ELKOMIKA | ISSN (p): 2338-8323 | ISSN (e): 2459-9638 | Vol. 7 | No. 3 | Halaman 544 – 558
DOI : http://dx.doi.org/10.26760/elkomika.v7i3.544 September 2019

Pengamanan Pesan pada *Steganografi* Citra dengan Teknik Penyisipan *Spread Spectrum*

SOFIA SAIDAH, NUR IBRAHIM, MOCHAMMAD HALDI WIDIANTO

Universitas Telkom Bandung
Email : sofiahsaidahsfi@telkomuniversity.ac.id

Received 22 Juli 2019 | *Revised* 9 Agustus 2019 | *Accepted* 22 Agustus 2019

ABSTRAK

Pada studi ini, dilakukan penggabungan metode - metode untuk memperkuat dan meningkatkan sisi keamanan proses pertukaran informasi atau pesan digital. Metode yang digunakan diantaranya adalah metode kriptografi dan metode steganografi. Implementasi pada sistem yang dibangun dilakukan dengan menyandikan pesan pada penerapan metode steganografi citra dalam menyembunyikan pesan tersandi yang dihasilkan ke dalam sebuah citra warna (RGB) dalam domain Discrete Cosine Transform dengan teknik penyisipan Spread Spectrum. Hasil penelitian menunjukan bahwa kualitas dari stego image sangat mirip dengan cover citra yang digunakan, berdasarkan perolehan nilai performansi objektif PSNR diatas 30 db dan subjektif MOS di atas nilai 4.

***Kata kunci**: Steganografi, Discrete Cosine Transform, Spread Spectrum, PSNR, SNR*

ABSTRACT

In this study, a combination of methods was used to strengthen and enhance the security side of the process of exchanging information or digital messages. The methods used include cryptographic methods and steganography methods. The implementation of the system built is done by encoding the message on the application of the image steganography method in hiding the encrypted message generated into a color image (RGB) in the Discrete Cosine Transform domain with the Spread Spectrum insertion technique. The results of the study show that the quality of the stego image is very similar to the cover image used, based on the acquisition of an objective performance value of PSNR above 30 db and subjective MOS above a value of 4.

***Keywords**: Steganografi, Discrete Cosine Transform, Spread Spectrum, PSNR, SNR*

1. PENDAHULUAN

Perkembangan dan kemajuan teknologi komunikasi *digital* yang pesat, terdapat banyak kemungkinan tindak kejahatan *digital* yang terus bertambah dan berkembang. Tindak kejahatan *digital* berupa pencurian maupun penyadapan informasi adalah beberapa isu ancaman keamanan yang harus diamati dan diperhatikan untuk diminimalisir.

Seminar nasional Indonesia *Cyber Crime Summit* (ICCS) pada tahun 2014, yang diselenggarakan oleh Institut Teknologi Bandung (ITB) didukung oleh PT. Telkom Indonesia, Tbk. menyatakan berdasarkan sumber data dari Kementrian Komunikasi dan Informasi (Kemkominfo) di tahun 2013, Indonesia merupakan negara nomor satu sumber serangan kejahatan *cyber* dengan tingkat presentasi 38,0% dimana telah terjadi 42 ribu target serangan setiap harinya **(ITB, 2014)**.

Terkait berdasarkan pokok bahasan di atas, maka aspek-aspek keamanan meliputi kerahasiaan (*secrecy*) dan orisinilitas informasi (*authencity*) menjadi hal yang sangat penting untuk tetap terjaga dengan sebaik-baiknya. Adapun beberapa metode keamanan pengiriman informasi atau pesan yang dapat digunakan untuk memperkuat serta meningkatkan sisi keamanan pada proses pertukaran pesan, di antaranya dengan menggunakan metode penyandian pesan yang disebut dengan metode *kriptografi* dan metode penyembunyian pesan ke dalam sebuah media yang disebut dengan metode *steganografi*.

Steganografi merupakan seni dan ilmu dalam penyembunyian pesan ke dalam suatu media atau *cover*, dimana keberadaan pesan tersebut hanya dapat diketahui oleh orang-orang tertentu **(Alfian Zakaria, 2015) (Chudasama, 2016)**. Dibanding *kriptografi* yang keberadaan pesannya dapat diketahui dengan jelas, *steganografi* memanfaatkan kelemahan indera manusia agar pesan rahasia tidak dapat diidentifikasi **(Alfian Zakaria, 2015).** Bagi sebuah komputer, citra merupakan sebuah matriks yang setiap angka pada elemennya merepresentasikan intensitas cahaya pada titik-titik yang disebut *pixel* (Piksel). Piksel-piksel tersebut membentuk data dari sebuah citra yang biasa kita lihat. Biasanya sebuah citra terdiri dari 1 (*grayscale*) atau 3 *layer* (berwarna). *Steganografi* citra adalah *steganografi* yang paling populer, yang mana pesan rahasia disisipkan ke dalam citra *digital* selayaknya menyisipkan *noise* yang tidak dapat terdeteksi oleh mata manusia **(Neil F. Johnson, 2001).**

Berdasarkan literatur dan jurnal penelitian sebelumnya, *Image Steganography Using Discrete Cosine Transform* (*DCT*) *and Blowfish Algorithm* **(Gunjal & Jha, 2014)** menjelaskan bahwa penggunaan algoritma *kriptografi Blowfish* dan *steganografi* citra transformasi kosinus diskrit dapat memperkuat tingkat keamanan dalam pertukaran pesan. *Image Steganography Using DCT Technique* **(Sharma & Kumar, 2015)** menjelaskan bahwa penyembunyian pesan kedalam sebuah citra dengan penggunaan transformasi kosinus diskrit (*DCT*) dapat memperkecil kemungkinan perubahan yang terjadi pada citra hasil penyembunyian pesan. *Spread Spectrum and Discrete Cosine Transform (DCT) Based Steganography* **(Gouda, 2015)** menjelaskan bahwa pada citra hasil penyembunyian pesan dengan penggunaan transfomasi kosinus diskrit (*DCT*) dan teknik penyisipan *Spread Spectrum* dihasilkan nilai *BER* dan *PSNR* yang lebih baik bila dibandingkan dengan tanpa atau dilakukannya transformasi lain **(Hannan dkk, 2017)**.

