SIMULASI DAN ANALISIS KEAMANAN TEKS MENGGUNAKAN METODE STEGANOGRAFI DISCRETE WAVELET TRANSFORM (DWT) DAN METODE ENKRIPSI CELLULAR AUTOMATA

Simulation and analysis of text security using dicrete wavelet transform steganography method and cellular automata encryption method

Tamardi Pranata Tampubolon.[1], Rita Magdalena.[2], Nur Andini.[3]
Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom Bandung
[1] tamardi@students.telkomuniversity.ac.id, [2] ritamagdalena@telkomuniversity.ac.id, [3] nurandini@telkomuniversity.ac.id

Abstrak

Steganografi merupakan teknik menyembunyikan pesan rahasia kedalam *cover* media sehingga orang lain tidak mengetahui isi atau keberadaan dari pesan tersembunyi tersebut. Pesan rahasia yang dikirimkan dapat berupa *text, image, voice,* maupun *video*. Untuk media penyembunyian juga dapat berupa *text, image, voice* maupun *video.* Pada tugas akhir ini dilakukan perancangan sistem dengan metode *Discrete Wavelet Transform* dan metode enkripsi *Cellular Automata*. Kedua metode ini digabungkan dan digunakan untuk menyembunyikan suatu pesan rahasia yang berupa *text* untuk mendapatkan tingkat keamanan yang lebih tinggi. Tugas akhir ini bertujuan untuk menyediakan dua level tingkat keamanan. Pada level pertama menyembunyikan pesan tersebut dengan menggunakan teknik steganografi dan juga menggunakan *password* khusus untuk dapat mengakses informasi yang ada di dalam *text*. Pada tingkat kedua menggunakan sistem 2D *Cellular Automata*. Hasil yang diperoleh dari tugas akhir ini didapatkan citra stego dengan kualitas yang sangat baik diatas (PSNR ≥ 39 dB), dengan nilai MOS (Mean Opinion Score) sekitar 4,6 – 5 didapatkan dari 30 pengamat, dan sebuah citra CA yang berupa gambar tidak jelas tetapi memiliki pesan rahasia di dalamnya, dengan nilai CER yang sangat baik tanpa *noise* pada semua layer *red, green and blue* yaitu 0% dengan batas maksimal jumlah karakter pesan yaitu 8192 karakter. Sistem diuji dengan beberapa gangguan yaitu *noise* Gaussian, *noise* Salt & Paper dan rescale

Abstract

Steganography is a technique to hide secret messages within a cover media so that people will not know the content or the existence of the said message. The sent secret message can be in the form of text, image, voice, and video. The hidden secret message can also be in the form of text, image, voice, or video. This final paper designs a system using Discrete Wavelet Transform method and Cellular Automata encryption method. These two methods are combined and used to hide a secret message in text form to achieve a higher level of security. This final paper aims to provide two levels of security. The first level is to hide a message using steganography and uses a special password to access information within the text. The second level uses a 2D Cellular Automata system. The result of this final paper achieves a stego image with a great quality (PSNR ≥ 35 dB), with a MOS (Mean Opinion Score) around 4.6 -5 acquired from 30 observers and a CA image in poor quality containing a secret message with a CER score that is excellent without noise in all red, green, blue layers (0%) with a maximum character count of 8192 characters. The system is tested with several noise which are Gaussian noise, Salt & Paper noise and Rescale.

