STEGANOGRAFI ENHANCED LEAST SIGNIFICANT BIT PADA KARAKTER KHUSUS CITRA TULISAN ARAB

ENHANCED LEAST SIGNIFICANT BIT STEGANOGRAPHY TO ARABIC SPECIAL CHARACTER

Neng Anggi Iliadi[1], Bambang Hidayat[2], Nur Andini[3]
[1,2,3]Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro – Universitas Telkom
Jl.Telekomunikasi No.1, Dayeuh Kolot, Bandung 40257 Indonesia anggiiliadi@telkomuniversity.ac.id[1], bhidayat@telkomuniversity.ac.id[2], nurandini@telkomuniversity.ac.id[3]

ABSTRAK

Saat ini pertukaran informasi dapat dilakukan dengan sangat mudah. Misalnya saja, saat ini sudah banyak cara untuk mengirimkan suatu informasi dari pengirim ke penerima pada jarak yang cukup jauh. Salah satunya dengan melalui internet. Ditengah-tengah perkembangan teknologi informasi yang kian semarak, internet tidak lagi menjamin penyediaan informasi yang aman. Berbagai mesin-pencari (*search-engine*) terus berkembang ditambah dengan serangan *virus*, penyadap, *spam* maupun *hacker* yang menjamur dapat mencuri data-data yang bisa bersifat rahasia. Oleh karena itu, untuk meningkatkan keamanan terhadap informasi dapat dilakukan upaya dengan menyembunyikan pesan kedalam suatu media lain. Teknik tersebut disebut dengan teknik steganografi. Pada penelitian ini dirancang sebuah simulasi dan analisis steganografi teks sebagai pesan dengan menggunakan citra tulisan Arab sebagai *cover*. Sistem ini dirancang meliputi proses segmentasi untuk mendapatkan tanda baca "*fathah*" yang akan digunakan sebagai *host* dan proses steganografi menggunakan metode penyisipan *Enhanced Least Significant Bit* (ELSB). Dengan hasil yang diperoleh dari penelitian ini adalah mendapatkan tanda baca "*fathah*" dengan akurasi rata-rata pada tiga sumber data, diantaranya: *Scan* Al-Qur"an sebesar 85.43%, Google sebesar 89.10% dan *Scan* Tulisan Tangan sebesar 87.78%. Penggunaan metode penyisipan ELSB berhasil menyisipkan pesan dengan tidak merusak kualitas citra dari citra aslinya dengan nilai PSNR terendah sebesar 145.925 dB dan nilai MSE terbesar sebesar 0.0299, didapatkan pada Data 6 - Google dengan panjang pesan sebesar 287 karakter. Hasil *Mean Opinion Score* (MOS) untuk pengujian kualitas citra dengan skala maksimum 5, menunjukkan nilai rata-rata total sebesar 4.58. Dengan skema 1 dapat bertahan terhadap manipulasi berupa *cropping* pada data stego, tetapi rentan terharap serangan *noise gaussian* dann *salt and pepper* dengan *density* 0.01 dengan nilai maksimum pada BER 0.50463 dan CER 0.37037. Sedangkan dengan manipulasi cropping pada skema 2, didapatkan BER 0.4475 dan CER 0.0185, tetapi dapat bertahan dari serangan *gaussian* dan *salt and pepper* pada semua *density* pengujian. Serta waktu komputasi terbesar pada Data 8 – Google dengan panjang pesan sebesar 786 karakter, memiliki waktu penyisipan 3.8596 detik dan waktu ekstraksi 5.3717 detik.

Kata Kunci : **Segmentasi, Tulisan Arab, Steganografi, *Enhanced Least Significant Bit***

ABSTRACT

Currently the exchange of information can be done very easily. For example, now many ways to transmit the information from the sender to the receiver at a considerable distance. One of them is through the internet. Amid the development of information technology is more lively, the internet is no longer ensure the provision of secure information. Various search-engine continues to grow coupled with the virus, bugs, spam and hackers who can steal mushrooming data can be confidential. Therefore, to improve the security of the information can be made an attempt to hide a message into other media. The technique called steganography techniques. In this final project designed a simulation and analysis of text steganography as a message using the Arabic as a cover image. The system is designed include the segmentation process to get the punctuation "fathah" that will be used as a host and steganography using Enhanced Least Significant Bit (ELSB). And the results of this final project is to get the punctuation "fathah" with an average accuracy on three sources of data, such as:85.43% from Scan Qur'an, 89.10% from Google and 87.78% from Scan Handwriting. Use of the method ELSB successfully insert message by not damaging the image quality of the original image with the PSNR VALUE lowest of 145 925 dB and MSE value lagest of 0.0299, obtained on Data 6 - Google with the message length of 287 characters. Results Mean Opinion Score (MOS) for testing image quality with a maximum scale of 5, shows the average value of a total of 4,58. With the first scheme can withstand manipulations such as cropping stego data, but vulnerable against to attack gaussian noise dann salt and pepper with 0,01 density with maximum BER value at 0.50463 and CER value at 0.37037. While the manipulation cropping in the second scheme, obtained BER value at 0.4475 and CER value at 0.0185, but can withstand the attack gaussian and salt and pepper on all density testing. As well as the largest computing time on Data 8 - Google with the message length of 786 characters, has a 3.8596 second insertion and extraction time of 5.3717 seconds.

