Steganografi Pada Citra JPEG Dengan Metode Sequential Dan Spreading

I Nyoman Piarsa
Staf Pengajar Teknologi Informasi, Fakultas Teknik, Universitas Udayana
E-mail: manpits@gmail.com

Abstrak

Faktor keamanan data dalam proses pertukaran data antar perangkat informasi dalam sebuah jaringan informasi menjadi sebuah topik permasalahan yang sangat penting untuk diperhatikan seiring dengan kerahasiaan dari data yang dimiliki. Teknik kriptografi yang menyandikan informasi menjadi sekumpulan kode-kode acak terkadang tidak cukup dalam penyembunyian informasi karena bentuk informasi yang dikirimkan akan memudahkan pihak ketiga untuk menerka dan memecahkan sandi dari enkripsi tersebut. Alternatif lain adalah dengan menggunakan metode steganografi yang bertujuan untuk menyembunyikan informasi yang sebenarnya dalam sebuah data yang tidak dicurigai oleh pihak ketiga sebagai pesan rahasia.

Teknik steganografi pada penelitian ini diimplementasikan pada data citra dengan format JPEG menggunakan metode sequential (low bit coding) dan spreading. Metode sequential melakukan penyisipan secara berurutan pada koefisien dari DCT sedangkan metode spreading melakukan penyisipan secara acak berdasarkan proses hashing yang digunakan. Proses pengujian yang dilakukan terdiri dari perbandingan kapasitas perhitungan dengan kapasitas pengujian, perhitungan statistik error measurement, pengujian dengan metode MOS untuk mengukur kualitas data citra serta ketahanan teknik steganografi yang digunakan terhadap penyerangan yang dilakukan.

Hasil pengujian menunjukkan bahwa teknik steganografi dengan transformasi DCT bisa menghasilkan data hiding dengan tingkat validitas mencapai 100% dengan catatan bahwa data citra memiliki kapasitas penyisipan yang memadai. Penyisipan data yang dilakukan tidak berpengaruh terlalu banyak pada kualitas data citra yang dihasilkan, serta nilai PSNR yang dimiliki data citra terstego lebih besar sama dengan 30 dB. Tingkat kemiripan antara citra asli dengan citra terstego mencapai 96%. Teknik steganografi dengan metode spreading dan sequential tidak robust terhadap manipulasi yang dilakukan pada media stegonya sehingga data yang ada akan rusak jika terjadi manipulasi sekecil apapun pada media stegonya

Kata kunci: *informasi, keamanan data, citra jpeg, enkripsi dan steganografi.*

Abstract

Data security factors in the process of information data exchange between devices within a network is very important issue to be considered along with the confidentiality of data. Cryptographic techniques to encode information into a set of random code sometimes is not enough in hiding information because the information submitted form will allow third parties to guess and crack password of the encryption. Another alternative is to use steganographic method that aims to hide the information in a data format which is not suspected by any third party as a secret message.

Steganographic techniques in this research implemented in a JPEG image by using the sequential method (low-bit coding) and spreading. Sequential method insert data sequentially of the DCT coefficients while the method of spreading conduct random insertion process-based hashing used. The tests consists of comparisons calculation capacity versus testing capacity, the calculation of statistical measurement error, the test with MOS method to measure image data quality and durability steganographic techniques that are used against attacks.

The results show that the technique of steganography with DCT transformation can generate data hiding with validity rates reached 100% with a note that the image data has an adequate insertion capacity. Insertion of data do not affect too much on the quality of the resulting image, and the PSNR values of stego image greater or equal to 30 dB. Level of

similarity between the original image with the stego image is 96%. Steganographic techniques with spreading and sequential method is not robust against manipulation by the stego media so existing data will be damaged if there is a slight manipulation of the stego media.

Key words: information, data security, image jpeg, encryption and steganography.

1. PENDAHULUAN

Perkembangan teknologi informasi yang terjadi dalam beberapa dekade terakhir ini telah mengalami kemajuan yang cukup pesat serta melahirkan beberapa inovasi baru dalam bidang komunikasi. Pertukaran berbagai informasi dan data dalam sebuah jaringan akan menimbulkan suatu masalah baru dalam hal keamanan data tersebut manakala data atau informasi yang dikirim tersebut memiliki aspek kerahasiaan yang cukup berharga dan tidak boleh diakses oleh sembarang orang yang tidak berhak. Permasalahan tersebut membuat aspek keamanan dalam bidang komunikasi data merupakan suatu hal yang harus mendapatkan perhatian yang cukup serius karena menyangkut kerahasiaan suatu informasi atau data yang cukup berharga bagi beberapa orang dimana data atau informasi tersebut dikirim melalui jaringan internet seperti e-mail contohnya.

Beberapa cara telah dilakukan untuk menjaga keamanan dan kerahasiaan suatu data (seperti dokumen penting, e-mail, serta data yang bersifat rahasia) dari pihak-pihak yang tidak berkepentingan terhadap data tersebut, salah satunya cara adalah menggunakan kriptografi. Metode kriptografi menjamin keamanan data tersebut dengan cara mengenkripsi data tersebut dengan mengubahnya menjadi kode-kode acak yang bersifat random sehingga membuat data tersebut tidak dapat dibaca dan dimengerti oleh pihak lain. Sampai sekarang metode-metode tersebut masih digunakan oleh beberapa pihak untuk menjaga kerahasiaan data mereka baik dalam proses transaksi secara on-line ataupun sekedar mengirim data kepada seseorang lewat jaringan internet. Penggunaan metode kriptografi tersebut memang cukup membuat kerahasiaan serta keamanan data tersebut tetap terjaga. Tetapi penggunaan metode enkripsi tersebut tidak selalu menjamin keamanan data tersebut. Penggunaan metode enkripsi yang umum seperti RSA atau algoritma DES pada beberapa jaringan akan membuat suatu kecurigaan yang sangat besar bagi beberapa pihak yang terkait. Dalam hal ini, beberapa pihak seperti badan intelijen negara serta beberapa ISP (Internet Service Provider) akan dengan sangat mudah menemukan data di dalam suatu jaringan internet yang telah dienkripsi karena data tersebut bukan merupakan jenis data yang biasanya dijumpai karena data yang telah terenkripsi adalah merupakan data yang berisi kode-kode acak yang sangat sulit untuk dimengerti oleh orang awam sehingga dapat diibaratkan dengan melihat noda hitam di atas kertas putih atau dengan kata lain dapat dianggap sebagai hal yang tidak lazim.

