Implementasi Steganografi dengan Menggunakan Metode *Masking and Filtering* untuk Menyisipkan Gambar ke dalam Citra Digital

Farikhatur Ro'isa[1], I Made Suartana[2]

[1] Jurusan Teknik Informatika/Teknik Informatika, Universitas Negeri Surabaya
[2] Jurusan Teknik Informatika/Teknik Informatika, Universitas Negeri Surabaya
[1]Farikhaturroisa@mhs.unesa.ac.id
[3]madesuartana@unesa.ac.id

***Abstrak*— Untuk menjaga kerahasiaan informasi rahasia agar tidak dapat diketahui oleh pihak ketiga dan hanya diketahui oleh pihak tertentu saja, maka dibutuhkan sebuah cara yang digunakan untuk menyembunyikan informasi rahasia tersebut dengan menggunakan teknik Steganografi. Steganografi adalah teknik menyembunyikan pesan ke dalam media lainnya (*cover image*), seperti *image, video, audio,* ataupun *video* sehingga secara kasat mata media penampung yang telah ditambahakan informasi rahasia terlihat sama tidak ada perbedaan dengan sebelum ditambahkan informasi rahasia. Pada penelitian ini, Steganografi diterapkan dengan menyisipkan gambar sebagai pesan rahasia ke media yang juga berupa gambar. Citra digital adalah salah satu media penampung yang banyak digunakan dalam penyembunyian data, akan tetapi saat dilakukan modifikasi gambar informasi rahasia rentan rusak atau hilang. Metode *masking and filtering* termasuk dalam *spatial domain*, pada metode ini penyisipan informasi rahasia dilakukan dengan cara memanipulasi nilai *luminance* pada gambar yang digunakan sebagai media penampung. *Masking* berfungsi untuk menandai tempat pada gambar yang bisa disisipkan. *Filtering* berfungsi untuk melewatkan nilai pada bagian yang telah ditandai. Hasil yang diperoleh dari penelitian ini adalah kualitas gambar setelah disisipi dengan informasi rahasia tidak mengalami perubahan yang berarti, setelah dilakukan proses penyisipan informasi rahasia kedalam gambar dan dilakukan proses ekstraksi, informasi rahasia dapat diungkap kembali, dengan adanya proses *editing* terhadap gambar maka dapat merusak informasi rahasia yang sudah disisipkan dan mengakibatkan informasi rahasia tidak terdeteksi dan tidak dapat diekstraksi, dan waktu yang dibutuhkan untuk proses ekstraksi De*coding*) lebih cepat dibandingkan dengan waktu yang dibutuhkan untuk proses penyisipan (*Encoding*).**

Kata Kunci*— Steganografi, *Masking and Filtering,* Citra Digital, *Encoding, Decoding.

I. PENDAHULUAN

Steganografi yaitu ilmu dan seni penyembunyian pesan rahasia (*hiding message)* ke media tertentu oleh karena itu pesan rahasia tidak dapat dilihat oleh pihak lain kecuali pihak yang mengirim dan menerima pesan. Steganografi memerlukan dua syarat yaitu media penampung yang akan digunakan untuk tempat menyembunyikan data dan data rahasia yang akan digunakan sebagai data yang akan disembunyikan. Media penampung pesan berupa audio, image, video, serta teks. Penggunaan Steganografi sebagai salah satu cara yang dapat digunakan untuk melindungi data yang sangat penting dikarenakan data-data tersebut bersifat rahasia. Teknik dari steganografi ini adalah pengirim menyembunyikan pesan rahasia kedalam media penampung supaya tidak diketahui oleh orang ketiga yang tidak berwenang akan mengakses pesan tersebut, penerima harus mengekstraksi untuk dapat mengambil pesan rahasia yang sudah dikirim oleh pengirim.

Beberapa penelitian mengenai steganografi telah banyak dilakukan sebelumnya diantaranya adalah penelitian yang dilakukan oleh Za'imatun Niswati [2] yang berjudul steganografi berbasis Least Significant Bit (LSB) untuk menyisipkan gambar ke dalam citra gambar. Ada pula penelitian yang dilakukan oleh Dedi Darwis pada tahun 2016 yang berjudul implementasi Teknik Steganografi Least Significant Bit (LSB) dan Kompresi untuk Pengamanan Data Pengiriman Surat Elektronik. Masking and filtering tergolong kedalam Spatial Domain. Menyembunyikan pesan dikerjakan dengan cara mengatur nilai luminance gambar. Penerapannya dalam gambar yang memiliki warna atau berskala keabuan (Grayscale). Masking mempunyai fungsi untuk menandai tempat dalam gambar yang dapat dilakukan penyisipan pesan, tetapi filtering mempunyai fungsi memasukkan nilai pada tempat yang sudah diberi tanda. Metode Masking and filtering ini terbatas dalam gambar 24 bit warna atau berskala keabuan (Grayscale). Metode tersebut hampir sama dengan metode watermark, yang mana sebuah gambar ditandai akan digunakan sebagai penyembunyian suatu pesan rahasia. Keadaan tersebut boleh dilakukan, misalkan melalui cara merubah tingkat luminance dalam sebagian gambar.

