Kode/Nama Rumpun Ilmu*	: **459 / Ilmu Komputer**
Bidang Fokus**	: **Teknologi Informasi dan Komunikasi**

LAPORAN AKHIR

PENELITIAN HIBAH INTERNAL

PERANCANGAN *HIDDEN MESSAGE* STEGANOGRAFI DENGAN METODE *LEAST SIGNIFICANT BIT INSERTION* (LSB) BERBASIS MATLAB

PENELITI :

IR. NIZIRWAN ANWAR, MT (NIDN 0424076401)

FAKULTAS ILMU KOMPUTER

UNIVERSITAS ESA UNGGUL

OKTOBER 2017

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT yang telah melimpahkan ridho-Nya dan rahmat-Nya, sehingga penulis dapat menyelesaikan penyusunan laporan penelitian ini. Shalawat dan salam semoga senantiasa tercurahkan kepada junjungan kita Nabi Muhammad SAW sehingga penulis dapat menyelesaikan laporan penelitian hibah internal dengan berjudul "**PERANCANGAN STEGANOGRAFI *HIDDEN MESSAGE* DENGAN METODE *LEAST SIGNIFICANT BIT INSERTION* (LSB) BERBASIS MATLAB"** hingga batas waktu yang telah ditentukan. Semoga laporan penelitian ini dapat memberikan manfaat bagi sivitas akademika Universitas Esa Unggul.

Penulis menyampaikan rasa terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu baik secara langsung maupun tidak langsung dalam penyusunan laporan ini hingga selesai kepada ;

1. Bapak **Dr. Ir. H. Arief Kusuma AP, MBA** selaku Rektor Universitas Esa Unggul Jakarta.
2. Bapak **Dr. Hasyim, SE, MM, M.Ed** selaku Kepala Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) Universitas Esa Unggul Jakarta.
3. Bapak **Dr. Ir. Husni S. Sastramihardja, MT** selaku Dekan Fakultas Ilmu Komputer Universitas Esa Unggul Jakarta.
4. **Orang Tua dan keluarga (istri dan anak2**) serta para karib kerabat yang telah memberikan semangat serta do'a sehingga penulis dapat menyelesaikan laporan ini.

Demikianlah laporan penelitian ini penulis sampaikan. Tidak ada yang dapat diberikan selain mohon iringan doa semoga apa yang telah dijalankan dapat berkontribusi dalam memnbangun atmosfir akademik dan menjadi amal shaleh serta memperoleh balasan pahala dari Allah SWT.

Jakarta, Oktober 2017

Ir. Nizirwan Anwar, MT

HALAMAN PENGESAHAN
PENELITIAN HIBAH INTERNAL

Judul Penelitian	:	**Perancangan Steganografi *Hidden Message* dengan metode *Least Significant Bit Insertion* (LSB) berbasis Matlab**
Kode/Nama Rumpun Ilmu	:	**459 / Ilmu Komputer**

Ketua Peneliti

a.	Nama Lengkap	:	**Ir. Nizirwan Anwar, MT**	**L / ~~P~~**
b.	NIDN	:	**0424076401**	
c.	Jabatan Fungsional	:	**Lektor Kepala**	
d.	Program Studi	:	**Teknik Informatika**	
e.	Nomor HP	:	**(+62) 877 7449 2649**	
f.	Alamat surel (e-mail)	:	**nizirwan.anwar@esaunggul.ac.id**	

Usulan Penelitian Tahun ke-	:	**1 (satu)**
Biaya Penelitian Keseluruhan	:	**Rp 15.000.000,-**
Biaya Penelitian :		
• diusulkan ke DRPM	:	**Rp -**
• dana internal PT	:	**Rp 15.000.000,-**

Jakarta, Oktober 2017

Mengetahui,
Dekan Fakultas Ilmu Komputer

Dr. Ir. Husni Setiawan Sastramihardja, MT
NIK 214030494

Ketua Peneliti,

Ir. Nizirwan Anwar, MT
NIK 217080700

Menyetujui,
Ketua LPPM UEU

Dr. Hasyim,SE, MM, MEd
NIK 201040164

ABSTRAK

Steganografi (*steganography*) adalah ilmu teknik atau seni untuk menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat di-akses oleh orang lain yang tidak mempunyai kewenangan. Dalam hal keamanan data (image, teks atau audio) sebaiknya mengikuti sesuai 5 (lima) kaidah utama adalah faktor *confidentiality, integrity, availability, authenticity,* dan *non-repudiation*. Metode algoritma LSB merupakan salah satu metode yang pada umumnya digunakan steganografi dimana proses penggabungan pesan yang berisi teks disimpan dalam image tertentu dalam hal ini format *image* yang dilakukan penelitian ini JPG dan BMP dengan ukuran resolusi tertentu. Penelitian ini menghasilkan setelah proses pengujian dan penganalisaan dengan menggunakan aplikasi berbasis matriks (Matlab – Mfile) tidak terdapat perubahan yang siginifikan baik kualitas image (*cover* maupun *stego*) dan teks.

Kata Kunci : Steganografi, Cover Image, Stego-Image, Metode LSB

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1. Latar Belakang

Manusia sebagai makhluk sosial, sejak lahir sampai mati selalu hidup dalam masyarakat, tidak mungkin manusia di luar masyarakat. Aristoteles mengatakan bahwa makhluk hidup yang tidak hidup dalam masyarakat ialah sebagai seorang malaikat atau hewan. Keutuhan manusia akan tercapai apabila manusia sanggup menyelaraskan perannya sebagai makhluk ekonomi dan sosial yang punya karakteristik salah satu nya saling bertukar informasi (file, teks, gambar, video atau media lainnya) Sebagai makhluk sosial (*homo socialis*), manusia tidak hanya mengandalkan kekuatannya sendiri, tetapi membutuhkan manusia lain dalam beberapa hal tertentu.

Dalam dunia globalisasi teknologi informasi yang dipengaruhi oleh beberapa proses faktor antara lain oleh bisnis dan tata kerja, ekonomi, sosial, sumber daya sosial-budaya, dan lingkungan alam. Dan berdampak berkembang teknologi bagaimana *exchange* (pengirim ↔ penerima) data hanya dapat dilihat, dibaca dan di-akses hanya orang yang tepat (penerima) dan dapat bertanggung jawab, sesuai 5 (lima) kaidah utama dalam keamanan data adalah faktor *confidentiality*, *integrity*, *availability, authenticity*, dan *non-repudiation*. Kata steganografi berasal dari bahasa Yunani yaitu steganos yang artinya tersembunyi atau terselubung dan graphein, yang artinya menulis, sehingga kurang lebih artinya adalah “menulis tulisan yang tersembunyi atau terselubung” (Sellars, 1996).

Dalam mencegah keamanan data, teknik steganografi merupakan salah satu teknik untuk menyembunyikan dan pesan tersebut sehingga selain pengirim dan penerima tidak dapat mengetahui atau menyadari bahwa ada suatu pesan yang bersifat ‘rahasia’. Dan sebaliknya dalam teknik kriptografi merupakan teknik menyamarkan dari suatu pesan akan tetapi tidak dapat menyembunyikan bahwa ada suatu pesan tersbut.