Pada studi ini telah dilakukan penelitian, implementasi dan pengujian sistem pada penerapan metode *kriptografi* dan penerapan metode *steganografi* citra *digital* domain *Discrete Cosine Transform (DCT)* dengan teknik penyisipan *Spread Spectrum* yang dapat digunakan sebagai variasi model sistem keamanan lainnya.

Metode Citra

Metode penerapan *steganografi* citra memiliki dua buah kawasan (domain) yang dapat digunakan yaitu domain spasial dan domain frekuensi **(Sharma & Kumar, 2015)** . Dalam domain spasial, bit-bit pesan disisipkan secara langsung ke dalam intensitas *pixel cover* citra sedangkan dalam domain frekuensi, bit-bit pesan disisipkan pada *pixel cover* citra hasil transformasi domain frekuensi yang dilakukan terlebih dahulu. Perbedaan pengaruh penggunaan kawasan (domain) dalam menyisipkan bit-bit pesan dapat mempengaruhi nilai kemiripan dan ketahanan antara *stego image* yang dihasilkan dengan *cover* citra yang digunakan **(Gouda, 2015)**.

Salah satu transformasi domain frekuensi yang diterapkan pada tugas studi ini adalah dengan penggunaan transformasi domain *Discrete Cosine Transform* (*DCT*) **(Sharma & Kumar, 2015)**. *Discrete Cosine Transform* (*DCT*) bukan merupakan teknik penyisipan, namun merupakan sarana atau teknik transformasi domain *cover* citra sebelum bit-bit pesan disisipkan. Teknik ini merupakan teknik transformasi yang mengubah sinyal dari representasi kawasan spasial ke dalam representasi kawasan frekuensi dengan memecah ukuran *pixel cover* citra kedalam blok-blok ukuran 8 x 8 pada fungsi sinyal *cosinus*.

Input proses transformasi domain *DCT* yaitu *cover* citra berupa matriks dengan dimensi dua (2D) yaitu m x n maka, persamaan *DCT* untuk setiap blok matriks ukuran 8 x 8 dituliskan pada Persamaan (1) sebagai berikut :

$$s(u,v)=C(v)\sum_{y=0}^{m-1}\left[C(u)\sum_{x=0}^{n-1}s(x,y)\cos\frac{(2x+1)u\pi}{2n}\right]\cos\frac{(2y+1)v\pi}{2m} \quad (1)$$

berikut persamaan *Invers DCT* untuk blok matrik berukuran 8 x 8 dalam mengembalikan nilai hasil transformasi domain *DCT* kedalam nilai domain spasial kembali dituliskan pada Persamaan (2) sebagai berikut :

$$s(x,y)=\sum_{y=0}^{m-1}\sum_{x=0}^{n-1}s(u,v)C(u)C(v)\cos\frac{(2x+1)u\pi}{2n}\cos\frac{(2y+1)v\pi}{2m} \quad (2)$$

dimana;

a. m dan n adalah banyaknya kolom dan baris.
b. u = 0 s.d. m-1 dan v = 0 s.d. n-1.
c. S(u,v) adalah *pixel cover* citra transformasi domain *DCT*
d. S(x,y) adalah *pixel cover* citra domain spasial.
e. C (u) = $\sqrt{\frac{1}{n}}$, u = 0 ; $\sqrt{\frac{2}{n}}$, $1 \leq u \leq n-1$
f. C (v) = $\sqrt{\frac{1}{m}}$, v = 0 ; $\sqrt{\frac{2}{m}}$, $1 \leq v \leq m-1$
g. $\pi = 180^0$

Setelah itu dilakukan kuantisasi dan *dekuantisasi* dari blok-blok matriks *pixel* transformasi *DCT* yang dihasilkan dengan ukuran 8 x 8 untuk menyisipan bit-bit pesan kedalam *pixel* transformasi *DCT* yang dihasilkan **(Setyaningsih, 2015)**. Kuantisasi pada *pixel* transformasi

DCT diperlukan karena *pixel* transformasi *DCT* yang dihasilkan tidak berbentuk bilangan bulat melainkan berbentuk bilangan desimal.

Nilai kuantisasi matriks *pixel* transformasi *DCT* didapat dengan membagi setiap elemen dalam blok-blok matriks koefisien *DCT* dengan tabel matriks kuantisasi dan kemudian hasilnya dibulatkan ke dalam bilangan bulat terdekat. Pada Persamaan (3) dan (4) ditunjukan kuantisasi dan *dekuantisasi*, sedangkan ilustrasi kuantisasi dan *dekuantisasi DCT block* ditunjukan pada Gambar 1.

$$s^{Q}(u,v) = round\left(\frac{s(u,v)}{Q(u,v)}\right) \tag{3}$$

$$s^{D}(u,v) = s(u,v) * Q(u,v) \tag{4}$$

$$= \begin{bmatrix} 162 & 40 & 20 & 72 & 30 & 2 & -1 & -1 \\ 30 & 108 & 10 & 32 & 27 & 5 & 8 & -2 \\ -94 & -60 & 12 & -43 & -31 & 6 & -3 & 7 \\ -38 & -83 & -5 & -22 & 3 & 5 & -1 & 3 \\ -31 & 17 & -5 & -1 & 4 & -6 & 1 & -6 \\ 0 & -1 & 2 & 0 & 2 & 2 & 8 & 2 \\ 4 & -2 & 2 & 6 & 8 & -1 & 7 & 2 \\ -1 & 1 & 7 & 6 & 2 & 0 & 5 & 0 \end{bmatrix} \quad Q_{50} = \begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

$$^{Q} = \begin{bmatrix} 10 & 4 & 2 & 5 & 1 & 0 & 0 & 0 \\ 3 & 9 & 1 & 2 & 1 & 0 & 0 & 0 \\ -7 & -5 & 1 & -2 & -1 & 0 & 0 & 0 \\ -3 & -5 & 0 & -1 & 0 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad ^{D} = \begin{bmatrix} 160 & 44 & 20 & 80 & 24 & 0 & 0 & 0 \\ 36 & 108 & 14 & 38 & 26 & 0 & 0 & 0 \\ -98 & -65 & 16 & -48 & -40 & 0 & 0 & 0 \\ -42 & -85 & 0 & -29 & 0 & 0 & 0 & 0 \\ -36 & 22 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Gambar 1. Ilustrasi Kuantisasi dan *Dekuantisasi DCT*

