Program Studi Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

Tugas Kecil II (Tucil II) IF4020 Kriptografi Sem. I Tahun 2025/2026

Steganografi pada Berkas Audio dengan Metode *Multiple-LSB*

Batas pengumpulan	:	Sabtu, 4 Oktober 2025, Pukul 23.59 WIB
Tempat pengumpulan	:	Form Pengumpulan
Anggota kelompok	:	2 orang
QnA	:	Sheet QnA
Revisi I	:	Senin, 29 September 2025, Pukul 09:36 WIB - Perpanjangan deadline hingga Sabtu, 4 Oktober 2025, Pukul 23.59 WIB
Revisi II	:	Jumat, 3 Oktober 2025, Pukul 15:00 WIB - Spesifikasi Peak signal-to-noise ratio (PSNR) menjadi bonus dan panjang kunci Vigenere dibebaskan.

Latar Belakang

Selain dengan enkripsi, keamanan pesan juga dapat menggunakan teknik steganografi. Pesan rahasia disimpan di dalam data multimedia seperti teks, citra (gambar), audio, dan video sedemikian sehingga keberadaan pesan tidak dapat dideteksi. Pada tugas besar kali ini pesan disembunyikan di dalam berkas digital. Berkas audio yang dijadikan cover adalah audio dengan kompresi lossy (MP3).

Spesifikasi dan Ketentuan Program

A. Ketentuan Umum

Perangkat lunak yang akan dibuat memiliki fitur untuk menyisipkan dan mengekstrak berkas pesan rahasia (*secret message*) dari sebuah berkas audio digital MP3 (*cover message*) dengan metode *multiple-LSB*. Penyisipan dapat dilakukan pada sebuah titik acak berdasarkan *seed* yang diberikan. Program juga mendukung enkripsi berkas sisipan dengan *extended Vigenère cipher* (256 karakter).

Berikut detail aturan umum yang berlaku.

- Berkas audio dapat berupa mono (1 *channel*) atau stereo (2 *channel*).

- Program menerima berkas pesan rahasia dengan sembarang tipe (*extension*) dan sembarang ukuran.
- Program mendukung metode *multiple-LSB* dalam rentang 1 bit LSB hingga 4 bit LSB.
- Program steganografi dan enkripsi-dekripsi cipher harus dibuat sendiri.
- Pustaka pengolahan audio MP3 dapat diambil dari kode yang sudah ada asalkan disebutkan sumbernya.
- **[Kreatifitas]** Pemilihan kakas dibebaskan (Java, C, C++, Python, Go, dll.).
- **[Kreatifitas]** Program dapat memainkan (*playback*) berkas audio (*cover message*) asli dan berkas yang sudah disisipi pesan (*stego-audio*) melalui sebuah pemutar audio. Implementasinya dibebaskan.
- **[Kreatifitas]** Dibebaskan untuk menambah fitur lain yang relevan.

B. Penyisipan Pesan

Berikut ketentuan tambahan fitur penyisipan pesan.

- Masukan untuk penyisipan berupa
    - berkas audio digital MP3 (*cover message*),
    - berkas pesan rahasia (*secret message*),
    - pilihan penggunaan enkripsi/tidak,
    - pilihan penggunaan titik mulai sisip acak/tidak,
    - pilihan n-LSB yang ingin digunakan,
    - kunci stego/*seed*.
- Kunci stego berupa sebuah kata kunci ~~(maksimal 25 karakter~~) memiliki dua fungsi:
    - kunci enkripsi-dekripsi cipher Vigenère
    - *seed* pembangkit titik acak.

