IMPLEMENTASI SKEMA STEGANOGRAFI DENGAN METODE *SELECT LEAST SIGNIFICANT BITS* (SLSB) PADA PESAN TERENKRIPSI UNTUK PENGIRIMAN MMS

E. Haodudin Nurkifli[1)], **Edi Winarko**[2)]
[1)]Jurusan Teknik Informatika Politri "Tala" Kalimantan Selatan
Jalan A Syairani, Pelaihari, Kalimantan Selatan
[2)] Program Studi Monodisiplin S2/S3 Ilmu Komputer UGM
Gedung SIC, Lantai 3 Sekip Utara Yogyakarta Telp (0274)-555133
Yogyakartae-mail : [1)] it.freshndin@gmail.com, [2)]ewinarko@gmail.com

Abstrak

Penelitian ini membahas steganografi dengan skema Select Least Significant Bits (SLSB), pesan teks yang akan disisipkan berupa pesan asli, pesan terkompresi, pesan terenkripsi, pesan terkompresi dan terenkripsi. Algoritma enkripsi menggunakan algoritma Elgamal Elliptic Cruve Cryptography (Elgamal ECC) dan algoritma kompresi menggunakan algoritma Huffman Code. Proses-proses yang ada pada sistem: proses penyisipan satu bit perpixel, dua bit perpixel dan tiga bit perpixel.

Pengujian kebutuhan bit pesan asli 150 karakter ≈ 200 bit, penghematan bit setelah dilakukan kompresi mencapai 50.8%, penambahan bit setelah dilakukan enkripsi rata-rata mengalami penambahan lima kali lipat dari pesan asli, pesan terkompresi dan terenkripsi mengalami reduksi penghematan bit mencapai 55.32 %, kebutuhan bit dari Tree pembentuk Huffman Code rata-rata 12464 bit .

Pengujian untuk mengetahui kehandalan gambar steganografi: Analisis histogram, RS Analisis, dan pengujian kualitas citra. Pengujian dengan histogram tidak mampu mendeteksi gambar steganografi, pengujian pada gambar bertipe bitmap seluruh histogram dari gambar hasil steganografi tidak jauh berbeda dengan histogram gambar asli. Pengujian juga dilakukan dengan menggunakan RS Analisis untuk mengetahui prosesntase nilai estimasi pendeteksian pesan yang disisipkan pada gambar. Hasil pengujian dengan RS Analisis, gambar steganografi dengan gambar asli memiliki nilai estimasi yang tidak jauh berbeda.

Pengujian yang terakhir menggunakan pengujian kualitas citra secara obyektif berdasarkan batas error pada citra. Parameter pengujian kualitas citra: Mean Sequare Error (MSE), Peak Signal to Noise Ratio (PSNR in dB), Normalized Cross-Correlation (NCC), Average Difference (AD), Structural Content (SC), Maximum Difference (MD), Normalized Absolute Error (NAE). Pengujian kualitas citra menunjukkan semua gambar steganografi memiliki nilai batas error yang tidak jauh berbeda dengan nilai batas error dari gambar asli.

Kata Kunci**:** *Selected Least Significant Bits (SLSB), Huffman Code, Elgamal ECC, Pengujian steganografi*

1. PENDAHULUAN

Multimedia Message Service (MMS) merupakan suatu layanan yang diberikan oleh telepon seluler kepada penggunanya untuk melakukan komunikasi melalui pengiriman pesan singkat yang berisi teks dan multimedia. MMS sangat populer, selain dikarenakan biayanya yang murah, pesan yang dikirimkan dapat diterima oleh penerima dengan baik dan cepat. Komunikasi melalui media MMS bukanlah komunikasi *point-to-point*, akan tetapi pesan yang dikirimkan melalui media MMS tidak langsung sampai pada tujuan, melainkan terlebih dulu ke server pada jaringan MMS kemudian baru disampaikan pada penerima pesan. Pada jaringan MMS tersebut, keamanan pesan sangatlah terancam untuk dibaca oleh orang lain. Perlu sebuah pengamanan agar isi pesan yang dikirimkan melalui media MMS tetap terjaga dan hanya dapat dibaca oleh orang yang berhak membacanya. Solusi yang ditawarkan adalah pengamanan pesan pada MMS dengan Steganografi.

Jagdale dkk. (2010) menyatakan bahwa perangkat *handphone* memiliki memori dan daya proses yang kecil maka dari itu perlu algoritma yang tepat untuk diterapkan dalam perangkat *handphone*. José dan Maria (2010) menyatakan bahwa steganografi menggunakan metode *Select Least Significant Bits* (SLSB) bekerja pada domain spasial, steganografi yang bekerja pada domain spasial lebih sederhana dan lebih cepat dibandingkan dengan steganografi yang bekerja pada domain frekuensi. Jagdale dkk (2010) juga menyatakan bahwa *Elliptic curve Cryptography* (ECC) muncul sebagai kriptografi kunci publik pada lingkungan *mobile device*. Dibandingkan dengan kriptografi seperti *Rivest Shamir Adleman (*RSA), *Diffie Hellman* (DH), ECC menawarkan keamanan yang setara dengan ukuran kunci lebih kecil dan perhitungan lebih cepat.

