PEMANFAATAN KOMPRESI HUFFMAN UNTUK OPTIMASI UKURAN GAMBAR PADA SISTEM *STEGANOGRAPHY* MENGGUNAKAN METODE *LEAST SIGNIFICANT BIT* (LSB)

Yaddarabullah[1], Nazori AZ[2]

Program Studi Magister Ilmu Komputer, Program Pascasarjana, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Uttara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5869225
[1]nongkrek@gmail.com, [2]nazori.agani@gmail.com

ABSTRAK

Internet saat ini telah menjadi bagian yang sangat penting bagi infrastruktur komunikasi di dunia. Pertukaran informasi melalui internet memiliki banyak kelebihan dibandingkan dengan media komunikasi lainnya, terutama dari segi kecepatannya. Namun informasi yang dikirimkan melalui internet tidak dapat dijamin keamanannya. Penyadapan terhadap informasi rahasia sering terjadi pada media komunikasi ini. Umumnya komunikasi melalui internet tidak aman. Salah satu teknik mengamankan data adalah dengan cara di sembunyikan ke dalam bentuk data yang berbeda, hal ini di kenal dengan sebutan sistem steganography. Permasalahan yang sering di hadapi dalam sistem steganography adalah hasil ukuran file yang di sisipkan data asli akan menjadi membesar. Untuk mengatasi masalah tersebut dapat di lakukan dengan memampatkan ukuran data yang akan di sisipkan, sehingga ukuran file asli dengan file stego tidak memiliki perbedaan yang signifikan. Metode yang di gunakan untuk pemampatan adalah teknik kompresi huffman dan metode penyisipan menggunakan LSB (Least Significant Bit). Hasil eksperimen menunjukkan pengujian terhadap ukuran citra asli dengan citra stego sama, rata-rata waktu penyisipan adalah 61,8 ms, rata-rata waktu ekstrasi adalah 20,4 ms, nilai keakuratan ekstrasi teks adalah 99,95%, pengujian keamanan citra stego dengan metode Sample Pairs menujukkan rata-rata nilai 0,004, dengan metode RS Analysis rata-rata nilai 0,09, dengan metode Standar Fusion rata-rata nilai 0,1165.

Kata Kunci:*Steganography*, *Least Significant Bit*, Kompresi *Huffman*, *Steganalysis*, Optimasi *File Stego*

I. PENDAHULUAN

1.1. Latar Belakang

Teknologi informasi dewasa ini berkenbang dengan pesat sehingga proses pengiriman informasi dan pertukaran data sangat cepat. Data atau informasi yang di pertukarkan sebaiknya sampai ke tujuan dan hal ini memerlukan sebuah sistem untuk dapat menjamin data yang di pertukarkan adalah asli. Sistem keamanan dapat berfungsi sebagai sebuah cara untuk melindungi data yang di pertukarkan. Terdapat beberapa usaha untuk menangani masalah keamanan data rahasia yang dikirimkan melalui internet, diantaranya adalah menggunakan teknik kriptografi dan steganografi. *Steganography* adalah teknik menyembunyikan data rahasia ke dalam data lainnya sehingga perubahan yang terjadi tidak terlihat mencurigakan. Satu hal esensial yang menjadi kelebihan *steganography* adalah kemampuannya untuk menipu persepsi manusia, manusia tidak memiliki insting untuk mencurigai adanya arsip-arsip yang memiliki informasi yang tersembunyi di dalamnya, terutama bila arsip tersebut tampak seperti arsip normal lainnya. Teknik ini sering digunakan untuk menghindari kecurigaan orang dan menghindari keinginan orang untuk mengetahui isi pesan rahasia tersebut. Informasi asli dapat di sembunyikan ke dalam bentuk file yang berbeda dengan data asli seperti file citra, teks, video atau audio. Teknik *steganography* juga dapat di lengkapi dengan penyandian terhadap data yang di sembunyikan. Penyandian ini di lakukan untuk memastikan hak dari pengaksesan data tersebut. Hanya orang yang mengetahui sandi tersebut yang dapat mengekstrak data asli[1].

Saat ini telah di ketahui bahwa terdapat banyak metode yang di gunakan untuk mengimplementasikan sistem *steganography* yaitu dengan menggunakan teknik LSB (*Least Significant Bit*), *Redundat Pattern Encoding*, *Substitution*, *Transform Domain*, *Distortion* dan *Spread Spectrum Method*[2]. Namun begitu terbentuk pula suatu teknik yang dikenal dengan steganalysis, yaitu suatu teknik yang digunakan untuk mendeteksi penggunaan *steganography* pada suatu arsip. Seorang *steganalyst* tidak berusaha untuk melakukan dekripsi terhadap informasi yang tersembunyi dalam suatu arsip, yang dilakukan adalah berusaha untuk menemukannya. Terdapat beberapa cara yang dapat digunakan untuk mendeteksi *steganography* seperti melakukan pengamatan terhadap suatu arsip dan membandingkannya dengan salinan arsip yang dianggap belum direkayasa. Salah satu permasalahan yang sering di hadapi dalam sistem *steganography* adalah hasil ukuran file yang di sisipkan data asli akan menjadi membesar. Jika media yang di gunakan sebagai hasil dari *steganography* adalah file citra dan file citra tersebut berukuran besar namun memiliki resolusi yang kecil, ini akan menimbulkan kecurigaan orang terhadap penggunaan *steganography*.

Berdasarkan permasalahan tersebut maka di perlukan sebuah teknik untuk mengoptimasi hasil file yang telah di sisipkan data asli agar tidak menimbulkan kecurigaan terhadap stego file dan memaksimalkan ukuran file hasil *steganography*.

1.2. Identifikasi Masalah

Berdasarkan uraian yang terdapat pada latar belakang, maka permasalahan yang ditemukan dalam penelitian ini adalah sebagai berikut :

a. Bagaimanakah penerapan keamanan pada data dapat di lakukan yaitu dengan teknik penyisipan data ke dalam bentuk data yang lain.
b. Bagaimanakah optimasi di lakukan terhadap data yang di sisipkan ke dalam data yang lain untuk mencegah kecurigaan dari file yang telah di sisipkan data.

1.3. Batasan Masalah

Adapun batasan dalam ini adalah sebagai berikut :

a. Data yang dapat di sisipkan adalah data tekstual.
b. Media yang di pakai untuk penyisipan data adalah citra dijital.
c. Teknik yang di gunakan untuk penyisipan adalah menggunakan metode LSB *(Least Significant Bit)*.
d. Teknik yang di gunakan untuk optimasi ukuran file hasil penyisipan adalah dengan menggunakan teknik kompresi *huffman*.