1. Pendahuluan

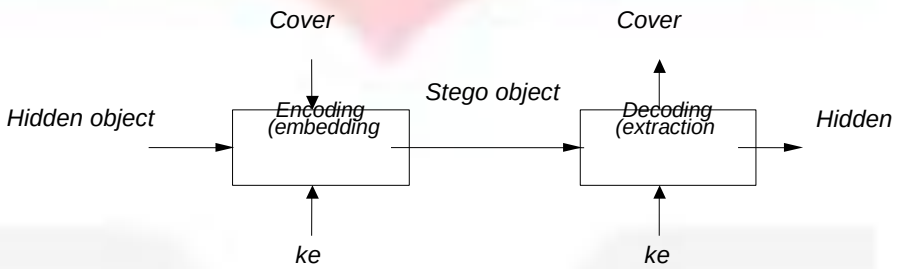
Pada perkembangan teknologi yang semakin pesat saat ini menjadikan pertukaran informasi semakin mudah dan cepat. Informasi sangat penting untuk melanjutkan kelangsungan hidup. Tetapi di sisi lain informasi dapat menjadikan suatu ancaman yang dapat membahayakan. Sehingga kerahasiaan dan keamanan suatu informasi menjadi sesuatu yang sangat penting. Untuk mengamankan suatu informasi dibutuhkan suatu sistem untuk melindungi informasi tersebut. Oleh karena itu, dibuat berbagai macam Metode penyembunyian pesan rahasia yang dinamakan Steganografi. Steganografi merupakan suatu teknik menyembunyikan pesan kedalam media lain sehingga keberadaan pesan tidak diketahui oleh orang lain [1] Dengan berkembangnya steganografi yang ada teknik untuk menjamin kerahasiaan suatu pesan yang di kirimkan. Pesan yang telah disembunyikan ini ternyata pihak-pihak yang tidak berwenang seperti *hacker* mampu untuk membongkar algoritmanya. Hal ini tentunya sangat berbahaya jika pesan yang pesan yang kita kirimkan berisi pesan yang sangat rahasia. Oleh karena itu dalam Tugas Akhir ini dilakukan simulasi proses steganografi dan di tambahkan dengan metode kriptografi untuk mengenkripsi pesan yang telah disembunyikan. Dengan adanya metode ini diharapkan tingkat keamanan suatu pesan yang dikirimkan dapat menyulitkan pihak yang tidak berwenang untuk membaca pesan yang kita kirimkan dan pesan yang dikirimkan sampai dengan aman. Pada Tugas akhir ini dilakukan perancangan sistem pengamanan pesan rahasia berupa *text* dengan menggunakan metode enkripsi *Cellular Automata*. *Cellular Automata* adalah kumpulan sel yang diwarnai pada grid dengan bentuk tertentu yang berkembang melalui sejumlah langkah waktu dikrit sesuai aturan berdasarkan kondisi

sel-sel tetangga. Untuk metode steganografi digunakan metode *Discrete Wavelet Transform* (DWT) dengan membagi citra menjadi subband-subband yang memiliki frekuensi tinggi dan frekuensi rendah. Sehingga dengan menggabungkan kedua metode ini dapat meningkatkan sistem kemanan pesan rahasia yang dikirimkan dengan baik.

2. Dasar Teori /Material dan Metodologi/perancangan

A. Steganografi

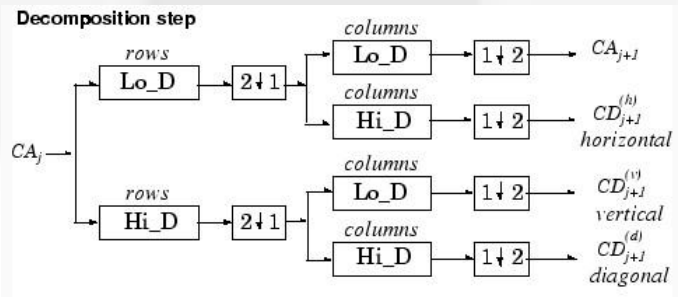
Steganografi berasal dari Bahasa Yunani, yaitu *"steganos"* yang artinya "tulisan tersembunyi *(covered witing)*". Steganografi merupakan ilmu dan seni menyembunyikan pesan rahasia sedemikian sehingga keberadaan pesan tidak terdeteksi oleh indera manusia [2]. Steganografi juga berbeda dengan kriptografi, yaitu terletak pada hasil keluarannya. Hasil dari kriptografi biasanya berupa bentuk data yang berbeda dari bentuk aslinya dan biasanya datanya seolah-olah berantakan (tetapi dapat dikembalikan ke bentuk semula). Sedangkan hasil keluaran dari steganografi ini memiliki bentuk yang sama dengan aslinya, tentunya persepsi disini oleh indera manusia, tetapi tidak oleh computer atau perangkat pengolahan data digital lainnya.