Penelitian ini mengembangkan sistem yang mengkombinasikan keunggulan kriptografi dan keunggulan steganografi, kriptografi digunakan agar pesan tidak dapat dibaca dan staganografi digunakan agar pesan tidak dapat diketahui keberadaanya. Ide dasar penelitian ini, menyisipkan pesan pada media gambar sebelum pesan disispkan dilakukan kompresi atau enksripsi. Kompresi pesan dilakukan untuk mengantisipasi pembengkakan pada ukuran pesan. Kompresi dilakukan juga bertujuan untuk mengantisipasi pada serangan steganalisis dengan

visual attack dan statistical attack, karena semakin kecil ukuran pesan yang disispkan akan semkain mengurangi steganalisis mendeteksi keberadaan pesan Anneria (2008). Algoritma yang digunakan adalah *Select Least Significant Bits* (SLSB) untuk menyisipkan pesan pada media gambar, *Huffman code* untuk kompresi dan dekompresi pesan, *Elgamal Elliptic Curve Cryptography* untuk enkripsi dan dekripsi.

Pengujian dilakukan untuk mengetahui kehandalan gambar steganografi. Metode pengujian: Analisis histogram, Steganalisis dengan RS Analisis, pengujian kualitas citra secara obyektif dengan *Mean Sequare Error (MSE), Peak Signal to Noise Ratio (PSNR in dB), Normalized Cross-Correlation (NCC), Average Difference (AD), Structural Content (SC), Maximum Difference (MD), Normalized Absolute Error (NAE).*

2. TINJAUAN PUSTAKA

Menurut Morkel dkk. (2005), steganografi adalah ilmu dan seni menyembunyikan keberadaan komunikasi. Menggunakan steganografi, pesan rahasia dapat disisipkan ke dalam sebuah media yang tidak mencurigakan dan mengirimnya tanpa ada seorangpun yang mengetahui keberadaan pesan tersebut. Jose dan Maria (2010) menyatakan bahwa SLSB merupakan penyempurnaan dari proses metode LSB. Metode SLSB ini melakukan teknik penyisipan tidak pada semua bit akhir tetapi menyisipkan pada beberapa bit pada satu warna dasar yang dominan. Penyisipan bit-bit pada warna dasar dominan bertujuan untuk dapat menjaga gambar agar tampak seperti yang asli dan tidak terjadi perubahan yang signifikan. Ada tiga proses penyisipan pesan, satu bit perpixel, dua bit perpixel dan tiga bit perpixel.

Menurut Salomon (2007), kompresi data ialah proses pengubahan sekumpulan data menjadi suatu bentuk kode untuk menghemat kebutuhan tempat penyimpanan dan waktu untuk transmisi data. Cormen dkk. (2003) menyatakan bahwa *Huffman code* digunakan secara luas dan sangat efektif untuk kompresi data. Bisa menghemat 20%-90% dari ukuran semula, tergantung tipe karakter yang dikompresi. Algoritma huffman menggunakan tabel yang menyimpan frekuensi kemunculan dari masing-masing karakter yang digunakan dalam pesan dan dikodekan dalam bentuk biner.

Menezes dkk. (1996) menyatakan bahwa kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Menurut Stinson (2003), skema enkripsi *ElGamal ECC* merupakan pengembangan dari algoritma enkripsi Elgamal yang diterapkan pada aritmetika kurva *elliptic*. Parameter-parameter domain kriptografi kurva *elliptic* adalah $T = (p, A, B, G , N_G , e)$, dengan persamaan kurva *elliptic* $y^2 = x^3 + Ax + B \pmod p$. Parameter-parameter tersebut perlu diketahui oleh setiap pengguna dalam suatu *cryptosystem* yang menggunakan algoritma *ElGamal ECC* sebagai dasar skema enkripsi. Proses-proses yang terjadi dalam enkripsi algoritma Egamal ECC adalah: mengambil parameter domain T {p, A, B, G, Ng, e} dan kunci public PB, inputkan plainteks, membuat plainteks menjadi numerik, merepresentasikan number dari plainteks menjadi titik, menentukan bilangan bilangan bulat interval 0-e-1, menghitung x dikali j atas mod p, menghitung akar sj dalam mod p, mengisi PM dengan xj dan akar, enkripsi pesan yang menghasilkan PC. Proses dekripsi elgamal dimulai dari membaca ciphertext PC, melakukan proses dekripsi pada PC dengan kunci privat V dan parameter domain T{p,A,e} agar menjadi PM yang masih berupa titik, merepresentasikan PM menjadi nilai numerik M dengan banyak percobaan e, nilai M dierubah menjadi sebuh pesan asli kembali.

