* atau stego, yaitu data yang telah disisipkan pesan rahasia. Di bagian *detector*, *Embedded Data* akan menjadi

masukannya yang kemudian diproses untuk didapatkan kembali pesan rahasia yang tersimpan di dalamnya [1].

Penelitian mengenai steganografi telah banyak dilakukan, namun sepanjang pengetahuan saya, kebanyakan metode yang ada hanya dapat diterapkan pada berkas citra, sedangkan metode yang dapat digunakan untuk berkas bertipe audio masih sangat terbatas. Beberapa metode yang telah ada mencakup *Low Bit Encoding*, *Echo Hiding*, *Spread Spectrum*, *Phase coding* [2], dan menggunakan transformasi *wavelet* [3]. Namun, metode ini memiliki kelemahan dimana berkas audio *cover* dan *secret message* tidak dapat dikembalikan persis seperti asalnya dikarenakan adanya modifikasi pada domain spasial ataupun domain frekuensi. Modifikasi tersebut bersifat *irreversible* atau tidak dapat dikembalikan. Hal ini tentu harus dihindari karena informasi pada *secret message* bersifat sensitif dan harus dikembalikan tanpa ada sedikitpun informasi yang hilang.

Untuk mendapatkan kembali data *cover* dan *secret message* tanpa kehilangan informasi, harus dilakukan modifikasi yang bersifat *reversible* pada berkas. Hal itu dapat dilakukan dengan menggunakan metode transformasi *Difference Expansion* yang pertama kali diusulkan oleh Tian [4]. Setelah itu banyak metode yang diajukan sebagai pengembangan metode ini, seperti *Reduced Difference Expansion* dan *Quad Smoothness* [5], tetapi metode tersebut hanya dapat diaplikasikan pada berkas dengan tipe citra.

Dalam tugas akhir ini, metode transformasi bersifat *reversible* yang awalnya hanya dapat diterapkan pada berkas citra akan dicoba diterapkan pada berkas bertipe audio. Sebelum metode dapat diterapkan tentu harus dilakukan beberapa tahap *pre-processing* agar metode yang dimaksud dapat diterapkan pada berkas audio. Tahap ini mencakup pembentukan segmen sampel audio dan partisi bit pada sampel audio.

4. RUMUSAN MASALAH

Rumusan masalah yang diangkat dalam tugas akhir ini dapat dipaparkan sebagai berikut:

1. Bagaimana cara menerapkan metode steganografi yang bersifat *reversible* pada berkas bertipe audio?
2. Bagaimana cara memproses berkas audio, agar metode yang awalnya hanya dapat diterapkan pada berkas citra dapat diterapkan pada berkas audio?
3. Pengembangan apa yang dapat dilakukan pada metode agar kapasitas data yang disisipkan dapat ditambahkan tanpa mengurangi kualitas audio secara signifikan?

5. BATASAN MASALAH

Permasalahan yang dibahas pada tugas akhir ini memiliki beberapa batasan antara lain:

1. Metode hanya diterapkan pada berkas audio dengan ekstensi WAV

2. Penerapan metode tidak mencakup proses pengiriman data stego melalui jaringan
3. *Secret Message* atau *Payload* adalah sebuah pesan teks

6. TUJUAN PEMBUATAN TUGAS AKHIR

Tujuan dari pembuatan tugas akhir ini adalah untuk menerapkan metode steganografi yang bersifat *reversible* pada berkas audio dan menganalisis performa dari metode yang digunakan dibandingkan dengan metode yang telah ada.

7. MANFAAT TUGAS AKHIR

Manfaat dari hasil pembuatan tugas akhir ini antara lain:

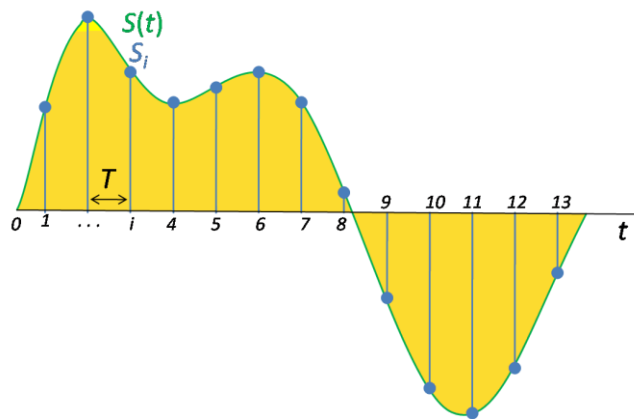
1. Memberikan metode alternatif untuk steganografi pada berkas audio yang bersifat *reversible*
2. Memberikan konsep sistem pengiriman berkas sensitif yang aman dan memiliki kapasitas yang cukup besar

