JURNAL FASILKOM: Jurnal teknologi inFormASi dan ILmu KOMputer **P-ISSN : 2089-3353**
Volume No. 11 no.3 | Desember 2021: 143-1349 **E-ISSN : 2808-9162**

Implementasi Steganografi Dengan Metode *End Of File* (EOF) Untuk Menyisipkan Pesan Teks Pada Gambar

Tri Handayani[1], Tri Yuliati[2], Siti Patimah[3]
[1]Informatika, Sekolah Tinggi Teknologi Dumai
[2]Informatika, Sekolah Tinggi Teknologi Dumai
[3]Informatika, Sekolah Tinggi Teknologi Dumai
[1]trihandayani.stt@gmail.com, [2]triyuliati00@gmail.com, [3]SitiPatimah87@gmail.com

Abstract

Confidentiality and security are important aspects needed in the process of exchanging messages or information through networks or the internet. In maintaining data security, this information is usually hidden. Various security techniques have been developed to protect the confidentiality of messages or information to avoid unauthorized third parties. This research resulted in an Implementation of Steganography with the End Of File Method for Inserting Text Messages in Images which is able to provide security protection for secret messages that are complicated to crack. Changes in the size of the stegoimage file to be larger than the size of the coverimage before the embedd and extract process, this is because the size of the inserted file and its information is added to the more hidden data information, the larger the resulting size will be. The test results show that in the fidelity testing process, there is no MSE result which only produces a value of "0" and PSNR produces a value of "∞" (infinite) inserting a message at the end of the file without changing the pixel color intensity value.

Keywords: End Of File, MSE, Steganografi, PSNR, Embedding

Abstrak

Kerahasiaan dan keamanan merupakan aspek penting yang dibutuhkan dalam proses pertukaran pesan atau informasi melalui jaringan atau internet. Dalam menjaga keamanan data informasi ini biasanya disembunyikan keberadaannya. Berbagai macam teknik keamanan telah dikembangkan untuk melindungi kerahasiaan pesan atau informasi agar terhindar dari pihak ketiga yang tidak memiliki hak. Penelitian ini menghasilkan suatu Implementasi Steganografi dengan Metode End Of File untuk Menyisipkan Pesan Teks Pada Gambar yang mampu memberikan proteksi keamanan pesan rahasia yang rumit untuk dipecahkan. Perubahan Ukuran pada file stegoimage menjadi lebih besar dari ukuran coverimage sebelum di proses embedd dan ekstrak, hal ini dikarenakan ukuran dari file yang disisipkan beserta informasinya semakin banyak ditambah informasi data yang disembunyikan maka akan semakin besar pula ukuran yang dihasilkan. Hasil pengujian menunjukkan bahwa pada proses pengujian tahap fidelity tidak nampak hasil MSE yang hanya menghasilkan nilai "0" dan PSNR menghasilkan nilai "∞" (tak hingga) menyisipkan pesan diakhir file tanpa merubah nilai intensitas warna pikselnya.

Kata kunci: *End Of File, MSE, Steganografi, PSNR, Embedding*

1. Pendahuluan

Penerapan teknologi di bidang pengamanan data dan informasi sudah banyak dilakukan. Ancaman terhadap keamanan informasi bisa terjadi ketika informasi yang dikirimkan tidak ditujukan kepada semua orang namun hanya kepada orang tertentu, terutama bila informasi yang diberikan bersifat rahasia. Saat ini sudah banyak terjadi kejahatan di dunia maya, dimana informasi rahasia bisa diambil seorang hacker tanpa diketahui. Hal ini menimbulkan kekhawatiran bagi pemilik informasi rahasia tersebut.

Dalam proses pertukaran pesan dan informasi dalam dunia maya, kerahasian dan keamanan data dan informasi menjadi hal penting. Oleh karena itu, informasi yang akan dikirim dapat di jaga melalui teknik penyembunyian data. Salah satu teknik menyembunyikan informasi yaitu steganografi. Steganografi adalah cara untuk menyembunyikan informasi yang bersifat rahasia dengan menggunakan media lain sebagai pembawa informasi ini [1]. selain itu Steganografi juga bisa dikatakan sebagai teknik cara untuk menyembunyikan data di dalam media digital sehingga data rahasia tersebut tidak diketahui oleh orang lain. Stegano membutuhkan dua bagian yaitu media penampung dan data yang disembunyikan [2,3]. Steganografi berasal dari kata Steganos yang memiliki arti menyembunyikan dan Graptos yang memiliki arti tulisan sehingga arti steganografi adalah tulisan yang disembunyikan. Steganografi merupakan cara komunikasi rahasia dengan menyembunyikan pada objek yang terlihat tidak berbahaya atau mencurigakan. Steganografi bekerja dengan menyisipkan pesan pada objek lain [4,5].