Gambar 1 Proses Steganografi [2]

B. Discrete Wavelet Transform (DWT)

Discrete Wavelet Transform mengubah representasi sinyal waktu diskret ke representasi wavelet diskrit. Transformasi Wavelet selain mampu memberikan informasi frekuensi yang muncul, juga dapat memberikan informasi tentang skala atau durasi waktu.Wavelet dapat digunakan untuk menganalisa suatu bentuk gelombang (sinyal) sebagai kombinasi dari waktu (skala) dan frekuensi. Analisis data pada transformasi wavelet dilakukan dengan cara mendekomposisi suatu sinyal ke dalam komponen frekuensi yang berbeda-beda, dan selanjutnya sesuai dengan skala resolusinya masing-masing, komponen-komponen tersebut dapat dianalisis [4]. Prinsip dasar dari DWT adalah bagaimana cara mendapatkan representasi waktu dan skala dari sebuah sinyal menggunakan teknik pemfilteran digital dan operasi *sub-sampling*. Sinyal pertama-tama dilewatkan pada rangkaian filter *high-pass* dan *low-pass*, kemudian setengah dari masing- masing keluaran diambil sebagai *sample* melalui operasi *sub-sampling*. Proses ini disebut sebagai proses dekomposisi



Gambar 2 *Two-Dimensional* DWT [4]

Dimana:
cAj = Citra input
cA+1 = Koefisien aproksimasi (LL)
$cD^{(h)}_{j+1}$ = Koefisien detail horizontal (LH)

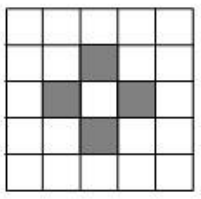
$cD^{(v)}_{j+1}$ = Koefisien detail vertikal (HL)
$cD^{(d)}_{j+1}$ = Koefisien detail diagonal (HH)

Citra masukan diinterpretasikan sebagai sinyal, didekomposisi menggunakan Lo_D (*Low Pass Filter Decomposition)*. Kemudian dilakukan *down-sampling* dua. Keluaran berupa sinyal frekuensi rendah dan sebanyak dua kali, terhadap baris dan kolom sehingga diperoleh empat *sub-band* keluaran yang berisi informasi frekuensi rendah dan frekuensi tinggi.

C. Cellular Automata (CA)

Secara teoritis, *cellular automata* pertama kali diperkenalkan pada tahun akhir tahun 1940-an oleh John Von Neumann dan Stanislaw Ulam sebagai model sederhana untuk mempelajari proses biologi seperti *self-reproduction organism.* Secara praktis, *cellular automata* berkembang ketika pada akhir tahun 1960-an John Conway membuat *game of life* yang mampu memodelkan kehidupan nyata secara sederhana [3]. *Cellular automata* adalah sebuah array dengan *automata* yang identik, atau disebut juga sel, yang saling berinteraksi satu sama lain. Array tersebut dapat membentuk susunan sel 1 dimensi, 2 dimensi maupun 3 dimensi. Susunan sel-sel tersebut dapat membentuk *grid* segi empat sederhana maupun susunan lain seperti sarang lebah yang terdiri dari bagian-bagian berbentuk segi enam (heksagonal)[5]. Sel yang terletak ditengah adalah sel A. Sel berwarna abu-abu adalah neighbours dari sel A.

Von Neuman neighbourhood
N = { U (Utara), T (Timur), S (Selatan), B (Barat) }, r = 1.

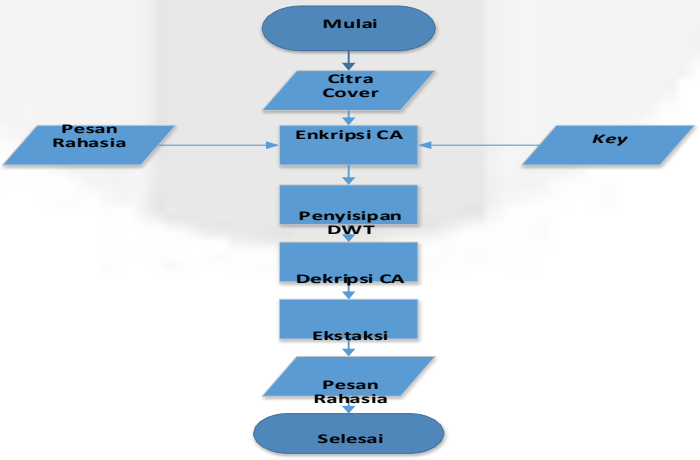


Gambar 3 Von Neumann neighbourhood [2]

