e-ISSN 2597-4963 dan p-ISSN 1858-4853

STEGANOGRAFI PADA VIDEO MENGGUNAKAN METODE LEAST SIGNIFICANT BIT (LSB) DAN END OF FILE (EOF)

Ulan Ari Anti [1)], Awang Harsa Kridalaksana [2)], Dyna Marisa Khairina [3)]

[1, 2, 3)]Program Studi Ilmu Komputer,Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Mulawarman
Alamat Jl. Panajam Kampus Gunung Kelua Universitas Mulawarman Samarinda
E-Mail : ulan.ilkom@gmail.com [1)], awangkid@gmail.com [2)], dyna.ilkom@gmail.com [3)]

ABSTRAK

Steganografi adalah teknik dan seni untuk menyembunyikan pesan atau informasi dalam suatu media, seperti teks, gambar, audio ataupun video yang bertujuan untuk menghindari kecurigaan dari orang yang tidak berhak. Untuk itu diperlukan sebuah perangkat lunak yang dapat menyembunyikan informasi yang bersifat rahasia pada sebuah media yaitu video. Penyembunyian data pada file video dikenal dengan istilah steganografi video. Metode steganografi yang dikenal diantaranya metode Least Significant Bit (LSB) dan Metode End Of File (EOF). Tujuan penelitian yakni untuk mengimplementasikan metode LSB dan EOF untuk menyisipkan pesan teks ke dalam file video. Hal ini diperlukan karena sering terjadi bahwa pesan teks yang dikirim merupakan suatu pesan rahasia yang tidak boleh diketahui sembarang orang. Dua metode yang dapat digunakan adalah Metode LSB dan metode EOF. Metode LSB bekerja dengan mengganti bit terakhir kode biner citra dengan kode biner pesan, sedangkan metode EOF bekerja dengan menambahkan nilai desimal pesan ke dalam pixel citra terakhir. Kelebihan metode LSB adalah ukuran dimensi video yang mengandung pesan tidak berubah, sedangkan kekurangannya adalah kapasitas pesan yang akan disisipkan terbatas sesuai dengan jumlah frame. Sebaliknya metode EOF mempunyai kelebihan dapat menyisipkan pesan dalam jumlah yang tidak terbatas, sedangkan kekurangannya adalah dimensi video akan bertambah

Kata Kunci : Steganografi; Video; Embedding; Extraction; EOF; LSB.

1. PENDAHULUAN

Kerahasian dan keamanan merupakan aspek penting yang dibutukan dalam proses pertukaran pesan atau informasi melalui jaringan atau internet. Berbagai macam teknik keamanan telah dikembangkan untuk melindungi kerahasian pesan atau informasi agar terhindar dari pihak ketiga yang tidak memiliki hak, salah satunya yaitu steganografi. Ilmu Steganografi sejalan dengan ilmu Kriptografi akan tetapi keduanya memiliki perbedaan. Steganografi bertujuan untuk merahasiakan atau menyembunyikan pesan rahasia melalui sebuah media. Sedangkan kriptografi hanya bersifat menyamarkan sebuah pesan rahasia namun tidak menyembunyikanya. Steganografi sering dimple-mentasikan melalui media digital , dimana bentuk dari pesan rahasia (embedded messages) atau media penampung (cover-object) dapat berbentuk teks, citra, audio maupun video. Dengan kata lain sebuah data berupa teks dapat disembunyikan kedalam sebuah citra digital.

Teknik steganografi memiliki beberapa metode yang dapat digunakan, seperti metode Least Significant Bit (LSB) dan metode End Of File (EOF). Kedua metode ini memiliki ciri tersendiri dalam proses penyembuyian data, selain itu metode ini sendiri masih digunakan dalam pengembangan ilmu steganografi ini sendiri untuk menciptakan metode-metode baru dalam dunia steganografi. Pada penelitian sebelumnya dengan judul Steganografi Video Menggunakan Metode End Of File [1] menjelaskan tentang bagaimana menyisipkan pesan rahasia berupa teks pada sebuah citra digital video, namun perbedaan terlihat dari ukuran video yang akan bertambah ketika disisipkan pesan pada cirta terakhir. Serta hasil penelitian sebelumnya Keamanan Data Dengan Menggunakan Algoritma Rivest Code 4 (RC4) Dan Steganografi Pada Citra Digital [2] menjelaskan tentang bagaimana mengembangkan agar pesan yang disembunyikan tidak hanya berupa pesan rahasia tapi pesan yang telah di enkripsikan menggunakan algoritma RC4. Dengan menambahkan kriptografi ke dalam pesan rahasia yang disembunyikan ke dalam gambar akan memperkuat keamanan dari pesan rahasia.

Berdasarkan dari latar belakang, peneliti ingin mengembangkan agar pesan rahasia tidak hanya disimpan dalam gambar tetapi juga dapat disimpan dalam video digital. Media penampung video dipilih karena banyaknya data yang dapat disembunyikan di dalamnya, serta fakta bahwa video merupakan "streams" dari beberapa image menyebabkan adanya distorsi pada salah satu frame image tidak akan dilihat dengan mudah dengan mata manusia [3]. Steganografi pada video (video steganography) ini akan menggunakan dua metode yaitu LSB dan EOF.