Alternatif baru ditawarkan dalam dunia komunikasi untuk mengatasi masalah tersebut serta untuk menjaga kerahasiaan serta keamanan data tersebut tanpa menimbulkan beberapa kecurigaan bagi pihak-pihak yang bersangkutan. Alternatif tersebut dikenal dengan teknik penyembunyian data dalam sebuah data yang dipakai sebagai media stego atau lebih dikenal dengan teknik steganografi yaitu menyembunyikan data dalam sebuah medium yang dapat berupa jenis data apapun seperti file image, audio, video, maupun jenis data yang lainnya. Penggunaan teknik steganografi yang biasanya digabungkan dengan metode enkripsi tersebut menyebabkan data yang disembunyikan akan terlihat seperti data biasa karena yang terlihat adalah bentuk data pembungkusnya bukan data yang telah terenkripsi sehingga tidak akan menimbulkan kecurigaan bagi pihak lainnya.

2. KAJIAN PUSTAKA

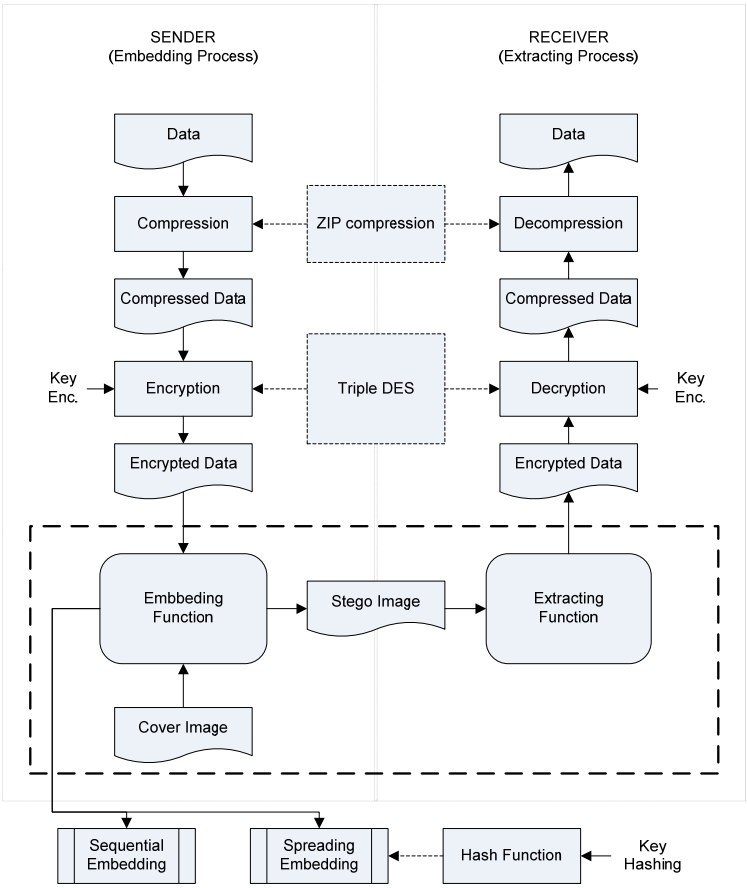
2.1. Steganografi

Steganografi / *Steganography*[1] merupakan seni untuk menyembunyikan pesan di dalam pesan lainnya sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu di dalam pesan tersebut. Kata steganografi (*steganography*) berasal dari bahasa Yunani *steganos*, yang artinya 'terselubung', dan *graphein*, yang artinya 'menulis' sehingga kurang lebih artinya "menulis (tulisan) terselubung". Teknik ini meliputi banyak sekali metode komunikasi untuk menyembunyikan pesan rahasia. Metode ini termasuk tinta yang tidak tampak, microdots, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar.

Walaupun steganografi dapat dikatakan mempunyai hubungan yang erat dengan kriptografi, tapi metoda ini sangat berbeda dengan kriptografi. Kriptografi mengacak pesan sehingga tidak dimengerti, sedangkan steganografi menyembunyikan pesan sehingga tidak terlihat. Pesan dalam cipherteks mungkin akan menimbulkan kecurigaan sedangkan pesan yang dibuat dengan steganografi tidak akan. Kedua teknik ini pada umumnya selalu dikombinasikan untuk mendapatkan metode pengiriman rahasia yang sulit dilacak. Pertama pesan dienkrip, kemudian cipherteks disembunyikan dengan cara steganografi pada media yang tampak tidak mencurigakan.

2.2. Proses Steganografi

Penelitian steganografi ini menggunakan 3 (tiga) tahapan dalam prosesnya yaitu tahapan kompresi (untuk memperbesar kapasitas penyisipan), enkripsi (untuk lebih menjaga keamanan data) dan embedding (proses penyisipan data pesan ke media stego).

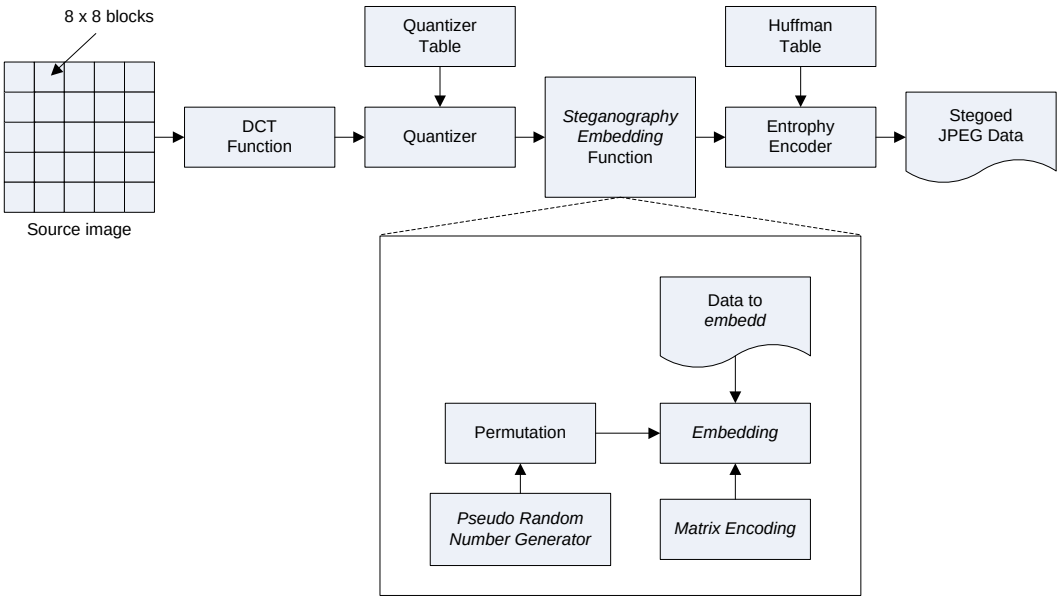


Gambar 1 Blok diagram dari tahapan Steganografi[4]

