STEGANOGRAFI DENGAN MENGGUNAKAN METODE DIVISION *ARITHMATIC AND GENERELAIZED EXPLOITING MODIFICATION DIRECTION* DAN *CODING BCH*

STEGANOGRAPHY USINGDIVISIONARITHMATIC AND GENERELAIZED EXPLOITING MODIFICATION DIRECTION METHODANDCODING BCH

Mahdan Muqotirullah Al Askariyy[1], Bambang Hidayat[2], I Nyoman Apraz Ramatryana[3]
[1,2,3]Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro – Universitas Telkom
Jl.Telekomunikasi No.1, Dayeuh Kolot, Bandung 40257 Indonesia alaskariyy@telkomuniversity.ac.id[1], bhidayat@telkomuniversity.ac.id[2], Ramatryana@telkomuniversity.ac.id[3]

ABSTRAK

Pertumbuhan teknologi sangat pesat pada era modern. Pertukaran informasi terjadi setiap saat. Beragam cara untuk saling bertukar informasi sudah banyak dilakukan dan semakin berkembang. Banyak pihak tak bertanggung jawab mencuri data data yang kita kirimkan. Hal ini menyebabkan perlu adanya teknik yang dapat menanggulangi permasalahan tersebut. Teknik yang sangat sering digunakan oleh masyarakat saat in adalah steganografi. Dalam tugas akhir ini akan dirancang suatu sistem steganografi dengan metode *Division Arithmetic and Generalized Exploiting modification Direction*. Metode ini mampu menampung pesan rahasia yang cukup besar. Pada sistem yang akan dirancang ini ditambahkan suatu teknik *error correction* dengan metode BCH. Hasil yang diperoleh dari Tugas Akhir ini adalah mendapatkan total pesan yang dapat disisipkan dari tiga cover image dengan ukuran sama yauitu 300x300 piksel didapat rata-rata kapasitas bit per piksel 'baboon' 1,3743556, 'fist' 1,7987556, 'straw' 1,6506667, 'lena' 1,572994. Berhasil menyisipkan pesan dengan tidak merusak kualitas citra dari citra aslinya dengan nilai PSNR terendah sebesar 50,38509 dB dan nilai MSE terbesar sebesar 0.353422, didapatkan pada penyisipan citra 'lena' dengan panjang pesan sebesar 190x190 piksel. Dengan skema 1 dan 2 sistem dapat bertahan pada serangan noise 'salt & pepper' dengan density 0.0001 dengan nilai BER 0, dan pada noise 'gaussian' dengan nilai varian 0.0000001. Dengan nilai BER maksimal sebesar 0.427615 pada penyisipan pesan 256x256 dengan cover 'lena'. Sedangankan dengan manipulasi *cropping resizing* dan *compressing* sistem mengalami *error*. Sementara untuk hasil waktu komputasi terendah pada proses penyisipan adalah 0,7979267 detik pada proses ekstraksi pesan 24x24 piksel dan tertinggi 37,97552 detik pada penyisipan pesan 190x190 piksel. Sedangkan untuk proses ekstraksi paling pendek 7,4029921 detik pada proses ekstraksi pesan 24x24 piksel dan paling panjang 365,1651 detik pada penyisipan pesan 190x190 piksel. Sistem juga dapat bertahan pada analisis *bitplane attack*.

Kata kunci : Steganografi, Hamming code, bitplane attack, Division Arithmetic and Generalized Exploiting modification Direction, BCH code

ABSTRACT

Rapid growth of technology in the modern era. The exchange of information occurs at any time. Various ways to exchange information has been done and is growing. Many irresponsible parties theft of proprietary data that we send. This leads to the need for techniques that can cope with these problems. Technique very often used by people currently in is steganography. In this final project will be designed a system steganographic method and Generalized Arithmetic Division Exploiting Direction modification. This method is able to accommodate a secret message that is big enough. On the system to be designed is added to a technique BCH error correction method. The results of this final task is to get the total message that can be inserted from three cover image with the same size of 300x300 pixels yauitu obtained an average capacity of bits per pixel 'baboons' 1.3743556 'fist' 1.7987556 'straw' 1 , 6506667, 'lena' 1.572994. Successfully insert message by not damaging the image quality of the original image with the lowest value of 50.38509 dB PSNR and MSE greatest value of 0.353422, obtained upon insertion image 'lena' with message length of 190x190 pixels. With schemes 1 and 2 the system can withstand the attack noise 'salt and pepper' with a density of 0.0001 with a BER value 0, and the noise 'gaussian' with the variance value 0.0000001. With a maximum BER value of 0.427615 at 256x256 message insertion to cover 'lena'. Sedangankan with manipulation cropping resizing and compressing system is experiencing errors. As for the results of computational time lows in the insertion process is 0.7979267 seconds in the extraction process messages 24x24 pixels and highest message insertion 37.97552 seconds at 190x190 pixels. While for most short-extraction process 7.4029921 seconds in the extraction process messages 24x24 pixels and the longest 365.1651 seconds at 190x190 pixels message insertion. The system can also withstand the attack Bitplane analysis.