Keywords: Segmentation, Arabic, Steganography, Enhanced Least Significant Bit

1. Pendahuluan

Steganografi adalah sebuah ilmu dan seni menyembunyikan pesan rahasia di dalam suatu media sehingga keberadaan pesan tersebut sulit untuk diidentifikasi. Steganografi membutuhkan dua properti: wadah penampung atau biasa disebut sebagai *host* dan data rahasia yang akan disembunyikan ke dalam *host* disebut pesan (*message*). Dengan penelitian sebelumnya analisis dan simulasi steganografi pada sinyal audio tiga dimensi berbasis *Enhanced Least Significant Bit* (ELSB) dapat disimpulkan bahwa dengan rancangan sistem audio steganografi dengan metode penyisipan yang telah disimulasikan mampu bekerja dengan baik. Tetapi sistem tersebut tidak tahan terhadap berbagai serangan. Karena pengujiannya saat pemberian *noise* langsung pada data yang tidak terkena *channel coding* dan modulasi[3]. Oleh karena itu, ada penelitian ini dibuat suatu sistem yang dapat mengelola teknik steganografi pada citra tulisan Arab. Dimana tulisan Arab sendiri merupakan satu tulisan yang menghadirkan tantangan khusus untuk aplikasi pengenalan karakter[5]. Citra tulisan Arab tersebut selanjutnya dilakukan proses pendeteksian tanda baca "*fathah*" yang akan dijadikan *host* pada sistem steganografi. Untuk pemilihan tempat penyisipan (*host*) pada tanda baca "*fathah*" ini dilakukan untuk mendapatkan keamanan yang lebih baik dari proses steganalisis (*fidelity* tinggi) dibandingkan pada keseluruhan citra[4]. Selanjutnya pada tanda baca "*fathah*" tersebut disisipkan pesan (*message*) berupa teks dengan menggunakan metode *Enhanced Least Significant Bit* (ELSB). Sistem ELSB ini merupakan modifikasi dari LSB, dimana ELSB ini berkerja dengan dua skema. Skema pertama adalah dengan mengacak nomor bit dari *file host* yang digunakan untuk *embedding* pesan. Sedangkan cara kedua adalah dengan mengacak sampel *host* yang mengandung bit pesan berikutnya[3].

2. Dasar Teori

A. Steganografi

Steganografi berasal dari bahasa Yunani *steganos* yang artinya "tersembunyi" dan *graphein* yang artinya "menulis". Steganografi (*steganography*) adalah ilmu dan seni menyembunyikan pesan rahasia (*hiding message*) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia [7]. Dalam pengimplemantasiannya, steganografi menggunakan berbagai macam objek multimedia baik sebagai *host* maupun *message* seperti *file* citra, audio, teks atau video.

B. *Enhanced Least Significant Bit Steganography* (ELSB)

Enhanced Least Significant Bit merupakan modifikasi dari metode *Least Significant Bit*. Metode ini dapat dilakukan dengan dua cara. Cara pertama adalah dengan mengacak nomor bit dari *file host* yang digunakan untuk *embedding* pesan. Sedangkan cara kedua adalah dengan mengacak sampel *host* yang mengandung bit pesan berikutnya. Pada ELSB, letak bit pada *host* yang digunakan untuk menyisipkan pesan tidak selalu sama. Pamilihan bit untuk meletakkan bit-bit pesan mempunyai aturan sebagai berikut.

Tabel 1. Skema Pemilihan Letak Bit Pesan [2]

MSB Pertama	MSB Kedua	Letak bit pesan pada *host*
0	0	LSB 3
0	1	LSB 2
1	0	LSB 1
1	1	LSB 1

Selain pemilihan letak bit untuk menyimpan bit dari pesan, dilakukan juga pemilihan *sample* yang digunakan untuk penyisipan bit pesan. Tabel 2 di bawah ini menunjukkan skema pemilihan *sample* dari *file host.*

Tabel 2. Skema Pemilihan Sampel [2]

MSB Pertama	MSB Kedua	MSB Ketiga	Sampel yang berisi bit pesan berikutnya
0	0	0	i+1
0	0	1	i+2
0	1	0	i+3
0	1	1	i+4
1	0	0	i+5
1	0	1	i+6
1	1	0	i+7
1	1	1	i+8

C. Citra Digital

Citra digital dapat dinyatakan sebagai suatu fungsi dua dimensi *f(x,y)*, dimana x maupun y adalah posisi koordinat sedangkat *f* merupakan amplitude pada posisi *(x,y)* yang sering dikenal sebagai intensitas atau grayscale. Nilai intensitas tersebut dalam bentuknya diskrit dari mulai 0 sampai dengan 255 [6].

Dalam komputer, citra digital disimpan sebagai suatu *file* dengan format tertentu. Format citra tersebut menunjukkan cara sebuah citra digital disimpan, misalnya apakah dengan suatu kompresi atau tidak. Contoh format citra yang digunakan pada proses steganografi ini adalah.BMP. Format BMP adalah format penyimpanan standar tanpa kompresi yang umum dapat digunakan untuk menyimpan citra biner hingga citra warna [6].