2.3. Steganografi pada JPEG format

Selain metode *sequential* (*low bit coding*) yang umum digunakan dalam proses steganografi, metode *spreading* juga merupakan salah satu algoritma yang dipakai dalam melakukan proses steganografi pada citra dengan format JPEG. Alur dari algoritma *spreading* ini dapat dilihat seperti diagram blok pada Gambar 2.

Terdapat beberapa proses tambahan yang harus dilakukan pada proses embedding data, algoritma ini menggunakan metode *hashing* untuk mendapat posisi *offset* pada data citra untuk melakukan penyisipan data pada koefisien DCT. Algoritma ini juga menggunakan *matrix encoding* untuk melakukan optimasi pada proses *embedding* data.



Gambar 2 Alur algoritma spreading[2]

Adapun urutan tahapan-tahapan yang harus dilakukan dalam implementasi algoritma ini adalah sebagai beikut :

1. Melakukan proses kompresi citra JPEG. Dimulai dari pengambilan blok 8x8 pada citra asli, lalu dilanjutkan dengan proses transformasi DCT. Setelah itu dilanjutkan dengan proses kuantisasi. Hentikan proses kompresi sementara sampai pada tahap kuantisasi.
2. Menginisialisasi PRNG (*pseudo random generator number*) dengan menggunakan key dari kata sandi yang diberikan.
3. Melakukan proses permutasi dengan menggunakan parameter PRNG dan jumlah dari koefisien DCT.
4. Menentukan nilai k dari kapasitas *embedding* pada data citra dan dari panjang data pesan yang akan disisipkan.
5. Menentukan panjang dari *code word* (array yang akan menampung koefisien *non zero*) dengan rumus, yaitu n = 2k – 1.
6. Melakukan proses *embedding* untuk menyisipkan data pesan dengan algoritma (1, n, k) untuk *matrix encoding*.
   a. Mengisi array buffer dengan koefisien *non zero* (koefisien DCT yang <> 0).
   b. Melakukan proses *hashing* pada buffer (untuk menghasilkan nilai *hash* dengan k *bit-places*).
   c. Menambahkan k bit berikutnya dari data pesan pada nilai hash (lakukan pada bit per bit dengan operator XOR).
   d. Jika hasil yang didapatkan sama dengan 0, maka nilai buffer dibiarkan tetap dan tidak diubah. Tetapi jika hasil yang didapat sama dengan nilai rentang index pada buffer, yaitu 1 ... n, maka nilai absolut dari elemen pada index tersebut harus dikurangi 1.
   e. Melakukan pengecekan jika koefisien yang dirubah tidak sama dengan 0. Jika sama, maka terjadi proses *shrinkage*. Jika peristiwa ini terjadi maka tambahkan satu koefisien *non zero* pada buffer dan hilangkan nilai koefisien 0 tadi. Lalu ulangi langkah 6a
   f. Jika tidak terjadi peristiwa *shrinkage* maka isi buffer dengan koefisien DCT selanjutnya (dimulai dari index koefisien terakhir ditambah satu). Jika masih ada data pesan yang akan disisipkan maka ulangi langkah 6a.
   g. Jika semua proses *embedding* telah selesai, maka lanjutkan proses kompresi data JPEG hingga tahap kompresi akhir (proses *Huffman coding*, RLE dan seterusnya).
7. Output berupa data citra JPEG yang terstego.

3. HASIL DAN PEMBAHASAN

Pengujian dilakukan terhadap 30 (tiga puluh) buah data citra serta 5 (lima) buah *file* teks dengan ukuran yang berbeda. Tujuan dari pengujian ini adalah untuk menjawab beberapa hal penting yang berkaitan dengan kemampuan dari proses steganografi dalam menyisipkan data pesan yang tersembunyi dengan menggunakan metode *sequential/low bit coding* dan *spreading.*

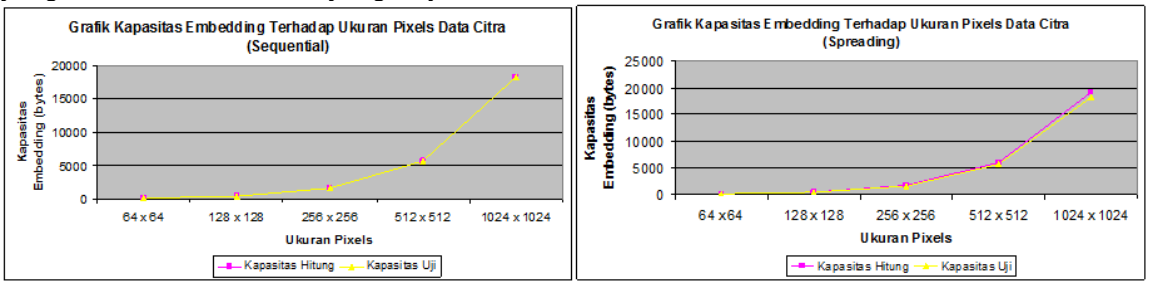
3.1. Pengujian kapasitas embedding

Pengujian kapasitas embedding ini dilakukan untuk mengetahui tingkat kapasitas embedding yang dapat digunakan dalam setiap data citra serta faktor-faktor yang dapat mempengaruhi besar kapasitas embedding itu sendiri.

