ALGORITMA KRIPTOGRAFI EL-GAMAL UNTUK PENGAMANAN PESAN PADA STEGANOGRAFI CITRA DOMAIN *DISCRETE COSINE TRANSFORM* DENGAN TEKNIK PENYISIPAN *LEAST SIGNIFICANT BIT*

EL-GAMAL ALGORITHM CRYPTOGRAPHY FOR SECURITY MESSAGE ON DISCRETE COSINE TRANSFORM DOMAIN OF IMAGE STEGANOGRAPHY WITH LEAST SIGNIFICANT BIT INSERTION TECHNIQUE

Enrico Wiratama Purwanto[1], Dr.Ir. Bambang Hidayat, DEA[2], Sofia Saidah S.T., M.T.[3]
Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom
enricowiratama@students.telkomuniversity.ac.id

Abstrak

Pada tugas akhir ini, dilakukan penggabungan beberapa buah metode untuk memperkuat serta meningkatkan sisi keamanan dalam proses pertukaran informasi atau pesan digital. Beberapa metode yang digabungkan diantaranya adalah metode kriptografi dan metode steganografi. Implementasi pada sistem yang dibangun dilakukan dengan menggabungkan penerapan metode *algoritma kriptografi El-Gamal* dalam menyandikan pesan pada penerapan metode *steganografi citra* dalam menyembunyikan pesan tersandi yang dihasilkan kedalam sebuah citra warna (RGB) dalam domain *Discrete Cosine Transform* dengan teknik penyisipan *Least Significant Bit*. Berdasarkan dari beberapa pengujian yang telah dilakukan pada sistem, telah diperoleh beberapa hasil performansi dengan nilai rata-rata meliputi *Avalanche Effect* sebesar 70,4828%, *Peak Signal to Noise Ratio* (PSNR) sebesar 40,9554%, *Mean Opinion Score* (MOS) sebesar 4,5024, *Bit Error Rate* (BER) dan *Character Error Rate* (CER) sebesar 0%.

Kata Kunci : Algoritma Kriptografi El-Gamal, Steganografi Citra, Discrete Cosine Transform, Least Significant Bit

Abstract

In this final project, several methods have been combined to strengthen and enhance the security side in the exchange process of the digital information or message. Some of the combined methods used are cryptography and steganography methods. Implementation of the built system is done by combining the application of *El-Gamal cryptography algorithm* in encrypting the message on application of the *image steganography* method in concealing the encrypted messages generated into a color image (RGB) on the *Discrete Cosine Transform* domain with the insertion technique of *Least Significant Bit*. Based on some tests that have been done on the system, the result of average performances score is showed by *Avalanche Effect* of 70.4828%, *Peak Signal to Noise Ratio* (PSNR) of 40.9554%, *Mean Opinion Score* (MOS) of 4,5024, *Bit Error Rate* (BER) and *Character Error Rate* (CER) of 0%.

Keyword : El-Gamal Cryptography Algorithm, Image Steganography, Discrete Cosine Transform, Least Significant Bit

1. Pendahuluan.

Seiring dengan perkembangan dan kemajuan teknologi komunikasi digital yang pesat saat ini, tidak menutup kemungkinan bahwa tindak kejahatan digital pun dapat ikut bertambah dan berkembang. Pencurian maupun penyadapan informasi merupakan sebuah isu keamanan yang harus diperhatikan. 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 meningkatkan keamanan pertukaran pesan, diantaranya dengan menggunakan metode penyandian pesan yang disebut dengan metode kriptografi dan metode penyembunyian pesan ke dalam sebuah media yang disebut dengan metode steganografi.

Berdasarkan penelitian sebelumnya, *Image Steganography Using Discrete Cosine Transform (DCT) and Blowfish Algorithm* [1] menjelaskan bahwa penggunaan algoritma kriptografi *Blowfish* dan steganografi citra transformasi kosinus diskrit dapat memperkuat tingkat keamanan dalam pertukaran pesan. *Image Steganography Using DCT Technique* [2] menjelaskan bahwa penyembunyian pesan kedalam sebuah citra dengan penggunaan transformasi kosinus diskrit (DCT) dapat memperkecil kemungkinan perubahan yang terjadi pada citra hasil penyembunyian pesan. *Least Significant Bit (LSB) and Discrete Cosine Transform (DCT) Based Steganography*

[3] menjelaskan bahwa pada citra hasil penyembunyian pesan dengan penggunaan transfomasi kosinus diskrit (DCT) dan teknik penyisipan *Least Significant Bit* (LSB) dihasilkan nilai BER dan PSNR yang lebih baik bila dibandingkan dengan tanpa atau dilakukannya transformasi lain.

Pada tugas akhir ini, penelitian serta pengujian dilakukan dengan melakukan penggabungan metode kriptografi dan metode steganografi dalam meningkatkan keamanan proses pertukaran pesan. Penerapan metode kriptografi yang dipilih adalah algoritma kriptografi El-gamal pada penerapan metode steganografi citra *Discrete Cosine Transform* (DCT) dengan teknik penyisipan *Least Significant Bit* (LSB) dalam menambahkan variasi model keamanan yang baru.