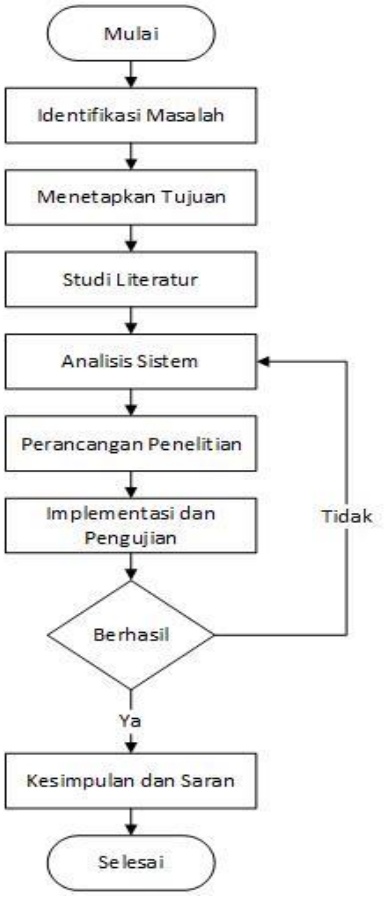
Masking and filtering tergolong kedalam Spatial Domain. Menyembunyikan pesan dikerjakan dengan cara mengatur nilai luminance gambar. Penerapannya dalam gambar yang memiliki warna atau berskala keabuan (Grayscale). Masking mempunyai fungsi untuk menandai tempat dalam gambar yang dapat dilakukan penyisipan pesan, tetapi filtering mempunyai fungsi memasukkan nilai pada tempat yang sudah diberi tanda. Metode Masking and filtering ini terbatas dalam gambar 24 bit warna atau berskala keabuan (Grayscale). Metode tersebut hampir sama dengan metode watermark, yang mana sebuah gambar ditandai akan digunakan sebagai

penyembunyian suatu pesan rahasia. Keadaan tersebut boleh dilakukan, misalkan melalui cara merubah tingkat luminance dalam sebagian gambar.

Metode masking lebih bagus daripada metode LSB dikarenakan metode masking membolehkan adanya kompresi, pemotongan, dan sebagian proses yang dilakukan dalam gambar. Teknik masking melewatkan informasi ke dalam tempat tertentu sehingga pesan tersebut dapat semakin terselubung dibanding hanya sekedar menutupi tingkatan noise pada gambar. Oleh karena itu, dalam penelitian ini digunakan steganografi dengan menggunakan metode Masking and Filtering untuk menyisipkan gambar kedalam citra digital untuk tujuan proses penyisipan dengan metode masking and filtering terhadap ukuran gambar. Salah satu alternatif untuk menyimpan pesan rahasia ke dalam sebuah wadah citra digital adalah steganografi pada citra digital. Steganografi juga berfungsi untuk mengirimkan pesan rahasia, dikarenakan karakter dari steganografi itu sendiri yang susah untuk ditemui letaknya.

II. METODOLOGI PENELITIAN

Tahapan penelitian steganografi dengan menggunakan metode *Masking and filtering* untuk menyisipkan gambar kedalam citra digital dapat dilihat pada gambar 1:



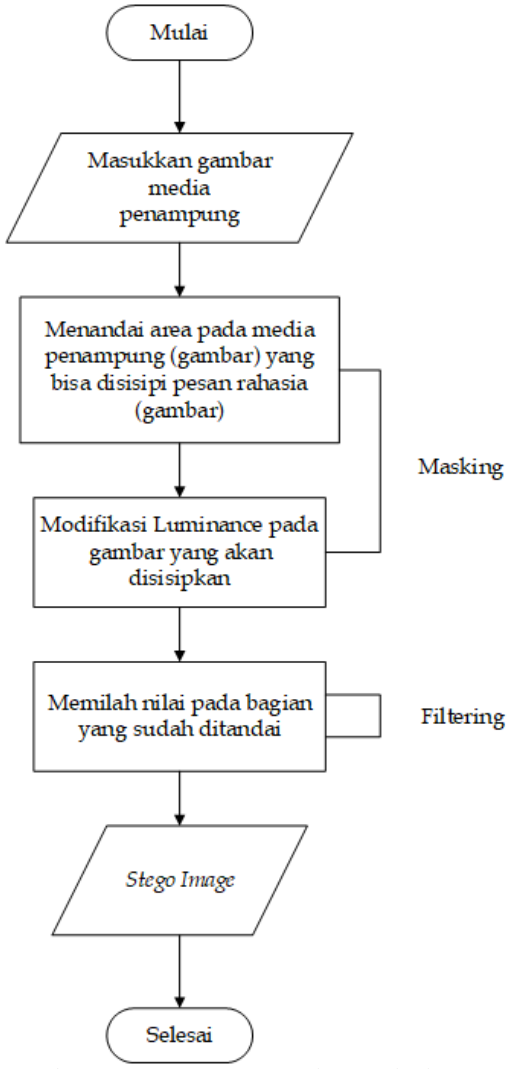
Gbr. 1 Alur Jalan Penelitian

Penelitian ini bertujuan untuk membandingkan metode Steganografi yaitu metode *masking and filtering* dalam penyisipan informasi rahasia (gambar) ke dalam gambar, membandingkan antara gambar sesudah dan sebelum disisipi dengan informasi rahasia (gambar), mengetahui kualitas gambar setelah disisipi dengan informasi rahasia (gambar), menganalisis penyebaran RGB (*Red, Green, Blue*) pada gambar yang disisipkan, dan menganalisis jumlah waktu yang digunakan untuk melakukan proses penyisipan dan pengekstrakan gambar.

