SNASTIKOM 2020
Program Studi Teknik Informatika, Fakultas Teknik dan Komputer, Universitas Harapan Medan
website: www.snastikom.com

MODIFIKASI PENYISIPAN PESAN PADA BIDANG WARNA CITRA DENGAN TEKNIK STEGANOGRAFI

Nadra Nur Aini Harahap
Universitas Harapan Medan, Nadranuraini23@gmail.com

Fera Damayanti
Universitas Harapan Medan, Jln. HM Joni No. 70, feradamayantii@gmail.com

Yessi Fitri Annisah Lubis
Universitas Harapan Medan, Jln. HM Joni No. 70, yessy.annisa@gmail.com

Abstract

The awareness of the importance of message security in today's digital era is marked by the development of information security applications. The need for security will increase if the information contains privacy values or certain interests. What's more, there are more and more acts of misuse of information (hacking) in cyberspace, causing this information to be protected from interference from unauthorized parties. One of the methods used is by applying steganography techniques. Steganography is a method that inserts information into other data media (such as digital images). The most commonly used steganographic method is the Least Significant Bit (LSB) method. The conventional LSB method works by inserting a message into the last bit (the eighth bit of the image color element) which is used as a cover to accommodate the message. In this study, the modification of the LSB method will be applied based on the selection of the image color fields, namely R (Red), G (Green), B (Blue) or RGB as well as modifications to the number of the last bit to be inserted (maximum 3 bits). The results of the implementation and testing of the system show that the selection of the color field and the number of bits to be inserted greatly affects the number of bits available from the cover image. The test results on the lenna.bmp image measuring 768 Kb, then the number of bits available if you only choose the Red (R) or Green (G) or Blue (B) color field and the number of bits inserted is 1 bit, then the maximum number of bits is obtained. that can be inserted is 32768 bits (4096 characters) message.

Keywords:
Digital Image, RGB Color Plane, Steganography, LSB, PSNR

Abstrak

Kesadaran pentingnya keamanan pesan pada era digital saat ini ditandai dengan berkembangnya aplikasi keamanan informasi. Kebutuhan keamaanan akan semakin meningkat jika informasi tersebut mengandung nilai-nilai privasi ataupun kepentingan tertentu. Terlebih lagi, aksi penyalahgunaan informasi (hacking) dalam dunia maya sekarang semakin banyak menyebabkan informasi tersebut harus dilindungin dari gangguan pihak-pihak yang tidak bekepentingan. Salah satu cara yang digunakan yaitu dengan menerapkan teknik steganografi. Steganografi merupakan suatu metode yang menyisipkan informasi ke dalam media data lainnya (seperti citra digital). Metode steganografi yang sering digunakan yaitu metode Least Significant Bit (LSB). Metode LSB konvensional bekerja dengan cara menyisipkan pesan kedalam bit terakhir (bit ke delapan dari elemen warna citra) yang dijadikan cover untuk menampung pesan. Pada penelitian ini akan diterapkan modifikasi metode LSB berdasarkan pemilihan pada bidang warna citra yaitu R (Red), G (Green), B (Blue) atau RGB serta modifikasi terhadap jumlah bit terakhir yang akan disisipkan (maksimal 3 bit). Hasil implementasi dan pengujian sistem menunjukkan bahwa pemilihan bidang warna dan jumlah bit yang akan disisipkan sangat berpengaruh terhadap jumlah bit yang tersedia dari cover citra. Hasil pengujian pada citra lenna.bmp yang berukuran 768 Kb, maka jumlah bit yang tersedia jika hanya memilih pada bidang warna Red (R) atau Green (G) atau Blue (B) serta jumlah bit yang disisipkan 1 bit, maka diperoleh maksimal jumlah bit yang dapat disisipkan yaitu sebesar 32768 bit (4096 karakter) pesan.

Kata Kunci:
Citra Digital, Bidang Warna RGB, Steganografi, LSB, PNSR

1. PENDAHULUAN

Keamanan suatu pesan pada era digital ini makin vital peranannya dalam berbagai aspek kehidupan, terutama untuk suatu pesan yang memiliki nilai lebih dibandingkan dengan pesan yang lain[1]. Upaya yang ilakukan untuk

melindungi kerahasiaan pesan dapat dilakukan dengan memberikan pengamanan terhadap pesan tersebut. Terdapat berbagai cara yang dapat digunakan untuk melindungi suatu pesan, misalnya dengan teknik kriptografi. Kriptografi adalah suatu ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikan pesan ke dalam bentuk yang tidak dapat dimengerti lagi maknanya [2]. Metode kriptografi dapat menjamin keamanan pesan dengan cara mengenkripsi pesan tersebut menjadi format yang tidak terbaca yang disebut ciphertext. Penggunaan metode enkripsi tidak selalu menjamin keamanan data, karena ciphertext yang dihasilkan dari enkripsi mengundang kecurigaan, dengan kata lain dapat dianggap sebagai hal yang tidak lazim. Hal yang menjadi kelemahan metode kriptografi adalah bahwa bentuk pesan hasil enkripsi akan menimbulkan kecurigaan pihak ketiga bahwa informasi yang dikirimkan adalah rahasia atau penting [3]

Guna menghindari permasalahan tersebut maka digunakan teknik steganografi. Teknik steganografi menggunakan dua media yang berbeda secara bersamaan, dimana salah satunya berfungsi sebagai media yang berisikan informasi informasi rahasia (dapat juga disebut secret file) dan yang lain berfungsi sebagai media pembawa informasi tersebut (carrier file) [4]. Media yang dapat digunakan sebagai pembawa informasi dapat berupa file citra, audio maupun video, namun pada penelitian ini digunakan citra digital sebagai carrier file. Penggunaan carrier file berupa citra digital dipilih karena adanya batasan kepekaan manusia dalam hal visualisasi. Hasil keluaran citra digital dari steganografi ini memiliki bentuk persepsi yang sama dengan aslinya, tentunya persepsi disini sebatas kemampuan indera manusia, tetapi tidak oleh komputer atau pengolah digital lainnya. Konsep steganografi adalah menyisipkan (embedding) dan ekstraksi (extracting) pada sebuah media citra seperti foto [5].