Kharrazi dkk. (2006) menyatakan bahwa pengertian steganalisis merupakan seni dan ilmu pengetahuan dalam mendeteksi ada-tidaknya pesan tersembunyi dalam suatu objek. Menurut Fridrich dan Goljan (2002) beberapa metode yang dilakukan untuk mengetahui pesan yang tersembunyi dalam gambar: Analisis Histogram, RS Analisis, Sample Pairs Analisis dan pengujian citra secara obyektif. Jose dan Maria (2010) dalam penelitiannya menjadikan metode-metode yang dilakukan oleh Fridrich dan Glojan sebagai metode untuk menguji kehandalan dari steganografi yang dibuatnya.

Gonzalez dan Woods (2008) menyatakan bahwa histogram adalah grafik yang menunjukan frekuensi kemunculan setiap nilai gradasi warna. Bila digambar pada koordinat kartesian maka sumbu x (absis) menunjuakn tingkat warna dan sumbu y (ordinat) menunjukan frekuensi kemunculan. Penelitian ini menggunakan histogram sebagai salah satu alat uji untuk mengetahui tingkat kehandalan gambar steganografi yang dihasilkan dengan cara membandingkan histogram gambar asli dengan histogram gambar steganografi menyesuaikan dengan penelitian jose dan maria (2010).

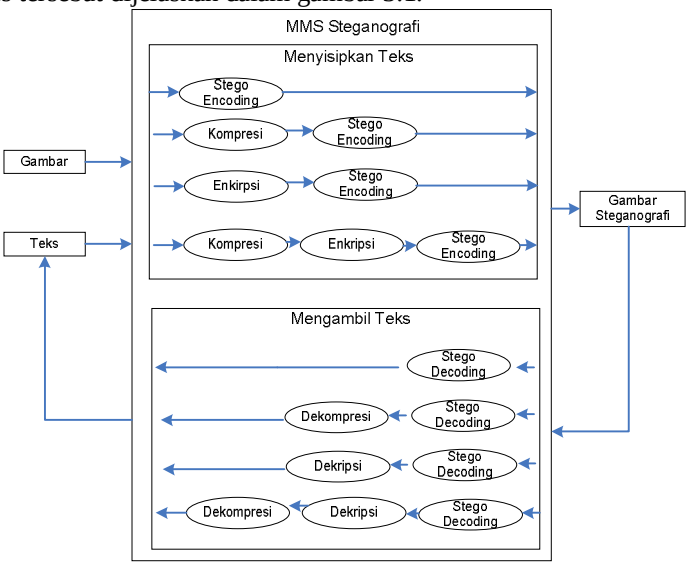
Menurut Fridrich dan Goljan (2005), RS Analisis merupakan teknik yang memanfaatkan korelasi spasial pada *stegoimage*. *RS-analysis* dapat mendeteksi penyisipan secara acak dengan akurat. Diberikan gambar yang kemudian dipartisi menjadi kelompok-kelompok *n pixel* yang bertetangga (*x1,...,xn*). Cara mendapatkan korelasi spasial, digunakan fungsi diskriminasi *f*, dimana *f* merupakan nilai absolut rata-rata dari perbedaan antara *pixel-pixel* yang bertetangga. Jika suatu kelompok semakin *noisy*, maka semakin besar nilai yang dihasilkan oleh fungsi *f*. Penyisipan steganografi meningkatkan *noisy* pada gambar, sehingga nilai yang dihasilkan oleh fungsi diskriminasi *f* akan meningkat.

Vora dkk. (2010) menjelaskan bahwa kriteria penilaian kualitas citra menggunakan kriteria Objektif yaitu yang didasarkan pada batas error yang diperbolehkan untuk citra yang diolah. Untuk citra asal x^ (m,n) dan citra yang telah disisipi pesan x(m,n) dengan ukuran yang sama M x N. parameter yang dijadikan sebagai kriteria

penilaian obyektif pada penelitian ini adalah: *Mean Square Error (MSE), Mean Average Error (MAE), Peak Signal to Noise Ratio (PSNR), Structural Content (SC), Maximum Difference (MD), Laplacian Mean Square Error (LMSE), Normalized Absolute Error (NAE).* Vora dkk (2010) juga menjelaskan pengukuran kualitas gambar dengan *Mean Square Error* (MSE). Jika nilai yang dihasilkan oleh MSE besar berarti gambar yang diuji berkualitas buruk. Nilai Rata-rata yang dihasilkan oleh *Mean Average Error* (MAE) besar berarti gambar yang diuji berkualitas buruk. Nilai yang dihasilkan oleh *Peak Signal to Noise Ratio* (PSNR) kecil berarti gambar yang diuji berkualitas buruk. Nilai yang dihasilkan oleh *Structural Content* (SC) besar berarti gambar yang diuji berkualitas buruk. Nilai yang dihasilkan *Maximum Difference* (MD) besar berarti gambar yang diuji memiliki kualitas yang buruk. Nilai yang dihasilkan *Normalized Cross-Correlation* (NCC) besar berarti gambar yang diuji memiliki kualitas yang buruk. Nilai yang dihasilkan oleh *Normalized Absolute Error* (NAE) besar berarti gambar yang diuji cobe memiliki kualitas buruk.

