Aplikasi Penyembunyian Pesan pada Citra dengan Metode AES Kriptografi dan Enhanced LSB Steganografi

Irpan Adiputra Pardosi *[1], Sunario Megawan[2], Nico Prasasty Sembiring[3]
Santa Lorena Barbara Purba[3]
STMIK Mikroskil, Jl. Thamrin No. 112, 124, 140, Telp. (061) 4573767, Fax. (061) 4567789
[1,2,3,4] Jurusan Teknik Informatika, STMIK Mikroskil, Medan
*[1]irpan@mikroskil.ac.id, [2]sunario@mikroskil.ac.id, [3]nicoprasastys@ymail.com,
[4]santalorena@ymail.com

Abstrak

Pengiriman data melalui internet sangat membutuhkan pengamanan data, selain menggunakan algoritma kriptografi dibutuhkan juga algoritma untuk membuat pihak ketiga tidak mencurigai pengiriman pesan yang terenkripsi sehingga tidak terlihat dengan menerapkan teknologi steganografi. Kombinasi kriptografi dengan steganografi dapat meningkatkan tingkat keamanan data dengan menyembunyikannya ke dalam media lain seperti citra. Penelitian ini menggunakan algoritma Advanced Encryption Standard (AES) sebagai pengaman pesan dengan mengenkripsi data dan algoritma steganografi Enhanced Least Significant Bit (Enhanced LSB) dengan formasi 2-3-3 bit sebagai algoritma penyembunyian pesan ke dalam citra. Pengujian dilakukan dengan mengukur kualitas citra hasil serta membandingkan ukuran citra hasil setelah disisipkan pesan. Hasil dari penelitian ini menyimpulkan algoritma AES dan Enhanced LSB formasi 2-3-3 ini dapat memberikan peningkatan kualitas pengamanan pada suatu media gambar, tanpa mengubah ukuran citra setelah disisip.

Kata kunci— *Keamanan data, kriptografi, steganografi, Advanced Encryption Standard (AES), Enhanced Least Significant Bit (Enhanced LSB).*

Abstract

Delivery of data via the internet requires data security, in addition to using a cryptographic algorithm algorithm is also needed technic to make the third party did not suspect that the encrypted message delivery so it is not visible with steganographic technology. The combination of cryptography with steganography will increase the level of data security by hiding it into an image. This study uses the Advanced Encryption Standard algorithm (AES) to encrypt the data and algorithms steganography Enhanced Least Significant Bit (LSB Enhanced) 2-3-3 bit formation as a concealment algorithm to the message in the image. Testing scenario is done by measurement quality of image result level and comparing the size of the image and the results of the initial image. Results from this study concludes AES algorithm and Enhanced LSB can provide increased security on a medium quality image, without changing the size of the image after messages had inserted.

Keywords— *Cryptography, steganography, Advanced Encryption Standard (AES), Enhanced Least Significant Bit (LSB Enhanced).*

1. PENDAHULUAN

Pengamanan data menggunakan kriptogafi saja tidak cukup, karena perubahan data masih terlihat dan sering membuat pihak ketiga menjadi curiga [1]. Penelitian ini membuat aplikasi dengan mengimplementasikan algoritma steganografi teks pada media citra, menjadi lebih kuat dan aman dengan menambah algoritma kriptografi didalamnya. Algoritma kriptografi yang digunakan adalah

algoritma *Advanced Encryption Standard* (AES). Dipilihnya algoritma ini dikarenakan masih lebih aman dibandingkan algoritma lain seperti DES [2]. Informasi yang terenkripsi menggunakan algoritma *Advanced Encryption Standard* (AES) tersebut kemudian dimasukkan ke dalam media gambar dengan menggunakan algoritma steganografi *Enhanced Least Significant Bit* (*Enhanced* LSB). Dipilihnya algoritma ini karena algoritma ini mengoptimalkan mekanisme *Least Significant Bit* (LSB) dengan memanfaatkan warna RGB pada keseluruhan pixel dalam citra dan dapat menampung sampai 3 bit dalam setiap pixel RGB [3]. Dengan metode formasi 2-3-3 bit ini akan meningkatkan kualitas citra dibanding LSB sederhana. Pengujian yang dilakukan pada citra hasil terhadap kualitas dan ukuran citra hasil. Aplikasi yang dikembangkan menerapkan kedua algoritma diatas dan membuktikan penyisipan pesan dalam citra aman berdasarkan hasil pengujian yang dilakukan.