Keywords: Steganografi, Hamming code, bitplane attack, Division Arithmetic and Generalized Exploiting modification Direction, BCH code

1. Pendahuluan

Pada penelitian sebelumnya digunakan teknik steganografi dengan metode *Division Arithmetic and Generalized Exploiting Modification Direction* yang merupakan pengembangan dari steganografi dengan metode LSB yang memiliki kelemahan terhadap *bit-plane attack* .Hal yang membedakan pada tugas akhir ini

terletak pada penambahan bit-error checking yang sangat berguna untuk mendeteksi apakah informasi yang dikirimkan masih utuh ataukah tidak[1]. Digunakan citra sebagai media untuk penyembunyian pesan. Metode ini dipilih karena memiliki kapasitas yang tinggi dalam penyembunyian pesannya, dan dapat tahan terhadap serangan bit-plane attack. Untuk menambah ketahanan sistem akan ditambah dengan pengkodean BCH. Penelitian bertujuan untuk mengetahui kapasitas penyisipan pada setiap citra *cover*, menganalisis nilai PSNR dan MSE, dan nilai BER bila diberi serangan. Juga menguji sistem dengan serangan *bitplane attack*. Metodologi penelitian yang akan dilakukan diantaranya adalah: Identifikasi masalah penelitian, Tahap pengumpulan data, Perancangan dan simulasi, Tahap analisis, dan yang terakhir tahap penyusunan laporan

2. Dasar Teori

A. Steganografi

Steganografi berasal dari bahasa Yunani *steganos* yang artinya "tersembunyi" dan *graphein* yang artinya "menulis". Steganografi (*steganography*) adalah ilmu dan seni menyembunyikan pesan rahasia (*hiding message*) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia.[6] Dalam pengimplemantasiannya, steganografi menggunakan berbagai macam objek multimedia baik sebagai *host* maupun *message* seperti *file* citra, audio, teks atau video.

B. Citra Digital

Citra digital dapat dinyatakan sebagai suatu fungsi dua dimensi *f(x,y)*, dimana x maupun y adalah posisi koordinat sedangkat *f* merupakan amplitude pada posisi *(x,y)* yang sering dikenal sebagai intensitas atau grayscale. Nilai intensitas tersebut dalam bentuknya diskrit dari mulai 0 sampai dengan 255. [5]

Dalam komputer, citra digital disimpan sebagai suatu *file* dengan format tertentu. Format citra tersebut menunjukkan cara sebuah citra digital disimpan, misalnya apakah dengan suatu kompresi atau tidak. Contoh format citra yang digunakan pada proses steganografi ini adalah.BMP. Format BMP adalah format penyimpanan standar tanpa kompresi yang umum dapat digunakan untuk menyimpan citra biner hingga citra warna. [5]

Selain format memiliki penyimpanan, citra digital juga dapat menampilkan warna yang merupakan kombinasi dari tiga warna dasar, yaitu merah, hijau, dan biru (*Red, Green, Blue*) yang disebut citra RGB. Setiap warna merupakan 1 layer (*gray-scale*) yang memiliki rentang nilai dari 0 sampai 255. Citra RGB memiliki kapasitas penyimpanan 8 bit per-*layer*nya. Dengan skala 256 per-*layer*nya, citra RGB memiliki warna total sebanyak 16.777.216 warna. Sedangkan pada citra, *black white* merupakan warna citra yang mewakili hitam dan putih. Pada MATLAB, nilai nol adalah hitam dan satu adalah putih.

C. Division Arithmatic and Generelized Exploiting Modification Direction

Untuk meningkatkan nilai entropi dan kapasitas maksimum, diusulkan sebuah metode penyisipan pesan berdasarkan DA-GEMD. Proses penyisipan pesan dengan metode DA-GEMD ini ditunjukan sebagaimana gambar. Pada dasarnya metode ini merupakan penggabungan antara dua metode yaitu *GEMD* dan *2-LSB.*

Kuo dan Wang mengembangkan metode penyembunyian data GEMD untuk meningkatkan kapasitas penyisipan dari metode EMD. Berdasarkan skema Kuo-Wang, berikut ini adalah fungsi ekstraksi baru yang ditawarkan

$$f_g(x_1, x_2, \dots, x_n) = \sum_{i=1}^{n} x_i \times (2^i - 1) \bmod 2^{n+1} \quad \text{.....(1)}$$

Dimana x_i adalah i_th piksel dan n adalah nomer piksel..

