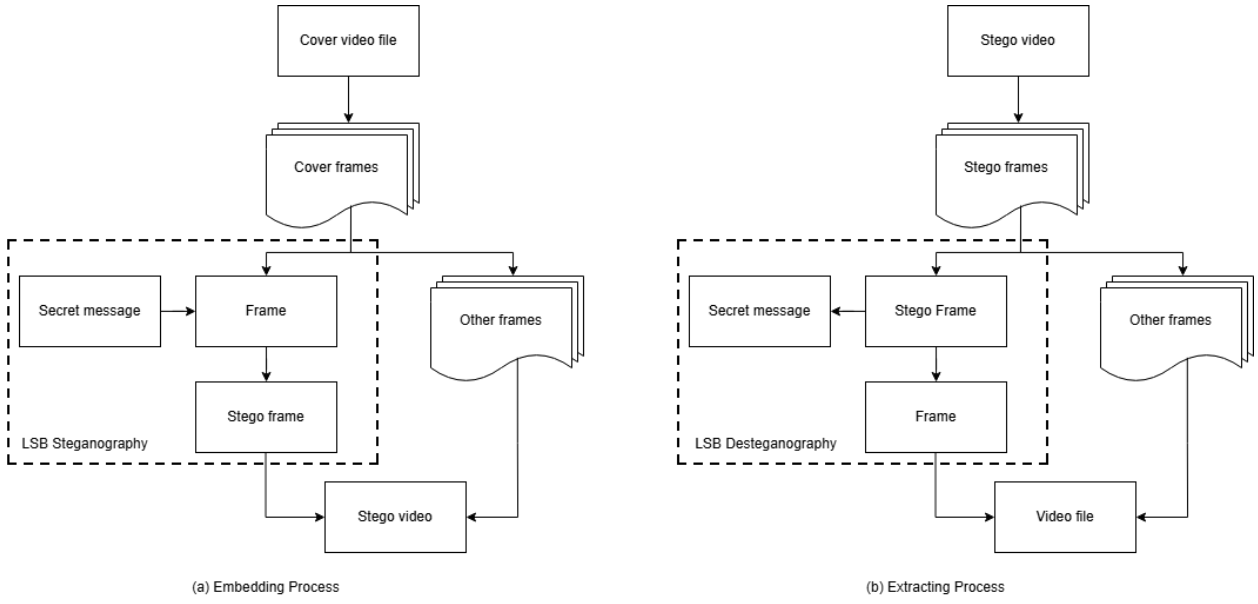
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

Tugas 2 II4021 Kriptografi – Semester II tahun 2025/2026
Steganografi LSB pada Berkas Video AVI

Batas pengumpulan	**:** Sabtu, 28 Maret 2026
Tempat pengumpulan	**:** Form Pengumpulan
Anggota kelompok	**:** 3 orang
Sheets kelompok	**:** Sheets Kelompok
QnA	**:** QnA Tugas II4021 Kriptografi

Latar Belakang

Steganografi merupakan teknik penyembunyian pesan rahasia sedemikian sehingga keberadaan pesan tersebut tidak mudah disadari. Berbeda dari kriptografi yang menitikberatkan pada pengamanan isi pesan, steganografi berfokus pada penyamaran pesan dengan memanfaatkan media pembawa. Pada tugas besar ini, media yang digunakan adalah berkas video dengan format AVI, sedangkan metode yang diterapkan adalah *Least Significant Bit* (LSB) pada *frame* video.



Gambar 1. Ilustrasi proses penyisipan dan ekstraksi pesan pada video

AVI (*Audio Video Interleave*) adalah salah satu format video digital yang dapat digunakan dalam steganografi. Video memiliki kapasitas untuk penyisipan data yang lebih besar dibandingkan

citra tunggal karena tersusun atas banyak *frame*, dengan setiap *frame* pada dasarnya merupakan sebuah citra. Format AVI sering digunakan dalam steganografi karena dapat bersifat *lossless*, sehingga perubahan kecil pada bit-bit piksel dapat tetap tersimpan dengan baik.

