



Quality Factor terhadap Kapasitas Pesan Rahasia pada Steganografi Citra JPEG dan Kualitas Citra Stego

Dian Hafidh Zulfikar

dianhafidhzulfikar@uin@radenfatah.ac.id

Universitas Islam Negeri Raden Fatah Palembang - Indonesia

Diterima: 30 Sep 2020 | Direvisi: 15 Okt - 09 Nov 2020
Disetujui: 09 Des 2020 | Dipublikasi: 28 Des 2020
Program Studi Sistem Informasi, Fakultas Sains dan Teknologi,
Universitas Islam Negeri Raden Fatah Palembang, Indonesia

ABSTRACT

One of the container media that is available and popular is the Joint Photographic Experts Group (JPEG) format image. This article aims to determine the effect of Quality Factor on the secret message capacity of JPEG image steganography and stego image quality. The quality of an image can actually be seen subjectively with the human eye, but this is relative between each individual. Because the assessment of the human eye varies from person to person. In addition, the effect of Quality Factor on secret message capacity is not yet known whether it has an impact. Therefore, in this study the Quality Factor is used to objectively see the secret message capacity of the JPEG image steganography and the quality of the stego image. The parameter used to determine the quality of an image is the Peak Signal to Noise Ratio (PSNR). PSNR will compare the quality of the original image (before steganography) with the stego image. The test results show that the Q Factor effect can affect the secret message capacity of the JPEG image steganography and the stego image quality. The bigger the Q Factor, the more the message capacity is generated. The greater the Q factor, the better the quality of the resulting stego image.

Keywords: *Stego image, Steganography, Joint Photographic Experts Group*

ABSTRAK

Salah satu media penampung yang mudah didapatkan dan populer digunakan adalah citra dengan format Joint Photographic Experts Group (JPEG). Artikel ini bertujuan untuk mengetahui efek Quality Factor terhadap kapasitas pesan rahasia pada steganografi citra JPEG dan kualitas citra stego. Kualitas sebuah citra sebenarnya dapat dilihat secara subyektif dengan mata manusia, namun hal ini bersifat relatif antara setiap individu. Karena penilaian mata antara orang satu dengan orang lain berbeda-beda. Selain itu juga, efek Quality Factor terhadap kapasitas pesan rahasia belum diketahui apakah memiliki dampak. Oleh karena itu pada penelitian ini digunakan Quality Factor untuk melihat secara objektif kapasitas pesan rahasia pada steganografi citra JPEG dan kualitas citra stego. Parameter yang digunakan untuk menentukan kualitas suatu citra adalah Peak Signal to Noise Ratio (PSNR). Parameter PSNR akan membandingkan kualitas citra asli (sebelum steganografi) dengan citra stego. Hasil pengujian bahwa efek Q Factor dapat mempengaruhi kapasitas pesan rahasia pada steganografi citra JPEG dan kualitas citra stego. Semakin besar Q Factor maka semakin meningkat pula kapasitas pesan yang dihasilkan. Semakin besar Q Factor maka semakin baik kualitas citra stego yang dihasilkan.

Kata Kunci: *Citra Stego, Steganografi, Joint Photographic Experts Group*

PENDAHULUAN

Steganografi merupakan domain keamanan yang sangat penting (Battikh et al., 2019). Pertukaran pesan ataupun informasi melalui suatu jaringan sangat penting untuk

dijaga. Apabila informasi tersebut jatuh ke pihak yang tidak berwenang, maka dapat menimbulkan kerugian (Gunawan & Fenando, 2018). Selain itu, terkait risiko keamanan yang juga tidak kalah pentingnya perlu untuk diperhatikan (Hamzah et al., 2020). Di sisi lain steganografi disebutkan sebagai perpaduan antara ilmu dan seni yang digunakan dalam berkomunikasi rahasia dengan cara menyembunyikan isi pesan ke dalam suatu media penampung tanpa menyebabkan media penampung berubah setelah dilakukan penyisipan (Abdel Wahab et al., 2019). Salah satu media penampung yang mudah didapatkan dan populer digunakan adalah citra dengan format *Joint Photographic Experts Group (JPEG)*. Metode steganografi dapat dikatakan baik apabila memenuhi beberapa faktor yaitu eksistensi dari informasi yang disisipkan tidak dapat diketahui (*imperceptibility*), kemudian keberadaan media penampung setelah disisipkan informasi rahasia tidak jauh berbeda dari aslinya (*fidelity*), informasi rahasia yang telah disisipkan harus tahan terhadap beberapa operasi yang mungkin diterapkan pada citra penampung tersebut (*robustness*) dan ada sifat (*Recovery*) dimana informasi yang disisipkan harus dapat diungkap kembali (Darwis, 2017).

