

Tugas Kecil II
IF4020 Kriptografi

Steganografi pada Berkas Audio dengan Metode *Multiple-LSB*



Disusun oleh:

| | |
|---------------------------|----------|
| Bryan Cornelius Lauwrence | 13522033 |
| Vanson Kurnialim | 13522049 |

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
2025

BAB I

Teori Singkat

Steganografi berasal dari bahasa Yunani, yaitu *steganos*, yang berarti tersembunyi dan *graphien*, yang berarti tulisan. Jadi, steganografi adalah ilmu dan seni menyembunyikan pesan rahasia dengan suatu cara, sedemikian sehingga tidak seorang pun yang mencurigai keberadaan pesan tersebut. Berbeda dengan kriptografi yang menyembunyikan makna pesan, steganografi bertujuan untuk menyembunyikan keberadaan pesan. Salah satu contoh steganografi yang umum adalah menyisipkan huruf-huruf pada suatu pesan rahasia di setiap kata terakhir pada suatu pesan *cover*-nya.

Pesan yang dapat disembunyikan dengan steganografi tidak hanya pesan fisik, tetapi juga pesan digital yang disembunyikan melalui suatu media digital (teks, audio, video, gambar, dll). Prosesnya melalui penyembunyian suatu pesan rahasia dalam sebuah file *cover* menghasilkan suatu *stego-object* yang secara kasat mata tidak berbeda dengan *cover* asli. Pesan rahasia pun dapat dienkripsi untuk lebih menyembunyikan rahasia apabila rahasia berhasil diekstrak oleh pihak lain.

Salah satu metode steganografi digital adalah metode LSB (*Least Significant Bits*). Idenya, dalam setiap *byte* yang bit-bitnya tersusun dari kiri ke kanan dalam urutan yang menurun. Jadi, bit paling kiri nilainya paling besar dan bit paling kanan nilainya paling kecil. Bit dengan nilai kecil itulah yang disebut sebagai LSB. Perubahan nilai LSB tidak akan mengubah nilai *byte* secara signifikan, misalnya 11010001 yang bernilai 209 akan menjadi 208 bila bit paling kanan diubah menjadi nol, tetapi akan menjadi 81 bila bit paling kiri diubah menjadi nol. Perubahan nilai tersebut akan sulit disadari manusia karena banyaknya nilai *byte*. Dengan demikian, pesan tersembunyi dapat dipecah bit-bitnya satu per satu dan disisipkan pada LSB dari *byte-byte cover* sehingga nilai *byte* akan berubah, tetapi perubahannya tidak kasat mata. Proses ekstraksinya pun dilakukan dengan mengambil kembali LSB dari *stego-object* dan disusun menjadi bentuk awal pesan rahasia.

Metode LSB memiliki beberapa varian. Yang pertama varian *sequential*, yaitu menyembunyikan pesan secara berurutan pada *cover* dimulai dari *byte* paling awal. Kedua, varian acak, yaitu pesan disembunyikan secara acak pada *byte* yang tidak menentu. Nilai acak diciptakan dari suatu kunci sebagai *seed* supaya bilangan acak tersebut tidak menghilang. Ketiga, m-bit LSB, yaitu menyisipkan rahasia dengan menggunakan sebanyak m bit LSB dari setiap *byte*. Cara ini dapat meningkatkan ukuran maksimal pesan rahasia yang ingin disembunyikan, tetapi nilai m tidak boleh terlalu besar karena dapat merusak kualitas *cover*. Terakhir, dengan menambahkan enkripsi pada pesan rahasia sebelum disisipkan pada *cover*.

File yang digunakan sebagai *cover* pada kasus ini adalah file berekstensi mp3, yaitu format kompresi data untuk encode audio digital yang umumnya musik. File MP3 menjadi populer karena mampu menyajikan kualitas audio yang baik dengan penyimpanan yang lebih hemat. Struktur MP3 pada dasarnya sebagai berikut:

[TAG v2] Frame1 Frame2 ... FrameN [TAG v1]

yang *tag*-nya menyimpan metadata terkait audio. *Frame* merupakan data-data suara yang setiap *frame*-nya merupakan suara untuk 0,026 detik.

Frame ditandai dengan adanya *header* 4 byte yang formatnya sebagai berikut (satu huruf merupakan satu bit):

AAAAAAAA AAABBCCD EEEFFGH IJJKLMM

A merupakan *frame synchronizer* yang seluruh bitnya bernilai 1, ini merupakan penanda mulainya *header*. B adalah versi ID MPEG, 00 adalah versi 2.5, 10 versi 2, dan 11 versi 1. C merupakan *layer*, 01 adalah *layer* III, 10 adalah *layer* II, dan 11 adalah *layer* I. D menandakan *frame* tersebut diproteksi oleh *checksum* atau tidak. E berisi *bitrate index* dalam kbps. F menyimpan *sampling rate frequency index*. G menandakan ada tidaknya *padding*. H tidak memiliki fungsi. I merupakan *channel*, 00 untuk stereo, 01 untuk joint stereo, 10 untuk dual, dan 11 untuk mono. J untuk ekstensi. K bernilai 1 jika audio memiliki hak cipta. L menandakan orisinalitas audio. Terakhir, M merupakan *emphasis*. Dengan demikian, *header* dari setiap *frame* sebaiknya tidak diubah karena dapat mengubah proses pengolahan audio atau bahkan menghilangkan suatu *header*.