Terakhir, dengan metode penyisipan menggunakan *spread spectrum*, konsep mendasar dari metode penyisipan ini adalah dengan menyisipkan sinyal informasi *narrowband* ke dalam *noise wideband* lalu menambahkan *noise* tersebut ke dalam *cover image*. *Noise* yang ditambahkan tersebut seperti *noise* yang terjadi pada saat proses akuisisi citra dan jika pada *level* rendah, tidak akan mudah terdeteksi oleh indera penglihatan manusia maupun analisis komputer tanpa menggunakan citra aslinya.

Secara umum proses *spread spectrum* ini digambarkan pada Gambar 1. Pada sistem ini, pesan teks diubah ke dalam bentuk biner kemudian pesan dikalikan dengan *pseudorandomnoise* sehingga menghasilkan *noise* informasi sesuai **(Bansal, 2014)**. Setelah itu *noise* informasi tersebut ditambahkan ke *cover image* dalam intensitas yang rendah agar tidak terdeteksi oleh mata manusia. Di sisi penerima, *stego image* diterima oleh penerima yang mempunyai kunci yang sama yaitu *pseudorandom-noise* yang sama untuk mengekstrak pesan yang diterima **(M.P.S. Bhatia, 2014).**

Berkaitan dengan format *object cover* yang dapat digunakan dalam pertukaran informasi dunia *digital* saat ini, hampir semua *file digital* dapat dijadikan sebagai *object cover* dalam properti penggunaan metode *steganografi*. Kendati demikian, format yang paling cocok untuk dijadikan *object cover digital* adalah format *file digital* yang memiliki nilai *redundancy bit* yang tinggi. *Redundancy bit* adalah bit yang dapat dirubah tanpa merubah banyak karakteristik *file* secara keseluruhan **(Massandy, 2017) (Negara, 2016)**.

2. METODOLOGI PENELITIAN

2.1 Perancangan dan Pemodelan Sistem

Perancangan sistem dijelaskan dengan diagram alir dibawah ini. Secara garis besar sistem tebagi menjadi beberapa proses. Pada Gambar 2 dan Gambar 3, ditunjukan proses penyisipan pesan (*embbeding*) dan proses ekstraksi pesan (*retrieval*) pada sistem.

2.2 Pengujian sistem

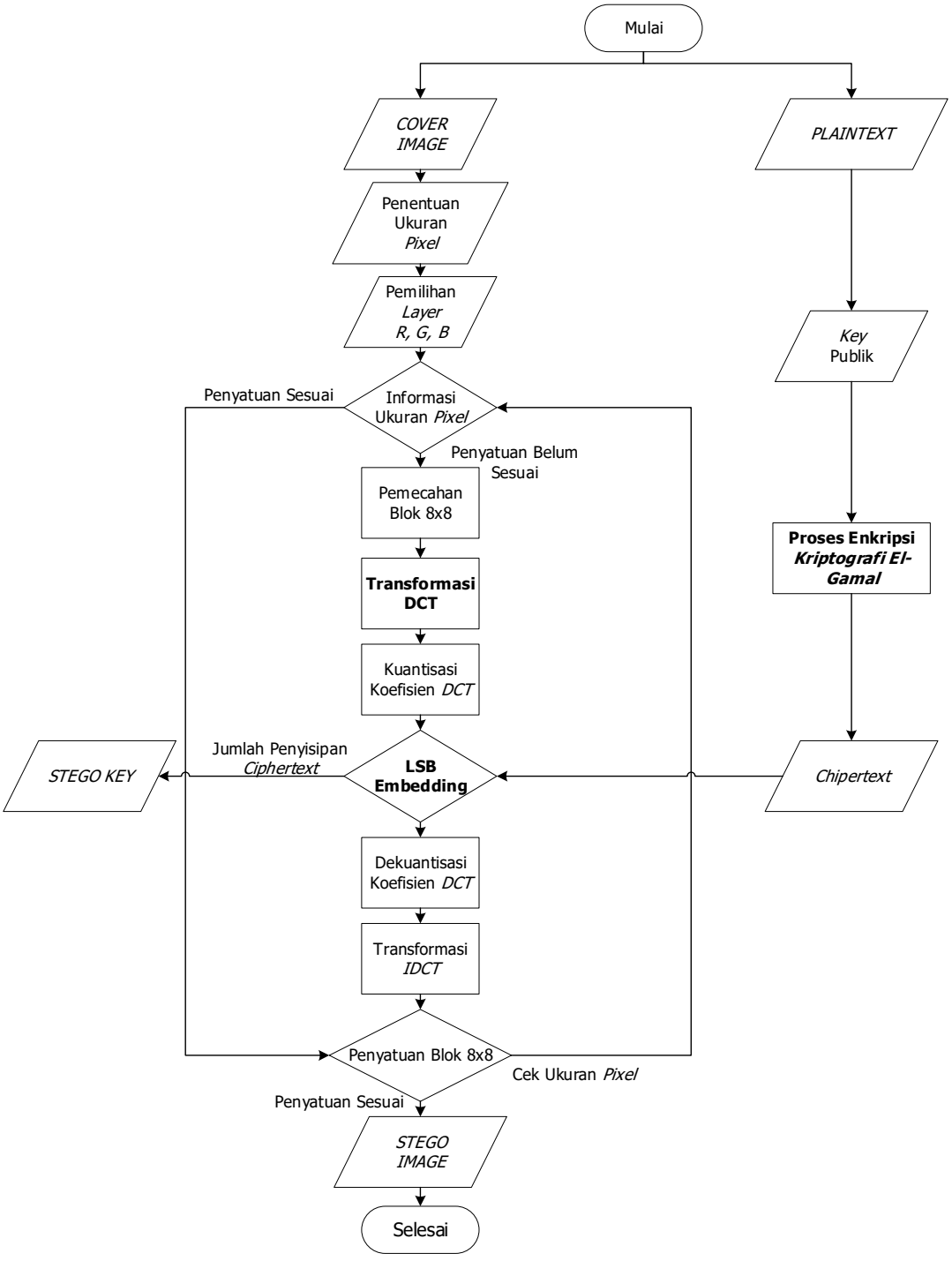
Pada *stego image* yang dihasilkan, selanjutnya akan dilakukan beberapa uji serangan yang bertujuan untuk mengetahui tingkat ketahanan sistem terhadap tindak perusakan yang terjadi pada proses implementasinya. Simulasi pengujian sistem dilakukan dengan pemberian serangan berupa gangguan *noise*, sebagai berikut :