Selain format memiliki penyimpanan, citra digital juga dapat menampilkan warna yang merupakan kombinasi dari tiga warna dasar, yaitu merah, hijau, dan biru (*Red, Green, Blue*) yang disebut citra RGB. Setiap warna merupakan 1 layer (*gray-scale*) yang memiliki rentang nilai dari 0 sampai 255. Citra RGB memiliki kapasitas penyimpanan 8 bit per-*layer*nya. Dengan skala 256 per-*layer*nya, citra RGB memiliki warna total sebanyak 16.777.216 warna. Sedangkan pada citra, *black white* merupakan warna citra yang mewakili hitam dan putih. Pada MATLAB, nilai nol adalah hitam dan satu adalah putih.

D. Tanda Baca Pada Tulisan Arab

Tanda baca atau lambang-lambang yang menyertai setiap huruf Arab yang berfungsi memberi sifat baca setiap huruf sehingga ia menjadi sebuah suku kata. Huruf Arab bisa dikatakan semua hurufnya konsonan. Walaupun ada huruf „alif" (a), ia adalah konsonan karena alif juga dibentuk oleh tanda baca dan akan menjadi suku kata sendiri. Alif bisa menjadi „i" dan bisa juga menjadi „u". Perlu diketahui, dalam bahasa Arab hanya ada tiga bentuk penyebutan vocal yaitu „a", „i" dan „u".

E. Parameter Pengujian

1. *Peak Signal-to-Noise Ratio* (PSNR)

PSNR merupakan nilai perbandingan antara harga maksimum dari intensitas citra terhadap *error* citra yaitu MSE. Untuk menghitung nilai PSNR digunakan persamaan 1 berikut [8]:

$$PSNR = 20 \log_{10} \frac{Ps}{\sqrt{MSE}} \quad \text{..... (1)}$$

Dimana, Ps = Daya Sinyal
MSE = Nilai Rata-rata Kuadrat *Error*

2. *Mean Square Eror* (MSE)

Mean Square Error (MSE) adalah rata-rata nilai error antara citra *cover* dengan citra stego. Secara matematis, *Mean Square Error* (MSE) dapat dirumuskan pada persamaan 2 sebagai beriku [8]:

$$MSE = \frac{1}{N}\sum_{N}^{N-1}[I_i - I'_i]^2 \quad \text{..... (2)}$$

Dimana, I(i) = data *host*, I"(i) = data stego, N = panjang data

3. *Character Error Rate* (CER)

CER merupakan persentase karakter penyisipan yang mengalami *error* dengan jumlah keseluruhan karakter pada citra stego. CER dihitung dengan menggunakan persamaan 3 sebagai berikut [8]:

$$CER = \frac{\text{Karakter Salah}}{\text{Panjang Pesan}} \quad \text{..... (3)}$$

4. *Bit Error Rate* (BER)

Jumlah bit yang salah dihitung dengan cara membandingkan setiap *file* citra sisipan asli dengan citra sisipan hasil ekstraksi. Persamaan *Bit Error Rate* tersebut dapat dihitung sebagai persamaan 4 berikut [8]:

$$BER = \frac{\Sigma \text{Bit Salah}}{\Sigma \text{Bit Total}} \quad \text{..... (4)}$$

5. *Mean Opinion Score* (MOS)

Mean Opinion Score (MOS) adalah parameter subjektif yang membandingkan perubahan objek sebelum dan sesudah disisipi informasi. Parameter ini dilakukan dengan menggunakan HVS (*Human Visual System*) atau sistem penglihatan manusia. Menurut ITU-T kriteria MOS adalah sebagai berikut:

Tabel 3. Kriteria Penilaian MOS Penyisipan Pesan (Rekomendasi ITU-T)

MOS	*Quality*	*Impairment*
5	Sangat Baik	Sangat Bagus
4	Baik	Bagus
3	Cukup	Sedang
2	Sedikit rusak	Buruk
1	Buruk Rusak Sangat	Sangat Buruk

Untuk menjamin diperolehnya hasil yang objektif dalam menggunakan parameter MOS, maka dibutuhkan minimal 30 responden atau lebih.

6. Akurasi

Akurasi adalah ukuran ketepatan sistem dalam mengenali input yang diberikan sehingga menghasilkan keluaran yang benar. Secara sistematis dapat dituliskan sebagai berikut :

$$akurasi = \frac{\Sigma True\ Positif - \Sigma True\ Negatif}{\Sigma Positif} \times 100\% \quad (5)$$

