

Implementasi Teknik Steganografi pada Gambar JPEG dan PNG dengan menggunakan Metode Adaptive Minimum Error Least Significant Bit Replacement (AMELSBR)

Muhammad Bachtiar Alifi¹, I Made Suartana²,

¹ Jurusan Teknik Informatika/Teknik Informatika, Universitas Negeri Surabaya

² Jurusan Teknik Informatika/Teknik Informatika, Universitas Negeri Surabaya

muhammadalifi@mhs.unesa.ac.id

madesuartana@unesa.ac.id

Abstrak— Pada era *modern* seperti saat ini, media *digital* menjadi suatu pilihan yang digunakan untuk membantu pekerjaan seseorang menjadi lebih cepat, efektif dan efisien. Kerahasiaan suatu informasi menjadi aspek yang sangat penting dalam media *digital*. Steganografi merupakan seni yang digunakan untuk menyembunyikan suatu pesan rahasia kedalam pesan yang berbentuk media lain baik berupa gambar, suara, atau video. Ada beberapa metode dalam steganografi yang dapat digunakan dalam mengamankan pesan salah satunya yakni metode *Adaptive Minimum Error Least Significant Bit Replacement (AMELSBR)*. Penelitian ini dilakukan untuk mengetahui kualitas dari *stego image* dan untuk melihat pengaruh manipulasi citra terhadap *stego image* yang dihasilkan. Metode *Adaptive Minimum Error Least Significant Bit Replacement (AMELSBR)* akan digunakan dengan memanfaatkan kapasitas penyisipan yang berbeda bergantung pada nilai pixel yang dapat dimaksimalkan dalam proses penyisipan untuk mengetahui kualitas dari *stego image*. Pesan rahasia (*ciphertext*) yang digunakan adalah file jenis .txt, kemudian file .txt akan disisipkan kedalam media penampung berupa gambar (*cover image*) dengan jenis file berformat jpg dan png, sehingga akan menghasilkan output berupa *stego image* dengan format yang sesuai dengan jenis file *cover image* yang digunakan. Nilai PSNR yang dihasilkan yakni antara 40,16 hingga 58,84 dB yang menunjukkan kualitas *stego image* yang tinggi. Dalam pengujian manipulasi citra, metode *Adaptive Minimum Error Least Significant Bit Replacement* tidak tahan terhadap manipulasi citra yakni *brightness*, *contrast*, dan *resize* dengan interval yang telah ditentukan, karena metode ini tidak berhasil mengembalikan pesan yang ada pada *stego image*.

Kata Kunci— Steganografi, *adaptive minimum error least significant bit replacement*, PSNR, *brightness*, *contrast*

I. PENDAHULUAN

Pada era *modern* seperti saat ini, media *digital* menjadi suatu pilihan yang umum untuk berinteraksi dengan orang lain. Media *digital* juga membantu pekerjaan seseorang menjadi lebih cepat, efektif dan efisien. Seiring dengan pesatnya perkembangan teknologi pada media *digital* maka semakin berkembang pula kejahatan terhadap keamanan pesan yang dikirim.

Semakin penting nilai dari sebuah pesan maka semakin berkembang pula metode yang digunakan dalam mengamankan pesan. Steganografi merupakan seni yang digunakan untuk menyembunyikan suatu pesan rahasia

kedalam pesan yang berbentuk media lain baik berupa gambar, suara, atau video. Steganografi memiliki dua tahapan dalam menyembunyikan pesan yakni melakukan penyisipan dan melakukan pengestrakan [1].

Untuk melakukan fungsi steganografi ada beberapa metode yang dapat digunakan. Metode yang digunakan dalam steganografi diantaranya yaitu *Least Significant Bit (LSB)*, *Masking and Filtering*, *Discrete Cosine Transform (DCT)*, atau *Spread-Spectrum Encoding*. Salah satu metode yang sering digunakan dalam melakukan fungsi steganografi yaitu *Least Significant Bit (LSB)*. *Least Significant Bit* ini sering digunakan untuk melakukan fungsi steganografi karena mudah dalam melakukan penyisipan pesan rahasia. Namun metode ini juga memiliki banyak kelemahan dalam melakukan fungsi steganografi diantaranya yaitu ketahanan terhadap manipulasi citra, sensitif terhadap manipulasi *stego image*, adanya *noise* yang tinggi dan *cropping* [2].