a. *Noise Gaussian / White Noise*
Pada sebuah citra, *noise* ini menyebabkan citra berwarna putih. Banyak atau sedikitnya *noise* dipengaruhi oleh nilai rata-rata (*mean*) dan nilai variasi (*variance*) dalam skala 0 s.d. 1. Semakin besar *mean* dan *variance* maka citra hasil penambahan *noise* akan semakin mendekati warna putih. Pada simulasi pengujian ini dilakukan pengujian pada sistem dengan inensitas *noise* untuk mengetahui ketahanan citra pada *stego image* yang dihasilkan.

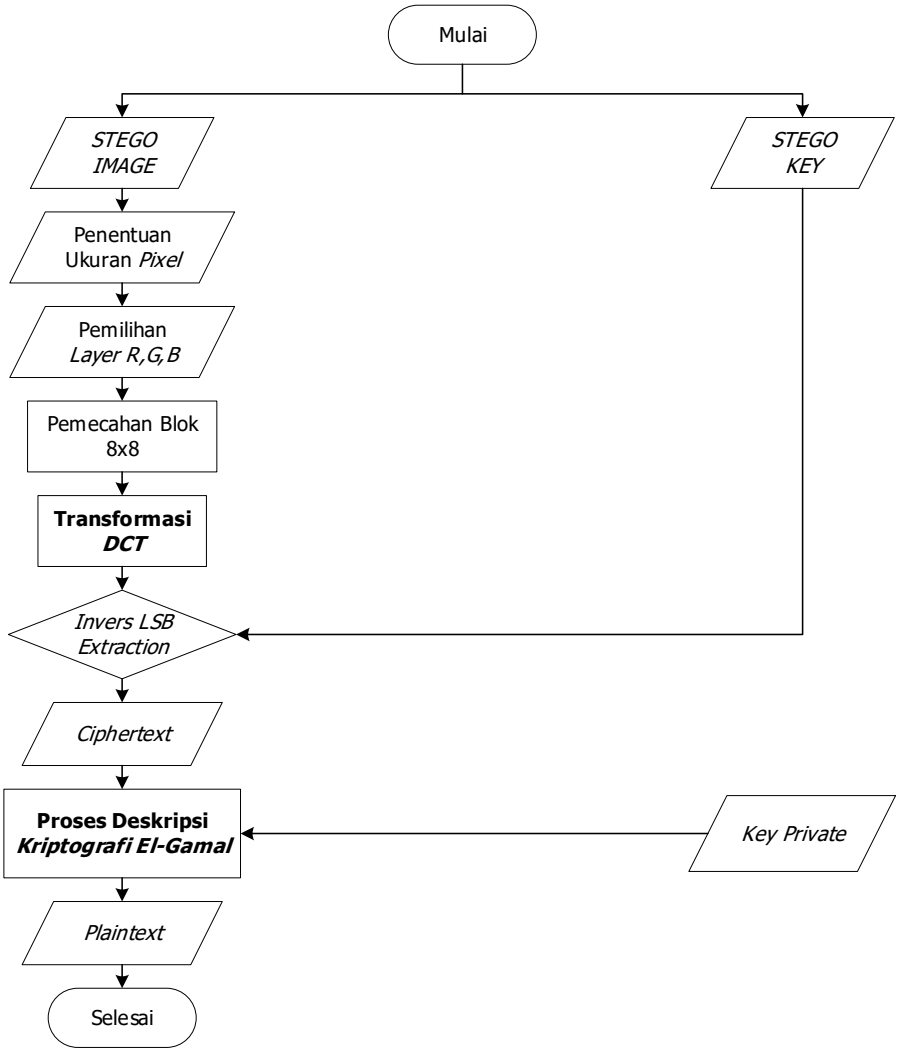
b. *Noise Salt and Pepper*
Pada sebuah citra, *noise* ini berupa titik-titik yang mirip seperti taburan garam dan lada. Pada citra *RGB* titik-titik (*noise*) tersebut berwarna *red* (merah), *green* (hijau) dan *blue* (biru). Titik-titik (*noise*) tersebut dipengaruhi oleh densitas (d) dalam skala 0 s.d. 1.

2.3 Penilaian Objektif

Penilaian objektif pada sistem adalah penilaian terkait dengan fakta matematis yang terukur. Penilaian objektif yang dilakukan pada sistem diantaranya adalah penilaian metode *kriptografi* dan metode *steganografi* sesuai dengan referensi yaitu *Peak Signal Noise to Ratio (PSNR), Bit Error Rate (BER), Character Error Rate (CER), dan Signal Noise Ratio (SNR).*



Gambar 2. Proses Penyisipan Pesan



Gambar 3. Proses Ekstraksi Pesan

3. HASIL PENGUJIAN DAN ANALISIS SISTEM

3.1 *Cover* Citra

Penggunaan citra warna (*RGB*) sebagai *object cover* dalam evaluasi skenario pengujian sistem menggunakan sebanyak tiga buah citra yang ditunjukan pada Gambar 4. Ukuran masing-masing *cover* citra yang digunakan berukuran 256 x 256, 512 x 512, dan 1024 x 1024 *pixel*.

