Implementasi Steganografi Pada Video untuk Pengiriman Pesan Rahasia

William Manuel Kurniawan – 13520020
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): 13520020@std.stei.itb.ac.id

***Abstract*—Steganografi video merupakan cabang dari steganografi digital yang berfokus pada penyembunyian informasi rahasia di dalam file video, dengan tujuan menjaga kerahasiaan data. Salah satu metode yang digunakan dalam steganografi digital adalah LSB dimana informasi rahasia disisipkan pada sebuah file tanpa mengubah hasil keluaran dari file tersebut. Fokus utama dari makalah ini adalah melakukan penyisipan informasi rahasia dalam bentuk video pada sebuah file video berbeda serta mengambil informasi rahasia tersebut kembali dalam bentuk video. Dalam makalah ini akan dibahas permasalahan yang dihadapi dalam melakukan steganografi video, solusi yang dibuat, serta hasil implementasi.**

Kata Kunci—Steganografi; video; LSB

I. PENDAHULUAN

Dalam era digital saat ini, kebutuhan akan keamanan informasi menjadi semakin penting seiring dengan meningkatnya penggunaan teknologi untuk komunikasi dan penyimpanan data. Salah satu metode yang digunakan untuk menjaga kerahasiaan informasi adalah steganografi. Steganografi adalah seni dan ilmu menyembunyikan pesan di dalam media lain sedemikian rupa sehingga keberadaan pesan tersebut tidak terdeteksi oleh pihak ketiga. Steganografi dapat dilakukan untuk berbagai macam bentuk data. Video merupakan salah satu bentuk data paling umum yang digunakan untuk komunikasi saat ini sehingga steganografi untuk video menjadi semakin penting.

Terdapat berbagai macam metode steganografi yang dapat digunakan tetapi steganografi pada dasarnya masih memiliki beberapa kebutuhan data serta pertimbangan yang sama. Data yang dibutuhkan untuk steganografi adalah sebagai berikut.

- Informasi Rahasia

  Informasi rahasia berbagai macam data biasanya dalam bentuk tulisan, gambar, atau file lain yang biasanya digunakan. Dalam konteks steganografi video, file yang biasanya digunakan adalah file dengan format .mp4 atau format .mkv

- Informasi *Cover*

  Informasi *cover* merupakan sebuah informasi yang akan terlihat oleh pihak lain. Informasi *cover* menyimpan informasi rahasia yang dapat diekstrak menggunakan metode tertentu.

Hal-hal yang biasanya dipertimbangkan dalam steganografi digital antara lain adalah sebagai berikut.

- Kapasitas informasi *cover*

  Ukuran informasi *cover* memiliki peran penting dalam steganografi digital. Hal ini disebabkan oleh fungsi informasi *cover* dalam menyimpan informasi rahasia. Informasi *cover* harus memiliki ukuran yang cukup dalam menyimpan informasi rahasia agar tidak terjadi masalah dalam penampilan informasi yang dihasilkan. Oleh karena itu, informasi *cover* harus memiliki ukuran yang cukup agar memiliki kapasitas tambahan yang dapat digunakan untuk menyisipkan informasi rahasia.

- Kualitas informasi rahasia

  Informasi rahasia terkadang tidak dapat disisipkan ke dalam informasi *cover* sehingga kualitas dari informasi rahasia kemungkinan akan menurun. Untuk melakukan steganografi digital dengan baik, perlu dipertimbangkan bagian data yang ingin dimasukkan agar tetap dapat dimengerti.

- Keamanan dan kerahasiaan

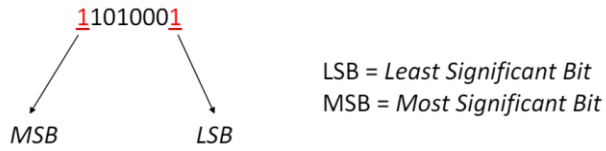
  Steganografi digital yang dilakukan harus memiliki kemampuan untuk menyembunyikan informasi rahasia dan menghindari deteksi dari pihak ketiga. Hal ini biasanya dilakukan dengan memanipulasi informasi rahasia dalam informasi *cover* agar hasil keluaran informasi *cover* tidak memiliki perubahan yang mudah terlihat oleh pihak lain.