Untuk mengatasi kelemahan pada metode *Least Significant Bit (LSB)* yang rentan terhadap *noise* yang tinggi pada citra *stego image* maka dikembangkan metode *Adaptive Minimum Error Least Significant Bit Replacement*. Dalam metode *Adaptive Minimum Error Least Significant Bit (AMELSBR)* citra penampung (*cover image*) akan dibagi terlebih dahulu kedalam beberapa blok yang memiliki ukuran 3 x 3 piksel dan dilakukan penyisipan dari setiap *pixel* menjadi berbeda-beda bergantung pada nilai toleransi *pixel* yang diperoleh terhadap penyisipan yang dilakukan sehingga mampu mengurangi *noise* pada citra. Pada penelitian yang sudah dilakukan sebelumnya dengan judul *Adaptive Minimum Error Least Significant Bit Replacement Method For Steganography Using JPG/JPEG and PNG Files* [3]. Dalam penelitian tersebut dijelaskan tentang penggunaan fungsi steganografi dengan metode *Adaptive Minimum Error Least Significant Bit Replacement (AMELSBR)* dengan menggunakan file jpg sebagai media penampung pesan, output berupa *stego image* dengan file berformat png serta pesan yang disisipkan berupa berkas text (.txt). Hasil penelitian tersebut menunjukkan bahwa dengan menggunakan metode AMELSBP dapat mengurangi *noise* yang tinggi pada citra *stego image*. Namun pada penelitian tersebut tidak dilakukan pengujian untuk mengetahui kualitas berdasarkan nilai PSNR (*Peak Signal to Noise Ratio*).

Sehingga berdasarkan permasalahan diatas penelitian ini akan mengembangkan fungsi steganografi dengan

menggunakan metode *Adaptive Minimum Error Least Significant Bit Replacement (AMELSBR)*. Pesan rahasia (*ciphertext*) yang menggunakan *file* jenis .txt, kemudian *file* .txt akan disisipkan kedalam media penampung berupa gambar (*cover image*) dengan jenis *file* berformat jpg dan png, sehingga akan menghasilkan *output* berupa *stego image* dengan format yang sesuai dengan jenis *file* *cover image* yang digunakan. Pada penelitian ini akan dilakukan pengujian pada kualitas *stego image* dengan mencari nilai PSNR dan melihat ketahanan citra terhadap perubahan yang dilakukan dengan melakukan pengujian manipulasi citra berupa *brightness*, *contrast* dan *resize*

II. METODE PENELITIAN

Dalam penelitian ini terdapat beberapa tahapan penelitian yakni meliputi identifikasi, studi literatur, analisis sistem, rancangan penelitian, implemetasi dan pengujian, analisis hasil serta kesimpulan. Tujuan dari penelitian ini yaitu untuk menerapkan salah satu metode dari steganografi yaitu *Adaptive Minimum Error Least Significant Bit Replacement* sebagai dasar untuk mengetahui pengaruh setelah dilakukan proses steganografi dan mengetahui kualitas citra hasil berupa *stego image*.