3. METODE PENELITIAN

Sistem yang dibangun merupakan sebuah sistem steganografi yang dapat menjadi alternatif untuk mengamankan pesan pada fasilitas *Multimedia Message Service* (MMS). Proses penyisipan pesan pada sistem: sisipkan pesan asli, sisipkan pesan terkompresi, sisipkan pesan terenkripsi, sisipkan pesan terkompresi dan terenkripsi, proses-proses tersebut dijelaskan dalam gambar 3.1.

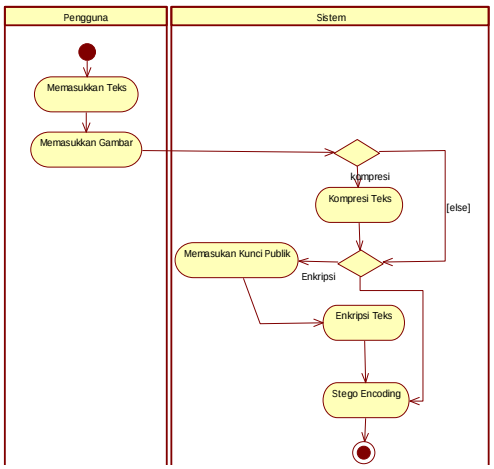


Gambar 3.1 Arsitektur Sistem.

Activity diagram dalam sistem terdapat dua activity yang menggambarkan alirian kejadian, pertama activity diagram untuk proses encode dan yang kedua activity untuk proses decode, dijelaskan pada gambar 3.2 dan 3.3.

a. *Activity diagram* steganografi proses *encoding*

Activity diagram steganografi dijelaskan pada gambar 3.2. *activity* diagram merupakan interaksi pengguna dengan sistem dan proses-proses yang dilakukan pengguna pada sistem.



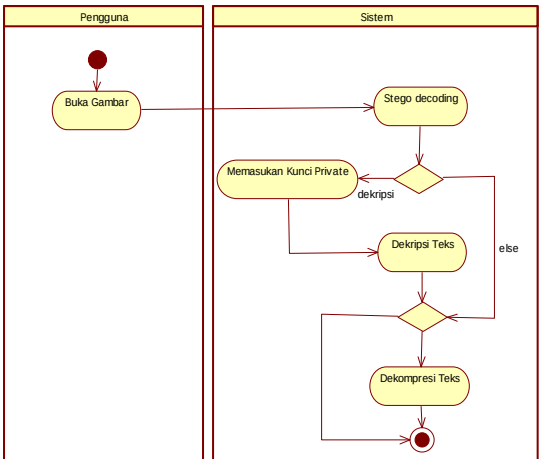
Gambar 3.2 *Activity Diagram* Steganografi SLSB *Encoding*

Proses dimulai pada saat pengguna memasukkan teks dan memasukkan gambar. Ada beberapa simbol keputusan di dalam a*ctivity diagram* ini artinya jika yang dipilih kompresi teks maka sistem melakukan kompresi

dan menyisipkan teks hasil kompresi pada media gambar (sistem melakukan proses *stego encoding*), dan jika yang dipilih enkripsi maka sistem melakukan enkripsi teks dan hasil enkripsi tersebut disisipkan pada media gambar (sistem melakukan *stego encoding*), sistem juga dapat melakukan proses kompresi, enkripsi dan *stego encoding*.

b. Activity diagram steganografi proses *decoding*

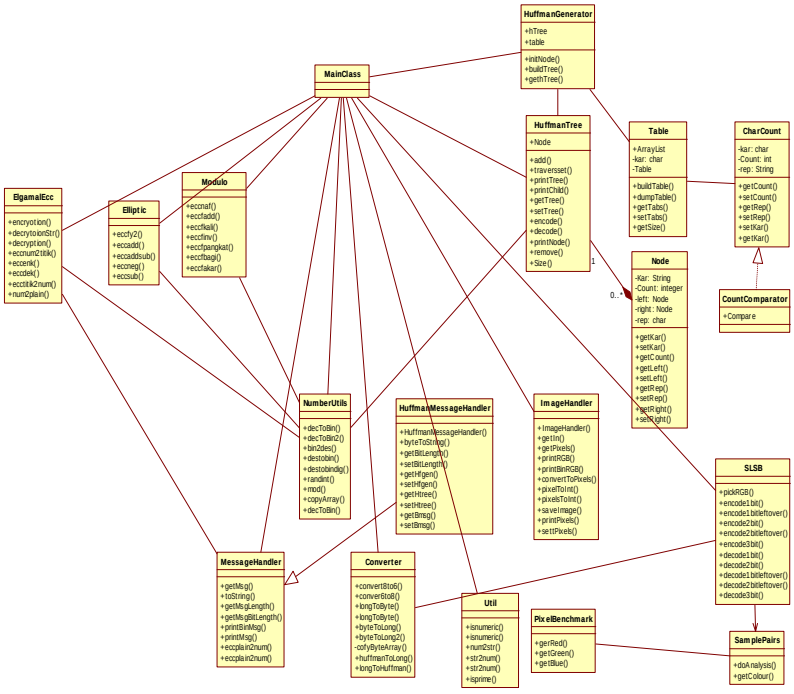
Actity diagram steganografi dijelaskan pada gambar 3.3 *Activity diagram* merupakan interaksi yang terjadi antara pengguna dengan sistem dan proses-proses yang dilakukan pengguna pada sistem.