A. *Metode Masking and Filtering*

Proses masking yang dilakukan pada citra mempunyai tujuan untuk menandai area pada citra yang akan disisipi dengan pesan tetapi proses filtering mempunyai tujuan untuk melintaskan nilai pada bagian yang telah berikan tanda. Pada proses Masking and Filtering dibagi menjadi dua yaitu penyisipan pesan dan pengekstrakan pesan. Berikut ini adalah Flowchart dari metode Masking and Filtering.[1]

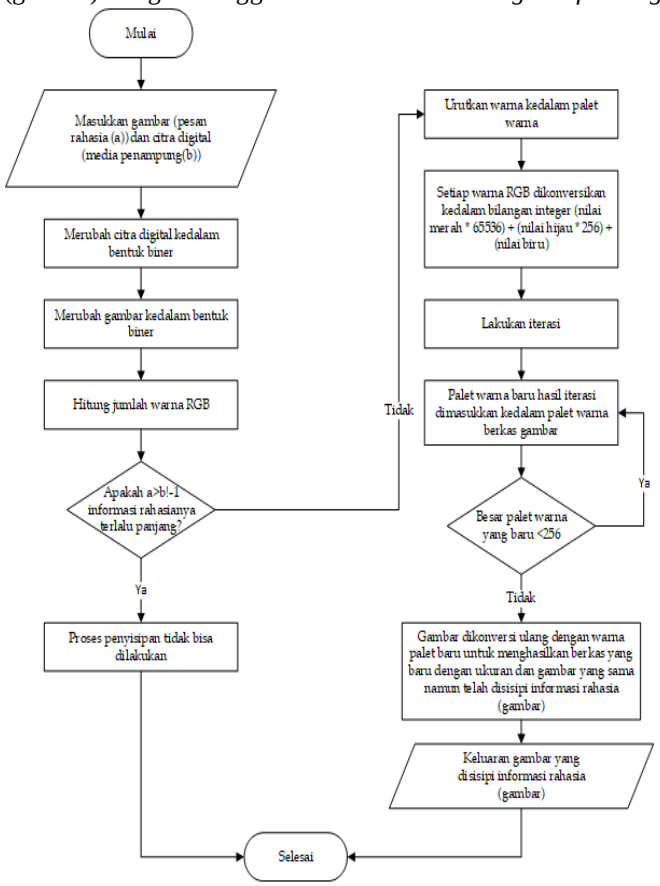
Teknik masking yaitu dengan cara menempatkan informasi dalam tempat yang significant maka pesan yang tersembunyi itu lebih menyatu dengan *cover image* dibandingkan dengan proses menyembunyikan yang ada pada level "noise".



Gbr. 2 *Flowchart Metode* Masking and Filtering

B. *Proses Penyisipan Informasi Rahasia (Encoding)*

Berikut ini adalah Flowchart penyisipan informasi rahasia (gambar) dengan menggunakan metode *masking and filtering:*



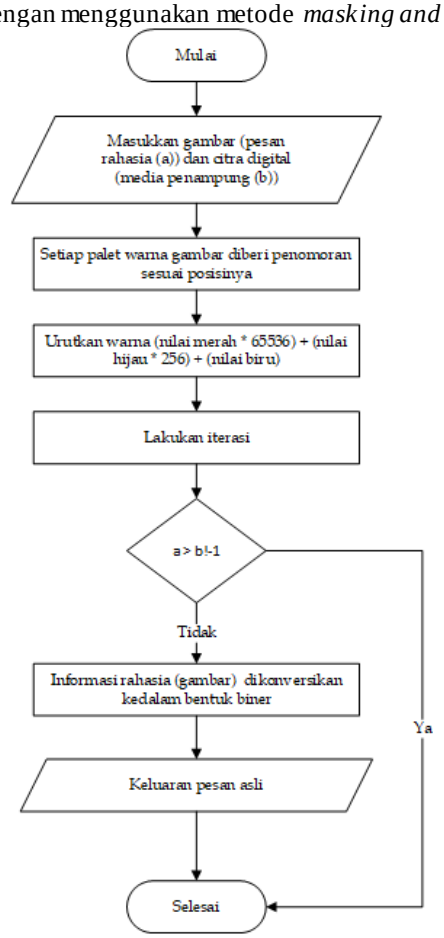
Gbr. 2 Flowchart Proses Penyisipan (*Encoding*)

