IMPLEMENTASI ALGORITMA *STEGANOGRAFI FIRST OF FILE* DAN *END OF FILE* UNTUK PENYISIPAN TEXT DALAM GAMBAR

Shabila Fitri Aulia[1], Siti Sa'uda[2]

Fakultas Ilmu Komputer, Universitas Bina Darma
Email: shabilafa@gmail.com**[1],** siti_sauda@binadarma.ac.id[2]

ABSTRAK

Kemajuan teknologi sudah sangat berkembang dengan pesat pada era sekarang. Kemajuan teknologi ini juga seiring dengan berkembangnya cara berkomunikasi baik secara lisan maupun tulisan. Dalam hal tulisan, menjaga aspek keamanan dan kerahasiaan data sangatlah penting. Banyak teknologi yang bisa dipakai untuk mengamankan data seperti kriptografi dan steganografi. Penelitian ini akan menggunakan Algoritma Steganografi First Of File dan End Of File untuk mengamankan data. Steganografi merupakan ilmu menyembunyikan pesan atau data ke dalam media. Metode First Of File dan End Of File merupakan salah satu dari banyaknya metode yang biasa digunakan pada Algoritma Steganografi.Umumnya,metodeFirst Of File dan End Of File tidak jauh berbeda. Metode First Of File akan menyisipkan pesan diawal file sedangkan End Of File akan menyisipkan pesan di akhir file. Teknologi ini juga dapat diaplikasikan kembali untuk tahun-tahun kedepannya. Penelitian ini menghasilkan gambaran setalah *studi review* penerapan algoritma steganografi FOF dan EOF , kecepatan steganografi dan juga perbedaan gambar setelah di steganografi dalam hal ukuran dan pixel gambar.

Kata Kunci: Teknologi, Steganografi, *First Of File* dan *End Of File*

ABSTRACT

Technological advances have developed rapidly nowadays. These technological advances are also in line with the development of ways of communicating both orally and in writing. In terms of writing, maintaining aspects of data security and confidentiality is very important. Many technologies can be used to secure data such as cryptography and steganography. This research will use the First of File and End of File Steganography Algorithms to secure data. Steganography is the science of hiding messages or data in the media. The First of File and End of File methods are one of the many methods commonly used in the Steganography Algorithm. Generally, the First Of File and End Of File methods are not much different. The First Of File method inserts a message at the beginning of the file, while End Of File inserts a message at the end of the file. This technology can also be applied again for the years to come. This research produces an overview after a review study of the application of the FOF and EOF steganographic algorithms, the speed of steganography and the differences in the image after steganography in terms of image size and pixel.

Keywords: *Technology, Steganography, First Of File and End Of File*

1. PENDAHULUAN

Dunia saat ini mengalami kemajuan peradaban dengan sangat cepat. Segala aspek kehidupan bertambah maju dengan teknologi yang selalu berkembang setiap waktu. Kemajuan teknologi yang berkembang dengan pesat menambah kemudahan dalam masyarakat. Salah satu hal yang paling berpengaruh saat ini adalah dengan adanya jaringan global seperti internet yang sekarang membuat komunikasi bisa diakses tanpa batas oleh siapapun, kapanpun dan dimanapun . Hal ini membuat kita harus meningkatkan keamanan dalam berkomunikasi untuk meminimalisir penyalahgunaan informasi ketika berkomunikasi. Pertukaran data atau informasi dalam bentuk text juga salah satu bentuk komunikasi melalui tulisan. Banyak sekali aplikasi yang bisa menunjang komunikasi dalam bentuk tulisan seperti whatsapp, e-mail, dan sebagainya. Namun, kebanyakan dari aplikasi tersebut masih memiliki tingkat keamanan yang menjamin kerahasiaan data yang rendah bila digunakan untuk bertukar data atau informasi. Pengamanan data atau informasi ini diperlukan guna meminimalisir terjadinya tindak kejahatan agar data atau informasi tidak mudah diakses atau disalahgunakan oleh sembarangan orang.Pengamanan data atau informasi biasa dilakukan dengan menggunakan teknik kriptografi.

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan atau data [1]. Selain dari kriptogragi, teknik pengamanan data atau informasi juga bisa menggunakan teknik steganografi. Steganografi adalah ilmu atau seni yang pesan rahasianya disembunyikan didalam suatu pesan lain yang menjadi cover sehingga tidak bisa mendeteksi keberadaan pesan rahasia tersebut [1]. Kelebihan steganografi dibanding kriptografi adalah pesan-pesannya tidak menarik perhatian orang lain sehingga dapat meminimalisir tingkat kecurigaan orang yang melihatnya. Pesan-pesan berkode yang terdapat dalam kriptografi walau sulit dipecahkan akan tetapi bisa membuat orang yang melihatnya menaruh rasa curiga yang bisa membahayakan keamanan informasi. Banyak metode atau teknik yang bisa dipakai dalam algortima steganografi seperti LSB (*Least Significant Bit Insertion*), First Of File dan End Of File.