Tabel 1 Data Pengujian kapasitas embedding terhadap ukuran pixels pada data citra (sequential)

Ukuran Pixels	Ukuran Data Citra (*bytes*)	Kapasitas embedding (*bytes*)		Kapasitas Uji (*bytes*)	
		Sequential	Spreading	Sequential	Spreading
64 x 64	1806	137	147	133	134
128 x 128	4526	462	496	458	464
256 x 256	13909	1617	1731	1613	1613
512 x 512	47401	5789	6155	5785	5783
1024 x 1024	154631	18264	19130	18260	18263

Grafik berikut menunjukkan pengaruh ukuran pixels terhadap kapasitas embedding yang dimiliki oleh data citra yang diujikan.



Gambar 3 Grafik kapasitas embedding terhadap ukuran pixels data citra

Kecenderungan yang diperoleh adalah semakin besar ukuran *pixels* dari data citra maka semakin besar pula kapasitas *embedding* yang dimiliki data citra tersebut. Sehingga dari pengujian dapat disimpulkan bahwa besar ukuran *pixels* mempunyai perbandingan yang searah dengan kapasitas *embedding* dari data citra.

3.2. Pengujian Statistik Data Citra Asli dan Data Citra Stego

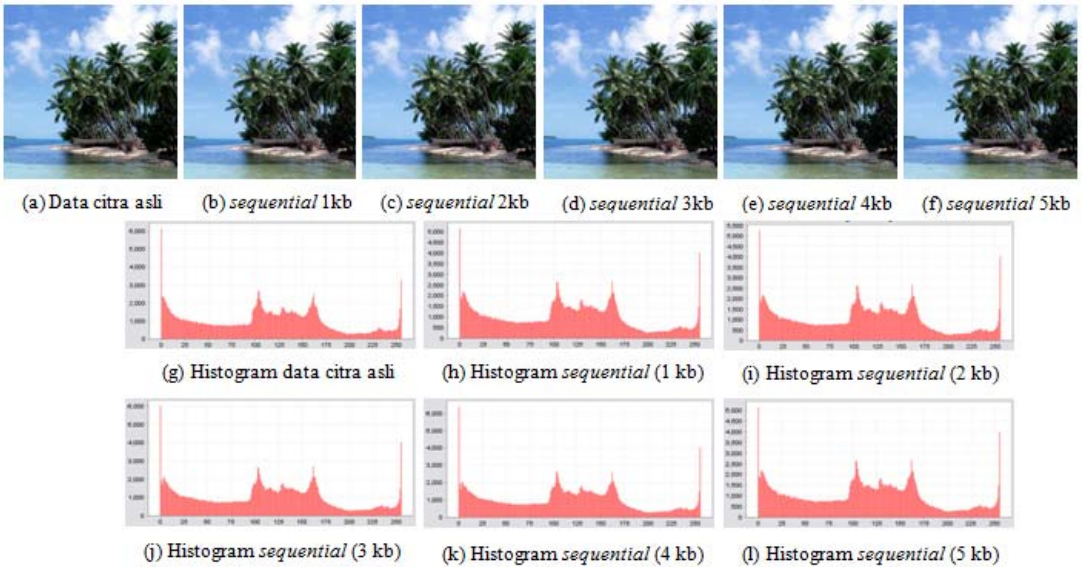
Pengujian statistik dilakukan dengan menghitung *error measurement* yang terjadi pada data citra yang asli dengan data citra yang telah mengalami proses steganografi (data citra terstego). Nilai yang digunakan dalam pengujian statistik ini antara lain [13] : *Maximum Absolute Difference* (MAD), *Normalized Euclidean Distance* (NED), *Average Quantization Error* (AVQ), *Signal-to-Noise Ratio*(SNR), *Peak Signal-to-Noise Ratio* (PSNR), *Pearson Correlation* (Corr).

3.2.1. Pengaruh jumlah penyisipan *bytes* terhadap nilai *error measurement*

Pengujian pertama digunakan sebuah sample citra untuk melakukan pengujian *embedding* 5 (lima) sample data teks dengan ukuran berbeda. Hasil pengujian *embedding* disajikan sebagai berikut.

Tabel 2 Data statistik error measurement dengan metode sequential

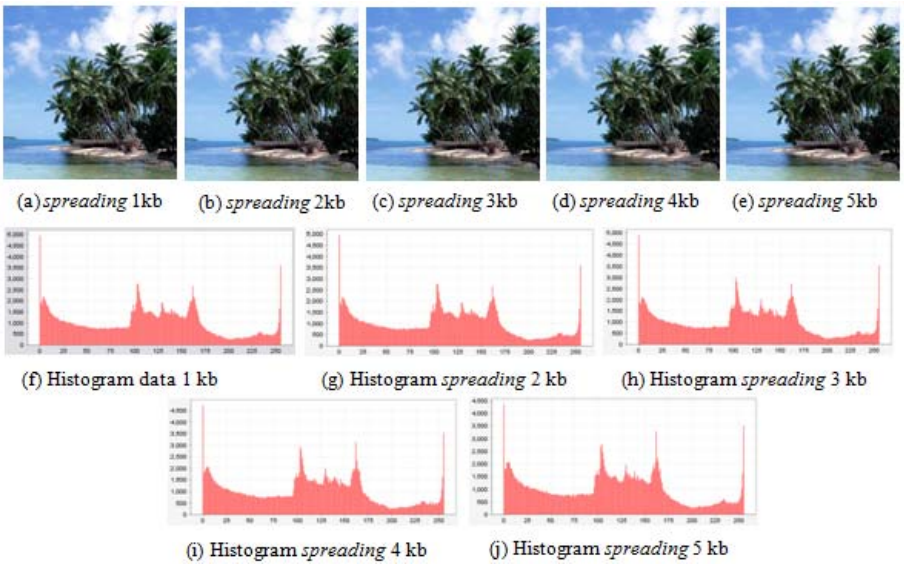
Data teks (*kilobytes*)	Error Measurement					
	MAD	NED	AQE	SNR	PSNR	Corr
1	30	0.005155	1.546835	40.05438	45.1205	0.996497
2	30	0.007269	2.159716	37.06888	42.1102	0.994389
3	36	0.008928	2.730948	35.28274	40.34929	0.992133
4	36	0.010189	3.283038	34.13467	38.58838	0.990435
5	36	0.011407	3.846665	33.1534	37.71688	0.988462



Gambar 4 Data citra dan histogram hasil pengujian metode sequential (semua sample teks)