Penyisipan pesan pada steganografi bisa menggunakan metode *end of file (EOF)*, dimana metode ini merupakan salah satu teknik yang menyisipkan pesan pada akhir file. Pada teknik ini data yang disisipkan diakhir diberi tanda khusus sebagai pengenal mulai dan akhir dari data tersebut. Metode ini digunakan dalam menyisipkan data yang memiliki ukuran file yang sama dengan ukuran file sebelum disisipkan dan ditambah dengan ukuran data yang disisipkan kedalam file tersebut [5].

Proses penyisipan pesan menggunakan metode End of File dapat dijabarkan sebagai berikut [6-8] :

1. Inputkan pesan yang akan disisipkan
2. Ubah pesan menjadi kode-kode desimal
3. Inputkan citra grayscale yang akan disisipi pesan
4. Dapatkan nilai derajat keabuan masing-masing piksel
5. Tambahkan kode desimal pesan sebagai nilai derajat keabuan diakhir citra.
6. Petakan menjadi citra baru

Penelitian tentang steganografi sebelumnya dilakukan oleh Pandapotan (2016) dengan judul analisa perbandingan *least significant bit (LSB)* dan *end of file (EOF)* untuk *steganografi* citra digital menggunakan matlab. Tujuan penelitin ini adalah mengetahui perbandingan *size file* dan kualitas citra digital setelah dilakukan penyisipan pesan dengan metode LSB dan EOF. Hasil penelitian ini menyebutkan bahwa metode LSB lebih baik digunakan karena *size file* tidak mengalami perubahan dengan citra yang asli [9].

Kemudian tahun 2017, Darwis dan Kisworo melakukan penelitian dengan judul Teknik Steganografi untuk penyembunyian pesan teks menggunakan algoritma *End Of File,* dalam penelitian ini menggunakan citra digital berformat JPG, hasil dari penelitian ini akan menghasilkan *stego image* yang tidak berubah secara signifikan serta proses pengambilan pesan yang relative cepat sehingga menjadikan alternatif pengiriman pesan agar terhindar dari pencurian dan sabotase [10].

Menurut penelitian yang dilakukan (Darwis, 2015) untuk mengukur kualitas citra yang dihasilkan dapat menggunakan parameter PSNR (*peak signal to noise ratioi)*. PNSR merupakan ukuran perbandingan antara nilai piksel *cover image* dengan nilai piksel pada citra *stego* yang dihasilkan. Langkah pertama adalah menentukan nilai rata-rata kuadrat *absolute error* antara cover image dengan citra *stego image* yaitu nilai MSE (*mean square error)*. Berikut adalah rumus PSNR untuk *cover image* [11] :

$$MSE_{AVG} = \frac{MSE_R + MSE_G + MSE_B}{X.Y} \quad (1)$$

dimana :
PSNR = Nilai PSNR
MSE = Nilai Men Square Error

$$PSNR = 10_{log10}\left(\frac{255^2}{MSE}\right) \quad (2)$$

dimana :
PSNR = Nilai PSNR
MSE = Nilai Men Square Error

Jika nilai PSNR yang dimiliki oleh *stegano image* bernilai tinggi maka citra terebut bisa dikatan berkualitas baik. Ada perbedaan antara cover image dengan stegano image setelah dilakukan penyisipan pesan rahasia dimana semakin tinggi kualitas yang dihasilkan *stegano image* maka semakin rendah niilai dari MSE.

Jurnal selanjutnya diambil dari (Irawati, 2018) dengan judul perancangan aplikasi steganografi menggunakan algoritma IDEA dan metode EOF. Penelitian ini melakukan salah satu teknik untuk mengamankan data yaitu dengan menggunakan algoritma international data encryption algorithm yang dikombinasikan dengan metode end of file. Dari hasil uji coba diketahui bahwa jika IDEA digabungkan menggunakan metode EOF maka proses enkripsi, deskripsi, penyisipan dan ekstraksi pesan dapat dilakukan dengan baik. Hasil penyisipan dapat menyembunyikan *plain text* dengan perbandingan dari gambar sebelum dan sesudah disisipkan tidak mengalami perubahan yang mencolok [12].