BAB II

Perancangan dan Implementasi

Program yang dibuat dirancang untuk melakukan dua operasi utama, yaitu penyisipan (*embedding*) pesan/berkas rahasia ke dalam berkas audio MP3 (*cover audio*), serta ekstraksi (*extracting*) pesan/berkas rahasia dari berkas audio yang merupakan *stego-object*. Terdapat program-program untuk mendukung fungsi lainnya seperti enkripsi dekripsi, pembangkit titik acak, serta pemutar audio.

Bahasa pemrograman yang digunakan untuk implementasi adalah Python 3.12. Arsitektur sistem dibagi menjadi beberapa modul utama, yaitu pemrosesan file, penyisipan dan ekstraksi pesan rahasia, enkripsi dan dekripsi, pembangkit titik acak, dan pemutar lagu. Masing-masing modul memiliki fungsi, parameter, dan tujuan sebagai berikut:

1. Pemrosesan file

Mengurusi segala proses perubahan berkas menjadi data dalam program (*binaries*) dan juga sebaliknya.

| FileProcessor.py | | | |
|------------------|--|--|---|
| Nama Fungsi | Parameter | Tipe Output | Tujuan |
| bstr | n: integer | string | Mengkonversi integer (0 - 255) menjadi 8-bit biner |
| read_input | path: string cover: boolean key: string null | cover.txt bila cover true atau sisip.txt | Membaca file berekstensi apapun dari path dan menyimpannya dalam representasi bit-bit di file txt. Bit dienkripsi jika key memiliki nilai |
| read_input_stega | path: string | stega.txt | Membaca <i>stego-object</i> path dan menyimpannya dalam representasi bit-bit di file txt. |
| write_stega | fileName: string key: string null | fileName | Membaca stega.txt (hasil sisip) dan menyimpannya ke fileName dengan menulis per bytenya. |

| | | | |
|-------------------|--|----------|--|
| read_write_secret | fileName: string key: string null | fileName | Membaca extracted.txt (hasil ekstraksi) dan menyimpannya ke fileName dengan menulis per bytenya. Mendekripsi jika key memiliki nilai |
|-------------------|--|----------|--|

2. Penyisipan dan ekstraksi pesan rahasia

Melakukan proses *embedding* file rahasia ke file *cover* serta *extracting* dari file yang diberikan. Proses *embedding* akan melewati header *frame* pertama serta *tag* MP3 bila ada.

| Sisip.py | | | |
|------------------------|--|-----------------|--|
| Nama Fungsi | Parameter | Tipe Output | Tujuan |
| bits_from_lines | lines: array of string | string | Menggabungkan setiap elemen array menjadi satu string dengan mengabaikan <i>whitespace</i> |
| lines_from_bits | bits: string chunk: integer | array of string | Memecah string panjang menjadi elemen array dengan panjang chunk per elemen (nilai default 8) |
| int_to_bits | value: integer width: integer | string | Mengubah bilangan bulat (0 - 255) menjadi biner sepanjang width |
| bits_to_int | b: string | integer | Mengubah string biner menjadi integer |
| find_max_start_sisip | nLSB: integer firstHeader: integer stego_metadata: integer | integer | Mencari lokasi index mulai maksimal yang dapat digunakan untuk proses penyisipan berdasarkan jumlah LSB, posisi header pertama, dan penyimpanan informasi sisip sebelum proses sisip |
| find_max_start_ekstrak | nLSB: integer firstHeader: integer stego_metadata: integer output_size: | integer | Mencari lokasi index mulai maksimal yang dapat digunakan untuk proses penyisipan berdasarkan jumlah LSB, posisi header pertama, penyimpanan informasi sisip, |

| | | | |
|---------------------|---|---------------|---|
| | integer | | dan ukuran file rahasia sebelum proses ekstraksi |
| find_spesific_index | firstHeader: integer stego_metadata: integer i: integer | integer | Mencari lokasi byte mulai spesifik dari file <i>cover</i> |
| find_audio_start | cover_bytes: array of integer | integer | Mengembalikan lokasi byte yang merupakan header pertama |
| sisip | random_seed: string null n_lsb: integer | stega.txt | Menyisipkan bit-bit dari sisip.txt ke cover.txt berdasarkan jumlah LSB. Memulai dari titik acak jika random_seed memiliki nilai |
| ekstrak | random_seed: string null | extracted.txt | Mengekstrak bit-bit rahasia dari stega.txt dan menyimpan hasilnya ke extracted.txt. Memulai dari titik acak jika random_seed memiliki nilai |

3. Enkripsi-Dekripsi

Enkripsi dan dekripsi menggunakan metode Vigenere Cipher. Namun, dalam kasus ini perputaran nilainya adalah 256 karena 1 byte bernilai 0 sampai 255 sehingga, pada proses enkripsi, nilai angka asli ditambah nilai kunci akan dimodulo dengan 256, begitu juga untuk proses dekripsi

| Vigenere.py | | | |
|------------------|---------------------------------|-------------|---|
| Nama Fungsi | Parameter | Tipe Output | Tujuan |
| encrypt_vigenere | plain: integer key: integer | integer | Menjumlahkan byte plain dengan byte key lalu dimodul dengan 256 |
| decrypt_vigenere | cipher: integer key: integer | integer | Mengurangi byte cipher dengan byte key lalu dimodul dengan 256 |