Gambar 3.3. *Activity diagram* steganografi slsb *decoding*

Proses pada *activity diagram* dimulai dari: pengguna melakukan buka gambar, sistem dapat melakukan *stego decoding* dan dekompresi, sistem dapat melakukan *stego decoding*, deskripsi, dekompresi, bahkan sistem hanya melakukan proses *stego decoding* saja tergantung dari gambar steganografi yang akan dibuka teksnya.

Masing-masing *Class* tedapat pada Gambar 3.4. Pada Gambar tersebut menunjukkan *Class* apa saja yang ada pada sistem dan menunjukkan interaksi dari masing-masing *class* .



Gambar 3.4 *Class* diagram sistem steganografi

Gamba 3.4 menjelaskan masing-masing hubungan dari class, main class akan memeanggil class *ElgamalEcc*, *Elliptic*, Modulo, *HuffmanGenerator*, HuffmanTree, SLSB, Converter, *HuffmanMessageHandler*, *ImageHandler*, MessageHandler, NumberUtil, Util. kelas utama ini berisi proses inti. Class SLSB memanggil class Converter dan NumberUtils, Class SamplePairs memanggil Class PixelBenchmark, class ElgamalEcc memanggil class MessageHandler, NumberUtils. Class Elliptic memanggil class NumberUtils. Class Modulo memanggil Class Numberutils. HuffmanTree memanggil class NumberUtils.

4. HASIL DAN PEMBAHASAN

Pengujian dilakukan untuk mengetahui kebutuhan bit yang digunakan, dimulai dengan pesan asli, pesan terkompresi, pesan terenkripsi, pesan terkompresi terenkripsi, kebutuhan bit dari *Tree* pada *Huffman Code*. Hasil pengujian dijelaskan pada tabel 4.1 sampai 4.5.

Tabel 4.1 Kebutuhan bit pada pesan asli (Plainteks)

No	Banyak karakter	Banyak bit
1	200 karakter	1600 bit
2	150 karakter	1200 bit
3	100 karakter	800 bit
4	50 karakter	400 bit

Tabel 4.1 menjelaskan kebutuhan bit dari banyak karakter pesan asli, berdasarkan hasil pengujian masing-masing karakter membutuhkan banyak bit 1600, 1200, 800, 400, semakin banyak karakter maka kebutuhan bit semakin banyak pula.

Tabel 4.2 Kebutuhan bit pesan terkomptesi

No	Banyak karakter	Banyak bit sebelum kompresi	Banyak bit setelah kompresi
1	200 karakter	1600 bit	795 bit
2	150 karakter	1200 bit	604 bit
3	100 karakter	800 bit	384 bit
4	50 karakter	400 bit	195 bit

Penjelasan tabel 4.2 merupakan analisis kompresi pesan dari empat percobaan didapat nilai rata-rata penghematan bit setelah mengalami proses kompresi adalah 50.81%. Berikutnya pengujian untuk mengetahui hasil penggunaan bit pada proses enkripsi.

Tabel 4.3 Kebutuhan bit pesan terenkripsi

No	Banyak karakter	Banyak bit sebelum Enkripsi	Banyak bit setelah Enkripsi
1	200 karakter	1600 bit	8448 bit
2	150 karakter	1200 bit	6400 bit
3	100 karakter	800 bit	4352 bit
4	50 karakter	400 bit	2176 bit

Penjelasan dari tabel 4.3 pembengkakan hasil enkripsi pesan bersifat tidak tetap dan sangat signifikan dikarenakan panjang kunci 32 bit relatif panjang. Berdasarkan empat pengujian didapat hasil rata-rata pembengkakan bit setelah mengalami enkripsi adalah 537.325%, pembengkakan bit sampai lima kali lipat dari pesan asli.

Tabel 4.4 Kebutuhan bit pesan terkompresi dan terenkripsi

No	Banyak karakter	Banyak bit setelah Enkripsi	Banyak bit setelah Kompresi dan Enkripsi
1	200 karakter	8448 bit	4224 bit
2	150 karakter	6400 bit	2400 bit
3	100 karakter	4352 bit	1920 bit
4	50 karakter	2176 bit	1024 bit

Penjelasan tabel 4.4 hasil analisis terhadap pengurangan pembengkakan dengan proses kompresi dan enkripsi. Berdasarkan empat pengujian didapat hasil pembengkakan bit yang dapat direduksi dengan menggunakan kompresi. Tingkat penyusutan bit mencapai 55.32 %. Berikutnya pengujian banyaknya bit pada *Tree* dari *Huffman Code*.