Tabel 3 Data statistik error measurement pada sebuah citra yang dipilih dengan metode spreading

Data teks (*kilobytes*)	Error Measurement					
	MAD	NED	AQE	SNR	PSNR	Corr
1	23	0.005273	1.780571	39.85741	45.1205	0.994972
2	33	0.008061	2.633772	36.17	41.1411	0.992397
3	35	0.010637	3.423045	33.76029	38.58838	0.989969
4	44	0.012153	4.203143	32.6031	37.33899	0.987153
5	44	0.014198	4.713135	31.25156	35.82631	0.985961



Gambar 5 Data citra dan histogram hasil pengujian metode spreading (semua sample teks)

Hasil pengujian menunjukkan bahwa ukuran data pesan yang disisipkan tidak terlalu mempengaruhi kualitas data citra yang dihasilkan dalam proses *embedding*. Sekilas kualitas citra terstego dibandingkan dengan kualitas citra asli tidak memiliki perbedaan yang signifikan bahkan perbedaan dan distorsi tersebut tidak terlihat. Hal yang sama juga dapat dilihat pada data histogram masing-masing citra tersebut.

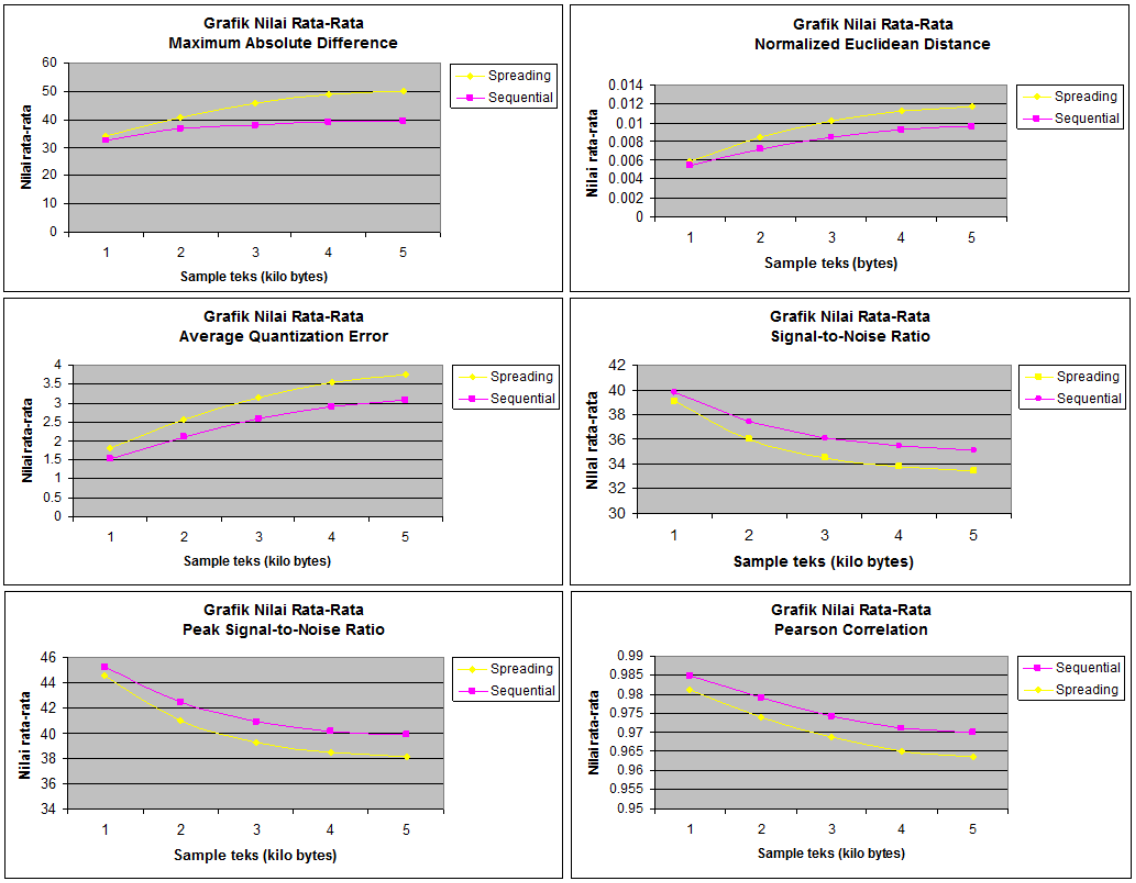
Pengujian berikutnya dilakukan pada 30 sample citra dengan meng-*embedding* ke-lima sample data teks dengan menggunakan metode *sequential* dan *spreading*.

Tabel 4 Nilai rata-rata error measurement 30 sample data citra untuk metode sequential

Data teks (*kilobytes*)	Error Measurement					
	MAD	NED	AQE	SNR	PSNR	Corr
1	32.4	0.005474	1.529533	39.80925	45.22248	0.984923
2	36.667	0.007202	2.089217	37.41286	42.44726	0.979284
3	38.1	0.008472	2.580346	36.06698	40.92374	0.974347
4	39.033	0.009214	2.91164	35.42993	40.14555	0.971113
5	39.333	0.009601	3.088245	35.14047	39.90031	0.969927

Tabel 5 Nilai rata-rata error measurement 30 sample data citra untuk metode spreading

Data teks (*kilobytes*)	Error Measurement					
	MAD	NED	AQE	SNR	PSNR	Corr
1	33.9	0.005952	1.801817	39.06144	44.50646	0.981002
2	40.733	0.008467	2.553017	36.02142	40.95175	0.974081
3	45.733	0.010182	3.146298	34.48915	39.26572	0.968911
4	48.767	0.011181	3.547169	33.79026	38.50696	0.965217
5	49.767	0.011694	3.748553	33.47351	38.16348	0.963609



Gambar 6 Nilai rata-rata error measurement pada embedding sample data teks

Hasil pengujian menunjukkan bahwa kedua metode menghasilkan citra output yang mempunyai kualitas yang cukup bagus, ditunjukkan dari nilai rata-rata untuk SNR dan PSNR.

