Jurnal Minfo Polgan
Volume 12, Nomor 2, Juni 2023
DOI : https://doi.org/10.33395/jmp.v12i2.12418
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Terbit : 01 Juni 2023

Implementasi Algoritma *Vigenere Cipher* Dan *End Of File* Pada Steganografi Video

[1]Minarni, [2] Aliyul Ikram, [3]Indra Warman, [4]Ganda Yoga Swara
[1, 2, 3, 4]Program Studi Teknik Informatika, Fakultas Teknik, Institut Teknologi Padang, Indonesia

[1]minarni1706@gmail.com, [2]aliyulikram@gmail.com, [3]indrawmn@gmail.com,
[4]gandayogaswara@gmail.com

ABSTRAK

Perkembangan teknologi informasi, jaringan, dan internet yang begitu pesat memberi kemudahan dalam bertukar informasi. Menjaga kerahasiaan dan keamanan informasi dari pihak yang tidak berkepentingan menjadi bagian penting dalam pertukaran informasi. **Penelitian** ini bertujuan untuk mengamankan pesan rahasia menggunakan kombinasi kriptografi dan steganografi dengan mengimplementasikan algoritma *Vigenere Cipher* yaitu mengubah pesan atau informasi menjadi format yang tidak dapat dibaca (pesan terenkrip) menggunakan deretan sandi *Caesar* berdasarkan huruf-huruf pada kunci. Pesan yang telah diubah, kemudian disisipkan pada akhir file video menggunakan metode *End Of File*. **Pengujian** dilakukan berdasarkan kriteria steganografi, yaitu *imperceptibility*, *fidelity*, *robustness* dan *recovery* pada beberapa file video berformat mp4 dengan variasi jumlah karakter yang disisipkan mulai dari 50 karakter sampai dengan 5000 karakter. **Hasil pengujian** *imperceptibility* terpenuhi karena pesan rahasia pada stego video tidak diketahui oleh orang lain. Berdasarkan *Fidelity*, *bit rate* dan *frame rate stego video* tidak mengalami perubahan setelah disisipkan pesan. Ini menandakan bahwa pengujian *fidelity*-nya sangat baik. Tetapi pada pengujian manipulasi file *stego video* dengan memotong dan memperlambat file *stego video*, pesan rahasia tidak bisa di*recovery*. Di sini terlihat bahwa dua kriteria steganografi terpenuhi. Pesan terenkrip dapat dibaca kembali dengan baik tanpa merusak file video. Dengan demikian steganografi dengan algoritma EoF dan algoritma *Vigenere Cipher* pada media video dapat mengamankan pesan atau informasi yang bersifat rahasia.

Kata Kunci: *End of File*; Kriptografi; Steganografi; Video; *Vigenere Cipher*

PENDAHULUAN

Perkembangan teknologi informasi, jaringan, dan internet yang begitu pesat memberi kemudahan dalam mendapatkan informasi. Informasi yang didapatkan dapat bersifat rahasia dan bersifat umum. Pada informasi yang rahasia dibutuhkan pengamanan dan penjagaan kerahasiaan informasi. Ini menjadi satu faktor utama suatu informasi, sehingga informasi hanya dapat digunakan oleh pihak yang berwenang atas informasi tersebut (Faris et al., 2023). Steganografi merupakan salah satu cara yang digunakan dalam mengamankan informasi yang dianggap rahasia. Pada steganografi dilakukan proses penyembunyian data rahasia ke dalam file lain yang bertujuan agar pihak lain tidak mengetahui pesan rahasia yang terkandung dalam file tersebut. Steganografi merupakan salah satu metode yang digunakan dalam menyembunyikan pesan berupa data menggunakan media digital. Steganografi digital menggunakan media digital berupa suara, gambar, teks maupun video sebagai wadah penampung atau sebagai data rahasia yang disembunyikan (Munir, 2004). Video merupakan media untuk menangkap, merekam, memproses, mentransmisikan dan menata ulang gambar bergerak. Video menjadi salah satu media untuk menyembunyikan pesan atau informasi rahasia yang dikenal dengan Steganografi Video (Liu et al., 2019). Metode *End Of File* (Eof) merupakan metode untuk menyisipkan pesan pada akhir berkas

Jurnal Minfo Polgan
Volume 12, Nomor 2, Juni 2023 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v12i2.12418 p-ISSN : 2089-9424

atau media penampung. Kelebihan metode ini pesan yang disisipkan tidak terbatas jumlahnya (Hutasoit, 2019). Untuk meningkatkan keamanan dari steganografi dapat dikombinasikan dengan kriptografi.

Kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan/data/informasi dengan menulis rahasia. Dengan tujuan untuk mengolah informasi menggunakan suatu algoritma sehingga pesan atau informasi tidak dapat dibaca atau dipahami oleh pihak yang tidak berhak. Pada kriptografi terdapat Enkripsi yaitu proses untuk mengamankan pesan asli *(plain text)* menjadi pesan tersembunyi *(ciphe rtext),* dan Dekripsi yaitu proses pengembalian pesan yang telah dienkripsi (Munir, 2006). Algoritma *Vigenere Cipher* salah satu dari banyak algoritma kriptografi yang bekerja mengkodekan teks alfabet menggunakan deretan kode *caesar* berdasarkan huruf-huruf pada kunci. Algoritma ini dapat mengganti pesan dengan menggabungkan 26 huruf alfabet (Permana, 2018). Penggabungan teknik steganografi dan kriptografi menjadi salah satu solusi untuk meningkatkan keamanan pesan dan data rahasia (Taha et al., 2019). Pesan terlebih dahulu dikodekan dengan algoritma kriptografi, kemudian pesan tersebut disembunyikan ke dalam suatu media pembawa pesan, sehingga tidak menimbulkan kecurigaan orang lain.