8. TINJAUAN PUSTAKA

8.1 Pemrosesan Sinyal Digital

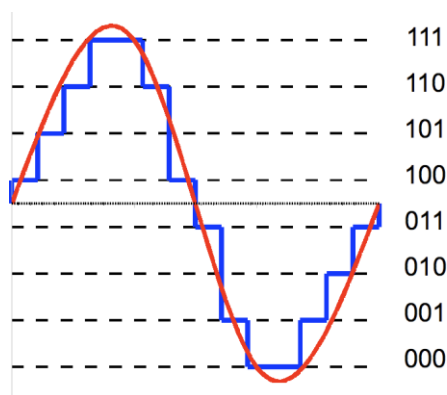
Pada komputer, berkas audio direpresentasikan oleh sinyal digital. Sinyal digital didapatkan dari sinyal analog yang diproses melalui tahap *sampling* dan *quantization*. Proses ini dimaksudkan untuk mengubah sifat sinyal analog yang aslinya bersifat kontinu menjadi bentuk diskrit.

Sampling merupakan proses reduksi gelombang sinyal kontinu menjadi sinyal diskrit dengan cara mengambil suatu titik sampel per satuan waktu. *Sample rate* menggambarkan berapa banyak sampel yang diambil setiap detiknya. Sebuah sinyal digital dengan sampling rate 44100Hz berarti dalam 1 detik dilakukan pengambilan sampel sebanyak 44100 kali [7]. Proses sampling ditunjukkan pada Gambar 1.



Gambar 1 Proses Sampling [7]

Sedangkan *quantization* merupakan proses pemetaan amplitudo dari setiap sampel yang telah diambil kedalam satuan diskrit. Setiap sampel pada berkas audio akan direpresentasikan dalam bilangan baik itu berbentuk bilangan bulat (*integer*) maupun *float*. Bilangan ini mewakili nilai amplitudo dari masing-masing sampel [7]. Proses *quantization* ditunjukkan pada Gambar 2.



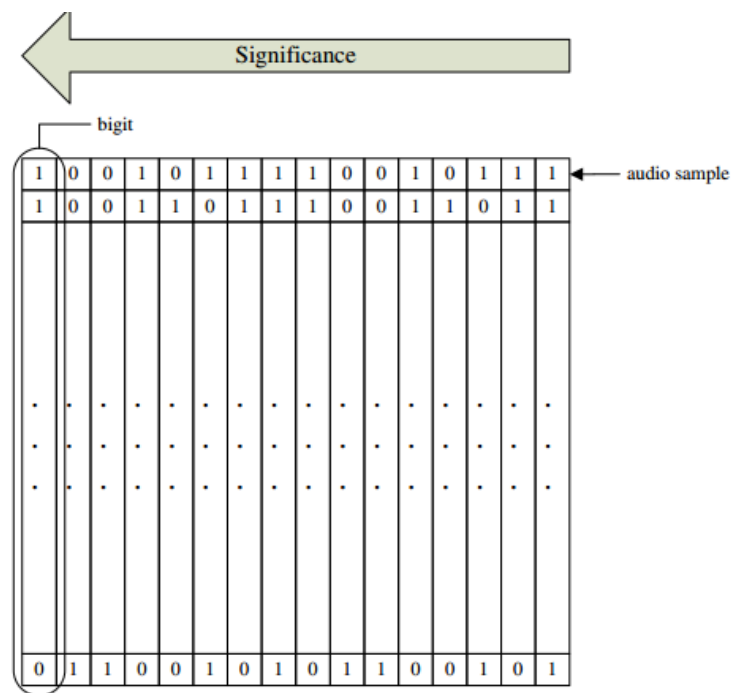
Gambar 2 Proses Quantization [7]

Setelah dilakukan proses *sampling* dan *quantization* setiap nilai sampel akan disimpan dalam bentuk bit. Besar berkas audio akan bergantung oleh jumlah sampling yang dilakukan dan juga kedalaman atau *depth* dari amplitudo yang disimpan.