1.4. Rumusan Masalah

Berdasarkan identifikasi masalah di atas, maka dapat di rumuskan permasalahan dalam ini adalah sebagai berikut :

a. Bagaimana mengimplementasikan teknik penyisipan data teks ke dalam citra dijital dengan menggunakan metode LSB (*Least Significant Bit*) dalam pengembangan aplikasi *steganography*.
b. Bagaimana optimasi dapat di lakukan sehingga ukuran citra dijital yang di hasilkan dari sistem *steganography* tidak terlalu besar dengan teknik kompresi *huffman*.

1.5. Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk menghasilkan sistem kemanan yang dapat menyisipkan data dokumen ke dalam citra dijital. Kualitas citra dijital yang telah di sisipkan data tidak mengalami perubahan signifikan dan ukuran nya tidak menjadi terlalu besar.

1.6. Manfaat Penelitian

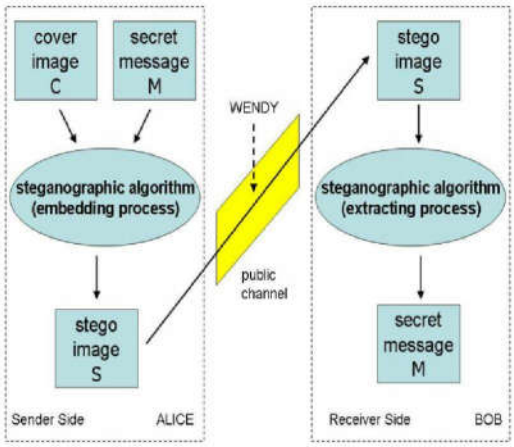
Manfaat yang di harapkan dari penelitian ini adalah dapat menjadi referensi untuk pengembangan sistem *steganography* ke dapannya dan menjadi bahan perbandingan untuk optimasi ukuran citra dijital hasil dari penyisipan data dengan teknik lainnya.

II. LANDASAN PEMIKRIAN

2.1. Tinjauan Pustaka

2.1.1. *Steganography*

Kata steganografi berasal dari bahasa Yunani *steganos* (*στεγανός*) yang berarti "ditutupi atau dilindungi", dan graphein (*γράνειν*) yang berarti "menulis". Dari asal katanya steganografi berarti "tulisan tersembunyi". Steganografi adalah seni dan ilmu menulis informasi tersembunyi sedemikian rupa sehingga tak seorang pun, selain pengirim dan penerima yang dituju, mengetahui keberadaan informasi tersebut. Secara umum, informasi akan muncul dalam bentuk yang lain: foto, artikel, daftar belanja, atau beberapa *covertext* lain. Secara klasik, informasi disembunyikan menggunakan tinta tak terlihat diantara garis-garis yang tampak dalam sepucuk surat pribadi[3]. Berbeda dengan kriptografi, pada steganografi dijital, data dijital atau informasi rahasia dibuat tidak terlihat karena informasi tersebut disembunyikan di dalam data digital yang lain, sedangkan pada kriptografi informasi rahasia dibuat sedemikian rupa menjadi tidak terbaca. Secara garis besar metode *Steganography* terdiri dari 2 bagian utama, yaitu proses penyembunyian data (*encode*) dan proses pengembalian data ke bentuk semula (*decode*). Kedua proses ini dilakukan dengan menggunakan sebuah kata kunci rahasia (*secret key*) yang akan digunakan di dalam prosesnya untuk meningkatkan keamanan data. Hasil yang didapat setelah proses *embedding* atau *encoding* disebut *Stego Object* (apabila media penampung hanya berupa data citra maka disebut *Stego Image*).



Gambar 1 : Proses Sistem *Steganography*[3]

2.1.2. Metode LSB

Cara paling umum untuk menyembunyikan pesan adalah dengan memanfaatkan *Least-Significant Bit* (LSB). Walaupun banyak kekurangan pada metode ini, tetapi kemudahan implementasinya membuat metode ini tetap digunakan sampai sekarang. Metode ini membutuhkan syarat, yaitu jika dilakukan kompresi pada stego, harus digunakan format lossless compression, karena metode ini menggunakan bit-bit pada setiap piksel pada citra. Jika digunakan format lossy compression, pesan rahasia yang disembunyikan dapat hilang. Jika digunakan image 24 bit color sebagai cover, sebuah

bit dari masing-masing komponen *Red, Green*, dan *Blue*, dapat digunakan sehingga 3 bit dapat disimpan pada setiap piksel. Sebuah image 800 x 600 piksel dapat digunakan untuk menyembunyikan 1.440.000 bit (180.000 bytes) data rahasia. Misalnya, di bawah ini terdapat 3 piksel dari image 24 *bit color* :

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

Jika diinginkan untuk menyembunyikan karakter A (10000001) dihasilkan :

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100110 11101001)

Dapat dilihat bahwa hanya 3 bit saja yang perlu diubah untuk menyembunyikan karakter A ini. Perubahan pada LSB ini akan terlalu kecil untuk terdeteksi oleh mata manusia sehingga pesan dapat disembunyikan secara efektif. Jika digunakan image 8 bit color sebagai *cover*, hanya 1 bit saja dari setiap piksel warna yang dapat dimodifikasi sehingga pemilihan image harus dilakukan dengan sangat hati-hati, karena perubahan LSB dapat menyebabkan terjadinya perubahan warna yang ditampilkan pada citra.

Akan lebih baik jika image berupa *image grayscale* karena perubahan warnanya akan lebih sulit dideteksi oleh mata manusia. Proses ekstraksi pesan dapat dengan mudah dilakukan dengan mengekstrak LSB dari masing-masing piksel pada stego secara berurutan dan menuliskannya ke output file yang akan berisi pesan tersebut. Kekurangan dari metode modifikasi LSB ini adalah bahwa metode ini membutuhkan "tempat penyimpanan" yang relatif besar. Kekurangan lain adalah bahwa stego yang dihasilkan tidak dapat dikompress dengan format *lossy compression* [18].