Tabel 1 Komparasi teknik pengamanan data [Popa, 1998]

	Confidentiality	Integrity	Unremovability
Encryption	√	×	√
Digital Signatures	×	√	×
Steganography	√ / ×	√ / ×	√

Pengaplikasian steganografi dengan menggunakan matlab adalah dengan menyisipkan pesan pada media gambar. Dengan metode ini pesan akan tersamarkan dengan baik pada file gambar yang dikirimkan, sehingga pengirim dapat dengan nyaman mengirimkan pesan rahasia pada gambar. Dengan cara ini akan sulit sekali untuk membaca secara kasat mata pesan yang disisipkan pada media gambar bila pesan tidak terlebih dahulu di ekstrak dari media gambarnya, dan pesan akan tersimpan dengan aman. Sebagai contoh, si pengirim mulai dengan berkas gambar biasa, lalu mengatur warna setiap pixel ke-n untuk menyesuaikan suatu huruf dalam alphabet (perubahannya begitu halus sehingga tidak ada seorangpun yang menyadarinya jika ia tidak benar-benar memperhatikannya).

Metode yang digunakan untuk penyembunyian pesan rahasia pada proto-type yang akan dibuat adalah dengan cara menyisipkan pesan ke dalam bit rendah LSB *(Least Significant Bit*) pada data pixel yang menyusun file gambar. Metode penyisipan LSB ini adalah menyisipi pesan bit tertentu pada representasi biner file gambar dengan representasi biner pesan rahasia yang akan disembunyikan.

1.2 Rumusan Masalah

Rumusan masalah dalam penelitian berdasarkan latar belakang diatas adalah ;

(a) Bagaimana keamanan data dan kinerja (*performance)* dengan metode LSB agar data selain dapat disembunyikan, dapat pula terjaga kerahasiaannya dari pihak yang tidak berwenang (pihak ketiga)

(b) Bagaimana ukuran (*size*) proses file sebelum (cover) dan setelah (*stego*) steganografi dengan metode LSB ?

(c) Bagaimana perubahan yang dialami oleh file asli dan file pesan hasil proses steganografi dengan menggunakan metode LSB ?

1.3. Batasan Masalah

Batasan masalah dalam penelitian adalah ;

(a) Bagaimana keamanan data dan kinerja (*performance)* dengan metode LSB agar data selain dapat disembunyikan, dapat pula terjaga kerahasiaannya dari pihak yang tidak berwenang (pihak ketiga)

(b) Bagaimana ukuran (*size*) proses file sebelum (cover) dan setelah (*stego*) steganografi dengan metode LSB ?

(c) Bagaimana perubahan yang dialami oleh file asli dan file pesan hasil proses steganografi dengan menggunakan metode LSB ?

1.4. Tujuan Penelitian

Penelitian ini bertujuan untuk menerapkan suatu sistem keamanan data dengan algoritma steganografi dengan metode LSB sebagai berikut ;

(a) Untuk melakukan pengamanan data dan kinerja (*performance)* dengan metode LSB agar data tersrbut tidak dapat di-akses orang lain dan dapat disembunyikan, dapat pula terjaga kerahasiaannya dari pihak yang tidak berwenang (pihak ketiga)

(b) Menguji dan menganalisa ukuran (*size*) proses file sebelum (cover) dan setelah (*stego*) steganografi dengan metode LSB.

(c) Menguji perubahan yang dialami oleh file master dan file pesan program dengan menggunakan aplikasi multi-purposes M-File (Matlab), baik ukuran dan kualitas file.

1.5 Luaran Penelitian

Tabel 2 Jenis Luaran terhadap Indikator Capaian

No	Jenis Luaran			
	Kategori	**Sub Kategori**	**Wajib**	**Tambahan**
1	Artikel ilmiah dimuat di jurnal	Internasional bereputasi		
		Nasional Terakreditasi		
		Internal / Eksternal ber ISSN	√	
2	Artikel ilmiah dimuat di prosiding	Internasional Terindeks		
		Nasional		√
3	*Invited speaker* dalam temu ilmiah	Internasional		
		Nasional		
		Forum Ilmiah Dosen	√	

BAB II

TINJAUAN PUSTAKA

2.1. Steganografi

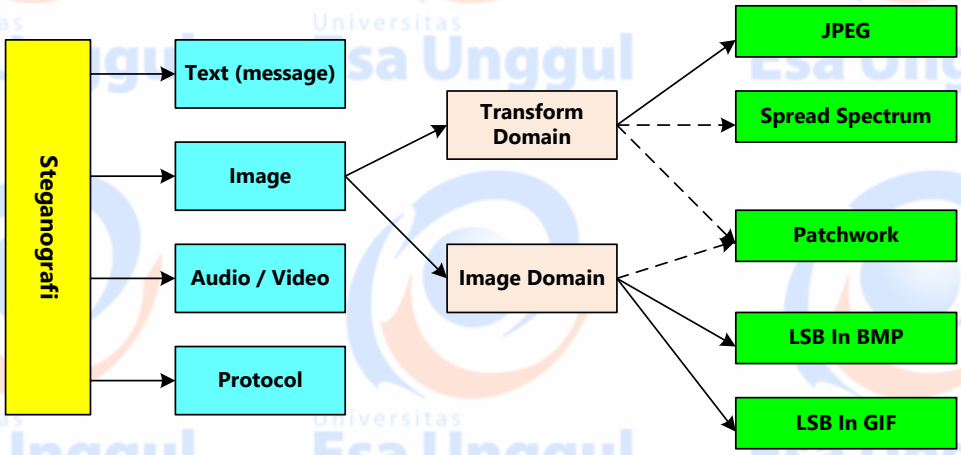
Steganografi adalah suatu teknik untuk menyembunyikan informasi yang bersifat pribadi dengan sesuatu yang hasilnya akan tampak seperti informasi normal lainnya. Media yang digunakan umumnya merupakan suatu media yang berbeda dengan media pembawa informasi rahasia, dimana disinilah fungsi dari teknik steganografi yaitu sebagai teknik penyamaran *(incognito techniques)* menggunakan media lain yang berbeda sehingga informasi rahasia dalam media awal tidak terlihat secara jelas oleh pihak ketiga. Dalam perang Dunia II, teknik steganografi umum digunakan oleh tentara Jerman dalam mengirimkan pesan rahasia dari atau menuju Jerman, (Morkel, et.all, 2005). Steganografi biasanya sering disalahartikan dengan kriptografi karenanya kedua konsep tersebut mempunyai tujuan untuk melindungi informasi. Perbedaan yang mendasar antara keduanya yaitu steganografi berhubungan dengan informasi tersembunyi sehingga tampak seperti tidak ada informasi tersembunyi sama sekali. Jika seseorang mengamati obyek yang menyimpan informasi tersembunyi tersebut, maka dia tidak akan menduga bahwa terdapat pesan rahasia dalam obyek tersebut, sehingga tidak dapat memecahkan informasi dari obyek tersebut. Pada umumnya, pesan steganografi muncul dengan obyek / data lain seperti gambar, artikel, daftar menu, atau pesan-pesan lainnya. Pesan yang tertulis ini merupakan tulisan yang menyelubungi (*envelop*) atau menutupi (*mask*). Pada metode steganografi cara ini sangat berguna jika digunakan pada cara steganografi komputer karena banyak format berkas digital yang dapat dijadikan media untuk menyembunyikan pesan. Format yang biasa digunakan di antaranya:

(a) Format *image* : bmp, gif, pcx, jpeg, gif, dll
(b) Format *audio* : wav, voc, mp3, dll.
(c) Format lain : teks file, html, pdf, dll.