Dimana,

$akurasi$ = Akurasi

$\Sigma True\ Positif$ = Jumlah *fathah* yang benar dan dikenali

$\Sigma True\ Negatif$ = Jumlah tanda baca yang dikenali tetapi bukan *fathah*

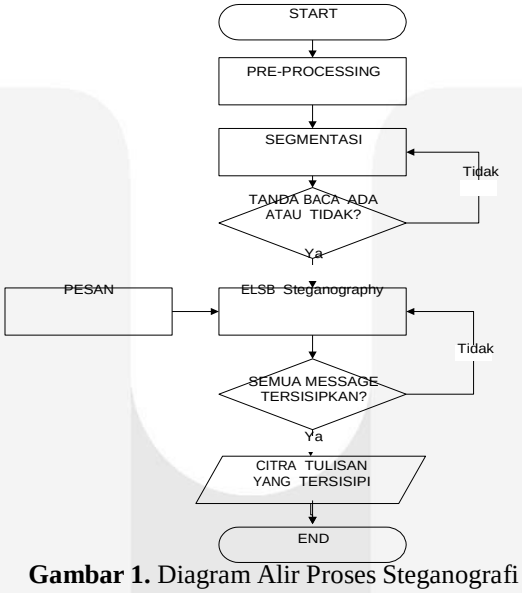
$\Sigma positif$ = Jumlah *Fathah* seluruhnya pada data

7. Waktu Komputasi

Waktu komputasi adalah waktu yang dibutuhkan sistem untuk melakukan suatu proses. Pada sistem ini, waktu komputasi dihitung dimulai pada proses penyisipan dan proses ekstraksi dari pertama sampai selesai.

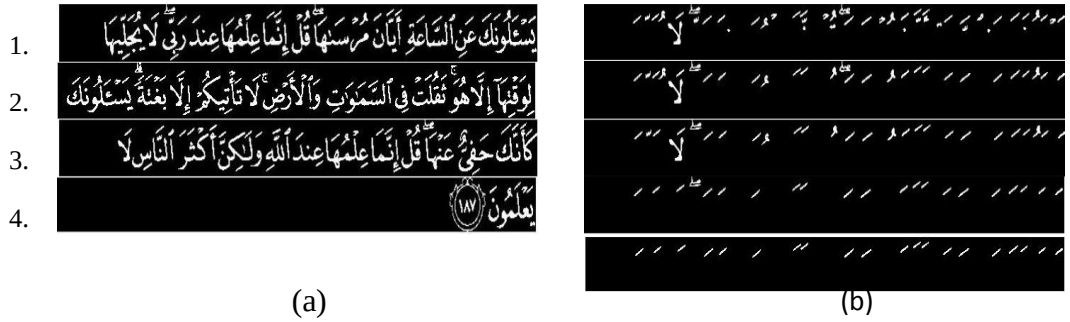
3. Perancangan Sistem

Pada Tugas Akhir ini, metode steganografi yang akan digunakan adalah *Enhanced Least Significant Bit* (ELSB). Secara garis besar, proses yang akan dilakukan dapat dilihat pada gambar 1. di bawah ini.



Gambar 1. Diagram Alir Proses Steganografi

Dimulai dengan proses *pre-processing* sistem ini dimulai, *yaitu* terdiri dari citra *black and white* dan invers dari citra *black and white*. Hal tersebut dilakukan untuk mempermudah proses selanjutnya, yaitu segmentasi karakter yang bertujuan mendapatkan tanda baca "*fathah*" yang akan dijadikan tempat untuk penyisipan pesan (*host*). Berikut gambar 2 adalah ilustrasi dari proses segmentasi karakter "*fathah*"sebagai berikut:



Gambar 2. (a) Ilustrasi Segmentasi Perbaris (b) Ilustrasi Mendapatkan Letak Fathah pada Baris 1

Pada tanda "*fathah"* tersebut, akan dilakukan proses penyisipan dengan menggunakan ELSB. Dengan aturan pemilihan LSB untuk meletakkan bit pesan mengikuti peraturan pemilihan bit seperti pada tabel 1.

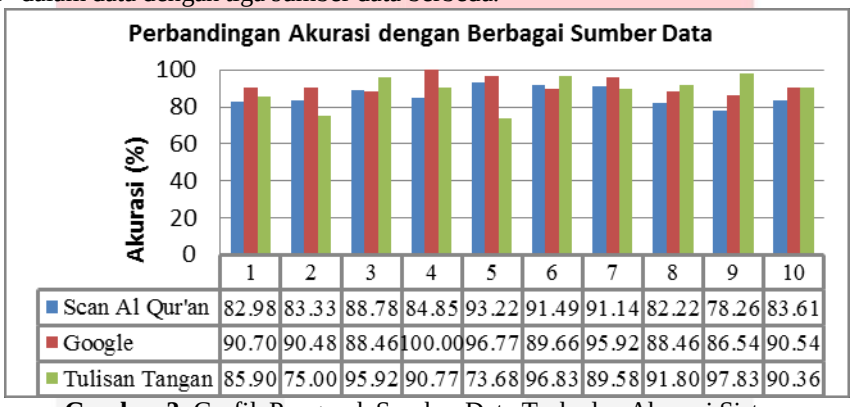
Untuk pemilihan sampel yang akan disisipi pesan dalam bit mengikuti aturan seperti dalam tabel 2. Bit pesan pertama diletakkan di sampel pertama dari *host* dan untuk bit selanjutnya mengikuti kondisi 3 MSB pertama dari sampel pertama.