$f_{GEMD}(.)$ dapat mengambil semua n-tuple $(x_1, x_2, \dots, x_n)$ dari partisi citra x_n kedalam *non-overlapping* n-piksel blok dengan cara *scanning* dari kiri ke kanan setiap baris dan dari atas kebawah, seperti ditunjukan oleh gambar . Fungsi GEMD dapat mengambil (2^{n+1})-ary data m dari partisi pesan rahasia M dari setiap blok.

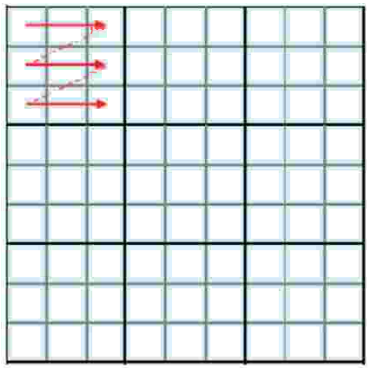
Algoritma penyisipan DA-GEMD

Beberapa notasi didefinisikan untuk membantu pengenalan skema DA-GEMD:

x_n : *Grayscale cover image*

$f_{GEMD}(.)$: Ambil semua 9 piksel $(x_1, x_2, \dots, x_9)$ dengan cara membagi-bagi *cover image* x_n kedalam piksel 3 x 3 untuk setiap blok dengan memindai dari kiri ke kanan dan dari atas ke bawah, seperti ditunjukan oleh gambar XXX

$f_{GEMD\_s}(.)$: Ambilsetiap *n*-bit binary data *m* dengan membagi pesan rahasia *M* dari setiap blok.



Gambar 1. *Pola penyebaran DA-GEMD*

Input : *Cover image* dan data rahasia berbentuk bit
Output : *Stego image*
(DA-GEMD-1) : Ambil semua piksel 3x3 dari setiap blok (, , ... ,) dari dan .
(DA-GEMD-2) : Untuk setiap blok,
1.Hitung *quotient set Q* dan residu RR :
$Q = \{ [x_i/4]$, untuk i=1,2,...,9$\}$.....(2)
$RR = \{ [\bmod 4$, untuk i=1,2,...9$\}$.....(3)
2.Cari median dari *Q* sebagai nilai dari
3.Hitung nilai perbedaan antara dan
4.Sesuai dengan dua kondisi, kita dapat menyisipkan n-bit pesan rahasia kedalam dari i = 1,2,...,9.
Kondisi A : 0,
Gunakan 2-LSB untuk mengganti dua LSB dengan pesan rahasia.
Kondisi B : 0,
if = 0, *then* = + 1,
else if = 3, = − 1, =
x'_i = 4 + , dan sisipkan pesan rahasia menggunakan algoritma GEMD.

Algoritma Ekstraksi DA GEMD
Input : *stego image*
Output : pesan rahasia *bit-stream* M
(DA-GEMD-E-1): Dapatkan semuapiksel 3×3 untuk setiap blok (, ,.....,) dari dan .
(DA-GEMD-E-2) : Untuk setiap blok,
1.Hitung *quotient set QE*dan residu *RRE* :
$QE = \{ [x_i/4]$, untuk i=1,2,...,9$\}$.....(4)
$RRE = \{ \bmod 4$, untuk i=1,2,...9$\}$.....(5)
2.Cari median dari *QE*sebagai nilai dari
3.Hitung nilai perbedaan antara dan
4.Sesuai dengan dua kondisi, kita dapat mendapatkan n-bit pesan rahasia kedalam dari i = 1,2,...,9.
Kondisi A : 0,
Gunakan 2-LSB untuk mengambil dua LSB sebagai pesan rahasia.
Kondisi B : 0,
Gunakan algoritma GEMD untuk untuk mengabil pesan rahasia.
Maka didapat pesan rahasia $m=(\|)$
(DA-GEMD-E-3): Gabungkan seluruh *m* dari setiap blok untuk membentuk pesan rahasia *M*.

D. BCH Codes

Kode BCH merupakan salah satu teknik pengkodean yang merupakan pengimplementasian dari channel coding. Kode BCH mempunyai kemampuan untuk mengkoreksi semua bentuk acak dari "t" error dengan algoritma pengkodean yang sederhana dan mudah diimplementasikan. Dengan memanfaatkan kode ini, Diharapkan kesalahan yang terjadi pada bit-bit informasi dapat dideteksi dan dikoreksi.

