Steganografi : Penyembunyian Pesan pada Citra Digital dengan Kakas Image Editor dengan Pengubahan Pixel secara Manual

Aridarsyah Eka Putra
13507058
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
ariedz@students.itb.ac.id

Abstract - Citra Digital adalah representasi dari gambar dua dimensi menggunakan bilangan biner. Bergantung pada resolusinya yang "fixed" atau tidak, citra digital bisa disebut sebagai vector ataupun raster. Namun, secara umum yang disebut dengan "citra digital" biasanya adalah citra raster yang disebut juga sebagai citra bitmap.

Citra raster adalah struktur data yang merepresentasikan punya sejumlah set nilai digital yang terbatas, yang umum disebut sebagai pixels (picture elements).

Piksel adalah unsur gambar atau representasi sebuah titik terkecil dalam sebuah gambar grafis yang dihitung per inci (penjelasan lebih rinci bias di lihat di bab berikutnya).

Kata Kunci - piksel, steganografi, citra digital, RGB, CMYK.

I. PENDAHULUAN

Komunikasi merupakan kebutuhan manusia, salah satu cara melakukan komunikasi ini adalah dengan melakukan pengiriman pesan. Dilatarbelakangi oleh kebutuhan manusia tersebut, teknologi komunikasi dewasa ini maju dengan pesat.Dengan kemajuan teknologi tersebut, manusia dapat melakukan pengiriman pesan dengan mudah di mana saja dan kapan saja dengan menggunakan berbagai media.

Dengan semakin mudahnya manusia dalam melakukan pengiriman pesan, semakin mudah pula pesan tersebut dicuri atau dilihat oleh pihak yang tidak bertanggung jawab.Hal tersebut menjadi masalah yang cukup serius karena pesan yang dikirim dapat merupakan pesan penting yang rahasia.

Salah satu cara yang bisa dipakai dalam meminimalisasi dan menghindari pesan yang kita kirim terlihat oleh adanya pihak-pihak yang tidak bertanggung jawab, salah satu pilihan yang bisa dipakai adalah steganografi.

Berbeda dengan kriptografi yang membuat hasil enkripsi dari pesan yang ada menjadi sesuatu yang aneh dan ganjil sehingga menyebabkan orang yang melihat akan curiga bahwa ada sesuat di dalamnya, dengan steganografi kecurigaan tersebut bisa dihilangkan sehingga orang-orang yang tidak mempunyai kepentingan tersebut tidak menyadari akan adanya pesan rahasia ataupun pesan yang tersembunyi di dalamnya.

Steganografi yang baik adalah steganografi yang tidak terdeteksi atau tidak menimbulkan kecurigaan bahwa ada pesan tersembunyi di dalam cover-text, cover-image, ataupun cover-audio sebagai tempat file digital disembunyikan.

Steganografi yang umum dilakukan secara automatis dengan menggunakan software perangkat lunak yang spesifik, dengan menggunakan metode LSB umumnya.Oleh karena harus menggunakan perangkat lunak yang spesifik tersebut, hanya sebagian orang yang menggunakan ataupun mengerti tentang steganografi, umumnya orang yang memang expert dalam bidang ini ataupun orang yang mengambil mata kuliah yang berhubungan dengan steganografi.

Di sini penulis ingin agar orang-orang awam-pun mengetahui apa itu steganografi dan bisa mengaplikasikannya, karena itu penulis membuat satu cara steganografi yang mudah dimengerti oleh orang awam sekali-pun. Untuk itu dalam makalah ini kakas yang akan digunakan-pun adalah kakas yang sangat familiar di telinga orang, seperti Microsoft Paint atau Adobe Photoshop.