Steganografi digital dapat dilakukan menggunakan berbagai macam metode tetapi secara umum bekerja dengan menyembunyikan informasi rahasia ke dalam bit-bit dari informasi *cover*. Salah satu metode yang digunakan untuk steganografi adalah metode *Least Significant Bits* (LSB). LSB merupakan salah satu metode paling terkenal untuk melakukan steganografi digital karena kemudahan metode yang dilakukan serta kerahasiaan yang baik dari hasil metode tersebut. Implementasi LSB dalam steganografi video akan menghasilkan beberapa masalah baru yang harus diurus agar informasi rahasia dapat diproses. Masalah dan solusi dari masalah tersebut akan dibahas secara lebih lanjut beserta dengan implementasinya.

II. Teori Dasar

A. *Least Significant Bits*

Least Significant Bits (LSB) merupakan sebuah metode steganografi digital yang sering digunakan untuk segala macam bentuk data. *Least Significant Bits* bekerja berdasarkan prinsip perubahan nilai yang terjadi dari pengubahan 1 bit dalam sebuah byte. Dalam sebuah byte, terdapat 8 bit yang disusun dari kiri ke kanan dengan bit paling kanan yang disusun dianggap sebagai LSB dan bit paling kiri dianggap sebagai *Most Significant Bits* (MSB).



Gambar 1. Penjelasan LSB dan MSB

Berdasarkan penjelasan tersebut, dapat diketahui bahwa nilai byte tidak memiliki perubahan banyak ketika LSB diubah. Steganografi LSB bekerja dengan mengambil data cover per byte dan menyisipkan informasi rahasia pada bit paling tidak signifikan. Perhitungan byte saat pengubahan LSB dapat dilihat sebagai berikut.

- byte 01000111 = 71
- byte 01000110 = 70

Dari perhitungan tersebut dapat dilihat bahwa tidak terjadi banyak perubahan nilai dalam sebuah byte sehingga ada beberapa aplikasi tertentu dimana hasil perubahan byte sulit terlihat oleh pengguna. Salah satu aplikasi tersebut terdapat pada file gambar. File gambar direpresentasikan secara digital menggunakan konsep pixel. Pixel menyimpan warna pada posisi gambar tertentu dengan menggunakan 3 bytes. Masing-masing byte tersebut menyimpan data untuk warna merah, hijau, dan biru atau dikenal sebagai RGB agar dapat merepresentasikan warna apapun yang diinginkan. Contoh pengubahan LSB pada suatu pixel dapat terlihat dari tabel contoh awal berikut.

	R	G	B
Integer	71	23	255
Binary	01000111	00010111	11111111

Dari tabel data warna dalam pixel, dapat dilihat bahwa nilai tertinggi yang dapat didapatkan adalah 255 dengan nilai terendah adalah 0. Dari tabel tersebut, dilakukan pengubahan LSB dari 1 menjadi 0 sebagai berikut.

	R	G	B
Integer	70	22	254
Binary	01000110	00010110	11111110

Hasil perubahan warna dari nilai RGB adalah sebagai berikut.

Gambar 2. Perbandingan Warna dari Pengubahan LSB

Dari kedua warna tersebut dapat dilihat bahwa warna tidak mengalami banyak perubahan sehingga perubahan tidak mudah diketahui oleh manusia. Dengan menyimpan data rahasia per bit dalam LSB pixel, data dapat disimpan tanpa mengubah gambar secara signifikan.

B. *Matroska Video File*

Matroska Video File atau dikenal sebagai file .mkv merupakan sebuah format file container yang dapat digunakan untuk menyimpan video. File .mkv pertama kali diluncurkan pada tahun 2002 dalam proyek Matroska yang didirikan oleh Steve Lhomme. File .mkv memiliki salah satu fitur untuk melakukan *lossless video compression* dimana kompresi file video dilakukan tanpa membuang informasi dari video. Keuntungan dari tipe kompresi tersebut adalah informasi rahasia yang disisipkan ke dalam video tidak akan mengalami perubahan saat kompresi. Tipe kompresi video tersebut dibutuhkan untuk melakukan steganografi video agar tidak terjadi permasalahan proses steganografi akibat dari perubahan data dalam gambar. Format file .mkv memiliki kelemahan dimana ukuran file biasanya akan menjadi lebih besar dibandingkan dengan file pemutaran video lain berhubungan dengan teknik kompresi yang digunakan.