Encoding BCH

Message input yang berupa image biner(*black and white*) dibah kedalam matriks 5 kolom sebelum di *encoding BCH* karena akan digunakan BCH(15,5). Jika masukannya kurang dari kelipatan 5 maka *message* akan ditambah *zero padding* terlebih dahulu. Parameter yang digunakan adalah m=4, k=5, n=2^{m-1} dan t=2.

Masing-masing kolom diproses sebagai berikut:

a. Setiap 5 bit masukan (kolom) diubah ke dalam polynomial m(x).
Misal : 10001 → m(x) = 1.x^0+0. +0. x^2+0. x^3+1. x^4 = 1+x^4.....(6)

b. Nilai generator polinomial yang tetap untuk BCH (15,5).
g(x) = 1+𝑥 +𝑥2+𝑥4+𝑥5+𝑥8+𝑥10.....(7)
c. Perkalian antara x^{n-k} dan m(x).
$x^{n-k} = x^{15-10} = x^{10}$.....(8)
d. Pembagian antara xn-k.m(x) terhadap g(x). Didapatkan hasil pembagian v(x) dan sisa pembagian h(x).
e. Didapatkan codeword
c(x) = h(x) + x^{n-k} dan m(x).....(9)
Codeword tersebut diubah kembali kedalam bit-bit biner, sehingga hasil keluaran berupa matriks 15 kolom denganjumlah baris yang sama. Bit-bit inlah yang kemudian akan disisipkan

***Decoding* BCH**

Message yang didapat dari hasih ekstraksi steganografi yang berupa bit-bit terlebih dahulu diubah kedalam sebuah matriks 15 kolom. Parameter yang akan digunakan adalah m=4, k=5, n=15, dant=3.

Masing masing kolom diproses sebagai berikut :

a. Didapatkan r(x) disisi penerima.
b. Hitung sindrom S = (S1,S2,…,S6) dari polinomial terimaan r(x).
c. Tentukan *error location* polynomial σ(x) dari komponen sindrom S1,S2,…,S2t menggunakan algoritma *Berlekamp-Massey*.

μ	$\sigma^{(\mu)}$**(X)**	d_μ	l_μ	**μ-**l_μ
-1	1	1	0	-1
0	1	S1	0	0
1	1+ S1X			
2				
3				
...				
6				

Tabel 1 *Proses Iterasi algoritma Berlekamp-Massey*

$d_{\mu+1} = d_{\mu+2} + x^{(\mu+1)} d_{\mu+1} + \cdots + x_{\mu+1}^{(\mu+1)} d_{\mu+2-l\ \mu}$.....(10)
Jika d_μ=0, maka :
$\sigma^{(\mu+1)}(X)=\sigma^{(\mu)}(X)$.....(11)
$x_{\mu+1} = x_\mu$.....(12)
Jika $d_\mu \neq 0$, maka :
$\sigma^{(\mu+1)}(X) = \sigma^{(\mu)} d_\mu + d_\mu d_\rho^{-1} x^{(\mu-\rho)} \sigma^{(\rho)}(x$ .....(13)
$x_{\mu+1} = \max(x_\mu, x_\rho + \mu + \rho)$.....(14)

d. Tentukan error location numbers β1,β2,…βv dengan mencari akar-akar σ(x).
e. Perbaiki error dengan mengganti bit 0 menjadi bit 1, atau sebaliknya.

Kembalikan ke ukuran matriks semula, dengan membuang bit 0 tambahan pada BCH *encoding*. Hasil keluaran diubah menjadi matriks sesuai panjang dan lebar *message image*.

E. Parameter Pengujian

1. *Peak Signal-to-Noise Ratio* (PSNR)

PSNR merupakan nilai perbandingan antara harga maksimum dari intensitas citra terhadap *error* citra yaitu MSE. Untuk menghitung nilai PSNR digunakan persamaan 1 berikut [6]:

$$PSNR = 20 \log_{10} \frac{Ps}{\sqrt{MSE}} \quad \text{.....(15)}$$

Dimana, Ps = Daya Sinyal
MSE = Nilai Rata-rata Kuadrat *Error*

2. *Mean Square Eror* (MSE)

Mean Square Error (MSE) adalah rata-rata nilai error antara citra *cover* dengan citra stego. Secara matematis, *Mean Square Error* (MSE) dapat dirumuskan pada persamaan 2 sebagai beriku [6]t:

$$MSE = \frac{1}{N}\sum_{i=1}^{N}[I(i) - I'(i)]^2 \quad \text{.....(16)}$$

Dimana, I(i) = data *host*, I'(i) = data stego, N = panjang data

3. *Bit Error Rate* (BER)