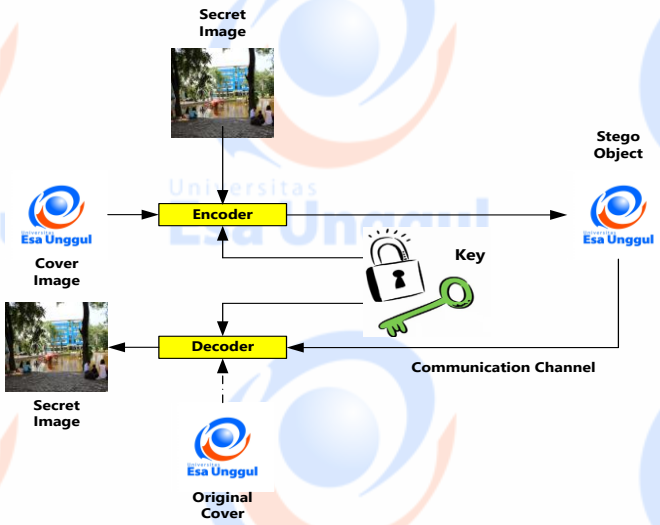
Kelebihan steganografi jika dibandingkan dengan kriptografi adalah pesan-pesannya tidak menarik perhatian orang lain. Pesan-pesan berkode dalam kriptografi yang tidak disembunyikan,

walaupun tidak dapat dipecahkan, akan menimbulkan kecurigaan. Seringkali, steganografi dan kriptografi digunakan secara bersamaan untuk menjamin keamanan pesan rahasianya.

Sebuah pesan steganografi (*plaintext*), biasanya pertama-tama dienkripsikan dengan beberapa arti tradisional, yang menghasilkan *ciphertext*. Kemudian, covertext dimodifikasi dalam beberapa cara sehingga berisi *ciphertext*, yang menghasilkan *stegotext*. Contohnya, ukuran huruf, ukuran spasi, jenis huruf, atau karakteristik *covertext* lainnya dapat dimanipulasi untuk membawa pesan tersembunyi; hanya penerima (yang harus mengetahui teknik yang digunakan) dapat membuka pesan dan mendekripsikannya.



Gambar 1 Kategori Steganografi (penulis – edit, 2017)



Gambar 2 Proses Steganografi (penulis – edit, 2017)

Format gambar digital memiliki 2 (dua) parameter:

- *spatial resolution* : pixels x pixels
- *color encoding* : bits / pixel

Misalkan asumsikan terdapat gambar dengan resolusi 100 x 100 dan color encoding 24 bits (R=8 bits, G=8 bits, B=8 bits) per pixel, maka color encoding akan mampu mewakili 0 .. 16.777.215 (mewakili 16 juta warna), dan ruang disk yang dibutuhkan = 100 * 100 * 3 byte (karena RGB) = 30.000 bytes = 30 KB atau 100 * 100 * 24 bits = 240000 bits.

Pada steganografi, image yang biasa digunakan adalah image 24 bit, karena image tersebut dapat menyediakan space yang besar untuk disisipi oleh data. Pixel penyusun image ini tersusun atas 3 warna primer yaitu merah, hijau, dan biru (RGB). Masing-masing warna primer tersusun atas 1 byte data. Untuk image 24 bit berarti menggunakan 3 bytes per pixel untuk merepresentasikan nilai warna pixel. 3 bytes data ini dapat berupa hexadesimal, desimal, atau biner.

Table 3 Jenis Image dan ukuran bitnya (Rafael C. Gonzalez et.all, 2002)

Jumlah Bit	Keterangan
1	Binary-value image (0 – 1)
8	Gray level (0 – 255)
16	High colour (216)
24	True Colour (224)
32	True Colour (232)

2.1.1. Sifat dan Cara Kerja Steganografi

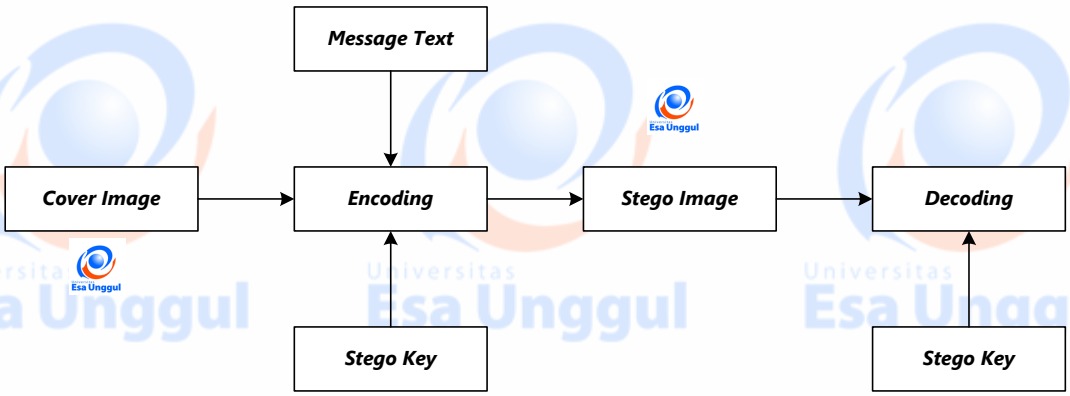
Pada penelitian media yang digunakan yaitu file format image, adapun beberapa pengertian yang akan digunakan pada aplikasi steganografi yang akan dibuat (M. Husain, 2013):

(a) *Embedde- message* : pesan yang disembunyikan dapat dalam format teks atau *image*.

(b) *Cover-image* : pesan yang digunakan untuk menyembunyikan *embedded message* .

(c) *Stego-image* : pesan yang sudah berisi pesan *embedded message*.

(d) *Stego-key* : kunci digunakan berupa sebuah algoritma yang digunakan untuk melakukan penyisipan dan ekstraksi pesan rahasia dari *stego image*



Gambar 3 Diagram Proses *Embedded* (encoding) dan *Extraction* (decoding)

2.1.2. Manfaat Steganografi

Steganograpi juga dapat digunakan sebagai cara untuk menjaga atas kerahasiaan informasi yang berharga, untuk menjaga data tersebut dari kemungkinan sabotasi, pencuri, atau dari pihak yang tidak berwenang dan menjaga kualitas image (MSE dan PSNR) sebelum dan sesudah proses steganografi dengan metode algorutma LSB

2.2. Kriteria Steganografi

Penyembunyian data rahasia ke dalam image digital akan mengubah kualitas image tersebut. Kriteria yang harus diperhatikan dalam penyembunyian data (Munir,2015) antara lain ;

(1) *Fidelity*. Mutu image penampung tidak jauh berubah. Setelah penambahan data rahasia, image hasil steganografi masih terlihat dengan baik. Pengamat tidak mengetahui kalau di dalam image tersebut terdapat data rahasia.