No	*File Cover* Citra	No	*File Cover* Citra	No	*File Cover* Citra
1	 Lena Ekstensi:.*bmp*	2	 *Airplane* Ekstensi:.*bmp*	3	 Buah Ekstensi:.*bmp*

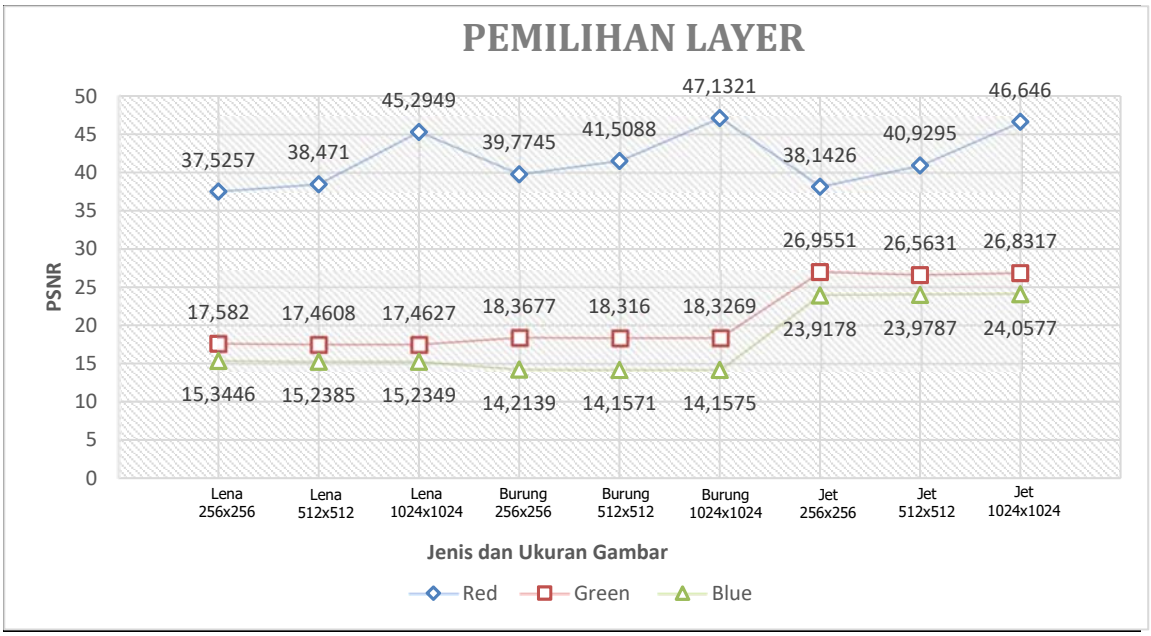
Gambar 4. Citra yang Digunakan

3.2 Skenario Pengujian

Pada skenario proses pengujian sistem, telah dilakukan beberapa skenario evaluasi pengujian, di antaranya sebagai berikut :

1. Skenario evaluasi kapasitas penyisipan *cover* citra citra terhadap jumlah karakter *plaintext* dan *ciphertext*.
2. Skenario evaluasi pemilihan *layer* warna pada *cover* citra.
3. Skenario evaluasi performansi sistem tanpa gangguan berupa *noise* meliputi penilaian *PSNR*, *BER, CER,* dan *MOS, SNR.*
4. Skenario evaluasi performansi sistem dengan gangguan *noise* meliputi penilaian *BER* dan *CER* terhadap akurasi pesan yang dapat diungkap atau ekstraksi.

3.3 Pengujian *Layer* Warna *Cover* Citra



Gambar 5. Grafik Pemilihan *Layer* Warna

Pemilihan *layer* warna dalam sistem dilakukan untuk mengetahui *layer* warna terbaik pada tiga buah *cover* digunakan dalam proses penyisipan pesan berupa *ciphertext* berdasarkan penerapan metode *steganografi*. Terdapat tiga buah *layer* warna yaitu *Red Layer, Green Layer*, dan *Blue Layer* pada cover citra warna (*RGB*) yang diuji berdasakan penggunaan masing-masing nilai ukuran *pixel cover* citra yang di jelaskan pada Gambar 5.

3.4 Pengujian Performansi Sistem Tanpa Gangguan *Noise*

Pada pengujian performansi sistem, dilakukan pengujian dengan memilih tiga buah *sample* karakter pesan *plaintext* yang digunakan sebesar 21, 42, dan 63 karakter. Pemilihan jumlah karakter yang digunakan dalam pengujian ini mengacu pada jumlah karakter maksimum kapasitas ukuran *pixel* 256 x 256 sebagaimana jumlah karakter pembanding terbesar di antara ukuran *pixel* uji lainnya dengan jumlah karakter *plaintext* sama dengan 64, dapat dilihat pada Tabel 1 – Tabel 6.

a. Citra ke-1: Lena

Tabel 1. Pengujian Performansi Objektif Citra Lena

No	ΣKarakter Uji *Plaintext*	ΣKarakter Uji *Cipher Text*	Ukuran *Pixel Cover*	Evaluasi Performansi Sistem			
				PSNR	BER	*CER*	SNR
1	21	42	256 x 256	36,69	0	0	45,75
			512 x 512	38,52	0	0	40,64
			1024 x 1024	45,36	0	0	34,86
2	42	84	256 x 256	34,61	0	0	42,32
			512 x 512	38,49	0	0	38,62
			1024 x 1024	45,32	0	0	35,67
3	63	126	256 x 256	35,53	0	0	42,55
			512 x 512	38,47	0	0	36,78
			1024 x 1024	45,29	0	0	31,24