Berikut ini adalah proses dari penyisipan isi informasi rahasia yang berupa gambar kedalam sebuah citra digital: [3]

1. Menentukan informasi rahasia (gambar) mana yang disisipkan, selanjutnya mengubah gambar ke bentuk biner.
2. Kemudian di depan rangkaian bilangan biner ditambahkan angka 1 selanjutnya mengkonversikan rangkain itu dalam bentuk desimal. Kebanyakan bilangan tersebut adalah bilangan yang besar. Bilangan tersebut disebut dengan bilangan a.
3. Selanjutnya menentukan tempat gambar yang akan disisipi oleh citra digital. Menghitung berapa jumlah warna pada gambar. Jumlah tersebut disebut sebagai b. Jika a > b! – 1 bahwa gambar terlalu panjang oleh karena itu proses penyisipan tidak dapat dilakukan.
4. Kemudian mengurutkan warna yang ada di palet warna sesuai urutan naturalnya. Dimana tiap-tiap warna yang mempunyai format RGB dikonversikan dengan menggunakan rumus:
   (nilai merah * 65536) + (nilai hijau * 256) + (nilai biru)
   selanjutnya dilakukan pengurutan palet warna dengan didasarkan pada besar bilangan integer yang menggantikan warna tersebut.
5. Selanjutnya melakukan iterasi pada variable i dengan nilai i dari 1 hingga b. Disetiap warna urutan b – 1 akan dipindah ke tempat yang baru yakni a mod i, selanjutnya a akan dibagi dengan i.
6. Kemudian palet warna baru yang dihasilkan dari iterasi pada langkah yang sudah dilakukan sebelumnya akan dimasukkan ke dalam palet warna berkas citra digitalnya. Jika salah satu tempat diisi oleh dua buah warna seharusnya warna yang sebelumnya akan ditempati warna tersebut maka akan dipindah ke satu tempat yang ada di tempat berikutnya.
7. Selanjutnya jika hasil dari palet warna yang baru lebih kecil daripada 256, lalu palet warna urutan yang terakhir diisi dengan warna yang ada diakhir dari palet warna yang sebelumnya.
8. Setelah itu mengkompresi kembali berkas citra digital menggunakan palet warna yang baru, digunakan agar dihasilkan berkas yang baru yang mempunyai ukuran dan gambar yang sama tetapi dalam keadaan gambar tersebut sudah disisipi informasi rahasia (gambar).
9. Keluaran gambar yang disisipi informasi rahasia (gambar).

C. *Proses Ekstraksi Informasi Rahasia(Decoding)*

Berikut ini adalah Flowchart penyisipan informasi rahasia (gambar) dengan menggunakan metode *masking and filtering*:



Gbr. 3 Flowchart Ekstraksi (*Encoding*)

Berikut ini adalah proses dari penyisipan isi informasi rahasia yang berupa gambar kedalam sebuah citra digital: [3]

1. Memasukkan gambar yang digunakan sebagai pesan rahasia dan citra digital yang digunakan sebagai media penampung.
2. Kemudian disetiap palet warna gambar diberikan penomoran yang sesuai dengan posisinya.
3. Selanjutnya mengurutkan warna palet
   (nilai merah * 65536) + (nilai hijau * 256) + (nilai biru)
4. Selanjutnya lakukan iterasi nilai i dari 0 ke b sampai 1.
   Dimana
   a = a (b-1) + warna ke 1
   nilai i dari 1 ke b-1
   iterasi ke b
   jika a > b!-1 maka akan keluar
   jika k > nilai warna maka k – 1
   mengkonversikan m ke dalam bentuk biner
5. Keluaran yang dihasilkan pesan asli

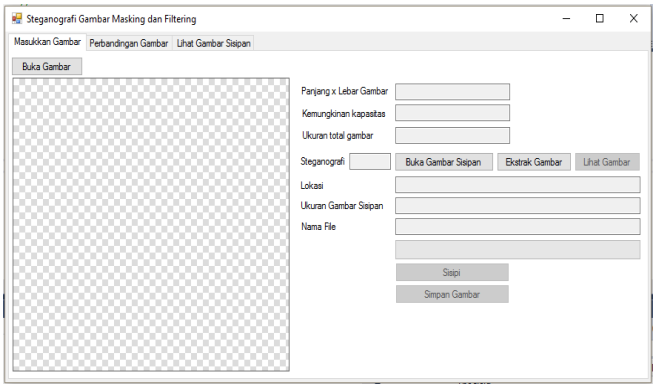
III. HASIL DAN PEMBAHASAN

A. *Hasil Implementasi*

Implementasi dari Steganografi dengan menggunakan metode *masking and filtering* untuk menyisipkan gambar kedalam citra digital dapat dilihat dibawah ini:

1. Tampilan utama

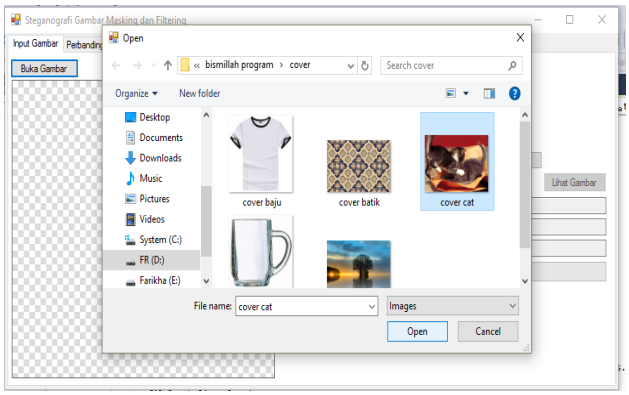
   Pertama kali saat menjalankan aplikasi steganografi dengan metode masking and filtering ini, tampilan yang akan diperlihatkan ke pengguna adalah seperti pada gambar 4:



Gbr. 4 Tampilan Awal

2. Tampilan Buka Gambar

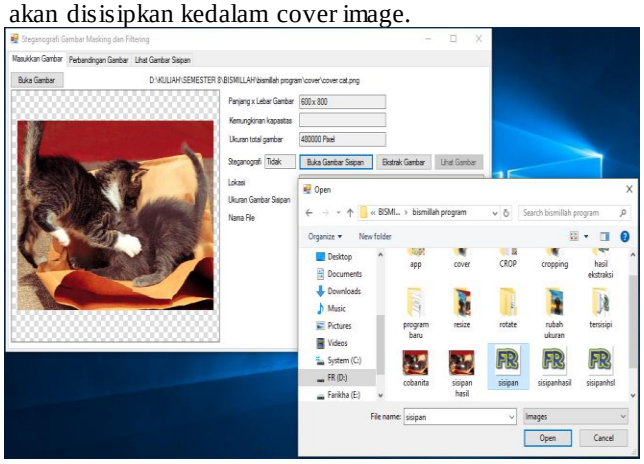
   Untuk membuka gambar mana yang akan dijadikan cover image, maka yang harus dilakukan tekan tombol “Buka Gambar”, sehingga akan muncul lokasi dimana file akan disimpan yang digunakan untuk memilih gambar yang akan dijadikan cover image.



Gbr. 5 Tampilan Buka Gambar

3. Tampilan Buka Gambar yang Disisipkan

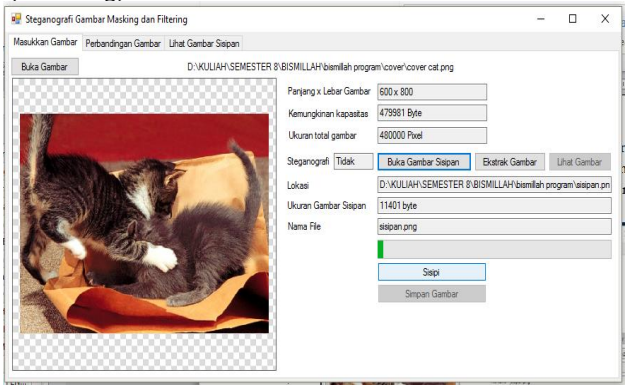
   Untuk membuka gambar mana yang akan dijadikan sebagai informasi rahasia yang akan disisipkan kedalam cover image, maka yang harus dilakukan tekan tombol “Buka Gambar Sisipan”, sehingga akan muncul lokasi diman file akan disimpan yang digunakan untuk memilih gambar yang akan dijadikan sebagai informasi rahasia yang akan disisipkan kedalam cover image.



Gbr. 6 Tampilan Buka Gambar yang Disisipkan

4. Tampilan Proses Penyisipan (*Encoding*)

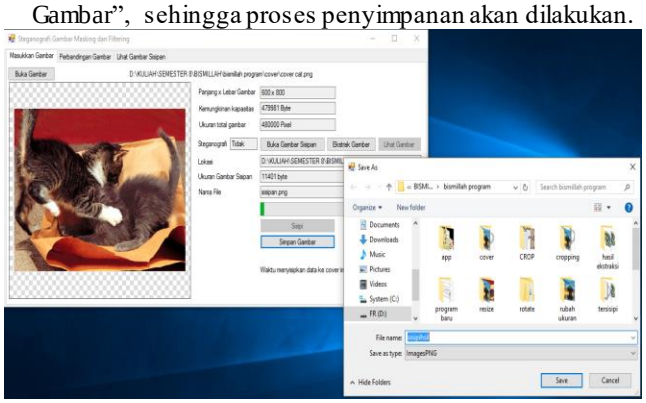
   Untuk melakukan proses penyisipan informasi rahasia (gambar) kedalam cover image, maka yang harus dilakukan tekan tombol “Sisipi”, sehingga proses penyisipan (Encoding) akan dilakukan.



