MENYISIPKAN INFORMASI BERDASARKAN FUZZY COLOR HISTOGRAM MENGGUNAKAN METODE STEGANOGRAFI (DWT) DISCRETE WAVELET TRANSFORM

INFORMATION HIDING BASED ON FUZZY COLOR HISTOGRAM USING DISCRETE WAVELET TRANSFORM (DWT) STEGANOGRAPHY METHOD

Clara Amanda[1], Dr. Ir. Bambang Hidayat, DEA[2], Rian Febrian Umbara, S.Si., M.Si.[3]

Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom
[1]claraamanda.keil@gmail.com, [2]bbhtelkom@gmail.com, [3]rianum123@gmail.com

ABSTRAK

Pertukaran informasi berkembang dengan pesat akibat teknologi yang semakin canggih dan memberikan pengaruh besar bagi kehidupan manusia. Keamanan dan kerahasiaan data merupakan hal yang sangat penting seiring berkembangnya teknologi dengan memanfaatkan media digital sebagai media pertukaran informasi. Untuk menjamin keamanan dan kerahasiaan data diperlukan suatu teknik, salah satunya adalah *Steganography*.

Pada tugas akhir ini dilakukan simulasi *Steganography* untuk menyisipkan pesan teks (.txt) pada *image* (.jpg). Metode yang digunakan untuk menyisipkan pesan adalah *Discrete Wavelet Transform* (DWT). Penyisipan pesan ini dilakukan dengan cara mengganti nilai koefisien yang dibawah nilai *threshold* dengan pesan rahasia. Sedangkan *Fuzzy Color Histogram* (FCH) merepresentasikan sekumpulan *pixel* pada *image* yang akan disisipi *secret message* (teks). Berawal dengan melakukan pembagian layer pada *image* yang terpilih untuk dilakukan penyisipan teks, kemudian dilanjutkan dengan penentuan *value* representasi data menggunakan *Fuzzy Color Histogram*, setelah itu ditransformasikan menggunakan *Inverse Discrete Wavelet Transform* untuk mendapatkan *Stegano Object.*

Dari hasil penelitian, sistem steganografi menggunakan DWT menghasilkan performansi *imperceptibility* antara *cover object* dan citra stego sangatlah mirip dengan kapasitas penyisipan yang lebih banyak. Kesimpulan ini ditunjukan dengan hasil nilai PSNR sebesar 79.44 dB dan nilai MSE sebesar 0,02721 pada *cover object* yang disisipi pesan sepanjang 1279 karakter. Performansi *robustness* pada citra stego mempunyai nilai BER sebersar 0 (nol) artinya tidak ada bit error dalam melakukan ekstraksi pada saat tanpa serangan.

Kata Kunci : *Steganografi, Fuzzy Color Histogram, DWT, Citra Digital*

ABSTRACT

The exchange of information is growing rapidly due to increasingly sophisticated technologies and provide a major influence on human life. Security and confidentiality of data is very important in a row with the development of technology by using digital media as the medium of information exchange. Some technique should be required in order to ensure the security and confidentiality of data, one of which is Steganography.

This final project simulated the Steganography to interpolate a text message (.txt) into an image (.jpeg). The data encryption process is already done before conducting the interpolation. The method used to interpolate the message is *Discrete Wavelet Transform* (DWT). This message interpolation is conducted by replacing the coefficient value located below the threshold value with cryptic messages. Whereas, the *Fuzzy Color Histogram* (FCH) will represent a group of pixel of an image which will be interpolated by cryptic messages (text). Starting with segmenting the choosen image to conduct the interpolation of text, then proceed with determining the value of data representation using *Fuzzy Color Histogram*, finally it will be transformed using *Inverse Discrete Wavelet Transform* to get the *Stegano Object.*

The result of research, steganography system using DWT generate imperceptibility performance between cover object and stego image. These results are similar and generate more storage capacity. In conclusion, the result shows that PSNR is 79.44 dB, MSE is 0,02721 on cover object that embeded 1279-character of message. Robustness performance on stego image has BER value of zero which means there is no bit error in conducting extraction.

Kata Kunci *: Steganografi, Fuzzy Color Histogram, Discrete Wavelet Transform, Digital Image*

1. Pendahuluan

Keamanan dan kerahasiaan data merupakan hal yang sangat penting seiring berkembangnya teknologi dengan memanfaatkan media digital sebagai media pertukaran informasi. Untuk menjaga kerahasiaan informasi telah dikembangkan teknik *Cryptoghraphy*, kemudian diperbaiki dengan teknik *Steganography.*

Steganography adalah seni atau ilmu menyembunyikan pesan rahasia ke dalam media lain yang berupa teks, gambar, suara, ataupun video yang tidak mencurigakan sehingga pesan rahasia tersebut tidak diketahui oleh orang yang tidak berkepentingan. Pesan teks dan image merupakan suatu informasi yang sering dipertukarkan dalam kehidupan sehari-hari. Hal inilah yang mendasari untuk menggunakan pesan teks sebagai informasi yang disembunyikan (secret message) dan image sebagai media penyimpanannya (cover object).

Dua hal penting dalam Steganography adalah kapasitas penyisipan informasi (payload capacity) dan kemampuan menyembunyikan informasi (imperceptibility). Jika kapasitas ditingkatkan, maka adakalanya kemampuan untuk menyembunyikan informasi akan berkurang dan begitu sebaliknya. Untuk itu pemilihan metode Steganography dapat disesuaikan dengan kebutuhan, apakah kapasitas penyisipan atau kemampuan penyembunyian informasi yang diutamakan.

Pada Tugas Akhir ini metode yang digunakan adalah Discrete Wavelet Transform (DWT) yang membagi citra menjadi subband-subband yang memiliki frekuensi tinggi dan frekuensi rendah. Kemudian Fuzzy Color Histogram (FCH) yang menenentukan alokasi sekelompok pixel yang disisipi.