Tabel 2. Pengujian Performansi Subjektif Citra Lena

No	ΣKarakter Uji *Plain text*	ΣKarakter Uji *Cipher text*	Ukuran *Pixel Cover*	*MOS* (Mean Opinion Score) n=30
1	21	42	256 x 256	4,50
			512 x 512	4,56
			1024 x 1024	4,46
2	42	84	256 x 256	4,43
			512 x 512	4,48
			1024 x 1024	4,50
3	63	126	256 x 256	4,46
			512 x 512	4,43
			1024 x 1024	4,56

b. Citra ke-2:*Airplane*

Tabel 3. Pengujian Performansi Objektif Citra Airplane

No	ΣKarakter Uji *Plain text*	ΣKarakter Uji *Cipher text*	Ukuran *Pixel Cover*	Evaluasi Performansi Sistem			
				PSNR	**BER**	***CER***	**SNR**
1	21	42	256 x 256	35,34	0	0	46,54
			512 x 512	41,06	0	0	40,17
			1024 x 1024	46,73	0	0	36,06
2	42	84	256 x 256	35,24	0	0	48,28
			512 x 512	40,97	0	0	43,74
			1024 x 1024	46,69	0	0	38,05
3	63	126	256 x 256	35,15	0	0	46,77
			512 x 512	40,93	0	0	41,66
			1024 x 1024	46,64	0	0	35,88

Tabel 4. Pengujian Performansi Subjektif Citra *Airplane*

No	ΣKarakter Uji *Plaintext*	ΣKarakter Uji *Cipher Text*	Ukuran *Pixel Cover*	***MOS*** **(Mean Opinion Score) n=30**
1	21	42	256 x 256	4,33
			512 x 512	4,40
			1024 x 1024	4,50
2	42	84	256 x 256	4,36
			512 x 512	4,43
			1024 x 1024	4,56
3	63	126	256 x 256	4,44
			512 x 512	4,46
			1024 x 1024	4,63

c. Citra ke-3:Buah

Tabel 5. Pengujian Performansi Objektif Citra Buah

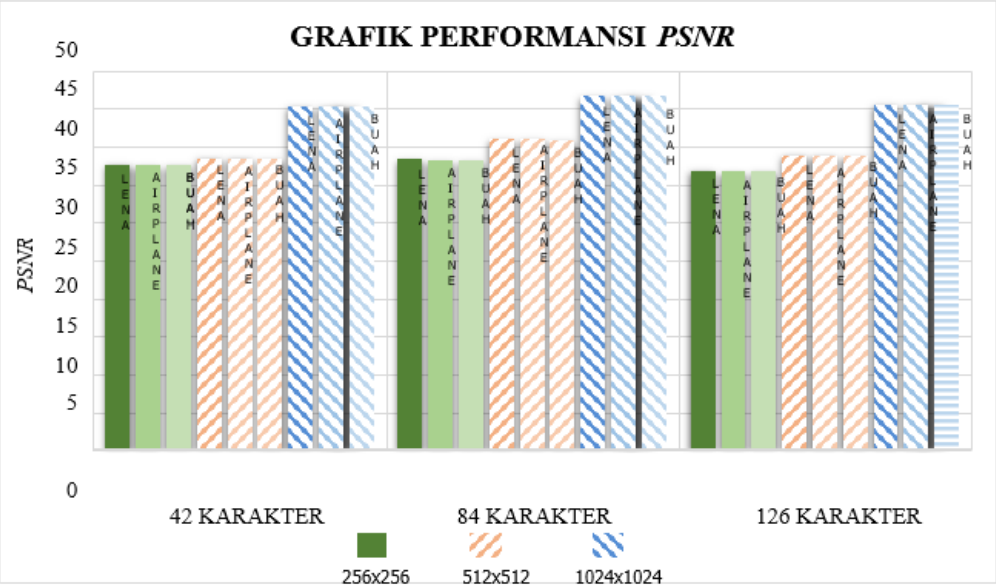
No	ΣKarakter Uji *Plaintext*	ΣKarakter Uji *Cipher Text*	Ukuran *Pixel Cover*	Evaluasi Performansi Sistem			
				PSNR	**BER**	***CER***	**SNR**
1	21	42	256 x 256	36,87	0	0	46,54
			512 x 512	38,91	0	0	40,17
			1024 x 1024	45,59	0	0	36,06
2	42	84	256 x 256	36,79	0	0	48,28
			512 x 512	38,87	0	0	43,74
			1024 x 1024	45,56	0	0	38,05
3	31	126	256 x 256	36,79	0	0	46,77
			512 x 512	38,84	0	0	41,66
			1024 x 1024	45,52	0	0	35,88

Tabel 6. Pengujian Performansi Subjektif Citra Buah

No	ΣKarakter Uji *Plaintext*	ΣKarakter Uji *Ciphertext*	Ukuran *Pixel Cover*	*MOS* (*Mean Opinion Score*) n=30
1	21	42	256 x 256	4,46
			512 x 512	4,50
			1024 x 1024	4,60
2	42	84	256 x 256	4,56
			512 x 512	4,50
			1024 x 1024	4,56
3	63	126	256 x 256	4,60
			512 x 512	4,50
			1024 x 1024	4,70