2.1.3. Kompresi *Huffman*

Salah satu teori yang dapat digunakan untuk mengompresi data adalah dengan kode *Huffman*. Kode ini dikemukakan oleh David A. *Huffman*, seorang doktor teori informasi (*information theory*) lulusan MIT (*Massachusets Institute of Technology*) pada tahun 1952. Dalam kompresi data, kode *Huffman* adalah kode-kode biner yang mengodekan suatu simbol tertentu pada suatu data. Kode-kode tersebut dibentuk dengan memperhatikan frekuensi kemunculan simbol tertentu pada data tersebut. Kode *Huffman* tidak bersifat unik, kode untuk setiap simbol berbeda pada setiap data berbeda yang dikompres. Dalam pembentukannya, Kode *Huffman* menerapkan konsep kode awalan (*prefix code*), yang merupakan himpunan kode basis dua, sedemikian sehingga tidak ada anggota himpunan yang merupakan awalan dari anggota yang lain, supaya pada proses dekoding, tidak ada keambiguan antara satu simbol dengan simbol yang lain. Kode awalan yang merepresentasikan simbol yang lebih sering muncul menggunakan rangkaian biner yang lebih pendek daripada kode yang digunakan untuk merepresentasikan simbol yang lebih jarang muncul. Dengan demikian jumlah bit yang digunakan untuk menyimpan informasi pada suatu data bisa lebih pendek.

2.1.4. *Steganalysis*

Pengertian steganalisis mengacu pada seni dan ilmu pengetahuan dalam mendeteksi ada-tidaknya pesan tersembunyi dalam suatu objek. Steganalisis untuk metode LSB terdiri dari metode subjektif dan metode statistik Metode subjektif melibatkan indera penglihatan manusia untuk mengamati bagian gambar yang dicurigai, sehingga disebut juga visual attack. Salah satu teknik steganalisis secara visual adalah metode *enhanced* LSB. Metode ini menampilkan bit-bit terakhir dari sebuah citra dan mengandalkan penglihatan manusia untuk menentukan ada tidaknya pesan rahasia dalam citra. Metode statistik yang akan dibahas adalah metode uji *chi-square* dan metode *RS-analysis*. Uji chi-square terbukti handal dalam mendeteksi pesan rahasia yang disisipkan secara sekuensial. Metode lainnya adalah *RS-analysis* yang terbukti handal dan akurat dalam mendeteksi pesan rahasia yang disisipkan secara acak.

2.2. Tinjauan Penelitian Terkait

Tinjauan studi dalam penelitian ini mengacu kepada beberapa penelitian terkait yang sudah di lakukan sebelumnya, antara lain :

a. Penelitian yang di lakukan oleh Rosziati Ibrahim, Ph.D dan Teoh Suk Kuan dari *Faculty of Computer Science and Information Technology*, University Tun Hussein Onn Malaysia dengan paper yang berjudul *Steganography Algorithm to Hide Secret Message Inside an Image* dan di publikasi dalam *Journal Computer Technology and Application 2, page 102-108, February 2011*[4]. Pada penelitian ini di ajukan algoritma untuk teknik pengamanan dengan dua layer (pertama menggunakan akses kontrol username dan password, kedua dengan menerapkan secret key pada proses *steganograpgy*).
b. Penelitian yang di lakukan oleh Ravinder Reddy dan Roja Ramani dari *Department of Master of Computer Applications, Teegala Krishna Reddy Engineering College* dengan paper yang berjudul *The Process of Encoding and Decoding of Image Steganography Using LSB Algorithm dan di publikasi pada IJSET, Vol.2, Issue 11, Page 1488-1492, November 2012*[1]. Pada penelitian ini di gunakan metode Least Significant Bit untuk menyisipkan data asil ke dalam citra. Untuk mengotimasi ukuran stego image di gunakan JPEG *Compression* dan hasil dari *stego image* dalam bentuk citra JPEG
c. Penelitian yang di lakukan oleh Morteza Bashardoost, Ghazali Bin Sulong dan Parisa Gerami dari *Faculty of Computing, Universiti Teknologi Malaysia* dengan paper yang berjudul *Enhanced LSB Image Steganography Method By Using Knight Tour Algorithm, Vigenere Encryption and LZW Compression* dan di publikasi dalam *International*

Journal of Computer Science Issues, Vol 10, Issue 2, No.1, March 2013[5]. Pada penelitian ini untuk penyisipan data asli menggunakan metode *Least Significant Bit* dan untuk optimasi ukuran stego image di ajukan penggunaan algoritma *Lempel-Ziv-Welch* (LZW) untuk mengkompresi data asli sebelum di sisipkan ke dalam citra dijital.

d. Penelitian yang di lakukan oleh Parul, Manju dan Dr. Harish Rohil dari *Department of Computer Science and Applications, Ch. Devil lal University and Department of Computer Engineering. CDL Govt. Ploytechnic ES* dengan paper yang berjudul *Optimized Image Steganography Using Dicrete Wavelet Transform (DWT)* dan di publikasi dalam *International Journal of Recent Development in Engineering and Technology, Volume 2, Issue 2, February 2014*[6]. Pada penelitian ini di gunakan metode *Dicrete Wavelet Transform* yang membagi sinyal (high and low frequency). *High frequency* di gunakan untuk menyimpan informasi pesan asli dan *low frequency* untuk menyimpan pixel citra. Hal ini di lakukan untuk mengoptimasi ukuran *stego image*. Dengan menggunakan metode *Dicrete Wavelet Transform* dapat dilakukan pula penyisipan data teks ke dalam citra.
e. Penelitian yang di lakukan oleh Maya CS dan Sabarinath G dari *Department of Electronics and Communication, St. Joseph's College of Engineering and Technology, Palai, India*, dengan paper yang berjudul *An Optimized FPGA Implementation of LSB Replacement Steganography Using DWT* dan di publikasi dalam *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, Special Issue 1, December 2013*[7].
   Pada penelitian ini di gunakan metode *Dicrete Wavelet Transform* untuk mengkompresi citra stego. Sedangkan untuk penyisipannya menggunakan metode LSB dengan di optimasi menggunakan FPGA.

2.3. Hipotesis

Hipotesis dari penelitian ini yaitu dapat menerapkan sistem keamanan terhadap data rahasia dengan menggunakan *steganography* dengan metode LSB (*Least Significant Bit*) dan optimasi ukuran file hasil *steganography* dengan menggunakan teknik kompresi *huffman*. Sistem *steganography* ini akan di lengkapi dengan validasi yang mengukur ketersediaan ruang pixel untuk data yang di sisipkan.