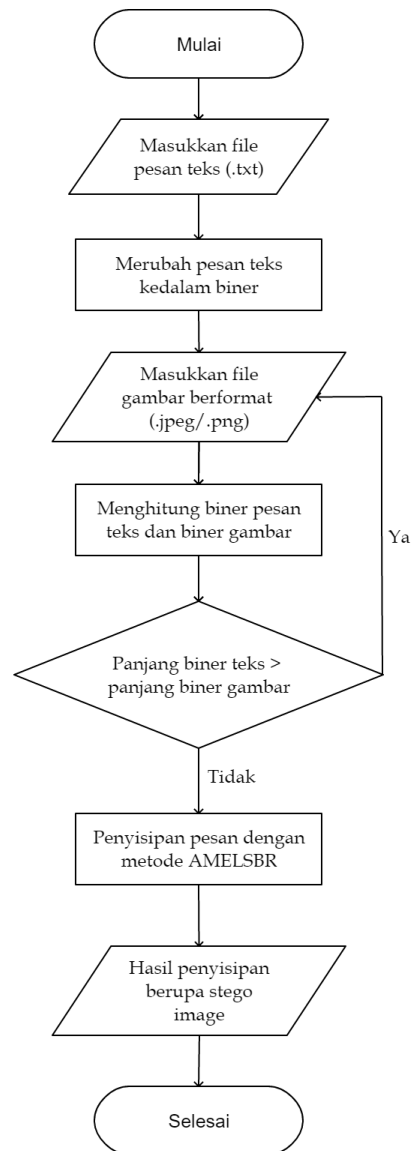
Proses penyisipan pesan (*embedding*) pada metode *Adaptive Minimum Error Least Significant Bit (AMELSBR)* citra penampung (*cover image*) akan dibagi terlebih dahulu kedalam beberapa blok. Setiap blok memiliki ukuran 3 x 3 piksel atau sama dengan 9 piksel. Kemudian akan diterapkan tiga tahapan utama disetiap blok penyisipannya. Beberapa tahapan dalam melakukan proses penyisipan menggunakan metode *Adaptive Minimum Error Least Significant Bit Replacement* diantaranya yaitu *Capacity Evaluation*, *Minimum Error Replacement* dan *Error Diffusion*. Sedangkan dalam proses ekstraksi, tahapan yang dilakukan adalah *Capacity Evaluation*.

Evaluasi Kapasitas harus dilakukan terlebih dahulu sebelum melakukan penyisipan pesan. Tahapan ini dilakukan berdasarkan pada karakteristik *Human Visual Eyes (HVS)* yang tidak sensitif terhadap perubahan warna dan *noise* yang ada didalam citra. Mencari nilai dari variasi warna (*colour variation*) dari sebuah *pixel*. Selanjutnya mencari nilai kapasitas penyisipan sejumlah K-bit dengan menggunakan nilai variasi warna. Dan melakukan evaluasi kapasitas dari sejumlah K-bit untuk menyesuaikan dengan karakteristik lokal dari sebuah *pixel*. *Minimum Error Replacement* dilakukan untuk meminimalkan perubahan yang terjadi terhadap *pixel* citra penampung akibat dari proses penyisipan. Mencari nilai *embedding error* yakni selisih nilai (dalam bentuk desimal) pada komponen warna yang terpilih pada sebuah *pixel* yang akan dilakukan pengecekan nilai *error* pada saat sebelum (*original*) dan sesudah dilakukan proses penyisipan. Kemudian melakukan pengubahan pada bit ke K+1 akan dilakukan apabila nilai *embedding error* memenuhi syarat pada saat pengecekan. *Error Diffusion* langkah yang dilakukan untuk mengimprovisasi kualitas dari citra hasil (*stego image*) dan ketika dilakukan proses ekstraksi pesan rahasia. *Error*

Diffusion digunakan dalam metode AMELSBRR dengan tujuan untuk menekan *noise* yang ada pada gambar.

A. Proses Encoding

Encoding merupakan suatu proses untuk menyisipkan pesan rahasia kedalam media penampung pesan (*cover image*). sehingga media penampung yang telah disisipi pesan rahasia akan menjadi *stego image*. Dalam proses *encoding* ada beberapa tahapan yakni pada Gbr 1 :



Gbr. 1 Alur *Encoding* AMELSBRR

Berikut adalah tahapan proses *encoding* :

1. Masukkan pesan (*Plaintext*) digunakan untuk memilih pesan rahasia yang akan disisipkan dalam bentuk *file* (.txt).

2. Pada proses ini pesan teks akan dirubah kedalam bentuk biner untuk diproses ditahap berikutnya.
3. Masukkan gambar (*cover image*) digunakan untuk memilih gambar yang akan digunakan sebagai media penampung pesan dalam bentuk *file* (.jpeg/.png).
4. Pada proses ini gambar (*cover image*) akan dirubah kedalam bentuk biner untuk diproses ditahap berikutnya.
5. Pada proses ini akan dihitung nilai biner gambar dan nilai biner *plaintext*, apabila nilai biner *plaintext* lebih banyak dari nilai biner gambar, maka penyisipan pada gambar tidak bisa dilakukan dan proses akan kembali mencari media *cover* gambar yang lainnya.
6. Jika nilai biner memenuhi untuk dilakukan proses penyisipan maka proses selanjutnya yaitu melakukan penyisipan dengan metode *Adaptive Minimum Error Least Significant Bit Replacement*.
7. Pada proses penyisipan pesan menggunakan AMELSBK kapasitas penyisipan pesan akan dicari dengan mencari nilai variasi warna dengan menggunakan persamaan (1)