2. TINJAUAN PUSAKA

A. Steganografi

Kata steganografi (*steganography*) berasal dari bahasa Yunani yaitu *steganos* yang artinya tersembunyi atau terselubung dan *graphein*, yang artinya menulis, sehingga kurang lebih artinya adalah "menulis tulisan yang tersembunyi atau terselubung" [4]. Secara umum steganografi merupakan seni atau ilmu yang digunakan untuk

e-ISSN 2597-4963 dan p-ISSN 1858-4853

menyembunyikan pesan rahasia dengan segala cara sehingga selain orang yang dituju, orang lain tidak akan menyadari keberadaan dari pesan rahasia tersebut. Dari definisi diatas, maka dapat disimpulkan bahwa steganografi dibuat untuk membantu mengamankan informasi dengan cara menyembunyikan pesan pada media gambar, audio, ataupun video, agar pihak lain tidak mengetahui keberadaan informasi rahasia tersebut, kecuali si pengirim pesan dan penerima pesan.

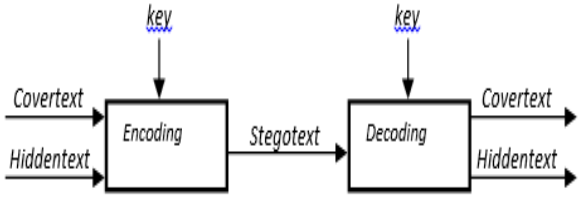
Dalam proses Steganografi terdapat beberapa kriteria yang harus dipenuhi, kriterianya adalah sebagai berikut [5]:

1. *Impercepbility*
   Keberadaan pesan tidak dapat dipersepsi oleh indra manusia, baik indra pendengaran maupun indra penglihatan.
2. *Fidelity*
   Mutu dari citra penampung tidak jauh berubah. Setelah penambahan pesan rahasia, citra hasil steganografi masih terlihat dengan baik. Pengamat tidak mengetahui kalau di dalam citra terdapat pesan rahasia
3. *Recovery*
   Pesan rahasia yang disembunyikan di dalam citra digital harus dapat diungkapkan kembali seperti aslinya.

Terdapat beberapa istilah yang berkaitan dengan steganografi:

1. *Hiddentext* atau *embedded message* ; pesan yang disembunyikan.
2. *Covertext* atau *cover-object* ; pesan yang digunakan untuk menyembunyikan *embedded message*.
3. *Stegotext* atau *stego-object* ; pesan yang sudah berisi *embedded message.*

Steganografi menggunakan media gambar ini, *hidden text* atau *embedded message* yang dimaksudkan adalah teks yang akan disisipkan ke dalam *covertext* atau *coverobject* yaitu file gambar yang digunakan sebagai media penampung pesan yang akan disisipkan. Dari hasil *encoding* atau e*mbedding* pesan kedalam file gambar akan dihasilkan *stegotext* atau *stego-object* yang merupakan file gambar yang berisikan pesan *embedding*.



Gambar 1. Cara Kerja Steganografi Secara Umum (Sumber : Krisnawati, 2008)

Penyisipan pesan ke dalam media *covertext* dinamakan encoding, sedangkan ekstraksi pesan dari *stegotext* dinamakan decoding. Kedua proses ini memerlukan kunci rahasia (*stegokey*) agar hanya pihak yang berhak saja yang dapat melakukan penyisipan dan ekstraksi pesan, seperti yang terlihat pada gambar 1.

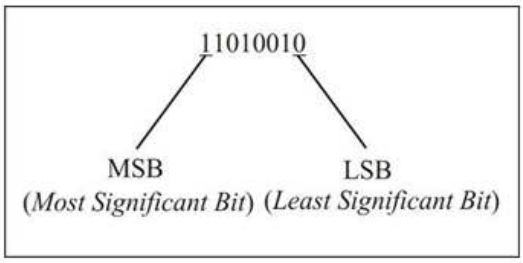
Pada dasarnya, terdapat tujuh teknik yang digunakan dalam steganografi [4] :

1. *Injection* (Penanaman) Merupakan suatu teknik menanamkan pesan rahasia secara langsung ke suatu media. Salah satu masalah dari teknik ini adalah ukuran media yang diinjeksi menjadi lebih besar dari ukuran normalnya sehingga mudah dideteksi. Teknik itu sering juga disebut *Embedding*.
2. Substitusi Data normal digantikan dengan data rahasia. Biasanya, hasil teknik itu tidak terlalu mengubah ukuran data asli, tetapi tergantung pada file media dan data yang akan disembunyikan. Teknik substitusi bisa menurunkan kualitas media yang ditumpangi.
3. *Transform Domain* (Transformasi Domain) Teknik ini sangat efektif. Pada dasarnya, transformasi domain menyembunyikan data pada "*transform space*".
4. *Spread Spectrum* Sebuah teknik pentransmisian menggunakan *pseudo-noise code,* yang independen terhadap data informasi sebagai modulator bentuk gelombang untuk menyebarkan energy sinyal dalam sebuah jalur komunikasi (*bandwidth*) yang lebih besar daripada sinyal jalur komunikai informasi. Oleh penerima, sinyal dikumpulkan kembali menggunakan replika *pseudo-noise code* tersinkronisasi.
5. *Statistical Method* Teknik ini disebut juga skema *steganographic* 1 bit. Skema tersebut menanamkan 1 bit informasi pada media tumpangan dan mengubah statistic walaupun hanya 1 bit. Perubahan statistik ditunjukkan dengan indikasi 1 dan jika tidak ada perubahan, terlihat indikasi 0. Sistem ini bekerja berdasarkan kemampuan penerima dalam membedakan antara informasi yang dimodifikasi dan yang belum.
6. *Distortion* Metode ini menciptakan perubahan atas benda yang ditumpangi oleh data rahasia.