8.2 Intelligent Partitioning

Perbedaan besar sampel pada citra yaitu sebesar 8 bit dibandingkan dengan besar sampel pada audio yang umumnya sebesar 16 bit menyebabkan tidak dapatnya diterapkan metode steganografi citra pada berkas audio. Untuk mengatasi hal tersebut, perlu dilakukan tahap partisi untuk membagi sampel audio yang memiliki besar 16 bit menjadi dua bagian. Penyisipan data akan dilakukan pada masing-masing bagian tersebut [8].

Partisi dilakukan dengan cara merepresentasikan gelombang audio sebagai 16 buah *array* individual yang disebut *bigit*.



Gambar 3
Representasi *array* gelombang audio [8]

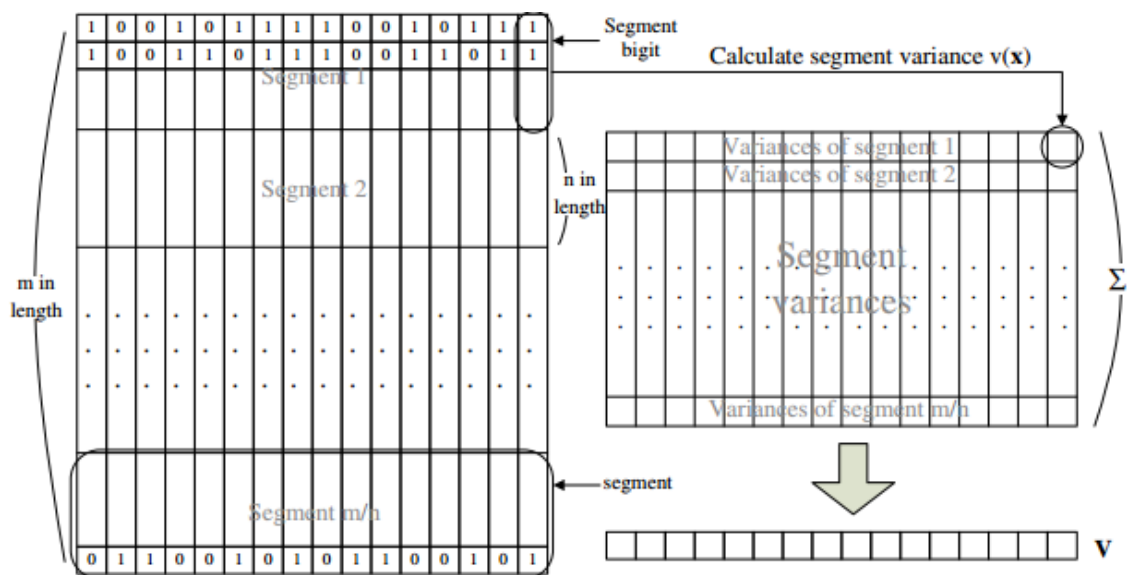
Setiap kolom adalah sampel dari audio dan setiap baris adalah satu *array* *bigit* dari gelombang audio. Untuk mempartisi *array* 16bit ini menjadi dua bagian, akan dibentuk dua grup *array* yang masing-masing memiliki *bigit array* dengan panjang 8 bit. Kombinasi dari grup ini akan mempengaruhi kapasitas data yang dapat disisipkan.

Skema partisi yang akan dilakukan bergantung dari nilai *variance* tiap *bigit*. Untuk masukkan gelombang audio M , pertama, hitung *variance* V dengan proses yang ditunjukkan pada Gambar 4, dimana m adalah panjang dari gelombang dan n adalah panjang dari segmen. *Variance* V adalah vektor yang

menunjukkan jumlah dari *variance* pada tiap segmen dari setiap bitit pada M. Untuk setiap segment, *variance* segment $v(x)$ ditunjukkan oleh (1).

$$v(x) = \sum_{j=1}^n (x_j - a(x))^2 \quad (1)$$

Dimana x adalah vektor $(x_1, x_2, x_3 \dots x_n)$ yang merepresentasikan satu buah segmen bitit dan $a(x)$ adalah rata-rata dari x yang dibulatkan. Untuk mencari V , *variance* dari semua segmen untuk setiap bitit harus ditemukan terlebih dahulu, kemudian semua *variance* tersebut dijumlahkan dan menghasilkan V .