  Perhatikan contoh berikut dengan kunci stego = “STEGANO”.
    - Kunci stego sebagai kunci cipher, langsung digunakan.
    - **[Kreatifitas]** Kunci stego sebagai *seed*, dibebaskan untuk mengubah *string* menjadi sebuah bilangan acak. Misalnya,
        a. nilai-nilai integer dari string ’STEGANO’ dijumlahkan, yaitu Int(’S’) + Int(’T’) + Int(’E’) + Int(’G’) + Int(’A’) + Int(’N’) + Int(’O’) = …
        b. atau, hanya mengambil sebagian huruf dari STEGANO, misalnya karakter pada posisi ganjil saja, yaitu Int(’S’) + Int(’E’) + Int(’A’) + Int(’O’) = …

- Gunakan hanya *audio data samples*, yaitu bagian yang merepresentasikan suara untuk manipulasi bit atau penyisipan apapun.
- **[Kreatifitas]** Beberapa properti berkas pesan rahasia dan karakteristik metode penyisipan dapat disimpan agar informasinya tersimpan untuk proses ekstraksi. Berikut contoh informasi yang dapat disimpan.
    - Tipe/ekstensi berkas (misalnya, .jpeg, .pdf, .doc, .exe, dll.).
    - Nama berkas asli, agar dapat muncul ketika pengguna ingin menyimpan hasil ekstraksi.
    - Ukuran berkas pesan rahasia.
    - Pilihan penggunaan enkripsi/tidak, pilihan penggunaan titik mulai sisip acak/tidak, dan pilihan n-LSB yang ingin digunakan.

  Berikut beberapa metode penyimpanan yang dapat digunakan, tanpa membatasi metode kreatif lainnya.
    - Penggunaan beberapa bit awal untuk menyimpan informasi seperti ekstensi berkas atau ukuran berkas. Juga, penggunaan beberapa bit awal untuk menyimpan informasi pilihan dalam bentuk *flag boolean*.
    - Penggunaan *signature* untuk menandai awal dan akhir lokasi sisipan serta pilihan *n-bit* yang dipakai (lihat Audio Steganography Method Using Least Significant Bit (LSB) Encoding Technique).

  Dibebaskan untuk memilih informasi yang disimpan dan metode penyimpanan yang digunakan agar sesuai.
- **JANGAN** menyisipkan kunci ke berkas stego.
- Program dapat menolak penyisipan jika ukuran pesan rahasia melebihi batas kapasitas sisip.
- Kapasitas sisip dihitung sebelum memulai proses penyisipan, dengan mempertimbangkan pilihan penggunaan enkripsi, penggunaan titik mulai sisip acak, pilihan n-LSB, serta faktor lainnya yang relevan (misalnya, keterangan tipe, nama, dan ukuran berkas pesan, *flag*).
- Program dapat menyimpan stego-*audio* dengan nama yang dapat diatur pengguna (*save as*).

C. Ekstraksi Pesan

Berikut ketentuan tambahan fitur penyisipan pesan.

- Masukan untuk ekstraksi berupa
    a. berkas audio digital MP3 yang telah disisipi (*stego-audio*),
    b. kunci stego/*seed*.
- Program dapat menyimpan berkas pesan rahasia hasil ekstraksi dengan nama yang dapat diatur pengguna (*save as*).

BONUS

- Membuat pustaka pengolahan audio sendiri.
    - **[Kreatifitas]** Gunakan metode konversi yang dibahas pada Audio Steganography Method Using Least Significant Bit (LSB) Encoding Technique atau metode lain yang relevan.
- Menambahkan opsi untuk menggunakan **salah satu** dari metode penyisipan berikut.
    - *Parity coding*
    - *Echo hiding*
    - *Phase coding*
    - *Spread spectrum*

- Program dapat menampilkan ukuran kualitas audio hasil steganografi dengan PSNR (Peak Signal-to-Noise Ratio). PSNR adalah metrik yang umum digunakan untuk mengukur perbedaan bit-bit antara berkas cover dan berkas stego. PSNR dihitung dengan persamaan berikut pada audio PCM (Pulse Code Modulation) seperti WAV, dan bukan MP3