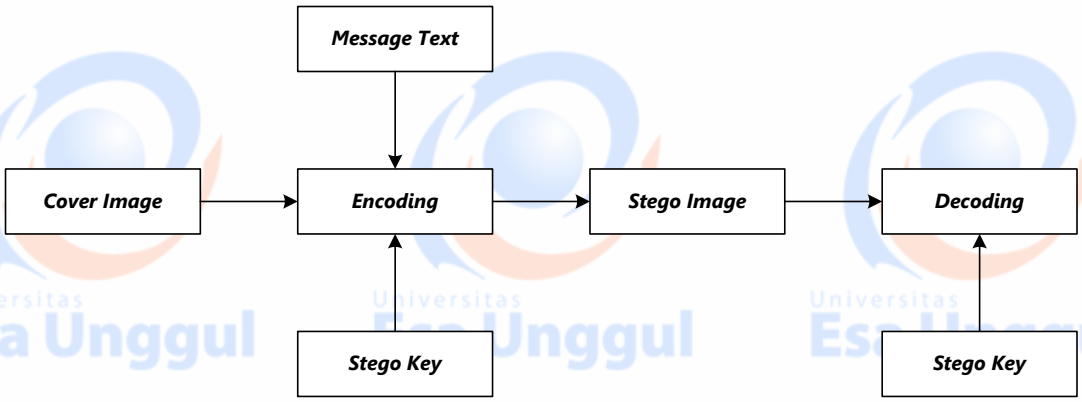
(2) *Robustness*. Data yang disembunyikan harus tahan terhadap manipulasi yang dilakukan pada image penampung (seperti pengubahan kontras, penajaman, pemampatan, rotasi, perbesaran gambar, pemotongan (*cropping*), enkripsi, dan sebagainya). Bila pada image dilakukan operasi pengolahan image, maka data yang disembunyikan tidak rusak.

(3) *Recovery*. Data yang disembunyikan harus dapat diungkapkan kembali (*recovery*), dimana tujuan steganografi adalah data hiding, maka sewaktu-waktu data rahasia di dalam image penampung harus dapat diambil kembali untuk digunakan lebih lanjut.

2.3. Metode LSB pada media *image* (gambar)

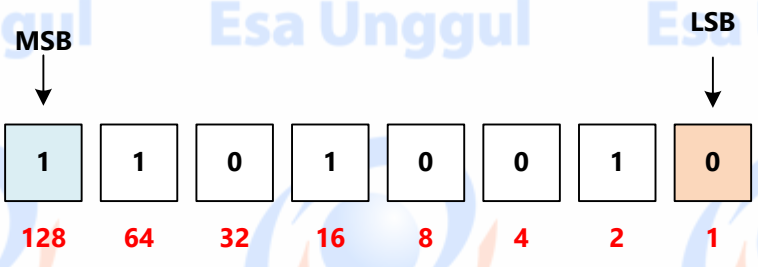
Metode ini bekerja dengan cara mengganti bit terakhir dari masing-masing piksel dengan pesan yang akan disisipkan. LSB mempunyai kelebihan yakni ukuran gambar tidak akan berubah. Sedangkan kekurangannya adalah pesan/data yang akan disisipkan terbatas, sesuai dengan ukuran image. Salah satu *cover image* yang dapat digunakan untuk menyembunyikan pesan adalah image digital warna 24 bit. Setiap pixel pada image warna 24 bit memiliki warna yang merupakan

kombinasi dari tiga warna dasar *Red, Green, Blue* (RGB). Sedangkan satu pixel image warna 24 bit diwakili oleh tiga byte, dimana masing-masing byte merepresentasikan warna *Red, Green, Blue*. Penyisipan pesan ke dalam *cover image* dinamakan encoding, sedangkan ekstraksi pesan dari *stego* image dinamakan decoding.



Gambar 4 Diagram Proses *Embedded* (encoding) dan *Extraction* (decoding)

Metode *Least Signification Bit* (LSB) merupakan metode yang cukup sederhana dalam melakukan proses steganografi. Selain itu, proses penyisipan dan ekstraksi dari metode ini juga relatif cukup cepat. Metode LSB menyisipkan pesan ke dalam *cover image* pada bit yang paling kurang berarti. Untuk LSB 1 bit, bit yang disisipi adalah bit ke-8 untuk setiap byte, perubahan nilai desimal dari satu byte menjadi satu nilai lebih tinggi, atau satu nilai lebih rendah, atau sama dari nilai desimal dari satu byte sebelum terjadi penyisipan. Sedangkan untuk metode LSB 2 bit, bit yang disisipi adalah bit ke-7 dan bit ke-8 untuk setiap byte. Sehingga perubahan nilai pada 2 bit terakhir berkisar antara nol sampai dengan tiga dari nilai byte sebelum terjadi penyisipan. Untuk menyisipkan pesan ke dalam pixel yang ditentukan secara acak.



Gambar 5 Ilustrasi MSB dan LSB

Sebuah image merupakan kumpulan dari titik-titik yang disebut pixel. Pada image warna 24 bit, setiap
pixel berukuran 3 byte dimana setiap byte mewakili warna dari setiap komponen *Red, Green, Blue.* Misalkan terdapat 2 pixel, dimana nilai intensitas setiap warna pada setiap pixel setelah dikonversikan ke dalam biner memberikan nilai biner sebagai berikut

00100111	**11101001**	**11001000**
00100111	**11001000**	**11101001**

Untuk menyisipkan sebuah **karakter "F" dengan bilangan biner 01000110 (kode ASCII 70)** ke dalam 2 pixel image warna tersebut, setiap 2 bit dari pesan yang dimulai dari MSB disisipkan ke dalam 2 bit LSB dari setiap byte image warna.

Hasil penyisipannya memberikan nilai pixel baru sebagai berikut:

00100101	**11101000**	**11001001**
001001110	**11001000**	**11101001**

Contoh lain penggunaan metode LSB ;

Misal pesan yang akan disisipkan **5 bit = 11010**, maka jumlah byte yang digunakan = 5 byte

0010110 11001001 11111001 10001000 10100011

(byte yang digunakan untuk penyisipan pesan)

Proses penyisipan pesan

11010

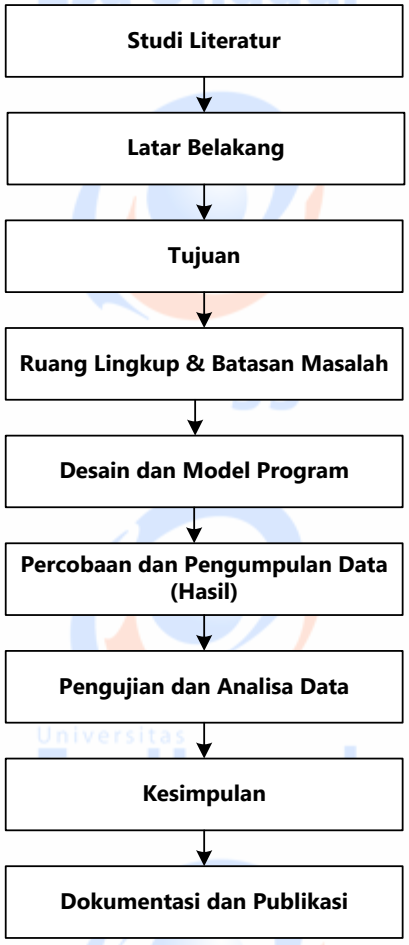
Hasil penyisipan menjadi ;

00101101 **1100100**1 **1111100**0 **1000100**1 **1010001**0

BAB III

METODOLOGI PENELITIAN

3.1. Tahapan Penelitian



Gambar 6 Tahapan perancangan penelitian

Penelitian ini bertujuan untuk mengimplementasikan metode LSB pada proses penyisipan pesan gambar ke dalam image gambar menggunakan perangkat lunak bebasis matriks (MATLAB). Metode LSB bekerja dengan mengganti bit terakhir kode biner image dengan kode biner pesan sebagai nilai derajat keabuan image pada akhir image (*stego*).