2. Dasar Teori

2.1. Definisi Citra Digital

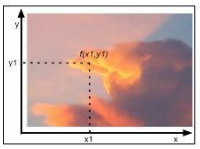
Citra merupakan suatu fungsi kontinyu dari intensitas cahaya atau derajat keabuan dalam bidang 2 dimensi yang dapat direpresentasikan dengan f(x,y), dimana x dan y merupakan kordinat spasial dan nilai f(x,y) sebanding dengan skala intensitas cahaya dari citra pada titik tersebut.

Citra digital dinyatakan dengan matriks berukuran N x M (baris/tinggi=N, kolom/lebar=M).

N = jumlah baris $0 \le y \le N - 1$
M = jumlah kolom $0 \le x \le M - 1$
L = maksimal warna intensitas $0 \le f(x,y) \le L - 1$ (gray level)

$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) & \cdots & f(0,M-1) \\ f(1,0) & f(1,1) & \cdots & f(1,M-1) \\ \vdots & \vdots & & \vdots \\ f(N-1,0) & f(N-1,0) & \cdots & f(N-1,M-1) \end{bmatrix} \quad (2.1)$$

Terlihat pada Gambar 2.1 Ilustrasi Citra Digital [10] yang direpresentasikan dengan f(x,y).



Gambar 2. 1 Ilustrasi Citra Digital

2.2. Fuzzy Color Histogram (FCH)

Fuzzy Color Histogram (FCH) merupakan salah satu metode untuk mempresentasikan informasi warna dalam citra digital ke dalam bentuk histogram. Metode ini mempertimbangkan persamaan warna pada tiap pixel warna yang terasosiasikan ke semua *bin* histogram melalui *fuzzy set membership function*. Pada FCH, satu warna dapat masuk ke dalam dua *bin* histogram atau lebih dengan derajat keanggotaan yang berbeda [3].

2.3. Transformasi Wavelet

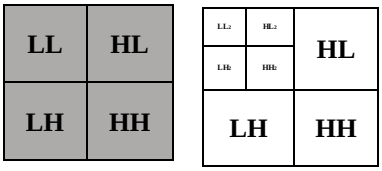
Transformasi Wavelet merupakan perbaikan dari Transformasi Fourier. Transformasi Wavelet selain mampu memberikan informasi frekuensi yang muncul, juga dapat memberikan informasi tentang skala atau durasi waktu. Wavelet dapat digunakan untuk menganalisa suatu bentuk gelombang (sinyal) sebagai kombinasi 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. Sehingga dapat dikatakan, koefisien wavelet mengandung informasi hasil transformasi yang telah terkompresi.

2.4. Discrete Wavelet Transform (DWT)

Prinsip dasar dari DWT adalah bagaimana mendapatkan representasi waktu dan skala dari sebuah sinyal menggunakan teknik pemfilteran digital dan operasi *subsampling.* Implementasi DWT dapat dilakukan dengan cara melewatkan sinyal frekuensi rendah dan frekuensi tinggi [21]. Sinyal pertama-tama dilewatkan pada rangkaian *filter high pass* dan *low pass*, kemudian setengah dari masing-masing keluaran diambil sebagai *sample* melalui operasi *subsampling.* Proses ini disebut sebagai proses dekomposisi satu tingkat. Keluaran dari *filter low pass* digunakan sebagai masukkan di proses dekomposisi tingkat berikutnya. Proses ini diulang sampai tingkat proses dekomposisi yang diinginkan. Gabungan dari keluaran-keluaran *filter high pass* dan satu keluaran *filter low pass* yang terakhir, disebut sebagai koefisien *wavelet* yang berisi informasi sinyal hasil transformasi yang telah terkompresi.

Proses dekomposisi pada sebuah citra akan menghasilkan empat sub bidang citra dari citra asli, dimana keempat sub bidang citra tersebut berada dalam kawasan wavelet. Keempat sub bidang citra tersebut adalah Low-Low (LL), Low-High (LH),

High-Low (HL), dan High-High (HH) [21]. Gambar 2.11 dibawah ini menunjukkan Matrik DWT maju [21].



Gambar 2. 2 Matriks DWT Maju

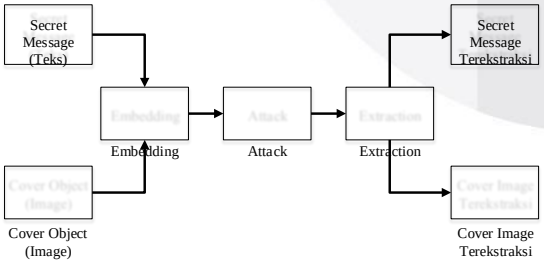
Sebagian besar informasi citra terdapat pada sub band LL, untuk melakukan dekomposisi tingkat dua akan dilakukan pada sub band tersebut. Pada dekomposisi tingkat dua akan dihasilkan empat sub band baru untuk menggantikan sub band LL. Empat subband yang dihasilkan adalah LL_2, HL_2, LH_2, dan HH_2.

2.5. Inverse Discrete Wavelet Transform (IDWT)

IDWT merupakan proses rekontruksi sinyal dengan arah berwalawanan dari proses DWT, dimana dilakukan proses *upsampling* dan *filter* dengan koefisien-koefisien *filter* balik. Proses *upsampling* dilakukan dengan mengembalikan dan menggabungkan sinyal seperti semula dengan cara menyisipkan sebuah kolom berharga nol diantara setiap kolom dan melakukan konvolusi pada setiap baris dengan *filter* satu dimensi. Hal yang sama dilakukan dengan menyisipkan sebuah baris nol diantara setiap baris dan melakukan konvolusi pada setiap kolom dengan *filter* yang lainnya.

3. Perancangan Sistem

Secara umum, sistem *Steganography* pada *image* dilakukan pada Tugas Akhir ini terdiri dari dua proses, yaitu proses penyisipan dan proses ekstraksi.