3. PEMBAHASAN

A Diagram Sistem

Pada perancangan dan implementasi sistem, akan dijelaskan secara umum tentang alur atau tahapan sistem yang akan diteliti lebih lanjut. Konfigurasi yang dirancang pada tugas akhir ini terdiri dari 4 proses, yaitu mulai dari proses Enkripsi teks dan proses penyisipan serta untuk pengambilan pesannya dilakukan proses dekripsi dan ekstraksi. Pada proses penyisipan menggunakan metode *Discrete Wavelet Tansform* (DWT) dan pada proses enkripsi menggunakan metode *2D Cellular Auomata*. Gambaran umum dari perancangan sistem dapat dilihat pada diagram alir berikut :



Gambar 4 Gambaran Blok Sistem Secara Umum.

Sistem ini secara umum dapat dijelaskan sebagai berikut:

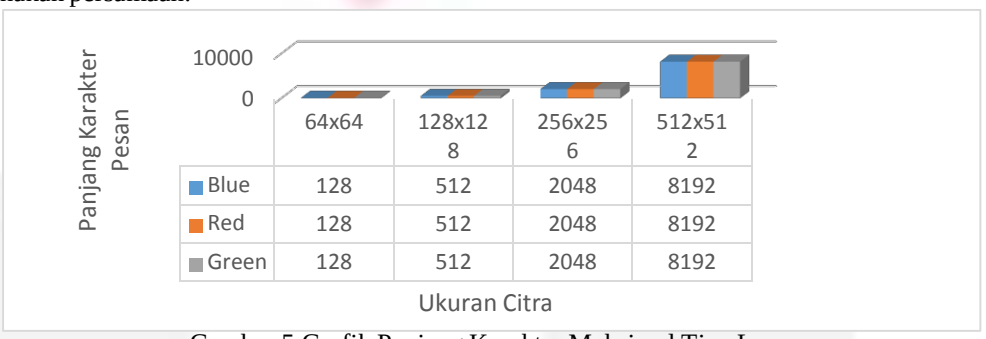
1. Pesan rahasia dienkripsi menggunakan metode *Cellular Automata* (CA) kemudian disisipkan pada citra *cover* melalui proses penyisipan, menghasilkan citra stego. Dimana orang lain hanya melihat sebuah gambar tanpa mengetahui bahwa di dalam gambar telah disisipkan sebuah pesan rahasia.
2. Citra stego kemudian diuji dengan beberapa serangan.
3. Disisi penerima, citra stego didekripsi dan diekstraksi yang hasilnya adalah pesan rahasia yang diinginkan pengirim.

4 Analisis Data Hasil Pengujian Sistem

Berdasarkan skenario pengujian yang telah ditetapkan sebelumnya, maka dilakukan analisis sebagai berikut:

A. Pengujian Kapasitas Tampung Pada Tiap Layer

Pengujian ini dilakukan untuk mengetahui kapasitas maksimum pada tiap layer yang disisipkan pesan. Untuk masing-masing layer *red*, *green* dan *blue* menggunakan ukuran citra 512x512, 256x256, 128x128 dan 64x64. Pada Gambar 5 merupakan hasil pengujian kapasitas tampung dapat dilihat pada gambar 5 dengan menggunakan persamaan:

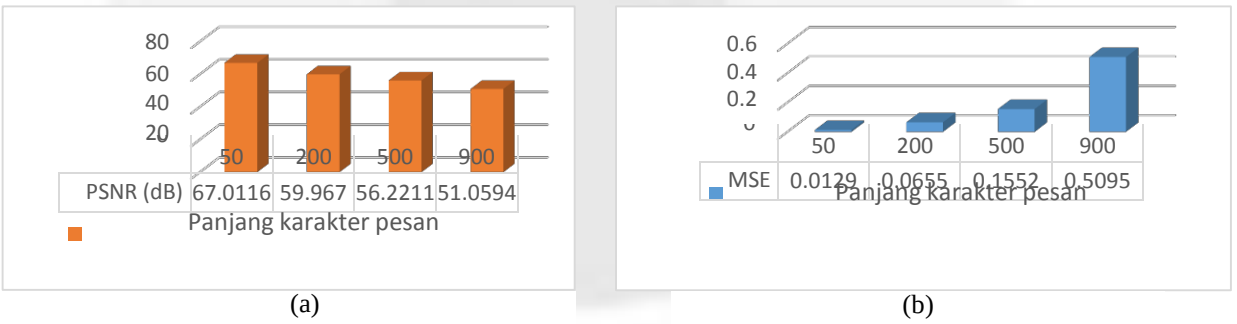


Gambar 5 Grafik Panjang Karakter Maksimal Tiap Layer

Berdasarkan tabel dan grafik Gambar 5, dapat di lihat kapasitas tampung tiap layer *red*, *green* dan *blue* adalah sama pada setiap ukurannya.

B. Pengujian Pengaruh Banyaknya Pesan Rahasia

Pada pengujian ini sistem diuji dengan menyisipkan pesan rahasia yang panjang karakternya berbeda dengan menggunakan citra *cover* berukuran 256x256 dengan format bitmap untuk mengetahui pengaruhnya terhadap nilai PSNR pada citra stego. Banyaknya karakter pesan yang disisipkan bermacan-macam yaitu 50, 200, 500 dan 900 karakter.



(a) (b)

Gambar 6 grafik (a) PSNR pada citra stego dengan panjang pesan berbeda dan (b) MSE pada citra stego dengan panjang pesan berbeda

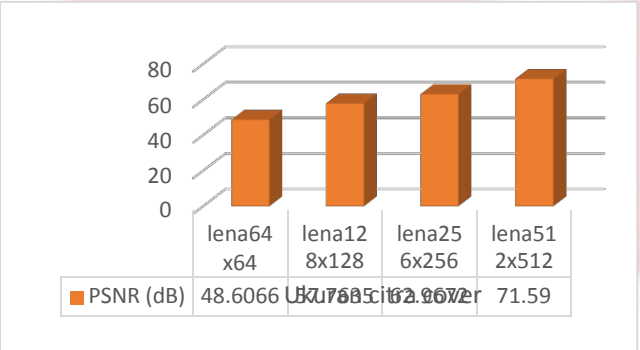
Dapat dilihat pada tabel dan grafik diatas nilai MSE 0.0129 dan nilai PSNR adalah 67.0016 dB pada citra *cover* lena256x256 yang disisipkan panjang pesan 50 karakter dan pada citra yang sama disisipkan panjang pesan 900 karakter didapatkan nilai MSE 0.5095 dan nilai PSNR 51,0594 dB. Hal ini menunjukkan bahwa penyisipan yang dilakukan dengan panjang pesan yang berdeda-beda menghasilnya MSE dan PSNR berbeda juga. Semakin banyak jumlah karakter pesannya maka nilai MSE akan semakin besar dan nilai

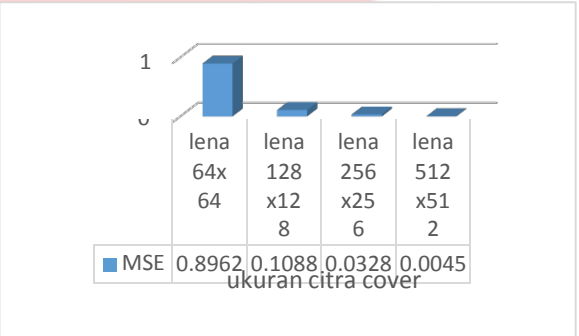
PSNR akan semakin kecil, begitu sebaliknya semakin kecil jumlah karakter pesannya nilai MSE akan semakin kecil dan nilai PSNR akan semakin besar.