3.2.2. Pengaruh ukuran pixels data citra terhadap nilai *error measurement*

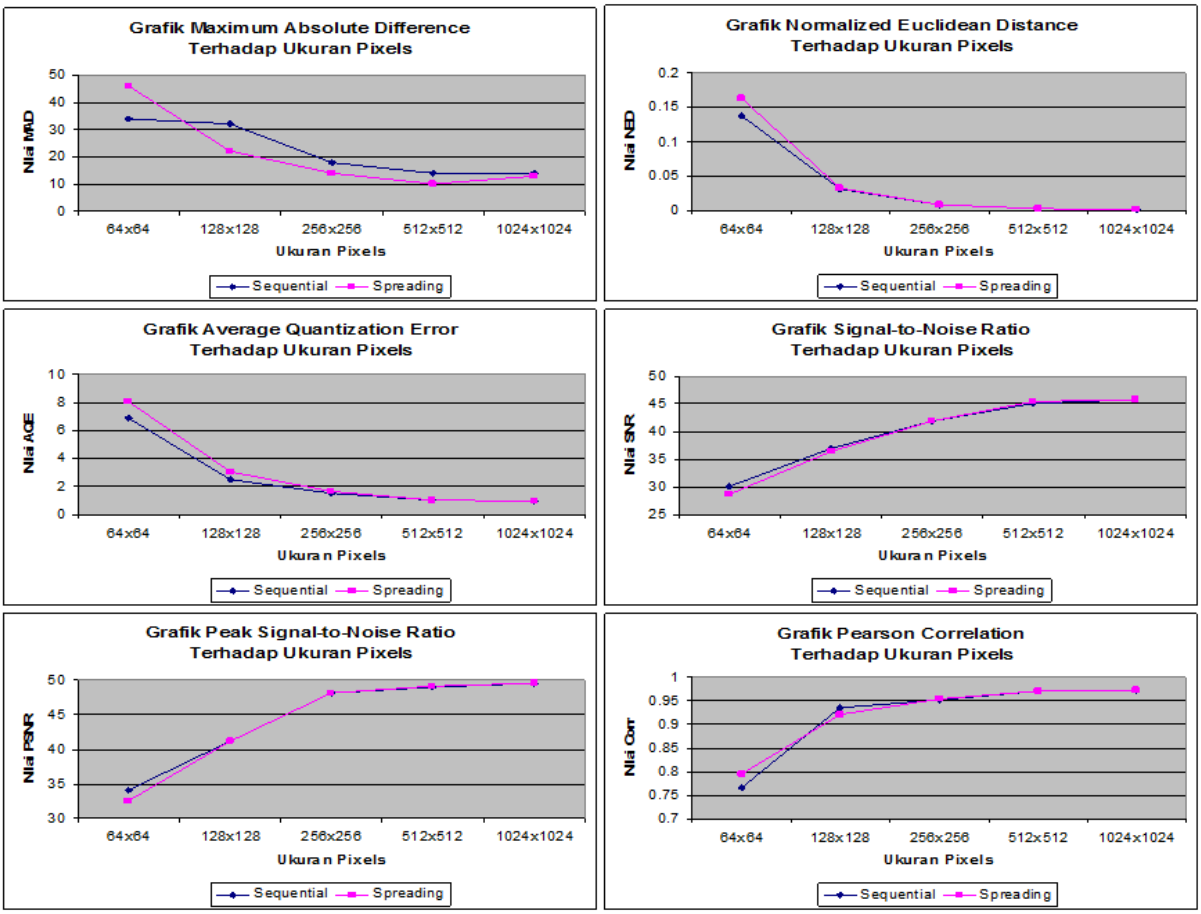
Pengujian dilakukan pada sebuah sample citra yang dipilih, memilki ukuran *pixel* yaitu 64x64, 128x128, 256x256, serta 512x512 *pixel*. Hasil pengujian *embedding* sebagai berikut:

Tabel 6 Data pengujian pengaruh ukuran pixels terhadap error measurement (sequential)

Ukuran Pixels	Error Measurement					
	MAD	NED	AQE	SNR	PSNR	Corr
64x64	34	0.1376776	6.8948257	30.111474	34.151404	0.7663323
128x128	32	0.0312741	2.5308529	36.974909	41.141104	0.9355016
256x256	18	0.0089523	1.5502978	41.825288	48.130804	0.9515505
512x512	14	0.0030639	1.0419203	45.124042	48.991199	0.9711906
1024x1024	14	0.001433	0.9886923	45.707647	49.571191	0.9724178

Tabel 7 Data pengujian pengaruh ukuran pixels terhadap error measurement (spreading)

Ukuran Pixels	Error Measurement					
	MAD	NED	AQE	SNR	PSNR	Corr
64x64	46	0.1626737	8.0746003	28.662873	32.567779	0.794704
128x128	22	0.0329109	3.0549178	36.531159	41.141104	0.9220173
256x256	14	0.0089439	1.6846132	41.833553	48.130804	0.9549142
512x512	10	0.002985	1.0477657	45.350788	49.217851	0.9717263
1024x1024	13	0.0014252	0.9893081	45.755227	49.618774	0.9724016



Gambar 7 Pengaruh pengujian ukuran pixels terhadap error measurement

Hasil pengujian menunjukkan bahwa ukuran *pixel* mempunyai pengaruh yang cukup besar terhadap nilai *error measurement* antara citra terstego dengan citra asli.