Steganografi pada citra digital dapat dijadikan alternatif untuk menyimpan pesan rahasia ke dalam wadah citra digital. Steganografi dapat juga digunakan untuk menyampaikan pesan rahasia, karena sifat dari steganografi yang sulit dideteksi keberadaannya. Steganografi berbeda dengan kriptografi, ini karena steganografi menyembunyikan pesan di dalam sebuah objek sedemikian rupa hingga tidak menimbulakn kecurigaan [5]. Tujuan steganografi adalah untuk menyembunyikan pesan di dalam gambar sedemikian rupa sehingga tidak memungkinkan orang lain untuk mendeteksi bahwa ada pesan rahasia yang ada dalam gambar [6].

Pada penelitian ini akan dibahas steganografi menggunakan media penampung berupa citra digital. Dimana fokus penelitian ini adalah untuk menerapkan modifikasi teknik steganografi. Prosess penyisipan pesan dapat dipilih berdasarkan pemilihan color plane (bidang warna) citra yaitu R (Red), G (Green), B (Blue) atau RGB serta jumlah bit yang akan disisipkan (maksimal 3 bit). Proses penyisipan pesan kedalam citra berdasarkan color plane dan jumlah bit yang akan disisipkan tentunya akan berpengaruh terhadap maksimal pesan yang dapat disisipkan. Hal ini dilakukan guna membandingkan citra stegano yang dihasilkan, sehingga dapat dipilih citra stegano mana nantinya yang akan digunakan sebagai output terakhir dari steganografi guna menghindari citra steganografi yang dihasilkan tidak mengalami perubahan yang signifkan dari citra asli.

Penelitian terdahulu yang relevan dapat dijadikan sebagai data pendukung. Oleh karena itu, peneliti melakukan kajian terhadap beberapa hasil penelitian berupa jurnal seperti yang dilakukan oleh [7] dengan menyisipkan pesan ke dalam citra pada ruang warna YcbCr (luminance and chrominance). Hasil penelitian menunjukkan bahwa steganografi pada ruang warna YcbCr dapat meningkatkan nilai PSNR menjadi 54,7 dB (decibel), hasil ini sangat baik dalam steganografi citra yang berarti kesalahannya akan sangat sederhana. [4] hasil pengujian menunjukkan bahwa hasil aplikasi steganografi pasti invisible atau tidak terlihat secara kasat mata serta pengujian MSE (Means Sequare Error) dan PSNR (Peak Signal-to-noise Ratio) menunjukkan bahwa ukuran pixel sangat mempengaruhi banyak text yang dapat disisip ke dalam citra gambar.

Penelitian lain dilakukan oleh [8], skema perbaikan dilakukan dengan hanya menggunakan pixel citra bernomor ganjil saja yang digunakan untuk menyimpan bit pesan. Berdasarkan kalkulasi yang sudah dilakukan, teknik LSB termodifikasi memiliki nilai yang lebih baik untuk kedua parameter (MSE dan PSNR) dibandingkan teknik LSB konvensional. Teknik LSB termodifikasi menghasilkan nilai 1,80 10-5 dan 95,61010 dB untuk parameter MSE dan PSNR, sedangkan teknik LSB konvensional menghasilkan nilai 1,98 10-5 dan 95,20893 dB

Berdasarkan penenelitian terdahulu yang relevan dengan pokok permasalahan yang sedang dibahas dengan masalah pengamanan data, maka pada penelitian ini penulis akan menganalisa teknik steganografi berdasarkan pemilihan bidang warna (color plane) pada cover citra serta mengimplementasikannya kedalam sebuah aplikasidengan judul “Modifikasi Penyisipan Pesan Pada Bidang Warna Citra dengan Teknik Steganografi”.

2. HASIL DAN PEMBAHASAN

Terdapat beberapa cara untuk mengamankan data yaitu dengan cara kriptografi dan steganografi yang dapat diimplementasikan dalam sebuah aplikasi untuk menyamarkan pesan. Steganografi merupakan suatu teknik pengamanan data dengan cara menyisipkan pesan kedalam suatu media seperti citra digital. Steganografi berbeda dengan kriptografi, hal ini karena steganografi menyembunyikan pesan di dalam sebuah objek sedemikian rupa sehingga tidak menimbulkan kecurigaan. Konsep steganografi adalah menyisipkan pesan (embedding) dan ekstraksi pesan (extracting) pada sebuah media citra digital sehingga kerahasiaan datanya tetap terjamin aman dan secara

kasat mata tidak terjadi perubahan pada citra tersebut meskipun telah disisipi pesan yang rahasia. Salah satu metode yang digunakan untuk teknik steganografi adalah dengan menggunakan metode LSB (Least Significant Bit).

Ada banyak algoritma yang sesuai dengan metode steganografi, dan salah satu algortima yang popular dan sering digunakan untuk menyembunyikan sebuah gambar atau data yaitu algoritma Least Significant Bit (LSB). Menurut [6], metode LSB salah satu teknik yang banyak digunakan dan berfungsi baik untuk teknik steganografi penyisipan pada gambar, karena dengan metode ini tidak banyak perubahan pada gambar setelah disisipi pesan teks sehingga tidak menimbulkan kecurigaan bagi pihak yang tak bertanggung jawab. Metode LSB memiliki kapasitas embedding data yang relative tinggi dan relative mudah untuk di implentasikan dan dikembangkan serta digabungkan dengan metode teknik keamanan data lainnya. Namun teknik LSB ini sangat rentan terhadap ketahanan data jika terjadi penambahan noise sehingga dapat mengurangi kinerjanya.