2. Dasar Teori

2.1. Algoritma Kriptografi El-Gamal

Algoritma kriptografi El-Gamal dikemukakan oleh seorang ilmuwan Mesir bernama Taher El Gamal pada tahun 1985 dalam makalah berjudul "*A public key cryptosystem and a signature scheme based on discrete logarithms*" [4] [5]. Pada dasarnya, implementasi matematis algoritma kriptografi El-Gamal dari awal proses enkripsi hingga proses dekripsi menggunakan perhitungan modulo [6]. Proses dalam implementasi algoritma kriptografi El-Gamal terdiri dari tiga buah proses algoritma, yaitu algoritma pembentukan kunci kriptografi, algoritma enkripsi, dan algoritma dekripsi. Berikut ini, beberapa properti besaran yang digunakan dalam penggunaan algoritma kriptografi El-Gamal ditunjukan pada Tabel 2.1 :

Tabel 2.1 Properti Besaran Algoritama Kriptografi El-Gamal

Simbol	Keterangan	Sifat	Syarat
p	Bilangan Prima	Public	∞
g	Bilangan Acak	Public	$g < p$
x	Bilangan Acak	Private	$1 \leq x \leq p-2$
y	Kunci Publik	Public	-
k	Bilangan Acak	Private	$0 \leq k \leq p-1$
m	Plaintext	Private	$0 \leq m \leq p-1$
a dan b	*Ciphertext* 1 dan 2	Private	∞

a. Algoritma Pembentukan Kunci Kriptografi [5] [6]

Input :

1. Sembarang bilangan prima, *p*.
2. Sembarang bilangan acak *g*, sesuai syarat Tabel 2.1.
3. Sembarang bilangan acak x, sesuai syarat Tabel 2.1.

Proses :

1. Hitung nilai *y*, dengan persamaan :

$$y = g^x \bmod p \tag{2.1}$$

Output :

1. Keluaran berupa bilangan *y*.
2. Kunci publik (*y*, g, *p*).
3. Kunci *private* (*x*,*p*).

b. Algoritma Enkripsi [5] [6]

Input :

1. Susun *plaintext* menjadi blok-blok *m1*, *m2*, dst. sesuai syarat Tabel 2.1.
2. Tentukan bilangan acak *k* sepanjang jumlah *plaintext*, sesuai syarat Tabel 2.1.

Proses :

1. Setiap blok *m* di enkripsi dengan persamaan :

$$a = g^k \bmod p \tag{2.2}$$

$$b = y^k m \bmod p \tag{2.3}$$

Output :

1. Pasangan *a* dan *b* adalah *ciphertext* untuk blok pesan *m*.
2. Penyajian *ciphertext* seperti berikut : *a1 b1 a2 b2* dst.

c. Algoritma Dekripsi [5] [6]

Input :

1. Kunci *private* (*x*,*p*).

Proses :

1. Konversi *ciphertext* ke dalam *plaintext*, dengan persamaan :

$$m = b(a^x)^{-1} \, mod \, p \quad (2.4)$$

dimana,

$$(a^x)^{-1} = a^{p-1-x} \, mod \, p \quad (2.5)$$

Output :

1. *Plaintext* yang dihasilkan berupa *m* dalam desimal ASCII.
2. Lakukan penyusunan pesan *m* yang dihasilkan dan lakukan konversi karakter.

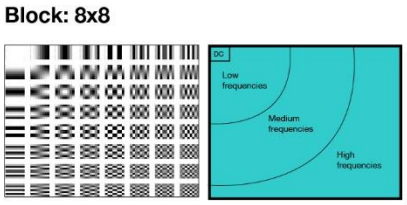
2.2. *Steganografi Citra Digital*

Pengertian "citra" pada steganografi citra digital menyatakan bahwa, *cover object* yang dipilih dan digunakan sebagai media dalam menyembunyikan pesan adalah file gambar (*image*). Ruang penyisipan pesan berada pada nilai intensitas cahaya atau *pixel cover* citra yang digunakan.

Terkait dengan penerapan steganografi citra dalam sistem, pada *cover* citra terlebih dahulu dilakukan perubahan transformasi sehingga bit-bit pesan akan disisipkan ke dalam koefisien citra transformasi (*pixel* transformasi). Penggunaan transformasi digunakan sebagai upaya untuk menghasilkan nilai kemiripan dan ketahanan yang lebih tinggi antara *stego image* yang dihasilkan dengan *cover* citra yang digunakan [2] [3] [7]. Salah satu jenis transformasi *cover* citra yang diterapkan pada tugas akhir ini adalah transformasi kosinus diskret atau *Discrete Cosine Transform* (DCT) [2] [7].