C. Pengujian Pengaruh Besarnya Citra *Cover*

Pada pengujian ini sistem diuji dengan menyisipkan jumlah pesan yang konstan ke berbagai ukuran citra *cover*. Ukuran citra *cover* yang digunakan yaitu 64x64, 128x128, 256x256 dan 512x512. Untuk panjang pesan yang disisipkan yaitu 100 karakter. Hasil pengujian pengaruh besarnya citra *cover*.

.





(a) (b)

Gambar 7 grafik (a) PSNR pada citra cover berbeda

dan (b) MSE pada citra cover berbeda

Dapat dilihat dari tabel dan grafik diatas nilai MSE adalah 0.8962 dan nilai PSNR adalah 48,6066 dB pada citra *cover* lena64x64 yang disisipkan panjang pesan 100 karakter dan pada panjang pesan yang sama disisipkan pada citra *cover* lena512x512 didapatkan nilai MSE 0.0045 dan nilai PSNR 71.59 dB. Sehingga, penyisipan yang dilakukan dengan pada citra *cover* yang berbeda-beda menghasilkan MSE dan PNSR yang berbeda juga. Semakin kecil ukuran citra *cover* maka nilai MSE akan semakin besar dan nilai PNSR akan semakin kecil, begitu pula sebaliknya semakin besar ukuran citra *cover* maka nilai MSE akan semakin kecil dan nilai PSNR akan semakin besar.

D. Pengujian Pengaruh Besarnya Citra *Cover* pada pesan karakter maksimal

Pada pengujian ini sistem diuji dengan menyisipkan pesan rahasia yang panjang karakternya berbeda dengan menggunakan citra *cover* berukuran Lenna512x512, Lena256x256, Lena128x128 Lena64x64, Baboon512x512, Babbon 256x256, Baboon 128x128, Babbon 64x64, Pepper512x512, Pepper256x256, Pepper128x128, Pepper 64x64, View512x512, View256x256, View128x128 dan View64x64 dengan format bitmap untuk mengetahui pengaruhnya terhadap nilai PSNR dan MSE pada citra stego. Banyaknya karakter pesan yang disisipkan adalah pesan karakter maksimal pada setiap citra *Cover* yaitu 8192, 2048, 512 dan128 karakter dapat di lihat pada Tabel 1.

Tabel 1 Nilai PSNR dan MSE

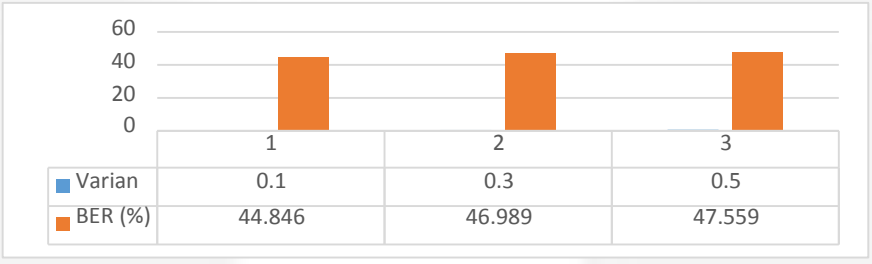
Layer	Ukuran Citra *Cover*	Jumlah Karakter yang Disisipkan	PSNR(dB)	MSE
Red	Lena512x512	8192	41.5806	4.5188
	Lena256x256	2048	44.6688	2.2192
	Lena128x128	512	47.0394	1.2857
	Lena64x64	128	48.9078	0.8362
	Baboon512x512	8192	39.7406	6.9027
	Baboon256x256	2048	42.4990	3.6575
	Baboon128x128	512	44.1235	2.5161
	Baboon64x64	128	42.6213	3.5559
	Pepper512x512	8192	40.7718	5.4437
	Pepper256x256	2048	43.4749	2.9214
	Pepper128x128	512	44.4697	2.3233

	Pepper64x64	128	43.0250	3.2402
	View512x512	8192	40.4380	5.8787
	View256x256	2048	43.3948	2.9758
	View128x128	512	45.8548	1.6889
	View64x64	128	47.6401	1.1196