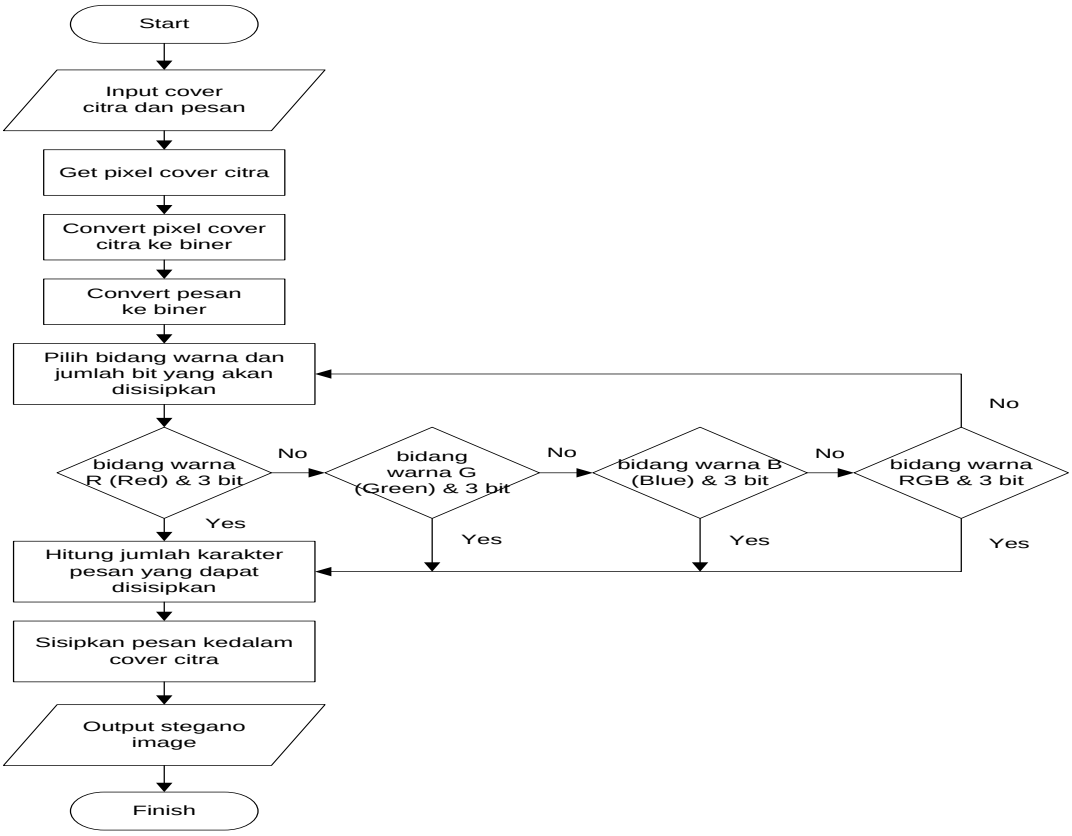
Pada citra 24 bit, setiap pixel terdiri dari 3 byte yang merepresentasikan warna red (merah), green (hijau), dan blue (biru). Sebagai contoh dalam gambar yang berukuran 600 x 500 pixel, satu pixel berukuran 3 byte (sehingga bisa disisipkan 3 bit pada setiap pixel), maka dapat disisipkan pesan sebanyak 600 x 500 x 3 = 900000 bit, atau dengan kata lain 900000 / 8 = 112500 byte pesan yang dapat disisipkan (1 byte = 8 bit) [1]. Pada susunan bit didalam sebuah byte (1 byte = 8 bit), ada bit yang paling berarti (Most Significant Bit atau MSB) dan bit paling kurang berarti (Least Significant Bit atau LSB), karena yang dirubah hanya LSB maka perubahan gambar tidak akan mudah dilihat oleh indra pengelihatan manusia. Sebagai contoh byte 11010010, pada angka bit 1 (angka pertama dan cetak tebal) merupakan MSB, sedangkan angka bit 0 (angka terakhir dan cetak tebal) merupakan LSB. Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan byte tersebut menyatakan warna merah, maka perubahan satu bit LSB tidak mengubah warna merah tersebut secara berarti. Mata manusia tidak dapat membedakan perubahan kecil tersebut [9].

Pada penelitian ini, nilai PSNR akan digunakan untuk mengetahui perbandingan kualitas citra cover sebelum dan sesudah di sisipkan pesan. Pengujian terhadap hasil stego image dilakukan dengan melihat nilai Peak Signal-to-Noise Ratio (PSNR) yang diukur dalam satuan decibel (db). PSNR digunakan dengan tujuan untuk mengetahui kualitas citra cover sebelum dan sesudah disisipkan pesan rahasia, dikatakan baik jika citra memiliki nilai PSNR di atas 30db [5].

PSNR memiliki standar nilai pada setiap cover image yang disisipkan pesan yaitu >30db sementara MSE sebaliknya semakin kecil semakin baik. Jika nilai tersebut telah dipenuhi maka gambar tersebut telah memenuhi syarat imperceptibility. Imperceptibility adalah keberadaan pesan rahasia yang tidak dapat dilihat atau dipersepsi oleh panca indra seperti mata. Contohnya jika pesan berupa teks dan disisipkan pada sebuah citra maka penyisipan pesan membuat citra sukar dibedakan atau dilihat oleh mata. Sedangkan kualitas citra yang dikatakan tidak cukup baik berada dibawah 30db [5].