Sedangkan untuk proses ekstraksi adalah proses kebalikan dari proses penyisipan. Dimana data yang telah tersisipi diubah menjadi bentuk bilangan biner 8 bit, kemudian pemilihan bit dan sampel untuk mendapatkan bit-bit pesan satu-persatu mengikuti aturan ELSB seperti yang ditunjukkan pada tabel 1. dan tabel 2. Bit-bit pesan yang telah didapatkan kemudian diubah menjadi nilai desimal yang mewakili nilai ASCII dari setiap karakter kemudian nilai ASCII tersebut diterjemahkan kembali menjadi deretan karakter. [2]

4. Hasil Pengujian

A. Perbandingan Akurasi Terhadap Tiga Sumber Data

Berikut gambar 3. perbandingan akurasi hasil pengujian proses segmentasi dalam mendapatkan tanda baca "*Fathah*" dalam data dengan tiga sumber data berbeda.



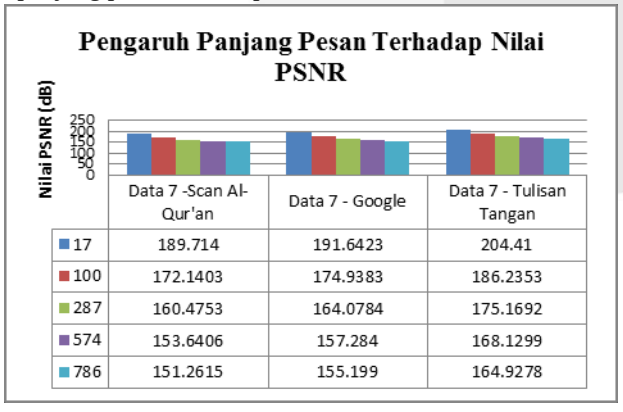
	1	2	3	4	5	6	7	8	9	10
Scan Al Qur'an	82.98	83.33	88.78	84.85	93.22	91.49	91.14	82.22	78.26	83.61
Google	90.70	90.48	88.46	100.00	96.77	89.66	95.92	88.46	86.54	90.54
Tulisan Tangan	85.90	75.00	95.92	90.77	73.68	96.83	89.58	91.80	97.83	90.36

Gambar 3. Grafik Pengaruh Sumber Data Terhadap Akurasi Sistem

Hasil yang diperoleh pada gambar 6 dikarenakan data citra memiliki penulisan tanda baca yang berbeda-beda pada setiap sumber data, dari mulai panjang dan lebar dari tanda baca "fathah" yang kadang terlalu jauh.

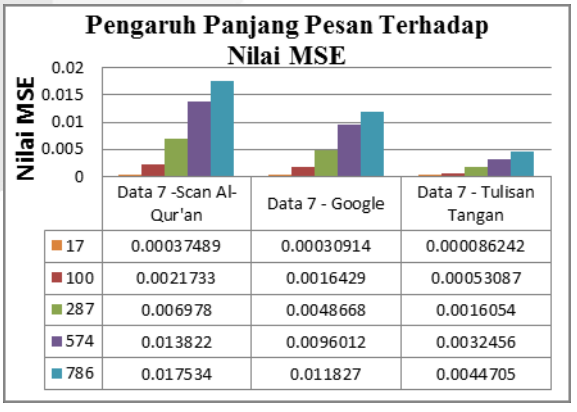
B. Pengaruh Panjang Pesan Terhadap Nilai SNR dan MSE

Tiga sample citra stego dari tiga sumber data disisipkan pesan dengan panjang pesan yang berbeda-beda mulai dari 17, 100, 287, 574 sampai dengan 786 karakter. Semakin panjang pesan teks maka semakin banyak pula bit yang harus disisipkan pada citra *host*, artinya semakin banyak derau atau *noise* yang ditambahkan ke dalam citra *host* tersebut. Berikut ini adalah hasil grafik yang memperlihatkan pengaruh panjang pesan terhadap nilai PSNR dan MSE.



	Data 7 -Scan Al-Qur'an	Data 7 - Google	Data 7 - Tulisan Tangan
17	189.714	191.6423	204.41
100	172.1403	174.9383	186.2353
287	160.4753	164.0784	175.1692
574	153.6406	157.284	168.1299
786	151.2615	155.199	164.9278

(a)



	Data 7 -Scan Al-Qur'an	Data 7 - Google	Data 7 - Tulisan Tangan
17	0.00037489	0.00030914	0.000086242
100	0.0021733	0.0016429	0.00053087
287	0.006978	0.0048668	0.0016054
574	0.013822	0.0096012	0.0032456
786	0.017534	0.011827	0.0044705

(b)

Gambar 4. Pengaruh Panjang Pesan Terhadap (a) Nilai PSNR dan (b) Nilai MSE

Dari gambar 4 terlihat bahwa semakin besar ukuran pesan yang disisipkan maka akan mengakibatkan nilai PSNR semakin menurun, sedangkan nilai MSE yang dihasilkan semakin besar. Pada sistem ini dihasilkan nilai PSNR terendah sebesar 145.925 dB, dan nilai MSE tertinggi sebesar 0.0299. Hal tersebut menunjukan, Nilai PSNR dan MSE tersebut baik yang artinya rata-rata nilai *error* antara citra asli dengan citra stego semakin kecil perbedaannya.