B. Least Significant Bit

Penyembunyian pesan dilakukan dengan menggantikan bit-bit didalam segmen citra dengan bit-bit pesan rahasia. Metode yang paling sering digunakan adalah metode modifikasi LSB (*Least Significant Bit*) pada citra penampung. Pada susunan bit di dalam sebuah *byte* (1 *byte* = 8 bit), ada bit paling signifikan yang disebut MSB (*Most Significant Bit*) dan bit yang paling kurang signifikan atau LSB (*Least Significant Bit*).

e-ISSN 2597-4963 dan p-ISSN 1858-4853



Gambar 2. contoh susunan bit pada LSB dan MSB

Contoh susunan bit pada byte yang menjelaskan bit yang cocok untuk diganti adalah bit LSB, sebab penggantian hanya mengubah nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan *byte* di dalam gambar menyatakan warna tertentu, maka perubahan pada bit LSBnya tidak mengubah warna secara signifikan. Sebelum melakukan penggantian bit-bit LSB, semua data citra yang tidak bertipe 24 bit diubah terlebih dahulu menjadi format 24 bit. Jadi setiap data piksel sudah mengandung komponen warna merah, hijau dan biru (RGB). Nilai dari bit-bit yang kurang signifikan atau LSB dari setiap *byte* di dalam bitmap digantikan dengan bit-bit pesan yang akan disembunyikan. Jika *byte* merupakan komponen hijau (G), maka penggantian satu bit LSB-nya hanya mengubah sedikit kadar warna hijau, dan perubahannya tak terdeteksi oleh mata manusia [6].

Contoh penggunaan Metode LSB pada tahapan encode ;

1. Misalkan penyisispan pada citra 24-bit. Setiap pixel panjanganya 24 bit (3 x 3 byte, masing-masing komponen R (1 byte), G (1 byte), B (1 byte)).
   00110011 10100010 11100010 (misal pixel warna merah)
   Misalkan embedded message : **010**
   Encoding 00110010 10100011
   11100010
   (pixel warna 'merah berubah sedikit'. Tidak dapat dibedakan secara visual dengan citra aslinya)
2. Jika pesan = 10 bit, maka jumlah byte yang digunakan = 10 byte
   00110011 10100010 11100010
   10101011 00100110
   10010110 11001001 11111001
   10001000 10100011
   Pesan : **1110010111**
   Hasil penyisipan pada bit LSB :
   00110011 10100011 11100011
   10101010 00100110
   10010111 11001000 11111001
   10001001 10100011

C. Metode End *Of File* (EOF)

Metode EOF merupakan salah satu metode yang digunakan dalam steganografi. Metode ini menggunakan cara dengan menyisipkan data pada akhir *file*. Sehingga, tidak akan mengganggu kualitas data awal yang akan disisipkan pesan. Namun, ukuran *file* setelah disisipkan pesan rahasia akan bertambah. Sebab, ukuran *file* yang asli akan ditambah dengan ukuran *file* yang disisipkan [7]. EOF menggunakan karakter yang berbeda sebagai penanda awal penyisipan pesan dan penanda akhir penyisipan pesan. Metode EOF menggunakan kelemahan indera manusia yang tidak sensitif sehingga seakan-akan tidak ada perbedaan yang terlihat antara sebelum atau sesudah pesan disisipkan [8].

Dalam EOF pesan yang akan disisipkan pada media akan dikonvert kedalam nilai desimal berdasarkan tabel ascii. Kode ASCII (*American Standart Code for Informatian Interchange*) merupakan representasi numerik dari karakter-karakter yang digunakan pada komputer, dengan ketentuan huruf a-z, A-Z, 0-9 dan simbol standar pada keyboard.