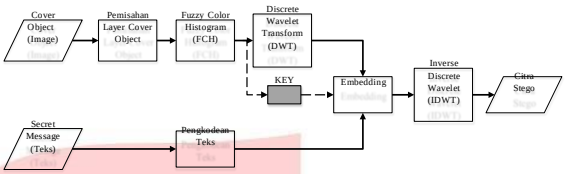


Gambar 3. 1 Blok Diagram Sistem

Berdasarkan Gambar 3.1 Blok Diagram Sistem [23] merupakan blok diagram sistem *steganography* secara umum. Proses *steganography* tersebut dilakukan pada *cover object* dengan menyisipkan *secret message* yang berupa teks. Keluaran dari proses penyisipan ini adalah citra stego. Sebelum dilakukan ekstraksi, untuk menguji kehandalan sistem maka citra stego tersebut diberi serangan. Selanjutnya citra stego tersebut diekstrak kembali sehingga terpisah antara *cover object* terekstraksi dengan *secret message* terekstraksi.

3.1. Poses Penyisipan

Untuk memudahkan dalam proses ekstraksi maka diperlukan kunci (key) dalam sistem ini. Sebelum dilakukan penyisipan pesan, terdapat banyak proses yang harus dilalui. Terlihat pada Gambar 3.2 Proses penyisipan dan key.



Gambar 3. 2 Proses Penyisipan dan Key

Secret message yang digunakan berupa teks. Teks tersebut diubah ke bilangan ASCII, setelah itu diubah kembali ke bilangan hexadesimal lalu ke biner melalui proses pengkodean teks. Kunci yang digunakan pada sistem ini berupa lokasi tempat dilakukan penyisipan hasil dari penentuan *value* pada Fuzzy Color Histogram.

3.1.1. Pemisahan Layer Cover Object

Cover Object yang digunakan pada Tugas Akhir ini adalah citra RGB. C*over object* tersebut terlebih dahulu dilakukan pemisahan layer daerahnya menjadi tiga layer yaitu layer *R*, layer *G*, dan layer *B* dimana sebuah *pixel* dari citra RGB diwakili 3 *byte* dan masing-masing *byte* tersebut merepresentasikan warna merah (*red*), hijau (*green*) dan biru (*blue).*

3.1.2. Fuzzy Color Histogram (FCH)

Penentuan *value* yang sudah diklasifikasikan oleh FCH dengan *range* 0-255. Prosesnya dapat dilihat pada Gambar 3.3 berikut.

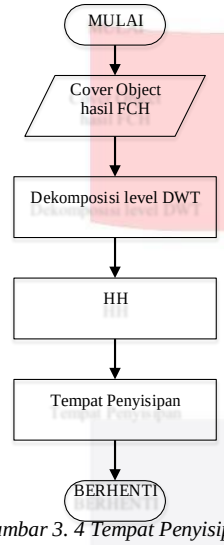
Gambar 3. 3 Diagram Alir Proses Klasifikasi FCH

Proses klasifikasi yang sesuai dengan FCH merupakan proses penjumlahan nilai kemunculan *gray level* pada histogram. Langkah pertama yang dilakukan adalah dengan melakukan perhitungan jumlah piksel pada *Cover Object*, kemudian ditentukan batas keanggotaan *fuzzy* dari hasil pembagian jumlah piksel dengan daerah yang diinginkan. Setelah mendapat batas-batas

keanggotaan *fuzzy* tersebut, langkah selanjutnya menjumlahkan nilai kemunculan *gray level* tersebut hingga mencapai batas-batasan fuzzy yang telah ditentukan. Hal tersebut dilakukan untuk memperoleh kawasan yang terpilih yang terbaik dalam lokasi penyisipan.

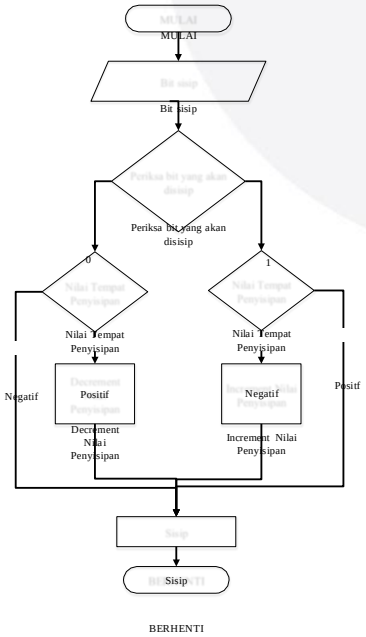
3.1.3. Discrete Wavelet Transform (DWT)

Pada proses dekomposisi, subband HH dipilih sebagai tempat untuk menyisipkan *secret message* kemudian dilakukan penyisipan. Dapat dilihat pada Gambar 3.4 Tempat Penyisipan.



Gambar 3. 4 Tempat Penyisipan

Setelah dilakukan pemilihan tempat penyisipan, selanjutnya dilakukan penyisipan *secret message* yang telah dikodekan ke dalam citra cover yang sudah di DWT dan dipilih tempat penyisipannya. Dapat dilihat pada Gambar 3.5 merupakan *flowchart* proses penyisipan.



Gambar 3. 5 Proses Penyisipan

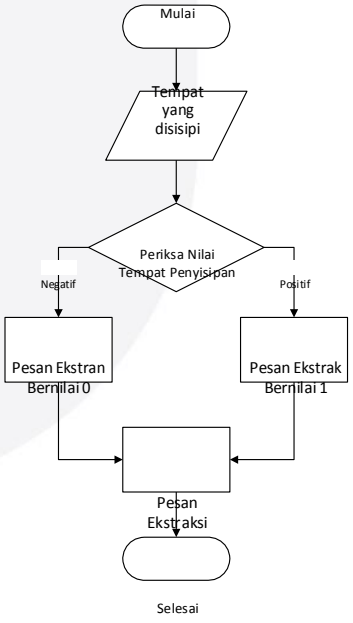
Hal pertama yang dilakukan adalah pemeriksaan nilai pada tempat penyisipan, jika bit yang akan disisip merupakan bit 0 sementara nilai tempat penyisipan positif maka dilakukan decrement nilai penyisipan terlebih dahulu. Namun, jika bit yang akan disisip merupakan bit 1 sementara tempat penyisipan negatif maka dilakukan increment nilai penyisipan.