$$V = \text{round} \left\{ \frac{(|C-A| + |A-B| + |B-C| + |C-D|)}{4} \right\} (1)$$

Dimana :

- V : variasi warna (*colour variation*)
- Round : fungsi matematik untuk pembulatan

kemudian dari nilai tersebut akan digunakan untuk mencari ukuran kapasitas penyisipan menggunakan persamaan (2)

$$K = \text{round} (|\log_2 V|) (2)$$

Dimana :

- K : kapasitas penyisipan pada *pixel* P dalam *bit*
- V : variasi warna (*colour variation*)
- Round : fungsi matematik untuk pembulatan

selanjutnya mencari nilai *embedding error* dengan menggunakan persamaan (3) dan (4)

$$Er_1 = \text{Abs}[P(x,y) - P'(x,y)] (3)$$

$$Er_2 = \text{Abs}[P(x,y) - P''(x,y)] (4)$$

Dimana :

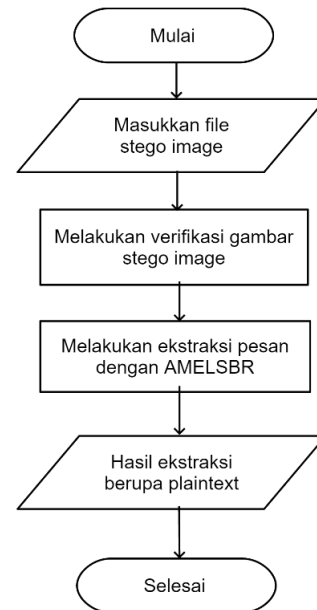
- Er : nilai *embedding error*
- Abs : nilai absolut
- P(x,y) : *pixel* P asli
- P'(x,y) : *pixel* P tanpa mengubah bit ke K+1

- P''(x,y) : *pixel* P dengan mengubah bit ke K+1

8. Setelah proses penyisipan dilakukan maka hasil dari proses penyisipan akan keluar berupa *stego image*.

B. Proses Decoding

Decoding merupakan suatu proses untuk mengekstrak pesan rahasia dari *stego image* sehingga pesan yang telah disisipkan dapat dikembalikan seperti semula. Dalam proses *decoding* ada beberapa tahapan yakni pada Gbr 2 :



Gbr. 2 Alur proses *decoding* AMELSBK

Berikut adalah tahapan proses *decoding* :

1. Masukkan gambar (*stego image*) digunakan untuk memilih gambar yang akan dilakukan ekstraksi.
2. Pada proses ini *stego image* akan diverifikasi apakah dalam format .jpeg/.png atau bukan.
3. Melakukan proses ekstraksi dengan menggunakan metode *Adaptive Minimum Error Least Significant Bit Replacement*.

III. HASIL DAN PEMBAHASAN

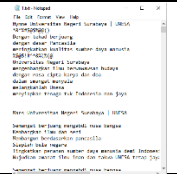
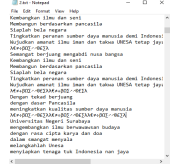
Penelitian implementasi teknik steganografi metode AMELSBK ini dibuat dengan menggunakan *software* PHP Storm 2019 dengan bahasa pemrograman PHP.

A. Data Penelitian

Data yang digunakan dalam penelitian ini adalah data berupa *file* teks berformat .txt sebagai berkas yang akan disisipkan dan gambar berformat jpg dan png yang akan digunakan sebagai media penampung. Berkas txt yang digunakan memiliki beberapa ukuran *file* dan media penampung yang digunakan

memiliki dimensi yang berbeda. Ukuran *file* pesan .txt yang akan disisipkan harus lebih kecil dari cover image, Karena ukuran *cover image* terkecil memiliki ukuran 27 Kb maka ukuran *file* txt yang digunakan yakni 15,57 Kb dan 24,4 Kb. Ukuran *file* pesan digunakan sebagai variabel untuk mengetahui pengaruh dari dimensi dan format *file* yang berbeda-beda. Data penelitian ditunjukkan pada Tabel I,II,III dan IV.