Gbr. 7 Tampilan Proses Penyisipan (*Encoding*)

5. Tampilan Simpan Gambar yang Disisipi

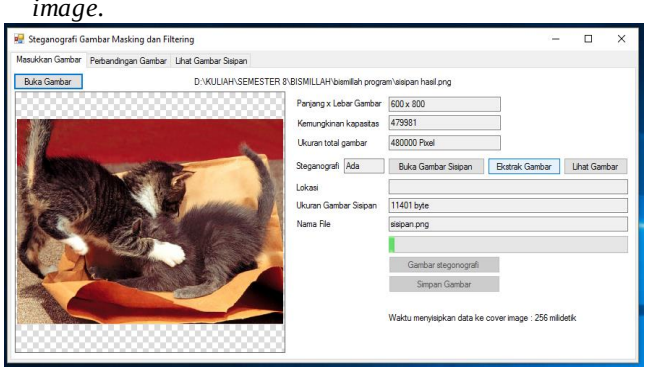
Untuk melakukan proses penyimpanan informasi rahasia (gambar) yang sudah disisipkan kedalam cover image, maka yang harus dilakukan tekan tombol "Simpan Gambar", sehingga proses penyimpanan akan dilakukan.



Gbr. 8 Tampilan Simpan Gambar yang Disisipi

6. Tampilan Proses Ekstraksi (*Decoding*)

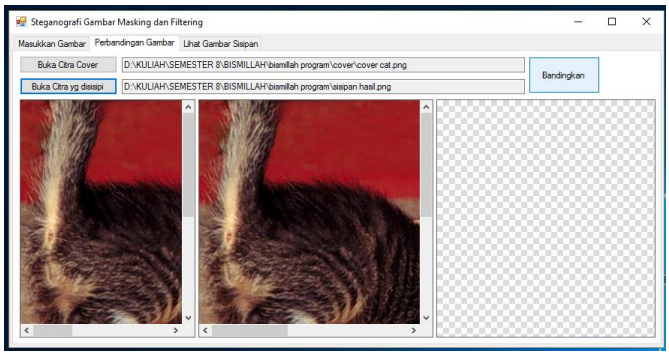
Untuk melakukan proses ekstraksi informasi rahasia (gambar) yang sudah disisipkan kedalam cover image, pertama tekan tombol "Buka Gambar Tersisipi" sama dengan proses buka gambar yang sudah dilakukan pada saat memasukkan gambar yang akan dijadikan *cover image*.



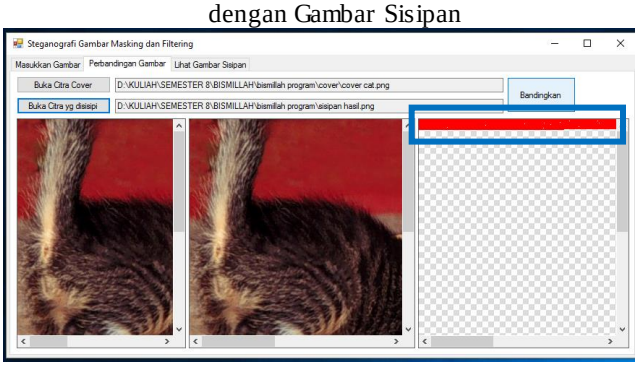
Gbr. 9 Tampilan Proses Ekstraksi (*Decoding*)

7. Tampilan Membandingkan Cover Image dengan Gambar Hasil Sisipan

Untuk melakukan proses membandingkan anatara cover image dengan informasi rahasia (gambar), pertama tekan tombol "Buka Citra Cover" digunakan untuk membuka gambar yang akan dijadikan cover image, kemudian tekan tombol "Buka Citra yang Disisipi" digunakan untuk membuka gambar yang sudah disisipi dengan informasi rahasia (gambar), dan yang terakhir tekan tombol "Bandingkan" untuk memulai proses membandingkan hasil gambar sebelum disisipi informasi rahasia (gambar) dan sesudah disisipi informasi rahasia (gambar).



Gbr. 10 Tampilan Membandingkan *Cover Image* dengan Gambar Sisipan



Gbr. 11 Tampilan Hasil Perbandingan

B. *Pengujian Kualitas Gambar*

Pengujian terhadap kualitas gambar yang sudah disisipkan kedalam cover image apakah menimbulkan kecurigaan atau tidak. Pengujian ini dapat dikatakan berhasil jika kualitas gambar yang dihasilkan tidak mengalami perubahan yang besar jika dibandingkan dengan gambar asli sebelum dilakukan penyisipan gambar ke dalam cover image. Gambar yang dihasilkan tidak berbeda jauh dengan gambar asli.

C. *Pengujian Ketepatan Penyisipan Informasi Rahasia (Gambar) ke dalam Gambar*

Proses penyisipan dapat dikatakan berhasil jika ukuran informasi rahasia (gambar) lebih kecil dibandingkan dengan ukuran cover image. Jika ukuran informasi rahasia (gambar) yang disisipkan lebih besar dari kapasitas cover image maka tidak dapat dilakukan proses penyisipan.