Penelitian ini bertujuan untuk mengimplementasikan algoritma *Vigenere Cipher* untuk mengenkripsikan pesan, kemudian pesan yang telah terenkrip disisipkan menggunakan metode *End of File* untuk meningkatkan keamanan data atau pesan atau informasi pada file video.

TINJAUAN PUSTAKA

Penelitian tentang penggabungan steganografi dan kriptografi yang menjadi acuan dalam penelitian ini, diantaranya penelitian tentang menjaga keamanan data berupa dokumen ujian dengan mengimplementasikan algoritma kriptografi RC4 dan 3DES dan steganografi algoritma *End of File.* Media penampung yang digunakan berupa video. Hasil yang diperoleh berupa kualitas video tidak mengalami perubahan setelah disisipkan file, file yang sudah diencode tidak dapat dibuka oleh siapapun kecuali yang memiliki password, file hasil decode tidak mengalami perubahan (Basim & Painem, 2020). Penelitian tentang kombinasi kriptografi kunci publik dengan steganografi *Least Significant Bit* (LSB) untuk penyisipan jalur penerbangan UAV rahasia dalam media digital. Eksperimen dilakukan dengan media gambar, video, dan audio. Hasil yang diperoleh seluruh eksperimen mencapai nilai di atas 30 (Wastupranata, 2022). Penyisipan teks pada citra menggunakan algoritma EoF dan algoritma OTP, dengan tujuan untuk memperoleh *cipher* yang lebih kuat dengan menyisipkan pesan ke dalam citra agar tidak mudah disadap. Hasil dari penelitian ini menunjukkan bahwa penggunaan algoritma *One Time Pad* dan *End Of File* dapat mengamankan pesan yang disisipkan ke dalam citra sekaligus mengamankan kunci untuk kebutuhan data (Prahmana, 2022). Penelitian tentang penyisipan teks pada file audio dengan menggabungkan metode *Least Significant Bit* (LSB) dengan algoritma *Vigenere Cipher*. Hasil penelitian menunjukkan bahwa penerapan kedua metode ini pada media audio dapat menyisipkan dan menguraikan kembali pesan yang telah terenkrip tanpa merusak file audio (Minarni & Redha, 2020). Penelitian tentang implementasi vigenere cipher dan beaufort cipher mampu mengamankan suatu pesan menjadi pesan rahasia. Vigenere cipher dan beaufort cipher dapat berfungsi dengan baik saat dikombinasikan (Ryan et al., 2020)

METODE PENELITIAN

Penelitian dilaksanakan berdasarkan siklus pengembangan sistem metode *waterfall*, terdiri dari analisis, desain, implementasi, dan pengujian (Rosa, 2016). Langkah-langkah tersebut dapat dijelaskan sebagai berikut.

Analisis Kebutuhan

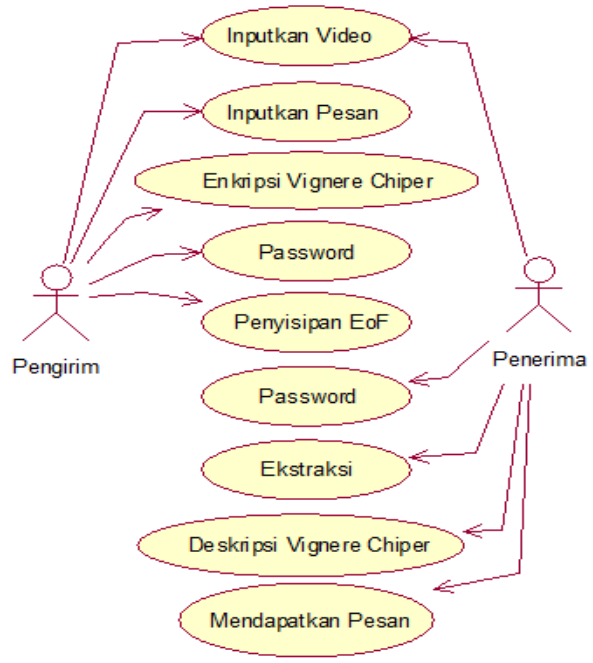
Pada penelitian ini dibangun sebuah aplikasi yang berfungsi untuk menyisipkan pesan pada video dengan menggabungkan metode *End Of File* (Eof) dengan algoritma kriptografi *Vigenere Cipher* bertujuan memberikan keamanan ganda pada pesan yang akan disembunyikan. Aplikasi ini dibangun menggunakan *Visual Basic 6.* Fokus dari program ini menyisipkan

Jurnal Minfo Polgan
Volume 12, Nomor 2, Juni 2023 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v12i2.12418 p-ISSN : 2089-9424

informasi/pesan pada piksel dari video. Sebelum disisipkan, pesan dienkripsi menggunakan algoritma *Vigenere Cipher*. File video yang akan disisipkan, terlebih dahulu diubah ke dalam bentuk desimal. Pesan hasil enkripsi disisipkan pada bagian akhir file video. Analisis kebutuhan dalam penelitian ini meliputi bahan berupa file video berformat mp4 dengan ukuran 5 MB sampai dengan 30 MB sebagai media penampung, dan pesan berupa text. Fitur-fitur yang harus disediakan pada sistem untuk digunakan oleh pengguna dalam melakukan penyisipan pesan pada video dan memperoleh kembali pesan engan mengekstrak file video tersebut.