Tahapan penelitian diatas secara garis besar yang dilakukan adalah sebagai berikut:

(a) Studi literatur

Studi literatur adalah studi pustaka yang membahas teknik penyembunyian, ekstraksi, enkripsi, dekripsi dengan algoritma yang bersangkutan.

(b) Tahapan operasional

Tahapan dengan steganografi algoritma metode LSB, menuangkan tujuan, ruang lingkup dan batasan masalah yang akan diharapkan dalam penelitian.

(c) Perancangan program (model) dan *coding*

Perancangan program yaitu membuat rancangan interface serta membuat diagram algoritma steganografi metode LSB. Pengkodean dilakukan untuk mengimplementasikan perancangan program ke dalam bahasa pemrograman Matlab (M-File).

(d) Pengujian dan Analisa Data

Pengujian dan dilanjutkan dengan menganalisa data terhadap program yang telah dibuat.

(e) Penyusunan dan pendokumentasian serta publikasi

Penyusunan laporan hasil analisis dibuat ke dalam format penulisan ilmiah (sesuai ketentuan), mendokumentasikan (upload ke SIMHRM-UEU) dan mempublikasikan pada journal ilmiah.

3.2. Metode LSB dalam proses Encoding dan Decoding

3.2.1. LSB Encoding (*Cover Image*)

Dalam melakukan metode LSB pada proses *encoding* dan *decoding* dengan menggunakan *stego-key*. Pada proses encoding, dilakukan penyisipan pesan rahasia ke dalam *cover image* , hasilnya adalah *stego image*.

Masukan : *Cover image*

Luaran : *Stego image*

Proses :

(1) Transformasi image ke dalam bentuk biner

(2) Mengubah sekuensial (urutan) biner dari pesan menjadi rangkaian bit yang disimpan dalam bentuk array satu dimensi.

(3) Menentukan letak pixel pada *cover image* yang akan disisipi pesan

(4) Transformasi nilai setiap *pixel* dari *cover image* ke dalam nilai *Red*, *Green*, dan *Blue* (RGB).

(5) Transformasi nilai RGB pada setiap letak piksel yang diperoeh dari hasil langkah 2 ke dalam bentuk biner

(6) Sisipkan setiap 2 bit pesan ke dalam bit 7 dan 8 pada setiap nilai RGB

(7) Simpan *cover image* yag sudah disisipi pesan menjadi file *stego image*.

3.2.2. LSB Decoding *(Stego Image)*

Pada proses decoding dilakukan ekstrasi pesan dari *stego image*, hasilnya adalah pesan teks.

Masukan : *Stego image*,

Luaran : *Cover Image dan Teks*

Proses :

(1) Bangkitkan m bilangan acak menggunakan algoritma LSB untuk mendapatkan letak pixel pada *stego* image yang disisipi pesan.

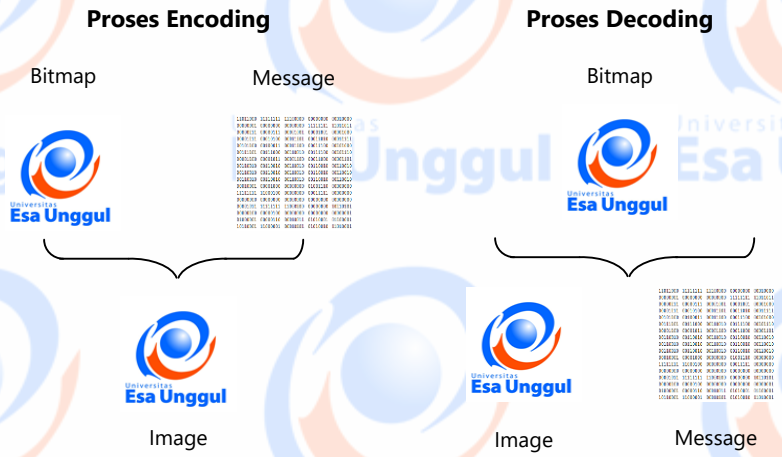
(2) Transformasi nilai setiap pixel dari *stego* image ke dalam nilai RGB.

(3) Transformasi nilai RGB pada setiap letak piksel yang disisipi pesan ke dalam bentuk biner.

(4) Salin setiap 2 bit pesan pada bit 7 dan 8 dari setiap nilai RGB hasil langkah 3 ke dalam suatu array satu dimensi.

(5) Transformasikan setiap 8 bit menjadi bentuk karakter.

(6) Tampilkan pesan.



Gambar 7 Proses Encoding dan Decoding

3.3 Proses Penelitian

Dalam penelitian steganografi dengan metode LSB pada media yang bersifat digital dengan format JPG dan BMP dengan ukuran resolusi tertentu, diuraikan pada langkah-langkah sebagai berikut;

(1) Mempersiapakan digital image dalam format JPG dan BMP (studi kasus logo Universitas Esa Unggul)

(2) Program aplikasi yang digunakan dalam metode pembuatan dana tau perancangan dengan aplikasi Matlab.

(3) Metode yang digunakan dalam penggunaan steganography adalah penggunaan metode LSB dalam pengamanan data (file).

(4) Memproses image RGB menjadi image gray dan image binary, dengan menggunakan aplikasi matlab serta mempersiapkan teks pada bit tertentu yang akan disisipkan dalam proses steganography.

(5) Menampilkan hasil proses steganografi sebelum dan sesudahnya dalam satu tampilan.

(6) Menghitung dan menganalisa membahas perubahan ukuran file image sebelum dan setelah disisipkan pesan teks serta kualitas image (faktor MSE dan PSNR)

3.4 Rancangan Steganografi Metode LSB

Program yang dalam dimaksudkan dalam penulisan ini adalah program yang mana disertai dengan user interface, sehingga mudah untuk digunakan. Program dirancang dengan menggunakan bantuan Matlab, alasan digunakannya Matlab adalah karena lengkapnya fasilitas yang dimiliki oleh Matlab dalam melakukan operasi operasi matrik ataupun array dalam sebuah data. Seperti yang kita ketahui bahwa Elemen Elemen unsur warna (RGB/Gray/Binary) pada citra sebenarnya dapat diartikan sebagai sebuah matrik, oleh karena itu dengan menggunakan Matlab. Operasi pemodifikasian menjadi lebih mudah. Selain itu pada Matlab juga terdapat Tools khusus yang menangani media media berupa citra digital. Program didesain tanpa menggunakan User, dan dilengkapi dengan halaman untuk melakukan analisis terhadap citra atau gambar inputan dan dilengkapi pula dengan halaman yang digunakan untuk menyisipkan data rahasia. Dalam program dilengkapi juga dengan informasi mengenai nilai elemen elemen citra inputan, baik itu citra penampung maupun citra stego.

Dan melakukan dalam menganalisa perubahan ukuran file image sebelum dan setelah disisipkan pesan teks serta kualitas image (faktor MSE dan PSNR) apakah akan mengalami distorsi dalam image asli-nya dan teks yang disispkan.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Proses Embedding dan Extraction

4.1.1 Cara Kerja Metode LSB.

Konsep kerja metode Least Significant Bit (LSB) dalam melakukan penyisipan pesan ke dalam media image adalah melakukan modifikasi terhadap bit-bit setiap pixel image yang menjadi cover (image penampung pesan). Bit paling akhir (least) dari setiap pixel akan digantikan dengan bitbit dari pesan yang akan disembunyikan. Proses pengungkapan atau pengambilan pesan dari dalam image penampung dilakukan dengan mengambil bit-bit pixel image hasil yang berada pada posisi akhir, kemudian dikonversikan menjadi karakter. Proses utama dalam metode LSB adalah proses embedding dan proses ekstraction.