Jumlah bit yang salah dihitung dengan cara membandingkan setiap *file* citra sisipan asli dengan citra sisipan hasil ekstraksi. Persamaan *Bit Error Rate* tersebut dapat dihitung sebagai persamaan 4 berikut [6]:

$$BER = \frac{\Sigma \text{Bit Salah}}{\Sigma \text{Bit Total}} \quad \text{.....(17)}$$

4. Waktu Komputasi

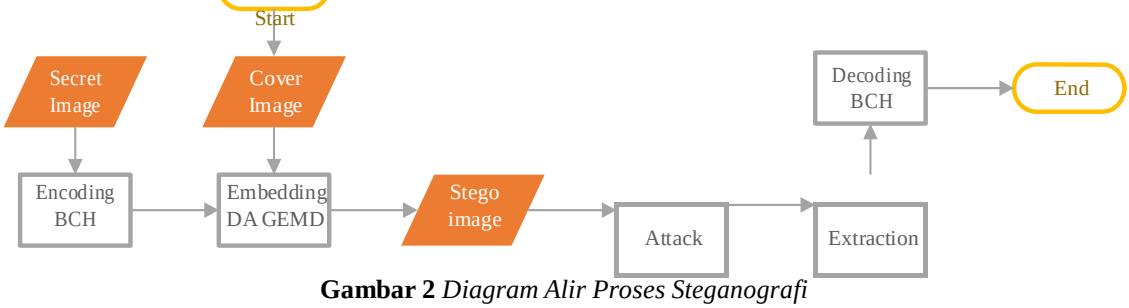
Waktu komputasi adalah waktu yang dibutuhkan sistem untuk melakukan suatu proses. Pada sistem ini, waktu komputasi dihitung dimulai pada proses penyisipan dan proses ekstraksi dari pertama sampai selesai.

5. Bitplane Attack

Salah satu keunggulan dari metode DA GEMD adalah ketahanan terhadap serangan bitplane attack. Bitplane attack adalah cara yang paling sederhana untuk menganalisis sebuah stego image dengan mengambil hanya n-bit paling belakang dari setiap piksel citra stego. Dengan n adalah banyaknya bit plaing belakang yang akan diambil.

3. Perancangan Sistem

Dalam tugas akhir ini dirancang suatu sistem yang dapat menjalankan proses steganografi dengan menggunakan metode Division Arithmatic and Generalized Esploiting Modification Direction yang juga menggunakan coding BCH, proses yang akan dilakukan dapat dilihat pada gambar 1. di bawah ini.



Gambar 2 *Diagram Alir Proses Steganografi*

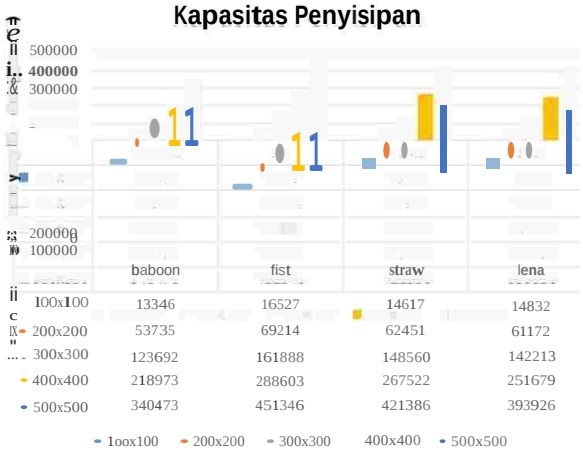
Sistem secara umum dapat dijelaskan sebagai berikut:

a. *Cover Image* merupakan citra rgb dengan ukuran 100 x 100 sampai 500 x 500 dan *embedded image* harus berupa citra biner dengan format *.bmp* dengan bermacam ukuran.
b. Pada *embedded image* akan terlebih dahulu dilakukan coding BCH sehingga membuat keluaran pesan rahasia menjadi sedikit lebih besar
c. Pesan yang telah di encoding dengan coding BCH lalu masuk kedalam proses steganography dengan metode *Division Arithmatic and Generelized Exploiting Direction*.
d. Cover image yang telah disisipi oleh embedding image bernama stego image yang merupakan gambar hasil penyisipan steganografi yang selanjutnya akan dikirimkan ke penerima dan dilakukan proses ekstraksi.
e. Gambar stego image yang diterima lalu akan dilakuan attack atau penyerangan untuk melihat seberapa kuat stego image tersebut terhadap serangan serangan yang dilancarkan terhadapnya.
f. Setelah penerima menerima stego image lalu akan dilakukan proses ekstraksi terhadap *stego image* tersebut menggunakan ekstraksi dengan metode *Division Arithmatic and Generelized Exploiting Direction.*
g. Embedding image yang telah diekstraksi lalu di decode BCH untuk mengkoreksi kesalahan yang terdapat dalam image yang diterima .