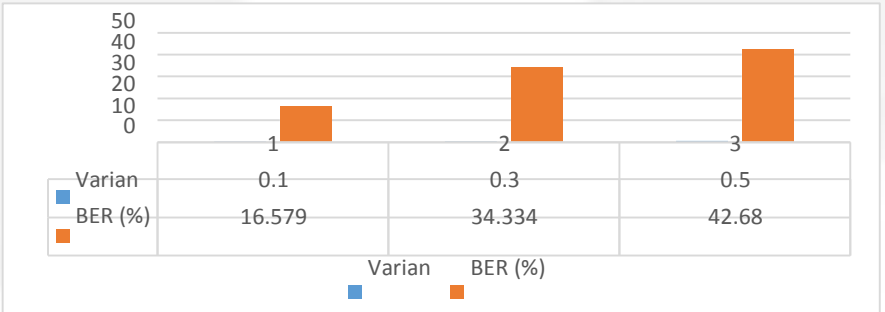
Dapat dilihat dari tabel bahwa nilai MSE adalah 0.8362 dan nilai PSNR adalah 48.9078 dB pada citra *cover* lena64x64 yang disisipkan panjang pesan 128 karakter dan pada panjang pesan yang sama disisipkan pada citra *cover* lena512x512 didapatkan nilai MSE 4.5188 dan nilai PSNR 41.7350 dB dan pada panjang pesan 8192 karakter. Sehingga, penyisipan yang dilakukan dengan pada citra *cover* yang berbeda-beda menghasilkan MSE dan PNSR yang berbeda juga. Semakin kecil ukuran citra *cover* maka nilai MSE akan semakin besar dan nilai PNSR akan semakin kecil, begitu pula sebaliknya semakin besar ukuran citra *cover* maka nilai MSE akan semakin kecil dan nilai PSNR akan semakin besar.

E. Pengaruh Pemberian *Noise* Gaussian, *Noise* Salt & Pepper dan Rescale

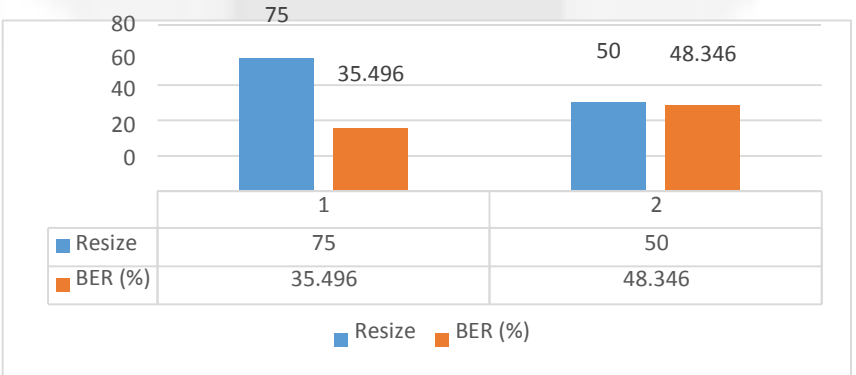
Pengujian dilakukan pada citra *cover* yang telah ditentukan dengan panjang karakter pesan 8192, 2048, 512 dan 128. Untuk ukuran citra yang digunakan yaitu Lenna512x512, Lena256x256, Lena128x128 Lena64x64, Baboon512x512, Babbon 256x256, Baboon 128x128, Babbon 64x64, Pepper512x512, Pepper256x256, Pepper128x128 dan Pepper 64x64 yang diuji pada semua layer. Hasil citra stego diberi serangan berupa *noise* Gaussian dan *noise* Salt & Pepper pada seluruh komponen citra stego. Kemudian dilakukan ekstraksi kembali terhadap pesan rahasia yang telah disisipkan. Pengujian ini bertujuan untuk mengetahui ketahanan sistem terhadap gangguan dengan menghitung nilai CER pesan rahasia hasil ekstraksi dari citra stego yang telah diberikan serangan dan dapat dilihat pada gambar 8, 9 dan 10