Desain

Pada tahap ini dilakukan perancangan aplikasi yang memberikan gambaran umum aplikasi yang yang akan dibangun menggunakan *use case diagram*. Pada gambar 1 dapat dijelaskan terdapat dua aktor yaitu pengirim dan penerima. Proses yang dilakukan, pengirim menginputkan sebuah video, pesan yang akan disisipkan lalu pesan tersebut dienkripsikan terlebih dahulu, sebelum proses penyisipan dilakukan masukan password terlebih dahulu, hasil enkripsi disisipkan dan diolah oleh sistem dan dijadikan video yang sudah berisi pesan (*stego video*). Penerima menginputkan *stego video*, lalu memasukan kunci steganografi (password) yang dikirim oleh pengirim ke dalam sistem dan sistem mengeluarkan pesan, pesan yang sudah didapat akan didekripsi terlebih dahulu agar isi pesan dapat dibaca.



Gambar 1. *Use Case Diagram* Aplikasi Steganografi Video

Implementasi

Tahap ini merupakan tahapan pembuatan program berdasarkan hasil desain sebelumnya. Di sini terdapat dua proses yang dilakukan, yaitu Proses Encoding merupakan proses menyisipkan pesan ke dalam media video (*stego video*). Proses Decoding yaitu proses mengambil kembali pesan dari *stego video*.

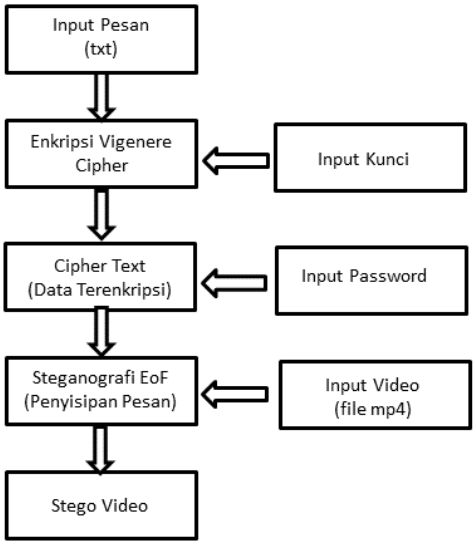
Encoding

Gambar 2 menampilkan proses encoding. Langkah awal menginputkan pesan teks yang akan disisipkan. Kemudian pesan tersebut dienkripsi menggunakan algoritma *Vigenere Cipher*. Algoritma ini memanfaatkan bujur sangkar *Vigenere Cipher*, di mana setiap baris dalam bujur sangkar menyajikan huruf-huruf *cipher text* (Munir, 2006). Untuk proses enkripsi menggunakan persamaan 1 (Qowi & Hudallah, 2021).

Jurnal Minfo Polgan
Volume 12, Nomor 2, Juni 2023
DOI : https://doi.org/10.33395/jmp.v12i2.12418
e-ISSN : 2797-3298
p-ISSN : 2089-9424

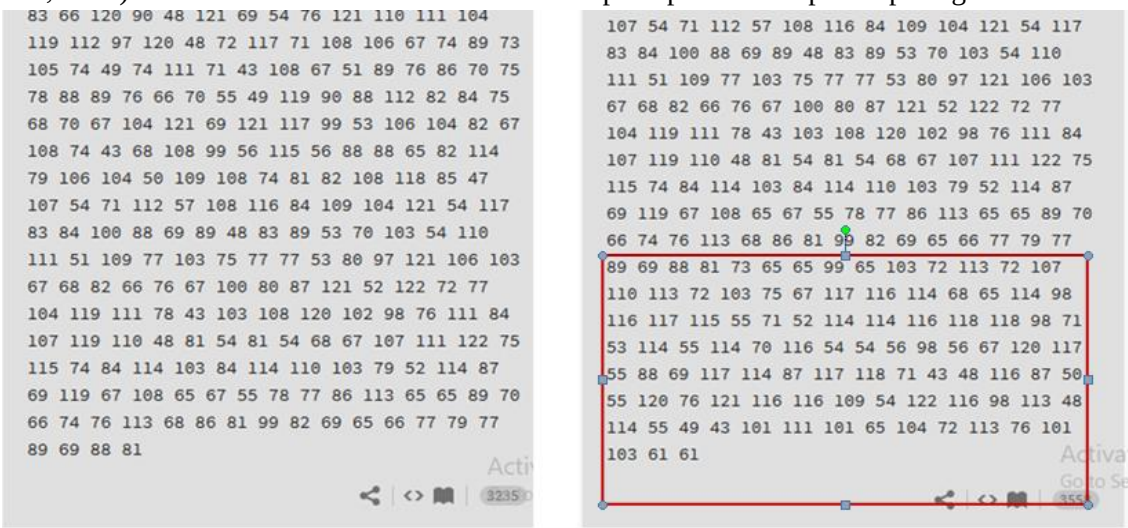
$$\boldsymbol{C = E(P, K) = (P + K) mod\ 26} \qquad (1)$$