Penelitian ini hanya berfokus pada penerapan algoritma steganografi *first of file* dan *end of fie* sebagai *studi review* sehingga menghasilkan perangkat sebuah perangkat lunak yang dapat melakukan proses penyisipan text dalam gambar dengan algoritma steganografi *first of file* dan *end of file*.

2. METODOLOGI PENELITIAN

Metode yang digunakan dalam penelitian ini adalah metode deskriptif. Metode ini mengumpulkan dan menyajikan data untuk mengemukakan suatu masalah pada objek penelitian. Tujuannya adalah untuk menarik kesimpulan dari pembahasan yang telah dilakukan [2].

2.1 Metode Pengumpulan Data

1) **Studi Literatur**
   Penulis mencari bahan yang mendukung dalam pendefinisian masalah konsep-konsep dasar yang melandasi landasan teori penulis dalam melakukan penulisan penelitian ini melalui buku-buku, internet dan lain sebagainya yang erat kaitannya dengan objek permasalahan.
2) **Pengumpulan dan Analisis Data**
   Penulis pada tahap ini melakukan pengumpulan dan analisa data yang berhubungan dengan algoritma steganografi first of file dan end of file.

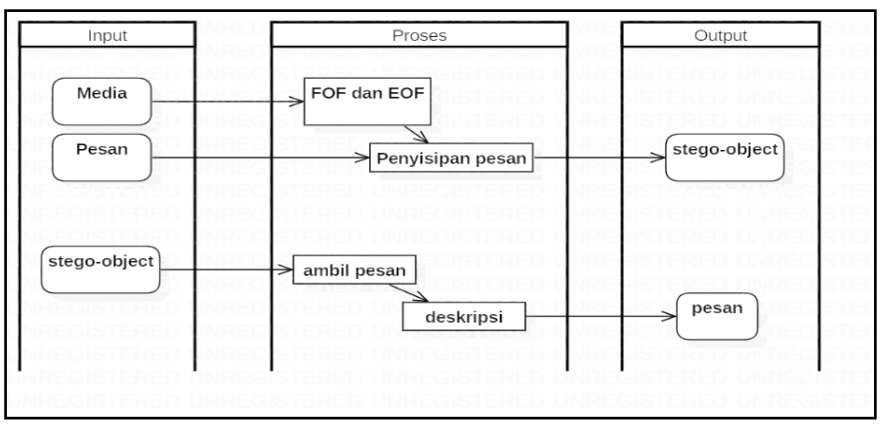
2.2 Metode PengembanganAplikasi

Penelitian ini akan menggunakan metode RUP untuk pengembangan sistem. Tahapan-tahapan dalam metode RUP ini dirasa cocok dalam pembangunan sistem. Adapun tahapan-tahapannya adalah sebagai berikut [3]:

1. *Inception* (Permulaan)
2. *Elaboration* (Perluasan/perencanaan)
3. *Construction* (Konstruksi)
4. *Transition* (Transisi)

2.3 Deskripsi Umum Sistem

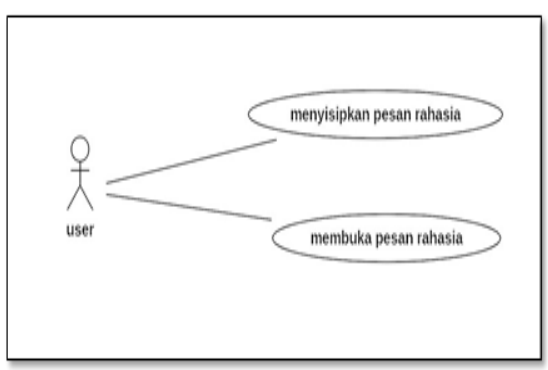
Secara umum, merahasiakan pesan dan mengambil kembali pesan yang telah disembunyikan adalah proses yang ada pada aplikasi steganografi. Hal ini juga ada pada rancang bangun perangkat lunak steganografi penyisipan text ke dalam gambar dengan metode first of file dan end of file yang dibahas dalam tugas akhir ini. Kebutuhan utama pada rancang bangun perangkat lunak ini adalah kebutuhan akan data-data inputan. Media penyisipan dalam sistem ini adalah gambar dengan format jpeg, dan jpg sedangkan teks sebagai bentuk pesan yang akan disisipkan. Untuk lebih jelasnya dapat dilihat pada gambar berikut:



Gambar 1. Deskripsi Umum Sistem

2.4 *Use Case* Diagram

Berdasarkan gambaran umum yang telah didefinisikan, dapat digambarkan sebagai berikut:



Gambar 2. Use Case Diagram

Tabel 1. Penjelasan *Use Case*

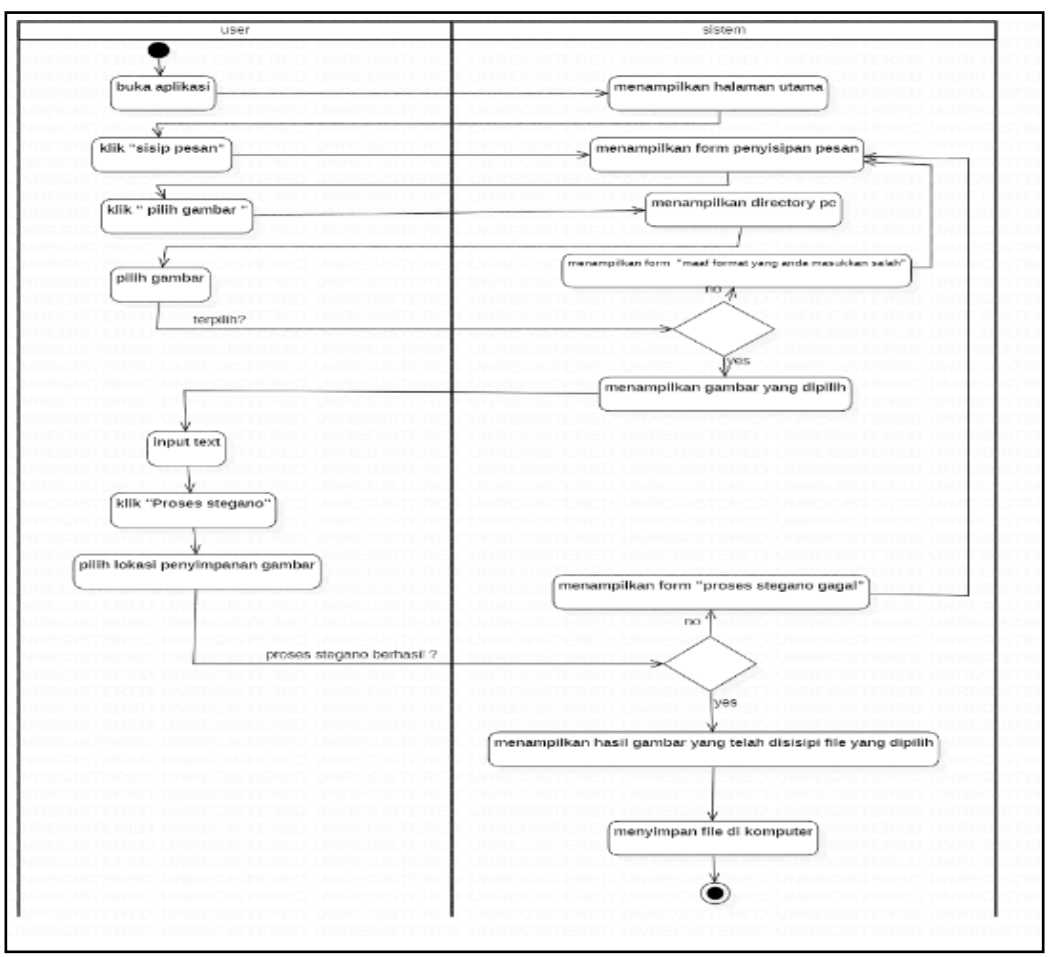
No	Use Case	Penjelasan
1	Menyisipkan pesan rahasia	Untuk menyisipkan pesan dalam bentuk text ke dalam gambar
2	Membuka pesan rahasia	Untuk melihat pesan text yang telah disisipkan dalam gambar

2.5 Activity Diagram

Berikut adalah rancangan *activity diagram* dari perangkat lunak yang dibuat:

a. *Activity Diagram* Sisip Pesan

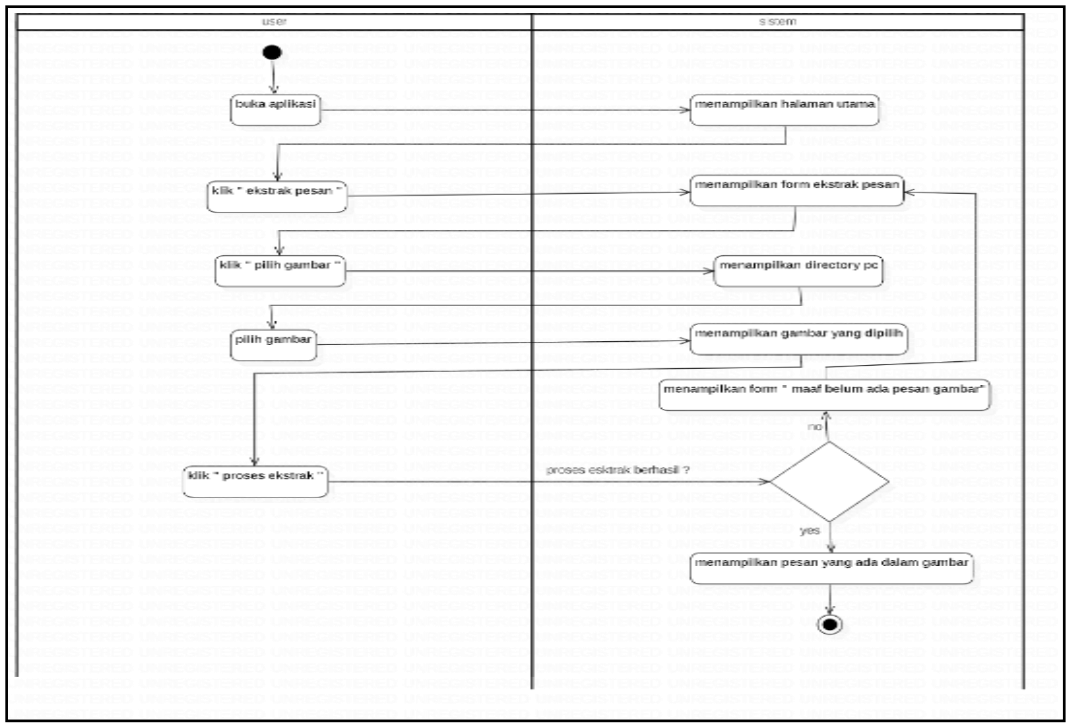
Diagram ini akan menjelaskan aktivitas apa saja yang ada pada menu sisip pesan untuk menyisipkan pesan rahasia ke dalam gambar. Berikut activity diagram pada menu sisip pesan:



Gambar 3. *Activty Diagram* Sisip Pesan

b. *Activity Diagram* Ekstrak Pesan

Diagram ini akan menjelaskan aktivitas apa saja yang muncul pada menu ekstrak pesan untuk melihat pesan rahasia atau teks yang telah disisipkan dalam gambar. Berikut adalah activity diagram pada menu ekstrak pesan :



Gambar 4. *Activity Diagram* Ekstrak Pesan

2.6 Algoritma Steganografi

Steganografi adalah ilmu atau seni yang pesan rahasianya disembunyikan didalam suatu pesan lain yang menjadi cover sehingga tidak bisa mendeteksi keberadaan pesan rahasia tersebut [1]. Terdapat beberapa istilah yang berkaitan dengan steganografi yaitu [4]:

1) Hiddentext atau embedded message merupakan informasi atau pesan yang disembunyikan.
2) Covertext atau cover-object merupakan media penampung pesan.
3) Stegotext atau stego-object merupakan media yang sudah disisipkanpesan.
4) Stegokey merupakan kunci untuk menyisipkan pesan atau membaca pesan

2.7 Algoritma *First of File*

First of File adalah salah satu teknik atau metode yang pesannya disembunyikan atau disisipkan pada awal file. Secara umum, penggunaan metode FOF menggunakan tanda khusus yang disebut flag dalam proses penyisipan pesan teks dan file dokumen ke dalam citra digital [5]. Berikut adalah contoh gambar yang nilainya disisipi *chipper text* dengan menggunakan metode steganografi *First of File.* Nilai chipertext ditandai dengan angka berwarna merah.

R=48 G=91 B=125	R=49 G=90 B=120	R=67 G=103 B=129	R=77 G=108 B=129	R=92 G=119 B=136	R=114 G=130 B=143
R=52 G=89 B=118	R=42 G=79 B=106	R=48 G=82 B=107	R=61 G=93 B=116	R=80 G=111 B=132	R=97 G=120 B=134

Gambar 5. Nilai RGB Citra Asli

R=83 G=69 B=77	R=73 G=78 B=65	R=82 G=32 B=80	R=82 G=79 B=80	R=79 G=83 B=65	R=76 G=32 B=85
R=48 G=91 B=125	R=49 G=90 B=120	R=67 G=103 B=129	R=77 G=108 B=129	R=92 G=119 B=136	R=114 G=130 B=143
R=52 G=89 B=118	R=42 G=79 B=106	R=48 G=82 B=107	R=61 G=93 B=116	R=80 G=111 B=132	R=97 G=120 B=134

Gambar 6. Nilai RGB citra yang Sudah Disisipi Pesan dengan Teknik *First of File*

2.8 Algoritma *End of File*

Teknik *End of File* memiliki fungsi yang hamper sama dengan metode *First of File*. Metode ini merupakan kebalikan dari FOF karena menambahkan pesan rahasia pada akhir file. Berikut adalah contoh gambar yangnilainyadisisipi chipper textdenganmenggunakanmetoe steganografi *end of file*. Nilai chipertext ditandai dengan angka berwarna merah.