2.3. *Transformasi Kosinus Diskrit (DCT)*

Transformasi kosinus diskrit (DCT) merupakan teknik transformasi yang mengubah sinyal dari representasi domain spasial ke dalam representasi domain frekuensi dengan karakterisitik memecah ukuran *pixel cover* citra menjadi blok-blok dengan ukuran 8 x 8 [2]. Dalam transformasi DCT pada blok ukuran 8 x 8 yang dilakukan, terdapat beberapa sub-band frekuensi yang dihasilkan yakni sub-band frekuensi rendah, menengah, dan tinggi yang ditunjukan pada Gambar 2.1 [1].

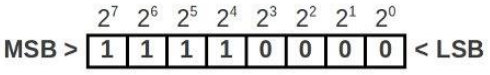


Gambar 2.1 Frekuensi Domain DCT [9]

Berdasarkan daerah frekuensi yang dihasilkan oleh transformasi DCT pada Gambar 2.1, sebagian besar energi sinyal atau bagian visual citra yang paling penting terletak pada daerah frekuensi rendah dan energi sinyal yang kurang penting terletak pada daerah frekuensi tinggi. Pada umumnya energi sinyal di frekuensi tinggi akan hilang ketika dilakukan proses kuantisasi. Oleh karena itu, agar visibilitas *cover* citra tidak terpengaruh pada proses penyisipan pesan dalam ranah DCT, maka pesan disisipkan dengan memodifikasi energi sinyal atau koefisien transformasi yang dihasilkan pada sub-band frekuensi menengah [1].

2.4. *Least Significant Bit (LSB)*

Least Significant Bit (LSB) merupakan teknik penyisipan pesan yang paling sederhana dan cepat dalam pengggunaan metode steganografi. Pesan disembunyikan dengan menyisipkannya bit-bit pesan pada bit terendah atau bit yang paling kanan dari 1 byte pixel cover dimana 1 byte = 8 bit [8].



Gambar 2.2 Daerah Penyisipan LSB

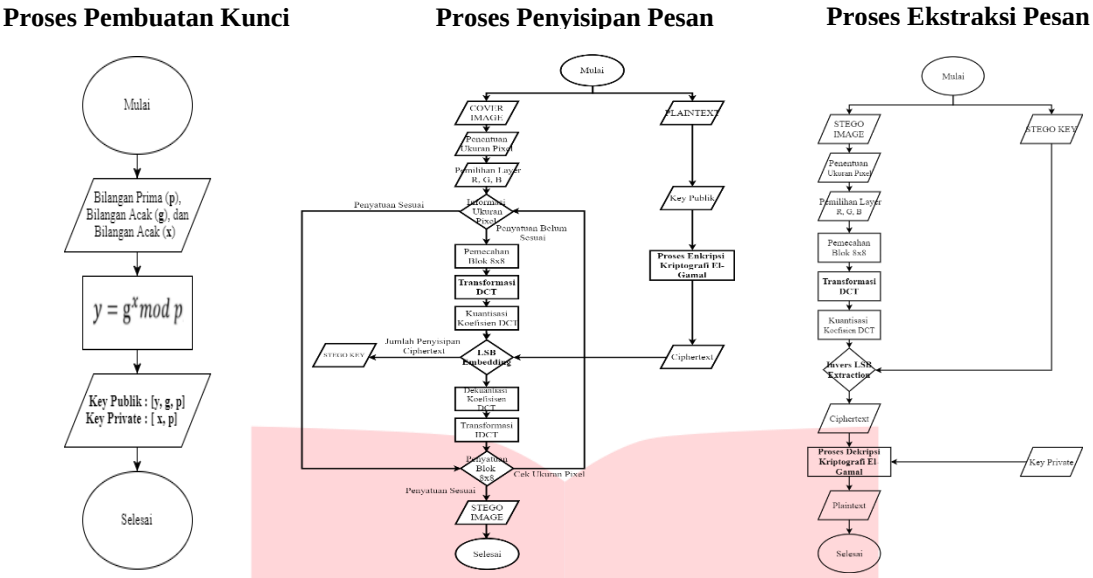
Pada Gambar 2.2 penyisipan bit-bit pesan yang dilakukan dengan teknik LSB hanya mengubah nilai *pixel cover* menjadi satu byte lebih tinggi atau satu lebih rendah dari nilai *pixel* sebelumnya. Hal ini dikarenakan nilai bit paling kanan di representasikan sebesar 2^0 atau 1 sehingga oleh karena hal tersebut maka, penyisipan bit-bit pesan tidak mempengaruhi perubahan *pixel* yang dilakukan secara berarti [8].

3. Perancangan Sistem

3.1. Desain Sistem

Perancangan sistem dijelaskan dengan diagram alir dibawah ini dimana secara garis besar sistem terbagi menjadi tiga buah proses, yakni proses pemebentukan kunci kriptografi, proses penyisipan pesan dan proses

ekstraksi pesan. Properti input yang digunakan dalam sisetem yaitu pesan berupa teks dan *cover* citra berupa citra warna (RGB).