2. METODE PENELITIAN

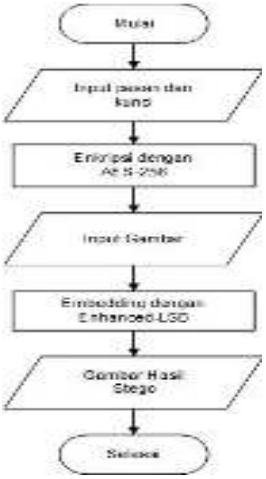
Pengujian yang akan digunakan pada penelitian ini meliputi pengujian terhadap *fidelity,* ukuran citra hasil dan *recovery* dari citra hasil penyisipan. Pengujian *fidelity* bertujuan untuk memastikan kualitas citra setelah disipkan dengan membandingkan nilai rasio citra dengan metode PSNR (Peak Signal to Noise Ratio) setelah disisi pesan enkripsi. Pengujian *recovery* dapat dibuktikan dengan kemampuan aplikasi untuk melakukan ekstraksi pesan dari citra hasil berupa pesan terenkripsi kemudian mendekripsi pesan menjadi plainteks semula serta memastikan tidak adanya (tidak signifikan) perubahan ukuran citra setelah proses penyisipan sehingga dapat menghindari kecurigaan pihak lain.

2.1 Analisis Masalah

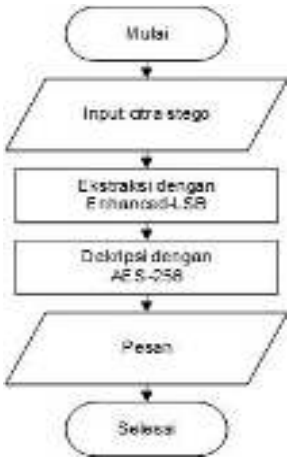
Proses penyisipan pesan yang telah di enkripsi pada citra tentu memiliki beberapa permasalahan termasuk untuk mengecek apakah pesan sudah benar dan tepat disisipkan dalam citra, citra hasil penyisipan juga tidak membuat kecurigaan pada pihak lain karena ukuran citra hasil yang menjadi besar. Pesan yang disisipkan ke dalam citra tidak bisa berupa data selain teks dan proses penyisipan dapat dilakukan jika pesan sudah terenkripsi (chiperteks). Aplikasi yang akan dikembangkan harus mampu menyelesaikan permasalahan tersebut, baik dari segi keamanan, ukuran dan *fidelity*

2.2 Analisis Proses

Pada bagian ini akan menjelaskan bagaimana cara kerja dari algoritma AES (*Advanced Encyption Standart*) dan algoritma E-LSB (*Enhanced Least Significant Bit*) yang terdiri dari proses enkripsi sampai proses penyispan yang ditunjukkan pada gambar 1, dan poses ekstraksi dan proses dekripsi yang ditunjukkan pada gambar 2.

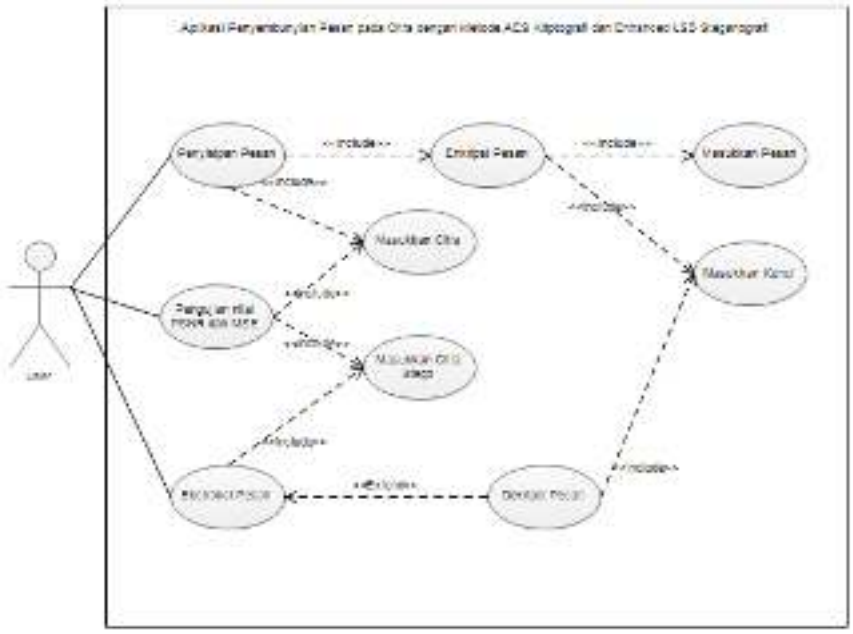


Gambar 1. Flowchart Proses Penyisipan.