R=58 G=86 B=107	R=49 G=77 B=98	R=46 G=78 B=101	R=50 G=86 B=110	R=54 G=98 B=125	R=75 G=111 B=133
R=69 G=65 B=32	R=60 G=87 B=106	R=62 G=91 B=109	R=56 G=87 B=107	R=52 G=89 B=108	R=73 G=102 B=116

Gambar 7. Nilai RGB Citra Asli

2.9 Implmentasi Algoritma *First Of File dan End Of File*

Algoritma *First of File* dan *End of File* merupakan algoritma sederhana yang dapat digunakan dalam pembangunan perangkat lunak ini. Teknik first of file dilakukan dengan car a menyisipkan nilai ascii tiap karakter pada pixel atas gambar dan teknik end of file dilakukan dengan cara menyisipkan nilai ascii tiap karakter pada pixel gambar bawah.

R=58 G=86 B=107	R=49 G=77 B=98	R=46 G=78 B=101	R=50 G=86 B=110	R=54 G=98 B=125	R=75 G=111 B=133
R=69 G=65 B=32	R=60 G=87 B=106	R=62 G=91 B=109	R=56 G=87 B=107	R=52 G=89 B=108	R=73 G=102 B=116
R=78 G=73 B=86	R=52 G=82 B=83	R=73 G=84 B=65	R=83 G=32 B=66	R=73 G=78 B=65	R=86 G=82 B=77

Gambar 8. Nilai RGB Citra yang Sudah Disisipi Pesan dengan Teknik *End of File*

Langkah – langkah proses penyisipan pesan rahasia ke dalam citra digital ialah sebagai berikut [6]:

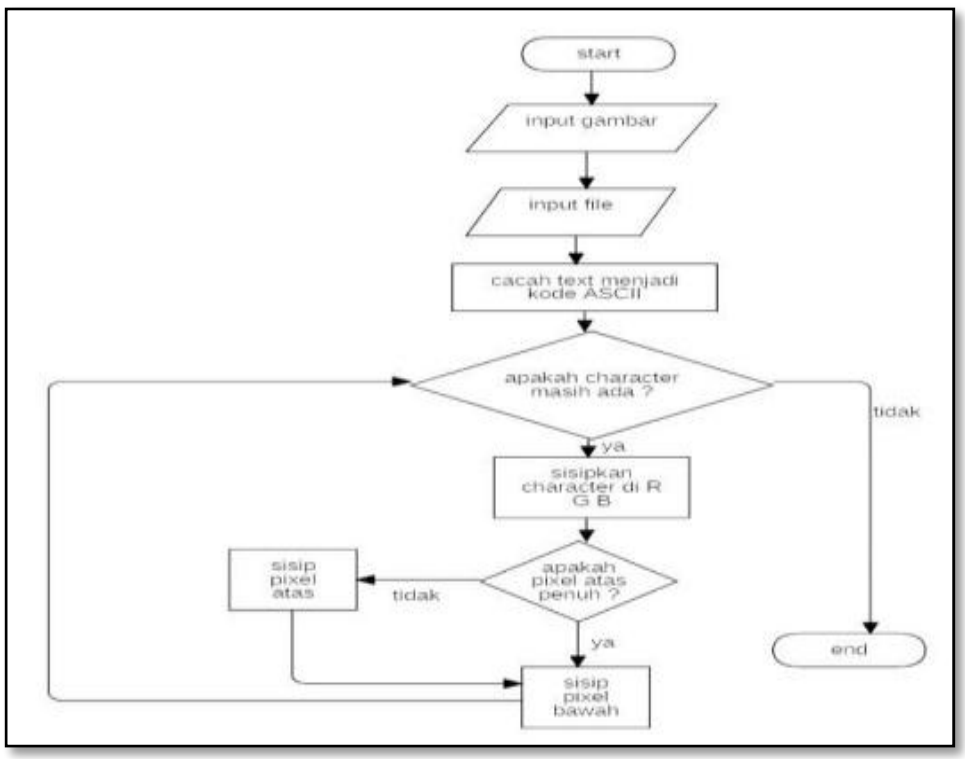
1) Masukan media penampung berupa citra digital bereksistensi jpeg,jpg
2) Masukan pesan rahasia berupa file dokumen bereksistensi doc, docx atau txt.
3) Melakukan proses stegano dengan metode FOF dan EOF
4) Simpan citra digital yang telah disisipi pesan rahasia.