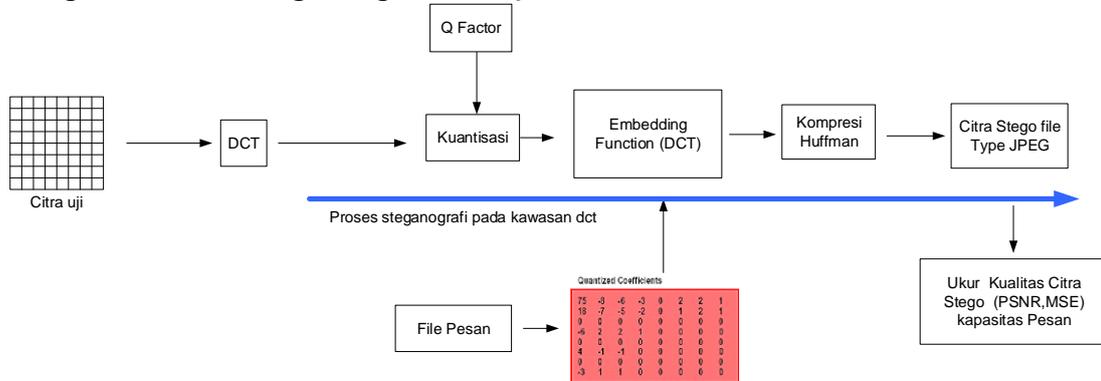
Steganografi pada citra *JPEG* dilakukan pada tahapan proses kompresi citra *JPEG* (Jóokay & Moravčík, 2010; Zulfikar & Harjoko, 2016). Proses kompresi pada citra merupakan proses untuk menghilangkan informasi yang tidak diperlukan, hal ini dilakukan untuk mengurangi kapasitas dari citra *JPEG*. Proses ini dilakukan pada tahapan pembentukan citra *JPEG*, terjadi pada proses kuantisasi pada nilai koefisien *Discrete Cosine Transform (DCT)*. Proses steganografi pada citra *JPEG* dilakukan setelah proses kompresi, yaitu setelah proses kuantisasi nilai *DCT* dilakukan. Pada penelitian (Pandit et al., 2013), digunakan *Quality Factor* untuk mengatur (besar/kecil) kompresi citra *JPEG* yang akan dilakukan. Pada penelitian (Singh, 2017), dijelaskan bahwa setiap format citra memiliki katakteristik masing-masing serta kelebihan dan kelemahannya masing-masing.

Citra *JPEG* digunakan dalam penelitian ini, dimana citra *JPEG* ini banyak dimanfaatkan untuk berbagai keperluan, khususnya untuk transmisi data di jaringan *internet* (Darbani et al., 2019). Berdasarkan (w3techs.com, 2020), citra dengan format *JPEG* berada pada peringkat kedua paling populer, dengan sebaran 72,2% penggunaan citra *JPEG* dari berbagai situs di internet. Artikel ini bertujuan untuk mengetahui efek *Quality Factor* terhadap kapasitas pesan rahasia pada steganografi citra *JPEG* dan kualitas citra stego. Citra yang merupakan hasil dari proses steganografi inilah yang disebut citra stego (Nur'aini, 2019). Kualitas sebuah citra sebenarnya dapat dilihat secara subyektif dengan mata manusia (Andriotis et al., 2013), namun hal ini bersifat relatif antara setiap individu. Masing-masing individu memiliki penilaian yang berbeda ketika mereka melihat secara langsung dengan menggunakan mata mereka (Altaay et al., 2012). Selain itu juga, efek *Quality Factor* terhadap kapasitas pesan rahasia belum diketahui apakah memiliki dampak. Oleh karena itu pada penelitian ini digunakan *Quality Factor* untuk melihat secara objektif kapasitas pesan rahasia pada steganografi citra *JPEG* dan kualitas citra stego. Dalam hal menentukan kualitas suatu citra secara umum parameter yang dapat digunakan adalah *Peak Signal to Noise Ratio (PSNR)* (Ansari et al., 2020). Dimana pada parameter *PSNR* akan membandingkan kualitas citra asli (sebelum steganografi) dengan citra stego (Kim et al., 2019).

METODOLOGI PENELITIAN

Gambaran umum penelitian pada artikel ini ditunjukkan pada Gambar 1 dimana citra asli akan dibagi ke dalam kelompok 8x8 pixel, selanjutnya citra mengalami proses yang disebut *Discrete Cosine Transform (DCT)* (Mythili et al., 2019), dan kuantisasi pada koefisien *DCT* dengan nilai *Quality Factor (Q Factor)* yang bervariasi. Tahap kuantisasi ini dilakukan untuk pembentukan citra yang baru, kemudian frekuensi yang tinggi

tersebut, diseleksi dan selanjutnya dihilangkan yang terikat pada pengaturan *Q Factor* yang telah ditentukan (Krasmla et al., 2017). Sampai tahap inilah proses penyisipan pesan pada steganografi citra *JPEG* dilakukan. Kemudian dilakukan proses kompresi citra menggunakan *Huffman Encoder* (Kim et al., 2019) yang akhirnya akan menghasilkan citra stego dengan format *JPEG*.



Gambar 1. Tahapan Penelitian

Nilai-nilai koefisien *DCT* tersebut adalah $F(u,v)$ dari suatu blok 8×8 dari citra pixel $f(x,y)$ dinyatakan pada persamaan (1) (Darbani et al., 2019).

$$F(u,v) = \frac{1}{4} C(u)C(v) \left[\sum_{x=0}^7 \sum_{y=0}^7 f(x,y) \cos \frac{(2x+1)u\pi}{16} \cos \frac{(2y+1)v\pi}{16} \right] \quad (1)$$

Dari persamaan (1), nilai $F(u,v)$ berbentuk matriks 2-dimensi 8×8 dimana:
 $u,v,x,y = 0,1,2,\dots,7$;
 x,y adalah koordinat spasial dari domain asal;
 u,v adalah koordinat frekuensi pada domain transformasi;
 $C(u), C(v) = 1/\sqrt{2}$ Untuk $u,v = 0$;
 $C(u), C(v) = 1$, untuk lainnya.