Gambar 3.1 Diagram Alir Desain Sistem

3.2. Proses Pemebentukan Kunci Kripografi

Algoritma dalam pembuatan kunci publik dan kunci private :

a. ***Langkah 1*:** Masukan bilangan prima **(p)**, bilamgan acak **(g)**, dan bilangan acak **(x)** sesuai syarat pada Tabel 2.1 Properti Besaran Algoritma Kriptografi El-Gamal.
b. ***Langkah 2*:** Lakukan pembuatan kunci kriptografi, persamaan 2.1
c. ***Langkah 3*:** Kunci publik untuk skema enkripsi pesan dan kunci private untuk skema dekripsi pesan dihasilkan.

3.3. Proses Penyisipan

Pada proses penyisipan dalam sistem terdapat dua buah skema yang dilakukan, skema tersebut adalah skema enkripsi pesan menggunakan metode algoritma kriptografi El-Gamal dan skema penyisipan pesan terhadap *cover* citra menggunakan metode steganografi.

a. Skema Enkripsi Pesan

Algoritma untuk melakukan enkripsi pesan asli atau *plaintext* menjadi *ciphertext* :

***Langkah 1*:** Masukan pesan atau *plaintext* yang akan di enkripsi.
***Langkah 2*:** Masukan kunci publik yang dihasilkan
***Langkah 3*:** Lakukan proses enkripsi, persamaan 2.2 dan 2.3.
***Langkah 4*:** *Ciphertext* kriptografi El-Gamal dihasilkan.

b. Skema Penyisipan Pesan

Algoritma untuk menyisipkan *ciphertext* ke dalam *cover* citra metode steganografi :

***Langkah 1*:** *Read ciphertext* kemudian rubah ke dalam bentuk biner.
***Langkah 2*:** *Read cover* citra.
***Langkah 3*:** Lakukan penentuan ukuran *pixel* yang akan digunakan.
***Langkah 4*:** Lakukan pemilihan *layer* warna.
***Langkah 5*:** Lakukan pemecahan blok-blok piksel citra dengan ukuran 8 x 8.
***Langkah 6*:** Lakukan transformasi kosinus diskrit (DCT) pada setiap blok pixel yang tersedia.
***Langkah 7*:** Lakukan kuantisasi koefisien DCT pada setiap blok pixel.
***Langkah 8*:** Lakukan LSB untuk menyisipkan bit-bit *ciphertext* pada. koefisien DCT frekuensi tengah setiap blok ukuran 8 x 8.
***Langkah 9*:** *Stego Key* dihasilkan untuk proses ekstraksi pesan.
***Langkah 10*:** Lakukan *invers* mulai dari langkah 7 sampai dengan langkah 5.
***Langkah 11*:** *Stego image* dihasilkan.

3.4. Proses Ekstraksi

Pada proses ekstraksi terdapat dua buah skema yang dilakukan, skema tersebut adalah skema ekstraksi pengungkapan *ciphertext* dari *stego image* dan skema dekripsi *ciphertext* algoritma kriptografi El-Gamal kedalam pesan asli**.**

a. Skema Ekstraksi Ciphertext

Algoritma dalam mengungkapkan *ciphertext* dari *stegoimage* :

Langkah 1: Read stego image.
Langkah 2: Lakukan penentuan ukuran pixel stego image.
Langkah 3: Lakukan pemilihan layer warna pada stego image.
Langkah 4: Lakukan pemecahan blok-blok piksel stego image dengan ukuran 8 x 8.
Langkah 5: Lakukan transformasi kosinus diskrit (DCT) pada setiap blok pixel yang tersedia.
Langkah 6: Lakukan kuantisasi koefisien DCT pada setiap blok pixel.
Langkah 7: Lakukan invers LSB pada koefisien DCT frekuensi tengah untuk setiap blok dengan Stego Key.
Langkah 8: Ciphertext dihasilkan.

b. **Skema Dekripsi Ciphertext**

Algoritma untuk menngungkap *ciphertext* ke dalam pesan asli atau *plaintext*

Langkah 1: Read ciphertext.
Langkah 2: Masukan kunci private yang dihasilkan
Langkah 3: Lakukan proses dekripsi, persamaan 2.5 dan 2.5.
Langkah 4: Pesan (plaintext) dihasilkan.