Pada penelitian ini penulis melakukan teknik penyembunyian informasi yang bersifat rahasia di dalam informasi yang tidak bersifat rahasia dengan teknik steganografi.

2. Metode Penelitian

2.1 Pengumpulan Data

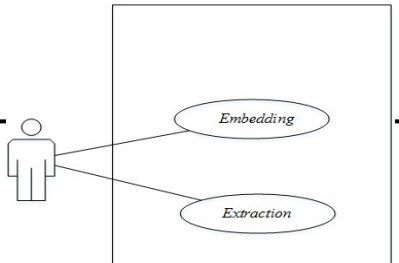
Metode penelitian ini menggunakan metode Studi pustaka yang dilakukan dengan mencari referensi serta mempelajari buku-buku dan *literatur* (situs *internet*) lainnya yang berhubungan dengan penelitian terutama yang berkaitan dengan implementasi steganografi pada citra digital. Sedangkan dalam observasi dilakukan dengan melakukan pengamatan langsung atau atau me1lihat kejadian yang terjadi. Citra yang digunakan dalam penelitian ini adalah citra digital berwarna dengan format png.

2.2 Alat dan Perancangan Sistem

Paga bagian ini akan dijelaskan mengenai alur sistem yang akan dibuat berupa proses yang akan terjadi dalam sistem dan dipresentasikan dengan diagram *UML (Unified Modelling Language)* diantarannya *Use Case Diagram, Activity Diagram, Sequence Diagram,*.

2.2.1 Use Case Diagram

Use Case Diagram merupakan suatu bentuk diagram yang menggambarkan aktor pengirim dan penerima akan menjalankan sistem dengan cara memilih terlebih dahulu sesuai kebutuhan, jika memilih *embedding* maka pengirim akan menginput *password, upload coverimage* dan *input* pesan rahasia. Sedangkan jika memilih *extraction* maka penerima akan menginput *password* dan *upload cover image* pada sistem tersebut.



Gambar 1. *Use Case Diagram*

Adapun keterangan dari gambar 1 dapat dilihat pada tabel 1 dan tabel 2:

Tabel 1. Definisi Aktor

No	Aktor	Deskripsi
1	Pengirim atau Penerima	Orang yang menggunakan sistem dan melakukan proses embedding dan *extraction* dengan menginputkan data pada sistem.

Tabel 2. Definisi Use Case

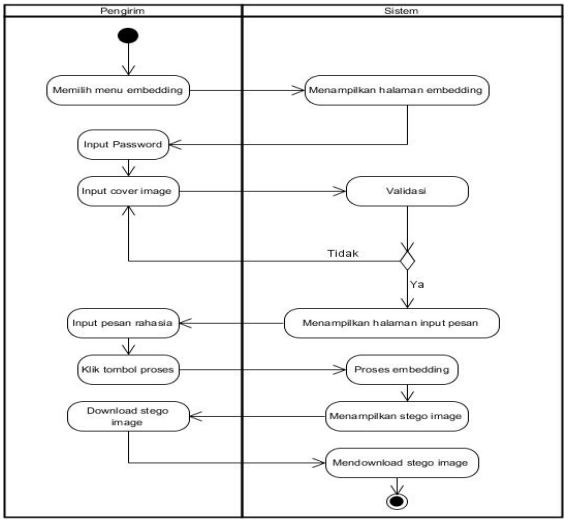
No	Aktor	Deskripsi
1.	*Embedding*	Proses penyisipan pesan rahasia dengan steganografi pada citra digital
2.	*Extraction*	Proses ekstraksi stegoimage untuk mengetahui pesan rahasia tersembunyi pada citra digital.

2.2.2. Activity Diagram

Activity Diagram merupakan suatu diagram yang dapat menampilkan secara detail urutan proses sistem.

1. *Activity Diagram Menu Embedding*

Adapun *activity diagram* pada *menu embedding* pada sistem sebagai berikut:

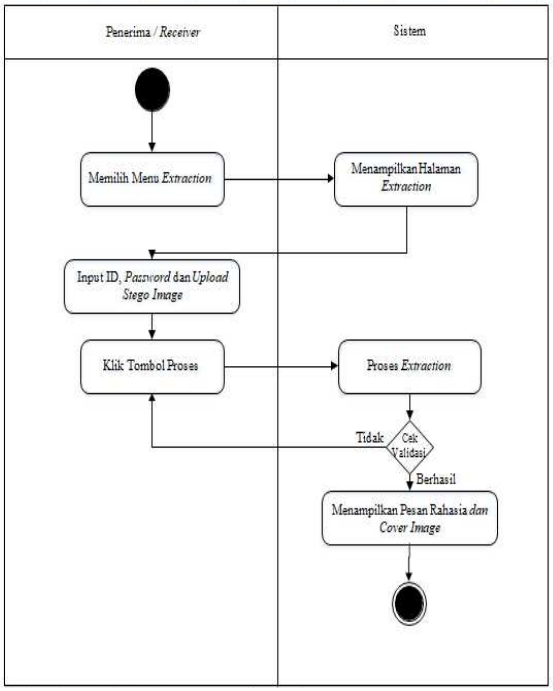


Gambar 2. Activity Diagram Menu *Embedding*

Pada gambar 2. *Activity Diagram* menu *embedding* adalah tahap penyisipan pesan rahasia pada citra digital oleh pengirim/*sender* ke dalam sistem dengan *input password, upload, cover image* dan *input* pesan rahasia maka sistem akan memeriksa jika ukuran *coverimage* melebihi batas yang telah ditetapkan maka tidak dapat memproses penyisipan pesan rahasia.

2. *Activity Diagram Menu Extraction*

Adapun *activity diagram* pada *menu extraction* pada sistem sebagai berikut:



Gambar 3. *Activity Diagram* Menu *Extraction*

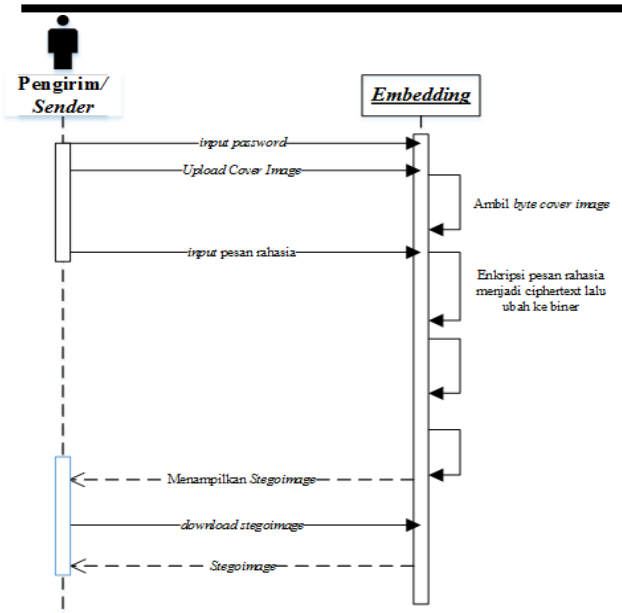
Pada gambar 3. *Activity Diagram* menu *extraction* adalah tahap ekstraksi penyisipan pesan rahasia pada *stegoimage* oleh penerima/*receiver* ke dalam sistem dengan *input* ID, *password* dan *upload stegoimage* maka sistem akan mengekstraksi *stegoimage* tersebut. Tidak dapat mengekstraksi *stegoimage* jika *password* tidak sama dengan yang dibuat oleh pengirim/*sender.*

2.2.3. *Sequence Diagram*

Sequence diagram merupakan gambaran dari interaksi antara objek yang mengidentifikasi komunikasi antara objek-objek tersebut. Adapun *sequence diagram* Adapun *sequence diagram* pada sistem sebagai berikut:

1. *Sequence Diagram* Menu *Embedding*

Adapun *sequence diagram* menu *embedding* pada sistem dapat dilihat pada gambar 4.