Dilanjutkan dengan proses kuantisasi dengan menggunakan persamaan (2).

$$F_Q(u,v) = \text{Round} \left(\frac{F[u,v]}{q[u,v]} \right) \quad (2)$$

Dengan ketentuan, $(q[u,v])$: tabel kuantisasi.

Tabel kuantisasi dihitung dengan Persamaan (3) Notasi F digunakan untuk sebagai *Q Factor* yang diinginkan, interval nilai mulai dari 1 sampai 100.

$$Q_{i,j} = \left\lceil \frac{50 + S + D_{i,j}}{100} \right\rceil \quad (3)$$

Dengan ketentuan:

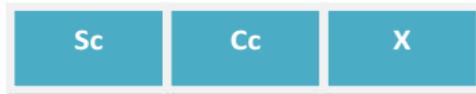
Q_{ij} : *Quantization Step*; D_{ij} : Elemen standar matrik kuantisasi.

Untuk menentukan parameter S yang digunakan, tergantung dari nilai F yang diinginkan, ketentuan parameter S adalah jika nilai $F \geq 50$ maka Nilai $S = 200 - 2F$ selain itu nilai $S = 5000/Q$ (Cogranne, 2018).

Nilai koefisien *Discrete Cosine (DC)* dari blok yang digabungkan yang selanjutnya disebut proses *Entropy Coding*, metode *Differential Pulse Code Modulation (DPCM)* diterapkan pada tahapan ini karena nilai-nilai koefisien *DC* antar blok tidak terlalu

berbeda (Bao et al., 2020). Nilai *DC* kemudian dikompresi menggunakan metode *huffman encoder*, namun urutan angka-angka tersebut akan diubah bentuknya menjadi pasangan-pasangan berupa (*size, amplitude*) dimana *size* menyatakan jumlah bit yang diperlukan untuk merepresentasikan jumlah angka *DPCM* dan *amplitude* menyatakan angka tersebut dalam bit (Jóokay & Moravčík, 2010). Selanjutnya dilakukan *Zig-zag scanning*, yaitu proses yang merubah matriks 8x8 hasil proses kuantisasi ke dalam vektor 1×2^8 , dengan pembacaan secara *zig-zag scanning*.

Pada proses *zig-zag scanning* ini koefisien *DCT* terkuantisasi yang bernilai nol cenderung terdeteksi secara urutan. *Run Length Code (RLC)* yaitu proses serangkaian simbol yang berurutan dikodekan menjadi suatu kode yang terdiri dari simbol tersebut dan jumlah pengulangannya. Data masukan akan dibaca dan sederetan karakter yang sesuai dengan karakter yang sudah ditentukan sebelumnya disubstitusi dengan kode tertentu. Kode khusus ini biasanya terdiri dari tiga buah karakter. Dapat dilihat pada Gambar 2.



Gambar 2. Karakter pada Run Length

Sumber: (Jóokay & Moravčík, 2010)

Pada penelitian ini citra uji akan diklasifikasikan berdasarkan kompleksitas citra dengan menggunakan *Gray-Level Co-occurrence Matrix (GLCM)*. Komponen Entropi sendiri merupakan satu fitur yang digunakan untuk mengukur kompleksitas atau keacakan suatu nilai pixel citra. Nilai Entropi akan bernilai tinggi ketika citra tidak seragam atau acak, sebaliknya akan bernilai rendah ketika keacakan nilai pixel citra semakin seragam atau cenderung sama.

Pengukuran Kapasitas Pesan Rahasia

Menurut (Abdel Wahab et al., 2019), proses penyisipan pesan dilakukan pada proses kompresi citra *JPEG*, yang dilakukan pada *output* nilai koefisien *DCT* hasil kuantisasi disesuaikan dengan tabel kuantisasi yang digunakan. Untuk menentukan kapasitas pesan yang dapat disisipkan, yaitu dengan cara menghitung nilai total koefisien *DCT* dikurangi dengan koefisien *DC*, koefisien *DCT* bernilai nol. Dapat dilihat pada persamaan (4).

$$\text{Kapasitas} = \#DCT(\text{total}) - \#DCT(-1) - \#DCT(1) - DCT(0) - \#DCT(\text{dc}) \quad (4)$$

Dengan ketentuan:

$\#DCT(\text{total})$: Total koefisien *DCT*,

$\#DCT(-1)$: Total koefisien *DCT* bernilai -1,

$\#DCT(1)$: Total koefisien *DCT* bernilai 1,

$\#DCT(0)$: Total koefisien *DCT* bernilai 0,

$\#DCT(\text{dc})$: Total koefisien *DC*.

Pengukuran Kualitas Citra

Dua parameter yang paling umum digunakan untuk menentukan kualitas citra asli dengan citra stego adalah *Mean Square Error (MSE)* dan *Peak signal to Noise Ratio (PSNR)* (Ansari et al., 2020; Malathi et al., 2020). Rumus untuk menghitung nilai *MSE*, dapat dilihat pada persamaan (5).

$$MSE = \frac{1}{M \times N} \sum_{x=1}^M \sum_{y=1}^N [I(x,y) - I'(x,y)]^2 \quad (5)$$

Dengan ketentuan:

MSE : Nilai *Mean Square Error* citra steganografi,

M : Panjang citra stego (dalam pixel),

N : Lebar citra stego (dalam pixel),

$I(x,y)$: Nilai pixel dari citra penampung (*cover image*),

$I'(x,y)$: Nilai pixel pada citra stego (*stego-image*).