Gambar 4 Menghitung variance [8]

Setelah V ditemukan, kita akan membentuk sebuah *array* yang berisikan *variance* yang telah diurutkan. M kemudian dibagi menjadi dua bagian yaitu $M1$ dan $M2$ berdasarkan urutan *array* tersebut. Langkah terakhir adalah mencatat kombinasi pembagian kedalam sebuah *array* partisi P . *Array* P akan menjadi acuan dalam proses *decoding* untuk menyusun kembali data sampel ke posisi semula.

8.3 Reduced Difference Expansion

Reduced Difference Expansion merupakan pengembangan dari metode *Difference Expansion*. Pada DE, proses *embedding* atau penyisipan menyebabkan adanya kenaikan dari selisih nilai piksel hampir sebesar dua kali, oleh karena itu diusulkan persamaan baru yang dapat memperkecil selisih pada proses *embedding* tersebut [5] seperti dijabarkan pada (2).

$$\bar{v} = \begin{cases} v, & \text{if } v < 2 \\ v - 2^{\lfloor \log_2 v \rfloor - 1}, & \text{if } v \geq 2 \end{cases} \quad (2)$$

Setelah persamaan diatas diaplikasikan pada pasangan pixel, pixel tersebut akan ditandai dengan nilai 1. Pixel yang tidak operasikan akan ditandai dengan nilai 0. Nilai-nilai ini kemudian akan disimpan dalam *location map*. *Location map* ini akan digunakan pada proses rekonstruksi, tiap pixel yang ditandai 1 akan dilakukan operasi (3) untuk mendapatkan nilai aslinya, sedangkan pixel bertanda 0 akan dilakukan (4) untuk mendapatkan nilai aslinya.

$$v = \bar{v} + 2^{\log_2 |\bar{v}|} \quad (3)$$

$$v = \bar{v} + 2^{\log_2 |\bar{v}|} - 1 \quad (4)$$

8.4 SciPy Stack

SciPy Stack adalah kumpulan dari beberapa perangkat lunak berbasis *open-source* yang digunakan untuk kepentingan komputasi dan sains dengan menggunakan bahasa python [9]. Secara garis besar SciPy terdiri atas beberapa perangkat inti yaitu:

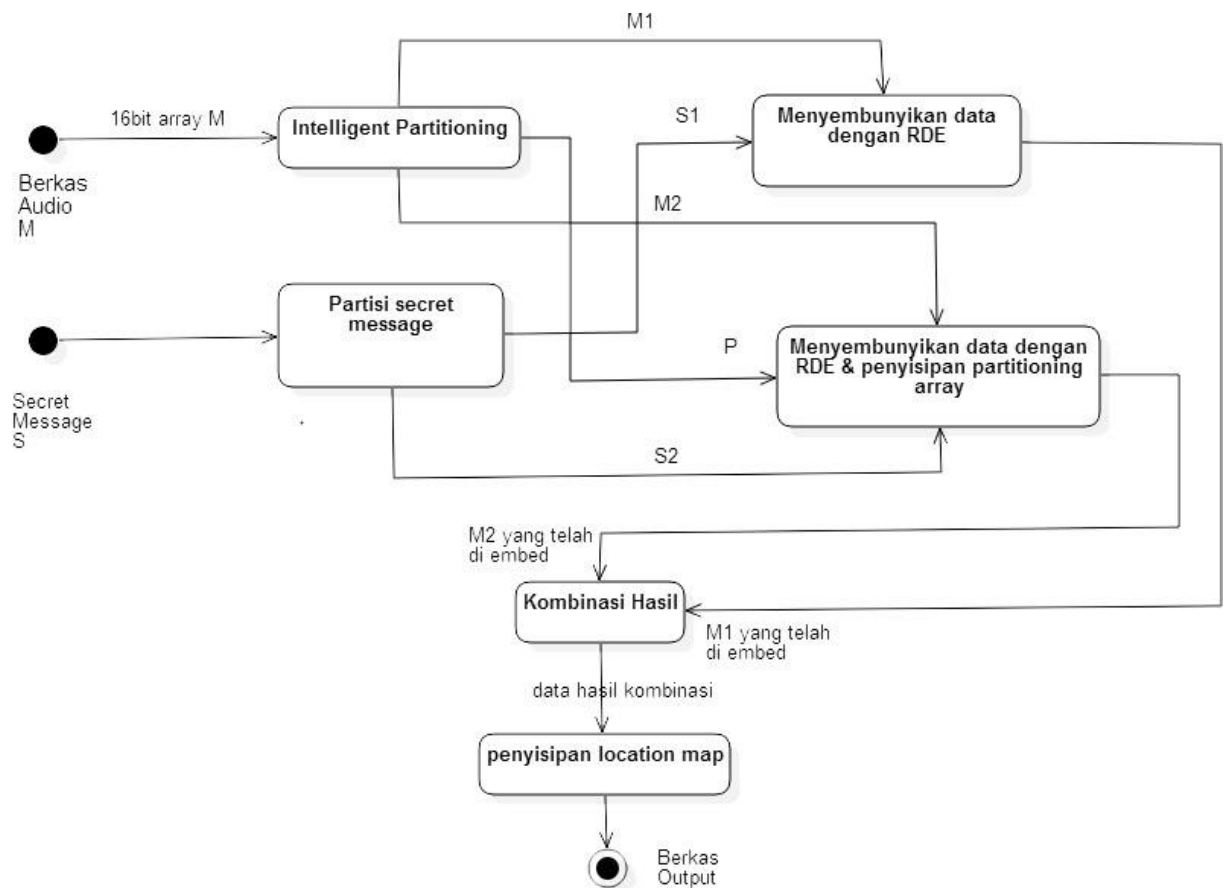
- Python sebagai basis bahasa pemrograman
- NumPy, modul python untuk komputasi numerik
- SciPy Library, pustaka yang berisikan kumpulan algoritma dan kaskas kerja, termasuk kaskas untuk pemrosesan sinyal
- Matplotlib, modul yang berguna untuk merepresentasikan plot dan graf
- Pandas, antarmuka untuk struktur data
- Sympy, modul untuk matematika simbolis dan aljabar computer
- iPython, antarmuka interaktif untuk mengetes kode
- nose, kerangka kerja untuk pengetesan kode python

9. RINGKASAN ISI TUGAS AKHIR

Berkembangnya teknologi jaringan terutama *internet* memberikan dampak besar pada distribusi dan pengiriman berkas *digital*. Ada kalanya berkas *digital* yang dikirimkan bersifat rahasia atau *confidential* seperti, data catatan kesehatan dan pesan militer, sehingga harus dipastikan isi dari berkas hanya diketahui oleh pihak yang berhak. Salah satu metode yang dapat digunakan untuk menjaga kerahasiaan adalah steganografi.