4. Hasil Pengujian

A. Kapasitas penyisipan

Berikut gambar 3 yang menunjukan kapasitas yang didapat dari empat buah citra yang berbeda namun dengan ukuran yang sama.

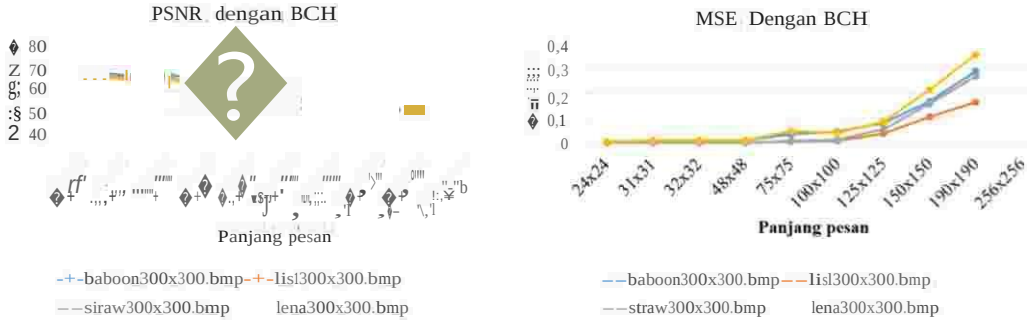


Gambar 3. *Grafik Pengaruh Sumber Data Terhadap Akurasi Sistem*

Dari gambar 3 diatas bisa kita lihat bahwa panjang pesan yang bisa disisipkan berbanding lurus dengan besarnya ukuran citra cover. Semakin besar ukuran citra cover maka semakin besar pula pesan yang dapat disisipkan. Hal ini berlaku untuk keempat citra cover yang digunakan. Namun sesuai yang bisa dilihat pada gambar 3 setiap citra cover memiliki kapasitas yang berbeda beda meskipun dengan ukuran yang sama.

B. Pengaruh Panjang Pesan Terhadap Nilai SNR dan MSE

Panjangnya pesan yang akan disisipkan sangat berpengaruh terhadap stego image yang dihasilkan. Semakin panjang atau dalam hal ini semakin besar ukuran gambar pesan yang akan disispkan maka makin banyak pula bit yang harus disisipkan pada cover image. Artinya makin banyak pula bit-bit dalam cover image yang dirusak atau diganti. Hal tersebut tentu akan sangat berpengaruh pada nilai PSNR dan MSE. Ukuran pesan yang akan digunakan beragam mulai dari 24 x 24 sampai pesan berukuran 256 x 256 piksel



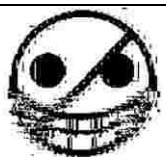
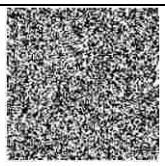
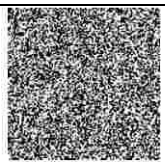
Gambar 4. *Pengaruh panjang pesan*

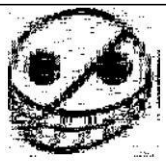
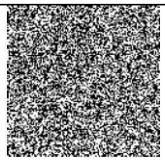
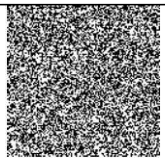
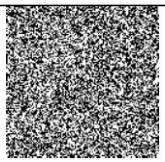
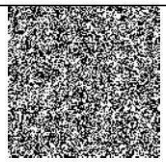
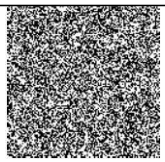
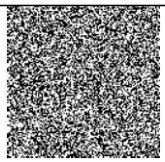
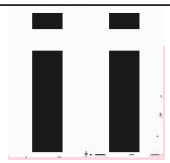
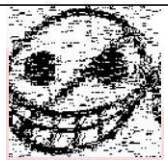
Dari gambar 4 di atas dapat dilihat bahwa semakin besar panjang pesan yang disisipkan maka nilai PSNR nya akan semakin menurun atau berbanding terbalik. Nilai tersebut masih menunjukannilai yang berada pada nilai standaryang ditentukan oleh International Federation of the Phonographic Industry (IFPI) yaitu diatas 20 dB. MSE yang dihasilkan terlihat semakin menaik atau semakin besar nilainya berbanding lurus dengan panjangnya pesan yang disisipkan.

C. Pengaruh *noise* dan manupulasi

data citra yang telah tersisipi diuji dengan menggunakan serangan berupa penambahan serangan noisegaussian dan salt and pepper dengan nilai density yang berbeda-beda. Data yang diujikan disisipkan dengan pesan sesuai pada gambar 5 dengan ukuran 125x125. Kemudian setelah diberi serangan, hasil pesan yang terekstrak dapat dilihat pada tabel 2.