III. RANCANGAN PENELITIAN

3.1. Metode Penelitian

Metode penelitian yang di gunakan dalam penelitian ini adalah metode penelitian eksperimen. Metode eksperimen adalah sebagai metode penelitian yang digunakan untuk mencari pengaruh perlakuan tertentu terhadap yang lain dalam kondisi yang terkendalikan[8]. Eksperimen merupakan modifikasi kondisi yang dilakukan secara sengaja dan terkontrol dalam menentukan peristiwa atau kejadian, serta pengamatan terhadap perubahan yang terjadi pada peristiwa itu sendiri[9].

3.2. Metode Pengumpulan Data

Metode pengumpulan data yang di gunakan dalam penelitian ini adalah pengamatan atau observasi. Observasi adalah pengamatan dan pencatatan secara sistimatik terhadap unsur-unsur yang tampak dalam suatu gejala atau gejala-gejala dalam objek penelitian[10].

3.3. Teknik Analisis Data

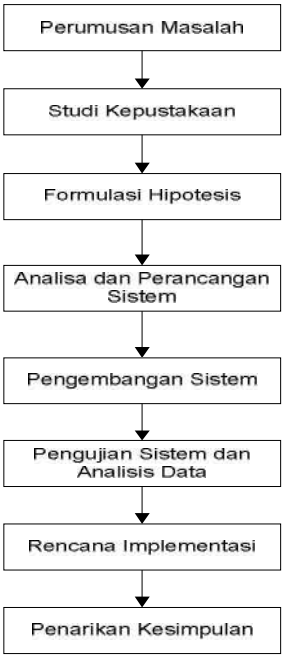
Teknik analisis data dalam penelitian ini menggunakan pendekatan kualitatif dimana data yang telah ada di analisa menggunakan analisis data statistik. Analisis data secara kualitatif di lakukan dengan menganalisa besaran teks yang di kompresi pada saat sebelum di sisipkan dan performa aplikasi pada saat kompresi dan penyisipan teks. Selain itu di lakukan analisa untuk perbandingan dari hasil penggunaan kompresi dalam optimasi ukuran pada sistem *steganography* dengan tanpa penggunaan kompresi untuk melihat efektifitas penggunaan kompresi dalam hal optimasi citra hasil penyisipan. Analisis data statistik yang dilakukan adalah terhadap frekuensi satuan warna dari citra asli di bandingkan dengan citra hasil penyisipan teks untuk melihat kualitas citra hasil penyisipan.

3.4. Langkah-langkah Penelitian

Tahapan penelitian yang di lakukan dalam rangka penelitian pemanfaatan kompresi *huffman* untuk optimasi hasil citra dijital pada sistem *steganography* ini adalah sebagai berikut

a. Perumusan Masalah
b. Studi Kepustakaan
c. Formulasi Hipotesis
d. Analisa dan Perancangan Sistem
e. Pengembangan Sistem
f. Pengujian Sistem dan Analisis Data
g. Rencana Implementasi
h. Penarikan Kesimpulan

Berikut adalah alur yang merepresentasikan dari langkah-langkah penelitian yang di lakukan :

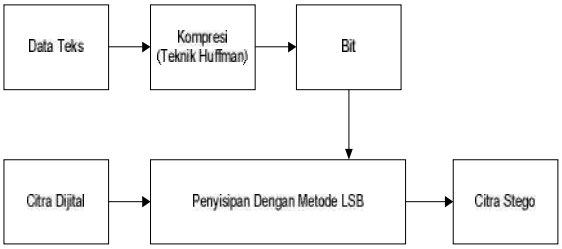


Gambar 2. Langkah-langkah Penelitian

IV. ANALISIS, INTERPRESTASI DAN IMPLIKASI PENELITIAN

4.1. Proses *Encode*

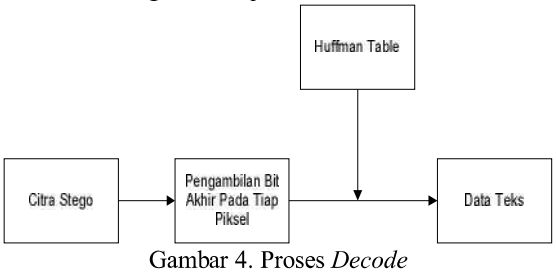
Proses *encode* adalah proses untuk peyisipan teks ke dalam citra yang di sertai dengan teknik kompresi *huffman*. Berikut adalah diagram dari proses *encode*.



Gambar 3. Proses *Encode*

4.2. Proses *Decode*

Proses *decode* adalah proses untuk ekstrasi teks dari citra stego yang di sertai dengan teknik dekompresi *huffman*. Berikut adalah diagram dari proses *decode*.

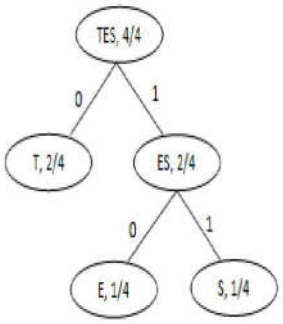


Gambar 4. Proses *Decode*

4.3. Mekanisme Kerja Sistem

Berikut adalah simulasi perhitungan dan mekanisme kerja proses encode data teks.

a. Terdapat citra dijital dengan dimensi 3 x 3, di dapatkan setiap piksel terdiri dari 3 blok (Read, Green dan Blue), maka di dapatkan total blok adalah 27 blok = 27 byte.
b. Terdapat teks yang akan di sisipkan, sebagai contoh: TEST
   TEST → 4 Karakter → 4 Byte = 32 bit
   Untuk mengurangi jumlah bit yang dibutuhkan, panjang kode untuk tiap karakter dapat dipersingkat, terutama untuk karakter yang frekuensi kemunculannya besar dengan menggunakan pohon *huffman*.



Gambar 5. Pohon *Huffman*

Berdasarkan pohon *huffman* frekuensi munculnya karakter dari data teks, maka di dapatkan dari tabel *huffman* berikut, maka di dapatkan tabel berikut :

Tabel 1. Susunan Frekuensi *Huffman*

Karakter	Frekuensi	Kode Huffman
T	2	0
E	1	10
S	1	11

Properti pohon *huffman* :

a. Setiap internal node teridiri dari 2 anak.
b. Jumlah frekuensi terdikit sebagai akar.
c. Jumlah bit yang di butuhkan pada kompresi.

$$B(T) = \sum_{i=1}^{n} f(C_i).d_T(C_i),$$

Keterangan :

$B(T)$ = Jumlah bit dari hasil kompresi Frekuensi dari karakter
$d_T(C_i)$ = Panjang dari kode *huffman* untuk tiap karakter ke - i

Berdasarkan rumus di atas, maka di dapatkan jumlah bit hasil kompresi :

$B(T)$ = (2x1) + (1x2) + (1x2) = 6 bit

c. Selanjutnya byte hasil kompresi di sisipkan ke dalam citra dijital, yaitu dengan meletakkan setiap bit dari byte hasil kompresi ke dalam bit terakhir tiap byte dari citra.