Keterangan:
C=*Cipher Text*= Pesan Hasil Enkripsi
E(P,K) = Enkripsi P menggunakan K
P=*Plain Text* = Pesan Asli
K=*Key*=Kunci untuk melakukan Enkripsi dan Dekripsi



Gambar 2. Diagram Blok Encoding

Setelah pesan terenkripsi menghasilkan *cipher text*, kemudian file video diinputkan sebagai media penampung *cipher text*. *Cipher text* disisipkan menggunakan metode *End Of File* (EoF). Langkah-langkah metode EoF dapat dijelaskan sebagai berikut: File video diubah menjadi menjadi piksel desimal, kemudian inputkan *cipher text* dan password. *Cipher text* dan password juga diubah ke dalam bentuk decimal. Kemudian password disisipkan di awal dan akhir *cipher text*. Hasil ini disisipkan di akhir file sehingga diperoleh *stego video* (video yang telah disisipkan pesan) (Riadi et al., 2021). Hasil video sebelum dan sesudah disisipkan pesan ditampilkan pada gambar 3.



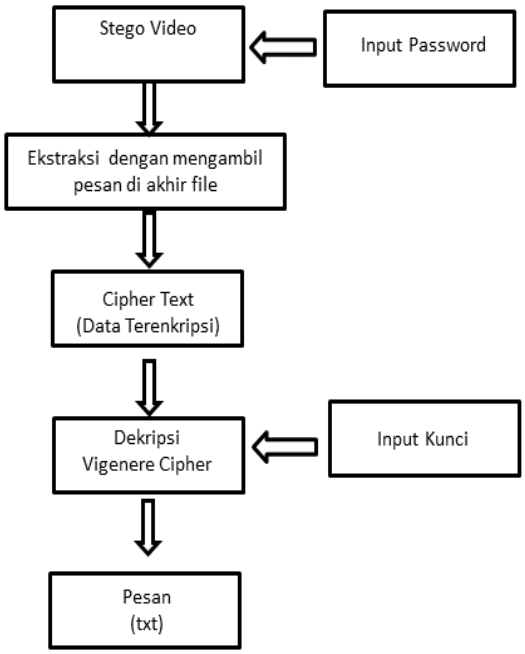
(a) (b)

Gambar 3. (a) Sebelum disisipkan pesan; (b) Setelah disisipkan pesan 50 karakter

Jurnal Minfo Polgan
Volume 12, Nomor 2, Juni 2023 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v12i2.12418 p-ISSN : 2089-9424

Decoding

Proses untuk mengambil kembali pesan yang ada di dalam file video ditunjukkan pada gambar 4.



Gambar 4. Diagram Blok Decoding

Langkah pertama *stego video* diinputkan dan diubah menjadi bentuk piksel desimal, kemudian diinputkan password yang telah diubah menjadi bentuk piksel desimal. Kemudian pesan terenkrip (*cipher text*) diambil pada piksel *stego video* berdasarkan password yang telah diinputkan. Kemudian password dipisahkan dari *stego video*, dan didapatkanlah *cipher text*. Selanjutnya dilakukan tahap dekripsi menggunakan persamaan 2 algoritma *Vigenere Cipher* (Munir, 2006).

$$\boldsymbol{P = (C - K) mod\ 26} \quad (2)$$

Sehingga menghasilkan *plain text* atau pesan asli dapat diperoleh kembali.

Pengujian

Tahapan ini dilakukan untuk melihat kemampuan dari aplikasi yang sudah dibangun berdasarkan kriteria steganografi yang baik, yaitu pesan atau informasi yang disisipkan tidak dapat dikenali oleh orang (*Imperceptibility*), media penampung yang berisikan pesan tidak mengalami perubahan dari file aslinya (*fidelity*), pesan rahasia yang disisipkan harus memiliki ketahanan terhadap beberapa operasi yang mungkin dikenakan pada media penampung (*robustness*) dan pesan harus dapat diperoleh kembali (*recovery*) (Zulfikar, 2020).