Kemudian untuk menghitung nilai *PSNR*, dapat dilihat pada persamaan (6).

$$PSNR = 10 \cdot \log_{10} \left(\frac{MAX_i^2}{MSE} \right) \quad (6)$$

Sumber Citra Uji

Data citra pada penelitian ini yaitu dari <http://sipi.usc.edu/database/database.php> dari *USC University of Southern California*. Sebagian dapat dilihat pada Gambar 3.



Gambar 3. Beberapa Variasi Citra Uji yang Digunakan

HASIL DAN PEMBAHASAN

Pada penelitian ini, pengujian citra dilakukan berdasarkan tahapan penelitian yang telah ditampilkan pada Gambar 1. Selanjutnya, citra *JPEG* yang akan diujicobakan memiliki ukuran 128 x 128 pixel dengan jumlah citra uji sebanyak 15 citra. Berikut ini adalah hasil pengujian berdasarkan masing-masing parameternya.

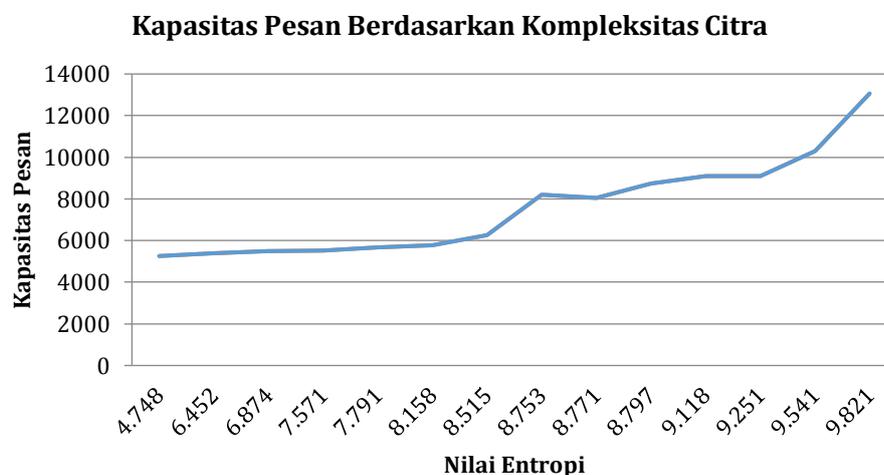
Pengujian Antara Keacakan (Kompleksitas) Nilai Pixel Citra Asli dengan Kapasitas Citra *JPEG*

Pada Tabel 1 ditampilkan hasil pengujian kapasitas penyisipan pada citra asli berdasarkan keacakan (kompleksitas) nilai pixel citra dengan *Q Factor* yang sama. Dalam hal ini digunakan nilai *Q Factor* adalah 100.

Tabel 1. Perbandingan Kapasitas Penyisipan pada Citra Asli Berdasarkan Kompleksitas Citra dengan Q Factor 100

No	Citra Asli	Nilai Entropi	Kapasitas Penyisipan (bits)
1	Verylow1.jpg	4.748	5257
2	Verylow2.jpg	6.452	5398
3	Verylow3.jpg	6.874	5495
4	Low1.jpg	7.571	5512
5	Low2.jpg	7.791	5670
6	Low3.jpg	8.158	5774
7	Middle1.jpg	8.515	6270
8	Middle2.jpg	8.753	8201
9	Middle3.jpg	8.771	8049
10	High1.jpg	8.797	8735
11	High2.jpg	9.118	9086
12	High3.jpg	9.251	9087
13	Veryhigh1.jpg	9.541	10303
14	Veryhigh2.jpg	9.821	13062
15	Veryhigh3.jpg	9.920	13076

Selanjutnya, pada Gambar 4, dapat dilihat bahwa kapasitas citra memiliki kecenderungan untuk meningkat seiring meningkatnya keacakan (kompleksitas) nilai pixel citra. Hal ini menunjukkan keberagaman nilai DCT hasil kuantisasi selain 0 dan 1 yang semakin banyak, dimana pada nilai-nilai selain 0 dan 1 itulah pesan rahasia akan disisipkan.

**Gambar 4. Grafik Perbandingan Kapasitas Penyisipan Citra Asli Berdasarkan Kompleksitas Citra dengan Q Factor**

Keterkaitan Antara Kapasitas Pesan dengan *Quality Factor (Q Factor)*

Pada Gambar 5 menampilkan data nilai kapasitas pesan rahasia berdasarkan variasi Q Factor yang digunakan. Dari hasil yang diperoleh, Q Factor berdampak terhadap kapasitas pesan yang akan ditampung oleh citra penampung, dimana semakin besar Q Factor maka semakin meningkat pula kapasitas pesan yang dihasilkan. Hal ini disebabkan pada Q Factor yang rendah dapat menyebabkan citra penampung mengalami

proses kompresi yang tinggi, sehingga banyak informasi citra yang dihilangkan, sedangkan pada *Q Factor* yang tinggi, citra penampung mengalami proses kompresi yang rendah, sehingga hanya sedikit informasi yang dihilangkan.