4. Pengujian Sistem dan Analisis

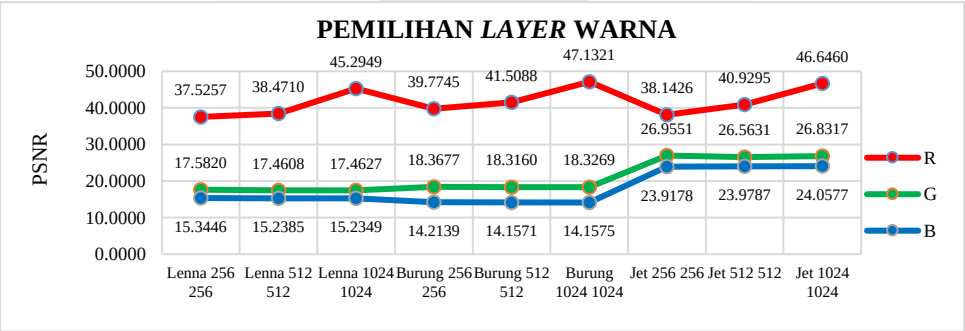
Untuk melakukan analisa terhadap sistem yang telah dihasilkan maka, pada jurnal ini dilakukan beberapa skenario evaluasi pengujian, diantaranya sebagai berikut :

1. Skenario evaluasi pemilihan *layer* warna pada *cover* citra terhadap nilai PSNR.
2. Skenario evaluasi kapasitas penyisipan *cover* citra terhadap jumlah karakter *plaintext* dan *ciphertext*.
3. Skenario evaluasi performansi algoritma kriptografi El-Gamal.
4. Skenario evaluasi performansi sistem tanpa dan dengan gangguan *noise*.

Berikut ini merupakan hasil evaluasi yang dianalisis berdasarkan skenario evaluasi yang telah dilakukan diantaranya :

4.1. Pengujian Pemilihan *Layer* Warna Pada *Cover* Citra Terhadap Nilai PSNR

Dalam hal meminimalisir kecurigaan yang mungkin terjadi terhadap *stego image* yang dihasilkan terkait dengan penyembunyian pesan yang dilakukan kedalam salah satu *layer* citra warna (RGB) *cover* citra maka, dilakukan sebuah pengujian berdasarkan pengaruh pemilihan *layer* warna terhadap nilai PSNR yang dihasilkan. Pada Gambar 4.1 ditunjukan pengaruh beberapa nilai PSNR yang dihasilkan oleh tiga buah *cover* citra yang digunakan terhadap masing-masing *layer* warna berdasarkan jumlah karakter yang sama dan ukuran *pixel* yang berbeda.

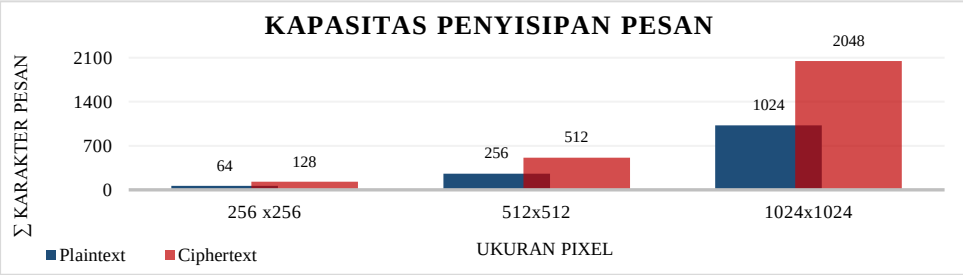


Gambar 4.1 Pemilihlan Layer Warna

Pengujian yang dilakukan pada Gambar 4.1, menunjukan perolehan nilai PSNR pada setiap pengujian masing-masing *layer* warna yang dihasilkan dengan rata-rata perolehan nilai sebesar 41,7139 untuk *layer* merah, 20,8740 untuk *layer* hijau, dan 17,8112 untuk *layer* biru. Dalam pengujian yang telah dilakukan maka disimpulkan bahwa *layer* warna yang optimal untuk digunakan pada *cover* citra pengujian adalah *Red Layer* atau *layer* merah.

4.2. Pengujian Kapasitas Penyisipan *Cover* Citra Terhadap Jumlah Karakter Pesan

Berdasarkan penggunaan teknik transformasi kosinus diskrit (DCT), teknik penyisipan *Least Significant Bit* (LSB), dan ukuran *pixel cover* citra digital yang digunakan pada sistem maka, diperoleh informasi mengenai kapasitas maksimum jumlah karakter pesan yang dapat disisipkan ke dalam sebuah *cover* citra. Berkaitan dengan penerapan algorima kriptografi El-Gamal maka, pesan yang disisipkan adalah karakter-karakter *ciphertext* yang dihasilkan.



Gambar 4.2 Kapasitas Karakter Ciphertext dan Plaintext Terhadap Ukuran Pixel

Pada Gambar 4.2 disajikan grafik perbandingan terkait kapasitas antara jumlah karakter *plaintext* dengan *ciphertext*. Berdasarkan jumlah karakter *ciphertext* yang dapat disisipkan kedalam *cover* citra dapat disimpulkan bahwa jumlah ukuran karakter *ciphertext* membutuhkan kapasitas sebesar dua kali lipat dari jumlah karakter *plaintext* sehingga ukuran *pixel cover* citra yang besar sangat mempengaruhi banyaknya karakter yang dapat digunakan pada sistem yang telah dibangun.