Berikut adalah meknisme kerja dari proses *decode* data teks dari *stego image*.

a. Terdapat citra dijital hasil penyisipan teks ke dalamnya dengan dimensi 3 x 3. Berdasarkan dimensi citra, maka di dapatkan jumlah blok yaitu 27 blok sama dengan 27 byte.
b. Ambil satu bit terakhir dari tiap byte pada citra, lalu susun menjadi byte data.
c. Cocokkan byte hasil dari proses nomor 2 dengan tabel *huffman*,
d. Susun karakter hasil dari pencocokkan.

4.4. Pengujian Sistem

Pada penelitian ini di terapkan suatu metode pemilihan sample citra dijital dan data teks untuk di uji secara acak. Terdapat lima citra asli dan lima data teks yang akan disisipkan. Berikut adalah tabel dari citra asli dan data teks yang akan disisipkan.

Tabel 2. Properti Citra Asli

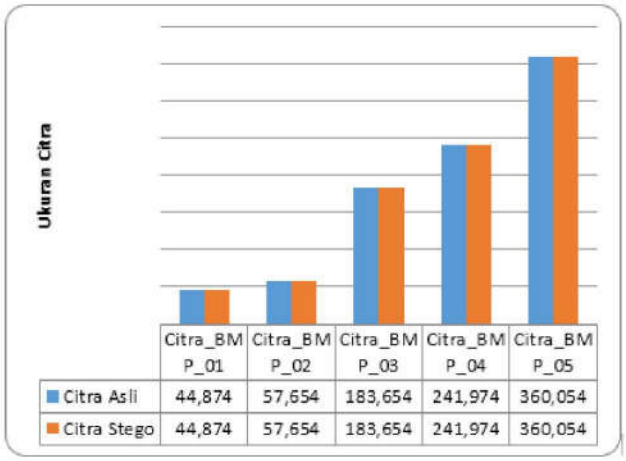
Nama Citra	Properti	
	Dimensi	Ukuran (byte)
Citra_BMP_01	179 x 83	44,874
Citra_BMP_02	128 x 150	57,654
Citra_BMP_03	300 x 204	183,654
Citra_BMP_04	288 x 280	241,974
Citra_BMP_05	400 x 300	360,054

Tabel 3 Properti Data Teks

No	Nama Data Teks	Ukuran (byte)
1	Teks_01	799
2	Teks_02	914
3	Teks_03	1,031
4	Teks_04	1,148
5	Teks_05	1,176

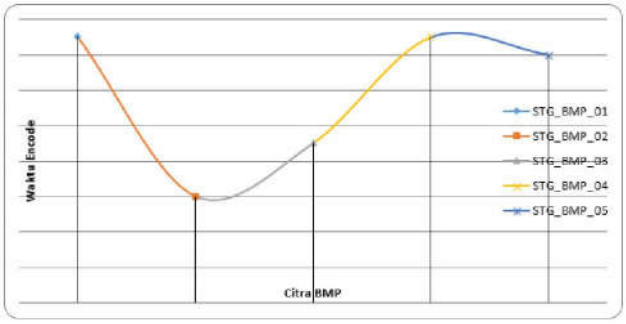
4.5. Pengujian Kualitas Sistem

Berdasarkan citra hasil penyisipan, di dapatkan ukuran citra hasil penyisipan jenis BMP sama dengan ukuran citra asli. Untuk tiap citra, misal citra pertama memiliki waktu *encode* yang berbeda, walaupun ukuran data teks yang di sisipkan adalah sama, begitu juga pada urutan citra kedua sampai kelima. Dengan demikian ukuran citra stego sama dapat di optimasi yang merupakan akibat dari penggunaan kompresi. Hal tersebut dapat di lihat dari gambar chart berikut:



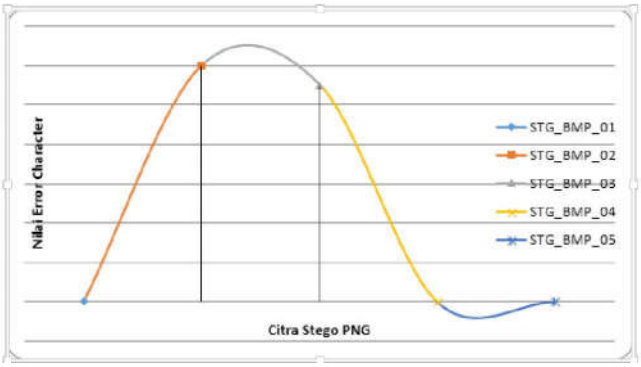
Gambar 6. Perbandingan Ukuran Citra

Berdasarkan hasil penyisipan, waktu peyisipan untuk tiap citra berbeda-beda, hal tersebut dapat di lihat pada chart berikut.



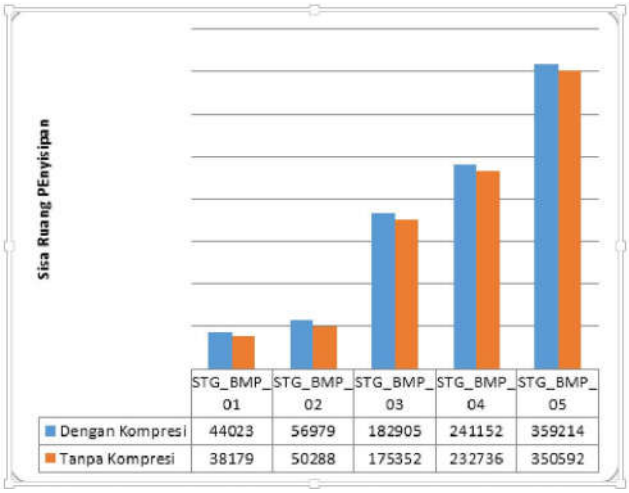
Gambar 7. Waktu Proses Encode Citra

Berdasarkan hasil ekstrasi dapat di simpulkan, bahwa data teks hasil ekstrasi cukup jelas dengan melihat rendahnya *Error Character* dan waktu ekstrasi untuk tiap citra berbeda-beda. Hal tersebut dapat di lihat dari chart berikut :