3.1.4. Inverse Discrete Wavelet Transform (IDWT)

Setelah proses penyisipan selesai, selanjutnya dilakukan proses rekontruksi kembali menggunakan Invers DWT (IDWT) sehingga menghasilkan citra stego. Proses IDWT merupakan proses pembalikan (sub level) dari proses DWT. Setelah melalui proses IDWT, maka langkah selanjutnya adalah penggabungan kembali daerah citra yang telah melalui proses sebelumnya dengan daerah citra warna lainnya. Hasil penggabungan ini adalah citra stego ataupun citra terekstraksi.

3.2. Proses Ekstraksi

Proses ekstraksi merupakan proses pembalikan dari proses penyisipan. Pertama yang harus dilakukan adalah mencari tempat yang disisipi secret message pada citra stegoi yang telah di DWT. Pencarian tempat ini sama dengan pencarian tempat penyisipan pada proses penyisipan. Dapat dilihat pada Gambar 3.6 Proses Ekstraksi merupakan *flowchart* proses ekstraksi.



Gambar 3. 6 ProsesEkstraksi

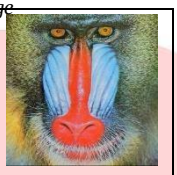
4. Pengujian dan Hasil Analisi

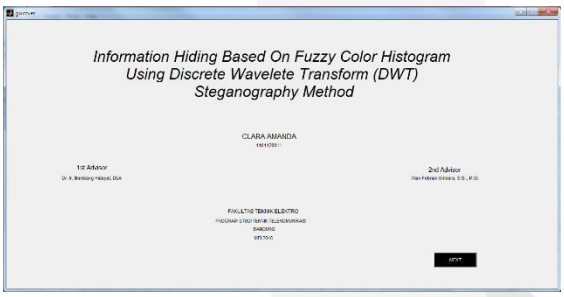
Tujuan dari pengujian ini adalah untuk mengetahui kualitas dan performansi dari sistem *Steganography* yang telah diimplementasikan. Parameter yang digunakan untuk mengetahui performansi sistem adalah BER, PSNR, MSE, dan waktu komputasi.

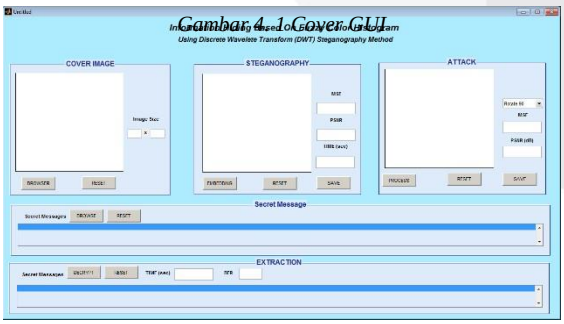
Pada pengujian ini digunakan *cover object* berupa citra RGB dengan format jpg. *Cover Object* yang digunakan ada empat yaitu Fruits, Leopard, Room, dan Victoria masing-masing memiliki dimensi 1024x1024 piksel, serta empat *secret message* 33, 198, 426, dan 12796 karakter. Simulasi pengujian sistem ini dilakukan menggunakan *software MATLAB 8.3 (R2014a).* Dapat dilihat pada

Gambar 4.1 *Cover GUI* dan Gambar 4.2. *Interface GUI.*

Tabel 4. 1 Secret Message

		
fruits.jpg	leopard.jpg	baboon.jpg
		
room.jpg	victoria.jpg	lena.jpg



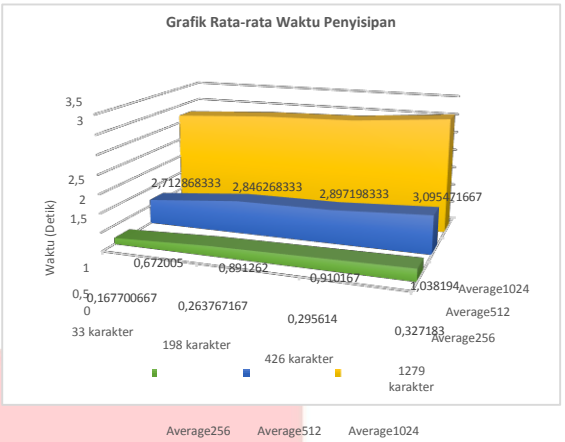


Gambar 4. 1 Cover GUI

Gambar 4. 2 Interface GUI

4.1. Analisis Waktu Penyisipan Terhadap Panjang Secret Message

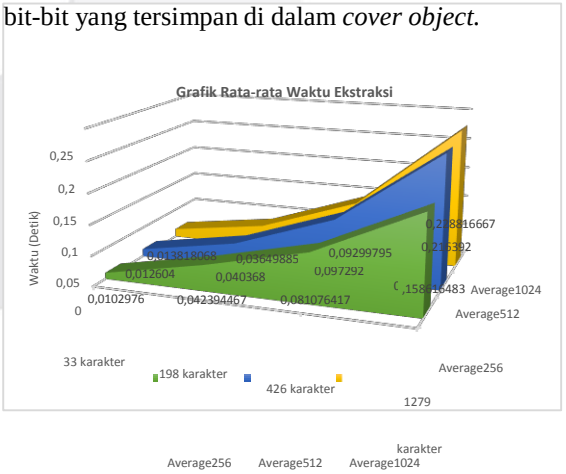
Berdasarkan pada Gambar 4.3 Grafik Rata-rata Waktu Penyisipan Pada Setiap Ukuran Dimensi, pertama yang dilakukan adalah membandingkan jumlah karakter yang berbeda-beda, yaitu 33 karakter, 198 karakter, 426 karakter, dan 1279 karakter dengan ukuran dimensi yang sama, dapat disimpulkan bahwa semakin banyak karakter yang disisip maka waktu penyisipan juga semakin lama.