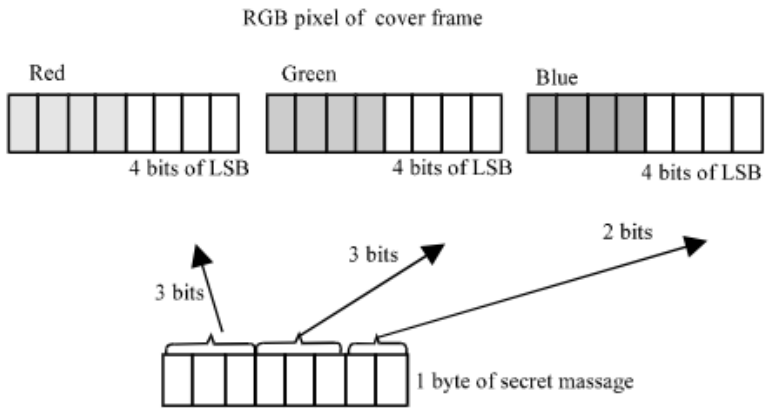
Spesifikasi dan Ketentuan Program

A. Ketentuan Umum

Program yang dibuat harus dapat melakukan **penyisipan** dan **ekstraksi** pesan rahasia pada berkas video AVI dengan metode ***Least Significant Bit*** **(LSB)**. Pesan yang disisipkan dapat berupa teks maupun berkas dengan tipe apa pun. Program juga harus mendukung opsi penyisipan secara sekuensial atau acak berdasarkan *seed* yang diberikan, serta enkripsi menggunakan **A5/1** sebelum pesan disisipkan ke dalam video.

Program harus memenuhi ketentuan umum berikut:

- Media pembawa yang digunakan adalah video digital berformat AVI.
- Program harus menghasilkan keluaran berupa *stego-video* yang juga disimpan dalam format AVI.
- Program menerima pesan dalam bentuk teks atau berkas dengan *extension* sembarang.
- Program mendukung metode penyisipan *LSB* pada piksel, misalnya setiap 8 bit pesan dibagi menjadi 3 bit pada R, 3 bit pada G, dan 2 bit pada B, atau skema lain yang dirancang sendiri. Konfigurasi dapat diatur saat program dijalankan.



Gambar 2. Contoh skema LSB 3-3-2. Sumber: Nados, W. L., & Rasheed, N. A. (2019)

- Implementasi steganografi dan enkripsi-dekripsi harus dibuat sendiri.
- Penggunaan pustaka untuk membaca, menulis, atau memproses video diperbolehkan, selama sumbernya disebutkan dengan jelas.
- Program diimplementasikan dengan bahasa **Python** atau **Java**.
- Antarmuka program dibuat dalam bentuk GUI. Pustaka GUI yang digunakan dibebaskan dan disesuaikan dengan bahasa pemrograman yang dipilih.
- Program dapat dijalankan setidaknya pada sistem operasi **Windows**.

B. Ketentuan Penyisipan Pesan

Masukan yang diperlukan pada proses penyisipan disajikan pada Tabel 1.

Komponen	Keterangan
Video cover	Berkas video AVI sebagai *cover-object*
Pesan rahasia	Teks atau berkas
Enkripsi	Pilihan penggunaan enkripsi atau tidak
Kunci A5/1	Digunakan jika enkripsi dipilih
Mode penyisipan	Sekuensial atau acak
Stego-key	Digunakan jika penyisipan acak dipilih
Keluaran	Nama berkas *stego-video*

Tabel 1. Masukan pada proses penyisipan pesan

Ketentuan proses penyisipan:

- Penyisipan dilakukan pada *frame-frame* video dengan metode LSB.
- Pesan disisipkan pada seluruh piksel pada setiap *frame*. Jika sebuah *frame* telah terisi penuh, proses penyisipan akan dilanjutkan ke *frame* berikutnya.
- Program harus mendukung dua mode penyisipan untuk seluruh *frame*:
    - Sekuensial, yaitu bit-bit pesan disisipkan pada posisi piksel yang berurutan.
    - Acak, yaitu bit-bit pesan disisipkan pada posisi piksel acak berdasarkan *seed* dari *stego-key* yang diberikan.
- Apabila enkripsi digunakan, pesan harus dienkripsi terlebih dahulu menggunakan **A5/1** sebelum disisipkan.
- Untuk enkripsi A5/1, *payload* dibagi ke dalam blok-blok 228-bit dan program membangkitkan nilai F_n secara otomatis untuk setiap blok.
- Beberapa properti berkas pesan rahasia dan karakteristik metode penyisipan dapat disimpan agar informasinya tersimpan untuk proses ekstraksi. Informasi ini dapat mencakup:
    - Jenis pesan, yaitu teks atau berkas.
    - *Extension* berkas apabila pesan berupa berkas.
    - Ukuran pesan.
    - Nama berkas asli.
    - Informasi apakah *payload* dienkripsi atau tidak.
    - Informasi apakah penyisipan dilakukan secara sekuensial atau acak.
    - Informasi lain yang diperlukan untuk membaca kembali *payload* secara benar.

Metode penyimpanan informasi tersebut dibebaskan, baik menggunakan *header*, penanda tertentu, maupun metode lain yang dianggap sesuai. Informasi yang disimpan dan metode penyimpanannya dapat ditentukan sesuai kebutuhan, selama proses ekstraksi tetap dapat dilakukan dengan benar.

- Kunci enkripsi dan *stego-key* **tidak boleh** disisipkan ke dalam *stego-video*.

C. Ketentuan Ekstraksi Pesan

Masukan yang diperlukan pada proses ekstraksi pesan disajikan pada Tabel 2.

Komponen	Keterangan
Stego-video	Berkas AVI yang telah disisipi pesan
Kunci A5/1	Digunakan jika pesan sebelumnya dienkripsi
Stego-key	Digunakan jika penyisipan sebelumnya dilakukan secara acak

Tabel 2. Masukan pada proses ekstraksi pesan

Ketentuan ekstraksi:

- Jika pesan yang ditemukan berupa teks, program cukup menampilkannya.
- Jika berupa berkas, program harus menyediakan mekanisme *save as* untuk menyimpan hasil ekstraksi sebagai file.
- Nama berkas asli harus ditampilkan sebagai nilai bawaan (*default*) pada saat penyimpanan hasil ekstraksi.

D. Ketentuan Tambahan

- Program harus menghitung kapasitas sisip sebelum proses penyisipan dilakukan.
- Program menolak penyisipan jika ukuran pesan rahasia melebihi batas kapasitas sisip.
- Program mampu menghitung dan menampilkan nilai kualitas visual secara otomatis setelah proses penyisipan atau ekstraksi selesai. Perhitungan mencakup:
    - **Mean Squared Error (MSE):** Menghitung rata-rata selisih kuadrat antara piksel *video cover* (C) dan *stego-video* (S).

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [C(i,j) - S(i,j)]^2$$

    - **Peak Signal-to-Noise Ratio (PSNR):** Menghitung rasio antara daya maksimum sinyal terhadap daya derau yang merusak. Nilai PSNR yang tinggi (dalam dB) menunjukkan kualitas steganografi yang lebih baik.

$$PSNR = 10 \times \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

    - Metrik ini harus ditampilkan pada antarmuka GUI untuk setiap *frame* yang diproses atau sebagai nilai rata-rata keseluruhan video.
- Program menyediakan fitur visualisasi untuk membandingkan histogram warna (Red, Green, Blue) antara *frame* pada video asli dengan *frame* pada *stego-video*.
- *Stego-video* yang dihasilkan harus tetap dapat dibuka dan diputar dengan baik.