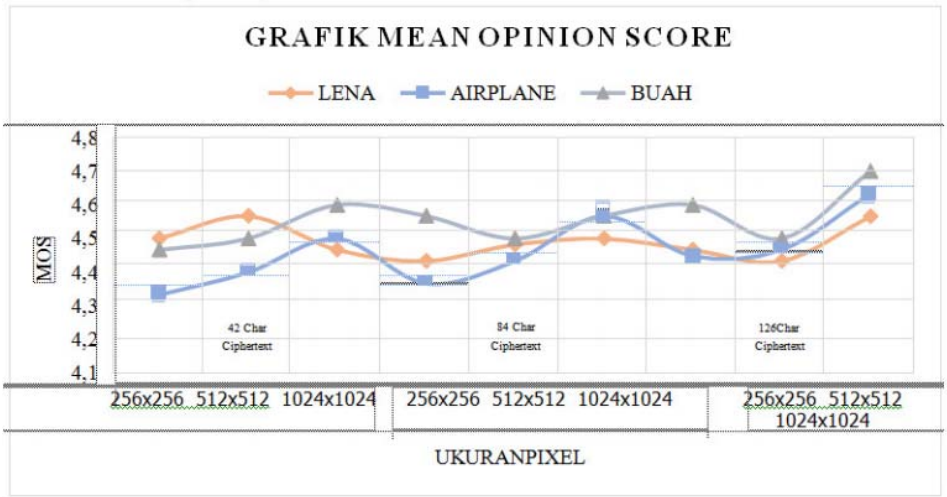
Dalam hasil analisis evaluasi penilaian objektif terhadap nilai *BER* dan *CER* yang dihasilkan oleh *stegoimage* tanpa diberikan gangguan yang digunakan maka, dinyatakan ketiga buah *stegoimage* memiliki nilai *BER* dan *CER* yang sangat baik dengan hasil nilai performansi sebesar 0 untuk semua pengujian yang telah dilakukan, ditunjukan pada Tabel 1, Tabel 3, dan Tabel 6. Perolehan nilai evaluasi performansi *BER* dan *CER* menandakan bahwa tidak ada bit maupun karakter pesan yang hilang maupun berubah atau *error* ketika dilakukan proses ekstraksi atau pengungkapan pesan pada *stego image* yang dihasilkan.

Pada Gambar 6 ditunjukan grafik nilai *PSNR* yang dihasilkan oleh ketiga *stego image*. Studi ini membuktikan grafik hubungan antara jumlah karakter *ciphertext* yang disisipkan terhadap ukuran *pixel cover* citra menunjukan bahwa nilai *PSNR* pada *stego image* akan menghasilkan nilai yang baik atau tinggi apabila ukuran *pixel cover* citra yang digunakan berukuran besar karena ukuran *pixel* menambahkan ruang bagi *stego image*. Pengaruh perbedaan jumlah karakter *ciphertext* yang disisipkan pada setiap ukuran *pixel* yang sama akan menyebabkan penurunan nilai *PSNR* pada *stego image* yang dihasilkan. Adapun penilaian *MOS* yang dihasilkan ditunjukan pada Gambar 7.



Gambar 6. Grafik Performansi *PSNR*

Pada Gambar 7, penilaian *MOS* yang dihasilkan dari penilaian sebanyak 30 responden menghasilkan nilai rata-rata sebesar 4,5. Dalam kriteria penilaian *MOS* yang dihasilkan maka, dapat dinyatakan bahwa pada studi ini menunjukan perbandingan kualitas antara *stego image* dengan *cover* citra tergolongakan membesar ketika ukuran *pixel* bertambah.



Gambar 7. Grafik Performansi *MOS*

3.5 Pengujian Performansi Sistem Dengan Gangguan *Noise*

Pada pengujian performansi sistem, telah dilakukan beberapa pengujian gangguan diantaranya adalah *Noise Gaussian* dan *Noise Salt & Pepper*. Pengujian performansi dengan pemberian *noise* pada sistem dilakukan sebagai analisa hasil evaluasi ketahanan *plaintext* yang dapat terungkap dari analisa nilai performansi *BER* dan *CER* yang dihasilkan. Dalam skenario pengujian performansi sistem dengan gangguan *noise*, pengujian dilakukan pada *cover* citra Lena dengan penentuan jumlah karakter penyisipan terhadap ukuran *pixel* yang digunakan sebagai data uji pengujian.

a. Noise Gaussian

Pada pengujian performansi terkait gangguan *Noise Gaussian* pada *stego image*, dilakukan pemilihan beberapa nilai *varians* dari rentang 0 s.d. 1. Pada Tabel 7 pengujian dilakukan sebanyak nilai rata-rata tiga kali percobaan untuk setiap ukuran *pixel*. Pada pengujian keberhasilan dan ketahanan *stego image* dalam mengungkapkan atau melakukan ekstraksi pesan dengan pemberian uji gangguan *Noise Gaussian*, maka dihasilkan evaluasi pada Tabel 7 yang menunjukan bahwa, nilai varians yang digunakan terkait gangguan *Noise Gaussian* akan merusak ketahanan dan pengungkapan pesan tersembunyi pada nilai varians sebesar 0,0006. Nilai varians maksimum yang dapat ditoleransi terkait keberhasilan dalam pengungkapan pesan dalam pemberian *Noise Gaussian* diperoleh dengan nilai varians sebesar ±0,0001. Hal ini membuktikan studi ini menghasilkan *BER* dan *CER* yang kecil jika terdapat gangguan *Noise Gaussian.*

Tabel 7. Pengujian Noise Gaussian

No.	Ukuran *Pixel*	Evaluasi Performansi *Noise Gaussian 42 Karakter Cipher text*					
		0,0001		0,0003		0,0006	
		BER	*CER*	BER	*CER*	BER	*CER*
1	256 x 256	0	0	0,22	0,53	0,36	1
2.	512 x 512	0	0	0,25	0,69	0,38	1
3.	1024 x 1024	0	0	0,25	0,71	0,39	1
No.	**Ukuran *Pixel***	**si Performansi *Noise Gaussian* 84 *Karakter Cipher text***					
		0,0001		**0,0003**		**0,0006**	
		BER	*CER*	BER	*CER*	BER	*CER*
1.	256 x 256	0	0	0,24	0,59	0,39	1
2.	512 x 512	0	0	0,24	0,61	0,40	1
3.	1024 x 1024	0	0	0,24	0,66	0,41	1
No.	**Ukuran *Pixel***	**si Performansi *Noise Gaussian 126 Karakter Cipher text***					
		0,0001		**0,0003**		**0,0006**	
		BER	*CER*	BER	*CER*	BER	*CER*
1	256 x 256	0	0	0,24	0,64	0,40	1
2.	512 x 512	0	0	0,26	0,65	0,40	1
3.	1024 x 1024	0	0	0,27	0,66	0,43	1