Pada penelitian ini akan diterapkan modifikasi steganografi dengan metode LSB pada bidang warna RGB serta modifikasi pada jumlah bit yang dapat disipkan. Prosess penyisipan pesan dengan modifikasi metode LSB dapat dipilih berdasarkan pemilihan color plane (bidang warna) citra yaitu R (red), G (green), dan B (blue) serta modifikasi terhadap jumlah bit terakhir (bit ke delapan dari elemen warna citra) dengan memilih jumlah bit yang dapat dipilih yaitu 1 bit dan maksimal 3 bit.

Penyisipan pesan kedalam citra berdasarkan pemilihan bidang warna dan jumlah bit yang dapat disisipkan akan berpengaruh terhadap maksimal pesan yang dapat disisipkan. Hal ini dilakukan guna membandingkan stego image (citra hasil penyisipan) yang dihasilkan, sehingga dapat dipilih stego image mana nantinya yang akan digunakan sebagai output terakhir guna menghindari citra stegano yang dihasilkan tidak mengalami perubahan yang signifkan dari cover citra asli. Gambar 1 menampilkan flowchart dari proses penyisipan pesan kedalam cover citra dengan modifikasi metode LSB.



Gambar 1. Flowchart Penyisipan Pesan

Citra yang akan digunakan pada proses steganografi adalah citra berwarna 24 bit, yaitu citra yang terdiri dari tiga warna R (Red), G (Green), dan B (Blue) masing-masing warna bernilai 8 bit maka pesan akan disisipkan kedalam bit R, bit G, dan bit B tiap-tiap pixel dari cover citra. Teknik penyisipan pesan dengan metode LSB konvensiaonal yaitu dengan mengganti 1 bit terakhir dari cover citra pada masing-masing warna RGB, sedangkan modifikasi yang dilakukan yaitu bisa memilih pada bidang warna dimana pesan akan disisipkan serta ditambahkan jumlah bit yang dapat disisipkan (maksimal 3 bit) yang akan digunakan.

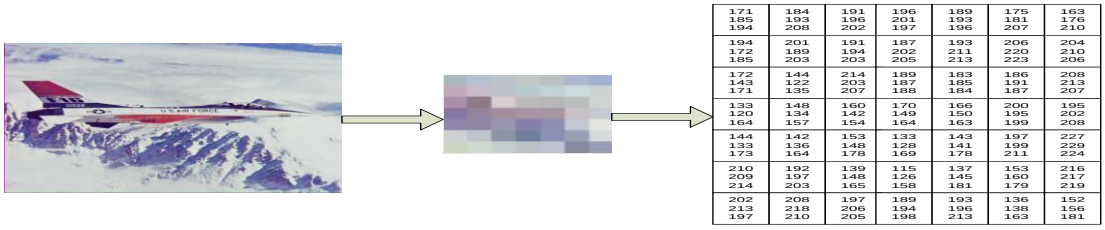
Berikut dijelaskan tahapan-tahapan yang dilakukan pada proses penyembunyian pesan kedalam citra dengan modifikasi metode LSB pada bidang warna RGB dan jumlah bit yang dapat disisipkan, yaitu sebagai berikut:

a. Tentukan pesan yang akan disisipkan
   Sebagai contoh dimisalkan pesan yang akan disipkan yaitu “NADRA”. Langkah awal yang dilakukan sebelum pesan dapat disisipkan kedalam cover citra yaitu mengkonversi pesan ke bilangan biner. Untuk mempermudah proses konversi digunakan bantuan tabel ASCII (American Standard Code for Information Interchange) yang merupakan suatu standar internasional dalam kode huruf dan simbol. Adapun hasil konversi pesan yang akan disisipkan ke dalam cover sitra dapat disajikan pada tabel 1.

Tabel 1. Hasil Konversi Pesan ke Biner

Pesan Teks	Bilangan Decimal	Bilangan Biner (8 bit)
N	78	01001110
A	65	01000001
D	68	01000100
R	82	01010010
A	65	01000001

b. Tentukan cover citra untuk menampung pesan yang akan disisipkan
   Setelah pesan teks dikonversi ke bilangan biner maka tahap selanjutnya yaitu mengambil nilai pixel dari cover citra yang akan disisipkan pesan. Seperti terlihat pada gambar 2 cover citra dataset memiliki resolusi yang besar yaitu 512x512, oleh karena itu guna mempermudah proses penyisipan pesan secara manual maka digunakan hanya 7x7 pixel dari cover citra seperti terlihat pada gambar 2.



171 185 194	184 193 208	191 196 202	196 201 197	189 193 196	175 181 207	163 176 210
194 172 185	201 189 203	191 194 203	187 202 205	193 211 213	206 220 223	204 210 206
172 143 171	144 122 135	214 203 207	189 187 188	183 185 184	186 191 187	208 213 207
133 120 164	148 134 157	160 142 154	170 149 164	166 150 163	200 195 199	195 202 208
144 133 173	142 136 164	153 148 178	133 128 169	143 141 178	197 199 211	227 229 224
210 209 214	192 197 203	139 148 165	115 126 158	137 145 181	153 160 179	216 217 219
202 213 197	208 218 210	197 206 205	189 194 198	193 196 213	136 138 163	152 156 181

Gambar 2. Potongan Pixel Cover Citra 7x7

Dari potongan pixel cover citra pada gambar 2 diperoleh nilai pixel RGB cover citra dalam format bilangan decimal, sehingga perlu dikonversi terlebih dahulu ke format biner. Hasil konversi pixel cover citra dari decimal ke biner disajikan pada tabel 2.