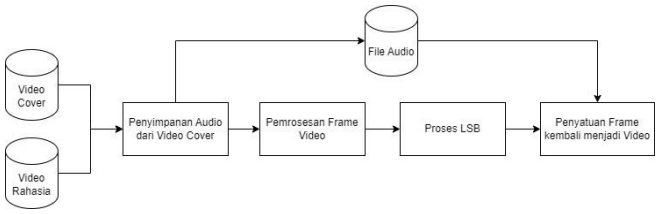
III. Deskripsi Masalah dan Rancangan Solusi

A. *Metode Steganografi Video untuk Video Rahasia*

Steganografi menggunakan file video tidak memiliki metode umum yang sering digunakan. Video dianggap sebagai media yang cocok untuk melakukan steganografi karena ukuran file *cover* yang relatif besar beserta kompleksitas file video. Untuk melakukan steganografi video, ditentukan bahwa lebih mudah menggunakan teknik yang sudah sering digunakan yaitu LSB. Video *cover* dan video rahasia dapat dipecah menjadi beberapa gambar. Dari gambar tersebut, dapat dilakukan LSB seperti biasa untuk menghasilkan gambar baru. Hasil akhir gambar-gambar baru tersebut kembali disambungkan menjadi sebuah video menggunakan bentuk *lossless compression*. Melalui metode tersebut, video dapat disimpan dalam video menggunakan steganografi.

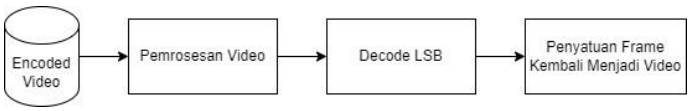
Steganografi menggunakan metode ini memiliki kekurangan dimana penyisipan data pada video *cover* kemungkinan tidak terlalu efisien akibat dari kurangnya pengertian dan perencanaan untuk teknik kompresi yang digunakan. Seperti pada penggunaan metode LSB lainnya, metode steganografi yang dibahas memiliki batasan dimana ukuran video *cover* harus lebih besar atau setidaknya sama dengan video rahasia. Selain batasan tersebut, metode memiliki kekurangan dimana video hasil steganografi akan memiliki penurunan kualitas berbentuk perubahan warna.

Cara kerja steganografi bagian encoding dapat dilihat pada gambar berikut.



Gambar 3. Proses Encoding Steganografi

Proses decoding steganografi dapat dilihat pada gambar berikut.



Gambar 4. Proses Decoding Steganografi

B. Perbedaan Frame Rate Antara Video Cover dan Video Rahasia

Frame rate merupakan jumlah gambar yang dihasilkan dalam video dalam kurun waktu tertentu, biasanya dihitung dalam jumlah frame per detik. *Frame rate* dapat menjadi masalah dalam proses pengubahan gambar steganografi kembali menjadi video karena dapat mengubah kecepatan pemutaran video menjadi lebih cepat atau lebih lambat. Jika video *cover* memiliki frame rate yang lebih kecil dari *frame rate* video rahasia, pemutaran video *cover* akan menjadi lebih cepat dibandingkan sebelum pemrosesan. Pengaturan lain dapat menghasilkan video *cover* yang berputar pada kecepatan yang sama tetapi video rahasia menjadi lebih pelan dari seharusnya. Masalah perbedaan *frame rate* dapat diselesaikan oleh pengguna jika pengguna mengetahui *frame rate* video rahasia dan melakukan pengaturan secara manual. Melalui pengaturan pengguna, program masih dapat mengambil video rahasia dari hasil steganografi dan memutarkannya pada kecepatan yang benar. Jika frame rate video rahasia tidak diketahui, maka perbedaan kecepatan video akan terjadi.