Tabel 8. Pengujian *Noise Salt & Pepper*

No.	Ukuran *Pixel*	Evaluasi Performansi *Noise Salt & Pepper 42* Karakter *Ciphertext*					
		0,0001		0,001		0,01	
		BER	*CER*	BER	*CER*	BER	*CER*
1	256 x 256	0	0	0,158	0,426	0,406	1
2.	512 x 512	0,005	0,031	0,208	0,507	0,404	1
3.	1024 x 1024	0,011	0,047	0,226	0,571	0,450	1
No.	**Ukuran *Pixel***	**Evaluasi Performansi *Noise Salt & Pepper 84* Karakter *Ciphertext***					
		0,0001		**0,001**		**0,01**	
		BER	*CER*	BER	*CER*	BER	*CER*
1	256 x 256	0,002	0,015	0,164	0,428	0,423	1
2.	512 x 512	0,010	0,023	0,226	0,531	0,453	1
3.	1024 x 1024	0,023	0,079	0,232	0,583	0,461	1
No.	**Ukuran *Pixel***	**Evaluasi Performansi *Noise Salt & Pepper 126* Karakter *Ciphertext***					
		0,0001		**0,001**		**0,01**	
		BER	*CER*	BER	*CER*	BER	*CER*
1	256 x 256	0,007	0,015	0,154	0,455	0,427	1
2.	512 x 512	0,171	0,052	0,202	0,545	0,450	1
3.	1024 x 1024	0,029	0,079	0,202	0,587	0,480	1

b. Noise Salt & Pepper

Pada pengujian performansi terkait gangguan *Noise Salt & Pepper*, dilakukan pemilihan beberapa nilai *density* dari rentang 0 s.d. 1. Pada Tabel 8 pengujian dilakukan sebanyak nilai rata-rata tiga kali percobaan untuk setiap ukuran *pixel*. Pengujian dalam keberhasilan pengungkapan pesan terkait dengan pemberian gangguan terhadap *stego image* berupa *Noise Salt & Pepper* pada Tabel 8 maka, studi ini menunjukkan bahwa dengan nilai *density* yang digunakan bernilai sama dengan atau lebih dari nilai 0,01 dari rentang 0 sampai dengan 1 maka dapat didapatkan hasil bahwa ketahanan pengungkapan pesan tersembunyi dalam *stego image* akan rusak seluruhnya atau rusak 100%. Sistem dapat mengungkapkan atau melakukan ekstraksi dengan nilai maksimum toleransi *density* sebesar ±0,0001. Nilai tersebut merupakan nilai yang dapat ditoleransi oleh sistem berdasarkan gangguan yang diberikan berupa *Noise Salt & Pepper*.

4. KESIMPULAN

Dalam upaya meningkatkan keamanan pengiriman informasi atau pesan dalam dunia *digital*, pada tugas akhir ini telah berhasil diselesaikan implementasi dari sebuah system. Pengamanan pesan pada *steganografi* citra domain *Discrete Cosine Transform* dengan teknik penyisipan *Spread Spectrum* memberikan variasi keamanan. Terkait dengan penerapan metode dan teknik yang digunakan dalam implementasi sistem, dihasilkan kualitas *stego image* yang sangat mirip dengan *cover* citra yang digunakan di lihat dari perolehan nilai performansi objektif *PSNR* diatas 30 dB dan subjektif *MOS* di atas nilai 4. Terkait dengan pengujian *Noise Gaussian* dan *Noise Salt & Pepper* yang dilakukan, sistem akan mentoleransi nilai *density* maupun nilai *varians* maksimum yang diberikan sebesar ±0,0001.

DAFTAR RUJUKAN

Alfian Zakaria, R. M. (2015). *Steganografi* Citra *Digital* Menggunakan Teknik *Discrete Wavelet Transform* pada Ruang Warna CIELab. *ITB*.

Bansal, D. (2014). *An Improved DCT based Steganography Technique*. *International Journal of Computer Applications, 102*(14), 46-49.

Chudasama, J. M. (2016). *Dual Steganography*: *A New Hiding Technique for Digital Communication. International Journal of Advanced Research in Electrical, Electronoc and Instrumentation Engineering*, 3184-3188.

Gouda, S. (2015). Least Significant Bit (*LSB*) and Discrete Cosine Transform (*DCT*) based Steganography. *International Journal of Emerging Trending Engineering and Basic Science (IJEEBS), 2*(1), 31-36.

Gunjal, M., & Jha, J. (2014). *Image Steganography Using Discrete Cosine Transform (DCT) and Blowfish Algorithm. International Journal of Computer Trends and Technology (IJCTT), 11*(4), 144-150.

H., H., B, G., & N, L. (2017). Implementasi Teknik *Watermarking* menggunakan FFT dan *Spread Spectrum Watermark* pada Data Audio *Digital*. *ELKOMNIKA, 4*(1), 98-109.

M.P.S. Bhatia, S. K. (2014). *An Image Steganography Method Using Spread Spectrum Technique. Proceedings of Fourth International Conference on Soft Computing for Problem Solving* (pp. 219-236). New Delhi: Springer India.

Massandy, D. T. (2017). *Algoritma Elgamal* Dalam Pengamanan Pesan Rahasia. *Makalah Strukdis 0910-056*.

Negara, I. K. (2016). Analisis dan Implementasi Gabungan *Kriptografi* Elgamal dan *Steganografi* Frame Dengan Menggunakan Kunci Citra *Digital*. *Jurnal Eksplora Informatika*, 141-150.

Neil F. Johnson, S. J. (2001). *Information Hiding: Steganography and Watermarking-Attacks and Countermeasures: Steganography and Watermarking - Attacks and Countermeasures.* London: *Kluwer Academic Publishing*.

ITB, S. (2014, 10 02). *Summit, Seminar Nasional Indonesia Cyber Crime*. Dipetik 2 5, 2017, dari STEI ITB Website: http://stei.itb.ac.id/id/blog/2014/10/03/indonesia-cyber-crime-summit-iccs-2014/

Setyaningsih, M. (2015). *Kriptografi & Implementasinya menggunakan MATLAB.* Yogyakarta: Penerbit ANDI Yogakarta.

Sharma, S., & Kumar, U. (2015). *Review of Transform Domain Techniques for Image Steganography. 3*(5), 2013-2016.