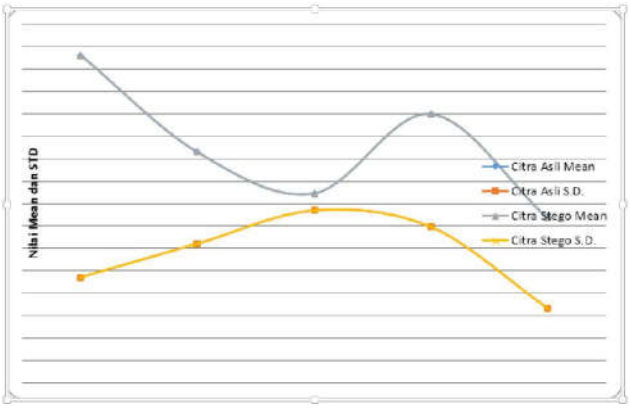
Gambar 8. Nilai *Error Character* Citra

Dengan menggunakan teknik kompresi maka ruang penyisipan data teks ke dalam citra menjadi lebih besar di karenakan pemampatan jumlah bit yang disisipkan. Dengan demikian penggunaan kompresi berdampak kepada ruang piksel yang akan di sisipkan menjadi lebih banyak. Berikut adalah chart yang menggambarkan perbandingan perbedaan penyisipan dengan teknik kompresi dan tanpa kompresi.



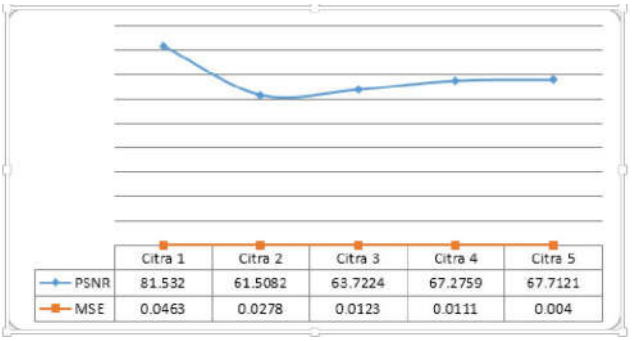
Gambar 9. Perbandingan Sisa Ruang Penyisipan Citra Stego BMP

Berdasarkan perbandingan nilai mean dan standar deviasi dari citra asli dengan citra stego, maka dapat di simpulkan bahwa terjadi penurunan pada standar deviasi dan mean. Jika terjadi penurunan pada standar deviasi maka di simpulkan bahwa intensitas warna berkurang demikian jika terjadi kenaikan standar deviasi maka terjadi peningkatan intensitas warna. Berikut adalah chart yang meggambarkan perbandingan nilai mean dan standar deviasi antara citra asli dan citra stego untuk tiap citra.



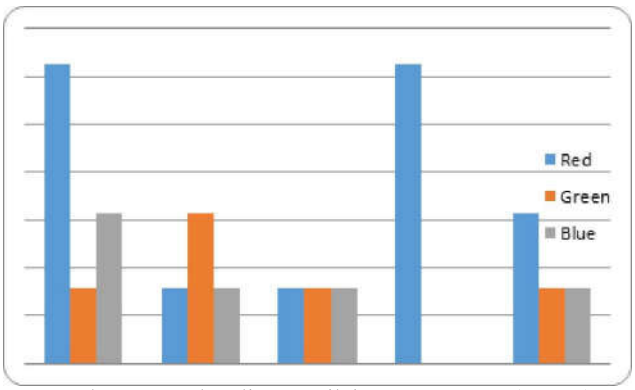
Gambar 10. Perbandingan Mean dan Standar Deviasi Citra BMP

Analisis kualitas citra menggunakan pengukuran terhadap PSNR dan MSE. Berikut adalah tabel analisa PSNR dan MSE terhadap tiap citra.



Gambar 11. Perbandingan PSNR dan MSE Citra BMP

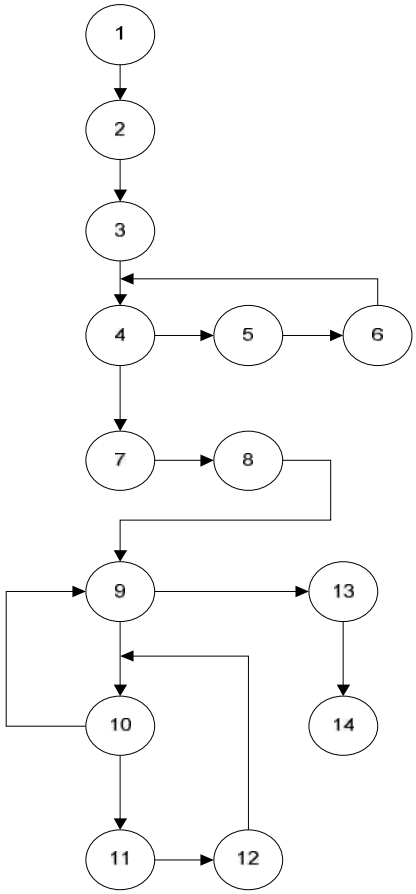
Analisis perbandingan nilai satuan warna di lakukan untuk dapat melihat perbedaan antara nilai satuan warna dari citra asli dengan nilai satuan warna citra stego. Berikut adalah chart presentase perbandingan nilai satuan warna (R,G,B).



Gambar 12. Perbandingan Nilai Satuan Warna (R,G,B)

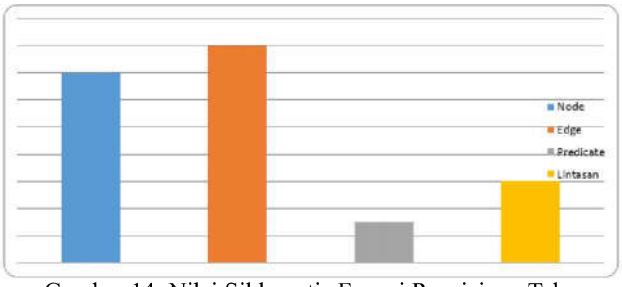
4.5.1. Pengujian Kompleksitas Sistem

Pengujian pertama di lakukan terhadap fungsi penyisipan data. Pengujian kompleksitas ini adalah mengkonversi setiap proses yang ada pada sistem menjadi sebuah flowgraphy. Berikut adalah *flowgraph* dari fnugsi penyisipan data.