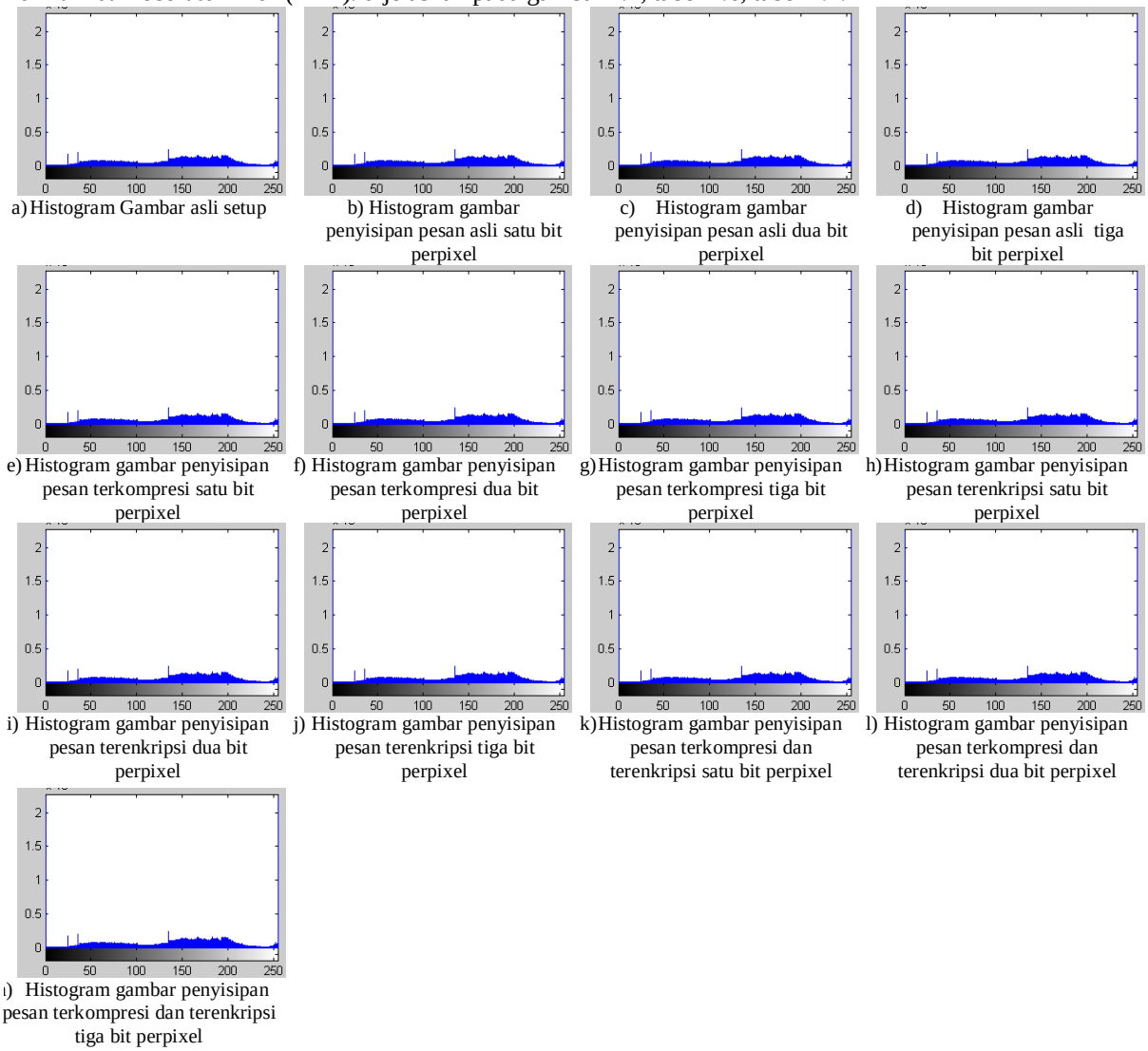
Tabel 4.5 Banyak bit dari *Tree* pada *Huffman Code*

No	Banyak karakter	Banyak bit dari *Tree* pada *Huffman Code*
1	150 karakter	11792 bit
2	150 karakter	13840 bit
3	150 karakter	11376 bit
4	150 karakter	12768 bit
5	150 karakter	12544 bit
6	150 karakter	14208 bit
7	150 karakter	10720 bit

Penjelasan tabel 4.5 hasil analisis terhadap banyak bit yang digunakan pada *Tree* dari *Huffman Code*. Berdasarkan tujuh pengujian didapat hasil kebutuhan bit dari 150 karakter dengan kalimat yang berbeda memiliki nilai rata-rata 12464 bit.