HASIL DAN PEMBAHASAN

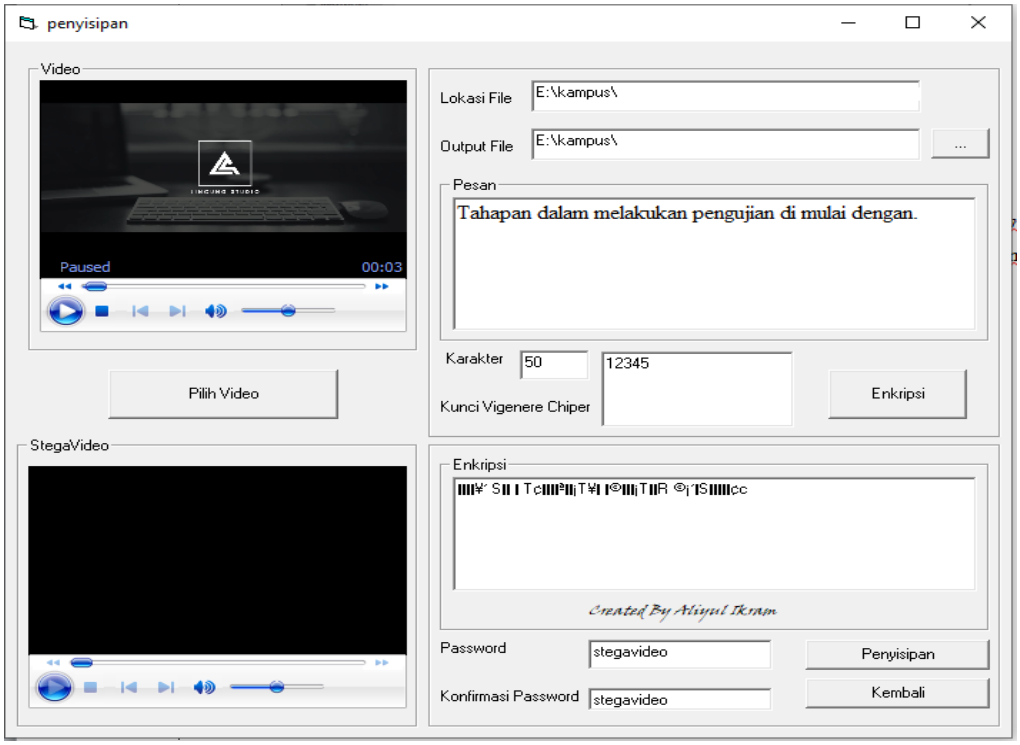
Halaman utama aplikasi *stego video* yang telah dibangun ditampilkan pada gambar 5. Halaman utama memiliki 3 menu, yaitu menu penyisipan pesan, menu ekstraksi, dan menu keluar.

Halaman Penyisipan

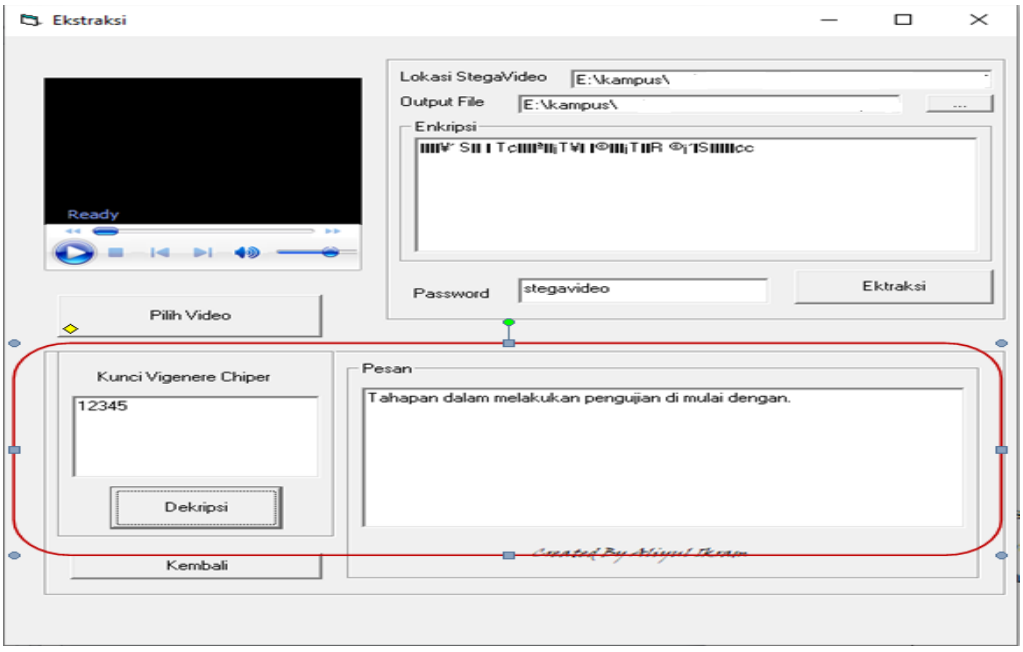
Halaman penyisipan digunakan untuk memproses encoding. Pada halaman ini terdapat 2 buah *Windows Media Player* yang berfungsi sebagai penampil video yang akan disisipkan pesan serta video hasil dari penyisipan, 5 buah *button* yaitu *button* “Pilih Video” yang berfungsi sebagai

Jurnal Minfo Polgan
Volume 12, Nomor 2, Juni 2023 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v12i2.12418 p-ISSN : 2089-9424

memilih video yang akan disisipkan pesan, *button output file "..."* yang berfungsi sebagai *button* penyimpan video hasil penyisipan, *button* "*Enkripsi*" yang berfungsi sebagai *button* perubahan pesan asli menjadi pesan acak yang menggunakan *Vigenere Cipher*, *button "*penyisipan" yang berfungsi sebagai *button* untuk menyisipkan pesan ke media Video yang digunakan, *button "*Kembali" yang berfungsi sebagai *button* kembali ke halaman menu pada aplikasi. Selain *button*, juga terdapat 3 buah *RichTextBox* yang berfungsi untuk tempat pesan serta kunci *Vigenere Cipher*, dan beberapa *component text* untuk *password*, tempat dimana lokasi simpan serta sebagai pemberitahu jumlah karakter yang akan disisipkan. Seperti yang ditunjukkan pada gambar 6.