TABEL I
DATA BERKAS PENYISIPAN

No	Nama File	Pesan Rahasia	Ukuran
1	1.txt		15,57 Kb
2	2.txt		24,4 Kb

TABEL II
DATA MEDIA PENAMPUNG (.JPG)

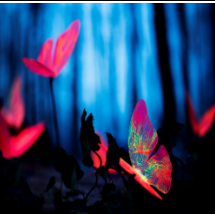
No	Nama File	Dimensi	Ukuran
1	Bird1.jpg	300 x 300	27,1 kb
2	Bird2.jpg	600 x 600	89 kb
3	Bird3.jpg	900 x 900	194 kb
4	Bird4.jpg	1200 x 1200	354 kb
5	Butterfly1.jpg	300 x 300	33,6 kb
6	Butterfly2.jpg	600 x 600	81,6 kb
7	Butterfly3.jpg	900 x 900	156 kb
8	Butterfly4.jpg	1200 x 1200	271 kb
9	Fruits1.jpg	300 x 300	68,1 kb
10	Fruits2.jpg	600 x 600	177 kb
11	Fruits3.jpg	900 x 900	320 kb
12	Fruits4.jpg	1200 x 1200	493 kb
13	Bridge1.jpg	300 x 300	65,2 kb
14	Bridge2.jpg	600 x 600	195 kb
15	Bridge3.jpg	900 x 900	383 kb
16	Bridge4.jpg	1200 x 1200	608 kb

TABEL III
DATA MEDIA PENAMPUNG (.PNG)

No	Nama File	Dimensi	Ukuran
1	Bird1.png	300 x 300	237 kb

No	Nama File	Dimensi	Ukuran
2	Bird2.png	600 x 600	938 kb
3	Bird3.png	900 x 900	2,02 Mb
4	Bird4.png	1200 x 1200	3,67 Mb
5	Butterfly1.png	300 x 300	145 kb
6	Butterfly2.png	600 x 600	534 kb
7	Butterfly3.png	900 x 900	1,19 Mb
8	Butterfly4.png	1200 x 1200	2,17 Mb
9	Fruits1.png	300 x 300	231 kb
10	Fruits2.png	600 x 600	809 kb
11	Fruits3.png	900 x 900	1,65 Mb
12	Fruits4.png	1200 x 1200	2,83 Mb
13	Bridge1.png	300 x 300	209 kb
14	Bridge2.png	600 x 600	743 kb
15	Bridge3.png	900 x 900	1,53 Mb
16	Bridge4.png	1200 x 1200	2,63 Mb

TABEL IV
DATA MEDIA PENAMPUNG

No	Nama File	Gambar
1	Bird	
2	Butterfly	
3	Fruits	
4	Bridge	

Berikut adalah salah satu hasil dari proses penyisipan pesan teks .txt kedalam *cover image* yang menghasilkan *stego image*

mencari nilai PSNR diperlukan nilai MSE (*Mean Square Error*) dengan persamaan (5)

$$MSE = \frac{1}{N} \sum_n |y(n) - x(n)|^2 \quad (5)$$

Keterangan :

$y(n)$ = data *cover image*

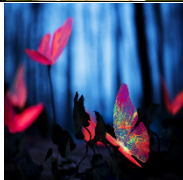
$x(n)$ = data *stego image*

N = dimensi gambar

Setelah mendapatkan nilai mse maka selanjutnya mencari nilai PSNR dengan persamaan (6)

$$PSNR = 10_{\log_{10}} \frac{255^2}{MSE} \quad (6)$$

TABEL V
DATA MEDIA PENAMPUNG

No	Nama File	Cover Image	Stego Image
1	Bird		
2	Butterfly		
3	Fruits		
4	Bridge		

Dari Tabel V gambar *cover image* dan *stego image* diatas dapat diketahui bahwa secara *visual* tidak terdapat perbedaan yang signifikan. Sehingga untuk mengetahui perbedaan keduanya maka dilakukan pengujian PSNR untuk melihat kualitas suatu citra *stego image* yang dihasilkan.