Gambar 2. Flowchart proses Ekstraksi.

Pemodelan sistem dengan use case pada gambar 3 dibawah digunakan untuk memudahkan pemahaman dari sistem yang dibuat sesuai dengan kebutuhan dan fungsi yang ada.



Gambar 3. Pemodelan sistem dengan Use Case

2.3 Kriptografi

Kriptografi adalah sebuah teknik rahasia di dalam penulisan dengan karakter khusus, dengan menggunakan huruf dan karakter diluar bentuk aslinya, atau dengan metode lain yang hanya dapat dipahami oleh pihak-pihak yang memiliki kunci, juga semua hal yang ditulis dengan cara seperti ini [4]. Terdapat dua proses penting dalam kriptografi yang berperan dalam merahasiakan informasi yakni enkripsi (*Encryption*) dan deskripsi (*Decryption*). Proses enkripsi dan deskripsi pada umumnya membutuhkan penggunaan sejumlah informasi yang rahasia yang sering disebut kunci (*Key).*

2.3.1 Algoritma AES (Advanced Encryption Standard)

AES merupakan algoritma penyandian pesan yang telah diresmikan oleh lembaga standar Amerika Serikat NIST (*National Institute of Standards and Technology*). AES sendiri merupakan algoritma kriptografi yang bersifat simetris. Dengan kata lain algoritma ini mempergunakan kunci yang sama saat proses enkripsi dan dekripsi [5].

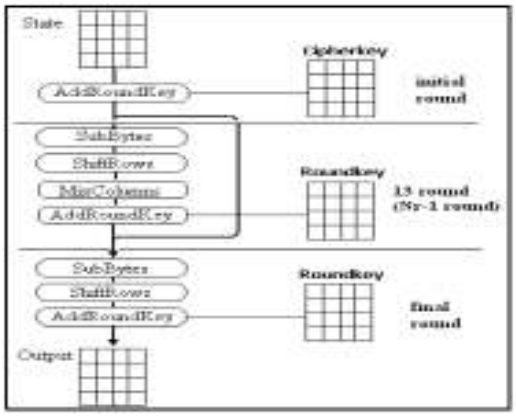
Untuk algoritma AES NIST memberikan spesifikasi terhadap panjang *block input*, *output*, dan *state* adalah 128 bit dinyatakan dengan Nb = 4 yang menunjukkan 32-bit words pada *chiper key*, dan untuk algoritma AES panjang kunci atau *chiper key* adalah 128, 192, dan 256 bit yang dinyatakan dengan Nk = 4, 6, 8 [3]. Tabel 1 memperlihatkan panjang kunci, besar *block*, dan jumlah *round* pada algoritma AES.

Tabel 1 Kombinasi kunci, block, dan round.[6]

	Key Length *(Nk words)*	Block Size *(Nb words)*	Number of Rounds *(Nr)*
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

2.3.2 Enkripsi AES-256 bit

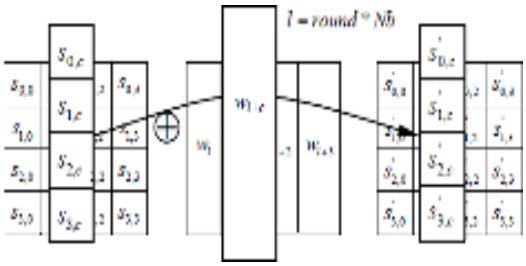
Algoritma AES menggunakan subtitusi, permutasi, dan sejumlah putaran (chipper berulang), dimana setiap putaran menggunakan kunci yang berbeda, kunci setiap putaran disebut sebagai *round* key. Gambar 1 memperlihatkan diagram proses enkripsi Algoritma AES-256 bit[7].