Gambar 8 Pengaruh pemberian *Noise* Gaussian



Gambar 9 Pengaruh pemberian *Noise* Salt & Pepper



Gambar 10 Pengaruh pemberian *Resize*

Berdasarkan tabel hasil pengujian *noise* Gaussian, *noise* Salt & Pepper dan rescale di atas, Semakin tinggi *varian* maka semakin tinggi BER dan semakin besar *Resize* maka semakin tinggi BER dengan hasil tersebut hasil ekstraksi pesannya kurang baik Pemberian *noise* menyebabkan perbedaan bit total citra stego yang cukup jauh yang menyebabkan sistem mendeteksi bahwa tidak ada pesan rahasia yang disisipkan pada citra sehingga pesan yang disisipkan tidak dapat terekstrak. Dengan demikian, dapat dikatakan bahwa sistem yang dibuat sangat rentan kehilangan pesan rahasia jika terkena *noise.*

F Pengaruh Ukuran Citra Cover terhadap Waktu Komputasi

Pengujian untuk mengetahui waktu komputasi dari ke-empat ukuran citra yang digunakan dengan citra *cover* yang berbeda. Ukuran citra yang digunakan yaitu 64x64, 128x128, 256x256 dan 512x512. Untuk penghitungan waktu komputasi dilakukan secara sistem *coding* dengan membuat *start* dan *stop*. Waktu komputasi rata-rata dihitung dari proses penyisipan pesan hingga proses ekstraksi pesan. Hasil perhitungan waktu komputasi dapat dilihat pada Tabel 2:

Tabel 2 Waktu Komputasi

Ukuran Citra	Panjang Pesan	Waktu Sisip dan Enkripsi Rata-rata (Detik)	Waktu ekstraksi Rata-rata (Detik)	Waktu Total (Detik)
64x64	128	0.74688	0.01179	0.758672
128x128	512	0.80627	0.03281	0.83908
256x256	2048	1.24533	0.0797	1.32503
512x512	8192	2.04845	0.20471	2.25316

Sesuai tabel hasil komputasi di atas, pada sistem ini proses komputasi membutuhkan waktu yang cukup lama untuk ukuran citra 512x512. Sedangkan untuk citra yang berukuran kecil hanya membutuhkan waktu yang sebentar. Hal ini dikarenakan sistem mencari tempat untuk melakukan penyisipan dan melakukan penyisipan, sehingga untuk citra yang berukuran besar dan tentunya dengan piksel yang besar akan membutuhkan waktu yang cukup lama juga untuk melakukan komputasi.

5 Penutup

Dari hasil pengujian yang dilakukan penelitian kali ini, dapat disimpulkan bahwa.

1. Sistem Steganografi *Discrete Wavelet Transform* mempunyai PSNR ≥ 39 dB dan akurasi 100% pada karakter maksimum yang dapat disisipkan dalam pesan.
2. Waktu komputasi yang dibutuhkan dalam penyimpanan pesan bergantung pada besarnya citra *cover*. Semakin besar citra *cover* maka semakin lama juga waktu komputasinya.
3. Akurasi dari sistem yang dibuat untuk penyisipan pesan rahasia sangat baik yaitu 100% pada saat tanpa serangan
4. Sistem tidak cukup baik dalam menanggapi serangan berupa *noise* Gaussian, *noise* Salt & Pepper dan resize

DAFTAR REFERENSI

[1] Wahana Komputer, Memahami Model Enkripsi dan Security Data, Yogyakarta: Andi, 2003.

[2] A. Sirandan, Simulasi dan Analisi keamanan teks menggunakan Metode Steganografi Discrete Transform, Bandung: Universitas Telkom, 2014.

[3] J. Tambunan, Simulasi Dan Analisis Keamanan Text Menggunakan Steganografi LSB Dan Cellular Automata, Bandung: Universitas Telkom, 2014.

[4] Y. Oktavianty, Simulasi dan Analisa peningkatan keamanan sistem Steganografi berbasis DWT (Discrete Wavelet Transform) dengan Enkripsi Baker Map pada Citra Digital, Bandung: Institut Teknologi Telkom, 2014.

[5] D. G. Green, Cellular Automata, http://life.csu.edu.au/complex/tutorials/tutorial1.html.1993, 8 Agustus 2014.