Sebagai contoh pada sebuah citra grayscale 6x6 piksel disisipkan pesan yang berbunyi "aku". Untuk menandai akhir pesan digunakan karakter yang jarang dipakai, misalnya karakter #. Sehingga pesan yang dimaksud adalah "#aku". Kode ASCII dari pesan diberikan sebagai berikut (Hariady,2015) :

97 107 117 35

Misalkan sebuah citra grayscale dengan kode warna:

196	10	97	182	101	40
67	200	100	50	90	50
25	150	45	200	75	28
176	56	77	100	25	200
101	34	250	40	100	60
44	66	99	125	190	200

Nilai desimal pesan berdasarkan tabel ascii disisipkan diakhir citra, sehingga citra menjadi:

196	10	97	182	101	40
67	200	100	50	90	50
25	150	45	200	75	28
176	56	77	100	25	200
101	34	250	40	100	60
44	66	99	125	190	200
97	**107**	**117**	**35**		

Teknik EOF tidak mengubah isi awal dari *file* yang disisipi. Sebagai contoh, jika pengguna menyisipkan sebuah pesan kedalam sebuah dokumen, isi dari dokumen tidak akan berubah. Ini yang menjadi salah satu keunggulan metode EOF dibandingkan dengan metode *steganografi* yang lain. Karena disisipkan pada akhir *file*, pesan yang disisipkan tidak akan bersinggungan dengan isi *file*, hal ini menyebabkan integrasi data dari *file* yang disisipi tetap terjaga [9].

D. Video Digital

Video merupakan sebuah film atau gambar hidup yang dihasilkan dengan rekaman dari orang dan benda (termasuk fantasi dan figure palsu) dengan menggunakan kamera, dan memiliki fungsi dua dimensi yang terbentuk dari penglihatan dalam suatu tempat (scene) yang merupakan basis dari pembentukan video. Secara umum video dibagi

e-ISSN 2597-4963 dan p-ISSN 1858-4853

menjadi dua macam, yaitu : Pengolahan citra mempunyai dua tujuan utama yaitu [10]:.

1. Analog, yaitu video hasil tangkapan lensa kamera terhadap tempat (scene) yang discene secara vertikal dan horizontal oleh video kamera.
2. Digital, yaitu video yang direpresentasikan sebagai sebuah matriks yang masing-masing elemennya merepresentasikan nilai intensitas.

Video digital pada dasarnya tersusun atas serangkaian frame. Rangkaian frame tersebut ditampilkan pada layar dengan kecepatan tertentu , tergantung pada frame rate yang diberikan (dalam frame per second). Jika frame rate cukup tinggi, mata manusia tidak dapat menangkap gambar atau frame, melainkan menangkapnya sebagai rangkaian yang kontinu/berlanjut (video).

Masing-masing frame merupakan citra digital. Suatu citra digital direpresentasikan dengan sebuah matriks yang masing-masing elemennya merepresentasikan nilai intensitas. Jika I adalah matriks dua dimensi, I (x,y) adalah nilai intensitas yang sesuai pada posisi baris x dan kolom y pada matriks tersebut. Titik-titik ditempatkan image di sampling disebut picture elements, atau sering dikenal sebagai piksel. *Pixel* atau piksel (*picture element* / unsur gambar) adalah titik–titik kecil. Gambar apapun yang tampak pada layar komputer sebenarnya tersusun dari titik-titik kecil.

Jika beberapa piksel diletakkan berderet maka yang tampak adalah sebuah garis. Jadi semua garis, sehalus apapun tampaknya pada layar komputer, sebenarnya adalah deretan piksel. Sebuah piksel memang bisa dianggap sebagai sebuah titik, namun dalam kenyataannya, piksel-piksel lebih mirip dengan persegi panjang kecil yang tingginya tidak sebanding dengan lebarnya.

a. Frame Rate
   Ketika serangkaian gambar mati yang bersambung dilihat oleh mata manusia, maka suatu keajaiban terjadi. Jika gambar-gambar tersebut dimainkan dengan cepat maka akan terlihat sebuah pergerakan yang halus, inilah prinsip dasar film, video dan animasi. Jumlah gambar yang terlihat setiap detik disebut dengan frame rate. Diperlukan frame rate minimal sebesar 10 fps (*frame rate per second*) untuk menghasilkan gambar pergerakan yang halus. Filmfilm yang kita lihat di 11 gedung bioskop adalah film yang diproyeksikan dengan frame rate sebesar 24 fps, sedangkan video yang kita lihat di televisi kirakira memiliki frame rate sebesar 30 fps (tepatnya 29.97 fps) untuk negara yang memakai format standar NTSC (*National Television Standards Comitte*) yaitu A merika Serikat, Jepang, Kanada, Mek siko dan Korea. Untuk negara Indonesia, Inggris, Australia, Eropa dan China format video standar yang digunakan adalah format PAL (Phase Alternate Line) dengan frame rate sebesar 25 fps. Sedangkan negara Perancis, Timur Tengah dan Afrika menggunakan format video standar SECAM (*Sequential Couleur Avec Memoire*) dengan frame rate sebesar 25 fps.
b. Resolusi dan Frame Size
   Lebar dan tinggi frame video disebut dengan frame size, yang menggunakan satuan pixel, misalnya video dengan frame size 640x480 pixel. Dalam dunia digital video, frame size disebut juga dengan resolusi. Semakin tinggi resolusi gambar maka semakin besar pula informasi yang dimuat, berarti akan semakin besar pula kebutuhan memory untuk membaca informasi tersebut. Misalnya untuk format PAL D1/DV berukuran 720x576 pixel, format NTSC DV 720x480 pixel dan format PAL VCD/VHS (MPEG1) berukuran 352x288 pixel sedangkan format NTSC VCD berukuran 320x240 pixel.
c. Kedalaman *Pixel*
   Kedalaman bit menentukan jumlah bit yang digunakan untuk mempresentasikan tiap piksel pada sebuah frame dan dinyatakan dalam *bit/pixel*. Semakin banyak jumlah bit yang digunakan untuk mempresentasikan sebuah piksel, yang berarti semakin tinggi kedalaman pikselnya, maka semakin tinggi pula kualitasnya. Kedalam *pixel* paling rendah terdapat pada *binary-value image* yang hanya menggunakan 1 bit untuk tiap *pixel*, sehingga hanya ada dua kemungkinan bagi tiap *pixel*, yaitu 0 (hitam) atau 1 (putih). Nilai 1 *byte* (8 bit) untuk tiap *pixel*, diperoleh 28 atau 256 level intensitas. Kemudian video dengan kedalam 16 bit biasanya disebut video *high color*, dimana setiap pixelnya diwakili oleh 2 *byte* atau 16 bit dengan memiliki 65.356 warna. Dalam formasi bitnya, nilai merah dan biru mengambil tempat di 5 bit di kanan dan kiri. Komponen hijau memiliki 5 bit ditambah 1 bit ekstra, pemilihan komponen hijau dengan deret 6 bit dikarenakan penglihatan manusia lebih sensitif terhadap warna hijau. Dengan demikian, semakin sedikit jumlah bit yang digunakan untuk tiap *pixel*, maka semakin turun pula kualitas gambar.