Gambar 4. Diagram Proses Enkripsi AES-256 bit. [7]

Untuk melakukan enkripsi diperlukan 4 proses transformasi *bytes*, yaitu *SubBytes*, *ShiftRows*, *Mixcolumns*, dan *AddRoundKey*. Dan pada putaran terakhir, yaitu putaran ke Nr-1 dilakukan transformasi serupa dengan putaran lain namun tanpa transformasi *MixColumns* [5]. Secara garis besar proses enkripsi AES-256 bit adalah sebagai berikut:

1. Transformasi *AddRoundKey*: pada transformasi ini, *state awal* (plainteks) di *XOR*-kan dengan state kunci. Tahap ini juga disebut *initial Round*. Ilustrasi dari transformasi *AddRoundKey* dapat dilihat pada gambar 5.

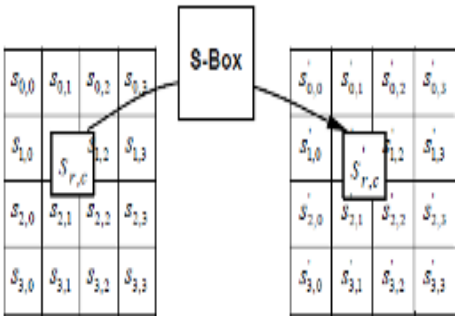


Gambar 5 Ilustrasi Transformasi AddRoundKey.[6]

2. Transformasi *SubBytes*: merupakan operasi yang melakukan substitusi tidak linear pada setiap *byte* dari $S_{0,0}$ sampai dengan $S_{3,3}$. Ada 2 cara melakukan perhitungan *SubByte* dengan cara mengganti setiap *byte state* dengan *byte* pada sebuah tabel S-Box, atau dengan melakukan perhitungan GF (2^8) [7]. Tabel S-Box dapat dilihat pada tabel 2. Gambar 6 merupakan ilustrasi dari transformasi *SubByte*.

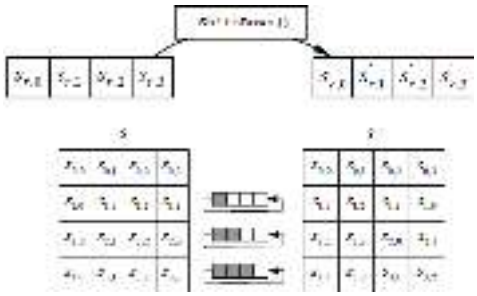
Tabel 2. S-Box [6].

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16



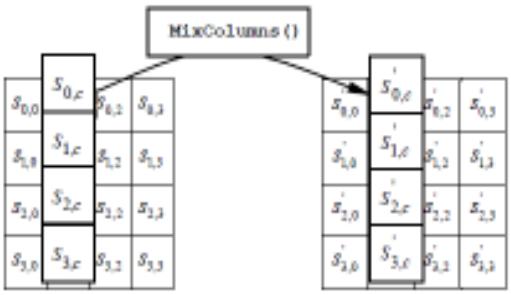
Gambar 6 Transformasi SubByte[6].

3. Transformasi *ShiftRows*: beroperasi pada tiap baris dari tabel *state*. Proses ini bekerja dengan cara mengeser *byte-byte* pada 3 baris terakhir (baris 1, 2, dan 3) dengan jumlah perputaran bergantung pada jumlah baris dan tidak melebihi Nb, dengan nilai Nb adalah 4 word dapat dilihat pada tabel 1. Dimana *byte* pada baris ke-1 akan digeser ke kiri sebanyak 1 kali, *byte* pada baris ke-2 akan digeser ke kiri sebanyak 2 kali, dan *byte* pada baris ke-3 akan digeser ke kiri sebanyak 3 kali. Sedangkan baris 0 tidak mengalami pergeseran. Ilustrasi dari transformasi *ShiftRows* dapat dilihat pada gambar 7.



Gambar 7 Ilustrasi Transformasi ShiftRows.[6]

4. Transformasi *MixColumns*: adalah mencampur nilai kolom-kolom pada suatu elemen pada satu elemen pada *state* keluaran [8]. Transformasi *MixColumns* beroperasi pada tiap kolom dari *state* dengan memperlakukan setiap 4 byte pada kolom *state* sebagai polinomial empat suku dalam Galois field atau GF (2^8) dan modulo (x^4+1) kemudian dikalikan dengan polinom tetap a(x), dinyatakan sebagai berikut $a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$. Ilustrasi dari transformasi *MixColumns* dapat dilihat pada gambar 8.