Gambar 6. Halaman Penyisipan Pesan



Gambar 7. Halaman Ekstraksi Pesan

Jurnal Minfo Polgan
Volume 12, Nomor 2, Juni 2023 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v12i2.12418 p-ISSN : 2089-9424

Halaman Ekstraksi

Halaman ekstraksi digunakan untuk memproses decoding. Halaman ini tidak jauh berbeda dengan halaman penyisipan, perbedaannya terdapat pada *button* "ekstraksi". Selain itu perbedaan pada *form* ekstraksi juga terletak pada posisi penginputan *password* dan penginputan pesan, dimana pada halaman ekstraksi tidak memiliki pengulangan *password* seperti pada *form* penyisipan, juga tidak memiliki kolom *text* yang dapat memberitahukan jumlah pesan yang telah disisipkan. Seperti ditunjukkan pada gambar 7.

Pengujian

Pengujian pada aplikasi steganografi video dengan EoF dan algoritma *Vigenere Cipher* menggunakan sampel file video dengan format mp4 sebagai media penampung berukuran 5 MB sampai dengan 30 MB. Pesan yang disisipkan berupa file format txt dengan jumlah karakter yang bervariasi. Ini ditujukan untuk mengetahui kemampuan dari aplikasi terkait dengan perubahan ukuran video setelah disisipkan pesan, waktu yang dibutuhkan untuk penyisipan dan ekstraksi pesan, *fidelity stego video (bit rate dan frame rate), robustness (cutting dan slowmotion) stego video.*

Perubahan Ukuran Video dan *Imperceptibility*

Pengujian perubahan ukuran video dilakukan dengan memasukkan beberapa karakter pesan pada berbagai macam file video dan kemudian dilihat perubahan dari ukuran video setelah disisipkan pesan.

Tabel 1. Pengujian Perubahan Ukuran Video

No	Pesan (Char)	Ukuran Video (Bytes)				
		1.Mp4 31,489,766	2.Mp4 19,572,630	3.Mp4 17,072,927	4.Mp4 22,357,604	5.Mp4 23,088,350
1	50	31,489,834	19,572,698	17,073,009	22,357,700	23,088,460
2	100	31,489,940	19,572,818	17,073,129	22,357,820	23,088,580
3	200	31,489,984	19,572,862	17,073,173	22,357,864	23,088,624
4	400	31,490,254	19,573,132	17,073,443	22,358,134	23,088,894
5	800	31,490,724	19,573,602	17,073,913	22,358,604	23,089,364
6	5000	-	19.577.649	-	-	-

Tabel 1 menunjukkan adanya perubahan ukuran dari file video menjadi *stego video*, berdasarkan jumlah karakter yang disisipkan. Semakin banyak karakter pesan yang disisipkan maka semakin besar ukuran file *stego*. Namun pada metode EOF pesan yang disisipkan bukan berupa pesan langsung, namun pesan yang sudah diubah ke dalam bilangan desimal dimana ini mempengaruhi ukuran penyimpanan pesan menjadi 2 kali atau lebih besar, seperti 10 karakter pesan yang disisipkan seharusnya akan memakan memori sebanyak 10 *bytes*, tetapi karena karakter pesan diubah ke dalam bentuk desimal, maka memori yang dibutuhkan menjadi total piksel jumlah karakter pesan yang ditambah dengan karakter kunci. Setelah pesan disisipkan di akhir file, piksel yang sudah disisipkan akan dikompres ulang dengan palet warna yang baru untuk menghasilkan file video yang baru yang disebut file *stego video*.

Kemudian dilakukan pengujian dengan beberapa aplikasi pembuka video bertujuan untuk melihat apakah file *stego video* masih bisa dibuka. Hasil pengujian ditunjukkan pada tabel 2. Di sini pengujian yang dilakukan terhadap berbagai aplikasi untuk membuka *stego video*. Hasilnya *stego video* tetap dapat dibuka atau masih bisa dibaca oleh berbagai aplikasi. Tidak ada perbedaan dengan file video asli, sehingga tidak diketahui ada pesan rahasia pada file video tersebut. Ini menunjukkan kriteria *imperceptibility* terpenuhi, bahwa pesan yang disisipkan tidak dikenali.

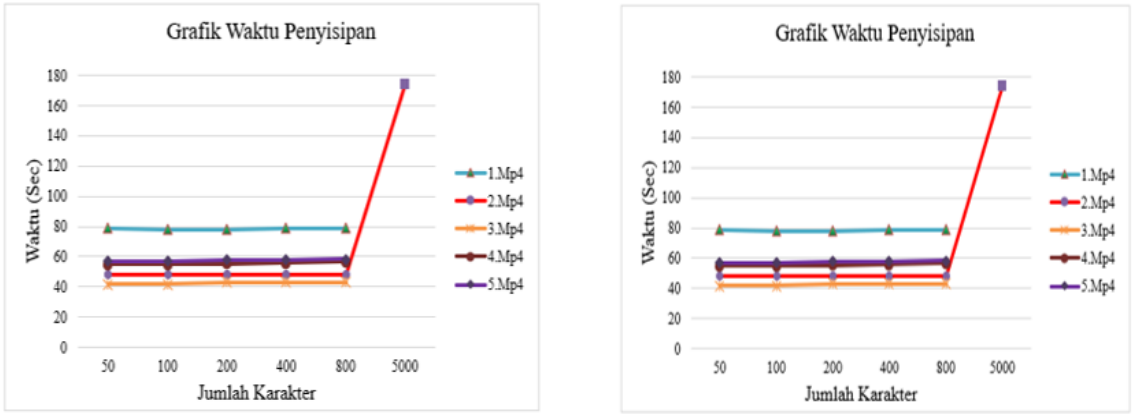
Jurnal Minfo Polgan
Volume 12, Nomor 2, Juni 2023 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v12i2.12418 p-ISSN : 2089-9424