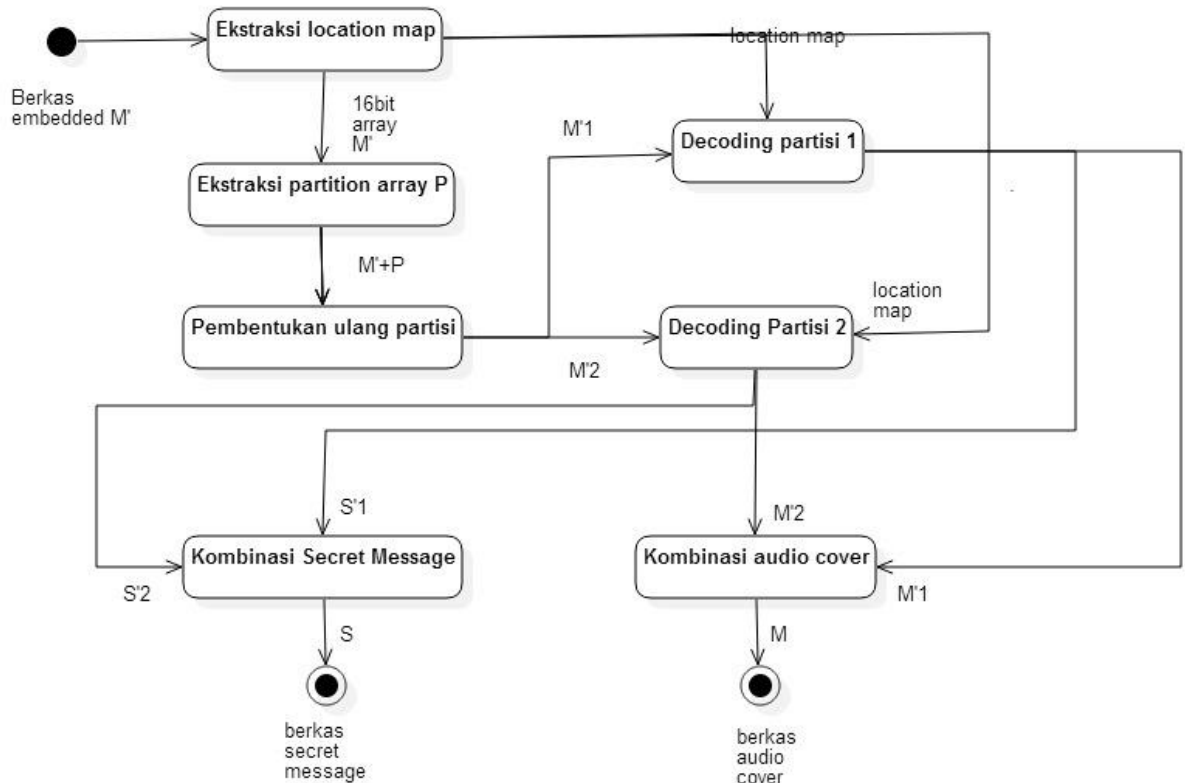
Untuk menyembunyikan data yang bersifat rahasia dan sensitif seperti data rekam medis atau pesan operasi militer, diperlukan metode transformasi data yang bersifat *reversible* agar data dapat dikembalikan persis seperti data aslinya. Transformasi reversible yang aslinya diterapkan pada citra akan diterapkan pada berkas audio dengan *pre-processing* terlebih dahulu.

Pada sistem steganografi yang akan dibangun kali ini ada beberapa tahap yang harus dilakukan sampai data *secret message* dapat disisipkan kedalam berkas *cover* dan menghasilkan file keluaran yang telah disisipi. Bagan sistem ini dapat dilihat pada Gambar 5.



Gambar 5 Bagan sistem embedding

Untuk mendapatkan kembali *secret message* serta berkas *cover* seperti semula, berkas yang telah di *embed* akan mengalami prosedur ekstraksi seperti yang digambarkan pada Gambar 6.