Pemanggilan pesan rahasia yang ada pada citra digital dilakukan dengan cara mengekstraksi data tersebut. Langkah-langkah untuk melakukan proses ektraksi data ialah sebagai berikut:

1) Masukkan gambar yang sudah disisipkan pesan rahasia
2) Lakukan proses ektraksi data.

2.10 Proses Penyisipan Pesan

Proses ini akan menjelaskan bagaimana sistem akan memasukkan tiap karakter pesan pada gambar dengan menggunakan metode yang digunakan. Penyembunyian pesan rahasia pada gambar (embedding) dapat dipengaruhi oleh beberapa aspek [7]. Proses penyisipan pesan ini akan digambarkan lebih jelas dengan menggunakan *flowchart* pberikut.



Gambar 9. *Flowchart* Penyisipan Pesan

Berdasarkan flowchart penyisipan pesan pada gambar 8 dapat dijelaskan bahwa:

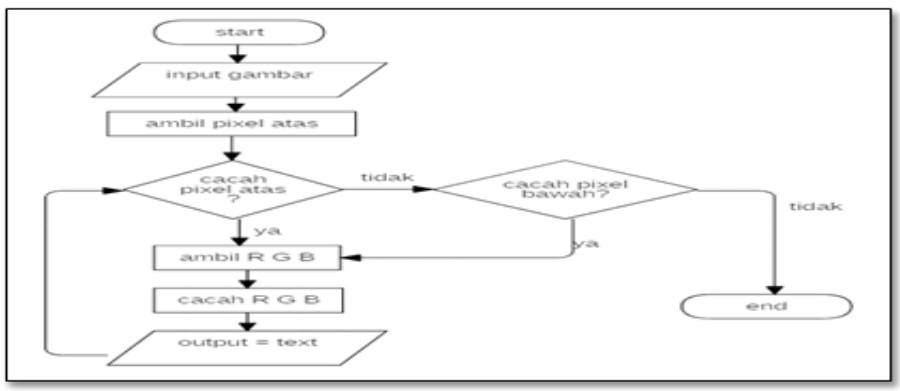
1) Penyisipan pesan rahasia dimulai dari menginputkan text atau pesan rahasia yang akan disembunyikan dan media gambar berformat jpeg atau jpg ke dalam sistem.
2) Selanjutnya, perangkat lunak akan membaca text dan mengubah text tersebut menjadi kode ascii. Setelah text dicacah menjadi kode ascii maka nilai tiap karakterakan disisipkan satu persatu kedalam nilai RGB pada tiap pixel. Pixel atas akan disisipi nilai terlebih dahulu. Jika

nilai pixel atas penuh maka akan menyisipkan nilai ke pixel bawah hingga nilai tiap karakternyahabis.

3) Hasil yang didapat dari proses ini adalah berupa stego- object (file baru yang telah disisipi pesan)

2.11 Proses Ekstrak Pesan

Proses ini akan menjelaskan bagaimana sistem mengambil nilai karakter pada gambar sehingga dapat melihat nilai pesan yang telah disisipkan pada gambar.



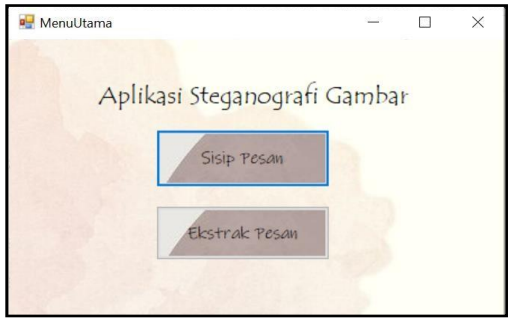
Gambar 10. *Flowchart* Ekstrak Pesan

3. HASIL DAN PEMBAHASAN

Hasil penelitian ini berupa rancangan perangkat lunak steganografi dan perbandingan antara perbedaan size, pixel dan waktu dalam melakukan proses penyisipan dan ekstrak pesan. Rancangan sistem di desain menggunakan UML. UML adalah sebuah teknik pengembangan sistem yang proses pendokumentasian dan spesifikasi sistemnya menggunakan bahasa grafis sebagai alat [8].

3.1 Tampilan Menu Utama

Pada menu ini, user dapat menggunakan 2 pilihan menu utama pada sistem yaitu menu sisip pesan apabila user akan menyisipkan teks pada gambar dan menu ekstrak pesan apabila user akan melihat isi pesan text dalam gambar.