Gambar 5. *Pesan rahasia*

Serangan	**Pesan Terekstraksi Tanpa BCH**	**Pesan Terekstraksi Dengan BCH**	**Serangan**	**Pesan Terekstraksi Tanpa BCH**	**Pesan Terekstraksi Dengan BCH**
Salt and Pepper 0.0001			*Gaussian* 0.000001		
Salt and Pepper 0.001			*Compressing*		

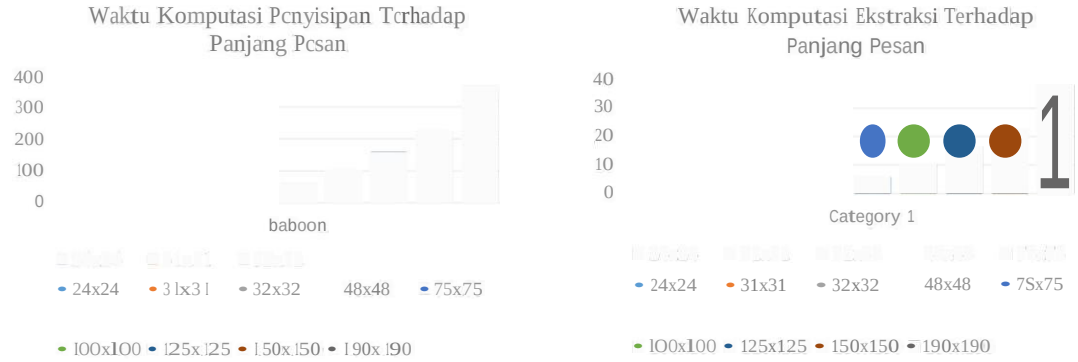
Salt and Pepper 0.01			*Resizing*		
Gaussian 0.0001			*Crop*		
Gaussian 0.00001					

Tabel 2. *Hasil ekstraksi terhadap serangan*

Dapat dilihat dari tabel 4.3 diatas bahwa sistem hanya kuat pada serangan Salt and Pepper dan Gaussian saja,itu pun pada nilai density yang cukup kecilsedangkan dengan serangan lain pesan yang dibaca menjadi error. Hal ini disebabkan oleh terlalu banyaknya bit yang salah pembacaan. Pada serangan dengan jenis manipulasi sistem tidak dapat bertahan pada parameter berapapun baik pada serangan compressing, resizing, ataupun cropping. Compressing akan mengalani error karena perubahan yang terjadi hampir di seluruh bit citra sehingga proses ekstraksi nya pun akan jadi rusak.

D. Waktu Komputasi

Data cover image disisipkan pesan dengan panjang pesan yang berbeda sesuai dengan yang terlampir. Kemudian dihitung waktu ketika proses penyisipan dan ketika proses ekstraksi. Dan gambar 6(a) merupakan grafik waktu komputasi untuk proses penyisipan, sedangkan gambar 6(b) merupakan grafik waktu komputasi untuk proses ekstraksi.

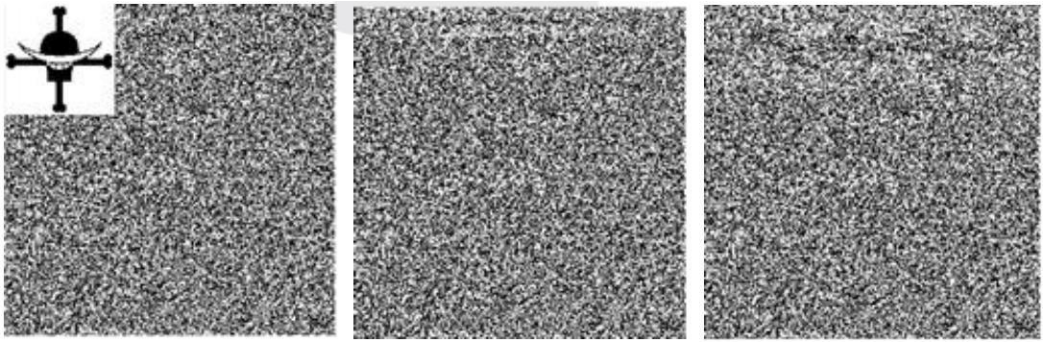


(a) (b)

Gambar 6. Waktu Komputasi (a) Penyisipan dan (b) Ekstraksi

E. *Bitplane Attack*

Pesan rahasia dengan ukuran 100x100 disisipkan pada citra ‘baboon’ dengan ukuran 300x300 piksel dengan tiga metode yaitu 2-LSB, DA GEMD, dan sistem yang digunakan yaitu DA GEMD dengan pengkodean BCH. Setelah itu akan dilakukan percobaan bitplane attack pada ketiga metode ini. Hasil dari serangan bitlpane attack bisa dilihat pada gambar 7 berikut