4.3. Pengujian Algoritma Kriptografi El-Gamal

Pada Tabel 4.3. dilakukan pengujian karakter *plaintext* menjadi *ciphertext* dalam mengetahui kekuatan enkripsi yang dihasilkan pada penilaian *Avalanche Effect* pada Tabel 4.1 dan penilaian *Brute Force Attack pada Tabel 4.2*. Pengujian dilakukan pada jumlah karakter yang berbeda sebanyak tiga kali percobaan.

Tabel 4.1 Pengujian Avalanche Effect

No.	∑ Karakter *Plaintext*	Karakter *Ciphertext*	Bit Beda	Avalanche (%)
1	6	@,▯n▯e▯S▯x }	65	67,7083
2	6	X▯;▯r▯:▯▯ }	69	71,8750
3	6	X▯; 9▯S@▯_	71	73,9583
4	15	▯1▯[@▯''@▯{▯▯ k▯''@▯ p N@▯]▯C	166	69,1667
5	15	▯▯]@▯ t <▯o▯▯^▯:▯r @''▯▯; p	168	70,0000
6	15	b▯]▯\@N@▯?▯@▯^ t▯e▯C@''▯a▯m▯▯'	174	72,5000
7	24	▯1▯]▯e▯: q▯?▯▯/ t .▯8@''@▯7@▯ ▯▯8@/▯e▯_@▯ev :@~	268	68,0203
8	24	X▯n▯r▯i@▯{@ ▯u t . p▯▯8@n▯▯▯▯▯ ^ 9 { @v▯ }	276	70,0508
9	24	▯1▯[▯r▯i@ }▯@ z▯S▯K▯a▯t▯C@n ▯@▯P▯W 9@?▯▯ m▯i w	280	71,0660

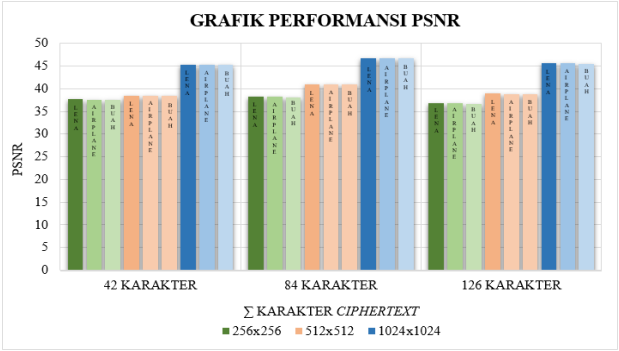
Tabel 4.2 Pengujian Brute Force Attack

No.	∑ Karakter *Plaintext*	∑ Karakter *Ciphertext*	*Cluster* (per Tahun) A	B	C
1	6	12	$1{,}1194 \times 10^{10}$	$1{,}1194 \times 10^{9}$	$1{,}1194 \times 10^{8}$
2	6	12	$1{,}3867 \times 10^{10}$	$1{,}3867 \times 10^{9}$	$1{,}3867 \times 10^{8}$
3	6	12	$1{,}8987 \times 10^{10}$	$1{,}8987 \times 10^{9}$	$1{,}8987 \times 10^{8}$
Rata-Rata			$\mathbf{1{,}4682 \times 10^{10}}$	$\mathbf{1{,}4682 \times 10^{9}}$	$\mathbf{1{,}4682 \times 10^{8}}$
4	15	30	$4{,}5851 \times 10^{46}$	$4{,}5851 \times 10^{45}$	$4{,}5851 \times 10^{44}$
5	15	30	$5{,}9056 \times 10^{46}$	$5{,}9056 \times 10^{45}$	$5{,}9056 \times 10^{44}$
6	15	30	$7{,}5904 \times 10^{46}$	$7{,}5904 \times 10^{45}$	$7{,}5904 \times 10^{44}$
Rata-Rata			$\mathbf{6{,}0270 \times 10^{46}}$	$\mathbf{6{,}0270 \times 10^{45}}$	$\mathbf{6{,}0270 \times 10^{44}}$
7	24	48	$4{,}4672 \times 10^{84}$	$4{,}4672 \times 10^{83}$	$4{,}4672 \times 10^{82}$
8	24	48	$6{,}6097 \times 10^{84}$	$6{,}6097 \times 10^{83}$	$6{,}6097 \times 10^{82}$
9	24	48	$1{,}4334 \times 10^{85}$	$1{,}4334 \times 10^{84}$	$1{,}4334 \times 10^{83}$
Rata-Rata			$\mathbf{8{,}4703 \times 10^{84}}$	$\mathbf{8{,}4703 \times 10^{83}}$	$\mathbf{8{,}4703 \times 10^{82}}$