Nama Citra Ori	Nilai Entropy	Kapasitas Penyisipan (bits)									
		Q_10	Q_20	Q_30	Q_40	Q_50	Q_60	Q_70	Q_80	Q_90	Q_100
Verylow1.jpg	4.748	34	149	312	452	580	740	983	1341	2194	5257
Verylow2.jpg	6.452	61	150	293	550	702	957	1056	1190	2548	5398
Verylow3.jpg	6.874	70	193	502	766	1052	1304	2346	2529	4122	5495
Low1	7.571	90	296	547	934	1041	1080	2411	2665	2856	5512
Low2	7.791	136	479	658	979	1045	1085	2339	2508	2690	5670
Low3	8.158	156	615	977	1587	1635	1665	3500	3597	3780	5774
Middle1	8.515	168	703	1019	1579	1642	1682	3449	3580	3831	6270
Middle2	8.753	283	862	1261	1833	1726	2003	3828	4053	4370	8201
Middle3	8.771	266	908	1110	1511	1534	2135	3355	4389	4390	8049
High1	8.797	230	989	1213	1790	1794	1795	3603	4603	4603	8735
High2	9.118	286	1027	1525	1850	2035	2006	3126	4289	4562	9086
High3	9.251	299	1196	1250	1991	2092	2109	4352	4522	4536	9087
Veryhigh1	9.541	280	1390	2068	3259	3263	3264	6950	6970	6971	10303
Veryhigh2	9.821	388	1871	3090	4292	4581	4680	8498	8987	9061	13062
Veryhigh3	9.920	760	1871	3837	4315	4648	4742	9334	9862	9931	13076

Gambar 5. Perbandingan Kapasitas Penyisipan Pesan Berdasarkan *Q Factor* Citra JPEG

Keterkaitan Antara Keacakan (Kompleksitas) Nilai Pixel Citra dengan Kualitas Citra Stego

Pada Gambar 6 menunjukkan uji coba citra JPEG (*pada citra middle1.jpg*) dengan *Q Factor* yang bervariasi. Dari uji coba ini, menjelaskan bahwa *Q Factor* yang rendah menyebabkan kualitas citra stego mengalami penurunan kualitas. Dapat dilihat, bahwa pemberian nilai *Q Factor* 10 (*Q10*), maka akan menghasilkan citra stego yang memiliki nilai *PSNR* yang rendah yaitu 23,60 dB. Sedangkan pemberian nilai *Q Factor* 100 (*Q100*), maka akan menghasilkan citra stego yang memiliki nilai *PSNR* yang tinggi yaitu 43,10 dB.

No	Citra Ori	Quality Factor	Citra Stego	PSNR/db	Ukuran Citra/bit
1.		Q10		23.60	1.6kb
		Q20		25.70	2.11kb
		Q30		29.06	3.10kb
		Q40		32.55	3.32kb
		Q50		33.89	3.48kb
		Q60		34.82	3.65kb
		Q70		34.99	4.36kb
		Q80		35.90	4.81kb
		Q90		39.29	4.81kb
		Q100		43.10	4.90kb

Gambar 6. Citra Stego *middle1.jpg* dengan *Q Factor* yang Bervariasi

Selanjutnya, pada Gambar 7 menunjukkan nilai *DCT* hasil kuantisasi pada citra stego (*image1.jpg*) dengan kompleksitas *middle*, ukuran blok 8×8 pixels, dan *Q Factor* yang bervariasi yaitu Q10, Q50, dan Q100. Didapat bahwa dimana bit pesan yang dapat disisipkan (*embedded bit*) mengalami kenaikan secara berurutan dari 4, 6, dan 12 bit. Secara histogram dapat juga dilihat pada Gambar 8.

No	Quality Factor	Embedded bit	Nilai Kuantisasi citra pada blok 8 x 8 pixel Posisi xblok 3, yblok 3										
			S(i,j)	i0	i1	i2	i3	i4	i5	i6	i7		
1	Q10	4	y0	77	3	0	0	0	0	0	0	0	0
			y1	8	4	0	0	0	0	0	0	0	0
			y2	0	0	0	0	0	0	0	0	0	0
			y3	3	0	0	0	0	0	0	0	0	0
			y4	0	0	0	0	0	0	0	0	0	0
			y5	0	0	0	0	0	0	0	0	0	0
			y6	0	0	0	0	0	0	0	0	0	0
			y7	0	0	0	0	0	0	0	0	0	0

(a) Implementasi pada *Q Factor* 10

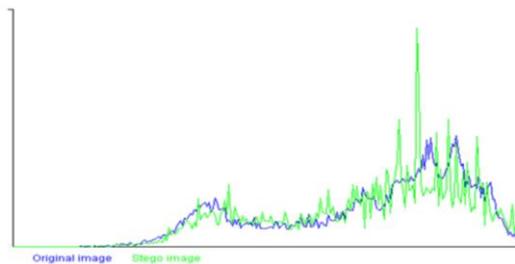
No	Quality Factor	Embedded bit	Nilai Kuantisasi citra pada blok 8 x 8 pixel Posisi xblok 3, yblok 3									
			S(i,j)	i0	i1	i2	i3	i4	i5	i6	i7	
5	Q50	6	y0	73	3	0	-2	1	0	0	0	0
			y1	5	5	1	0	-1	0	0	0	0
			y2	1	1	-1	1	-1	0	0	0	0
			y3	2	1	0	-1	0	0	0	0	0
			y4	1	1	0	0	0	0	0	0	0
			y5	1	0	0	0	3	0	0	0	0
			y6	0	0	0	0	0	0	0	0	0
			y7	0	0	0	0	0	0	0	0	0