Tabel 2. Pengujian File Stego Video Dengan 5 Aplikasi

No	Aplikasi	Pengujian Stego Video (pesan 50 karakter)				
		1.Mp4	2.Mp4	3.Mp4	4.Mp4	5.Mp4
1	Windows Media Player	Terbuka	Terbuka	Terbuka	Terbuka	Terbuka
2	GOM Player	Terbuka	Terbuka	Terbuka	Terbuka	Terbuka
3	Media Player Classic	Terbuka	Terbuka	Terbuka	Terbuka	Terbuka
4	Winamp	Terbuka	Terbuka	Terbuka	Terbuka	Terbuka
5	KMP Player	Terbuka	Terbuka	Terbuka	Terbuka	Terbuka

Waktu Penyisipan dan Ekstraksi Pesan

Pengujian waktu penyisipan dilakukan dengan menghitung lama proses aplikasi dalam menyisipkan pesan. Perhitungan dimulai saat video diubah ke bentuk *binary* sampai file video dikembalikan ke bentuk video. Pengujian waktu ekstraksi dilakukan dengan menghitung lama proses aplikasi dalam melakukan ekstraksi pesan. Perhitungan dimulai saat *stego video* diubah ke bentuk *binary* sampai pesan dapat dikeluarkan. Grafik waktu yang dibutuhkan untuk menyisipkan pesan dan mengekstrak pesan ditunjukkan pada gambar 8. Di sini terlihat bahwa ukuran video dan jumlah karakter pesan sangat mempengaruhi waktu penyisipan dan ekstraksi pesan, walaupun dalam hal ini perubahan waktu tidak terlalu jauh. Semakin besar ukuran video dan jumlah karakter pesan yang panjang, maka semakin lama waktu yang dibutuhkan dalam menyisipkan dan mengekstrak pesan.



(a) (b)

Gambar 8. (a) Grafik Waktu Penyisipan Pesan ; (b) Grafik Waktu Ekstraksi Pesan

Fidelity Stego Video

Pengujian *fidelity stego video* untuk melihat perubahan yang terjadi pada *frame rate* dan *bit rate* pada *stego video*. Di sini digunakan video 1.Mp4 yang asli dan juga yang sudah disisipkan pesan. Tabel 3 menunjukkan bahwa *frame rate* dan *bit rate* tidak mengalami perubahan dari video yang asli. Hal ini disebabkan oleh algoritma EOF melakukan penyisipan di akhir file sehingga tidak merusak kualitas atau komponen dari video tersebut. Ini memenuhi kriteria algoritma steganografi yang baik, bahwa media penampung dalam hal ini video tidak mengalami perubahan setelah dilakukan penyisipan pesan.

Jurnal Minfo Polgan
Volume 12, Nomor 2, Juni 2023 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v12i2.12418 p-ISSN : 2089-9424

Tabel 3. Pengujian *Fidelity Stego Video*

Pesan (Char)	*Stego Video*	*Frame Rate*	*Bit Rate*
Tanpa Pesan	1.Mp4 (asli)	24,00 fps	125kbps
50	1.Mp4	24,00 fps	125kbps
100	1.Mp4	24,00 fps	125kbps
200	1.Mp4	24,00 fps	125kbps
400	1.Mp4	24,00 fps	125kbps
800	1.Mp4	24,00 fps	125kbps

Robustness

Pengujian *robustness* yaitu pengujian terhadap manipulasi yang dilakukan pada *stego video*. Pengujian dilakukan pada video "1.Mp4" yang telah disisipkan pesan 50, 100, 200, 400 dan 800 karakter. Pengujian *Robustness* dilakukan dengan dua cara yaitu memotong (*cutting*) durasi video dan memperlambat video *(slow motion).*

Tabel 4. Penguiian *Robustness*

No	Pesan (Char)	Pengujian *Robustness*	
		Cutting	*Slow Motion*
1	50	Pesan tidak bisa di-*recovery*	Pesan tidak bisa di-*recovery*
2	100	Pesan tidak bisa di-*recovery*	Pesan tidak bisa di-*recovery*
3	200	Pesan tidak bisa di-*recovery*	Pesan tidak bisa di-*recovery*
4	400	Pesan tidak bisa di-*recovery*	Pesan tidak bisa di-*recovery*
5	800	Pesan tidak bisa di-*recovery*	Pesan tidak bisa di-*recovery*

Tabel 4 menunjukkan bahwa pesan tidak dapat di-*recovery* setelah dilakukan manipulasi pada file *stego video*. Ini disebabkan karena adanya perubahan pada komponen video dan pesan juga mengalami perubahan, sehingga pesan tidak dapat dikenali. Hal ini menunjukkan bahwa steganografi dengan algoritma EoF tidak tahan terhadap manipulasi.

Berdasarkan penjelasan di atas menunjukkan bahwa steganografi dengan algoritma EoF dan algoritma *Vigenere Cipher* pada media video memberikan keamanan ganda terhadap pesan atau informasi yang bersifat rahasia. Di mana pesan atau informasi dienkripsi terlebih dahulu. Pesan yang telah terenkrip disisipkan ke dalam file video dengan metode EoF pada akhir file video, sehingga pesan tidak dikenali dan tidak dapat dibaca oleh orang yang tidak berhak. Dari hasil pengujian dapat dilihat bahwa pesan yang terenkrip dapat dibaca kembali dengan baik tanpa merusak file video.