Gambar 4. 3 Grafik Rata-rata Waktu Penyisipan Pada Setiap Ukuran Dimensi Citra

4.2. Analisis Waktu Ekstraksi atau Deskripsi Terhadap Panjang Secret Message

Berdasarkan Gambar 4.4 Grafik Rata-rata Waktu Ekstraksi Pada Setiap Ukuran Dimensi Citra, semakin banyak bit *secret message* yang akan disisipkan, maka semakin banyak waktu yang dibutuhkan dalam proses ekstraksi pesan tersebut. Panjang *secret message* 1279 karakter memerlukan waktu lebih lama dibandingkan dengan panjang *secret message* 33, 198, dan 426 karakter dengan dimensi ukuran *cover object* yang sama. Hal yang sama dialami untuk ukuran dimensi citra yang semakin besar membutuhkan waktu yang lebih lama dalam karakter yang sama. Hal ini dapat terjadi karena sistem membutuhkan waktu untuk mencari bit-bit yang tersimpan di dalam *cover object.*

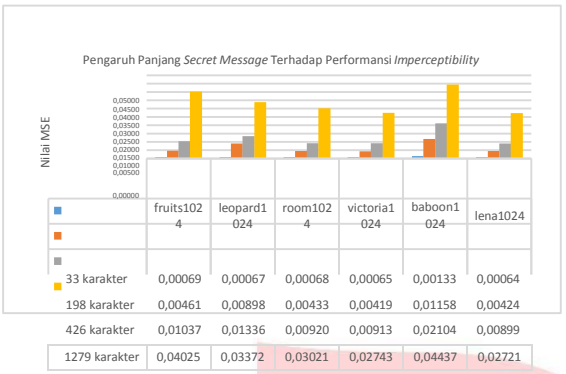


Gambar 4. 4 Grafik Rata-rata Waktu Ekstraksi Pada Setiap Ukuran Dimensi Citra

4.3. Analisis Pengaruh Panjang Secret Message Terhadap Performansi Imperceptibility (Tanpa Gangguan)

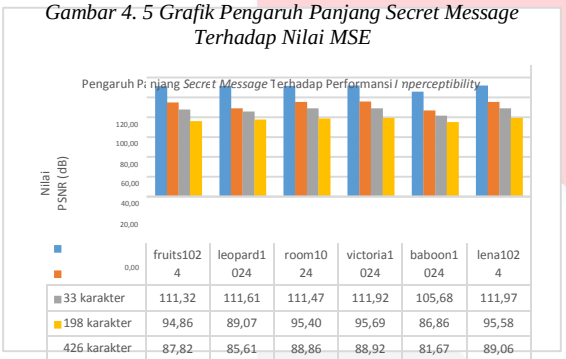
Dalam analisis ini dibandingkan nilai MSE (Mean Square Error) dan PSNR (Peak Signal to Noise Ratio) pada masing-masing *cover object* yang memiliki dimensi ukuran yang sama yaitu 1024 x

1024, tetapi jumlah karakter yang berbeda dari masing-masing *cover object* tersebut.



	fruits1024	leopard1024	room1024	victoria1024	baboon1024	lena1024
33 karakter	0,00069	0,00067	0,00068	0,00065	0,00133	0,00064
198 karakter	0,00461	0,00898	0,00433	0,00419	0,01158	0,00424
426 karakter	0,01037	0,01336	0,00920	0,00913	0,02104	0,00899
1279 karakter	0,04025	0,03372	0,03021	0,02743	0,04437	0,02721

Gambar 4. 5 Grafik Pengaruh Panjang Secret Message Terhadap Nilai MSE



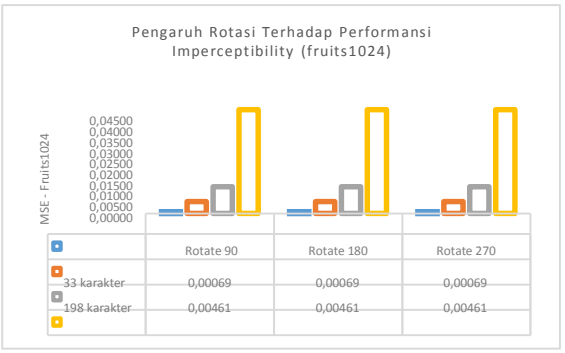
	fruits1024	leopard1024	room1024	victoria1024	baboon1024	lena1024
33 karakter	111,32	111,61	111,47	111,92	105,68	111,97
198 karakter	94,86	89,07	95,40	95,69	86,86	95,58
426 karakter	87,82	85,61	88,86	88,92	81,67	89,06
1279 karakter	76,04	77,57	78,53	79,37	75,19	79,44

Gambar 4. 6 Gambar 4. 6 Grafik Pengaruh Panjang Secret Message Terhadap Nilai PSNR

Dari Gambar 4.5 Grafik Pengaruh Panjang Secret Message Terhadap Nilai MSE dapat diketahui bahwa semakin panjang *secret message* yang disisipkan maka semakin besar tingkat error yang terjadi pada citra stego sehingga nilai MSE menjadi semakin tinggi dan nilai PSNR semakin rendah. Dapat dilihat nilai PSNR pada Gambar 4.6 yaitu grafik pengaruh *secret message* terhadap nilai PSNR. Hal ini terjadi karena semakin panjang *secret message* maka semakin banyak bit yang disisipkan sehingga akan semakin kecil kemiripan antara citra stego dengan citra aslinya. Nilai MSE merupakan nilai rata-rata kuadrat dari error, antara gambar asli dengan gambar hasil penyisipan. Sedangkan semakin turun nilai PSNR maka semakin turun kualitas citra.