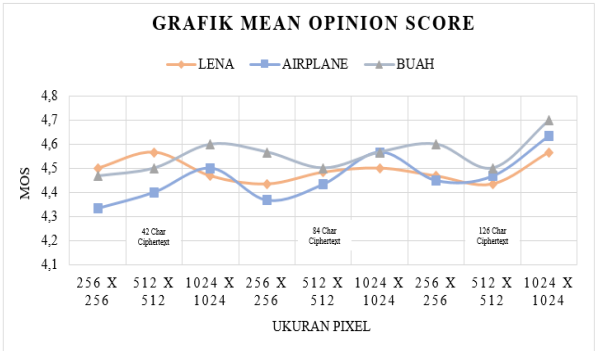
Pada Hasil evaluasi pengujian nilai *Avalanche Effect* yang ditunjukan pada Tabel 4.1 terkait kekuatan *ciphertext* yang dihasilkan nilai *Avalanche Effect* rata rata sebesar 70,4828 % dengan standar deviasi *sample* sebesar 2,0718%. Terkait Cluster yang digunakan pada pengujian *Brute Force Attack*, diasumsikan bahwa kekuatan komputasi komputer *Cluser A, Cluser B, Cluser C* adalah 10.000.000, 100.000.000, 1.000.000.000 komputasi/detik sehingga ditunjukan hasil pada Tabel 4.2.

4.4. Pengujian Performansi Sistem Tanpa Gangguan *Noise*

Dalam implementasi sistem dihasilkan performansi PSNR dan MOS dengan nilai rata-rata sebesar 40,9592 dB dan 4,5024 , Grafik penilaian PSNR dan MOS ditunjukun p ada Gambar 4.3 dan Gambar 4.4.



Gambar 4.4 Grafik Performansi PSNR Pengujian



Gambar 4.3 Grafik Performansi MOS Pengujian

Pada Gambar 4.3, 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. Kemudian, diperkuat dengan penilaian MOS sebagai penilaian subjektif, ditunjukan pada Gambar 4.4 dimana penilaian MOS menghasilkan nilai rata-rata sebesar 4,5024 dari penilaian sebanyak 30 responden. Dalam kriteria penilaian PSNR dan MOS yang dihasilkan maka,dapat dinyatakan bahwa perbandingan kualitas antara *stego image* dengan *cover* citra tergolong pada kriteria mirip hingga sangat mirip.

Terkait penilaian BER dan CER yang dihasilkan pada saat pengungkapan atau ekstraksi pesan, pengungkapan pesan dinyatakan berhasil 100% apabila nilai BER dan CER yang dihasilkan sama dengan 0%. Pada sistem, pengujian terkait ketahanan pesan yang dapat terungkap apabila dilakukan pengujian beberapa serangan berupa *Noise Salt & Pepper* dan *Noise Gaussian*, dihasilkan bahwa pengungkapan pesan berhasil 100% dengan nilai BER dan CER sama dengan 0% jika berada pada kondisi yang ditunjukan pada Tabel 4.2 dan Tabel 4.3.

Tabel 4.2 Pengujian Noise Gaussian

No.	Ukuran Pixel	Evaluasi Performansi Noise Gaussian *42 Karakter Ciphertext*					
		0,0001		0,0003		0,0006	
		BER	CER	BER	CER	BER	CER
1	256 x 256	0,0000	0,0000	0,2222	0,5397	0,3631	1
2.	512 x 512	0,0000	0,0000	0,2580	0,6984	0,3869	1
3.	1024 x 1024	0,0000	0,0000	0,2580	0,7143	0,3988	1
No.	**Ukuran Pixel**	**Evaluasi Performansi Noise Gaussian *84 Karakter Ciphertext***					
		0,0001		0,0003		0,0006	
		BER	CER	BER	CER	BER	CER
1	256 x 256	0,0000	0,0000	0,2432	0,5952	0,3988	1
2.	512 x 512	0,0000	0,0000	0,2440	0,6190	0,4077	1
3.	1024 x 1024	0,0000	0,0000	0,2431	0,6667	0,4196	1
No.	**Ukuran Pixel**	**Evaluasi Performansi Noise Gaussian *126 Karakter Ciphertext***					
		0,0001		0,0003		0,0006	
		BER	CER	BER	CER	BER	CER
1	256 x 256	0,0000	0,0000	0,2460	0,6455	0,4028	1
2.	512 x 512	0,0000	0,0000	0,2679	0,6508	0,4048	1
3.	1024 x 1024	0,0000	0,0000	0,2798	0,6667	0,4365	1

Tabel 4.3 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	0,0000	0,0000	0,1587	0,4268	0,4067	1
2.	512 x 512	0,0059	0,0317	0,2083	0,5079	0,4048	1
3.	1024 x 1024	0,0119	0,0476	0,2262	0,5714	0,4504	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	0,0020	0,0158	0,1647	0,4280	0,4236	1
2.	512 x 512	0,0109	0,0238	0,2262	0,5317	0,4538	1
3.	1024 x 1024	0,0238	0,0793	0,2321	0,5833	0,4613	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	0,0072	0,0159	0,1548	0,4550	0,4272	1
2.	512 x 512	0,1717	0,0529	0,2024	0,5450	0,4504	1
3.	1024 x 1024	0,0298	0,0794	0,2024	0,5873	0,4802	1