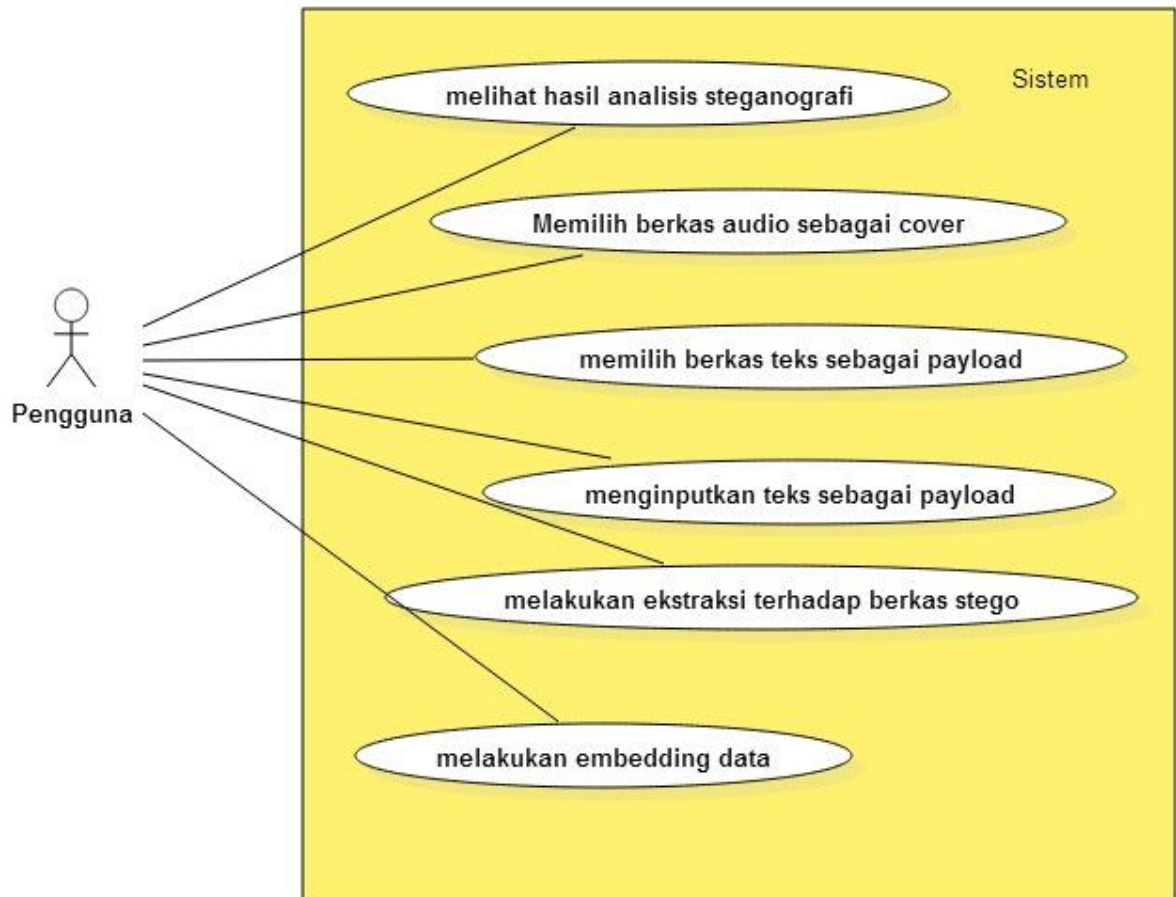
Gambar 6 Bagan sistem ekstraksi

Implementasi dari skema di atas akan dilakukan pada lingkungan sistem operasi Windows dengan menggunakan bahasa pemrograman python. Hasil akhirnya adalah perangkat lunak untuk melakukan steganografi serta melakukan ekstraksi terhadap berkas hasil steganografi tersebut. Diagram *Use Case* aplikasi dapat dilihat pada Gambar 7.

Adapun fitur dari aplikasi yang akan dibuat antara lain adalah:

- Pengguna dapat memilih berkas audio yang akan digunakan sebagai *cover*
- Aplikasi akan menampilkan kapasitas data yang dapat ditampung oleh audio tersebut
- Pengguna dapat memasukkan data teks atau memilih berkas teks yang akan menjadi *secret message*
- Pengguna dapat menentukan beberapa parameter pada proses steganografi yang akan mempengaruhi keluaran dari sistem

- Pengguna dapat melakukan ekstraksi pada berkas hasil steganografi dan mendapatkan berkas *cover* serta pesan rahasia yang asli
- Aplikasi dapat menampilkan analisa hasil steganografi seperti hasil pengujian segSNR dan besar data yang disimpan



Gambar 7 Diagram Use Case

10.METODOLOGI

1. Penyusunan proposal tugas akhir

Proposal Tugas Akhir ini berisi tentang deskripsi pendahuluan dari tugas akhir yang akan dibuat. Pendahuluan ini terdiri atas hal yang menjadi latar belakang diajukannya usulan tugas akhir, rumusan masalah yang diangkat, batasan masalah untuk tugas akhir, tujuan dari pembuatan tugas akhir, dan manfaat dari hasil pembuatan tugas akhir. Selain itu dijabarkan pula tinjauan

pustaka yang digunakan sebagai referensi pendukung pembuatan tugas akhir. Sub bab metodologi berisi penjelasan mengenai tahapan penyusunan tugas akhir mulai dari penyusunan proposal hingga penyusunan buku tugas akhir. Terdapat pula sub bab jadwal kegiatan yang menjelaskan jadwal pengerjaan tugas akhir.

2. Studi literatur

Pada tugas akhir ini, referensi yang akan dipelajari adalah sejumlah jurnal mengenai pemrosesan berkas audio, pemrosesan sampel, dan partisi sampel berkas audio, serta metode *reduced difference expansion* untuk melakukan penyisipan data atau *embedding*.