C. Pemutaran Audio dari Hasil Steganografi

Sebagian besar video yang dilihat memiliki suara sehingga video yang tidak memiliki suara biasanya terlihat aneh dan mencurigakan. Untuk menghindari hal tersebut, video harus dapat diputar dengan audionya. Berdasarkan rancangan awal, proses steganografi hanya mengubah video menjadi gambar untuk proses LSB dan membalikkan hasil gambar kembali menjadi video. Dalam proses awal ini, hasil video tidak memiliki audio. Proses selanjutnya adalah menambahkan audio ke hasil video yang dibuat. Dalam format .mkv, hal ini dapat dilakukan tanpa mengubah hasil gambar yang diekstrak dalam proses steganografi sehingga audio dapat diputar pada video *cover*. Pemutaran audio pada video rahasia menjadi hal yang lebih sulit karena dibutuhkan pengetahuan apakah urutan bit dalam video *cover* merupakan bagian audio yang ingin diputar atau gambar yang ingin dilihat. Salah satu cara untuk mengatasi masalah tersebut adalah melakukan steganografi sebanyak 2 kali dengan 1 video *cover* untuk video serta 1 video *cover* lain untuk file audio yang dapat disatukan pengguna.

IV. IMPLEMENTASI

Implementasi dilakukan menggunakan Bahasa pemrograman Python dengan bantuan pustaka ffmpeg dan Pillow untuk pemrosesan video.

A. Pemrosesan Video Menjadi Gambar dan Audio

Pemrosesan video bertujuan untuk memecahkan video menjadi file audio dan file gambar berdasarkan jumlah frame video *cover* dan video rahasia. Proses pemecahan video tersebut diimplementasikan pada kode berikut.

```
def extract_frames(video_path, output_dir):
    os.makedirs(output_dir, exist_ok=True)
    (
        ffmpeg
        .input(video_path)
        .output(os.path.join(output_dir,
'frame_%04d.png'), pix_fmt='rgb24')
        .run()
    )

def extract_audio(input_video_path, output_dir):
    os.makedirs(output_dir, exist_ok=True)
    stream = ffmpeg.input(input_video_path)
    audio = stream.audio
    audio = ffmpeg.output(audio,
os.path.join(output_dir, 'audio_0.mp3'),
acodec='libmp3lame')
    ffmpeg.run(audio)
```

Dalam kode yang dibuat, audio disimpan ke sebuah file .mp3 dalam sebuah folder yang dibuat secara otomatis. Gambar diambil per *frame* video yang dan disimpan ke sebual file .png yang disimpan pada folder baru.

B. Steganografi Frame Menggunakan LSB

Setelah didapatkan gambar-gambar untuk video *cover* dan video rahasia, dilakukan proses steganografi LSB menggunakan kode berikut.

```
def encode_image(cover_image_path,
secret_image_path, output_image_path):
    cover_image = Image.open(cover_image_path)
    secret_image = Image.open(secret_image_path)

    cover_image = cover_image.convert("RGB")
    secret_image = secret_image.convert("RGB")

    secret_image =
secret_image.resize(cover_image.size)

    encoded_image = Image.new("RGB",
cover_image.size)
```

```
    for x in range(cover_image.width):
        for y in range(cover_image.height):
            cover_pixel = cover_image.getpixel((x,
y))
            secret_pixel =
secret_image.getpixel((x, y))

            encoded_pixel = (
                (cover_pixel[0] & 0b11111110) |
(secret_pixel[0] >> 7),
                (cover_pixel[1] & 0b11111110) |
(secret_pixel[1] >> 7),
                (cover_pixel[2] & 0b11111110) |
(secret_pixel[2] >> 7)
            )

            encoded_image.putpixel((x, y),
encoded_pixel)

    encoded_image.save(output_image_path)
```

Kode bekerja dengan mengambil *frame* dari video *cover* dan video rahasia lalu mengubah data menjadi data RGB. Setelah data RGB berhasil diambil, ukuran gambar disesuaikan agar dapat dilakukan proses LSB. Setelah gambar disiapkan, dilakukan proses LSB pada setiap byte RGB yang menghasilkan gambar baru untuk disimpan ke dalam sistem.