E. Moving Picture Experts Group (MPEG-4)

Sebuah *video digital* terdiri dari *frame-frame* yang mana *frame-frame* tersebut dikompres menjadi sebuah *file* komputer yang hanya dapat dijalankan menggunakan sebuah perangkat lunak *multimedia player* (Ian,2003). Berdasarkan bentuk-bentuk kompresan dari *file video digital* tersebut, banyak bermunculan format-format *video digital* yang ditawarkan kepada pengguna dengan kelebihan dan kekurangannya masing-masing. Salah satu contoh format video digital adalah MP4. MPEG-4 Bagian 14 atau MP4 format *file*, secara resmi ISO / IEC 14496-14:2003, adalah sebuah standar format multimedia container yang ditetapkan sebagai bagian dari MPEG-4. Hal ini paling sering digunakan untuk menyimpan video digital dan digital stream audio, terutama yang didefinisikan oleh MPEG, tetapi juga dapat digunakan untuk

menyimpan data lain seperti subtitle dan gambar diam. Seperti format wadah paling modern, MPEG-4 Part 14 memungkinkan streaming melalui Internet. Trek petunjuk terpisah digunakan untuk menyertakan informasi dalam streming *file*. *File*name extension resmi untuk MPEG-4 Bagian 14 *file* adalah MP4, sehingga format wadah sering disebut hanya sebagai MP4 (Amont, Ratghent, Singer, 2007)[11].

3. HASIL DAN PEMBAHASAN

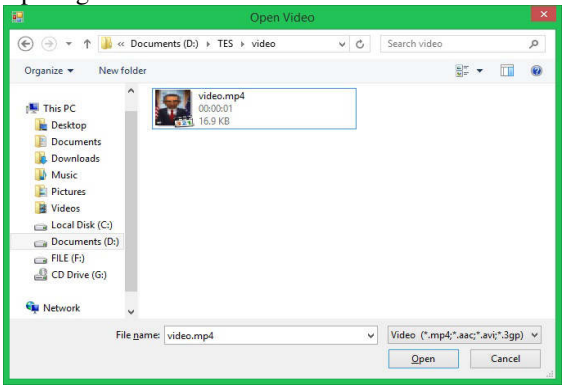
Pada halaman awal aplikasi terdapat menu-menu yang dapat dipilih oleh pengguna. Menu ini terdiri dari 4 sub menu yaitu menu Home, menu Penyisipan, menu Ekstraksi dan menu About. Seperti pada gambar 3.

Gambar 3. Halaman Awal Aplikasi

Pada menu penyisipan terdiri dari 4 sub menu yaitu menu Home, menu Penyisipan, menu Ekstraksi dan menu About. Seperti pada gambar 4.

Gambar 4. Halaman Menu Penyisipan

Langkah awal dalam melakukan proses penyisipan yaitu dengan menekan tombol open untuk menampilkan openfile dialog, setelah itu pengguna diminta untuk memilih video yang akan ditampilkan kedalam media player pada aplikasi. Openfile dialog hanya menampilkan file video berekstensi mp4 seperti gambar 5.