B. Pengujian PSNR

Pada penelitian steganografi metode AMELSBK ini pengujian awal yang dilakukan adalah PSNR (*Peak Signal to Noise Ratio*). Pengujian ini digunakan untuk melihat perbandingan kualitas suatu citra *cover* sebelum maupun sesudah disisipkan pesan dengan metode AMELSBK. Nilai PSNR diukur dengan menggunakan satuan desibel (dB). Untuk

TABEL VI
HASIL PENGUJIAN PSNR (.JPG)

No	Cover image	Dimensi	Hasil PSNR	
			txt1	txt2
1	Bird1.jpg	300 x 300	40,68 dB	38,64 dB
2	Bird2.jpg	600 x 600	50,39 dB	48,03 dB
3	Bird3.jpg	900 x 900	50,39 dB	52,23 dB
4	Bird4.jpg	1200 x 1200	57,87 dB	53,31 dB
5	Butterfly1.jpg	300 x 300	41,76 dB	38,91 dB
6	Butterfly2.jpg	600 x 600	47,90 dB	45,63 dB
7	Butterfly3.jpg	900 x 900	55,44 dB	52,65 dB
8	Butterfly4.jpg	1200 x 1200	58,84 dB	56,77 dB
9	Fruits1.jpg	300 x 300	47,36 dB	44,58 dB
10	Fruits2.jpg	600 x 600	46,14 dB	45,01 dB
11	Fruits3.jpg	900 x 900	53,86 dB	50,72 dB
12	Fruits4.jpg	1200 x 1200	52,60 dB	49,66 dB
13	Bridge1.jpg	300 x 300	43,16 dB	39,08 dB
14	Bridge2.jpg	600 x 600	49,61 dB	45,35 dB
15	Bridge3.jpg	900 x 900	49,69 dB	47,30 dB
16	Bridge4.jpg	1200 x 1200	52,09 dB	50,08 dB

TABEL VII
HASIL PENGUJIAN PSNR (.PNG)

No	Cover image	Dimensi	Hasil PSNR	
			txt1	txt2
1	Bird1.png	300 x 300	39,87 dB	37,29 dB
2	Bird2.png	600 x 600	49,50 dB	47,94 dB
3	Bird3.png	900 x 900	49,88 dB	49,74 dB
4	Bird4.png	1200 x 1200	55,34 dB	52,80 dB
5	Butterfly1.png	300 x 300	42,95 dB	41,68 dB
6	Butterfly2.png	600 x 600	51,37 dB	48,37 dB
7	Butterfly3.png	900 x 900	56,40 dB	51,82 dB
8	Butterfly4.png	1200 x 1200	56,78 dB	52,69 dB
9	Fruits1.png	300 x 300	42,35 dB	39,68 dB
10	Fruits2.png	600 x 600	49,98 dB	46,71 dB
11	Fruits3.png	900 x 900	50,83 dB	48,54 dB
12	Fruits4.png	1200 x 1200	55,19 dB	52,05 dB
13	Bridge1.png	300 x 300	36,69 dB	34,43 dB
14	Bridge2.png	600 x 600	40,16 dB	38,91 dB
15	Bridge3.png	900 x 900	44,03 dB	42,39 dB
16	Bridge4.png	1200 x 1200	50,37 dB	48,25 dB

Dari Tabel VI dan VII hasil pengujian PSNR diatas diketahui bahwa, nilai PSNR dari *file* berformat jpg tidak