4.1.2. Proses *Embedding* (Encoding)

Berdasarkan metode LSB, proses embedding pesan pada cover yang dijadikan sebagai penampung yaitu dengan tahapan memilih image cover, baca nilai desimal cover, konversi ke dalam bilangan biner, kemudian masukkan pesan, setelah itu jumlah pesan yang dijadikan sebagai kunci digabungkan dengan pesan yang ingin disembunyikan, maka hasil gabungan pesan dan kunci menjadi pesan yang akan disisipkan ke dalam image cover, setelah itu nilai pesan dikonversi ke dalam bilangan biner. Apabila jumlah biner pesan dapat ditampung semua pada image cover berdasarkan kriteria perhitungan jumlah piksel dibagi dengan 8 bit, maka dapat dilakukan proses penukaran bit. Setelah disisipkan pesan pada cover, hasil dari nilai biner cover baru dikonversi kembali ke dalam bilangan desimal dan kemudian dipetakan menjadi image baru atau *stego*image.

4.1.3. Proses *Extraction* (Decoding)

Pesan Berdasarkan Metode LSB. Adapun Proses extraction pesan dari hasil *stego*image, yaitu dengan tahapan masukkan *stego*image, setelah itu baca nilai piksel *stego*image dan konversi ke

bilangan biner, kemudian ambil nilai kunci dari 8 bit LSB biner image awal *stego*image dan dikonversi ke bilangan desimal, kemudian nilai kunci dikalikan dengan 8 bit untuk mengambil nilai bit pesan. Setelah itu ambil bit LSB dari setiap elemen piksel dimulai dari bit ke-9 hingga sejumlah perkalian kunci dengan 8 bit lalu ditambahkan dengan 8 bit kunci LSB, kemudian kelompokkan nilai bi-bit LSB menjadi 8 bit perkelompok, kemudian dikonversi ke dalam bilangan desimal. Setelah didapatkan bilangan desimal dari biner pengelompokan, konversi ke karakter, karakter yang dihasilkan tersebutlah yang menjadi pesan yang telah disembunyikan sebelumnya.

4.2 Kualitas Image

Steganografi image yang baik setidaknya harus memenuhi 4 kriteria yaitu tidak terlalu dapat dibedakan secara inderawi (*imperectible*), mutu image hasil steganografi masih cukup baik (*fidelity*), tahan terhadap operasi image dasar seperti rotasi dan perubahan ukuran image (robustness), dan pesan yang disisipi dapat dipisahkan kembali (*recoverable*). Kemudian melakukan pengujian dengan menghitung MSE dan PSNR. MSE *(Mean Square Error).*adalah nilai error kuadrat rata-rata antara image asli (cover-image) dengan image hasil penyisipan (*stego*-image). PSNR *(Peak Signal to Noise Ratio)* merupakan perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau (*noise*) yang berpengaruh pada sinyal tersebut. PSNR biasanya diukur dalam satuan decibel (dB). PSNR digunakan untuk mengetahui perbandingan kualitas image cover (asli) sebelum dan sesudah disisipkan pesan. Dan secara persamaan empirik direpresentasikan sebagai berikut ;

$$MSE = \frac{1}{M*N}\sum_{x=1}^{M} \quad \sum_{y=1}^{N}(S_{xy} - C_{xy})^2 \quad \text{..... [1]}$$

$$PNSR = 10 \log_{10} \frac{C_{MSE}^2}{MSE} \text{..... [2]}$$

Dimana:

- Cmax adalah nilai pixel terbesar pada keseluruhan image.
- x dan y adalah koordinat suatu titik pada image.
- M dan N adalah dimensi dari image.
- S adalah image tersisipi (*stego*-image)

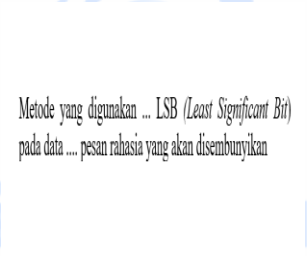
- C adalah image asli (*cover image*)

Untuk menentukan PSNR, terlebih dahulu harus ditentukan nilai MSE. Nilai PSNR ditentukan oleh besar atau kecilnya nilai MSE yang terjadi pada image. Semakin besar nilai PSNR, semakin baik pula hasil yang diperoleh pada tampilan image hasil. Sebaliknya, semakin kecil nilai PSNR, maka akan semakin buruk pula hasil yang diperoleh pada tampilan image hasil (*stego*). Nilai PSNR jatuh dibawah 30 dB mengindikasikan qualitas yang relative rendah, dimana distorsi yang dikarenakan penyisipan terlihat jelas, tetapi kualitas *stego*-image yang tinggi berada pada nilai 40dB dan diatasnya (Cheddad, 2010).

4.3. Hasil dan Luaran

Hasil dan luaran yang dilakukan meliputi aspek ukuran (size) - image cover dan image hasil (stegano image - dan kualitas image berdasarkan rumus empirik PSNR dan MSE image hasil (stegano image) terhadap image cover. Diperoleh hasil sebagai berikut

(a) Ukuran file tetap saat proses embedding (cover) dan ekstraksi (*stego*).
(b) Ukuran piksel/resolusi image tidak mengalami perubahan (tetap)
(c) Tidak mengalami perubahan kualitas image (MSE dan PSNR)

Cover image **(400x400)**		*Stego* Image (400x400)
		