Untuk membalikkan hasil dari steganografi, maka dilakukan proses *decoding* dengan menggunakan kode berikut.

```
def decode_image(encoded_image_path,
output_image_path):
    encoded_image = Image.open(encoded_image_path)
    decoded_image = Image.new("RGB",
encoded_image.size)

    for x in range(encoded_image.width):
        for y in range(encoded_image.height):
            encoded_pixel =
encoded_image.getpixel((x, y))

            decoded_pixel = (
                encoded_pixel[0] & 0b00000001,
                encoded_pixel[1] & 0b00000001,
                encoded_pixel[2] & 0b00000001
            )

            decoded_pixel = (
                decoded_pixel[0] << 7,
                decoded_pixel[1] << 7,
                decoded_pixel[2] << 7
            )

            decoded_image.putpixel((x, y),
decoded_pixel)

    decoded_image.save(output_image_path)
```

C. *Pembangunan Video dari Hasil Steganografi*

Setelah semua proses steganografi selesai, hasil steganografi kembali dikumpulkan menjadi sebuah video dalam format .mkv. Proses pembangunan video dilakukan menggunakan kode berikut.

```
video_stream =
ffmpeg.input(os.path.join(embedded_frames_path,
'frame_%04d.png'), framerate=12.5)
    audio_stream =
ffmpeg.input(os.path.join(audio_path,
'audio_0.mp3'))

    ffmpeg.output(video_stream, audio_stream,
output_video, vcodec='ffv1', pix_fmt='bgr0',
acodec='copy', shortest=None).run()
```

Program mengambil data gambar dan audio dengan pengaturan *frame rate* pada data gambar. Setelah itu, pustaka ffmpeg melakukan pemrosesan gambar dan audio menggunakan algoritma FF Video Codec 1 (FFV1) untuk *lossless compression*. Untuk pembalikkan hasil steganografi agar dapat mendapatkan video rahasia, digunakan kode berikut.

```
(
        ffmpeg
        .input(os.path.join(hidden_frames_path,
'frame_%04d.png'), framerate=43)
        .output(hidden_video, vcodec='ffv1',
pix_fmt='bgr0')  # Use FFV1 codec and keep RGB
format
        .run()
)
```

Pembalikkan video hasil steganografi dilakukan tanpa mengurus audio dari video rahasia tersebut dengan asumsi hanya gambar video yang dapat dikirimkan melalui steganografi.

V. PENGUJIAN DAN EVALUASI

A. *Pengujian dengan Pengaturan Frame Rate Manual*

Pengujian dilakukan menggunakan 2 video dengan resolusi yang sama (1280x720 pixel) dan *frame rate* kedua video tersebut diketahui. Salah satu video lebih panjang dari video yang lain dan diguanakan sebagai video *cover*. Video *cover* menggunakan *frame rate* sebesar 12.5 dan video rahasia menggunakan *frame rate* sebesar 30. Berikut adalah hasil steganografi video yang dilakukan.

Gambar 5. Perbandingan Video *Cover* dari Hasil Steganografi

Gambar pada bagian kiri menampilkan video *cover* sebelum steganografi dan gambar bagian kanan menampilkan video hasil steganografi. Dari hasil tersebut, dapat dilihat bahwa tidak terjadi perubahan pada gambar yang jelas terlihat oleh manusia. Video hasil steganografi juga berputar dengan kecepatan yang sama dibandingkan dengan video *cover* sehingga audio terlihat sesuai dengan video. Setelah melihat hasil steganografi, diambil video rahasia menggunakan program dengan hasil berikut.

Gambar 6. Perbandingan Video Rahasia dari Hasil Steganografi

Gambar bagian kiri menunjukkan video rahasia awal dan gambar bagian kanan menunjukkan hasil video rahasia setelah diproses menggunakan steganografi. Dapat dilihat bahwa terjadi perubahan warna yang besar pada video tetapi gambaran besar video masih dapat terlihat.