Berdasarkan pengujian dengan tiga nilai yang digunakan dalam pengujian *Noise Gaussian* dan *Noise Salt & Pepper* pada Tabel 4.2 dan Tabel 4.3, nilai yang digunakan tersebut menunjukan nilai *density* maupun nilai *varians* yang dapat di toleransi oleh sistem ketika diuji dengan kedua buah *noise* tersebut. Pada Tabel 4.2 dan Tabel 4.3 sistem akan mentoleransi nilai *density* maupun nilai *varians* maksimum yang diberikan sebesar 0,0001 atau 10^{-4} untuk pengungkapan pesan berhasil 100% dengan nilai BER dan CER yang dihasilkan sama dengan 0%.

5. Kesimpulan dan Saran

5.1. Kesimpulan

Berdasarkan hasil pengujian dan analisis pengujian sistem, maka dapat ditarik kesimpulan sebagai berikut :

1. Implemetasi penggunaan metode kriptografi dengan pengunaan algoritma kriptografi El-Gamal dan metode steganografi citra transformasi kosinus diskrit dengan penyisipan *Least Significant* Bit berhasil.
2. Terkait dengan penerapan metode dan teknik yang digunakan dalam implementasi sistem, dihasilkan kualitas *stego image* yang sangat mirip dengan *cover* citra yang digunakan dapat di lihat dari perolehan nilai performansi objektif PSNR dan subjektif MOS.
3. Pada proses penyisipan pesan bit-bit *ciphertext* yang dihasilkan terkait penggunaan algotima kriptografi El-Gamal, proses penyisipan memerlukan kapasitas ukuran *pixel cover* citra yang cukup besar.
4. Penggunaan algoritma kriptografi El-Gamal dinyatakan memiliki kekuatan enkripsi yang sangat kuat dengan nilai rata-rata lebih dari 50% dan pengujian komputasi *Brute Force Attack* yang sangat amat lama.
5. Kriteria *imperceptibility*, *fidelity*, *recovery* dapat terpenuhi dengan baik, namun kriteria *robustness* yang dihasilkan dapat dinyatakan baik apabila berada pada nilai dengan kondisi tertentu terkait dengan pengujian *Noise Salt & Pepper* dan *Noise Gaussian* yang dilakukan, dimana sistem akan mentoleransi nilai *density* maupun nilai *varians* maksimum sebesar 0,0001 atau 10^{-4}.

5.2. Saran

Adapun saran yang dapat diberikan untuk pengembangan sistem ini adalah sebagai berikut :

1. Penerapan sistem pada bahasa pemrograman lain seperti Android Studio, C++, Java, dan bahasa program lainnya.
2. Penerapan *cover* object lain seperti teks, audio dan video.
3. Penerapan teknik transformasi dan penyisipan lainnya.

Daftar Pustaka:

[1] M. Gunjal and J. Jha, "International Journal of Computer Trends and Technology (IJCTT)," *Image Steganography Using Discrete Cosine Transform (DCT) and Blowfish Algorithm*, vol. 11, no. 4, pp. 144-150, 2014.

[2] S. Sharma, "Review of Transform Domain Techniques for Image Steganography," *International Journal of Science and Research (IJSR)*, vol. 3, no. 5, pp. 2013-2016, 2015.

[3] S. R. Gouda, "Least Significant Bit (LSB) and Discrete Cosine Transform (DCT) based Steganography," *International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS)*, vol. 2, no. 1, pp. 31-36, 2015.

[4] D. Bansal, "An Improved DCT based Steganography Technique," *International Journal of Computer Applications* , vol. 102, no. 14, pp. 46-49, 2014.

[5] S. Sandro, "Pelita Informatika Budi Darma," *Perancangan Aplikasi Steganografi Untuk Menyisipkan Pesan Teks Pada Gambar Dengan Metode End of File*, vol. IV, no. Agustus, pp. 45-51, 2013.

[6] E. Triandini and I. K. R. Y. Negara, "Analisis dan implementasi gabungan kriptografi elgamal dan steganografi frame dengan menggunakan kunci citra digital," *EKSPLORA INFORMATIKA*, vol. 3, no. 2, pp. 141-150, 2014.

[7] D. T. Massandy, *Algoritma Elgamal Dalam Pengamanan Pesan Rahasia*, pp. 1-5.

[8] J. Gajjar, "Survey : Image Steganography using DCT Technique Narayan Shastri Institute of Technology," *IJSRD - International Journal for Scientific Research & Development* , vol. 3, no. 01, pp. 208-210, 2015.

[9] B. Cabrera, "Image Encoding," Monday Nov 2014. [Online]. Available: http://obsessive-coffee-disorder.com/image-encoding/. [Accessed Wednesday 12 2017].