memiliki perbedaan yang signifikan dengan file berformat png. Pengujian diatas juga menunjukkan bahwa semakin besar ukuran dimensi suatu cover image maka nilai PSNR yang dihasilkan semakin tinggi. Selain itu, semakin besar ukuran file .txt yang akan disisipkan maka nilai PSNR yang dihasilkan semakin rendah, hal ini dikarenakan semakin banyak bit pixel pada cover image yang mengalami perubahan sehingga menyebabkan adanya peningkatan noise pada stego image. Berdasarkan hasil pengujian PSNR diatas, nilai rata-rata yang dihasilkan untuk file jpg yaitu 48,94 dB dan untuk file png memiliki nilai rata-rata 47,03 dB sehingga menunjukkan bahwa stego image yang dihasilkan file jpg memiliki kualitas yang lebih tinggi karena memiliki keunggulan dalam menyisipkan data rahasia tanpa menimbulkan adanya perbedaan antara cover image dan stego image sehingga terlihat identik [4]. Kualitas dan kemiripan gambar hasil proses steganografi dengan gambar asli masih dapat dikatakan dalam kondisi baik jika nilai PSNR yang didapat berada diatas 40 dB [1].

C. Pengujian Pengekstrakan

Pesan yang telah berhasil disisipkan kedalam cover image kemudian akan dilakukan pengekstrakan untuk mengembalikan pesan dalam stego image untuk dibaca oleh penerima. Pengujian ekstraksi pesan ditunjukkan pada tabel berikut.

TABEL VIII
HASIL PENGUJIAN PENGEKSTRAKAN

No	Nama Stego Image	Hasil
1	Bird3.jpg	Tidak berhasil
2	Bird3.png	Berhasil
3	Butterfly3.jpg	Tidak berhasil
4	Butterfly3.png	Berhasil
5	Fruits3.jpg	Tidak berhasil
6	Fruits3.png	Berhasil
7	Bridge3.jpg	Tidak berhasil
8	Bridge3.png	Berhasil

Seperti ditunjukkan Tabel VIII hasil pengekstrakan pesan menggunakan metode AMELSBK menunjukkan bahwa pesan yang berhasil diekstrak merupakan pesan yang stego image nya memiliki format .png. Gambar (.png) termasuk kategori gambar lossless compression. Format file gambar (.png) ini tidak akan kehilangan data gambar berupa pixel ketika gambar disimpan atau dilihat. Namun untuk stego image yang berformat .jpg, pesan tidak dapat diekstrak kembali. Hal ini terjadi karena terdapat kelemahan dalam format .jpg, format ini bersifat lossy compression yang menyebabkan hilangnya beberapa data sehingga pesan tidak berhasil dikembalikan.

D. Pengujian Manipulasi Citra

Pada pengujian ini stego image hasil dari steganografi metode AMELSBK akan dilakukan pengujian dengan melakukan manipulasi penambahan dan pengurangan

brightness, contrast dan resize. Hal ini dilakukan untuk mengetahui ketahanan metode AMELSBK terhadap manipulasi pada gambar stego image.

TABEL IX
HASIL PENGUJIAN MANIPULASI BRIGHTNESS

No	Nama Stego Image	Tingkat Brightness	Hasil
1	Bird3.jpg	-120	Tidak berhasil
2	Bird3.png	-90	Tidak berhasil
3	Butterfly3.jpg	-60	Tidak berhasil
4	Butterfly3.png	-30	Tidak berhasil
5	Fruits3.jpg	30	Tidak berhasil
6	Fruits3.png	60	Tidak berhasil
7	Bridge3.jpg	90	Tidak berhasil
8	Bridge3.png	120	Tidak berhasil

TABEL X
HASIL PENGUJIAN MANIPULASI CONTRAST

No	Nama Stego Image	Tingkat Contrast	Hasil
1	Bird3.jpg	-120	Tidak berhasil
2	Bird3.png	-90	Tidak berhasil
3	Butterfly3.jpg	-60	Tidak berhasil
4	Butterfly3.png	-30	Tidak berhasil
5	Fruits3.jpg	30	Tidak berhasil
6	Fruits3.png	60	Tidak berhasil
7	Bridge3.jpg	90	Tidak berhasil
8	Bridge3.png	120	Tidak berhasil