Gambar 7. *Serangan bitplane attack*

Seperti bisa dilihat pada gambar 7 diatas, dengan gambar (a) merupakan gambar hasil bitplane attack dari stego image metode LSB sementara (b) hasil dari metode DA GEMD dan (c) hasil dari metode DA GEMD dengan pengkodean BCH. Bila penyisipan hanya dengan menggunaka metode LSB saja akan sangat mudah pesan yang tersembunyi dapat diambil oleh orang yang tidak bertanggung jawab karna bisa dikenali melalui pola yang teratur pada bit terakhir sebuah stego image. Sementara karena metode DA GEMD menggunakan metode penggabungan GEMD dan 2-LSB maka tanpa menghilangkan manfaat dari metode GEMD. Jadi sistem dapat memanfaatkan kelebihan dari metode 2-LSB untuk menambah kapasitas penyisipan juga tahan terhadap serangan bitplane attack.

5. Kesimpulan

Kesimpulan yang dapat diambil dari tahapan perancangan dimulai dengan kapasitas dari tiga buah citra cover dengan ukuran 300x300 piksel dan mendapatkan nilai banyak bit yang bisa disisipkan dalam citra cover dengan nilai 1,37435 untuk citra cover ‘baboon’, 1,79875 untuk citra cover ‘fist’, 1,65066 untuk citra cover ‘straw’, dan 1,58014 untuk citra cover ‘lena’. Sistem bekerja dengan cukup baik dengan nilai PSNR terendah sebesar 50,38509 dengan nilai MSE terbesar sebesar 0,35342 pada penyisipan pesan 190x190 piksel dengan ukuran cover 300x300 piksel. Panjang pesan berpengaruh terhadap nilai PSNR dan MSE. Semakin panjang pesan, maka semakin kecil nilai PSNR. Sedangkan, untuk nilai MSE, semakin panjang pesan, maka semakin besar pula nilai MSE yang diperoleh. 4. Nilai BER maksimum pada pemberian serangan pada skema 1 dengan serangan ‘salt & pepper’ adalah BER 0,427615 pada density 0,01 dan serangan ‘gaussian’ adalah 0,5130 pada varian 0,00001. Sedangkan pada skema 2 dengan serangan ‘salt & pepper’ adalah BER 0,427615 pada density 0,01 dan serangan ‘gaussian’ adalah 0,59939 pada varian 0,00001. 5. Sistem tidak dapat bertahan dengan manipulasi cropping resize dan compressing. sistem dapat memanfaatkan kelebihan dari metode 2-LSB untuk menambah kapasitas penyisipan juga tahan terhadap serangan bitplane attack. Waktu komputasi terbesar diperoleh pada penyisipan pesan 190x190 pada cover image 300x300 dengan waktu penyisipan 365,1651 dan waktu ekstraksi 37,97552 detik.

REFERENSI

[1] X. Zhang, and S. Wang, Effcient steganographic embedding by exploiting modification direction,Journal of IEEE Communications Letters, vol. 10, no. 11, pp. 781-783, 2006.

[2] W. C. Kuo, High-capacitySteganographic Method based on Division Arithmetic and Generalized Exploiting Modication Direction, Department of Computer Science and Information Engineering, National Yunlin University of Science & Technology.

[3] Munir, Rinaldi.2004 Steganografi dan Watermarking. Bandung. Intitut Teknologi Bandung

[4] Morkel, T., JHP. Eloff, dan MS. Oliver. An Overview of Image Steganography. Pretoria. Information and Computer Security Architechture (ICSA) Research Group, Departement of Computer Science, University of Pretoria.

[5] Calvianty, Intan Yusantina. 2009. Multiple Watermarking pada citra medis pada domain wavelett menggunakan BCH Encoding. Bandung: Institut Teknologi Telkom

[6] Gayathri, C.,Kalpana, V. Study on Image Steganography Technique’ . Tamilnadu. Computer Science Engineering, School of Computing, SASTRAUNIVERSITY.

[7] W. C. Kuo, Data hiding based on generalised exploiting modification direction method, Department of Computer Science and Information Engineering, National Yunlin University of Science & Technology.

[9] S. Lin, An Introduction to Error Correcting Codes, Prentice-Hall, Inc: New Jersey, 1970.

[10] J. C. Moreira dan P. G. Farrel, Essentials of Error Control Coding, England: John Wiley and Sons, Ltd, 2006.

[11] Purnomo, M. H., & Muntasa, A. 2010. "Konsep Pengolahan Citra Digital dan Ekstraksi Fitur". Surabaya: Graha Ilmu.