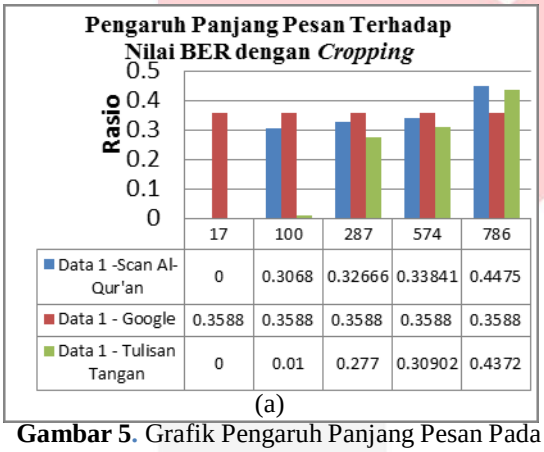
C. Pengaruh Ukuran Pesan Terhadap Nilai BER dan CER

Untuk mengukur kehandalan sistem dibuat 2 skema dengan menggunakan parameter BER dan CER, yaitu: Skema 1 (Steganografi ELSB dengan Segmentasi) dan Skema 2 (Steganografi ELSB tanpa Segmentasi)

1. Pengaruh Cropping Terhadap Nilai BER dan CER

Dengan menggunakan skema 1, nilai BER di hampir semua panjang pesan bernilai 0. Hal tersebut disebabkan proses penyisipan dilakukan hanya pada tanda baca "*fathah*" yang kemungkinan besar seseorang tidak akan melakukan *cropping* terhadap tulisan ataupun tanda baca pada citra *cover*. Maka dapat disimpulkan sistem steganografi ELSB dengan menggunakan proses segmentasi mampu bertahan terhadap serangan *cropping* sehingga mampu mengembalikan bit pesan yang telah disisipkan dengan sangat baik.

Selanjutnya untuk pengujian dengan menggunakan skema 2, yaitu steganografi ELSB tanpa segmentasi (keseluruhan) dengan manipulasi *cropping* dihasilkan perbandingan nilai BER dan CER sebagai berikut:



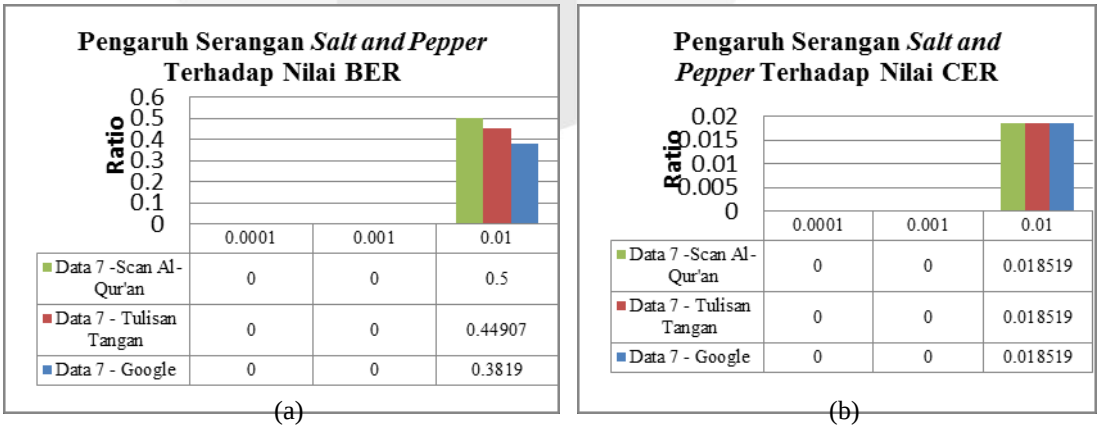
Gambar 5. Grafik Pengaruh Panjang Pesan Pada Skema 2 (a) Nilai BER (b) CER dengan Manipulasi *Cropping*

Hasil yang didapatkan pada gambar 5 dengan menggunakan skema 2 menunjukan sistem steganografi ELSB tanpa proses segmentasi (keseluruhan) rentan terhadap proses manipulasi *cropping*. Hal tersebut dikarenakan bit-bit *cover* yang tersisipi pesan kemungkinan besar terpotong sehingga menyebabkan bit-bit pesan hilang dan pesan tidak dapat terekstrak dengan baik.

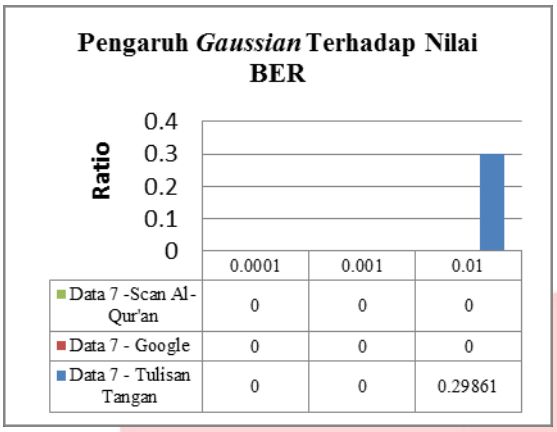
2. Pengaruh Serangan Terhadap Nilai BER dan CER