Gambar 11. Tampilan Menu Utama

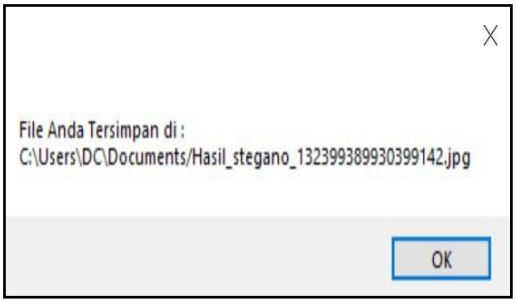
3.2 Tampilan Menu Sisip

Pada menu sisip, user dapat menginput pesan text yang akan disisipkan dan gambar sebagai media penampungnya. User akan memilih file gambar terlebih dahulu. Kemudian, user akan menginput pesan text yang akan disisipkan. Saat user selesai menginput gambar dan pesan yang akan disisipkan, user akan mengklik tombol proses stegano untuk memulai proses penyisipan teks dalam gambar. Sebelum proses berjalan, user akan diminta untuk memilih lokasi penyimpanan file gambar hasil stegano terlebih dahulu. Apabila telah selesai, maka file gambar yang telah distegano akan otomatis tersimpan di lokasi penyimpanan yang telah dipilih.

Gambar 12. Tampilan Menu Sisip

3.3 Tampilan Notifikasi Proses Penyisipan Berhasil

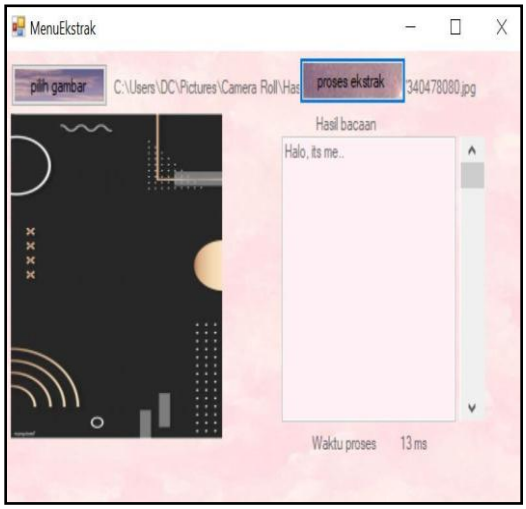
Berikut adalah tampilan notifikasi yang akan muncul saat sistem berhasil melakukan proses steganografi.



Gambar 13. Tampilan Notifikasi Proses Penyisipan Berhasil

3.4 Tampilan Menu Ekstrak

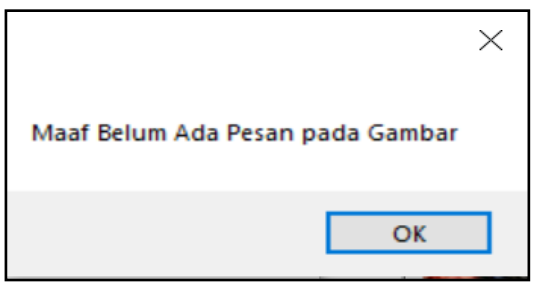
Pada menu ekstrak, user akan menginput gambar yang telah distegano untuk melihat isi pesan teks yang ada pada gambar. Saat gambar telah dipilih maka user akan mengklik tombol proses stegano untuk melihat isi pesan teks yang ada pada gambar.



Gambar 14. Tampilan Menu Ekstrak

3.5 Tampilan Notifikasi Gambar yang Tidak Memiliki Pesan

Pada saat user akan melakukan proses ekstrak, apabila user menginput gambar yang belum pernah distegano maka akan muncul notifikasi seperti berikut



Gambar 15. Tampilan Notifikasi Gambar yang Tidak Memiliki Pesan

3.6 Hasil Perbandingan Gambar Sebelum dan Sesudah di Steganorafi

Pengujian ini dilakukan untuk mengetahui lama proses stegano, perbedaan ukuran size, dan pixel gambar dengan menggunakan jumlah panjang karakter 160, format gambar yang sama dan spesifikasi leptop sebagai berikut:

1) Machine name: DESKTOP-8I7O6O5
2) Machine Id: {468D49A1-BF67-4976-A7B6-25AF1091A527}
3) Operating System: Windows 10 Pro 64-bit (10.0, Build 17134) (17134.rs4_release.180410-1804)
4) Language: English (Regional Setting: English)
5) System Manufacturer: Micro-Star International Co., Ltd.
6) System Model: GF63 8RC
7) BIOS: E16R1IMS.10B (type: UEFI)
8) Processor: Intel(R) Core(TM) i5-8300H CPU @ 2.30GHz (8 CPUs), ~2.3GHz
9) Memory: 8192MB RAM
10) Available OS Memory: 8038MB RAM
11) Page File: 4300MB used, 5082MB available