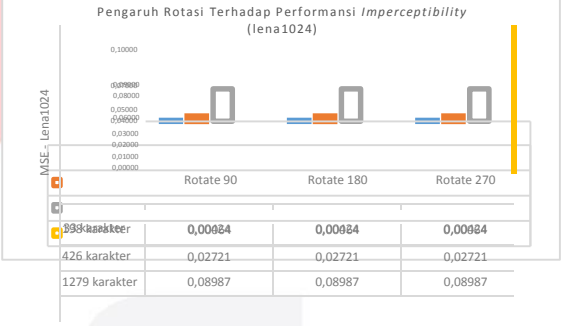
4.4. Analisis Pengaruh Serangan Rotasi Terhadap Performansi Imperceptibility

Pada sistem ini pengujian serangan rotasi hanya dilakukan pada sudut 90, 180, dan 270 yang merupakan sudut-sudut istimewa. Pengujian tersebut dilakukan terhadap *secret message* yang berbeda-beda yaitu 33, 198, 426, dan 1279 karakter. Berikut ini merupakan grafik pengaruh serangan rotasi terhadap nilai performansi *imperceptibility*. Dalam pengujian serangan rotasi ini, hanya menggunakan *cover object* Fruits dan Lena.



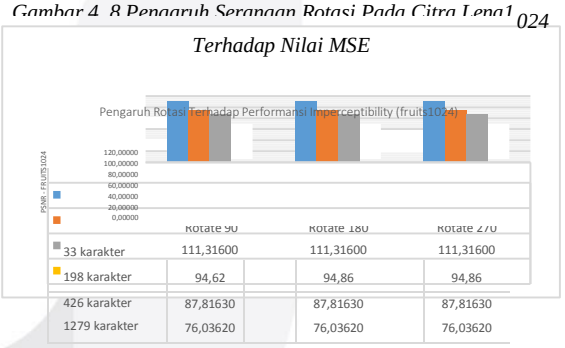
	Rotate 90	Rotate 180	Rotate 270
33 karakter	0,00069	0,00069	0,00069
198 karakter	0,00461	0,00461	0,00461
426 karakter	0,01037	0,01037	0,01037
1279 karakter	0,04025	0,04025	0,04025

Gambar 4. 7 Pengaruh Serangan Rotasi Pada Citra Fruits1024 Terhadap Nilai MSE



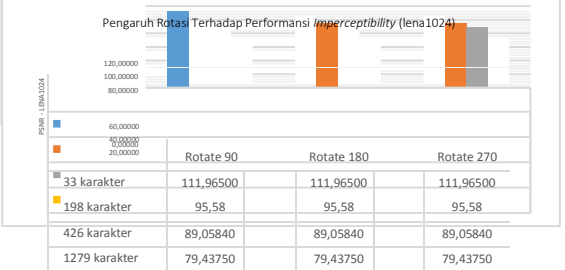
	Rotate 90	Rotate 180	Rotate 270
33 karakter	0,00024	0,00024	0,00024
198 karakter	0,00174	0,00174	0,00174
426 karakter	0,02721	0,02721	0,02721
1279 karakter	0,08987	0,08987	0,08987

Gambar 4. 8 Pengaruh Serangan Rotasi Pada Citra Lena1024 Terhadap Nilai MSE



	Rotate 90	Rotate 180	Rotate 270
33 karakter	111,31600	111,31600	111,31600
198 karakter	94,62	94,86	94,86
426 karakter	87,81630	87,81630	87,81630
1279 karakter	76,03620	76,03620	76,03620

Gambar 4. 9 Pengaruh Serangan Rotasi Pada Citra Fruits1024 Terhadap Nilai PSNR



	Rotate 90	Rotate 180	Rotate 270
33 karakter	111,96500	111,96500	111,96500
198 karakter	95,58	95,58	95,58
426 karakter	89,05840	89,05840	89,05840
1279 karakter	79,43750	79,43750	79,43750

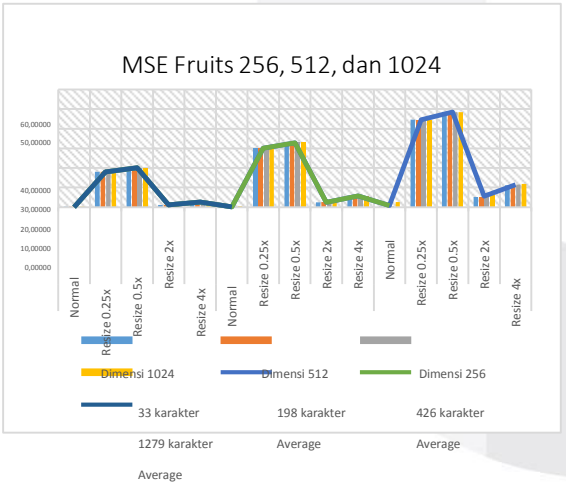
Gambar 4. 10 Pengaruh Serangan Rotasi Pada Citra Lena1024 Terhadap Nilai PSNR

Dari gambar grafik yang dihasilkan, dapat dilihat Gambar 4.7, Gambar 4.8, Gambar 4.9, dan Gambar 4.10 merupakan grafik pengaruh rotasi terhadap performansi *imperceptibility* pada citra fruits1024 dan lena1024 dengan meninjau nilai MSE dan PSNR pada hasil pengujian sistem tersebut. Pada serangan rotasi ini tidak terjadi perubahan yang

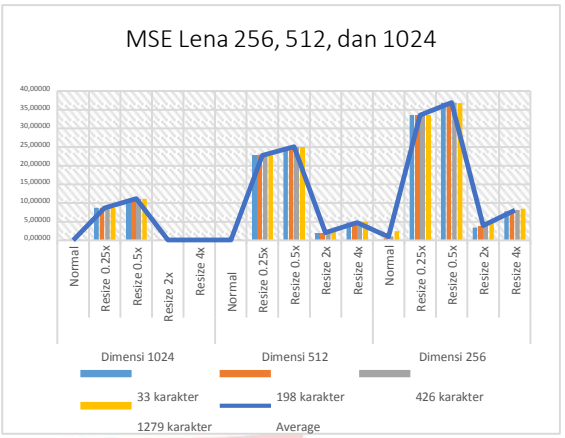
signifikan. Hal ini terjadi karena pada serangan rotasi terjadi pembalikan arah sesuai dengan besarnya rotasi yang dilakukan. Langkah-langkah proses serangan rotasi ini yaitu citra stego di rotasi sebesar sudut istimewa kemudian dilakukan proses pembalikan sesuai dengan rotasi diawal. Dapat diambil contoh, citra stego di rotasi sebesar 90 derajat kemudian dilakukan proses pembalikan arah sebesar -90 derajat. Dilakukan uji coba untuk 180 derajat dan 270 derajat.