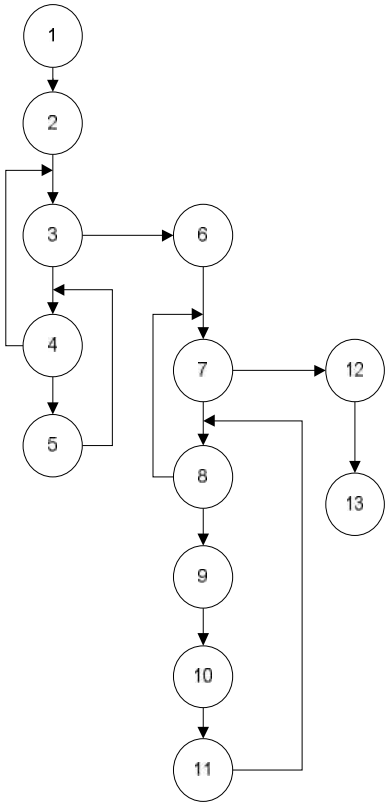
Gambar 13. *Flowgraph* Penyisipan

Berdasarkan perhitungan node, edge, predicate dan lintasan, maka di dapatkan sebanyak 14 *node*, 16 *edge*, 3 *predicate* dan 6 lintasan. Berikut adalah chart yang menggambarkan nilai dari hasil pengukuran kompleksitas siklomatis fungsi penyisipan pesan.



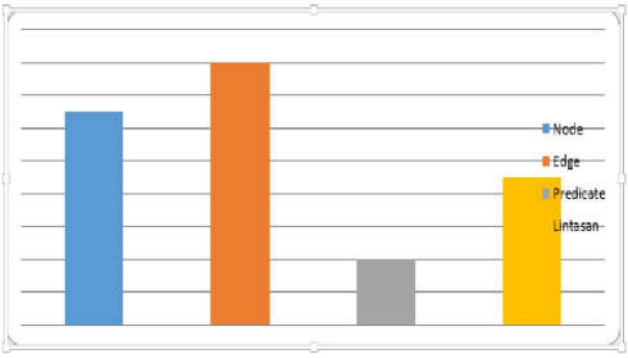
Gambar 14. Nilai Siklomatis Fungsi Penyisipan Teks

Pengujian kedua di lakukan terhadap fungsi ekstrasi data. Berikut adalah *flowgraph* dari fnugsi ektrasi data.



Gambar 15. *Flowgraph* Fungsi Ekstrasi

Berdasarkan perhitungan node, edge, predicate dan lintasan, maka di dapatkan sebanyak 13 *node*, 16 *edge*, 4 *predicate* dan 9 lintasan. Berikut adalah chart yang menggambarkan nilai dari hasil pengukuran kompleksitas siklomatis fungsi ekstrasi pesan.



Gambar 16. Nilai Siklomatis Fungsi Ekstrasi

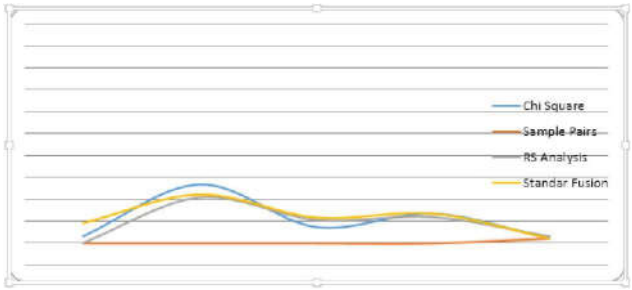
4.5.2. Pengujian Fungsionalitas Sistem

Berdasarkan pengujian terhadap setiap fungsi pada sistem *steganography* yang di kombinasikan dengan kompresi *huffman* maka di simpulkan fungsi pada sistem dapat berjalan dengan baik.

4.5.3. Pengujian Keamanan Citra Stego

Pengujian ini bertujuan untuk menguji terhadap citra stego agar dapat di ketahui apakah citra stego yang di hasilkan oleh sistem *steganography* dapat terdeteksi indikasi adanya data teks yang di sisipkan. Pengujian ini menggunakan perangkat lunak *StegExpose* yang menggunakan metode *Chi Square*, *Sample Pairs*, *RS Analysis*, *Standar Fusion* dan satu variable *Above Stego* yang berfungsi untuk menentukan apakah citra tersebut terindikasi data teks yang di sisipkan.

Berdasarkan hasil pengujian citra stego yang di uji di dapatkan beberapa citra stego untuk citra stego BMP terdapat satu citra yang terdeteksi dan empat citra tidak terdeteksi. Berikut adalah grafik perbandingan nilai dari metode *Chi Square*, *Sample Pairs*, *RS Analysis* dan *Standar Fusion* untuk tiap citra stego.



Gambar 17. Grafik Nilai Pengujian Keamanan Terhadap Citra Stego BMP

4.5.4. Pengujian Kepuasan Pengguna

Pengujian kepuasan pengguna sistem menggunakan pendekatan ISO 9126 yaitu dengan menguji tingkat kualitas masing-masing aspek berdasarkan empat karakteristik ISO 9126 yaitu *Functionality, Reliability, Usability dan Efficiency*. Berikut adalah tabel hasil pengujian

Tabel 4. Hasil Pengujian Pengguna Sistem

Aspek	Skor Aktual	Skor Ideal	% Skor Aktual	Kriteria
Functionality	351	450	78	Baik
Reliability	208	270	77	Baik
Usability	315	360	87.5	Baik
Efficiency	148	180	82	Baik
Total	1022	1260	81 %	Baik

Berdasarkan keseluruhan aspek dapat di simpulkan bahwa tingkat kualitas aplikasi secara keseluruhan dengan kriteria baik dengan presentase 81 %.

4.6. Implikasi Penelitian

4.6.1. Aspek Sistem

Dari segi sistem, implikasi penelitian yang di timbulkan dengan adanya sistem *steganography* yang di kombinasikan dengan kompresi *huffman* adalah tersedianya sistem yang dapat di gunakan untuk pengamanan data teks yang rahasia, seperti informasi akun, informasi personal, informasi transaksi, dan lainnya dengan dapat di sisipkan ke dalam citra dijital. Implikasi lainnya yang di akibatkan dari penggunaan teknik kompresi *huffman* pada sistem *steganography* adalah teroptimasi ruang penyisipan teks dan mengurangi dampak dari *steganalysis*.