3.3 Pengujian Kualitas Citra dengan MOS (*Mean Opinion Score*)

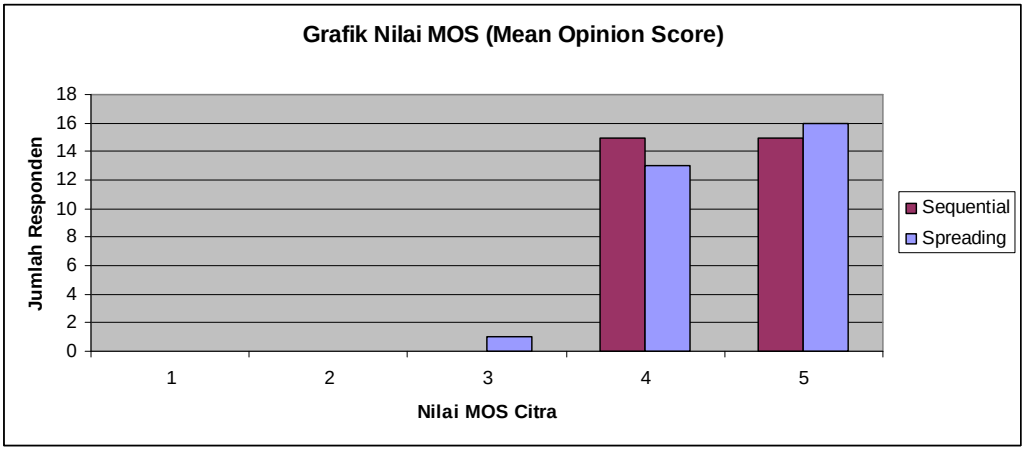
Pengujian kualitas data citra juga berkaitan dengan kemungkinan penyerangan steganografi dengan menggunakan metode *visual attack*. Pengujian ini diujikan dengan melakukan survey pada 30 koresponden yang menilai kualitas citra tersebut secara subyektif. Pengujian dilakukan dengan menganalisa citra yang telah mengalami proses steganografi baik dengan metode *sequential* dan *spreading*. Data citra tersebut dianalisa untuk mengetahui distorsi yang terjadi akibat proses steganografi serta analisa mengenai baik buruknya kualitas citra yang dihasilkan. Pengujian ini dilakukan dengan menggunakan HVS (*human visual system*) atau sistem penglihatan manusia.

Tabel dan grafik berikut menunjukkan hasil pengujian tersebut.

Tabel 8 Hasil pengujian metode MOS (Mean Opinion Score)

Nilai	Metode Embedding	
	Sequential	Spreading
1	0	0
2	0	0
3	0	1
4	15	13
5	15	16

MOS	4.5	4.5



Gambar 8 Grafik pengujian metode MOS (Mean opinion Score)

Tabel 9 *Keterangan nilai MOS* [15] *:*

MOS	Kualitas Citra	Keterangan
5	Sangat Bagus	Kesamaan citra mencapai 100 – 90%
4	Bagus	Kesamaan citra mencapai 90 – 70%
3	Sedang	Kesamaan citra mencapai 70 – 60%
2	Buruk	Kesamaan citra mencapai 60 – 40%
1	Sangat Buruk	Kesamaan citra mencapai < 40%

Tabel 8 serta grafik pada gambar 8 menunjukkan bahwa kualitas citra yang dihasilkan cukup bagus dimana dalam pengujian dengan metode MOS (*Mean opinion Score*), nilai MOS yang didapatkan oleh kedua metode tersebut adalah sama, yaitu 4.5 atau mendekati kualitas sangat bagus.

3.3. Pengujian Penyerangan pada Sistem Steganografi

Pengujian penyerangan teknik steganografi dilakukan dengan merusak data citra yang menjadi media stego serta ketahanan dari teknik steganografi tersebut terhadap manipulasi yang dilakukan pada media stego tersebut. Proses pengujian dilakukan dengan cara merubah format data citra JPEG terstego menjadi format citra lain dan/atau diikuti dengan proses manipulasi, kemudian dikembalikan lagi ke dalam format JPEG. Setelah itu dilakukan proses *extracting* untuk mendapatkan data *hiding*-nya. Hasil pengujian ketahanan yang dilakukan pada 5 (lima) buah sample citra terstego yang dipilih adalah sebagai berikut

.

Tabel 10 Hasil pengujian steganografi untuk robustness

Data Citra	Jumlah Bit Error (%)					Validitas (1 = valid, 0 = Tidak Valid)				
	TE1	TE2	TE3	TE4	TE5	TE1	TE2	TE3	TE4	TE5
Img001.jpg	100	100	100	100	100	0	0	0	0	0
Img002.jpg	100	100	100	100	100	0	0	0	0	0
Img003.jpg	100	100	100	100	100	0	0	0	0	0
Img004.jpg	100	100	100	100	100	0	0	0	0	0
Img005.jpg	100	100	100	100	100	0	0	0	0	0

Tabel 11 Tingkat keberhasilan proses ekstraksi pengujian ketahanan data hiding

Data Citra	Jumlah Bit Error (%)				
	TE1	TE2	TE3	TE4	TE5
Img001.jpg	0	0	0	0	0
Img002.jpg	0	0	0	0	0
Img003.jpg	0	0	0	0	0
Img004.jpg	0	0	0	0	0
Img005.jpg	0	0	0	0	0

Keterangan:
- TE1 : Pengujian perubahan format data dari JPEG ke GIF kemudian kembali ke JPEG
- TE2 : Pengujian perubahan level *brightness* / *contrast*
- TE3 : Pengujian perubahan saturasi warna pada data citra
- TE4 : Pengujian pemberrian efek *blur*
- TE5 : Pengujian *cropping*

Berdasarkan hasil pengujian, data hiding dalam data citra dengan format JPEG setelah mengalami kompresi mengalami kegagalan dalam proses ekstraksinya. Begitu pula ketika dilakukan pengujian terhadap manipulasi data citra seperti perubahan level *brightness* dan *contrast*, perubahan saturasi warna, pemberian efek *blur* serta manipulasi data citra dengan melakukan *cropping*, data *hiding* yang ada dalam media stego tersebut rusak ini terbukti ketika proses ekstraksi dilakukan, validitas data pesan yang tersimpan adalah 0% karena sama sekali tidak sama dengan data aslinya sehingga dapat dikatakan data rusak saat terjadi manipulasi pada media stego tersebut. Hal ini disebabkan karena bit-bit yang disisipkan dalam block DCT ketika ditransformasikan kembali menjadi domain waktu, nilai-nilainya akan disebarkan secara merata. Saat akan melakukan ekstraksi, nilai-nilai koefisen block DCT yang didapatkan dari hasil ekstraksi akan berbeda dengan saat sebelum disisipkan data hiding. Dari hasil pengujian didapatkan apabila ada perubahan pada bit-bit di domain waktu seperti ketika mengalami kompresi, akan berpengaruh terhadap nilai DCT-nya, dan menyebabkan nilai koefisian DCT berubah. Dengan pengujian ini, dapat dikatakan metode steganografi baik *spreading* maupun *sequential* tidak *robust* terhadap proses manipulasi pada data citra yang menjadi penampungnya.