TABEL I
HASIL KETEPATAN PENYISIPAN INFORMASI RAHASIA (GAMBAR) KE DALAM GAMBAR

Gambar Penampung	Ukuran Sebelum Disisipi	Kemungkinan Kapasitas	Informasi Rahasia (Gambar)	Ukuran Informasi Rahasia (Gambar)	Hasil	Ukuran Sesudah Disisipi
Cover cat.png	724 KB	479980	Sisipan.png	10.9 KB	Berhasil	1.07 MB
Cover baju.png	20.6 KB	50605	Sisipan.png	10.9 KB	Berhasil	41 KB
Cover batik.png	615 KB	264152	Sisipan.png	10.9 KB	Berhasil	662 KB
Cover pemandangan.png	0.97 KB	609581	Sisipan.png	10.9 KB	Berhasil	1.32 MB
Cover gelas.png	352 KB	271422	Sisipan.png	10.9 KB	Berhasil	370 KB

D. *Pengujian Gambar bisa Diekstraksi Kembali*

Pengujian ini bertujuan untuk membuktikan bahwa gambar yang sudah disisipi dapat diekstraksi kembali. Jika pengujian tersebut dilakukan dengan benar maka informasi

rahasia (gambar) dapat diekstarksi dan hasilnya sama dengan informasi rahasia (gambar) yang disisipkan melalui proses penyisipan sebelumnya.

TABEL II
HASIL EKSTRAKSI INFORMASI RAHASIA (GAMBAR)

Gambar Penampung	Ukuran Sebelum Disisipi	Kemungkinan Kapasitas	Informasi Rahasia (Gambar)	Ukuran Informasi Rahasia (Gambar)	Hasil
Cover cat.png	724 KB	479980	Sisipan.png	10.9 KB	Berhasil
Cover baju.png	20.6 KB	50605	Sisipan.png	10.9 KB	Berhasil
Cover batik.png	615 KB	264152	Sisipan.png	10.9 KB	Berhasil
Cover pemandangan.png	0.97 KB	609581	Sisipan.png	10.9 KB	Berhasil
Cover gelas.png	352 KB	271422	Sisipan.png	10.9 KB	Berhasil

E. *Pengujian Modifikasi Hasil Steganografi*

Pengujian ini dilakukan dengan cara memotong (*cropping*) beberapa bagian gambar yang dilsisipi dengan informasi rahasia (gambar) dapat dilihat pada tabel III, merubah ukuran (*Resize*) gambar yang sudah disisipi dengan informasi rahasia (gambar) dapat dilihat pada tabel IV, memutar (*Rotate*) gambar yang sudah disisipi dengan informasi rahasia (gambar) dapat dilihat pada tabel V.

TABEL III
HASIL MODIFIKASI (*CROPPING*)

No	Nama Gambar yang Disisipi	Ukuran Sebelum di *crop (pixel)*	Ukuran Sesudah di *crop (pixel)*	Hasil
1	Cat tersisipi.png	800 x 600	760 x 570	(Ekstraksi Gagal)
2	Baju tersisipi.png	225 x 225	200 x 225	(Ekstraksi Gagal)
3	Batik tersisipi.png	626 x 422	626 x 392	(Ekstraksi Gagal)
4	Pemandangan tersisispi.png	960 x 635	880 x 555	(Ekstraksi Gagal)
5	Gelas tersisipi.png	521 x 521	515 x 513	(Ekstraksi Gagal)

TABEL IV
HASIL MODIFIKASI (*RESIZE*)

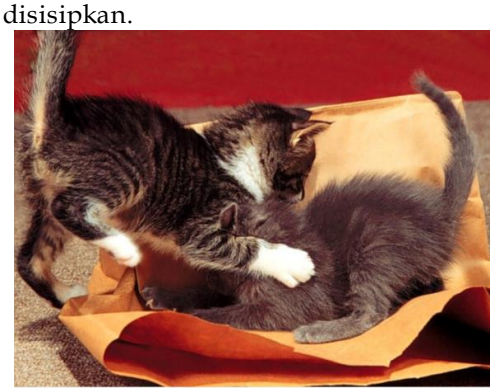
No	Nama Gambar yang Disisipi	Ukuran (*pixel*)		Perubahan Ukuran	Hasil
		Sebelum	Sesudah		
1	Cat tersisipi.png	800 x 600	400 x 300	-50%	Tidak dapat mendeteksi gambar sisipan (Ekstraksi Gagal)
2	Baju tersisipi.png	225 x 225	225 x 225	+20%	Tidak dapat mendeteksi gambar sisipan (Ekstraksi Gagal)
3	Batik tersisipi.png	626 x 422	313 x 211	-50%	Tidak dapat mendeteksi gambar sisipan (Ekstraksi Gagal)
4	Pemandangan tersisipi.png	960 x 635	768 x 508	-20%	Tidak dapat mendeteksi gambar sisipan (Ekstraksi Gagal)
5	Gelas tersisipi.png	521 x 521	573 x 573	-10%	Tidak dapat mendeteksi gambar sisipan (Ekstraksi Gagal)

TABEL V
HASIL MODIFIKASI (*ROTATE*)