3. Analisis dan desain perangkat lunak

Aktor atau pengguna dari aplikasi ini adalah pengguna yang hendak melakukan steganografi pada berkas audio. Fitur pada aplikasi ini antara lain:

1. Memilih berkas audio yang akan digunakan sebagai *cover*
2. Meng-*input*-kan teks atau memilih berkas teks yang akan digunakan sebagai *Secret Message*
3. Memilih beberapa parameter yang akan digunakan dalam proses steganografi seperti jumlah layer yang digunakan serta batas t pada proses *Reduced Difference Expansion*
4. Menuliskan file hasil *embedding* yang telah dilakukan
5. Membaca file hasil *embedding* dan mendapatkan kembali berkas yang menjadi *cover* dan *secret message* yang ada di dalamnya

4. Implementasi perangkat lunak

Implementasi perangkat lunak dilakukan dalam platform Windows menggunakan bahasa pemrograman python dengan menggunakan modul-modul bantuan yang terdapat dalam *SciPy Stack*.

5. Pengujian dan evaluasi

1. Pengujian segSNR

Pengujian segSNR adalah pengujian secara objektif yang merupakan pengembangan dari SNR (*Signal to Noise Ratio*). Pengujian ini dilakukan dengan cara membandingkan rata-rata jumlah dari sinyal asli dan noise tambahan pada tiap *frame* [6].

2. Pengujian kapasitas *Embedding Data*

Pengujian ini dimaksudkan untuk mengetahui seberapa banyak data *secret message* yang dapat disisipkan pada berkas audio.

3. Pengujian pengembalian data atau *data reversibility*

Pengujian ini dimaksudkan untuk mengetahui seberapa baik data *cover* dan *secret message* dapat dikembalikan menjadi bentuk asalnya.

6. Penyusunan Buku Tugas Akhir

Pada tahap ini dilakukan penyusunan laporan yang menjelaskan dasar teori dan metode yang digunakan dalam tugas akhir ini serta hasil dari implementasi aplikasi perangkat lunak yang telah dibuat. Sistematika penulisan buku tugas akhir secara garis besar antara lain:

1. Pendahuluan
 - a. Latar Belakang
 - b. Rumusan Masalah
 - c. Batasan Tugas Akhir
 - d. Tujuan
 - e. Metodologi
 - f. Sistematika Penulisan
2. Tinjauan Pustaka
3. Desain dan Implementasi
4. Pengujian dan Evaluasi
5. Kesimpulan dan Saran
6. Daftar Pustaka

11. JADWAL KEGIATAN

Tahapan	2015											
	Maret				April				Mei			
Penyusunan Proposal	■	■	■	■								
Studi Literatur			■	■	■	■						
Perancangan Sistem					■	■	■	■	■	■		
Implementasi							■	■	■	■	■	■
Pengujian dan Evaluasi									■	■	■	■
Penyusunan Buku											■	■

12. DAFTAR PUSTAKA

- [1] Ingemar, J. Cox . 2008 **.Digital watermarking and steganography Morgan Kaufmann**, Burlington:Morgan Kaufmann
- [2] Bilal, I., Roj, M.S., Kumar, R., Mishra, P.K., 11-13 Dec. 2014 , "Recent advancement in audio steganography", **Parallel, Distributed and Grid Computing (PDGC), 2014 International Conference on** , vol., no., pp.402,405
- [3] Santosa, R.A., Bao, P., 8-10 Juni 2005, "Audio-to-image wavelet transform based audio steganography" , **ELMAR, 2005. 47th International Symposium** , vol., no., pp.209,212
- [4] Jun Tian, Aug. 2003 , "Reversible data embedding using a difference expansion", **Circuits and Systems for Video Technology, IEEE Transactions on** , vol.13, no.8, pp.890,896
- [5] Tohari , Ahmad. , Holil, M. , 2014 , "Increasing the Performance of Difference Expansion-based Steganography for Securing Medical Data" **[unpublished]**.
- [6] Grundlehner, Bernard,et al. , 2005 "Performance assessment method for speech enhancement systems." **Proc. 1st annu. IEEE BENELUX/DSP valley signal process. symp.**
- [7] Zolzer , Udo. , 2008 , **Digital Audio Signal Processing** ,Hamburg:Wiley
- [8] Choi, Ka-Cheng. , Pun , Chi-Man., Chen, C.L Philip , Januari 2013 , "Application of a generalized difference expansion based reversible audio data hiding algorithm", **Multimedia Tools and Applications** , Impact Factor: 1.06
- [9] SciPy Team. 2012. **Scientific Computing Tools for Python** , <URL: <http://www.scipy.org/about.html>>.