II. LANDASAN TEORI

2.1 Steganografi

Steganografi berasal dari bahasa Yunani "steganos" yang artinya tulisan tersembunyi (covered writing), sedangkan steganografi sendiri adalah ilmu dan seni menyembunyikan (embedded) informasi dengan cara menyisipkan pesan rahasia di dalam pesan lain. Steganografi sebenarnya sudah diterapkan sejak zaman dahulu, steganografi dengan media kepala budak (dikisahkan oleh Herodatus, penguasa Yunani pada tahun 440 BC di dalam buku: Histories of Herodatus). Kepala budak dibotaki, ditulisi pesan, rambut budak dibiarkan tumbuh, budak dikirim.Di tempat penerima kepala budak digunduli agar pesan bisa dibaca. Adapun contoh lain dengan penggunaan tinta tak-tampak (invisible ink). Tinta dibuat dari campuran sari buah, susu, dan cuka. Tulisan di

atas kertas dapat dibaca dengan cara memanaskan kertas tersebut.

Salah satu alasan mengapa digunakan steganografi agar informasi yang akan disampaikan tidak diketahui karena disamarkan dengan pesan lain ataupun keberadaan informasi tersebut tidak diketahui. Berbeda dengan kriptografi, apabila plainteks sudah dienkripsi maka chiperteksnya akan terlihat sangat mencurigakan. Kita liat contoh yang kami ambil dari slide Pak Rinaldi Munir, prisoner's problem. Ada dua orang napi, napi yang satu mengirim pesan lari jam satu" lewat seorang sipir.Pesan tersebut tidak boleh secara gamblang disampaikan, agar tidak ditangkap oleh sipir.Cara agar pesan tidak diketahui yaitu dengan pesan dienkripsi dengan kriptografi atau disembunyikan dengan kriptografi. Dengan kriptografi tertentu, pesan dienkripsi menjadi xjT#9uvmY!rc$, cipherteks menjadi sangat mencurigakan bagi sipir. Kalau dengan steganografi huruf-huruf pesan disembunyikan pada huruf awal pesan ini, Lupakan asal rumor itu, jaga agar matamu sehat atau turunkan ubanmu, sipir kemungkinan tidak curiga sama sekali karena pesannya terlihat normal.

Pada kali ini, kami mempelajari steganografi digital, yaitu steganografi pada data digital dengan menggunakan komputer digital.Data digital tersebut bisa berupa teks, gambar, audio, dll.Cara penyembunyiannya juga beragam, bisa teks dalam audio, teks dalam gambar, gambar dalam gambar, dll. Properti-properti dari steganografi adalah:

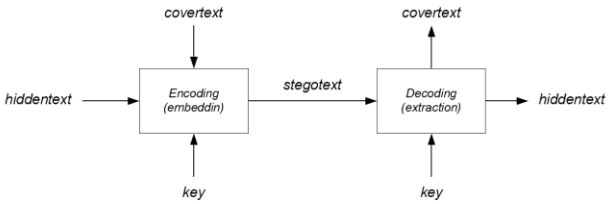
1.Embedded message (hiddentext): pesan yang disembunyikan. Bisa berupa teks, gambar, audio, video, dll

2.Cover-object (covertext): pesan yang digunakan untuk menyembunyikan embedded message. Bisa berupa teks, gambar, audio, video, dll

3.Stego-object (stegotext): pesan yang sudah berisi pesan embedded message.

4.Stego-key: kunci yang digunakan untuk menyisipan pesan dan mengekstraksi pesan dari stegotext.

Proses Steganografi secara umum adalah :



Gambar 1 Proses Steganografi

2.2 Citra Digital

Pada abstraksi di atasa sudah dijelaskan bahwa sitra digital adalah representasi dari gambar dua dimensi menggunakan bilangan biner. Bergantung pada resolusinya yang "fixed" atau tidak, citra digital bisa disebut sebagai vektor ataupun raster. Namun, secara umum yang disebut dengan "citra digital" biasanya adalah citra raster yang disebut juga sebagai citra bitmap.

Citra digital (citra raster) itu sendiri punya satu set nilai-nilai digital. Sebuah citra digital terdiri atas sejumlah piksel penyusunnya, sedangkan citra vector dihasilkan dari geometri matematis (vektor).Dalam istilah matematiknya sebuah vektor itu sendiri terdiri dari titik-titik yang punya arah dan panjang. Dalam makalah ini akan penulis akan tidak membahas citra vektor, tetapi akan lebih membahas citra raster.