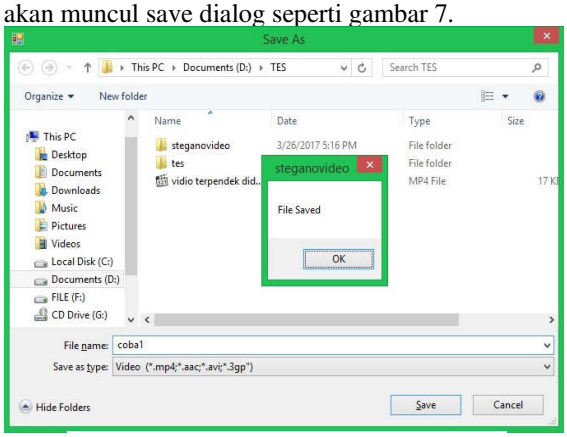
Gambar 5. Open Dialog Form Penyisipan

Setelah menginput video yang akan dijadikan sebagai cover maka user diminta untuk menginputkan kunci rahasia pada textbox private key dan pesan teks yang akan disisipkan pada textbox message seperti gambar 6.

Gambar 6. Proses Embedding

Perhatikan gambar 4.5 sebagai contoh pengguna memasukkan kunci yang berbunyi "admin" pada textbox private key dan "nama saya adalah ulan arianti" pada textbox message. Pengguna dapat melihat keterangan dari jumlah karakter pesan yang dimasukkan oleh pengguna adalah 29, sedangakan keterangan dari video yang dimasukkan adalah 30 fps, durasi 1 detik, jumlah bitrate 91 dan dimensi awal 202 x 360 dan duration process bergantung pada proses yang dipilih baik EOF maupun LSB memiliki durasi proses yang berbeda. Setelah pengguna memasukkan data yang diminta oleh sistem, maka selanjutnya pengguna menekan tombol penyisipan EOF atau LSB untuk melakukan proses penyisipan pesan pada file video.

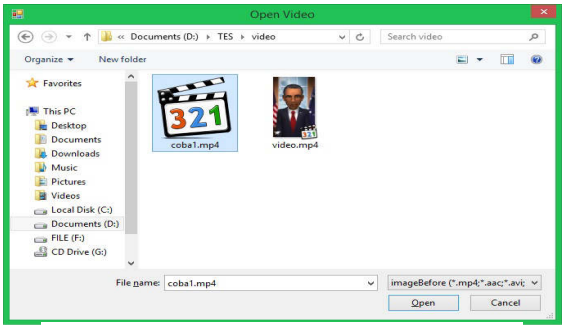
Proses penyisipan memerlukan beberapa waktu tergantung jumlah fps dan durasi pada file video. Pada proses ini aplikasi akan melakukan pembacaan frame video dan mengambil frame pixel terakhir pada proses penyisipan EOF untuk disisipkan pesan teks. Sedangkan pada LSB proses akan melakukan pembacaan pada sebuah frame dan merubah menjadi bit-bit, untuk disisipakn pesan. Setelah proses selesai maka user dapat menyimpan file video yang telah disisipkan pesan dengan menekan tombol save dan akan muncul save dialog seperti gambar 7.



Gambar 7. Save Dialog Form Embedding

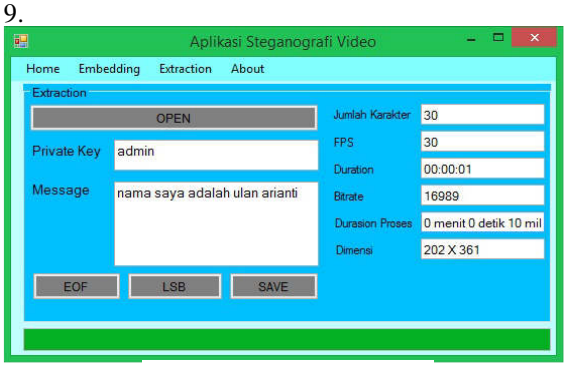
Selanjutnya adalah menu extraction. Pada form extraction user diminta untuk memasukkan stego video dengan menekan tombol open untuk menampilkan open dialog seperti gambar 8.

e-ISSN 2597-4963 dan p-ISSN 1858-4853



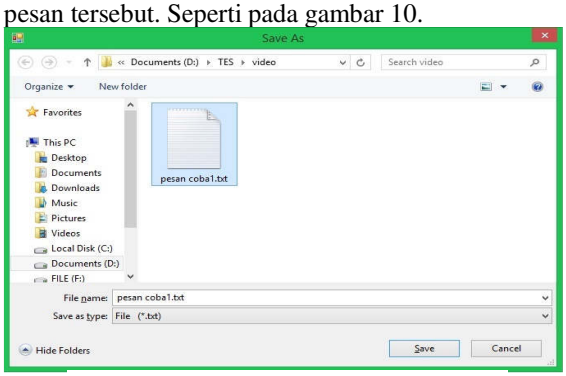
Gambar 8. Open File Dialog Form Extraction

Setelah video dimasukkan pengguna diminta untuk memasukkan kunci pada textbox private key agar proses ekstrasi dapat dilakukan seperti gambar 9.



Gambar 9. Proses Ekstraksi

Setelah pengguna memasukkan kunci pengguna diminta untuk menekan tombol EOF atau LSB agar proses ekstraksi pesan dapat dilakukan dan sistem akan menampilkan pesan pada textbox message. Setelah sistem menampilkan pesan pada textbox, user dapat memilih tombol save untuk menyimpan pesan tersebut. Seperti pada gambar 10.