Pengujian untuk mengetahui kehandalan gambar steganografi dari penelitian ini, pengujian kehandalan:: Histogram Analisis, Steganalisis dengan metode RS Analisis, Pengujian kualitas citra secara obyektif dengan tujuh parameter pengujian: *Mean Sequare Error (MSE), Peak Signal to Noise Ratio (PSNR in dB), Normalized*

Cross-Correlation (NCC), Average Difference (AD), Structural Content (SC), Maximum Difference (MD), Normalized Absolute Error (NAE). dijelaskan pada gambar 4.1, tabel 4.6, tabel 4.7.



a) Histogram Gambar asli setup
b) Histogram gambar penyisipan pesan asli satu bit perpixel
c) Histogram gambar penyisipan pesan asli dua bit perpixel
d) Histogram gambar penyisipan pesan asli tiga bit perpixel
e) Histogram gambar penyisipan pesan terkompresi satu bit perpixel
f) Histogram gambar penyisipan pesan terkompresi dua bit perpixel
g) Histogram gambar penyisipan pesan terkompresi tiga bit perpixel
h) Histogram gambar penyisipan pesan terenkripsi satu bit perpixel
i) Histogram gambar penyisipan pesan terenkripsi dua bit perpixel
j) Histogram gambar penyisipan pesan terenkripsi tiga bit perpixel
k) Histogram gambar penyisipan pesan terkompresi dan terenkripsi satu bit perpixel
l) Histogram gambar penyisipan pesan terkompresi dan terenkripsi dua bit perpixel
ı) Histogram gambar penyisipan pesan terkompresi dan terenkripsi tiga bit perpixel

Gambar 4.1 Perbandingan histogram

Gambar 4.1 menjelaskan hasil perbandingan histogram yang sukar untuk dibedakan. histogram gambar steganografi penyisipan pesan asli 1200 bit, pesan terkompresi 604 bit ditambah dengan Tree 10702, pesan terenkripsi 6400 bit, pesan terkompresi, terenkripsi 2400 bit ditambah dengan Tree 10720 bit pada gambar tidak mempengaruhi perubahan secara signifikan pada histogram dari gambar.

Tabel 4.6 Nilai estimasi pendeteksian pesan tersembunyi pada gambar setup

NO	Keluaran dari MMS Stego	RS Analisis		
		Red	***Green***	***Blue***
1	Gambar Asli	4.9447	3.92092	3.18177
2	Penyisipan pesan asli satu bit perpixel	4.97406	3.92092	3.18894
3	Penyisipan pesan asli dua bit perpixel	4.6029	3.92092	3.18615
4	Penyisipan pesan asli tiga bit perpixel	4.94863	3.92092	3.18893
5	Penyisipan pesan terkompresi satu bit perpixel	4.92481	3.92092	3.80154
6	Penyisipan pesan terkompresi dua bit perpixel	4.9401	3.92092	3.80154
7	Penyisipan pesan terkompresi tiga bit perpixel	4.90957	3.92092	3.80154
8	Penyisipan pesan terenkripsi satu bit perpixel	6.55588	3.92092	3.18896
9	Penyisipan pesan terenkripsi dua bit perpixel	4.97915	3.92092	3.18617
10	Penyisipan pesan terenkripsi tiga bit perpixel	4.5686	3.92092	3.18896

11	Penyisipan pesan terkompresi dan terenkripsi satu bit perpixel	6.29026	3.92092	3.81569
12	Penyisipan pesan terkompresi dan terenkripsi dua bit perpixel	4.81443	3.92092	3.81568
13	Penyisipan pesan terkompresi dan terenkripsi tiga bit perpixel	4.5096	3.92092	3.81568

Tabel 4.6 menjelaskan hasil pengujian menunjukkan perbandingan nilai deteksi pesan yang tidak terlalu jauh berbeda dibanding dengan nilai deteksi pesan tersembunyi pada gambar asli. Dua belas proses penyisipan memiliki hasil yang bagus pada pengujian RS Analisis dengan kata lain gambar steganografi yang dihasilkan sangat mendekati dengan gambar asli dan aman untuk dideteksi dengan steganlisis metode RS Analisis.

Tabel 4.7 Nilai batas error untuk citra steganografi dari gambar setup

No	Keluaran dari MMS Stego	*MSE*	*PSNR*	*NCC*	AD	*SC*	*MD*	*NAE*
1	Gambar Asli	0	99	1	0	1	0	0
2	Penyisipan pesan asli satu bit perpixel	0.0030	73.33	1	0.0030	1	1	0.000018
3	Penyisipan pesan asli dua bit perpixel	0.000916	78.51	1	0.000916	1	1	0.000005
4	Penyisipan pesan asli tiga bit perpixel	0.0019	75.33	1	-0.0016	1	0	0.0000095
5	Penyisipan pesan terkompresi satu bit perpixel	0.0219	64.73	0.99	0.0218	1.0003	1	0.000130
6	Penyisipan pesan terkompresi dua bit perpixel	0.0214	64.82	0.99	0.0214	1.0003	1	0.000127
7	Penyisipan pesan terkompresi tiga bit perpixel	0.0231	64.50	0.99	0.0203	1.0003	1	0.000134
8	Penyisipan pesan terenkripsi satu bit perpixel	0.0108	67.79	0.99	0.0101	1.0001	1	0.000064
9	Penyisipan pesan terenkripsi dua bit perpixel	0.0073	69.51	1	0.0063	1.0001	1	0.000043
10	Penyisipan pesan terenkripsi tiga bit perpixel	0.0219	64.73	0.99	0.0068	1.0001	3	0.000061
11	Penyisipan pesan terkompresi dan terenkripsi satu bit perpixel	0.0310	63.21	0.99	0.0304	1.0004	1	0.000184
12	Penyisipan pesan terkompresi dan terenkripsi dua bit perpixel	0.0274	63.76	0.99	0.0263	1.0004	1	0.000162
13	Penyisipan pesan terkompresi dan terenkripsi tiga bit perpixel	0.0396	62.15	0.99	0.0262	1.0004	3	0.000187