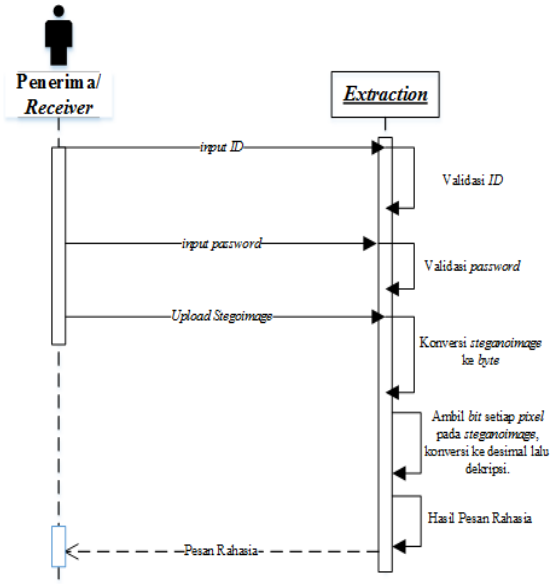


Gambar 4. *Sequence Diagram* Menu *Embedding*

Sequence Diagram proses penyisipan pesan ke dalam sebuah citra. Pada tahap penyisipan pesan, pengirim akan meng*input*kan *Password, Upload Cover Image* dan *Input* Pesan Rahasia untuk melakukan proses penyisipan/*embedding*. Setelah sistem memperoleh data *input*an, sistem akan enkripsi pesan rahasia lalu konversi karakter pesan rahasia ke desimal dan ke biner. Kemudian akan dilakukan proses penyisipan dan hasil yang diperoleh berupa *stegoimage.*

2. *Sequence Diagram* Menu *Extraction*

Adapun *sequence diagram* menu *embedding* pada sistem dapat dilihat pada gambar 5.



Gambar 5. *Sequence Diagram* Menu *Extraction*

Sequence Diagram menu Extraction menjelaskan proses ekstraksi *stegoimage* menjadi pesan teks asli atau *plaintext* pesan rahasia. Pada tahap ekstraksi *stegoimage* penerima akan meng*input ID, password* yang sama dengan pengirim lalu meng*upload stegoimage* untuk melakukan proses ekstraksi. Setelah sistem memperoleh data, sistem akan mengelompokkan *biner* setiap *pixel* pada *stegoimage* lalu dikonversi menjadi desimal dan didekripsi menjadi *plaintext.* Maka akan diperoleh pesan asli atau *plaintext* pesan rahasia.

3. Hasil dan Pembahasan

Pada proses analisa steganografi menggunakan End Of File dilakukan dua tahapan yaitu proses penyisipan/*embedding* pesan rahasia yang akan disembunyikan dan proses ekstraksi/*extraction.* Berikut adalah proses *embedding* pesan dengan uji coba dalam ruangan.png yang telah diresize menjadi 5 * 5 *pixel.*

INPUT:
Password : INF2020
Pesan Rahasia : pesan
Cover Image/Citra Digital : 5 x 5 *pixels*

Tabel 3. Citra Desimal *Pixel Cover Image*

Pixel	0			1			2			3			4		
5x5xRGB	R	G	B	R	G	B	R	G	B	R	G	B	R	G	B
0	14	16	16	55	42	31	117	97	52	45	34	22	25	23	19
1	13	16	17	29	22	17	55	53	45	48	41	31	8	11	11
2	3	10	12	45	44	34	70	66	45	78	52	30	0	6	10
3	0	6	10	0	4	9	59	54	41	18	17	15	0	4	8
4	0	4	8	0	3	8	46	41	27	39	37	24	6	9	11

Pada tabel 3 merupakan konversi *pixel* citra *cover image* yang dikonversikan ke desimal dan akan dilakukannya penyisipan pesan.

Proses:

1. Proses Konversi Nilai Desimal Pesan
Karakter Pesan dirubah kedalam nilai desimal berdasarkan urutan karakter pada tabel ASCII.

Pesan Rahasia : pesan

Tabel 4. Tabel Konversi Karakter Pesan Menjadi Nilai Desimal

p	e	s	a	n
112	101	115	97	110

Pada tabel 4. merupakan sebuah tabel konversi karakter pesan menjadi nilai desimal berdasarkan tabel ASCII.

2. Proses Konversi Nilai Desimal Pesan

Karakter Pesan dirubah kedalam nilai desimal berdasarkan urutan karakter pada tabel ASCII

Tabel 5. Konversi Pixel Citra *Cover Image*

Pixel	0			1			2			3			4		
	R	G	B	R	G	B	R	G	B	R	G	B	R	G	B
0	14	16	16	55	42	31	117	97	52	45	34	22	25	23	19
1	13	16	17	29	22	17	55	53	45	48	41	31	8	11	11
2	3	10	12	45	44	34	70	66	45	78	52	30	0	6	10
3	0	6	10	0	4	9	59	54	41	18	17	15	0	4	8
4	0	4	8	0	3	8	46	41	27	39	37	24	6	9	11
5	112	112	112	101	101	101	115	115	115	97	97	97	110	110	110

p	e	s	a	n
112	101	115	97	110

Pada tabel 5 dapat dilihat pesan yang telah dikonversikan kedalam bilangan desimal ASCII. Kemudian dilakukan penyisipan pada masing-masing nilai ASCII dari pesan rahasia pada bagian akhir. Setiap pixel akan diisi dengan nilai dari 1 huruf rahasia. Proses penyembunyian pesan kedalam citra gambar dilakukan dengan menambahkan pixel dari citra asli, jumlah yang ditambahkan sama dengan jumlah karakter yang akan disembunyikan dan tidak merubah ukuran file citra asli. Proses penabahan *pixel* inilah yang menyebabkan terjadinya perubahan ukuran tinggi dari citra hasil (*stegano image*).