Gambar 8 Ilustrasi Transformasi MixColumns. [6]

5. Transformasi *AddRoundKey*: Untuk setiap tahap proses enkripsi berikutnya yang digunakan adalah state dari hasil *MixColumns* di *XOR* kan dengan sub kunci yang dibangkitkan dari kunci utama dengan menggunakan proses *key schedule*. Ilustrasi *AddRoundKey* dapat dilihat pada gambar 5
6. *Final Round*: merupakan putaran terakhir dari proses enkripsi AES-256 (Nr-1) transformasi yang digunakan hanya *SubByte*, *ShiftRows*, dan *AddRoundKey*.

2.4 Steganografi

Steganografi berasal dari bahasa Yunani yaitu Steganós yang berarti menyembunyikan dan Graptos yang artinya tulisan, sehingga secara keseluruhan artinya adalah "tulisan yang disembunyikan" atau dapat didefenisikan sebagai "menulis (tulisan) terselubung"[1]. Secara umum steganografi merupakan ilmu yang mempelajari, meneliti, dan mengembangkan seni menyembunyikan sesuatu informasi. Dengan demikian keberadaan informasi tersebut tidak diketahui oleh orang lain. Tujuan dari steganografi adalah menyembunyikan keberadaan pesan dan dapat dianggap sebagai pelengkap dari kriptografi yang bertujuan untuk menyembunyikan isi pesan.

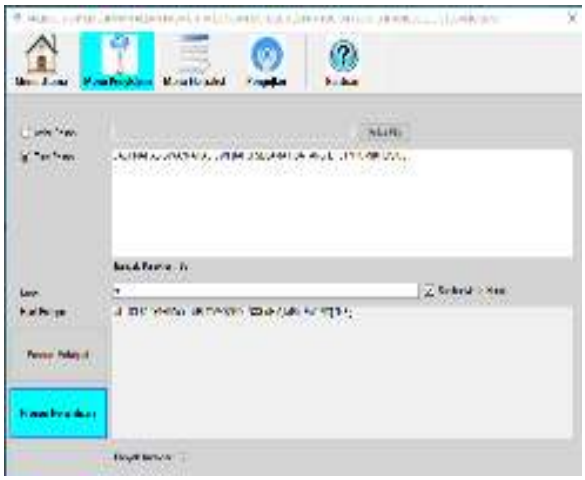
2.4.1 Steganografi *Enhanced Least Significant Bit* (E-LSB)

Tidak jauh berbeda dengan LSB, pada *Enhanced Least Significant Bit* (Enhanced LSB) dilakukan peningkatan dalam penyembunyian pesan yang awalnya hanya penyisipan pada 1 digit paling kanan, kini ditingkatkan dengan formasi 2-3-3 substitusi. Dengan menggunakan Enhanced LSB, keberadaan data yang disembunyikan lebih sulit untuk di deteksi dan dibutuhkan tidak hanya satu warna untuk menyembunyikannya. Sebagai contoh bit data rahasia yang pertama dan kedua di sembunyikan pada *byte* warna merah pada warna RGB, kemudian *byte* warna hijau menyembunyikan bit data rahasia yang ketiga, keempat dan kelima, selanjutnya bit data rahasia keenam, ketujuh dan kedelapan disembunyikan pada *byte* warna biru. Dengan formasi 2-3-3 substitusi ini maka setiap 1 pixel dari citra penampung dapat menampung 1 karakter pesan [8].

3. HASIL DAN PEMBAHASAN

3.1 Hasil

Hasil penelitian yang diperoleh dari uji coba aplikasi yang sudah dibuat terlihat pada gambar 9 dan 10 untuk proses enkripsi dan penyisipan pesan.



Gambar 9. Proses Enkripsi

Gambar 10. Proses Penyisipan.

Untuk melakukan proses ekstraksi pesan dari gambar, terlihat pada gambar 11 dan proses mendekripsi hasil ekstraksi dari gambar ditunjukkan pada gambar 12 dibawah ini. Validasi kunci tetap dilakukan untuk memastikan kunci yang valid terhadap proses dekripsi pesan dari hasil ekstraksi.

Gambar 11. Tampilan Form Menu Ekstraksi

Gambar 12. Tampilan Form Hasil Dekripsi

Gambar 13 merupakan pengujian hasil untuk memproleh nilai dari PSNR dan MSE dari citra hasil penyisipan untuk memastikan proses penyisipan data berhasil, dilakukan dengan mencari nilai MSE dan PSNRnya.