Tabel 2. Hasil Konversi Pixel Cover Citra ke Biner

(x,y)	0	1	2	3	4	5	6
0	R=10101011 G=10111001 B=11000010	R=10111000 G=11000001 B=11010000	R=10111111 G=11000100 B=11001010	R=11000100 G=11001001 B=11000101	R=10111101 G=11000001 B=11000100	R=10101111 G=10110101 B=11001111	R=10100011 G=10110000 B=11010010
1	R=11000010 G=10101100 B=10100101	R=11001001 G=10111101 B=11001011	R=10111111 G=11000010 B=11001011	R=10111011 G=11001010 B=11001110	R=11000001 G=11010011 B=11010101	R=11001110 G=11011100 B=11011111	R=11001100 G=11010010 B=11001110
2	R=10101100 G=10001111 B=10101011	R=10010000 G=01111010 B=10001000	R=11010110 G=11001011 B=11001111	R=10111101 G=10111011 B=10111100	R=10110111 G=10111001 B=10111000	R=10111010 G=10111111 B=10111011	R=11010000 G=11010101 B=11001111
3	R=10000101 G=01111000 B=10100100	R=10010100 G=10000110 B=10011101	R=10100000 G=10001110 B=10011010	R=10101010 G=10010001 B=10100100	R=10100110 G=10100000 B=10100011	R=11001000 G=11000100 B=11000111	R=11000100 G=11001010 B=11010000
4	R=10010000 G=10000101 B=10101101	R=10001110 G=10001000 B=10100100	R=10011001 G=10010100 B=10110010	R=10000101 G=10000000 B=10101001	R=10001111 G=10001101 B=10110010	R=11000101 G=11000111 B=11010011	R=11100011 G=11100101 B=11100000
5	R=11010010 G=11010001 B=11010110	R=11000000 G=11000101 B=11001011	R=10001011 G=10010100 B=10100101	R=01110100 G=01111110 B=10011110	R=10001001 G=10010001 B=10110101	R=10011001 G=10100000 B=10101111	R=11011000 G=11011001 B=11011011
6	R=11001010 G=11010101 B=11000101	R=11010000 G=11011010 B=11010010	R=11000101 G=11001110 B=11001110	R=10111101 G=11000010 B=11000100	R=11000001 G=11000100 B=11010101	R=10001000 G=10001010 B=10100011	R=10011000 G=10100110 B=10100001

c. Proses Penyisipan Pesan

Setelah mendapat nilai pixel dari cover citra dalam format biner, maka tahap selanjutnya yaitu melakukan proses penyisipan pesan. Misalkan bidang warna yang dipilih adalah R (Red) dan jumlah bit yang akan disisipkan sebanyak 1 bit, maka proses penyisipannya dapat dilakukan dengan cara mengganti 1 bit terakhir pada bidang warna R (Red) untuk setiap pixel cover citra, sehingga hasilnya dapat dilihat pada tabel 3

Tabel 3. Hasil Penyisipan Pesan kedalam Cover Citra

(x,y)	0	1	2	3	4	5	6
0	R=10101010 G=10111001 B=11000010	R=10111001 G=11000001 B=11010000	R=10111110 G=11000100 B=11001010	R=11000100 G=11001001 B=11000101	R=10111101 G=11000001 B=11000100	R=10101111 G=10110101 B=11001111	R=10100011 G=10110000 B=11010010
1	R=11000010 G=10101100 B=10100101	R=11001000 G=10111101 B=11001011	R=10111111 G=11000010 B=11001011	R=10111010 G=11001010 B=11001110	R=11000000 G=11010011 B=11010101	R=11001110 G=11011100 B=11011111	R=11001100 G=11010010 B=11001110
2	R=10101100 G=10001111 B=10101011	R=10010001 G=01111010 B=10001000	R=11010110 G=11001011 B=11001111	R=10111101 G=10111011 B=10111100	R=10110110 G=10111001 B=10111000	R=10111010 G=10111111 B=10111011	R=11010000 G=11010101 B=11001111
3	R=10000101 G=01111000 B=10100100	R=10010100 G=10000110 B=10011101	R=10100000 G=10001110 B=10011010	R=10101010 G=10010001 B=10100100	R=10100111 G=10100000 B=10100011	R=11001000 G=11000100 B=11000111	R=11000101 G=11001010 B=11010000
4	R=10010000 G=10000101 B=10101101	R=10001110 G=10001000 B=10100100	R=10011001 G=10010100 B=10110010	R=10000100 G=10000000 B=10101001	R=10001110 G=10001101 B=10110010	R=11000101 G=11000111 B=11010011	R=11100010 G=11100101 B=11100000
5	R=11010010 G=11010001 B=11010110	R=11000000 G=11000101 B=11001011	R=10001010 G=10010100 B=10100101	R=01110100 G=01111110 B=10011110	R=10001001 G=10010001 B=10110101	R=10011001 G=10100000 B=10101111	R=11011000 G=11011001 B=11011011
6	R=11001010 G=11010101 B=11000101	R=11010000 G=11011010 B=11010010	R=11000101 G=11001110 B=11001110	R=10111101 G=11000010 B=11000100	R=11000001 G=11000100 B=11010101	R=10001000 G=10001010 B=10100011	R=10011000 G=10100110 B=10100001

Seperti diketahui sebelumnya pesan yang akan disispkan yaitu “NADRA” dengan susunan biner setelah dikonversi “01001110 01000001 01000100 01010010 01000001”.