4.5. Analisis Pengaruh Serangan Resize Terhadap Performansi Imperceptibility

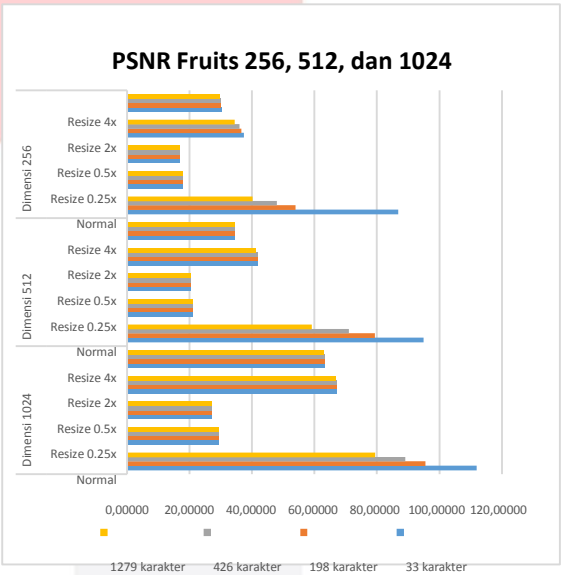
Dalam pengujian serangan rotasi ini, hanya menggunakan cover object Fruits dan Lena. Membandingkan nilai MSE dan PSNR pada citra Fruits dan Lena dengan dimensi yang berbeda-beda pada setiap citra terhadap secret message yang berbeda-beda yaitu 33, 198, 426, dan 1279 karakter. Proses resize yang dilakukan pada pengujian sistem ini dengan cara memperkecil ukuran piksel citra, kemudian dikembalikan lagi ke ukuran semula. Memperkecil ukuran piksel citra, maka akan menyebabkan beberapa nilai piksel berubah. Oleh karena itu, pengujian ini dilakukan untuk membuktikan kehandalan sistem dan atau besarnya pengaruh perubahan nilai-nilai piksel tersebut terhadap nilai MSE dan PSNR. Berikut ini merupakan grafik pengaruh serangan resize terhadap nilai performansi imperceptibility.



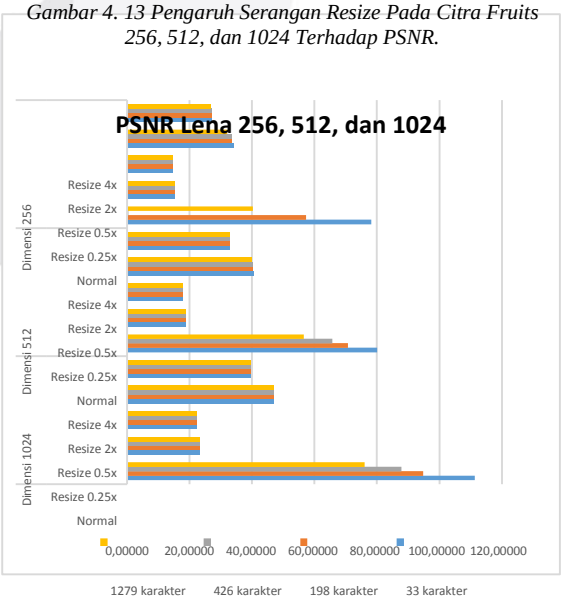
Gambar 4. 11 Pengaruh Serangan Resize Pada Citra Fruits 256, 512, dan 1024 Terhadap MSE.



Gambar 4. 12 Pengaruh Serangan Resize Pada Citra Lena 256, 512, dan 1024 Terhadap MSE.



Gambar 4. 13 Pengaruh Serangan Resize Pada Citra Fruits 256, 512, dan 1024 Terhadap PSNR.



Gambar 4. 14 Pengaruh Serangan Resize Pada Citra Lena 256, 512, dan 1024 Terhadap PSNR.

5. Kesimpulan dan Saran

Kesimpulan

1. Panjang *secret message* yang disisipkan pada *citra cover* mempengaruhi waktu penyisipan. Semakin panjang *secret message* yang disisipkan maka semakin lama waktu yang diperlukan untuk penyisipan.
2. Ukuran dimensi citra mempengaruhi waktu penyisipan. Semakin luas ukuran dimensi citra akan semakin lama waktu yang diperlukan untuk penyisipan dalam sistem ini.
3. Panjang *secret message* yang disisipkan pada *citra cover* mempengaruhi waktu ekstraksi. Semakin panjang bit-bit *secret message* yang disisipkan maka semakin lama waktu yang diperlukan untuk ekstraksi. Karena sistem membutuhkan waktu untuk mencari bit-bit yang tersimpan di dalam *cover object.*
4. Panjang *secret message* yang disisipkan mempengaruhi kualitas citra stego. Semakin panjang *secret message secret message* yang disisipkan maka semakin besar pula tingkat error yang terjadi sehingga kualitas stego menurun.
5. Citra stego tahan terhadap *rotasi*, hal ini terbukti pada nilai PSNR hasil serangan rotasi sebesar 90, 180, 270 derajat sama dengan nilai PSNR citra stego tanpa serangan.
6. Citra stego tahan terhadap *resize* dengan memperbesar ukuran citra stego, namun tidak tahan terhadap serangan *resize* dengan cara memperkecilukuran stego. Hal ini dibuktikan dengan nilai MSE hasil serangan *resize.* Semakin memperkecil ukuran piksel maka semakin besar nilai MSE dan semakin kecil pula nilai PSNR

Saran

1. Penyisipan *Secret Message* dilakukan secara acak pada *Cover Object.*
2. Mengimplementasikan sistem pada *hardware*, seperti FPGA.