Gambar 13.Tampilan Hasil Form Pengujian

3.2 Pembahasan

3.2.1 Pengujian Pengaruh Panjang Karakter Terhadap Nilai PSNR

Pengujian ini dilakukan untuk mengukur tingkat kualitas dari gambar setelah disisipkan pesan dengan resolusi gambar yang sama dan jumlah karakter pesan yang bervariasi. Dengan menggunakan jumlah karakter pesan yang bervariasi diharapkan dapat mengetahui seberapa besar perubahan yang terjadi pada gambar penampung dengan mengukur besarnya perubahan nilai PSNR dari gambar penampung tersebut.

Tabel 3 Citra Penampung ukuran 259 x 194 piksel.

Nama Gambar	Gambar	Resolusi Gambar
polos.bmp		259 x 194 piksel
Banyak warna.bmp		259 x 194 piksel
Banyak objek.bmp		259 x 194 piksel

Tabel 4 Tabel hasil pengujian dengan jumlah karakter yang bervariasi

Jumlah Karakter Pesan		Gambar polos.bmp	Gambar Banyak warna.bmp	Gambar Banyak objek.bmp
10	MSE	0.003994	0.001818	0.004027
	PSNR	72.117066	75.535525	72.081144
20	MSE	0.006309	0.00548	0.005871

	PSNR	70.131226	70.743231	70.443598
30	**MSE**	0.00672	0.005267	0.005267
	PSNR	69.856937	70.914826	70.914826
40	**MSE**	0.006707	0.007244	0.007981
	PSNR	69.86552	69.530805	69.110375
50	**MSE**	0.008312	0.009347	0.009779
	PSNR	68.93352	68.423921	68.228056
60	**MSE**	0.00814	0.009082	0.009473
	PSNR	69.024585	68.548997	68.365749
70	**MSE**	0.010104	0.011961	0.012432
	PSNR	68.086032	67.353074	67.185335
80	**MSE**	0.009925	0.012963	0.012784
	PSNR	68.163715	67.003786	67.064214
90	**MSE**	0.011736	0.015053	0.014515
	PSNR	67.435753	66.354686	66.512558
100	**MSE**	0.015172	0.017985	0.016088
	PSNR	66.320369	65.581736	66.065914
110	**MSE**	0.014774	0.018436	0.018436
	PSNR	66.435829	65.474146	65.474146
120	**MSE**	0.018423	0.019643	0.018741
	PSNR	65.477272	65.198647	65.402847
130	**MSE**	0.020904	0.022158	0.02099
	PSNR	64.928547	64.675566	64.910666
140	**MSE**	0.021103	0.022861	0.021401
	PSNR	64.887394	64.539878	64.826387
150	**MSE**	0.022609	0.025428	0.023849
	PSNR	64.588035	64.077643	64.356042
160	**MSE**	0.022682	0.026231	0.023975
	PSNR	64.57404	63.942664	64.33315
170	**MSE**	0.024539	0.029183	0.026662
	PSNR	64.232188	63.479491	63.871851
180	**MSE**	0.027571	0.03122	0.030072
	PSNR	63.726276	63.186512	63.349174
190	**MSE**	0.028142	0.03049	0.029528
	PSNR	63.637324	63.289231	63.428455
200	**MSE**	0.030298	0.032845	0.0311
	PSNR	63.316721	62.966102	63.203155

Dari tabel 4 dapat dilihat bahwa jumlah karakter pesan yang disisipkan pada setiap gambar penampung berpengaruh terhadap nilai PSNR yang dihasilkan atau dengan kata lain semakin banyak

karakter pesan yang disisipkan ke dalam gambar penampung, maka semakin berkurang kualitas gambar yang dihasilkan.

3.2.2 Pengujian Fidelity dan Recovery dari Kriteria Steganografi

Pengujian *Fidelity* dilakukan dengan melakukan penyisipan pesan dengan pesan adalah "PESANPESAN" dan kunci adalah "KUNCI" yang terlebih dahulu harus dienkripsi. Hasil dari pengujian yang ketiga untuk kriteria *fidelity* dan *recovery* dapat dilihat pada tabel 5.