Gambar 10. Save Dialog Form Extraction

Pada proses extraction, sistem akan membaca nilai pixel frame pada baris terakhir, kemudian sistem akan mengkonversi nilai pixel kedalam bentuk karakter pesan dengan menggunakan kode ascii. Tahapan selanjutnya adalah pengujian. Pengujian dilakukan untuk membandingkan ukuran video sebelum dan sesudah dilakukan proses steganografi berdasarkan jumlah karakter pesan yang disisipkan. Hasil dari pengujian tersebut terdapat pada tabel 1 dan tabel 2.

Tabel 1. Perbandingan Berdasarkan Ukuran Dan Dimensi pada EOF

No		EOF	
		Embedding	Extraction
1	Kunci	Stegano	Stegano
	Pesan	Ulan ari anti 1007055123	Ulan ari anti 1007055123
	Dimensi ideo	202 x 360	202 x 361
	Ukuran Video	16,9 kb	3.1 mb
	Bitrate	91 kbps	16986 kbps
2	Kunci	Stegano	Stegano
	Pesan	Ulan ari anti 1007055123 Ilmu komputer unmul samrinda	Ulan ari anti 1007055123 Ilmu komputer unmul samrinda
	Dimensi Video	202 x 360	202 x 361
	Ukuran Video	16,9 kb	3.1 mb
	Bitrate	91 kbps	16990 kbps

Tabel 2. Perbandingan Berdasarkan Ukuran Dan Dimensi Pada LSB

No		LSB	
		Embedding	Extraction
1	Kunci	Stegano	Stegano
	Pesan	Ulan ari anti 1007055123	Ulan ari anti 1007055123
	Dimensi Video	202 x 360	202 x 360
	Ukuran Video	16,9 kb	3.1 mb
	Bitrate	91 kbps	16992 kbps
2	Kunci	Stegano	Stegano
	Pesan	Ulan ari anti 1007055123 Ilmu komputer unmul samrinda	Ulan ari anti 1007055123 Ilmu komputer unmul samrinda
	Dimensi Video	202 x 360	202 x 360
	Ukuran Video	16,9 kb	3.1 mb
	Bitrate	91 kbps	16994 kbps

Berdasarkan pengujian membandikan ukuran video dengan durasi waktu satu detik menggunakan metode EOF dan LSB sebelum dan sesudah dilakukan proses penyisipan pesan, maka dapat dilihat dari tabel 1 dan 2 bahwa perbandingan ukuran video sebelum dan setelah dilakukan proses penyisipan mengalami perubahan dari segi ukuran video, dimensi video dan bitrate. Hal ini disebabkan karena terdapat pesan yang disisipkan sehingga video mengalami penambahan bitrate, dimensi dan ukuran video. Pada tabel 1 dapat dilihat pada kolom nomor 1 penyisipan pada EOF ukuran video sebelum disisipkan pesan adalah 16,9 Kb dengan dimensi 202x360 dan bitrate awal 91 mengalami penambahan ukuran menjadi 3.1 Mb dengan dimensi 640x361 serta penambahan bitrate menjadi 16986 kbps. Sedangkan penyisipan menggunakan LSB pada tabel 2 ukuran video sebelum disisipkan pesan adalah 16,9 Kb dengan dimensi 202x360 dan bitrate awal 91 mengalami penambahan ukuran menjadi 3.1 Mb dengan dimensi 640x360 serta penambahan bitrate

menjadi 16992 kbps. Kapasitas maksimal file pesan rahasia yang disisipkan tidak boleh melebihi kapasitas dari frame. Jumlah frame yang dihasilkan sebelum proses penyisipan dan ukuran masing-masing frame ditunjukkan pada program aplikasi. Sehingga user bisa menentukan ukuran file pesan rahasia yang disisipkan ke dalam file video tidak melebihi ukuran frame. Berdasarkan hasil pengujian, tidak semua file pesan rahasia yang mempunyai ukuran file lebih besar dari ukuran frame dapat disisipkan.

Pengujian sistem yang kedua adalah untuk melihat waktu yang dibutuhkan dalam melakukan proses penyisipan maupun proses ekstrasi berdasarkan jumlah frame dan durasi video. Hasil dari pengujian tersebut terdapat pada tabel 3 dan tabel 4.

Tabel 3. Tabel Pengujian Berdasarkan Waktu Proses EOF

No	Durasi (detik)	FPS	Kunci	Pesan	Waktu Proses EOF (menit:detik:milidetik)	
					Embedding	Extraksi
1	00:01	30	stegano	ulan ari anti	00:20:922	00:00:09
2	00:03	30	stegano	ulan ari anti	01:54:374	00:00:05
3	00:10	25	stegano	ulan ari anti	01:04:640	00:00:05
4	00:20	24	stegano	ulan ari anti	04:00:1280	00:00:05

Tabel 4. Tabel Pengujian Berdasarkan Waktu Proses LSB

No	Durasi (detik)	FPS	Kunci	Pesan	Waktu Proses LSB (menit:detik:milidetik)	
					Embedding	Extraksi
1	00:01	30	stegano	ulan ari anti	00:20:727	00:00:52
2	00:03	30	stegano	ulan ari anti	01:53:3127	00:00:52
3	00:10	25	stegano	ulan ari anti	01:04:7	00:00:411
4	00:20	24	stegano	ulan ari anti	04:16:5	00:00:121