E. Kreativitas

Metode implementasi untuk aspek-aspek berikut dibebaskan:

- Design GUI (selama memenuhi seluruh ketentuan program).
- Metode transformasi *stego-key* menjadi *seed* dibebaskan.
- Metode penyimpanan metadata yang diperlukan untuk proses ekstraksi.
- Pemilihan *frame* yang digunakan untuk penyisipan pesan, misalnya seluruh *frame*, *frame* tertentu, atau berdasarkan kriteria lain yang dirancang sendiri.

Bonus

- Program juga dapat melakukan penyisipan pada video cover digital *lossy* berformat MP4 dan menghasilkan keluaran dalam format yang sama. (15 Poin)

Pengumpulan

Pengumpulan dilakukan dengan melakukan ***release*** pada repositori Github sebelum tenggat waktu pengerjaan. Revisi pengumpulan dapat dilakukan dengan membuat release baru.

1. Repositori Perangkat Lunak

Repositori harus memuat:

a. Kode sumber (*source code*).
b. Berkas eksekutabel (*executable file*), jika relevan.
c. Folder berisi berkas uji.
d. Dokumen laporan
e. README yang minimal berisi:
    i. Nama dan deskripsi program.
    ii. Teknologi yang digunakan (*tech stack*).
    iii. Dependensi.
    iv. Tata cara menjalankan program.

2. Video Demo

Video demo berdurasi maksimal 10 menit, berisi:

a. Deskripsi singkat program.
b. Penjelasan singkat rancangan, terutama bagian yang dibebaskan atau dirancang sendiri.

c. Demo kasus uji utama (sesuai dengan ketentuan kasus uji pada 3.d.).

Apabila terdapat proses yang memerlukan waktu lama untuk dijalankan, video demo dapat dipotong pada bagian tersebut selama alur demonstrasi tetap jelas.

3. Laporan

Laporan diunggah pada repositori dengan nama **NIM1_NIM2_NIM3_Tugas2_II4021.pdf**, berisi:

a. Foto anggota kelompok di *cover* laporan sebagai pengganti logo gajah,
b. Pernyataan tidak melakukan kecurangan yang ditandatangani dengan format sebagai berikut:

Kami menyatakan bahwa kode program yang dihasilkan bukan merupakan hasil salinan mentah (*raw output*) dari *Generative AI*, melainkan hasil pengembangan dan penulisan mandiri. [Tanda tangan Mahasiswa 1] [Tanda tangan Mahasiswa 2] [Tanda tangan Mahasiswa 3] [Nama Mahasiswa 1] [Nama Mahasiswa 2] [Nama Mahasiswa 3]

c. Teori singkat mengenai steganografi, LSB, stream cipher, A5/1, dan konsep relevan lainnya,
d. Perancangan dan implementasi, pastikan untuk menjelaskan implementasi bagian yang dibebaskan dan bonus,
e. Pengujian program dan analisis hasil, dengan minimal kasus uji mencakup:
    i. Semua kombinasi konfigurasi (minimal 3 metode konfigurasi LSB dikombinasikan dengan seluruh metode penyisipan dan enkripsi). Analisis hasil PSNR dan Histogram untuk masing-masing kasus,
    ii. Penyisipan yang melebihi batas kapasitas sisip,
    iii. Penyisipan dengan berbagai jenis berkas (.txt, .pdf, .docx, .png, .jpg, .exe, dan lainnya),
    iv. Untuk setiap kasus uji, cek integritas berkas pesan rahasia asli dibandingkan dengan berkas pesan rahasia hasil ekstraksi (gunakan algoritma seperti md5sum atau sha256sum),
f. Kesimpulan dari hasil implementasi,
g. Daftar pustaka,
h. Lampiran berisi:
    i. Pranala repositori
    ii. Pranala video demo
    iii. Pembagian tugas

Referensi

Referensi berikut disediakan sebagai bahan pendukung, bukan sebagai batasan atau standar implementasi. Sumber lain yang relevan tetap dapat digunakan.

- Hiding Text in AVI Video File by Method of Least Significant Bit