Tabel 5 Hasil Pengujian Fidelity dan Recovery dari Kriteria Steganografi

Nama Citra yang diinput	Pengujian Kriteria Fidelity		Pengujian Kriteria Recovery
	Ukuran Citra Awal	Ukuran Citra Akhir	Berhasil/ Tidak
Chrysanthemum.bmp	3.05 kb	3.05 kb	Berhasil
Hydrangeas.bmp	12.0 kb	12.0 kb	Berhasil
Jellyfish.bmp	48.0 kb	48.0 kb	Berhasil
Pinguin.bmp	192 kb	192 kb	Berhasil
Tulips.bmp	768 kb	768 kb	Berhasil
polos.bmp	147 kb	147kb	Berhasil
Banyak warna.bmp	147 kb	147 kb	Berhasil
Banyak objek.bmp	147 kb	147kb	Berhasil

Hasil pengujian untuk kriteria *fidelity* dan *recovery* berdasarkan tabel 5 disimpulkan bahwa algoritma *Enhanced LSB* memenuhi kriteria steganografi untuk *fidelity* dan *recovery.* Tidak terjadi perubahan mutu dan ukuran penampung pada saat gambar penampung sudah disisipkan pesan dan pesan yang disisipkan sebelumnya dapat diekstrak tanpa kehilangan isi pesan.

4. KESIMPULAN

Dari hasil pengujian yang telah dilakukan, maka dapat diambil kesimpulan sebagai berikut:

1. Berdasarkan perhitungan nilai PSNR tidak didapat nilai dibawah 30 dB yang menunjukkan bahwa kualitas gambar cukup baik dan secara kasat mata tidak terlihat perubahan yang terjadi pada gambar.
2. Ukuran pesan akan mempengaruhi kualitas gambar ditinjau dari nilai PSNR yang didapatkan.
3. Algoritma *Enhanced Least Significant Bit* memenuhi 2 kriteria steganografi yang baik yaitu *fidelity* dan *recovery*.

5. SARAN

Adapun saran yang dapat disampaikan untuk pengembangan sistem lebih lanjut adalah kombinasi algoritma AES (*Advanced Encryption Standard*) dan algoritma *Enhanced Least Significant Bit* (E-LSB) dapat dikombinasikan lagi dengan algoritma lain agar diperoleh hasil yang lebih baik dan aplikasi yang lebih handal, seperti penambahan algoritma kompresi gambar agar gambar yang diperoleh dari aplikasi tersebut memiliki ukuran yang lebih kecil seperti algoritma RLE (*Run Length Encoding*), Entropy Encoding (Huffman, Aritmatik), *Adaptive Dictionary Based* (LZW), kemudian file yang ingin disisipkan ke dalam media gambar tidak hanya file *.txt saja tetapi dapat berupa file lainnya seperti file audio, video, dan sebagainya

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada semua pihak yang telah memberi dukungan moril dan materil terhadap penelitian ini.

DAFTAR PUSTAKA

[1] A. Singh and S. Malik, "Securing Data by Using Cryptography with Steganography," *International Journal of Advanced Research in Computer Science and Software Engineering,* vol. 3, no. 5, 2013.

[2] Sumitra, "Comparative Analysis of AES and DES Security," *International Journal of Scientific and Research Publication,* vol. 3, no. 1, 2013.

[3] P. E, "Case Based Reasoning untuk Mengindentifikasi Kerusakan Bangunan," Program Pasca Sarjana Ilmu Komputer, Universitas Gadjah Mada, Yogyakarta, 2006.

[4] Talbot, J., dan Welsh, D., 2006, Complexity and Cryptography An Intoroduction, Cambridge University Press, tersedia pada: http://cryptome.org/2013/01/aaron-swartz/Crypto-Complexity.pdf, tanggal akses : 10 Mei 2015.

[5] Sumitra, 2012, Comparative Analysis of AES and DES security Algorithms, Advanced Institute of Technology & Management, Palwal.

[6] NIST, "Advanced Encryption Standard (AES)," Federal Information Processing Strandard Publication 197, 2001.

[7] R. Munir, Kriptografi, Bandung: Penerbit Informatika, 2006.

[8] R. Sadikin, Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java, Yogyakarta: Andi, 2012.

[9] Castleman, Kenneth R., 2004, *Digital Image Processing*, Vol. 1, Ed.2, Prentice Hall, New Jersey.

[10] Gonzales, R., P. 2004, *Digital Image Processing* (*Pemrosesan Citra Digital*), Vol. 1, Ed.2, diterjemahkan oleh Handayani, S., Andri Offset, Yogyakarta.