Pengujian dilakukan untuk mengetahui apakah jumlah frame berpengaruh pada proses penyisipan maupun ekstrasi pada video tersebut, serta apakah durasi video berpengaruh terhadap waktu untuk melakukan proses tersebut. Pengujian perbandingan waktu untuk melakukan proses embedding dan extraction menggunakan metode EOF dan LSB berdasarkan jumlah fps dan durasi video dapat dilihat pada tabel 3 dan 4. Sebelum proses penyisipan, file video akan dibagi menjadi beberapa frame yang terdiri dari file Portable Network Graphics (.PNG). Pengujian waktu berdasarkan jumlah fps ini dapat dilihat pada kolom nomor 1 tabel 3 pada EOF dan LSB tabel 4 video dengan durasi 1 detik, fps 30 dan dimensi 202x360 kemudian masing-masing video disisipkan kunci berbunyi "stegano" dan pesan teks berbunyi "ulan ari anti". Pengujian dilakukan dengan melihat perbedaan waktu proses penyisipan, proses ekstraksi dari jumlah fps dan durasi video yang dimiliki oleh video dan dimensi video. Pada pengujian ini hasil yang didapat adalah waktu proses penyisipan pada EOF lebih lama dibandingkan waktu proses pada LSB, sedangkan waktu proses ekstraksi EOF lebih cepat dibandingkan dengan waktu proses LSB.

Dimensi video juga mempengaruhi dalam proses penyisipan semakin besar dimensi video maka semakin lama proses penyisipan dan ekstraksi video pada EOF ataupun pada LSB. Dimensi dapat di lihat pada tabel 3 dan 4. Dari pengujian waktu proses dengan membandingkan jumlah fps, durasi video dan dimensi video adalah semakin besar dimensi, jumlah fps dan semakin lama durasi maka semakin lama juga sistem melakukan proses embedding dan extraction. Hal ini dikarena kan jumlah fps, durasi video dan dimensi berpengaruh pada proses pembacaan frame pada file video. Hasil pengujian juga menunjukkan bahwa semakin besar file pesan rahasia yang disisipkan, semakin kecil tingkat keberhasilan proses penyisipan file pesan rahasia ke dalam file video.

4. KESIMPULAN

Berdasarkan pengujian yang telah dilakukan, didapatkan bahwa aplikasi steganografi video ini mampu menyimpan pesan teks tetapi ukuran teks tersebut tidak melebihi daya tampung *cover frame* video. Serta lama proses melakukan steganografi metode EOF dan LSB ditentukan oleh durasi, jumlah frame dan besar dimensi video. Proses *embedding* teks LSB memerlukan waktu yang lebih sedikit dibandingkan EOF dan sebaliknya proses ekstraksi EOF memerlukan waktu yang lebih sedikit dibandingkan LSB.

5. DAFTAR PUSTAKA

[1]. Maula, Ismiatul. 2016. Steganografi Teks Pada Video Menggunakan Metode End Of File (EOF). Skripsi. Universitas Mulawarman.

[2]. Hendrawati. 2013. Keamanan Data Dengan Menggunakan Algoritma Rivest Code 4 (RC4) dan Steganografi Pada Citra Digital. Skripsi. Univeristas Mulawarman.

[3]. Agrawal, V.K. 2007. Perceptual Watermarking of Digital Video using The Variable Temporal Length 3D-DCT. Thesis. Department of Electrical Engineering, Indian Institute of Technology, Kanpur

[4]. Ariyus, D. 2009. Keamanan Multimedia. Yogyakarta: Andi.

[5]. Vembrina, Y. (2006). Spread Spectrum Steganograpy. Bandung: Sekolah Teknik Elektro dan Informatika.

[6]. Rahim, M. 2006. Teknik Penyembunyian Data Rahasia Dengan Menggunakan Citra Digital Sebagai Berkas Penampung. Semarang : Universitas Diponegoro.

[7]. Agutaviana, ilmia. 2012. Aplikasi Pesan Rahasia Berbasis Web Menggunakan Vigenere Chiper Dan Steganografi End Of File . Skripsi. Universitas mulawarman

[8]. Edisuryana, M., Isnanto, R.R., Somantri, M.. 2013. Aplikasi Steganografi Pada Citra Berformat Bitmap Dengan Menggunakan

Metode End Of File. Jurnal Teknik Elektro. Universitas Diponegoro Semarang.

[9]. Sukrisno, U. E. (2007). Implementasi Steganografi Teknik EOF Dengan Gabungan Enkripsi Rijndael, Shift Cipher dan Fungsi Hash MD5. In Seminar Nasional Teknologi (SNT).

[10]. Ida Ayu Laksmi Dewi. 2015. Frame Rate Minimum Pada Video Tanpa Kompresi Menggunakan Normalized Frame Difference Sebagai Pendeskripsi Intensitas Gerak. Skripsi. Jurusan Teknik Elektro Fakultas Teknik Universitas Udayana.