Berdasarkan ukuran cover citra yang digunakan sebagai sampel diperoleh bahwa:

Total pixel cover citra = width x height

= 7 pixel x 7 pixel = 49 pixel

Setiap pixel citra bitmap disusun oleh 3 elemen warna yaitu red, green dan blue dan setiap satu elemen warna pixel terdiri dari 8 bit, sehingga setiap satu pixel terdiri dari 24 bit, maka diperoleh:

Total bit Cover Citra = Total Pixel Citra x 3

= 49 x 24 = 1.176 bit

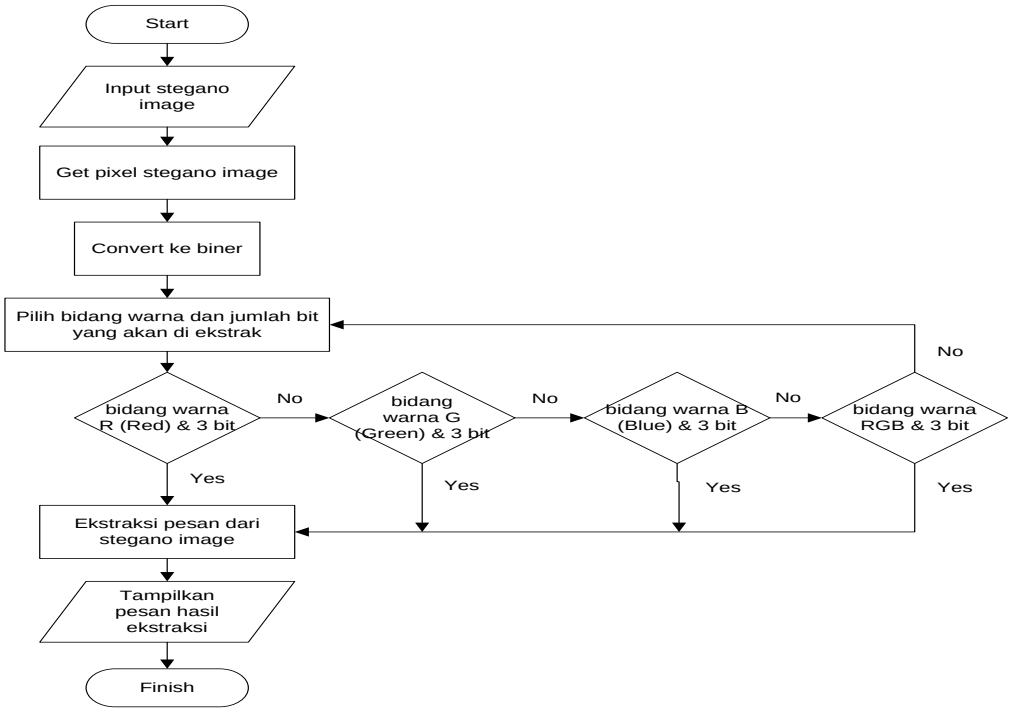
Berdasarkan perhitungan di atas, dapat disimpulkan bahwa total bit cover citra lebih besar dibandingkan dengan total bit pesan yang disisipkan (42 bit), sehingga proses penyembunyian pesan dapat dilakukan dengan menggunakan citra sampel. Perubahan pixel cover citra sebelum dan sesudah pesan disispkan dapat disajikan pada tabel 4.

Tabel 4. Perubahan Nilai Pixel Cover Citra

Sebelum							**Sesudah**						
171	**184**	**191**	196	189	175	163	**170**	**185**	**190**	196	189	175	163
185	193	196	201	193	181	176	185	193	196	201	193	181	176
194	208	202	197	196	207	210	194	208	202	197	196	207	210
194	**201**	191	**187**	**193**	206	204	194	**200**	191	**186**	**192**	206	204
172	189	194	202	211	220	210	172	189	194	202	211	220	210
185	203	203	205	213	223	206	185	203	203	205	213	223	206
172	**144**	214	189	**183**	186	208	172	**145**	214	189	**182**	186	208
143	122	203	287	185	191	213	143	122	203	287	185	191	213
171	135	207	188	184	187	207	171	135	207	188	184	187	207
133	**146**	160	170	**166**	200	**195**	133	**148**	160	170	**167**	200	**197**
120	134	142	149	150	195	202	120	134	142	149	150	195	202
164	157	154	164	163	199	208	164	157	154	164	163	199	208
144	142	153	**133**	**143**	197	**227**	144	142	153	**132**	**142**	197	**226**
133	136	148	128	141	199	229	133	136	148	128	141	199	229
173	164	178	169	178	211	224	173	164	178	169	178	211	224
210	192	139	115	**137**	**153**	216	210	192	**138**	**116**	137	153	216
209	197	148	126	145	160	217	209	197	148	126	145	160	217
214	203	165	158	181	179	219	214	203	165	158	181	179	219
202	208	197	189	193	136	152	202	208	197	189	193	136	152
213	218	206	194	196	138	156	213	218	206	194	196	138	156
197	210	205	198	213	163	181	197	210	205	198	213	163	181

Pada tabel 4 ditampilkan bahwa cover citra pada koordinat (0, 0) memiliki nilai RGB 171, 185, 194, setelah proses penyisipan pesa maka nilai pixel pada koordinat tersebut mengalami penurunan nilai R menjadi 170. Berdasarkan hasil penyisipan pada bidang warna R dan jumlah bit yang disisipkan 1 bit seperti telah dijelaskan sebelumnya dapat dilihat bahwa hanya ada 16 bit pada bidang warna R yang mengalami perubahan nilai dari total 49 bit pixel bidang warna R, dengan demikian cover citra sebelum dan sesudah disisipkan pesan tidak mengalami perubahan nilai pixel yang signifikan.

Proses ekstraksi yaitu proses pengambilan pesan yang tersembunyi pada citra digital. Proses ini akan menghasilkan pesan yang disembunyikan dengan masukan berupa stegano image. Gambar 3 menunjukkan flowchart untuk mengembalikan pesan teks yang telah disisipkan kedalam citra digital, sehingga menghasilkan pesan teks dari citra digital.