TABEL XI
HASIL PENGUJIAN MANIPULASI RESIZE

No	Cover image	Dimensi		Hasil
		sebelum	sesudah	
1	Bird3.jpg	900 x 900	810 x 810	Tidak Berhasil
2	Bird3.png	900 x 900	810 x 810	Tidak Berhasil
3	Butterfly3.jpg	900 x 900	765 x 765	Tidak Berhasil
4	Butterfly3.png	900 x 900	765 x 765	Tidak Berhasil
5	Fruits3.jpg	900 x 900	720 x 720	Tidak Berhasil
6	Fruits3.png	900 x 900	720 x 720	Tidak Berhasil
7	Bridge3.jpg	900 x 900	675 x 675	Tidak Berhasil
8	Bridge3.png	900 x 900	675 x 675	Tidak Berhasil

Hasil pengujian manipulasi citra hasil steganografi seperti ditunjukkan pada Tabel IX, stego image dilakukan pengujian tingkat brightness dengan menggunakan interval perubahan -120, -90, -60, -30, 30, 60, 90, 120. Kemudian dalam Tabel X dilakukan pengujian manipulasi contrast dengan nilai interval yang sama seperti pengujian brightness. Pada Tabel XI dilakukan pengujian resize dengan melakukan perubahan ukuran 10%, 15%, 20%, dan 25% dari ukuran semula. Dari

tabel pengujian manipulasi diatas menunjukkan bahwa pesan tidak berhasil dikembalikan setelah terjadi perubahan pada *stego image*. Hal ini disebabkan karena *stego image* yang digunakan tidak dominan warna hitam dan putih [5]. Selain itu ketika dilakukan modifikasi pada citra *stego image* seperti perubahan *brightness* dan *contrast* akan membuat *file* tidak berhasil dilakukan pengekstrakan [3].

KESIMPULAN

Kesimpulan yang dapat diambil dari hasil penelitian yang sudah dilakukan dengan menggunakan metode *Adaptive Minimum Error Least Significant Bit Replacement* menunjukkan bahwa penyisipan pesan kedalam gambar berhasil dilakukan. Hasil pengujian kualitas *stego image* dari proses steganografi menggunakan metode AMELSBP telah terbukti memiliki kualitas *stego image* yang tinggi karena nilai yang dihasilkan berada diatas 40 dB. Nilai PSNR yang dihasilkan yakni antara 40,16 hingga 58,84 dB. Dalam pengujian manipulasi citra, metode *Adaptive Minimum Error Least Significant Bit Replacement* tidak tahan terhadap manipulasi citra yakni *brightness*, *contrast*, dan *resize* dengan interval yang telah ditentukan, karena metode ini tidak berhasil mengembalikan pesan yang ada pada *stego image*.

UCAPAN TERIMA KASIH

Puji syukur penulis ucapkan kepada Allah SWT. yang telah memberikan ridho-Nya dan senantiasa memberikan kemudahan dan kelancaran dalam pengerjaan jurnal ini serta tak lupa penulis ucapkan terimakasih kepada semua pihak yang telah ikut berperan membantu proses pengerjaan jurnal ini sehingga jurnal ini dapat terselesaikan dengan baik.

REFERENSI

- [1] AL abaichi Ashwak., Salih Adnan., Al-Dabbas Maisa'a Abid Ali., 2020. Image Steganography Using Least Significant Bit and Secret Map Techniques. *International Journal of Electrical and Computer Engineering (IJECE)*, pp. 935-946
- [2] Elsamani, E. E., 2013. Comparison of LSB Steganography in BMP and JPEG Images. *International Journal of Soft Computing and Engineering (IJSCE)*, pp. 91-95.
- [3] Wamiliana, et al., 2015. Adaptive Minimum Error Least Significant Bit Replacement Method For Steganography Using JPG/JPEG And PNG Files. pp. 4987-4990.
- [4] Sadi, Ghania Al., 2015. Image Steganography Approach. *International Journal of Computer Science and Mobile Computing (IJCSMC)*. pp. 166-169
- [5] Hijriani, A., Wamiliana, & Panditwa, P. 2014. Implementasi Teknik Steganografi Menggunakan Metode Adaptive Minimum Error Least Significant Bit Replacement (AMELSBR). *Ilmu Komputer Unila Publishing Network*, 87-94.
- [6] Ansari, Arshiya Sajid, Mohammadi Mohammad Sajid, Parvez Mohammad Tanvir., 2019. A Comparative Study of Recent Steganography Techniques for Multiple Image Formats. *Computer Network and Information Security*. pp. 11-25.