B. Pengujian Tanpa Pengaturan Frame Rate

Pengujian dilakukan seperti pada bagian A tetapi *frame rate* untuk proses encoding dan decoding video memiliki pengaturan yang sama sebesar 12.5. Hasil video *cover* dan video rahasia menampilkan gambar yang sama dengan bagian A. Hasil kecepatan pemutaran video *cover* hasil steganografi juga masih sama dan audio masih berputar secara sinkron. Kecepatan pemutaran video rahasia yang diambil dari steganografi mengalami perubahan kecepatan dimana video berputar lebih lama dari input awal. Hal ini disebabkan oleh pemutaran video yang seharusnya memiliki *frame rate* sebesar 30 diputar dengan nilai sebesar 12.5. Dari pengujian ini, dibuktikan bahwa video yang memiliki *frame rate* berbeda harus dilakukan pengaturan tambahan oleh pengguna agar video dapat berputar secara normal.

C. Pengujian dengan Pengubahan LSB

Pengujian dilakukan dengan tujuan membandingkan hasil video jika pengubahan bits dalam video *cover* diubah. Pengujian awal menggunakan pengubahan 1 bit LSB yang menghasilkan video yang dapat dilihat pada gambar 5 dan gambar 6. Pengaturan manual dilakukan dalam program untuk mengubah cara pengubahan bits dari 1 bits LSB menjadi 2 bits LSB dengan harapan dapat meningkatkan detail dalam video rahasia. Berikut adalah pengaturan kode yang dilakukan.

```
encoded_pixel = (
                (cover_pixel[0] & 0b11111110) |
(secret_pixel[0] >> 6),
                (cover_pixel[1] & 0b11111110) |
(secret_pixel[1] >> 6),
                (cover_pixel[2] & 0b11111110) |
(secret_pixel[2] >> 6)
            )
```

```
            decoded_pixel = (
                encoded_pixel[0] & 0b00000001,
                encoded_pixel[1] & 0b00000001,
                encoded_pixel[2] & 0b00000001
            )

            decoded_pixel = (
                decoded_pixel[0] << 6,
                decoded_pixel[1] << 6,
                decoded_pixel[2] << 6
            )
```

Setelah dilakukan pengaturan ulang pada program, dilakukan kembali steganografi menggunakan video-video awal. Berikut merupakan perbandingan hasil steganografi video.

Gambar 7. Perbandingan Video *Cover* dari Hasil Steganografi 2 Bits

Gambar pada bagian kiri menampilkan video *cover* sebelum steganografi dan gambar bagian kanan menampilkan video hasil steganografi. Dari hasil tersebut, dapat dilihat bahwa perubahan dalam video masih minimal dan sulit diketahui oleh manusia. Perbandingan video rahasia awal dengan video rahasia hasil steganografi dapat dilihat pada gambar berikut.

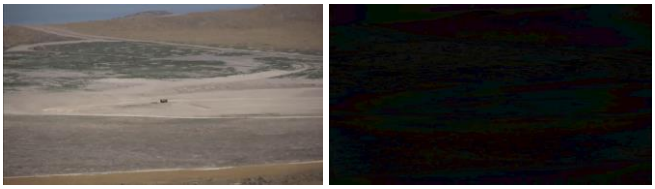
Gambar 8. Perbandingan Video Rahasia dari Hasil Steganografi 2 Bits

Gambar bagian kiri menunjukkan video rahasia awal dan gambar bagian kanan menunjukkan hasil video rahasia setelah diproses. Dapat dilihat bahwa terjadi perubahan warna dibandingkan steganografi awal. Meskipun terjadi perubahan warna, warna masih belum cukup detail sehingga detail gambar masih sulit terlihat. Untuk mencoba menambah detail video rahasia, dilakukan kembali percobaan ulang.

Percobaan ulang dilakukan dengan mengubah kembali LSB agar dilakukan pengubahan 4 bits dari video *cover*. Pengaturan program dilakukan seperti pengaturan pertama. Berikut merupakan perbandingan ulang hasil dari steganografi.