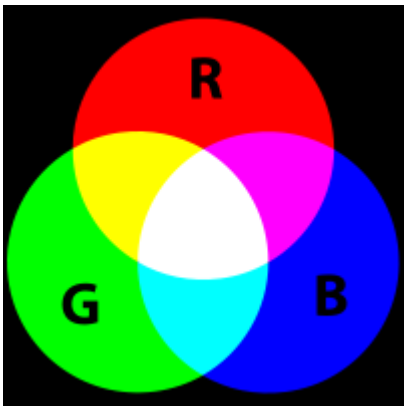
Biasanya kita bisa mengenali sebuah citra raster saat kita melihat hasil foto dari kamera digital ataupun hasil scan citra dari scanner. Seperti yang dijelaskan bahwa citra digital (untuk selanjutnya penulis akan menyebut istilah "citra raster" dengan "citra digital" akar lebih familiar di telinga pembaca) tersusun dari piksel-piksel.

Piksel adalah unsur gambar atau representasi sebuah titik terkecil dalam sebuah citra digital (elemen terkecil dari citra digital yang bisa direpresentasikan atau dikontrol).Tiap piksel punya alamat/address sendiri.Alamat tersebut berkorespodensi dengan koordinatnya.Bentuk/ struktur data dari piksel adalah grid dua dimensi, dan sering digambarkan sebagai dot.Tiap piksel adalah sampel dari citra yang asli, lebih banyak sampel yang ada semakin akurat gambaran yang ada terhadap citra yang asli.

Intensitas dari tiap piksel bermacam-macam.Dalam sistem pewarnaan citra, sebuah piksel menggambarkan digitasi dari warna.Variasi warna yang kontinu didekati menjadi diskrit dengan elemen-elemen piksel (warna-warna yang ada didekati dengan palet warna yang tersedia). Sebuah warna biasanya direpresentasikan oleh tiga atau empat komponen intensitas seperti RGB (red, green, blue) atau CMYK (cyan, magenta, yellow, black).

RGB

Pada model warna RGB sebuah warna direpresentasikan menjadi tiga komponen warna yaitu red(merah), green (hijau), dan biru(blue).



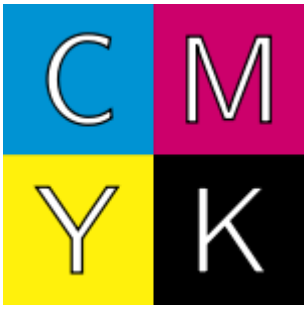
Gambar 2 Model Warna RGB

Tujuan utama dari model warna RGB ini adalah untuk sensing, representasi, dan penyajian citra di sistem-sistem elektronik seperti televisi ,komputer, dan fotografi

konvensional, dsb. Dengan membagi warna menjadi tiga komponen, memungkinkan untuk merepresentasikan sebagian warna yang ada selama berada di spektrum tiga warna tersebut (ada warna yang tidak bisa tepat direpresentasikan dengan RGB ini, tetapi bisa didekati)

CMYK

Pada model warna CMYK, sebuah warna dibagi menjadi empat komponen yaitu warna cyan (warna antara biru dan hijau), magenta (warna merah keunguan), yellow(kuning), dan key (hitam). Warna ini biasanya digunakan dalam proses percetakan.



Gambar 3 Warna-warna dalam CMYK

Jika RGB biasanya background (warna dengan elemen R, G, B dengan nilai 0 sama dengan warna hitam) dasarnya bewarna hitam, pada CMYK background (warna dengan elemen C, M, Y, K dengan nilai 0 sama dengan warna putih) dasarnya berwarna putih. Jadi berbeda bila pada RGB semua warna digabung menjadi terang (putih) atau disebut "additive combination", sedangkan pada CMYK bila digabung warna menjadi hitam/ menngurang tingkat terang dari warna yang biasa disebut dengan "substractive combination".

Gambar 4 Model Warna CMYK

III. METODE

Pada makalah ini akan dijelaskan bagaimana cara melakukan steganografi dengan pengubahan pixel secara manual pada citra digital, untuk melakukan itu maka kita harus mampu melakukan pengubahan manual piksel pada citra digital dan melakukan penyembunyian karakter-karakter pesan pada piksel-piksel tersebut.