Daftar Pustaka :

[1] Hartono, Meilissa Pratiwi. 2014. *Simulasi Dan Steganalisis Citra Digital Berbasis Domain Discrete Cosine Transform (DCT) Dan Domain Spasial*, **[Tugas Akhir]**. Jurusan Teknik Telekomunikasi, Fakultas Teknik Elektro dan Komunikasi. Bandung : Universitas Telkom.

[2] Alatas, Putro. 2009. *Implementasi Teknik Steganografi Dengan Metode LSB Pada Citra Digital*, **[Tugas Akhir]**. Jurusan Sistem Informasi, Fakultas Ilmu Komputer & Teknologi. Depok : Universitas Gunadarma.

[3] Kusumaningsih, Idaliana. 2009. *Ektraksi Ciri Warna, Bentuk, Dan Tekstur Untuk Temu Kembali Citra Hewan*, **[Tugas Akhir]**. Jurusan Ilmu Komputer, Fakultas Matematika Dan Ilmu Pengetahuan Alam. Bogor : Institut Pertanian Bogor. Juneja, Mamta. and Sandhu, Parvinder Singh., *Image Segmentation based Quality Analysis of Agricultural Productd using Emboss Filter and Hough Transform in Spatial Domain*, Kharar under Punjab Technical University, Punjab India.

[4] Elgammal, Ahmed. 2008. *Digital Imaging and Multimedia Histograms of Digital Images*. Departement of Computer Science, Rutgers University. From

[5] *Data Hiding Steganograph Pada File Image Menggunakan Metode Least Significant Bit*. Surabaya : ITS

[6] Agus Prihanto, Suluh Sri Wahyuningsih . 2009. *Penyembunyian Dan Pengacakan Data Text Menggunakan Steganografi Dan Kriptografi Triple Des Pada Image*,**[Jurnal].** Jurusan Teknik Informatika, Fakutas Teknologi Informasi Institut Teknologi Sepuluh Nopember – Surabaya

[7] Goodini, Saeede. 2014. *New Method of DWT-based Image Steganography by using Fuzzy Logic*. Master of Communication Engineering. Islamic Azad University : Iran.

[8] Peningkatan Kapasitas Informasi Tersembunyi Pada Image Steganografi Dengan Menggunakan Teknik Hybrid. Surabaya : ITS

[9] Rekamasanti, Farisah Qisthina. 2015. Implementasi Dan Analisis Video Steganografi Dengan Format Video Avi Berbasis LSB (Least Significant Bit) Dan SSB-4 (System Of Steganography Using Bit), **[Tugas Akhir]**. Jurusan Teknik Telekomunikasi, Fakultas Teknik Elektro dan Komunikasi. Bandung : Universitas Telkom

[10] Wilastri, Tiar. 2010. Desain dan Simulasi Steganography pada Citra Digital Menggunakan Metode Pengacakan LSB dan SSB-4, **[Tugas Akhir]**. Bandung : Sekolah Tinggi Teknologi Telkom Bandung

[11] RJ Anderson (ed.). *Information Hiding: 1st International Workshop, volume 1174 of Lecture Notes in Computer Science, Isaac Newton Institute* (Spring-Verlag, Berlin, Germany, 1996)

[12] Fatiha Djebbar, Bghdad Ayad, Karim Abed Meraim, dan Habib Hamam. 2012. *Comparative Study of Digital Audio Steganography Techniques.* From : Djebbar

et al. EURASIP Journal on Audio, Speech, and Music Processing 2012, **2012**:25

[13] Bret Dunbar. 2002. *A Detailed Look At Steganographic Techniques and Their Use In An Open Systems* **[Paper]**. *Environment* SANS Institute Reading Room.

[14] Masoud Nosrati, Ronak Karimi, and Mehdi Harini. *An Introduction To Steganography Methods. 2011. World Applied Programming, Vol (1), No (3), August 2011. 191-195. ISSN: 2222-2510. ©2011 WAP journal.*

[15] Ir. Rinaldi Munir, M.T. 2004. *Steganografi dan Watermarking,* **[Materi Kuliah ke-7 IF5054 Kriptografi],** Bandung : Institut Teknologi Bandung

[16] Putra, Darma. 2010. *Pengolahan Citra Digital.* Yogyakarta

[17] Aristya, Ni Made Lidya Dewi. 2013. *Simulasi Dan Analisis Steganografi Citra Digital Menggunakan Metode Advanced Encryption Standard dan BCH Code,* **[Tugas Akhir]**. Bandung : Universitas Telkom

[18] Ir. Rinaldi Munir, M.T. 2004. *Pengolahan Citra Digital,* BAB 11**,** Bandung : Institut Teknologi Bandung

[19] Cahyana ; T. Basarudin dan Danang Jaya. 2007. *Teknik Steganografi Citra berbasis SVD.* National Conference on Computer Science & Information Technology 2007. Januari 29-30,2007.

[20] Wahid, Muhamad Luthfi. 2014. *Analisis Dan Simulasi Steganografi Video Berbasis Deteksi Band Frekuensi Menggunakan Metode Discrete Wavlete Transform,* **[Tugas Akhir]**. Bandung : Universitas Telkom

[21] *Klasifikasi Motif Batik Banyuwangi Menggunakan Metode Ekstraksi Ciri Wavelet Dan Metode Klasifikasi Fuzzy Logic*

[22] Ju Han and Kai-Kuang Ma. 2002. *Fuzzy Color Histogram and Its Use in Color Image Retrieval,* IEEE Transactions On Image Processing

[23] Onistyami, Vika Fatwa. 2014. *Simulasi Dan Analisis Pengamanan Pesan Teks Pada Citra Digital Berdasarkan Steganografi Menggunakan DWT (Discrete Wavelet Transform),* **[Tugas Akhir]**. Bandung : Universitas Telkom