242 KB (JPG) 468 KB (BMP)	**Teks yang disisipkan (13,1 KB)**	**242 KB (JPG) 468 KB (BMP)**

Gambar 8 Proses Steganografi dengan Metode Algoritma LSB

Gambar 9 Tampilan 3 Image yang diuji dalam proses steganografi

Tabel 4 Hasil Steganografi metode LSB file image JPG

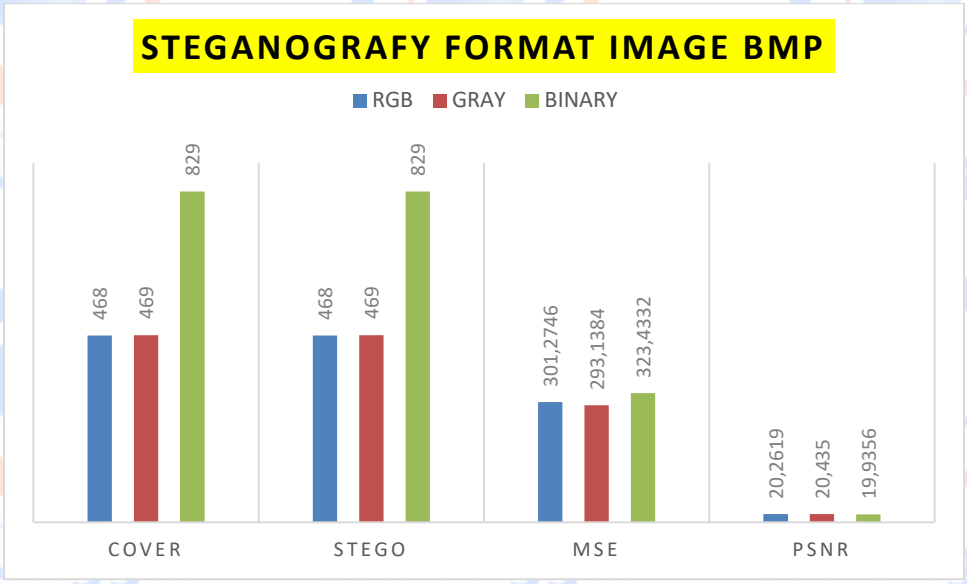
No.	Gambar (JPG)	Pesan (Text)	Size file (Kb)		Kualitas (dB)		Keterangan
			Cover	*Stego*	MSE	PSNR	
1	**RGB Cover 400x400 (24,2 KB)**	Metode yang digunakan ... LSB *(Least Significant Bit)* pada data .... pesan rahasia yang akan disembunyikan **13.1 KB 347 (ns) 407 (ws)**	**24,2**	**24,2**	**300,3893**	**20,3352**	Dari proses bahwa MSE > PSNR image tidak mengalami kerusakan (noise)
2	**Gray Cover 572x 495 (15.2 KB)**	kualitas image berdasarkan rumus empirik PSNR dan MSE steganografi **11.6 KB 46 (ns) 53 (ws)**	**15.2**	**15.2**	**306,8605**	**20,2633**	Dari proses bahwa MSE > PSNR image tidak mengalami kerusakan (noise)
3	**Biner Cover 400x400 (20.8 KB)**	perubahan ukuran file image sebelum dan setelah disisipkan pesan teks **11,5 KB 60 (ns) 69 (ws)**	**20.8**	**20.8**	**316,6011**	**19,9930**	Dari proses bahwa MSE > PSNR image tidak mengalami kerusakan (noise)

Analisa dari proses pengujian pada tabel 3 di atas dapat dilihat bahwa, semakin rendah Nilai MSE maka akan semakin baik, dan semakin besar nilai PSNR maka semakin baik kualitas *image* steganografi. Hal ini menunjukkan bahwa penyisipan file pesan dalam *image* cover adalah tidak mempengaruhi kualitas *image stego* dalam penglihatan manusia.

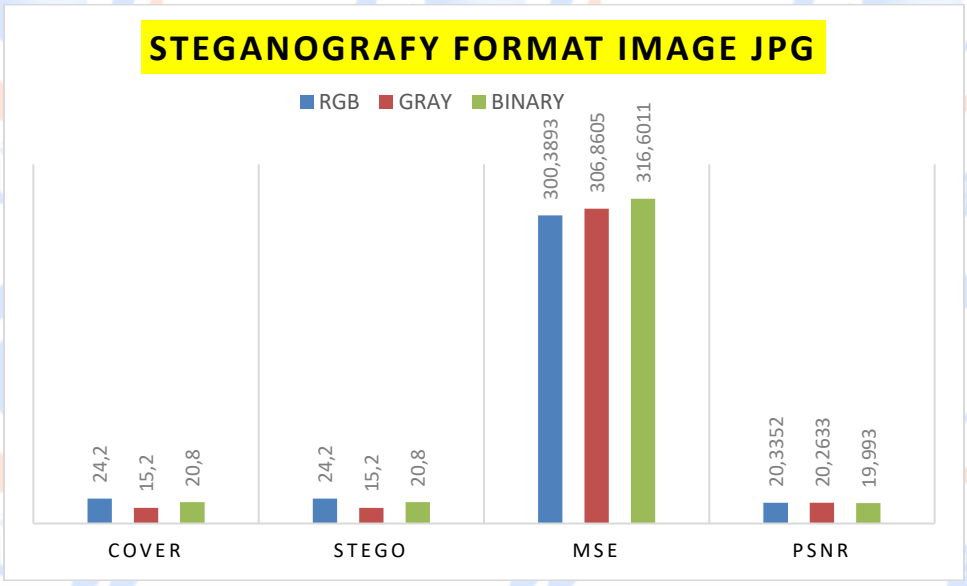
Tabel 5 Hasil Steganografi metode LSB file image BMP

No.	Gambar (JPG)	Pesan (Text)	Size file (Kb)		Kualitas (dB)		Keterangan
			Cover	*Stego*	MSE	PSNR	
1	 **RGB Cover 400x400 (468 KB)**	Metode yang digunakan ... LSB *(Least Significant Bit*) pada data .... pesan rahasia yang akan disembunyikan **13.1 KB 347 (ns) 407 (ws)**	**468**	**468**	**301,2746**	**20,2619**	Dari proses bahwa MSE > PSNR image tidak mengalami kerusakan (noise)
2	 **Gray Cover 572x 495 (469 KB)**	kualitas image berdasarkan rumus empirik PSNR dan MSE steganografi **11.6 KB 46 (ns) 53 (ws)**	**469**	**469**	**293,1384**	**20,4350**	Dari proses bahwa MSE > PSNR image tidak mengalami kerusakan (noise)
3	 **Biner Cover 400x400 (829 KB)**	perubahan ukuran file image sebelum dan setelah disisipkan pesan teks **11,5 KB 60 (ns) 69 (ws)**	**829**	**829**	**323,4332**	**19,9356**	Dari proses bahwa MSE > PSNR image tidak mengalami kerusakan (noise)

Analisa dari tabel 4 di atas dapat dilihat bahwa semakin rendah Nilai MSE maka akan semakin baik, dan semakin besar nilai PSNR maka semakin baik kualitas *image* steganografi. Hal ini menunjukkan bahwa penyisipan file pesan dalam *image* cover adalah tidak mempengaruhi kualitas *image stego* dalam penglihatan manusia.



Gambar 10 Perbanding Image RGB – GRAY – BINARY format BMP



Gambar 11 Perbanding Image RGB – GRAY – BINARY format JPG

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan, maka disimpulkan bahwa :

(a) Proses penyisipan metode LSB menggantikan hanya pada bit terakhir dari *image cover*, dan image setelah disisipkan pesan hanya mengalami sedikit penurunan kualitas yang tidak begitu berpengaruh secara signifikan bila dilihat oleh mata manusia, dan pada ukuran size file tidak mengalami perubahan (*cover* maupun *stego*)

(b) Image dengan ukuran 400x400 (RGB) dan 572x495 (Gray dan Biner) dapat menampung pesan sebanyak 480.000 (RGB) dan 566.280 (Gray dan Biner) karakter dengan metode algoritma LSB.

(c) Perubahan image pada compressing *image* pada format JPG mapun BMP yang dialami image masih terlihat jelas, hal ini sangat berguna dalam menjaga kerahasiaan data sehingga tidak banyak orang yang menyadarinya

5.2 Saran

Untuk penelitian lebih lanjut bagi yang berminat ini dapat menggunakan format *image* (yang lain, dengan menggunakan *feature* GUI Matlab agar dioperasikan dengan cara yang lebih optimal dan automacillay serta dibuat dalam bentuk database yang ter-repository hasil proses *cover image*, *stego-image* dan kualitas *image* nya dalam *back-end*.

Dan saran yang lain dapat pula menggunakan metode steganografi yang lain, misalnya *Algorithms and Transformation, End-Of-File, Redundant Pattern Encoding dan Spread Spectrum.*

DAFTAR PUSTAKA

Champakamala .B.S, Padmini.K, Radhika .D.K, “Least Significant Bit algorithm for image steganography”, International Journal of Advance Computer Technology, volume 3, number 4, August 2014

Bandyopadhyay, Samir Kumar, and Sarthak Parui. "A Method for Public KeyMethod of Steganography." International Journal of Computer Applications (IJCA), 7-10; 2010.