(b) Implementasi pada *Q Factor* 50

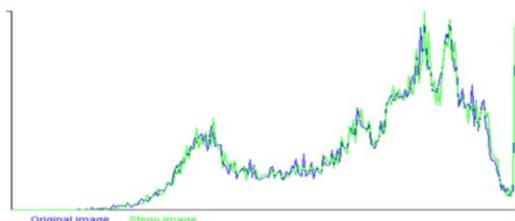
No	Quality Factor	Embedded bit	Nilai Kuantisasi citra pada blok 8 x 8 pixel Posisi xblok 3, yblok 3									
			S(i,j)	i0	i1	i2	i3	i4	i5	i6	i7	
10	Q100	12	y0	74	2	0	-2	2	0	0	0	0
			y1	5	5	1	0	-2	0	0	0	0
			y2	1	1	-1	2	-2	0	0	0	0
			y3	2	1	0	-2	0	0	0	0	0
			y4	1	1	0	0	0	0	0	0	0
			y5	2	0	0	0	4	0	0	0	0
			y6	0	0	0	0	0	0	0	0	0
			y7	0	0	0	0	0	0	0	0	0

(c) Implementasi pada *Q Factor* 100

Gambar 7. Nilai DCT Hasil Kuantisasi pada Citra *middle1.jpg* pada Blok 8x8 pixel dengan (a) Q10, (b) Q50, (c) Q100



(a) *Q Factor* 10



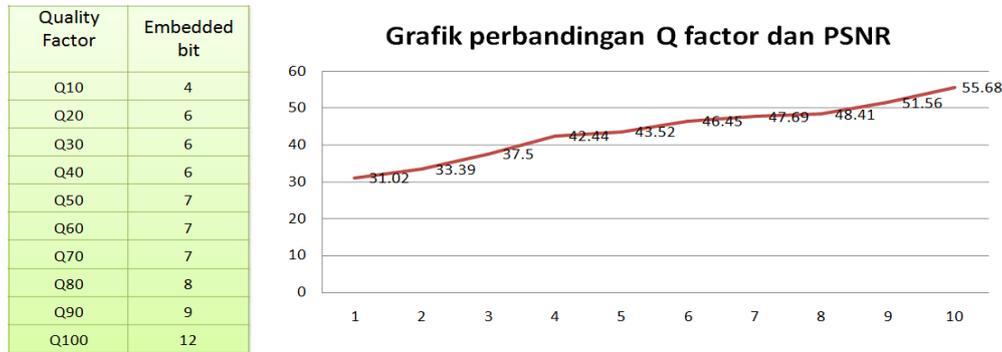
(b) *Q Factor* 100

Gambar 8. Histogram Citra *middle1.jpg* dengan (a) *Q Factor* 10 dan (b) *Q Factor* 100

Dari Gambar 8 (a), dapat dilihat bahwa terdapat perbedaan yang besar antara citra asli dengan citra stego. Sebaliknya pada Gambar 8 (b), dapat dilihat bahwa antara citra asli dengan citra stego dapat dikatakan sama (tidak terlalu berbeda). Hal ini secara sederhana dapat dijelaskan bahwa ketika *Q Factor* diatur rendah, maka pada proses kompresi banyak sekali informasi yang akan dihilangkan. Sebaliknya ketika *Q Factor* diatur tinggi, maka pada proses kompresi hanya sedikit informasi yang dihilangkan.

Pada Gambar 9 ditampilkan perbandingan *Q Factor* dengan nilai bit pesan yang mampu ditampung oleh citra penampung, semakin besar nilai *Q Factor* ternyata dari

hasil pengujian menunjukkan semakin besar juga kapasitas pesan yang bisa disisipkan, dapat dilihat juga grafik perbandingan Q Factor dengan dengan nilai $PSNR$, dimana semakin besar Q Factor semakin baik juga nilai $PSNR$ yang dihasilkan, terlihat grafik yang cenderung naik seiring meningkatnya nilai Q Factor.



Gambar 9. Grafik Perbandingan Variasi Q Factor dan Nilai $PSNR$ Citra *middle1.jpg*

Selanjutnya, pada Gambar 10 dapat dilihat secara rata-rata nilai $PSNR$ pada citra stego dengan Q Factor yang rendah menghasilkan nilai $PSNR$ yang rendah dari data $Q10$ didapatkan nilai $PSNR$ rata-rata yaitu 22,56 dB masih dibawah nilai $PSNR$ standar yaitu antara (30-50) dB, sebaliknya rata-rata nilai $PSNR$ dengan Q Factor yang tinggi didapatkan nilai $PSNR$ sebesar 46,54 dB yang mana nilai tersebut masih masuk dalam standar nilai $PSNR$ yang baik.