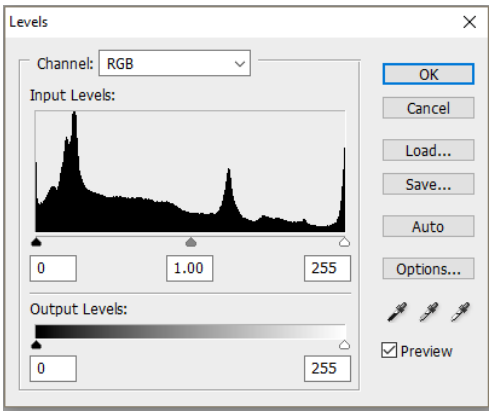
No	Nama Gambar yang Disisipi	Arah Putaran	Hasil
1	Cat tersisipi.png	- 90° putar ke kanan - 180° putar ke kanan - 270° putar ke kanan - 90° putar ke kiri - 180° putar ke kiri - 270° putar ke kiri	Tidak dapat mendeteksi gambar sisipan (Ekstraksi Gagal)
2	Baju tersisipi.png	- 90° putar ke kanan - 180° putar ke kanan - 270° putar ke kanan - 90° putar ke kiri - 180° putar ke kiri - 270° putar ke kiri	Tidak dapat mendeteksi gambar sisipan (Ekstraksi Gagal)
3	Batik tersisipi.png	- 90° putar ke kanan - 180° putar ke kanan - 270° putar ke kanan - 90° putar ke kiri - 180° putar ke kiri - 270° putar ke kiri	Tidak dapat mendeteksi gambar sisipan (Ekstraksi Gagal)
4	Pemandangan tersisipi.png	- 90° putar ke kanan - 180° putar ke kanan - 270° putar ke kanan - 90° putar ke kiri - 180° putar ke kiri - 270° putar ke kiri	Tidak dapat mendeteksi gambar sisipan (Ekstraksi Gagal)
5	Gelas tersisipi.png	- 90° putar ke kanan - 180° putar ke kanan - 270° putar ke kanan - 90° putar ke kiri - 180° putar ke kiri - 270° putar ke kiri	Tidak dapat mendeteksi gambar sisipan (Ekstraksi Gagal)

F. *Pengujian Analisis Histogram*

Pengujian ini bertujuan untuk mengetahui penyebaran RGB (*Red, Green, Blue*) pada gambar yang disisipkan.



Gbr. 4 Gambar yang Disisipi



Gbr. 5 Histogram Gambar yang Disisipi

G. *Pengujian Analisis Waktu*

Pengujian ini bertujuan untuk mengetahui waktu yang diperlukan dalam proses penyisipan dan ekstraksi informasi rahasia (gambar).

Pengujian dapat dilakukan dengan membandingkan waktu untuk mengetahui waktu yang diperlukan dalam proses penyisipan dan ekstraksi informasi rahasia (gambar).

TABEL VI

HASIL ANALISIS WAKTU

Gambar Penampung (*Cover Image*)	Ukuran	Kemungkinan Kapasitas	Informasi Rahasia (Gambar)	Ukuran	Waktu penyisipan (*Encoding*)	Waktu Ekstraksi (*Decoding*)
Cover cat.png	724 KB	479980 byte	Sisipan.png	10.9 KB	270 milidetik	200 milidetik
Cover baju.png	20.6 KB	50605 byte	Sisipan.png	10.9 KB	182 milidetik	174 milidetik
Cover batik.png	615 KB	264152 byte	Sisipan.png	10.9 KB	429 milidetik	166 milidetik
Cover pemandangan.png	0.97 MB	609581 byte	Sisipan.png	10.9 KB	287 milidetik	277 milidetik
Cover gelas.ong	352 KB	271422 byte	Sisipan.png	10.9 KB	195 milidetik	146 milidetik

IV. KESIMPULAN

Berdasarkan dari hasil penelitian yang sudah dilakukan oleh peneliti yaitu tentang Steganografi dengan menggunakan metode *masking and filtering* untuk menyisipkan gambar ke dalam citra digital dapat diambil kesimpulan bahwa penyisipan informasi rahasia (gambar) ke dalam citra digital dapat dilakukan dengan menggunakan metode *masking and filtering* tanpa menimbulkan kecurigaan pihak lainnya dan dengan adanya penyisipan informasi rahasia (gambar) ke dalam citra digital mengubah ukuran gambar yang sudah disisipi dengan informasi rahasia (gambar).

UCAPAN TERIMA KASIH

Ucapan syukur tetap tercurahkan kepada Allah SWT, yang memberikan kemudahan dalam proses penyusunan jurnal ini dan semua pihak yang selalu memberi semangat dan dukungan sehingga dapat terselesaikannya jurnal ini dengan baik.

REFERENSI

[1] Wendro, E. N. (2011). *Analisis Metode Masking-Filtering dalam Pengamanan Data Teks.* Skripsi S1 Medan: Univeritas Sumatera Utara.

[2] Niswati, Z. (Tanpa Tahun). Steganografi Berbasis Least Significant Bit (LSB) untuk Menyisipkan Gambar kedalam Citra Digital. Jurnal Faktor Exacta, 5(No 2), 181-191.

[3] Safa, E. (2014). Analisis Metode Masking-Filtering dalam Penyisipan Data Teks. Majalah Ilmiah Informasi dan Teknologi Ilmiah (INTI), IV(No 1), 53-58.