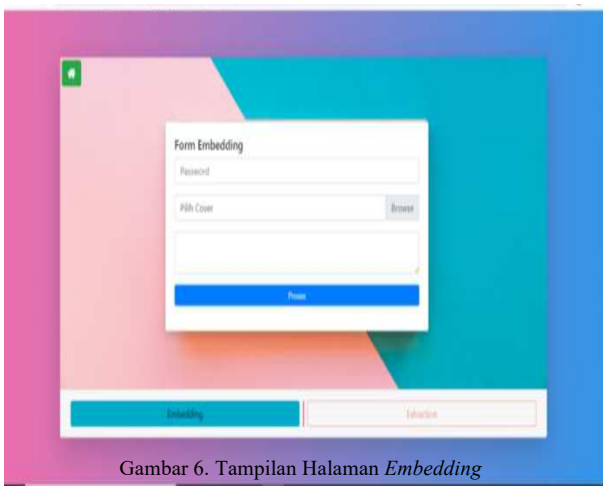
Tabel 6. Penyisipan karakter pesan pada akhir file

Pixel 5x5xRGB	*0*			*1*			*2*			*3*			*4*		
	R	*G*	*B*	*R*	*G*	*B*	*R*	*G*	*B*	*R*	*G*	*B*	*R*	*G*	*B*
0	14	16	16	55	42	31	117	97	52	45	34	22	25	23	19
1	13	16	17	29	22	17	55	53	45	48	41	31	8	11	11
2	3	10	12	45	44	34	70	66	45	78	52	30	0	6	10
3	0	6	10	0	4	9	59	54	41	18	17	15	0	4	8
4	0	4	8	0	3	8	46	41	27	39	37	24	6	9	11
5	112	112	112	101	101	101	115	115	115	97	97	97	110	110	110

Pixel 5x5xRGB	*0*			*1*			*2*			*3*			*4*		
	R	*G*	*B*	*R*	*G*	*B*	*R*	*G*	*B*	*R*	*G*	*B*	*R*	*G*	*B*
0	SO	DLE	DLE	7	*	US	U	a	4	-	"	SYN	EM	ETB	DC3
1	CR	DLE	DC1	GS	SYN	DC1	7	5	-	0	)	US	BS	VT	VT
2	ETX	LF	FF	-	,	"	F	B	-	N	4	RS	NULL	ACK	LF
3	NULL	ACK	LF	NULL	EOT	HT	;	6	)	DC1	DC1	SI	NULL	EOT	BS
4	NULL	EOT	BS	NULL	EXT	BS	.	)	ESC	NAK	NAK	CAN	ACK	HT	VT
5	p	p	p	e	e	e	s	s	s	a	a	a	n	n	n

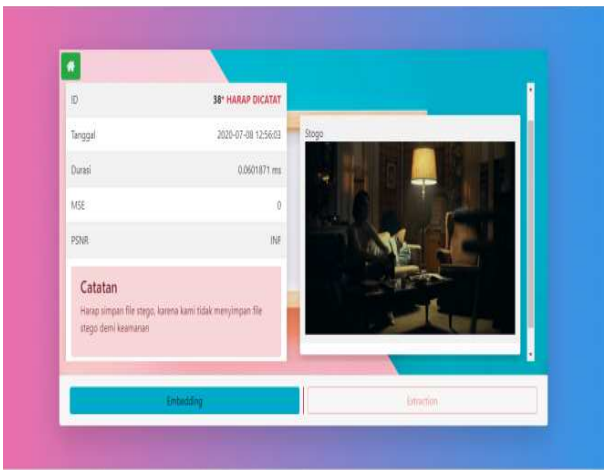
P	e	S	a	n

Pada tabel 6. Proses ekstraksi pesan rahasia yang telah disembunyikan pada citra digital, dilakukan berdasarkan metode *End Of File* yaitu dengan memasukkan *stegano image*, setelah itu baca nilai desimal *pixel* dari *stegano image*, kemudian nilai desimal dikonversi ke bentuk karakter, maka akan didapatkan hasil pesan yang disisipkan.