Tabel 4.7 Gambar hasil steganografi penyisipan pesan asli, pesan terkompresi, pesan terenkripsi, dan pesan terkompresi terenkripsi yang memiliki nilai batas error paling mendekati gambar asli diperlihatkan pada gambar steganografi penyisipan dua bit perpixel. Tabel 4.7 menjelaskan bahwa seluruh gambar steganografi memiliki nilai batas error yang tidak jauh berbeda dengan nilai batas error gambar asli.

5. KESIMPULAN

Berdasarkan implementasi dan pengujian yang dilakukan pada sistem steganografi, ada beberapa kesimpulan sebagai berikut:

a. Kebutuhan bit dari pesan yang dikompresi memiliki penghematan bit sampai 50.81 %.
b. Kebutuhan bit dari pesan yang dienkripsi memiliki pembengkakkan sebanyak lima kali lipat dari kebutuhan bit pesan asli.
c. Penambahan bit dari enkripsi pesan dapat direduksi dengan cara menggabungkan dengan kompresi, pesan dikompresi terlebih dahulu kemudian dienkripsi. Nilai reduksi dapat mencapai 55.32 %.
d. Banyaknya bit yang digunakan pada Tree pembentuk Huffman Code dengan 150 karakter menggunakan kalimat yang berbeda rata-rata 12464 bit.
e. Histogram tidak mampu membedakan secara jelas gambar steganografi dan gambar asli.
f. Nilai estimasi pendeteksian pesan tersembunyi secara keseluruhan untuk semua proses memiliki nilai estimasi yang tidak jauh berbeda dengan nilai estimasi gambar asli.
g. Nilai batas error untuk seluruh gambar steganografi memiliki nilai bagas error yang tidak jauh berbeda dengan nilai batas error gambar asli.
h. Proses penyisipan pesan asli pada gambar menunjukkan performa terbaik pada proses penyisipan dua bit perpixel.

i. Proses penyisipan pesan terkompresi dan penyisipan *tree* pada gambar menunjukkan performa terbaik pada proses penyisipan tiga bit perpixel.
j. Proses penyisipan pesan terenkirpsi pada gambar menunjukkan performa terbaik pada proses penyisipan tiga bit perpixel
k. Proses penyisipan pesan terkompresi dan terenkripsi serta penyisipan Tree pada gambar menunjukkan performa terbaik pada proses penyisipan tiga bit perpixel**.**

DAFTAR PUSTAKA

Anneria, Y.S, 2008, Program Stegonalis Metode LSB pada Citra dengan Enchanced LSB, Uji Chi-Squere, dan RS-Analysis, *Tugas Akhir*, Program Studi Teknik Informatika ITB, Bandung.

Cormen, T. H., Lesierson, C. E., Rivest, R. L., dan Stein, C., 2009, *Intordaction to Algorithms*, 3th edition ,The MIT Press, London.

Fridrich, J., dan Goljan, M., 2002, Practical Steganalysis of Digital Images – State of The Art, Department of Electrical Engineering, Binghamton.

Gonzalez, R. C., dan Woods, R. E., 2007, *Digital Image Processing*, 3rd edition, Pearson Prentice Hall, USA.

Jagdale, B. N., Bedi, R. K., dan Desai, S., 2010, *Securing MMS with High Performance Elliptic Curve Cryptography*, in International Jurnal of Computer Application, India.

José, J. R., dan Maria, J. M., 2010, *SLSB: Improving the Steganographic Algorithm LSB*, Spain.

Kharrazi, M., Secaner, H. S., dan Memon, N., 2006, *Improving Steganalysis by Fusion Technique: A Case Study with Image Steganography*, Polytechnic University Brooklyn, USA.

Menezes, J., van-Oorcshot, P. C., dan Vanstone, S. C., 1996, *Handbook of Applied Cryptography, CRC Press*, Inc. USA.

Morkel, T., Eloff, J. H. P., dan Olivier, M.S., 2005, *An Overview of Image Steganography*, ICSA Reaserch Group, Department Computer Sceince Pretoria, South Africa.

Stinson, D. R., 1995, *Cryptography Theory and Practice*, CRC Press, Inc, Florida

Vora, V. S., Suthar, A. C., Makwana, Y. N., dan Davda, S.J., 2010, Analysis of Compressed Image Quality Assessments, M.Tech Student in E &C Dept, CCET, Wadhwan-Gujarat.