KESIMPULAN

Algoritma *Vigenere Cipher* dan *End of File* telah diimplementasikan pada steganografi video yang digunakan untuk menyisip dan mengekstrak pesan rahasia. Hasil pengujian menunjukkan bahwa jumlah karakter pesan yang disisipkan menyebabkan perubahan ukuran file *stego video*, sehingga mempengaruhi waktu proses ketika penyisipan dan ekstraksi. Pengujian dilakukan berdasarkan kriteria steganografi, yaitu *imperceptibility*, *fidelity*, *robustness*, dan *recovery*. Hasil pengujian *imperceptibility* terpenuhi karena pesan rahasia pada stego video tidak diketahui oleh orang lain. *Fidelity*, *stego video* tidak mengalami perubahan setelah disisipkan pesan. Ini menandakan bahwa pengujian *fidelity*-nya sangat baik.. Tetapi pada pengujian manipulasi file *stego video* dengan memotong dan memperlambat file *stego video*, pesan rahasia tidak bisa di*recovery*. Di sini terlihat bahwa dua kriteria steganografi terpenuhi, dan pesan terenkrip dapat dibaca kembali dengan baik tanpa merusak file video. Dengan demikian steganografi dengan algoritma EoF dan algoritma *Vigenere Cipher* pada media video memberikan keamanan ganda terhadap pesan atau informasi yang bersifat rahasia.

Jurnal Minfo Polgan
Volume 12, Nomor 2, Juni 2023 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v12i2.12418 p-ISSN : 2089-9424

REFERENSI

Basim, Z., & Painem, P. (2020). Implementasi Kriptografi Algoritma RC4 Dan 3DES dan Steganografi Dengan Algoritma EOF Untuk Keamanan Data Berbasis Desktop Pada SMK As-Su'udiyyah. *Skanika*, *3*(4), 54–60.

Faris, F. A. E. F., Febi, F. Y., Iwan, I. I., & Pizaini, P. (2023). Kombinasi algoritma kriptografi vigenere cipher dengan metode zig-zag dalam pengamanan pesan teks. *Jurnal CoSciTech (Computer Science and Information Technology)*, *4*(1), 182–192.

Hutasoit, S. (2019). Implementasi Penyembunyian Pesan Teks pada Citra Gif dengan menggunakan Metode End Of File. *Jurnal Teknik Informatika UNIKA Santo Thomas*, *4*(2), 117–124.

Liu, Y., Liu, S., Wang, Y., Zhao, H., & Liu, S. (2019). Video steganography: A review. *Neurocomputing*, *335*, 238–250.

Minarni, M., & Redha, R. (2020). IMPLEMENTASI LEAST SIGNIFICANT BIT (LSB) DAN ALGORITMA VIGENERE CIPHER PADA AUDIO STEGANOGRAFI. *Jurnal Sains Dan Teknologi: Jurnal Keilmuan Dan Aplikasi Teknologi Industri*, *20*(2), 168–174.

Munir, R. (2004). Pengolahan citra digital dengan pendekatan algoritmik. *Informatika, Bandung*, *260*.

Munir, R. (2006). Kriptografi. *Informatika, Bandung*.

Permana, A. A. (2018). Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android. *Jurnal Al-Azhar Indonesia Seri Sains Dan Teknologi*, *4*(3), 110–115.

Prahmana, I. G. (2022). IMPLEMENTASI ALGORITMA OTP DAN STEGANOGRAFI EOF DALAM PENYISIPAN PESAN TEKS PADA CITRA. *JTIK (Jurnal Teknik Informatika Kaputama)*, *6*(2), 457–465.

Qowi, Z., & Hudallah, N. (2021). Combining caesar cipher and hill cipher in the generating encryption key on the vigenere cipher algorithm. *Journal of Physics: Conference Series*, *1918*(4), 42009.

Riadi, I., Sunardi, S., & Aryanto, D. (2021). Algoritma End of File dan Rijndael pada Steganografi Video. *JRST (Jurnal Riset Sains Dan Teknologi)*, *5*(1), 17–22.

Rosa, A. S. (2016). *Rekayasa perangkat lunak terstruktur dan berorientasi objek*.

Ryan, A. R., Perdana, A., & Budiman, A. (2020). Kombinasi Algoritma Beaufort Cipher Dan Vigenere Cipher Untuk Pengamanan Pesan Teks Berbasis Mobile Application. *Jurnal Minfo Polgan*, *9*(2), 12–17.

Taha, M. S., Rahim, M. S. M., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M. (2019). Combination of steganography and cryptography: A short survey. *IOP Conference Series: Materials Science and Engineering*, *518*(5), 52003.

Wastupranata, L. M. (2022). *Penyisipan Jalur Penerbangan UAV Rahasia Dalam Media Digital Dengan Steganografi Kunci Publik Elgamal*.

Zulfikar, D. H. (2020). Quality Factor terhadap Kapasitas Pesan Rahasia pada Steganografi Citra JPEG dan Kualitas Citra Stego. *JUSIFO (Jurnal Sistem Informasi)*, *6*(2), 89–100.