A. Pengubahan Pixel pada Citra Digital

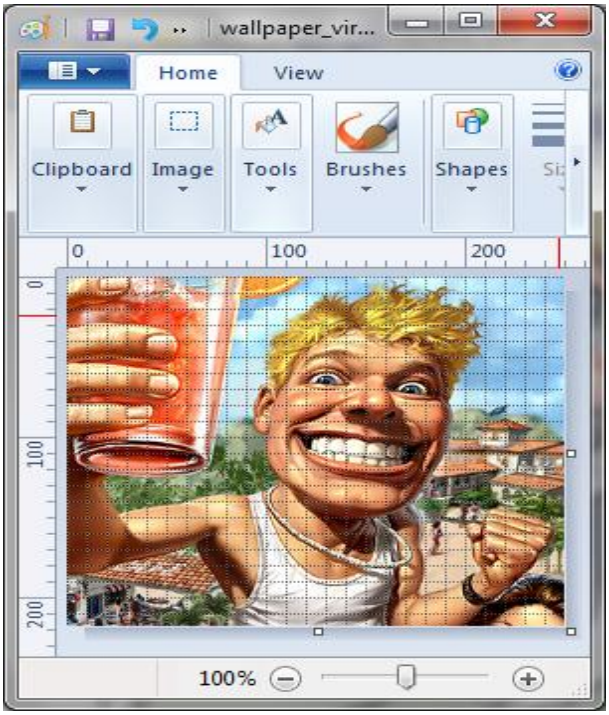
Pada makalah ini penulis ini akan menunjukkan pengubahan piksel pada citra digital berdasarkan berdasarkan model warna RGB, untuk model CMYK tidak akan dibahas terlalu jauh.

Langkah-langkah pengubahan piksel :

1. 1. Buka citra digital yang ada (untuk memudahkan pengubahan pixel, ubahlah view dari editor kakas menjadi gridlines view, untuk melihat piksel-piksel yang ada, pada penjelasan di bawah digunakan kakas Microsoft Paint).

Gambar 5 Citra Digital asli (belum terdapat pengubahan piksel)

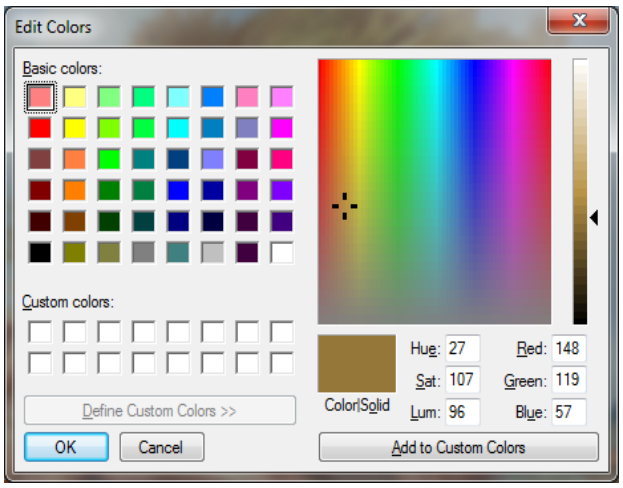
2. Kita ambil bagian yang ingin kita ubah pikselnya (lakukan sampling pada gambar).



Gambar 6 Citra Digital (setelah dilakukan sampling pada bagian tertentu)

3. Perbesar gambar sehingga ukuran gambar sama dengan jumlah satuan yang ada pada gambar (misal gambar dengan ukuran 100x100 piksel, maka jumlah grid-grid yang ada juga sama sejumlah 100x100 grid) dan sesuaikan besar alat penunjuk pada kakas yang dipakai menjadi satu piksel, sehingga penunjuk akan mengambil tepat satu piksel dari citra.