3.4. Analisa Keseluruhan

Hasil pengujian menunjukkan bahwa tingkat validitas data tidak dipengaruhi dari besarnya file, hanya saja besar kapasitas data yang bisa disisipkan berbeda-beda pada setiap data citra dan hal ini disebabkan karena tidak semua tempat pada block DCT dari setiap data citra yang dapat disisipkan bit-bit pesan. Hal ini sangat tergantung pada jumlah dari koefisien DCT yang nilainya tidak sama dengan ‘0’ dan ‘1’. Kapasitas data yang dapat disisipkan pada data citra juga dapat dipengaruhi oleh komposisi dan keragaman warna yang membentuk data citra tersebut, dengan kata lain dapat dikatakan bahwa data citra yang berukuran sama belum tentu mempunyai kapasitas *embedding* yang sama antara satu dengan yang lainnya. Kapasitas *embedding* sangat dipengaruhi oleh tingkat variasi komposisi dan keragaman warna yang membentuk data citra tersebut. Kapasitas *embedding* juga dipengaruhi oleh besarnya ukuran *pixels* pada data citra, dimana semakin besar ukuran *pixels* data citra maka semakin besar kapasitas yang dimiliki citra tersebut.

Apabila koefisien DC dari block DCT hasil ekstraksi dibandingkan dengan block DCT saat penyisipan terjadi pergeseran nilai lebih dari 1, berarti terjadi perubahan nilai koefisien DCT secara keseluruhan. Hal ini diakibatkan adanya perubahan nilai yang cukup besar pada *byte-byte* domain waktu seperti nilai 0 bergeser mundur menjadi 255 dan begitu juga sebaliknya

Jumlah *byte* yang disisipkan pada setiap block DCT pada setiap data citra berpengaruh kepada kualitas dari data citra yang dihasilkan. Semakin banyak jumlah *byte* yang disisipkan pada setiap block DCT, semakin rendah kualitas data citra yang dihasilkan. Nilai PSNR di bawah 30 dB mulai menunjukan kerusakan pada data citra. Dalam pengujian ini, tingkat

kualitas data citra yang dihasilkan pada metode *sequential* dan *spreading* memiliki kualitas yang cukup bagus dan memiliki nilai rata-rata lebih besar dari 30 dB. Tingkat kesamaan antara data citra asli dengan data citra yang terstego juga cukup tinggi, yaitu memiliki tingkat kesamaan rata-rata sebesar $\pm$ 96 % (di peroleh dari nilai rata-rata *pearson correlation* yang dimiliki).

Error measurement yang dihasilkan oleh metode *sequential* secara keseluruhan memiliki nilai yang lebih kecil jika dibandingkan dengan nilai *error* yang dihasilkan oleh metode *spreading*. Besar nilai e*rror measurement* yang dihasilkan juga dipengaruhi oleh besarnya ukuran data pesan yang disisipkan pada data citra tersebut, semakin besar ukuran data yang disisipkan maka nilai *error* yang dihasilkan akan semakin besar pula.

Untuk teknik penyisipan data *hiding* pada data citra dengan transformasi DCT, ternyata memilki sifat data *hiding* yang tidak *robust*, sangat rentan terhadap proses manipulasi wadah penampungnya. Tetapi teknik penyisipan ini cukup baik sebab bisa menghasilkan data *hiding* yang memiliki tingkat validitas mencapai 100 %, dan bisa dikatakan bahwa data hasil ekstraksi sama dengan data aslinya, tetapi dengan syarat bahwa data citra yang menjadi media stego-nya memiliki kapasitas *embedding* yang cukup untuk melakukan proses *embedding*.

4. KESIMPULAN

Analisa keseluruhan yang dapat diambil bedasarkan hasil pengujian yang diperoleh adalah bahwa metode steganografi dengan menggunakan data citra JPEG sebagai media stego merupakan alternatif yang cukup bagus dalam teknik penyembunyian data. Hal ini didukung dengan hasil data citra yang dihasilkan dari proses *embedding* tersebut memiliki tingkat kesamaan yang cukup tinggi dengan citra aslinya, yaitu sebesar $\pm$ 96 %, serta kualitas yang dihasilkan cukup bagus dengan memiliki nilai PSNR lebih besar dari 36 dB. Validitas data ekstraksi yang dimiliki juga mencapai 100 % dimana nilai validitas dari data yang terpotong akibat kapasitas *embedding* yang tidak mencukupi diabaikan.

5. DAFTAR PUSTAKA

[1] Berg G, Davidson, Ming-Yuan Duan, Paul G. 2003, Searching For Hidden Messages: Automatic Detection of Steganography. Washington: Computer Science Department, University at Albany (dokumen PDF).
[2] Simsek, B. 2004. Steganography In JPEG Images. Dokuz Eylul University (dokumen PDF).
[3] Van Droogenbroeck, M. 2002. Techniques for a Selective Encryption of Uncompressed and Compressed Images. Belgium: Department of Electricity, Electronics and Computer Science (dokumen PDF).
[4] Westfeld, A. 2001. F5-A Steganographic Algorithm, High Capacity Despite Better Steganalysis. Dresden: Technische Universitat at Dresden (dokumen PDF).
[5] http://en.wikipedia.org/wiki/Cryptography, diakses tanggal 12/02/2010.
[6] http://kremlinencrypt.com/algorithms.htm#DES, diakses tanggal 14/01/2010.
[7] http://www.fact-index.com/l/lo/lossless_data_compression.html, diakses tanggal 18/05/2010
[8] http://www.fact-index.com/l/lo/lossy_data_compression.html, diakses tanggal 11/10/2010
[9] http://www.fact-index.com/h/hu/huffman_coding.html, diakses tanggal 18/05/2010.
[10] http://en.wikipedia.org/wiki/JPEG, diakses tanggal 18/07/2010.
[11] http://www.fourcc.org/fccyvrgb.php, diakses tanggal 02/06/2010.
[12] http://www.cs.sfu.ca/CourseCentral/365/li/material/notes/Chap4/Chap4.2/Chap4.2.html, diakses tanggal 18/05/2010.
[13] http://osl.iu.edu/%7Etveldhui/papers/MAScThesis/node18.html, diakses tanggal 18/12/2010.
[14] http://en.wikipedia.org/wiki/PSNR, diakses tanggal 18/12/2010.
[15] http://en.wikipedia.org/wiki/ Mean_Opinion_Score, diakses tanggal 05/04/2010.