Katzenbeisser, Stefan and Fabien A.P. Petitcolas, “Information Hiding Techniques for Steganography and Digital Watermarking”, Artech House Inc. computing library, 2000, ISBN 1-58053-035-4

Stallings, William Cryptography and Network Security Principles and Practices, Fourth Editio, 2005, ISBN-10: 0-13-187316-4

R. Popa, An Analysis of Steganographic Techniques, The "Politehnica" University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering,http://ad.informatik.unifreiburg.de/mitarbeiter/will/dlib_bookmarks/digital-watermarking/popa/popa.pdf, 1998

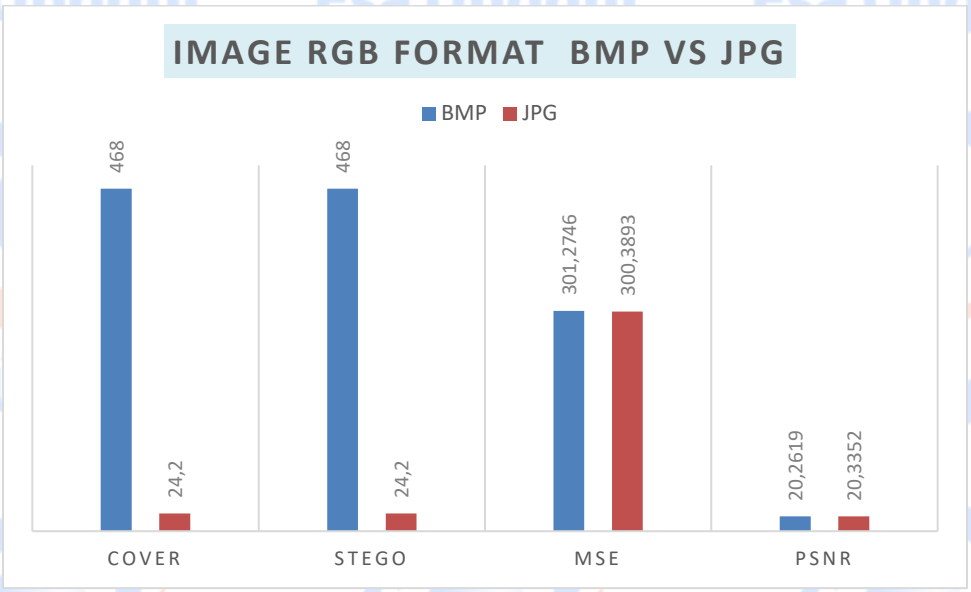
Munir, Rinaldi. Diktat Kuliah IF5054 Kriptografi. Bandung: Penerbit ITB. 2006

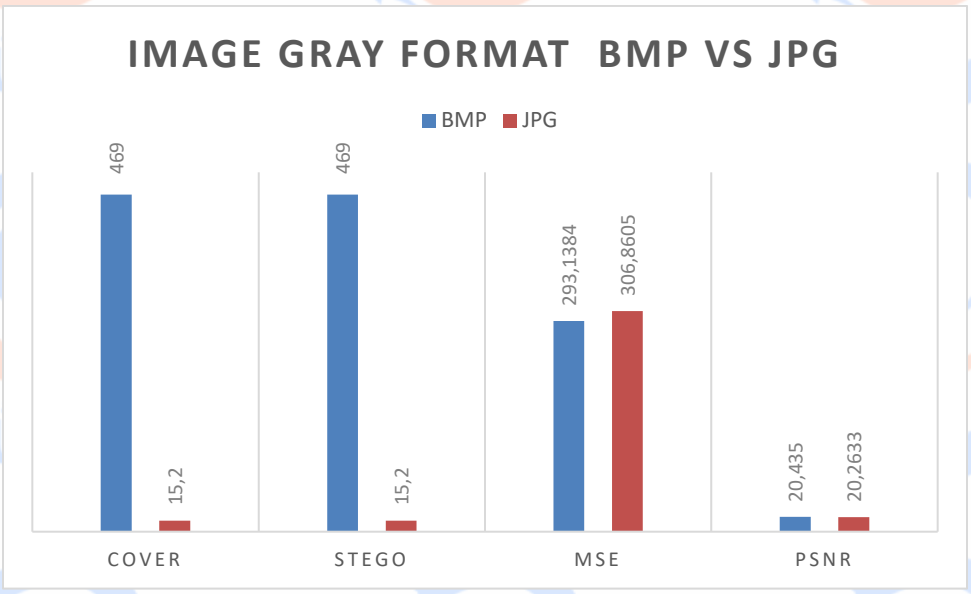
T. Morkel et.all, “ An Overview Of Image Steganography”, Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa, -

Ravinder Reddy Ch and Roja Ramani, “The Process of Encoding and Decoding of Image Steganography using LSB Algorithm”, IJCSET Volume 2, Issue 11, 1488-1492, November 2012

LAMPIRAN 1

PERBANDINGAN IMAGE RGB, GRAY DAN BINARY PADA FORMAT BMP DAN JPG





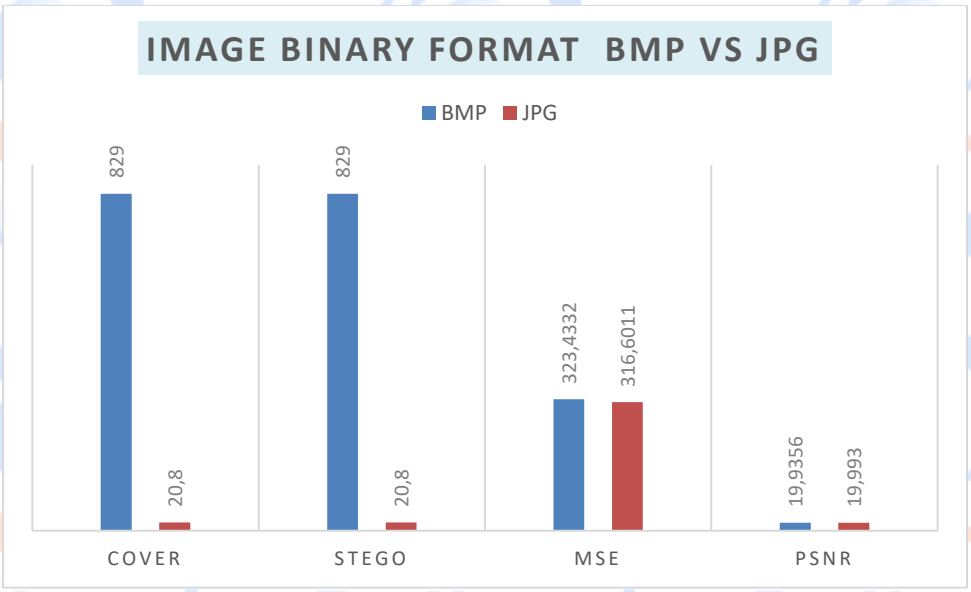


IMAGE BINARY FORMAT BMP VS JPG
BMP
JPG
829
20,8
829
20,8
323,4332
316,6011
19,9356
19,993
COVER
STEGO
MSE
PSNR