4. Pembangkit titik acak

Titik acak dibangkitkan dari suatu string. Metode yang digunakan adalah menjumlahkan representasi angka dari setiap karakternya yang dikalikan dengan posisi karakter tersebut. Persamaannya sebagai berikut:

$$\sum_{i=1}^n (i \times string_i)$$

dengan karakter pertama adalah karakter paling kiri.

| Randomizer.py | | | |
|-----------------|-----------------------------|-------------|---|
| Nama Fungsi | Parameter | Tipe Output | Tujuan |
| generate_random | key: string max: integer | integer | Menghasilkan angka acak yang berkisar dari 0 sampai max-1 |

5. Pemutar lagu

Memutar audio ketika berkas selesai disisip kedalam audio *cover* ataupun memutar audio sesuai masukan pengguna.

| PlaySong.py | | | |
|-------------|--------------------|----------------|-------------------------------------|
| Nama Fungsi | Parameter | Tipe Output | Tujuan |
| play_song | file_path : string | audio terputar | Memainkan audio sesuai dengan input |

Dengan memanfaatkan modul-modul di atas, operasi utama program ini secara umum berjalan dengan alur seperti berikut :

- Sisip (*embedding*)
 - Membaca audio cover menjadi data dan disimpan dalam cover.txt
 - Membaca berkas sisip menjadi data dan disimpan dalam sisip.txt
 - Melakukan enkripsi jika ada kepada konten dalam sisip.txt
 - Melakukan penyisipan dari sisip.txt ke dalam konten cover.txt dan disimpan dalam stega.txt
 - Mengubah stega.txt menjadi berkas audio yang telah berhasil disisip.
- Ekstraksi (*extracting*).
 - Membaca stega-audio menjadi data dan disimpan dalam stega.txt.

- Mengambil data sisipan dari *stega.txt* dan disusun kembali ke dalam *extracted.txt*
- Mengubah kembali data menjadi berkas rahasia yang berhasil diekstrak dari audio *cover*.

Segala aspek pemrograman dan komponen yang telah dijelaskan di atas akan dikumpulkan menjadi satu antarmuka (*interface*) CLI yang diurus oleh fungsi utama *Main.py*. Terdapat pilihan fitur sebagai berikut ketika program dijalankan:

1. Sisip pesan
 - a. Input nama file *cover* MP3 (harus berekstensi mp3)
 - b. Input nama file pesan rahasia dengan ekstensi apapun
 - c. Input nama file yang akan menjadi *stego-object* (harus berekstensi mp3)
 - d. Masukkan jumlah LSB untuk menyimpan berkas rahasia, bernilai 1, 2, atau 4
 - e. Masukkan kunci enkripsi bila ingin menggunakan enkripsi
 - f. Masukkan string pembangkit bilangan acak bila ingin menggunakan menggunakannya
 - g. Program akan menyisipkan pesan rahasia sesuai nama file pada tahap c dan memutar file *stego-object*.
2. Ekstrak pesan
 - a. Input nama file *stego-object* (harus berekstensi mp3)
 - b. Input nama file pesan rahasia hasil ekstraksi
 - c. Masukkan kunci enkripsi yang sama dengan yang sebelumnya digunakan
 - d. Masukkan string pembangkit bilangan acak yang sama dengan yang sebelumnya digunakan.
 - e. Program akan membuat file berkas rahasia dari file *stego-object* dan menyimpannya sesuai nama file pada poin b.
3. Putar lagu
 - a. Input nama file MP3 pada folder output.
 - b. Program akan menjalankan audio jika ditemukan file yang bersangkutan.

Untuk memudahkan pembeda jenis berkas, yang meliputi *cover*, berkas rahasia, *stego-object*, serta hasil ekstraksi, berkas yang akan digunakan harus berada pada folder penempatan yang sesuai. Ketentuannya ada sebagai berikut :

- Folder sound : berkas audio *cover* dan

- Folder output : berkas audio hasil sisip
- Folder secret : berkas yang ingin disembunyikan
- Folder ekstraksi : berkas sisip hasil ekstraksi

Proses sisip dan ekstraksi pasti bisa dilakukan, tetapi audio akan tetap rusak jika berkas rahasia cukup besar. Yang menyebabkan ini adalah format MP3 yang tersusun atas *frame-frame*. *Header* dari suatu *frame* memang bisa dilompati saat proses penyisipan karena adanya mulainya *header* ditandai dengan adanya *frame synchronizer*. Namun, proses penyisipan memiliki kemungkinan menambahkan *header* baru. Misalnya, byte audio awalnya berupa 1111111011101011 yang akan disisipi 2 nilai bit 10. Byte audio akan berubah menjadi 1111111111101010. Awalnya bukan *header*, tetapi berubah menjadi *header* setelah disisipi. Hal tersebut tidak memengaruhi proses ekstraksi karena dari *header* asli dapat dicari panjang *frame*. Namun, ketika audio *stego-object* dijalankan, audio akan rusak karena MP3 mendeteksi adanya *header* baru.