Gambar 3. Flowchart Ekstraksi Pesan

Analisis proses ekstraksi pesan merupakan proses untuk memperoleh kembali pesan rahasia yang telah disembunyikan kedalam cover citra. Proses ekstraksi pesan dari dalam cover citra adalah kebalikan dari penyisipannya. Dimulai dari mengambil stegano image lalu mengkonversi nilai RGB menjadi biner 8 bit.Sesuai dengan prosess penyisipan pesan dengan modifikasi metode LSB dapat dipilih berdasarkan pemilihan color plane (bidang warna) citra yaitu R (red), G (green), dan B (blue) serta modifikasi terhadap jumlah bit terakhir (bit ke delapan dari elemen warna citra) dengan memilih jumlah bit yang dapat dipilih yaitu 1 bit dan maksimal 3 bit. Hal yang sama juga berlaku untuk proses ekstraksi pesan dari dalam stegano image, yaitu harus menentukan atau memilih bidang warna dan jumlah bit yang akan diekstraksi dari dalam stegano image.

1. Ambil pixel stegano image dan konversi nilai pixel kebilangan biner (8 bit), seperti yang telah dijelaskan sebelumnya bahwa pada saat proses penyisipan pesan dipilih bidang warna R dan jumlah bit yang disisipkan 1 bit, maka dari tabel 4 diambil diperoleh nilai pixel untuk semua bidang warna R dari cover citra seperti terlihat pada tabel 5.

Tabel 5. Bidang Warna R Stegano Image

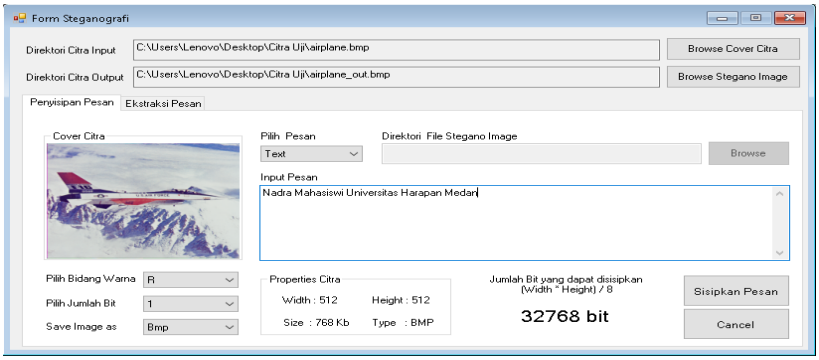
(x,y)	0	1	2	3	4	5	6
0	R=10101010	R=10111001	R=10111110	R=11000100	R=10111101	R=10101111	R=10100011
1	R=11000010	R=11001000	R=10111111	R=10111010	R=11000000	R=11001110	R=11001100
2	R=10101100	R=10010001	R=11010110	R=10111101	R=10110110	R=10111010	R=11010000
3	R=10000101	R=10010100	R=10100000	R=10101010	R=10100111	R=11001000	R=11000101
4	R=10010000	R=10001110	R=10011001	R=10000100	R=10001110	R=11000101	R=11100010
5	R=11010010	R=11000000	R=10001010	R=01110100	R=10001001	R=10011001	R=11011000
6	R=11001010	R=11010000	R=11000101	R=10111101	R=11000001	R=10001000	R=10011000

Berdasarkan tabel 5 selanjutnya ambil 1 bit terakhir dari masing-masing pixel sehingga diperoleh susunan bit pesan yaitu 01001110 01000001 01000100 01010010 01000001.

2. Bagi bit pesan menjadi 8 *bit* kemudain konversi ke *decimal* lalu ubah ke karakter sesuai dengan tabel ASCII sehingga diperoleh menjadi:
   01001110 ⟶ konversi ke *decimal* menjadi 78 (karakter N)
   01000001 ⟶ konversi ke *decimal* menjadi 65 (karakter A)
   01000100 ⟶ konversi ke *decimal* menjadi 68 (karakter D)
   01010010 ⟶ konversi ke *decimal* menjadi 82 (karakter R)
   01000001 ⟶ konversi ke *decimal* menjadi 65 (karakter A)
   sehingga diperoleh hasil ekstraksi isi pesan “NADRA”

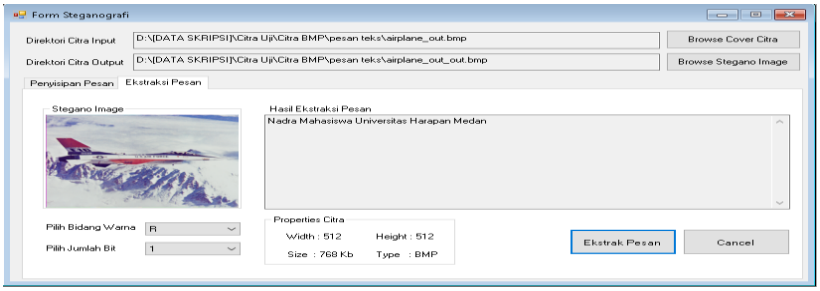
Setelah dilakukan beberapa tahapan dalam analisa sistem, selanjutnya dilakukan tahapan perancangan sistem. Tahap perancangan sistem terdiri dari tiga bagian yaitu perancangan use case diagram sistem untuk mendiskripsikan sebuah interaksi antara satu atau lebih aktor dengan sistem yang akan dibuat.

Implementasi antarmuka merupakan realisasi desain tampilan antarmuka dari setiap menu yang telah dirancang sebelumnya kedalam bahasa pemrograman. Aplikasi steganografi ini merupakan sebuah aplikasi yang dibuat untuk membantu untuk menyamarkan pesan agar terjamin kerahasiaannya dengan cara meyisipkannya kedalam citra digital. Aplikasi steganografi ini menggunakan modifikasi metode LSB pada bidang warna dan jumlah bit yang disisipkan.Antarmuka dari aplikasi steganografi ini, terdiri dari tiga menu utama, yaitu menu steganografi, menu pengujian, dan menu help.