4.6.2. Aspek Manajerial

Dari segi manajerial, implikasi yang di hasilkan dari penelitian ini adalah dengan sistem *steganography* yang di kembangkan dapat membantu pengguna dalam mengamankan komunikasi dan pertukaran informasi yang rahasia dengan menyisipkan pesan rahasia ke dalam citra dijital melalui jaringan lokal atau publik. Salah satu dampak yang di akibatkan dari penggunaan teknik kompresi adalah dapat memberikan ruang untuk menyembunyikan data teks. Mengingat banyak orang dari belahan dunia menggunakan jaringan publik (*internet*) secara bersama dan terbuka, maka semakin banyak potensi orang untuk mencurigai transaksi dan bahkan melakukan pencurian data agar mendapatkan informasi yang memiliki nilai sangat berharga.

4.6.3. Penelitian Lanjutan

Dari hasil penelitian yang telah di lakukan masih memiliki kekurangan dan memerlukan penelitian lanjutan guna menyempurnakannya. Berikut adalah beberapa hal yang perlu di lakukan dalam penelitian lanjutan.

a. Perlu di lakukan penelitian dengan di terapkannya enkripsi agar mengurangi dampak dari steganalysis
b. Perlu di lakukan penelitian terhadap penyisipan ke dalam citra yang memiliki kompresi seperti JPEG, PNG dan GIF dengan di kombinasikan dengan teknik kompresi terhadap data teks sebelum di sisipkan. Hal ini di karenakan citra JPEG, PNG dan GIF telah memiliki sistem kompresi citra yang mengakibatkan jika data teks yang terkompresi dan di sisipkan ke dalam citra JPEG/PNG/GIF akan bermasalah pada saat ekstrasi.
c. Perlu di lakukan penelitian dan kajian agar kompresi yang di lakukan bisa di terapkan ke jenis data selain teks agar dapat di sisipkan ke dalam citra dijital.
d. Perlu di lakukan penelitian dan kajian untuk komparasi dengan teknik kompresi data teks lainnya seperti dengan kompresi LZW atau teknik kompresi lainnya agar dapat di bandingkan dan di ketahui mana kompresi yang memiliki dampak optimasi terhadap ukuran citra hasil penyisipan paling baik.
e. Perlu di lakukan penelitian dan kajian terhadap media file yang di jadikan tempat penyisipan selain dari citra dijital, mungkin dapat menggunakan file audio atau video.
f. Perlu di lakukan penelitian dan kajian agar sistem *steganography* yang di kembangkan dapat di gunakan di berbagai platform seperti di sistem operasi linux, macintosh dan perangkat bergerak seperti android, IOS dan Blackberry.

V. PENUTUP

5.1. Kesimpulan

Setelah melalui serangkaian proses penelitian yang telah di lakukan dan hasil dari penelitian ini maka dapat disimpulkan mengenai beberapa hal, yaitu:

a. Dengan menerapkan *steganography* dalam hal pengamanan data teks, penyisipan dapat di lakukan dengan baik dan sekaligus dapat mengamankan data-data yang di komunikasikan melalui jaringan komputer.
b. Dengan merapkan teknik kompresi *huffman* terhadap data teks pada saat penyisipan akan mengoptimasi ukuran citra hasil penyisipan.
c. Dengan menerapkan teknik kompresi *huffman*, maka kualitas citra stego tidak jauh berbeda dengan citra aslinya.
d. Dengan menerapkan teknik kompresi *huffman*, maka akan mengurangi dampak dari *steganalysis*, hal ini di karenakan jumlah bit yang di sisipkan menjadi sedikit.

5.2. Saran

Berdasarkan hasil penelitian dari ini yang berjudul "Pemanfaatan Kompresi Huffman Untuk Optimasi Ukuran Gambar Pada Sistem Steganography Menggunakan Metode LSB", terdapat beberapa saran, yaitu:

a. Perlu di lakukan penelitian dengan di terapkannya enkripsi agar mengurangi dampak dari steganalysis
b. Perlunya di kembangkan algoritma dari sistem untuk dapat mengatasi penggunaan citra yang terkompresi seperti PNG, GIF dan JPEG.
c. Untuk kedepannya perlu di analisa agar sistem yang di kembangkan dapat di gunakan di berbagai platform seperti di platform mobile dan di website.
d. Perlu di lakukan analisa untuk membandingkan jika yang di kompresi adalah citra hasil penyisipan dengan jika yang di kompresi adalah pesan yang di sisipkan. Hal ini untuk mendapatkan komparasi kualitas citra stego dengan citra asli.

DAFTAR PUSTAKA

[1] Ravinder Reddy and Roja Ramani, *The Process of Encoding and Decoding of Image Steganography Using LSB Algorithm,* IJSET Vol.2 Issue 11, 2012

[2] C.P. Sumathi, T Santanam, G Umamaheswari, *A Study of Various Steganographic Techniques Used for Information Hiding,* IJCSES Vol.4 No.6, 2013

[3] Domenico Daniele Bloisi, Luca Iocchi, *Image based Steganography and Cryptography*, Computer Vision theory and applications Vol.1, 2007

[4] Rosziati Ibrahim and Teoh Suk Kuan, *Steganography Algorithm to Hide Secret Message inside an Image*, Computer Technology and Application 2, 2011

[5] Ghazali Bin Sulong and Parisa Gerami, *Enhanced LSB Image Steganography Method By Using Knight Tour Algorithm, Vigenere Encryption and LZW Compression,* International Journal of Computer Science Issues Vol 10, 2013

[6] Parul, Manju and Harish Rohil, *Optimized Image Steganography Using Dicrete Wavelet Transform (DWT),* International Journal of Recent Development in Engineering and Technology Volume 2 Issue 2, 2014

[7] Maya CS, Sabarinath G, *An Optimized FPGA Implementation of LSB Replacement Steganography Using DWT*, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, 2013

[8] Sugiyono, *Metode Penelitian Kuantitatif Kualitatif dan R&B,* Bandung:Alfabeta, 2009

[9] Ali, Mohammad, *Strategi Penelitian Pendidikan*, Bandung: Angkasa, 1993

[10] Nawawi, Hadari ,Martini, *Instrumen Penelitian Bidang Sosial*, Yogyakarta: Gadjah Mada University Press, 2006