Nama Citra	PSNR
Verylow1stego10.jpg	27.99
Verylow2stego10.jpg	29.13
Verylow3stego10.jpg	22.83
Low1stego10.jpg	26.38
Low2stego10.jpg	25.71
Low3stego10.jpg	23.02
Middle1stego10.jpg	23.60
Middle2stego10.jpg	23.03
Middle3stego10.jpg	22.53
High1stego10.jpg	25.88
High2stego10.jpg	20.55
High3stego10.jpg	22.31
Veryhigh1stego10.jpg	18.39
Veryhigh2stego10.jpg	15.69
Veryhigh3stego10.jpg	14.49
Rata-rata	22.56

(a) Q Factor 10

(b) Q Factor 100

Gambar 10. Perbandingan Rata-Rata Nilai $PSNR$ Antar Citra Asli dengan Citra Stego dengan (a) Q Factor 10, dan (b) Q Factor 100

Keterkaitan Antara Ukuran Pesan dengan Kualitas Citra

Pada Gambar 11 ditampilkan perbandingan nilai $PSNR$ citra stego dengan kompleksitas nilai pixel *middle* dengan Q Factor yang sama, dalam hal ini menggunakan Q Factor 100. Dapat dilihat, semakin besar ukuran citra yang disisipkan pesan rahasia, ternyata mempengaruhi nilai $PSNR$ yang dihasilkan dimana semakin besar citra yang disisipkan semakin rendah pula nilai $PSNR$ yang dihasilkan. Hal ini disebabkan semakin banyak pesan yang disisipkan, maka semakin banyak pula nilai DCT hasil kuantisasi yang berubah, yang tentunya ini akan berpengaruh terhadap kualitas citra yang dihasilkan.

Nama Citra Asli	Ukuran Pesan(bytes)	PSNR (db)	MSE
Middle1stego2.jpg	2	31.50	414.09
Middle1stego4.jpg	4	31.48	416.08
Middle1stego6.jpg	6	31.49	414.64
Middle1stego8.jpg	8	31.49	415.12
Middle1stego10.jpg	10	31.48	416.14
Middle1stego12.jpg	12	31.48	416.14
Middle1stego14.jpg	14	31.47	416.67
Middle1stego16.jpg	16	31.46	417.78
Middle1stego18.jpg	18	31.46	418.11
Middle1stego20.jpg	20	31.44	419.29
Middle1stego22.jpg	22	31.42	420.10
Middle1stego24.jpg	24	31.40	421.11

Gambar 11. Perbandingan Nilai PSNR Citra Stego Middle Berdasarkan Ukuran Pesan

KESIMPULAN

Berdasarkan hasil pengujian efek *Q Factor* terhadap kapasitas pesan rahasia pada steganografi citra *JPEG* didapatkan kesimpulan bahwa *Q Factor* mempengaruhi kapasitas pesan yang mampu ditampung oleh citra penampung, dimana semakin besar *Q Factor*, semakin meningkat juga kapasitas pesan yang dapat disisipkan. Hal ini disebabkan pada *Q Factor* yang rendah menyebabkan citra penampung mengalami proses kompresi yang besar, sehingga banyak informasi citra yang hilang. Sedangkan pada *Q Factor* besar, citra penampung mengalami proses kompresi yang rendah, sehingga hanya sedikit informasi yang hilang. Dapat dilihat dari hasil pengujian citra *verylow1.jpg* dengan kompleksitas rendah dimana nilai entropi 4.748 dengan *Q Factor 10 (Q10)* didapatkan kapasitas pesan rahasia sebesar 34 bits, sedangkan pada citra *veryhigh3.jpg* dengan kompleksitas tinggi dimana nilai entropi 9.920 dengan *Q Factor 100 (Q100)* didapatkan kapasitas pesan sebesar 13.076 bits.

Berdasarkan hasil pengujian efek *Q Factor* terhadap kualitas citra stego didapatkan kesimpulan semakin besar *Q Factor* maka semakin baik kualitas citra stego yang dihasilkan, namun ukuran citra stego juga semakin besar. Sebaliknya semakin kecil *Q Factor* maka kualitas citra stego yang dihasilkan semakin rendah, namun ukuran citra stego juga semakin kecil. Hal ini disebabkan ketika *Q Factor* besar tidak terlalu banyak informasi pada citra stego yang dihilangkan, berbeda dengan *Q Factor* kecil menyebabkan banyak informasi pada citra stego yang dihilangkan.

UCAPAN TERIMA KASIH

Ucapan terima kasih disampaikan kepada Lembaga Penelitian dan Pengabdian Kepada Masyarakat Universitas Islam Negeri Raden Fatah Palembang atas dukungan yang telah diberikan berupa bantuan dana penelitian pada klaster Penelitian Pembinaan/Peningkatan Kapasitas.