BAB III

Pengujian Program dan Analisis Hasil

Pengujian akan dilakukan dengan menyisipkan beberapa berkas dengan ekstensi dan besaran yang berbeda. Penilaian hasil akan dilakukan dengan membandingkan berkas sisipan dan berkas hasil ekstraksi serta kualitas audio *cover* sebelum dan sesudah penyisipan.

1. Kombinasi konfigurasi (penggunaan enkripsi dan titik acak)

| Kasus Uji | | Percobaan | Perbandingan Berkas |
|-----------|------------|--|---|
| Enkripsi | Titik Acak | | |
| No | No | <pre> Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 1 === Penyisipan Pesan Rahasia ke File Audio === Masukkan file beserta ekstensi! Masukkan nama file cover (mp3): campina.mp3 Masukkan nama file pesan rahasia: tes.txt Masukkan path file output penyisipan pesan (mp3): output-1-polos.mp3 Masukkan jumlah LSB yang digunakan (1, 2, 4): 1 Masukkan kunci enkripsi (tekan enter untuk tanpa kunci): Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): Menyisipkan berkas rahasia... Pesan berhasil disisipkan ke dalam output\output-1-polos.mp3 Tekan Enter untuk menghentikan pemutaran lagu... [✓] PSNR antara sound\campina.mp3 dan output\output-1-polos.mp3: 79.26 dB [Q] Kualitas masih baik (>= 30 dB) Hello from the pygame community. https://www.pygame.org/contrib Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 2 === Ekstraksi Pesan Rahasia dari File Audio === Masukkan nama file audio (mp3): output-1-polos.mp3 Masukkan nama file output ekstraksi pesan: hasil-1-1.mp3 Masukkan kunci dekripsi (tekan enter untuk tanpa kunci): Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): Mengekstrak berkas rahasia... Pesan berhasil diekstrak ke dalam ekstraksi\hasil-1-1.mp3 </pre> | <pre>\$ diff ekstraksi/hasil-1-1.txt secret/tes.txt (venv)</pre> <p>File sama</p> |
| Yes | No | <pre> Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 1 === Penyisipan Pesan Rahasia ke File Audio === Masukkan file beserta ekstensi! Masukkan nama file cover (mp3): campina.mp3 Masukkan nama file pesan rahasia: tes.txt Masukkan path file output penyisipan pesan (mp3): output-1-enkrip.mp3 Masukkan jumlah LSB yang digunakan (1, 2, 4): 1 Masukkan kunci enkripsi (tekan enter untuk tanpa kunci): kunci Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): Menyisipkan berkas rahasia... Pesan berhasil disisipkan ke dalam output\output-1-enkrip.mp3 Tekan Enter untuk menghentikan pemutaran lagu... [✓] PSNR antara sound\campina.mp3 dan output\output-1-enkrip.mp3: 78.81 dB [Q] Kualitas masih baik (>= 30 dB) </pre> | <pre>\$ diff ekstraksi/hasil-1-2.txt secret/tes.txt (venv)</pre> <p>File sama</p> |

| | | | |
|-----|-----|--|--|
| | | <pre> Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 2 === Ekstraksi Pesan Rahasia dari File Audio === Masukkan nama file audio (mp3): output-1-enkrip.mp3 Masukkan nama file output ekstraksi pesan: hasil-1-2.txt Masukkan kunci dekripsi (tekan enter untuk tanpa kunci): kunci Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): Mengekstrak berkas rahasia... Pesan berhasil diekstrak ke dalam ekstraksi\hasil-1-2.txt </pre> | |
| No | Yes | <pre> Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 1 === Penyisipan Pesan Rahasia ke File Audio === Masukkan file beserta ekstensi! Masukkan nama file cover (mp3): campina.mp3 Masukkan nama file pesan rahasia: tes.txt Masukkan path file output penyisipan pesan (mp3): output-1-3.mp3 Masukkan jumlah LSB yang digunakan (1, 2, 4): 1 Masukkan kunci enkripsi (tekan enter untuk tanpa kunci): Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): seed Menyisipkan berkas rahasia... Pesan berhasil disisipkan ke dalam output\output-1-3.mp3 Tekan Enter untuk menghentikan pemutaran lagu... [✓] PSNR antara sound\campina.mp3 dan output\output-1-3.mp3: 78.84 dB [✓] Kualitas masih baik (>= 30 dB) Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 2 === Ekstraksi Pesan Rahasia dari File Audio === Masukkan nama file audio (mp3): output-1-3.mp3 Masukkan nama file output ekstraksi pesan: hasil-1-3.txt Masukkan kunci dekripsi (tekan enter untuk tanpa kunci): Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): seed Mengekstrak berkas rahasia... Pesan berhasil diekstrak ke dalam ekstraksi\hasil-1-3.txt </pre> | <pre> C:\Users\Zaki\OneDrive\Desktop> diff secret\tes.txt ekstraksi\hasil-1-3.txt 0a1,2 \$ diff secret/tes.txt ekstraksi/hasil-1-3.txt (vnmv) </pre> <p>File sama</p> |
| Yes | Yes | <pre> Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 1 === Penyisipan Pesan Rahasia ke File Audio === Masukkan file beserta ekstensi! Masukkan nama file cover (mp3): campina.mp3 Masukkan nama file pesan rahasia: tes.txt Masukkan path file output penyisipan pesan (mp3): output-1-4.mp3 Masukkan jumlah LSB yang digunakan (1, 2, 4): 1 Masukkan kunci enkripsi (tekan enter untuk tanpa kunci): kunci Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): seed Menyisipkan berkas rahasia... Pesan berhasil disisipkan ke dalam output\output-1-4.mp3 Tekan Enter untuk menghentikan pemutaran lagu... [✓] PSNR antara sound\campina.mp3 dan output\output-1-4.mp3: 78.88 dB [✓] Kualitas masih baik (>= 30 dB) Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 2 === Ekstraksi Pesan Rahasia dari File Audio === Masukkan nama file audio (mp3): output-1-4.mp3 Masukkan nama file output ekstraksi pesan: hasil-1-4.txt Masukkan kunci dekripsi (tekan enter untuk tanpa kunci): kunci Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): seed Mengekstrak berkas rahasia... Pesan berhasil diekstrak ke dalam ekstraksi\hasil-1-4.txt </pre> | <pre> C:\Users\Zaki\OneDrive\Desktop> diff secret\tes.txt ekstraksi\hasil-1-4.txt 0a1,2 \$ diff secret/tes.txt ekstraksi/hasil-1-4.txt (vnmv) </pre> <p>File sama</p> |