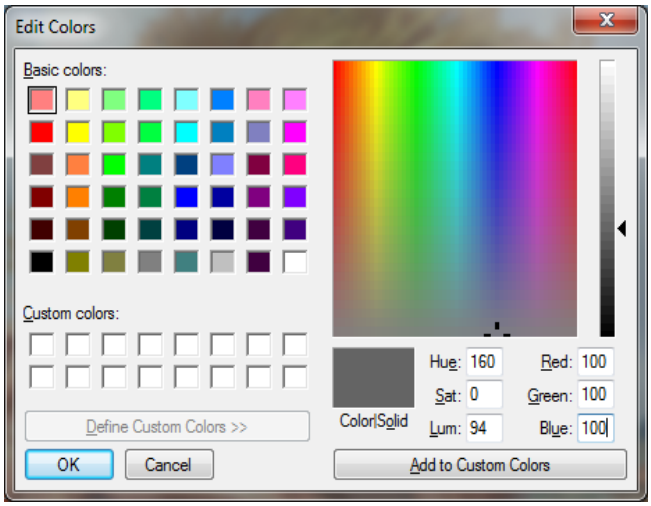
4. Kita ambil dot piksel yang akan kita rubah,misalnya piksel ke 200 (sumbu x) dari kiri 50 (sumbu y negatif) dari atas, dengan color picker. Kita akan mendapatkan warna-warna dalam RGB dalam menu edit color.



Gambar 7 Melihat nilai komponen warna dari piksel tertentu

Dari gambar di atas kita mendapatkan nilai-nilai dari komponen RGBnya (R= 148, G= 119, B= 57).

5. Dengan menu color editor kita akan merubah nilai-nilai RGB tersebut. Misal kita ubah nilai-nilai komponen RGBnya menjadi seperti ini, R= 100, G= 100, B= 100.



Gambar 8 Mengganti nilai dari komponen warna dari piksel tertentu.

6. Setelah kita dapatkan warna dengan nilai-nilai tadi gantilah penunjuk yang kita pakai, dari color picker menjadi brush untuk mengganti warna yang dimaksud, misal kita mengganti pada piksel yang tadi disebutkan (piksel ke 200 (sumbu x) dari kiri 50 (sumbu y negatif) dari atas). Hasilnya warna yang tadinya dengan nilai R= 148, G= 119, B= 57 akan berubah menjadi R= 100, G=100, B= 100.

Gambar 9 Pergantian warna pada piksel tertentu (dengan mengganti nilai dari kompnen RGBnya)

B. Pola Steganografi pada Piksel-Piksel Citra Digital

Seperti diketahui di atas bahwa komponen warna pada model warna RGB untuk tiap piksel pada citra digital terdiri dari tiga komponen warna, yairu merah, hijau, dan biru. Tiap-tiap pikes mempunyai komponen tersebut dan relative mempunyai nilai-nilai yang berbeda-beda tiap piksel. Untuk melakukan steganografi pada citra digital pada makalah ini, penulis akan memanfaatkan nilai-nilai tersebut.

Sebelum melangkah ke langkah-langkah steganografi, akan dijelaskan bentuk pesan yang nantinya akan disembunyikan pada citra digital. Pesan yang disembunyikan bisa berupa karakter A-Z ataupun semua karakter ASCII yang berjumlah 256 buah.Karakter ASCII tersebut bisadisembunyikan, mengingat nilai untuk komponen RGB tersebut juga berjumlah 256 buah (0-255).

Untuk melakukan steganografi pada makalah ini, kita membutuhkan:

- satu komponen nilai untuk menyembunyikan karakter-karakternya (plain teks terdiri dari banyak karakter, tiap karakter ditaruh pada satu nilai pada satu piksel)
- dan sisanya adalah dua komponen nilai untuk menunjukkan letak di mana karakter selanjutnya disembunyikan yaitusatu komponen nilai untuk memberikan letak pada sumbu X dan satu komponen untuk memberi letak pada sumbu Y. Kedua komponen ini akan menunjukkan koordinat piksel di mana karakter selanjutnya disembunyikan.