Data yang diujikan disisipkan pesan "*The Quick Brown Fox Jumps Over The Lazy Dog 0123456789*", kemudian diberi serangan. Berikut perbandingan nilai BER terhadap serangan *noise* dengan *density* yang berbeda-beda:

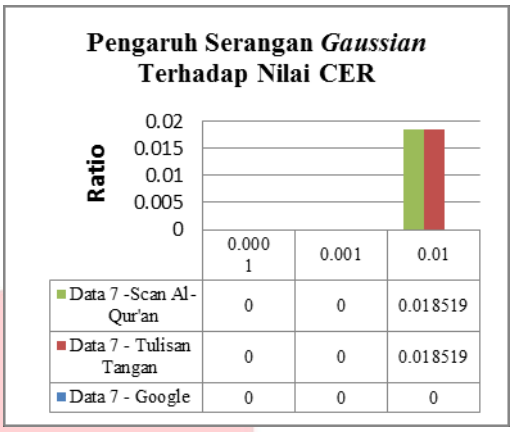
a. Skema 1 (Steganografi ELSB dengan Segmentasi)



Gambar 6. Grafik Pengaruh Serangan *Noise* (a) BER - *Salt and Pepper*



(c)



(d)

Gambar 7. Grafik Pengaruh Serangan *Noise* (c) BER - *Gaussian* (d) CER – *Gaussian*

Berikut hasil pesan yang telah terekstrak dapat dilihat di tabel 3 di bawah ini.

Tabel 3. Pesan Hasil Ekstraksi dengan Serangan

Serangan	Pesan Ekstraksi
Salt and Pepper 0.0001	*The Quick Brown Fox Jumps Over The Lazy Dog 0123456789*
Salt and Pepper 0.001	*The Quick Brown Fox Jumps Over The Lazy Dog 0123456789*
Salt and Pepper 0.01	.)iacCBBDA
Gaussian 0.0001	*The Quick Brown Fox Jumps Over The Lazy Dog 0123456789*
Gaussian 0.001	*The Quick Brown Fox Jumps Over The Lazy Dog 0123456789*
Gaussian 0.01	$ õÐéu©ãã@ªòo÷f¨îçX@JUap{@GVArlp$idhIRLDgC@4qvwUÚ{

Pada Skema 1, pesan dengan *density* 0.01 rusak, hal ini disebabkan serangan yang disebutkan merubah bit pada piksel *host* yang menyebabkan perubahan pada saat bit diubah ke dalam biner. Sehingga terjadi perubahan terhadap nilai-nilai bit pesan yang telah tersisipkan. Hal itu disebabkan karena *density noise* menyebar pada bit-bit pesan yang terkandung pada piksel citra yang menyebabkan bit-bit pesan berubah dari bit pesan aslinya.

b. Skema 2 (Steganografi ELSB Tanpa Segmentasi)

Pada Skema 2, pesan tahan terhadap serangan *salt and pepper* dan *gaussian* dengan berbagai *density*, hal tersebut disebabkan penyebaran *density* yang tersebar merata, sehingga tidak merubah bit pada piksel dan pesan yang disisipkan.

D. *Mean Opinion Score* (MOS)

MOS dilakukan untuk mengetahui kualitas citra setelah disisipkan pesan. Dengan panjang karakter pesan 17, 100, 287, 574 dan 786 karakter. Setelah melakukan survey terhadap 30 responden, didapatkan nilai dengan skala maksimum 5, dengan nilai rata-rata total sebesar 4.58. Dengan kata lain, hasil *Mean Opinion Score* (MOS) dapat dikategorikan baik.

Tabel 4. Pengujian MOS Terhadap Panjang Pesan Pada Tiga Sumber Data

Data 7 – Scan Al-Qur‟an

17		100	287	574	786
5	19	18	18	18	20
4	10	11	10	11	9
3	1	1	2	1	1
2	0	0	0	0	0
1	0	0	0	0	0

Data 7 – Google

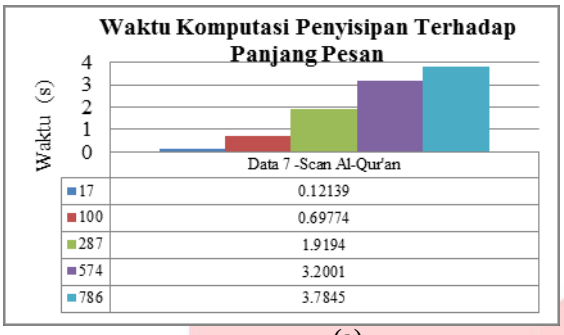
	17	100	287	574	786
5	19	19	18	17	18
4	9	10	10	11	11
3	2	1	2	2	1
2	0	0	0	0	0
1	0	0	0	0	0

Data 7 – Tulisan Tangan

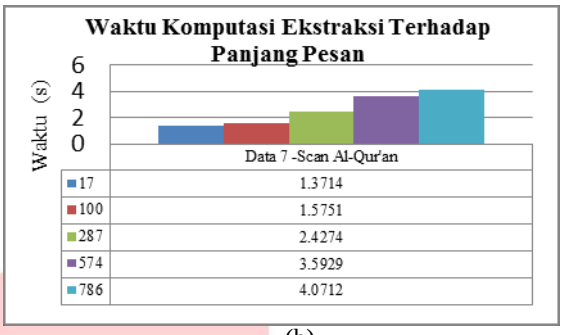
	17	100	287	574	786
5	18	19	19	19	19
4	10	10	10	11	10
3	2	1	1	0	1
2	0	0	0	0	0
1	0	0	0	0	0