Gambar 4. Tampilan Penyisipan Pesan Teks

Gambar 4 memperlihatkan proses penyisipan pesan teks kedalam citra dengan pengaturan pada bidang warna yang dipilih yaitu R (Red) serta jumlah bit yang disisipkan yaitu 1 bit. Citra yang dijadikan sebagai cover citra untuk menampung pesan yang akan disisipkan berformat .bmp dengan resolusi 512x512, maka jumlah bit yang dapat disipkan kedalm cover citra yaitu sebanyak 32768 bit, diperoleh dengan cara mengalikan resolusi cover citra (width * height) kemudian dibagi dengan 8.



Gambar 5. Tampilan Ekstraksi Pesan

Berdasarkan gambar 5. Proses ekstraksi pesan berhasil dilakukan, dimana pesan yang telh disisipkan sebelumnya kedalam cover citra dapat diekstrak untuk menampilkan pesan yang disembunyikan. Proses ekstraksi pesan dapat berhasil dilakukan jika bidang warna dan jumlah bit yang digunakan pada saat penyisipan pesan sama dengan bidang warna dan jumlah bit yang digunakan pada proses ekstraksi pesan.Jika tidak sama maka sistem akan menampilkan pesan kesalahan.

3. KESIMPULAN

Berdasarkan hasil analisa dan pengujian sistem pengamanan pesan dengan teknik steganografi menggunakan modifikasi metode LSB, maka didapatkan kesimpulan sebagai berikut:

a. Bidang warna (color plane) sebuah citra direpresentasikan dengan warna Red (R), Green (G), dan Blue (B). Teknik steganografi menggunakan pemilihan bidang warna dilakukan untuk memodifikasi metode LSB konvensional sehingga diperoleh maksimal bit yang dapat disisipkan ke dalam cover citra, dimana maksimal pesan yang dapat disisipkan tergantung pada resolusi/dimensi dari cover citra yang digunakan.
b. Hasil implementasi dan pengujian sistem menunjukkan bahwa pemilihan bidang warna dan jumlah bit yang akan disisipkan sangat berpengaruh terhadap jumlah bit yang tersedia dari cover citra. Citra lenna.bmp yang berukuran 768 Kb, maka jumlah bit yang tersedia jika hanya memilih pada bidang warna Red (R) atau Green

(G) atau Blue (B) serta jumlah bit yang disisipkan 1 bit, maka diperoleh maksimal jumlah bit yang dapat disisipkan yaitu sebesar 32768 bit (4096 karakter) pesan.

c. Modifikasi metode LSB pada pemilihan bidang warna dan jumlah bit berhasil di implementasikan ke dalam sebuah aplikasi untuk mengamankan pesan pada citra digital. Dari hasil pengujian kualitas terhadap 9 citra uji dengan jumlah pesan yang sama diperoleh nilai PSNR diatas 30 db. Nilai PSNR tertinggi yaitu pada citra airplane.bmp dengan nilai PSNR sebesar 84,231 db.

DAFTAR PUSTAKA

[1] A. Ardiansyah and M. Kurniasih, "Penyembunyian Pesan Rahasia Pada Citra Digital Dengan Teknik Steganograpi Menggunakan Metode Least Significant Bit," *Respati*, vol. 13, no. 3, 2018.

[2] R. Siringoringo, "ANALISIS PSNR PADA STEGANOGRAFI LEAST SIGNIFICANT BIT DENGAN PESAN TERENKRIPSI ADVANCED ENCRIPTION SYSTEM," 2016.

[3] T. E. Putri, M. R. Al Fauzan, and P. A. Sejati, "PERBAIKAN ALGORITMA STEGANOGRAFI TEKNIK LEAST SIGNIFICANT BITS UNTUK APLIKASI KEAMANAN DATA," *J. ONLINE Phys.*, vol. 3, no. 1, pp. 27–32, 2017.

[4] A. Apriansyah, H. Mukhtar, and M. Unik, "Implementasi Sistem Keamanan Pesan Text Dengan Teknik Steganografi Menggunakan Metode Least Significant Bit (LSB)," *J. CoSciTech (Computer Sci. Inf. Technol.*, vol. 1, no. 1, pp. 8–12, 2020.

[5] N. F. Hasan, C. N. Dengen, and D. Ariyus, "Analisis Histogram Steganografi Least Significant Bit Pada Citra Grayscale," *Digit. Zo. J. Teknol. Inf. dan Komun.*, vol. 11, no. 1, 2020.

[6] N. Nurhasanah, "Analisa Dan Implementasi Ketahanan Citra Digital Untuk Penyimpanan Data Teks Dengan Teknik Steganografi Menggunakan Metode LSB," *J. Ilm. Humanika*, vol. 3, no. 1, pp. 34–37, 2020.

[7] Z. A. Alwan, H. M. Farhan, and S. Q. Mahdi, "Color image steganography in YCbCr space.," *Int. J. Electr. Comput. Eng.*, vol. 10, 2020.

[8] N. A. Ramadhani, "Penerapan Steganografi Untuk Penyisipan Pesan Teks Pada Citra Digital Dengan Menggunakan Metode Least Significant Bit," *Naskah Publ. Progr. Stud. Tek. Inform.*, 2019.

[9] G. Wibisono, T. Waluyo, and E. I. H. Ujianto, "KAJIAN METODE METODE STEGANOGRAFI PADA DOMAIN SPASIAL," *JITK (Jurnal Ilmu Pengetah. Dan Teknol. Komputer)*, vol. 5, no. 2, pp. 259–264, 2020.