2. Kombinasi LSB

| Kasus Uji | Percobaan | Perbandingan Berkas |
|-----------|---|---|
| 1-LSB | <div><pre>Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 1 === Penyisipan Pesan Rahasia ke File Audio === Masukkan file beserta ekstensi! Masukkan nama file cover (mp3): campina.mp3 Masukkan nama file pesan rahasia: tes.txt Masukkan path file output penyisipan pesan (mp3): output-2-1.mp3 Masukkan jumlah LSB yang digunakan (1, 2, 4): 1 Masukkan kunci enkripsi (tekan enter untuk tanpa kunci): Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): Menyisipkan berkas rahasia... Pesan berhasil disisipkan ke dalam output\output-2-1.mp3 Tekan Enter untuk menghentikan pemutaran lagu... [✓] PSNR antara sound\campina.mp3 dan output\output-2-1.mp3: 79.26 dB 🔊 Kualitas masih baik (>= 30 dB)</pre></div> <div><pre>Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 2 === Ekstraksi Pesan Rahasia dari File Audio === Masukkan nama file audio (mp3): output-2-1.mp3 Masukkan nama file output ekstraksi pesan: hasil-2-1.txt Masukkan kunci dekripsi (tekan enter untuk tanpa kunci): Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): Mengekstrak berkas rahasia... Pesan berhasil diekstrak ke dalam ekstraksi\hasil-2-1.txt (venv)</pre></div> | <div><pre>Zaki@DESKTOP-0GQ6GVD MINGW64 ~/./0/1.KULIAH/Semester7/Kripto \$ diff secret/tes.txt ekstraksi/hasil-2-1.txt (venv)</pre></div> <p>File sama</p> |
| 2-LSB | <div><pre>Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 1 === Penyisipan Pesan Rahasia ke File Audio === Masukkan file beserta ekstensi! Masukkan nama file cover (mp3): campina.mp3 Masukkan nama file pesan rahasia: tes.txt Masukkan path file output penyisipan pesan (mp3): hasil-2-2.mp3 Masukkan jumlah LSB yang digunakan (1, 2, 4): 2 Masukkan kunci enkripsi (tekan enter untuk tanpa kunci): Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): Menyisipkan berkas rahasia... Pesan berhasil disisipkan ke dalam output\hasil-2-2.mp3 Tekan Enter untuk menghentikan pemutaran lagu... [✓] PSNR antara sound\campina.mp3 dan output\hasil-2-2.mp3: 75.13 dB 🔊 Kualitas masih baik (>= 30 dB)</pre></div> <div><pre>Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 2 === Ekstraksi Pesan Rahasia dari File Audio === Masukkan nama file audio (mp3): output-2-2.mp3 Masukkan nama file output ekstraksi pesan: hasil-2-2.txt Masukkan kunci dekripsi (tekan enter untuk tanpa kunci): Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): Mengekstrak berkas rahasia... Pesan berhasil diekstrak ke dalam ekstraksi\hasil-2-2.txt (venv)</pre></div> | <div><pre>Zaki@DESKTOP-0GQ6GVD MINGW64 ~/./0/1.KULIAH/Semester7/Kripto \$ diff secret/tes.txt ekstraksi/hasil-2-2.txt (venv)</pre></div> <p>File sama</p> |

| | | |
|-------|---|--|
| 4-LSB | <pre>Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 1 === Penyisipan Pesan Rahasia ke File Audio === Masukkan file beserta ekstensi! Masukkan nama file cover (mp3): campina.mp3 Masukkan nama file pesan rahasia: tes.txt Masukkan path file output penyisipan pesan (mp3): output-2-3.mp3 Masukkan jumlah LSB yang digunakan (1, 2, 4): 4 Masukkan kunci enkripsi (tekan enter untuk tanpa kunci): Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): Menyisipkan berkas rahasia... Pesan berhasil disisipkan ke dalam output\output-2-3.mp3 Tekan Enter untuk menghentikan pemutaran lagu... [✓] PSNR antara sound\campina.mp3 dan output\output-2-3.mp3: 70.05 dB 🔊 Kualitas masih baik (>= 30 dB) Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 2 === Ekstraksi Pesan Rahasia dari File Audio === Masukkan nama file audio (mp3): output-2-3.mp3 Masukkan nama file ekstraksi pesan: hasil-2-3.txt Masukkan kunci dekripsi (tekan enter untuk tanpa kunci): Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): Mengekstrak berkas rahasia... Pesan berhasil diekstrak ke dalam ekstraksi\hasil-2-3.txt</pre> | <pre>Zaki@DESKTOP-BGQ6QVD: ~/0/1.KULIAH/Semester7/Kriptografi \$ diff secret/tes.txt ekstraksi/hasil-2-3.txt (venv)</pre> <p>File sama</p> |
|-------|---|--|