E. Waktu Komputasi

Data citra *host* disisipkan pesan dengan berbagai ukuran pesan dari 17, 100, 287, 574 dan 786 karakter. Kemudian dihitung waktu komputasi proses penyisipan dan ketika proses ekstraksi dengan perbandingan panjang pesan yang digunakan sebagai pengujian, yaitu semakin panjang pesan yang digunakan, semakin lama proses penyisipan dan proses ekstraksi pada sistem.



(a)



(b)

Gambar 8. Waktu Komputasi (a) Penyisipan dan (b) Ekstraksi

5. Kesimpulan

Kesimpulan yang dapat diambil dari tahapan perancangan dimulai dengan proses segmentasi karakter untuk mendapatkan tanda baca "*fathah*" diperoleh akurasi rata-rata pada tiga sumber data, diantaranya: *Scan* Al-Qur‟an sebesar 85.43%, Google sebesar 89.10% dan *Scan* Tulisan Tangan sebesar 87.78%. Penggunaan metode penyisipan ELSB berhasil menyisipkan pesan dengan tidak merusak kualitas citra dari citra aslinya dengan nilai PSNR terendah sebesar 145.925 dB dan nilai MSE terbesar sebesar 0.0299, didapatkan pada Data 6 - Google dengan panjang pesan sebesar 287 karakter. Panjang pesan berpengaruh terhadap nilai PSNR dan MSE. Semakin panjang pesan, maka semakin kecil nilai PSNR. Sedangkan, untuk nilai MSE, semakin panjang pesan, maka semakin besar pula nilai MSE yang diperoleh. Hal tersebut menunjukan pengaruh panjang pesan terhadap kapasitas pesan pada *host*, artinya semakin banyak derau atau *noise* yang ditambahkan ke dalam *host*. Hasil *Mean Opinion Score* (MOS) untuk pengujian kualitas citra dengan skala maksimum 5, menunjukkan nilai rata-rata total sebesar 4.58. Dengan skema 1 dapat bertahan terhadap manipulasi berupa *cropping* pada data stego, tetapi rentan terharap serangan *noise gaussian* dann *salt and pepper* dengan *density* 0.01 dengan nilai maksimum pada BER 0.50463 dan CER 0.37037. Sedangkan dengan manipulasi *cropping* pada skema 2, didapatkan BER 0.4475 dan CER 0.0185, tetapi dapat bertahan dari serangan *gaussian* dan *salt and pepper* pada semua *density* pengujian. Serta waktu komputasi terbesar pada Data 8 – Google dengan panjang pesan sebesar 786 karakter, memiliki waktu penyisipan 3.8596 detik dan waktu ekstraksi 5.3717 detik.

REFERENSI

[1] Arifah, N., 2014, "*Steganalisis Pada Citra Digital Dengan Format JPEG Menggunakan Uji Chi- Square*", Fakutas Teknik Elektro, Universitas Telkom : Bandung.

[2] Asad, Muhammad; Gilani, Junaid; Khalid, Adnan., 2011, "*An Enhanced Least Significant Bit Modification Technique for Audio Steganography*", *Telecommunication Engineering Department, University of Engineering and Technology Taxila: Pakistan*.

[3] Hartoko, Carolus Ferdy Setiaji., 2014, "*Analysis and Simulation of Steganography on Three Dimensional Audio Signal Based on Enhanced Least Significant Bit"*. Fakultas Departemen Teknik Elektro dan Komunikasi, Universitas Telkom : Bandung.

[4] Lee, B., Tan, S.; Huang, M.; and Huang, J., 2014, "*Investigation on Cost Assignment in Spacial Image Steganography", IEEE Transactions On Information Forensics And Security*, VOL. 9, NO. 8.

[5] Mousa, Mahmoud A. A.; Sayed, Mohammed S; Abdalla, Mahmoud I., 2013, "*Arabic Character Segmentation Using Projection-Based Approach with Profile's Amplitude Filter*", *Deptartment of Computer and Systems Engineering, Zagazig University, Zagazig: Egypt*.

[6] Purnomo, M. H.; Muntasa, A., 2010, "*Konsep Pengolahan Citra Digital dan Ekstraksi Fiture"*. Graha Ilmu : Surabaya.

[7] Rinaldi, Munir., 2004, "*Steganografi dan Watermarkig"*, Departemen Teknik Informatika, Institut Teknologi Bandung: Bandung.

[8] Sirandan, A.; Magdalena, Rita.; Andini, Nur., 2014, "*Simulasi Dan Analisis Keamanan Teks Menggunakan Metode Steganografi Discrete Cosine Transform (DCT) dan Metode Enkripsi Cellular Automata"*. FakultasTeknik Departemen Elektro dan Komunikasi, Universitas Telkom: Bandung.