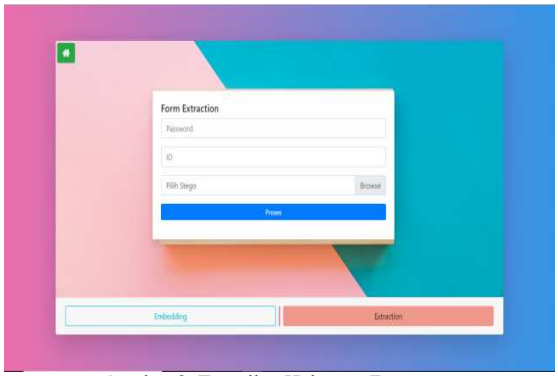
Gambar 6. Tampilan Halaman *Embedding*

Pada gambar di atas menunjukkan tampilan halaman *embedding*. Menyisipkan pesan rahasia dengan 3 inputan yaitu *password, upload cover image* dan *input* pesan rahasia. Setelah diproses *stegoimage* dapat didownload untuk dikirmkan pada penerima untuk diekstraksi.



Gambar 7. Tampilan Halaman *Output Embedding*

Pada gambar 7 Menampilkan hasil *embedding* berupa informasi terkait *embedding* tersebut seperti ID, Tanggal *Embedding,* durasi *embedding, MSE* dan *PSNR.*



Gambar 8. Tampilan Halaman *Extraction*

Pada gambar di atas menunjukkan tampilan halaman *extraction*. Setelah mendapatkan *stegoimage* dari *sender* dan akan dilakukannya ekstraksi dengan 2 inputan yaitu ID, *password* (yang sama dengan *password sender*) dan *upload stegoimage* lalu bisa diproses dan akan muncul pesan rahasia setelah diekstraksi.

Gambar 9. Tampilan Halaman *Output* Extraction

Pada gambar 9 menampilkan hasil *extraction* berupa pesan rahasia dan informasi terkait *extraction* tersebut seperti Tanggal *Embedding,* durasi *extraction* dan MSE, PSNR dan Pesan Rahasia.

Berikut adalah hitungan MSE dan PSNR pada uji coba Dalam Ruangan.png yang telah diresize menjadi 5 * 5 *pixels*.

Gambar	Panjang Huruf	Resolusi Gambar		Size		MSE	PSNR	Waktu Proses
		Asli	Stego	Asli	Stego			
	5	5 x 5 *pixel*	5 x 6 *pixel*	214 bytes	226 bytes	0	∞	0.00449085

Gambar 10. Tampilan Halaman *Output* Extraction

Untuk mengukur kualitas citra pada penelitian ini akan dilakukan pengujian pada 4 buah gambar berbeda sebagai *coverimage* terhadap Implementasi Steganografi dengan Metode *End Of File* untuk Menyisipkan Pesan Teks Pada Gambar. Adapun perbandingan hasil gambar (*cover image)* dan hasil gambar (*stegoimage)* setelah disisipkan pesan *text* steganografi dengan metode *End Of File* serta Kualitas citra hasil penyisipan pesan atau *stegoimage*.

Gambar		Panjang Huruf	Resolusi Gambar		Size		MSE	PSNR	Waktu Proses
Asli	Stego Image		Asli	Stego	Asli	Stego			
		450	450 x 675 *pixel*	450 x 676 *pixel*	58.1 kb	499 kb	0	∞	0.0282669 ms
		1000	1000 x 666 *pixel*	1000 x 667 *pixel*	174 kb	644 kb	0	∞	0.0527291 ms
		720	720 x 405 *pixel*	720 x 406 *pixel*	51.7 kb	269 kb	0	∞	0.0307031 ms
		40	40 x 28 *pixel*	40 x 29 *pixel*	1.50 kb	3.02 kb	0	∞	0.035593 ms
		350	354 x 472 *pixel*	354 x 473 *pixel*	28.4 kb	144 kb	0	∞	0.086498 ms

Gambar 11. Hasil Pengujian

Pada gambar 11 panjang huruf yang akan disisipkan tidak bisa diinput melebihi batas *width* p*ixel* pada citra cover, dapat dilihat perbandingan antara *coverimage* dan *stegoimage*, yang mana ukuran file mengalami perubahan akibat penabahan *pixel*, Jumlah *pixel stegano image* bertambah, kualitas citra digital tetap dan ukuran pada *height* citra hasil (*stegano image)* bertambah. MSE menunjukkan nilai 0 dikarenakan metode ini hanya menyisipkan pesan teks pada file gambar diakhirnya, bukan pada intensitas warna RGB suatu *pixel* sehingga tidak merubah maupun merusak nilai piksel gambar. Karena nilai MSE sebelumnya bernilai 0 maka nilai PSNR yang didapatkan menjadi tak hingga, Sehingga pada rumus PSNR menunjukkan terhadap MSE, jika nilai dibagi oleh nilai 0 maka akan menghasilkan nilai tak hingga.