Gambar 9. Perbandingan Video *Cover* dari Hasil Steganografi 4 Bits

Gambar pada bagian kiri menampilkan video *cover* sebelum steganografi dan gambar bagian kanan menampilkan video hasil steganografi. Dari gambar tersebut, dapat dilihat bahwa gambar hasil steganografi terasa lebih aneh dengan adanya cahaya berbeda warna di sebagian tempat. Hal ini dapat menjadi masalah karena kualitas video terlihat rendah dan mencurigakan bagi penonton. Berikut merupakan perbandingan video rahasia dari hasil steganografi.



Gambar 10. Perbandingan Video Rahasia dari Hasil Steganografi 4 Bits

Gambar bagian kiri menunjukkan video rahasia awal dan gambar bagian kanan menunjukkan hasil video rahasia setelah diproses. Dari gambar tersebut dapat dilihat bahwa terjadi banyak perubahan warna yang justru mengurangi ketajaman detail dalam video dan menjadi sulit dilihat. Dari pengujian yang dilakukan, ditentukan bahwa proses LSB dengan pengubahan 1 bit menghasilkan perubahan detail paling baik tanpa mengubah video c*over* secara signifikan.

VI. Kesimpulan dan Saran

Steganografi pada video menggunakan metode *Least Significant Bits* terbukti cukup mampu dalam menyembunyikan pesan rahasia berbentuk video lain. Video rahasia dapat dibaca oleh pengguna secara garis besar meskipun terjadinya penurunan kualitas video yang dapat menghilangkan detail akibat dari perubahan warna. Penyembunyian video tersebut dapat dilakukan secara efektif tanpa mengubah hasil pemutaran audio dan gambar dari video *cover* sehingga sulit diketahui oleh pihak lain. Dalam implementasi, ditemukan beberapa masalah yang harus diperhatikan seperti kecepatan perputaran video akibat masalah *frame rate* serta kualitas video rahasia berdasarkan pengubahan proses LSB. Dari pengujian ditentukan bahwa pengaturan *frame rate* manual serta proses LSB dengan pengubahan 1 bit menghasilkan video terbaik.

Algoritma yang digunakan untuk melakukan steganografi masih memiliki beberapa kekurangan dan dapat dibuat menjadi lebih baik di masa depan. Kekurangan pertama merupakan kurangnya pemutaran audio dari video rahasia akibat proses steganografi yang tidak lengkap. Hal lain yang dapat dilakukan adalah meningkatkan kualitas hasil steganografi untuk video rahasia dengan melakukan penyusupan bit video rahasia dalam beberapa pixel video *cover*. Pengubahan metode penyusupan akan menggunakan video *cover* yang lebih besar dari video rahasia agar leibh banyak data dapat disimpan. Melalui perbaikan tersebut, video rahasia dapat ditampilkan tanpa mengurangi kualitas gambar dan dapat ditampilkan dengan audionya.

Pranala Kode Program

Kode program implementasi dan video yang digunakan dapat diakses pada pranala berikut.

https://github.com/wmk567/steganografi_video

Ucapan Terima Kasih

Penulis mengucap syukur kepada Tuhan Yang Maha Esa atas berkat dan bimbingan-Nya dalam menyelesaikan makalah ini. Penulis juga mengucapakan terima kasih kepada Bapak Rinaldi Munir sebagai dosen mata kuliah IF4020 Kriptografi yang memberikan ilmu pengetahuan mengenai topik yang dibahas dalam makalah ini. Terakhir, penulis mengucapkan terima kasih kepada teman dan keluarga yang terus mendukung penulis dalam penulisan makalah ini.

Referensi

[1] Munir, Rinaldi. (2024). "Steganografi - Bagian 1" Program Studi Informatika ITB. https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2023-2024/07-Steganografi-Bagian1-2024.pdf

[2] Munir, Rinaldi. (2024). "Steganografi - Bagian 2" Program Studi Informatika ITB. https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2023-2024/08-Steganografi-Bagian2-2024.pdf

[3] Neeta, D., Snehal, K., and Jacobs, D. (2007). "Implementation of LSB Steganography and Its Evaluation for Various Bits." 2006 1st International Conference on Digital Information Management, Bangalore, India, pp. 173-178. doi: 10.1109/ICDIM.2007.369349. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4221886

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 12 Juni 2024

William Manuel Kurniawan