12) Windows Dir: C:\Windows
13) DirectX Version: DirectX 12
14) DX Setup Parameters: Not found
15) User DPI Setting: 120 DPI (125 percent)
16) System DPI Setting: 120 DPI (125 percent)
17) DWM DPI Scaling: UnKnown
18) Miracast: Available, with HDCP
19) Microsoft Graphics Hybrid: Supported

Tabel 2. Hasil Perbandingan

NO	Komponen Pengujian	Hasil Pengujian	Keterangan
1	Menu Utama	Halaman utama berhasil ditampilkan	Benar
2	Button 1 pada menu utama	Aplikasi berhasil menuju menu sisip	Benar
3	Button 2 pada menu utama	Aplikasi berhasil menuju menu ekstrak	Benar
4	Button 1 pada menu sisip	Menampilkan list directory pada pc	Benar
5	Button2 pada menu sisip	Menampilkan hasil dari steganografi gambar	Benar
6	Button 1 pada menu ekstrak	Menampilkan list gambar pada directory pc	Benar
7	Button 2 pada menu ekstrak	Menampilkan hasil pesan dari gambar	Benar

3.7 Hasil Pengujian *Blackbox* untuk Button

Cover Image	Stego Image	Ukuran Size		Lama Proses	
		Awal	Akhir	Sisip	Ekstrak
 Resolusi Pixel 474x758	 Resolusi Pixel 474x762	21.8 kb	274 kb	1645 ms	38 ms
 Resolusi Pixel 564x1003	 Resolusi Pixel 564x1003	77.2 kb	506 kb	2642 ms	18 ms
 Resolusi Pixel 564X1128	 Resolusi Pixel 564x1132	62.3 kb	734 kb	3198 ms	17 ms
 Resolusi Pixel 474x689	 Resolusi Pixel 474x673	28.2 kb	211 kb	2184 ms	111 ms

4. KESIMPULAN

Penelitian ini menghasilkan suatu perangkat lunak yang dapat menyisipkan pesan didalam gambar dengan format jpg dan jpeg. Hasil yang diperoleh berdasarkan pengujian *blackboxtesting* menunjukkan bahwa semua fungsi *button* perangkat lunak dengan penerapan algoritma *first of file* dan *end of file*sudah berfungsi dengan baik dan dapat digunakan oleh siapapun yang membutuhkan. Adapun permasalahan yang dihadapi saat ini adalah perangkat lunak ini masih berbasis desktop sehingga tidak semua orang dapat langsung menggunakan perangkat lunak ini secara langsung

dengan mudah. Kedepanny diharapkan agar perangkat lunak ini dapat berkembang menjadi bentuk website dan juga aandroid.

DAFTAR PUSTAKA

[1] Munir, Rinaldi. 2019. Kriptografi. 2nd ed. Bandung: Informatika Bandung.

[2] Muzakir, Ari. n.d. "IMPLEMENTASI TEKNIK STEGANOGRAFI DENGAN KRIPTOGRAFI KUNCI PRIVATE AES UNTUK KEAMANAN FILE GAMBAR BERBASIS ANDROID." 6.

[3] Rosa A.S, and M.Salahudin. 2018. Rekayasa Perangkat Lunak Terstruktur Dan Berorientasi Objek. Edisi Revisi. Bandung: Informatika.

[4] Gunawan, Indra. 2018. "Penggunaan Algoritma Kriptografi Steganografi Least Significant Bit Untuk Pengamanan Pesan Teks dan Data Video." J-SAKTI (Jurnal Sains Komputer dan Informatika) 2(1):57.

[5] Simanjuntak, Morigia. n.d. "PENGAMANAN FILE TEKS DENGAN ALGORITMA KRIPTOGRAFI KUNCI PUBLIK RABIN DAN ALGORITMA STEGANOGRAFI FIRST OF FILE DAN END OF FILE." 134.

[6] Sitorus, M. (2016). APLIKASI KEAMANAN DATA DENGAN TEKNIK STEGANOGRAFI MENGGUNAKAN METODE END OF FILE (EOF). https://doi.org/10.13140/RG.2.2.28364.00643

[7] Arfiyah. 2013. "Perbandingan Teknik Steganografi Dengan Metode First of File Dan End Of File Pada File Bitmap." Universitas Sumatera Utara.

[8] CA, Prof Dr Sri Mulyani, Ak. 2017. Analisis dan Perancangan Sistem Informasi Manajemen Keuangan Daerah: Notasi Pemodelan Unified Modeling Language (UML). Abdi Sistematika.