4. Kesimpulan

Dari penelitian ini dapat ditarik kesimpulan bahwa Semakin ditambah banyak informasi data yang disembunyikan maka akan semakin besar pula ukuran yang dihasilkan, hal ini terjadi karena perubahan ukuran pada file *stegoimage* menjadi lebih besar dari ukuran *cover image* sebelum di proses embedd dan ekstrak. menyisipkan pesan diakhir file tanpa merubah nilai intensitas warna pikselnya.sehingga

penerapan metode *end of file* menghasilkan kualitas gambar yang lebih baik namun ukuran file yang dihasilkan menjadi lebih besar dari sebelumnya.

Daftar Rujukan

[1] Indrayani R, 2019, *Human Perception Evaluation toward End of File Steganography Method's Implementation Using Multimedia File (Image, Audio, and Video)*, 4th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), 2019, pp. 200-204, doi: 10.1109/ICITISEE48480.2019.9003759.

[2] Jannah L. M., Santoso I, and Cristyono Y, 2018, *TRANSIENT*, 7(1), doi: https://doi.org/10.14710/transient.7.1.34-39

[3] Watni D dan Chawla S, 2019, *A Comparative Evaluation of Jpeg Steganography*," 5th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, India, Oct 10-12 2019, pp. 36-40, doi: 10.1109/ISPCC48220.2019.8988383.

[4] Aditya Y, Pratama A dan Nurlifa A, 2010, *Studi pustaka untuk steganografi dengan beberapa metode*," Seminar Nasional Aplikasi Teknologi Informasi 2010 (SNATI) Yogyakarta, 19 Juni 2010, pp. 32–35

[4] Irawati D.A dan Rachmawati, E.D, 2018, *Perancangan Aplikasi Steganografi Menggunakan Algoritma IDEA dan Metode EOF*, *Seminar Nasional Informatika*, ISSN : 1979-2328, pp 195-205

[5] Masri M., Masri M., Widya H dan Yuhendri D, 2019, *Perancangan Aplikasi Penyisipan Pesan Pada Pixel Citra Menggunakan Metode End Of File*, Journal of Electrical Technology, 4(3), pp 178 – 184

[6] Irawati D.A., Astiningrum M dan Dinda E.R, 2018, *Impelemntasi Algoritma Idea dan Metode End Of File Pada Gambar Untuk Menyembunyikan Pesan,* Jurnal Informatka Polinema 5(1), pp. 19-24, doi: https://doi.org/10.33795/jip.v5i1.237

[7] Martono, Irawan, "Penggunaan Steganografi Dengan Metode End Of File (EOF) Pada Digital Watermarking", Jurnal TICOM, Vol.2 No.1, September, 2013.

[8] Minarni., Fernando A.G, 2020, *Implementasi Algoritma End Of File (EOF) Pada Steganografi Citra,* Jurnal TEKNOIF, 8(1), pp. 25-31

[9] Pandapotan T, S., *Analisa Perbandingan Least Significant BIT (LSB) dan End of File (EOF) untuk Steganografi Citra Digital Menggunakan Matlab,* Jurnal INFOTEK, Oktober 2016, 1(3), pp.186-194

[10] Darwis D., Kisworo, 2017, *Teknik Steganografi Untuk Penyembunyian Pesan Teks Menggunakan Algoritma End Of File,* Jurnal Sistem Informasi dan Telematika EXPLORE, 8(2), pp. 98-108

[11] Darwis, D., 2015., *Implementasi Steganografi pada Berkas Audio Wav untuk Penyisipan Pesan Gambar Menggunakan Metode Low Bit Coding*., Program Studi Magister Ilmu Komputer Universitas Budi Luhur Jakarta. Jurnal Expert. ISSN : 2088-5555

[12] Irawati, D.A., Rachmawati, 2018, *Perancangan Aplikasi Steganografi Menggunakan Algoritma Idea dan Metode EOF,* Seminar Nasional Informatika 2018 (semnasIF 2018), ISSN : 1979 – 2328, pp. 195-20