DAFTAR RUJUKAN

- Abdel Wahab, O. F., Hussein, A. I., Hamed, H. F. A., Kelash, H. M., Khalaf, A. A. M., & Ali, H. M. (2019). Hiding Data in Images Using Steganography Techniques with Compression Algorithms. *Telkomnika (Telecommunication Computing Electronics and Control)*, 17(3), 1168–1175. <https://doi.org/10.12928/TELKOMNIKA.V17I3.12230>
- Altaay, A. A. J., Sahib, S. B., & Zamani, M. (2012). An Introduction to Image Steganography Techniques. *2012 International Conference on Advanced Computer Science*

- Applications and Technologies (ACSAT)*, 122–126. <https://doi.org/10.1109/ACSAT.2012.25>
- Andriotis, P., Oikonomou, G., & Tryfonas, T. (2013). JPEG steganography detection with Benford's Law. *Digital Investigation*, 9(3), 246–257. <https://doi.org/https://doi.org/10.1016/j.diin.2013.01.005>
- Ansari, A. S., Mohammadi, M. S., & Parvez, M. T. (2020). a Multiple-format Steganography Algorithm for Color Images. *IEEE Access*, 8, 83926–83939. <https://doi.org/10.1109/ACCESS.2020.2991130>
- Bao, Z., Guo, Y., Li, X., Zhang, Y., Xu, M., & Luo, X. (2020). Correction to : a Robust Image Steganography Based on the Concatenated Error Correction Encoder and Discrete Cosine Transform Coefficients. *Journal of Ambient Intelligence and Humanized Computing*, 11(5), 1903. <https://doi.org/10.1007/s12652-019-01376-1>
- Battikh, D., El Assad, S., Hoang, T. M., Bakhache, B., Deforges, O., & Khalil, M. (2019). Comparative Study of Three Steganographic Methods Using a Chaotic System and Their Universal Steganalysis Based on Three Feature Vectors. *Entropy*, 21(8), 1–36. <https://doi.org/10.3390/e21080748>
- Cogranne, R. (2018). *Determining JPEG Image Standard Quality Factor from the Quantization Tables*.
- Darbani, A., AlyanNezhadi, M. M., & Forghani, M. (2019). A New Steganography Method for Embedding Message in JPEG Images. *2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI)*, 617–621. <https://doi.org/10.1109/KBEI.2019.8735054>
- Darwis, D. (2017). Teknik Steganografi untuk Penyembunyian Pesan Teks Menggunakan Algoritma GIFSHUFFLE. *Jurnal Teknoinfo*, 11(1), 19. <https://doi.org/10.33365/jti.v11i1.6>
- Gunawan, C. E., & Fenando, F. (2018). Pengukuran Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Studi Kasus di PUSTIPD UIN Raden Fatah Palembang. *JUSIFO (Jurnal Sistem Informasi)*, 4(2), 121–132. <https://doi.org/10.19109/JUSIFO.V4I2.4107>
- Hamzah, R. F., Jaya, I. D., & Putri, U. M. (2020). Analisis Risiko Keamanan Sistem Informasi E-LKP Dengan Metode Octave Pada Perguruan Tinggi Negeri X. *Jusifo*, 6(1), 55–65. <https://doi.org/10.19109/jusifo.v6i1.5880>
- Jóokay, M., & Moravčík, T. (2010). Image-based JPEG Steganography. *Tatra Mountains Mathematical Publications*, 45(1), 65–74. <https://doi.org/10.2478/v10127-010-0006-9>
- Kim, C., Shin, D., Yang, C.-N., Chen, Y.-C., & Wu, S.-Y. (2019). Data Hiding Using Sequential Hamming + K with M Overlapped Pixels. *KSII Transactions on Internet and Information Systems*, 13(12), 6159–6174. <https://doi.org/10.3837/tiis.2019.12.020>
- Krasmala, R., Purba, A. B., & Lenggana, U. T. (2017). Kompresi Citra dengan Menggabungkan Metode Discrete Cosine Transform (DCT) dan Algoritma Huffman. *JOIN*, 2(1), 1–9.
- Malathi, P., Abhijeet Sridhar, M., Paliwal, A., & Gireesh Kumar, T. (2020). ScienceDirect ScienceDirect Maximizing the Embedding Efficiency Using Linear Block Codes Spatial and Transform Domains Maximizing the in Embedding Efficiency Using Linear Block Codes in Spatial and Domains M Transform. *Procedia Computer Science*, 167, 302–312. <https://doi.org/10.1016/j.procs.2020.03.227>
- Mythili, T., Sofiabanu, A., Mohanasundari, R., & Sreekanth, K. (2019). Data Hiding with Image and Audio Steganography Cryptosystem in Network. *International Journal of Recent Trends in Engineering & Research*, 5(2), 5–10.
- Nur'aini, S. (2019). Steganografi pada Digital Image Menggunakan Metode Least Significant Bit Insertion. *Walisongo Journal of Information Technology*, 1(1), 75–90. <https://doi.org/10.21580/wjit.2019.1.1.4025>

- Pandit, R., Khosla, N., Singh, G., & Sharma, H. (2013). Image Compression and Quality Factor in case of JPEG Image format. *International Journal of Advanced Research in Computer and Communication Engineering*, 2(7), 2578–2581.
- Singh, B. (2017). Image Steganography Using DWT and Semi Hexadecimal Code Based on PSNR. *International Journal of Emerging Research in Management and Technology*, 6(8), 230–234. <https://doi.org/10.23956/ijermt.v6i8.144>
- w3techs.com. (2020). *Usage Statistics of Image File Formats for Websites, December 2020*. https://w3techs.com/technologies/overview/image_format
- Zulfikar, D. H., & Harjoko, A. (2016). Perbandingan Kapasitas Pesan pada Steganografi DCT Sekuensial dan Steganografi DCT F5 dengan Penerapan Point Operation Image Enhancement. *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, 10(1), 35. <https://doi.org/10.22146/ijccs.11187>