    $x[n]$ = sampel PCM sebelum stego
    $y[n]$ = sampel PCM sesudah stego
    N = jumlah sampel ter-align
    $n = 0..N-1.$
    MAX = 32767 (16-bit PCM). Jika pakai float ternormalisasi [-1, 1], MAX = 1

$$\mathrm{MSE} = \frac{1}{N}\sum_{n=0}^{N-1}(x[n] - y[n])^2, \qquad \mathrm{PSNR} = 10\log_{10}\left(\frac{\mathrm{MAX}^2}{\mathrm{MSE}}\right)$$

~~dimana P0 dan P1 adalah kekuatan sinyal berkas audio sebelum dan sesudah penyembunyian pesan. Nilai minimal PSNR adalah 30 dB (jika kurang dari 30 dB berarti sinyal audio tersebut mengalami kerusakan yang berarti).~~ Ambang "30 dB" umum dipakai di citra, untuk audio tidak ada ambang PSNR baku, pakailah sebagai indikator relatif saja.

Berkas Pengumpulan

1. **Repositori perangkat lunak** berisi
    a. kode sumber (*source code*),
    b. berkas eksekutabel (*executable file*), jika relevan,
    c. sebuah folder berisi berkas uji,
    d. berkas README, minimal berisi
        i. nama dan deskripsi program,
        ii. kumpulan teknologi yang digunakan (*tech stack*),
        iii. dependensi,
        iv. tata cara menjalankan program.

2. **Video demo** berdurasi maksimal **5 menit**, berisi
    a. deskripsi singkat program,
    b. teknologi yang digunakan (*tech stack*),
    c. penjelasan singkat rancangan, terutama bagian yang dibebaskan atau sesuai kreatifitas dan bonus,
    d. demo kasus uji (yang utama, sesuai dengan ketentuan kasus uji pada 3.d.).

3. **Berkas laporan** dengan ketentuan nama **NIM1_NIM2_Tucil2_IF4020.pdf**, berisi
    a. (jika menggunakan *cover*) foto kelompok yang menggantikan logo Ganesha,
    b. **teori singkat**, minimal tentang steganografi, metode modifikasi LSB, berkas MP3, *echo hiding* (atau konsep bonus yang diambil), dan konsep relevan lainnya,

c. **perancangan dan implementasi**, pastikan untuk menjelaskan implementasi bagian yang dibebaskan atau sesuai kreatifitas dan bonus,
d. **pengujian program dan analisis hasil**, dengan minimal kasus uji mencakup
    i. semua kombinasi konfigurasi (penggunaan enkripsi dan titik mulai sisip acak),
    ii. berkas yang ingin disisipkan melebihi batas kapasitas sisip,
    iii. berbagai tipe berkas sisip, seperti .txt, .png, .pdf, .docx, .exe, dll.
    iv. (bukan keharusan, tetapi menarik untuk dicoba) berbagai genre musik sebagai berkas *cover*, seperti Jazz, Vocaloid, Afrobeat, dll.,
    v. untuk setiap kasus uji, cek integritas berkas pesan rahasia asli dibandingkan dengan berkas pesan rahasia hasil ekstraksi,
e. **kesimpulan dan hasil implementasi**
f. **daftar pustaka**
g. **lampiran** berisi
    i. pranala repositori perangkat lunak,
    ii. pranala laman *web* (jika relevan),
    iii. pranala video demo,
    iv. pembagian tugas,
    v. tangkapan layar dari GUI/CLI/laman *web*

Referensi dan Bahan Bacaan

Berikut bahan bacaan yang dapat menunjang pemahaman, **TANPA** membatasi kemungkinan adanya sumber tambahan lainnya.

- (PDF) Audio Steganography Method Using Least Significant Bit (LSB) Encoding Technique
- SECURE DATA TRANSMISSION IN MP3 FILE USING LSB AND ECHO HIDING
- INFORMATION HIDING USING AUDIO STEGANOGRAPHY – A SURVEY