3. Berkas melebihi kapasitas

| Kasus Uji | Percobaan |
|---|--|
| Cover: campina.mp3 Secret: campina.mp3 | <pre>Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 1 === Penyisipan Pesan Rahasia ke File Audio === Masukkan file beserta ekstensi! Masukkan nama file cover (mp3): campina.mp3 Masukkan nama file pesan rahasia: tes.mp3 Masukkan path file output penyisipan pesan (mp3): output-3-1.mp3 Masukkan jumlah LSB yang digunakan (1, 2, 4): 1 Masukkan kunci enkripsi (tekan enter untuk tanpa kunci): Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): Menyisipkan berkas rahasia... Terjadi kesalahan: Cover tidak cukup untuk berkas rahasia.</pre> |

4. Berbagai tipe berkas sisip

| Kasus Uji | Percobaan | Perbandingan Berkas |
|-----------|-----------|---------------------|
|-----------|-----------|---------------------|

| | | |
|-------------|--|--|
| <p>.txt</p> | <pre>Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 1 === Penyisipan Pesan Rahasia ke File Audio === Masukkan file beserta ekstensi! Masukkan nama file cover (mp3): campina.mp3 Masukkan nama file pesan rahasia: tes.txt Masukkan path file output penyisipan pesan (mp3): output-4-1.mp3 Masukkan jumlah LSB yang digunakan (1, 2, 4): 4 Masukkan kunci enkripsi (tekan enter untuk tanpa kunci): Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): Menyisipkan berkas rahasia... Pesan berhasil disisipkan ke dalam output\output-4-1.mp3 Tekan Enter untuk menghentikan pemutaran lagu... ✅ PSNR antara sound\campina.mp3 dan output\output-4-1.mp3: 70.05 dB 🔊 Kualitas masih baik (>= 30 dB)</pre> <pre>Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 2 === Ekstraksi Pesan Rahasia dari File Audio === Masukkan nama file audio (mp3): output-4-1.mp3 Masukkan nama file output ekstraksi pesan: hasil-4-1.txt Masukkan kunci dekripsi (tekan enter untuk tanpa kunci): Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): Mengekstrak berkas rahasia... Pesan berhasil diekstrak ke dalam ekstraksi\hasil-4-1.txt</pre> | <pre>zaki@DESKTOP-8GQ6GV0 MINGW64 ~/0/1.KULIAH/Semester7/Kriptografi \$ diff secret/tes.txt ekstraksi/hasil-4-1.txt (venv)</pre> <p>File sama</p> |
| <p>.png</p> | <pre>Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 1 === Penyisipan Pesan Rahasia ke File Audio === Masukkan file beserta ekstensi! Masukkan nama file cover (mp3): campina.mp3 Masukkan nama file pesan rahasia: tes.png Masukkan path file output penyisipan pesan (mp3): output-4-2.mp3 Masukkan jumlah LSB yang digunakan (1, 2, 4): 4 Masukkan kunci enkripsi (tekan enter untuk tanpa kunci): Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): Menyisipkan berkas rahasia... Pesan berhasil disisipkan ke dalam output\output-4-2.mp3 Tekan Enter untuk menghentikan pemutaran lagu... ✅ PSNR antara sound\campina.mp3 dan output\output-4-2.mp3: 50.07 dB 🔊 Kualitas masih baik (>= 30 dB)</pre> <pre>Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 2 === Ekstraksi Pesan Rahasia dari File Audio === Masukkan nama file audio (mp3): output-4-2.mp3 Masukkan nama file output ekstraksi pesan: hasil-4-2.png Masukkan kunci dekripsi (tekan enter untuk tanpa kunci): Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): Mengekstrak berkas rahasia... Pesan berhasil diekstrak ke dalam ekstraksi\hasil-4-2.png</pre> | <pre>zaki@DESKTOP-8GQ6GV0 MINGW64 ~/0/1.KULIAH/Semester7/Kriptografi \$ diff secret/tes.png ekstraksi/hasil-4-2.png (venv)</pre> <p>File sama, tapi file audio rusak</p> |

| | | |
|--------------|---|--|
| <p>.pdf</p> | <pre> Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 1 === Penyisipan Pesan Rahasia ke File Audio === Masukkan file beserta ekstensi! Masukkan nama file cover (mp3): campina.mp3 Masukkan nama file pesan rahasia: tes.pdf Masukkan path file output penyisipan pesan (mp3): output-4-3.mp3 Masukkan jumlah LSB yang digunakan (1, 2, 4): 4 Masukkan kunci enkripsi (tekan enter untuk tanpa kunci): Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): Menyisipkan berkas rahasia... Pesan berhasil disisipkan ke dalam output\output-4-3.mp3 Tekan Enter untuk menghentikan pemutaran lagu... ✅ PSNR antara sound\campina.mp3 dan output\output-4-3.mp3: 52.83 dB 🔊 Kualitas masih baik (>= 30 dB) Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 2 === Ekstraksi Pesan Rahasia dari File Audio === Masukkan nama file audio (mp3): output-4-3.mp3 Masukkan nama file output ekstraksi pesan: hasil-4-3.pdf Masukkan kunci dekripsi (tekan enter untuk tanpa kunci): Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): Mengekstrak berkas rahasia... Pesan berhasil diekstrak ke dalam ekstraksi\hasil-4-3.pdf </pre> | <pre> Zaki@DESKTOP-0GQ6GV0 MINGW64 ~/7.0/1.KULIAH/Semester7/Kriptografi \$ diff secret/tes.pdf ekstraksi/hasil-4-3.pdf (venv) </pre> <p>File sama, tapi file audio rusak</p> |
| <p>.docx</p> | <pre> Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 1 === Penyisipan Pesan Rahasia ke File Audio === Masukkan file beserta ekstensi! Masukkan nama file cover (mp3): campina.mp3 Masukkan nama file pesan rahasia: tes.docx Masukkan path file output penyisipan pesan (mp3): output-4-4.mp3 Masukkan jumlah LSB yang digunakan (1, 2, 4): 4 Masukkan kunci enkripsi (tekan enter untuk tanpa kunci): Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): Menyisipkan berkas rahasia... Pesan berhasil disisipkan ke dalam output\output-4-4.mp3 Tekan Enter untuk menghentikan pemutaran lagu... ✅ PSNR antara sound\campina.mp3 dan output\output-4-4.mp3: 53.35 dB 🔊 Kualitas masih baik (>= 30 dB) Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 2 === Ekstraksi Pesan Rahasia dari File Audio === Masukkan nama file audio (mp3): output-4-4.mp3 Masukkan nama file output ekstraksi pesan: hasil-4-4.docx Masukkan kunci dekripsi (tekan enter untuk tanpa kunci): Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): Mengekstrak berkas rahasia... Pesan berhasil diekstrak ke dalam ekstraksi\hasil-4-4.docx </pre> | <pre> Zaki@DESKTOP-0GQ6GV0 MINGW64 ~/7.0/1.KULIAH/Semester7/Kriptografi \$ diff secret/tes.docx ekstraksi/hasil-4-4.docx (venv) </pre> <p>File sama, tapi file audio rusak</p> |

| | | |
|-------------|--|--|
| <p>.md</p> | <pre>Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 1 === Penyisipan Pesan Rahasia ke File Audio === Masukkan file beserta ekstensi! Masukkan nama file cover (mp3): campina.mp3 Masukkan nama file pesan rahasia: tes.md Masukkan path file output penyisipan pesan (mp3): output-4-5.mp3 Masukkan jumlah LSB yang digunakan (1, 2, 4): 4 Masukkan kunci enkripsi (tekan enter untuk tanpa kunci): Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): Menyisipkan berkas rahasia... Pesan berhasil disisipkan ke dalam output\output-4-5.mp3 Tekan Enter untuk menghentikan pemutaran lagu... ✅ PSNR antara sound\campina.mp3 dan output\output-4-5.mp3: 77.38 dB 🔊 Kualitas masih baik (>= 30 dB)</pre> <pre>Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 2 === Ekstraksi Pesan Rahasia dari File Audio === Masukkan nama file audio (mp3): output-4-5.mp3 Masukkan nama file output ekstraksi pesan: hasil-4-5.md Masukkan kunci dekripsi (tekan enter untuk tanpa kunci): Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): Mengekstrak berkas rahasia... Pesan berhasil diekstrak ke dalam ekstraksi\hasil-4-5.md</pre> | <pre>zak1@DESKTOP-8Q96GVD MINGW64 ~/0/1.KULIAH/Semester7/Kriptografi \$ diff secret/tes.md ekstraksi/hasil-4-5.md (venv)</pre> <p>File sama</p> |
| <p>.exe</p> | <pre>Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 1 === Penyisipan Pesan Rahasia ke File Audio === Masukkan file beserta ekstensi! Masukkan nama file cover (mp3): campina.mp3 Masukkan nama file pesan rahasia: tes.exe Masukkan path file output penyisipan pesan (mp3): output-4-6.mp3 Masukkan jumlah LSB yang digunakan (1, 2, 4): 4 Masukkan kunci enkripsi (tekan enter untuk tanpa kunci): Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): Menyisipkan berkas rahasia... Pesan berhasil disisipkan ke dalam output\output-4-6.mp3 Tekan Enter untuk menghentikan pemutaran lagu... ✅ PSNR antara sound\campina.mp3 dan output\output-4-6.mp3: 48.53 dB 🔊 Kualitas masih baik (>= 30 dB)</pre> <pre>Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 2 === Ekstraksi Pesan Rahasia dari File Audio === Masukkan nama file audio (mp3): output-4-6.mp3 Masukkan nama file output ekstraksi pesan: hasil-4-6.exe Masukkan kunci dekripsi (tekan enter untuk tanpa kunci): Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): Mengekstrak berkas rahasia... Pesan berhasil diekstrak ke dalam ekstraksi\hasil-4-6.exe</pre> | <pre>zak1@DESKTOP-8Q96GVD MINGW64 ~/0/1.KULIAH/Semester7/Kriptografi \$ diff secret/tes.exe ekstraksi/hasil-4-6.exe (venv)</pre> <p>File sama, tapi file audio rusak</p> |

| | | |
|-----------|---|---|
| <p>.C</p> | <pre> Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 1 === Penyisipan Pesan Rahasia ke File Audio === Masukkan file beserta ekstensi Masukkan nama file cover (mp3): campina.mp3 Masukkan nama file pesan rahasia: tes.c Masukkan path file output penyisipan pesan (mp3): output-4-7.mp3 Masukkan jumlah LSB yang digunakan (1, 2, 4): 4 Masukkan kunci enkripsi (tekan enter untuk tanpa kunci): Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): Menyisipkan berkas rahasia... Pesan berhasil disisipkan ke dalam output\output-4-7.mp3 Tekan Enter untuk menghentikan pemutaran lagu... ✅ PSNR antara sound\campina.mp3 dan output\output-4-7.mp3: 75.15 dB 🔊 Kualitas masih baik (>= 30 dB) Tentukan fitur yang ingin digunakan: 1. Sisip Pesan 2. Ekstrak Pesan 3. Putar Lagu 4. PSNR Pilihan Anda: 2 === Ekstraksi Pesan Rahasia dari File Audio === Masukkan nama file audio (mp3): output-4-7.mp3 Masukkan nama file output ekstraksi pesan: hasil-4-7.c Masukkan kunci dekripsi (tekan enter untuk tanpa kunci): Masukkan seed pembangkit acak (tekan enter untuk tanpa seed): Mengekstrak berkas rahasia... Pesan berhasil diekstrak ke dalam ekstraksi\hasil-4-7.c </pre> | <pre> zaki@OLSKTOP-UAGGAVD: ~/0/1.KULIAH/semester/Kriptografi \$ diff secret/tes.c ekstraksi/hasil-4-7.c (venv) </pre> <p>File sama</p> |
|-----------|---|---|

Dari hasil percobaan tersebut, nilai LSB tidak memengaruhi file audio karena audio stego masih terdengar sama dengan audio *cover*. Penambahan enkripsi, titik acak, atau penanganan ekstensi pun berhasil diterapkan dengan baik karena berkas rahasia dapat diekstrak sesuai dengan berkas awal. Yang bermasalah adalah kerusakan berkas audio stego. Seperti dijelaskan pada bab II, *header-header* baru dapat terbentuk oleh metode LSB. Jadi, program yang dibuat dapat melakukan steganografi dengan baik, tetapi masih belum bisa menangani berkas rahasia yang besar, khususnya berkas rahasia yang memerlukan lebih dari satu *header*.

BAB IV

Kesimpulan

File MP3 kurang baik sebagai media steganografi dengan metode LSB karena terbentuk dari *frame-frame* yang ditandai dengan nilai byte di dalamnya. Pembuatan proses sisip dan ekstraksi dapat dilakukan dengan baik, tetapi tidak menjamin *cover* terdengar sama dengan awal sekalipun hanya memanfaatkan 1-LSB. Jadi, steganografi pada file MP3 kurang sesuai dengan metode LSB.

DAFTAR PUSTAKA

Munir, R. 2025. *08-Steganografi (Bagian 1)*. Diakses pada 24 September 2025, dari <https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2025-2026/08-Steganografi-Bagian1-2025.pdf>

The Editors of Encyclopaedia Britannica. 2025. *MP3*. Diakses pada 3 Oktober 2025, dari <https://www.britannica.com/technology/MP3>

Anonim. 2007. *Inside MP3*. Diakses pada 24 September 2025, dari <http://www.multiweb.cz/twoinches/mp3inside.htm>

LAMPIRAN

Repositori GitHub: <https://github.com/BryanLauw/Tucil-II-IF4020-Kriptografi>

Pranala video: <https://youtu.be/O763egPAHks>

PEMBAGIAN TUGAS

| NIM | Tugas |
|----------|--|
| 13522033 | <ul style="list-style-type: none">- Enkripsi dekripsi- Pembangkit titik acak- Pembacaan file- Laporan |
| 13522049 | <ul style="list-style-type: none">- Sisip dan ekstrak- Main program- PSNR- Pemutar lagu- Laporan |

DOKUMENTASI CLI

```
pygame 2.6.1 (SDL 2.28.4, Python 3.10.11)
Hello from the pygame community. https://www.pygame.org/contribute.html
Tentukan fitur yang ingin digunakan:
1. Sisip Pesan
2. Ekstrak Pesan
3. Putar Lagu
4. PSNR
Pilihan Anda: 1

=== Penyisipan Pesan Rahasia ke File Audio ===

Masukkan file beserta ekstensi!
Masukkan nama file cover (mp3): test.mp3
Masukkan nama file pesan rahasia: secret.jpg
Masukkan path file output penyisipan pesan (mp3): stega.mp3
Masukkan jumlah LSB yang digunakan (1, 2, 4): 2
Masukkan kunci enkripsi (tekan enter untuk tanpa kunci):
Masukkan seed pembangkit acak (tekan enter untuk tanpa seed):
```

Gambar dokumentasi CLI