Misal kita akan menyembunyikan kata STEGANOGRAFI pada citra digital :

- karakter A-Z diganti menjadi nilai dari 0-25
- komponen G digunakan untuk menyembunyikan karakter
- Komponen R digunakan untuk menunjukkan letak piksel selanjutnya pada sumbu X.
- Komponen B digunakan untuk menunjukkan letak piksel selanjutnya pada sumbu Y.
- Koordinat yang dimaksud adalah koordinat dari piksel yang menyembunyikan karakter sebelumnya, misalnya piksel pertama berada pada lokasi (0,0) mempunyai nilai R= 10, G= 5, B= 15, maka piksel selanjutnya berada pada 10 satuan piksel ke samping kanan (sumbu X positif) dan 15 satuan piksel kea rah bawah (sumbu Y negatif) dari piksel sebelumnya (0,0).

Koordinat Pixel	Nilai Komponen RGB			Urutan Karakter
	R	G	B	
0,0	2	18	4	S
2,4	3	19	2	T
5,6	3	4	4	E
8,10	92	6	5	G
100,15	2	0	25	A
102, 40	8	13	10	N
110, 50	10	14	5	O
120,55	10	4	15	G
130,70	3	17	11	R
133, 81	7	0	9	A
141, 90	59	5	110	F
200, 200	0	8	0	I

Tabel 1 Daftar piksel dengan beserta nilai dari komponennya yang telah diubah (mengandung kata "steganografi")

Dari tabel di atas dapat dilihat bahwa komponen R dan B adalah selisih antara satu piksel dengan satu piksel selanjutnya.

Dalam penentuan letak piksel tempat karakter selanjutnya akan diletakkan bisa dilakukan secara acak seperti yang dilakukan di atas ataupun dengan menggunakan pola matematis tertentu tergantung dari orang yang membuat steganografinya, asalkan nilai-nilai komponen yang dimasukkan bersesuaian antara sebuah piksel dengan piksel sebelumnya ataupun pikses sesudahnya (urutan karakter).

Untuk mempermudah, pada makalah ini karakter awal ditaruh pada piksel petama pada gambar (piksel dengan koordinat 0,0) dan karakter terakhir terletak pada pada piksel terakhir pada gambar, pada contoh di atas citra digital berukuran 200x200 piksel, jadi karakter terakhir berada pada koordinat 200,200.

Untuk melakukan penggantian piksel bisa dilakukan dengan metode pengubahan piksel secara manual pada bab III poin A.

C. Metode untuk Dekripsi

Untuk melakukan pada dekripsi pada steganografi dengan metode pada makalah ini tidak terlalu rumit.

Langkah-langkah dekripsi:

1. Untuk melakukan dekripsi, pertama kita perlu melihat piksel pertama pada citra digital yang terletak pada koordinat 0,0.
2. Setelah mendapatkan karakter pertama pada nilai komponen G pada piksel pertama tersebut , kita bisa melihat di mana karakter selanjutnya berada dengan melihat nilai komponen R dan B pada piksel pertama tersebut.
3. Melakukan iterasi langkah dua pada piksel-piksel selanjutnya sampai piksel yang kita ambil mencapai koordinat akhir dari citra digital (misal citra dengan resolusi 1024x768 piksel, maka koordinatnya adalah 1024,768)
4. Kita mendapatkan pesan rahasia yang disembunyikan pada pesan yang ada pada citra digital.
5. Jika kita mendapatkan pesan yang tidak bermakna, berarti kita salah saat melakukan pendekripsian yang bisa disebabkan karena kurangnya ketelitian atau bisa disebabkan oleh kesalahan dari pihak yang melakukan steganografi.

IV. IMPLEMENTASI

Setelah kita mendapatkan dua metode di atas, yaitu metode untuk mengubah piksel pada citra digital secara manual dan metode steganografinya pada piksel-piksel yang ada. Kita akan mencoba untuk menyembunyikan sebuah pesan pada citra digital.

Misal pesan yang akan kita sembunyikan sebagai berikut:

"Kode: 1234
Besok pagi, laporkan semua kejadian di TKP"

Kita ingin menyembunyikan pesan tersebut pada suatu citra digital dengan cara yang ada di makalah ini.

Langkah-langkah:

1. Kita buka suatu citra digital sembarang dengan kakas image editor (dalam implementasi steganografi ini,penulis menggunakan Microsoft Paint)

Gambar 10 Citra Digital yang akan disisipi pesan rahasia

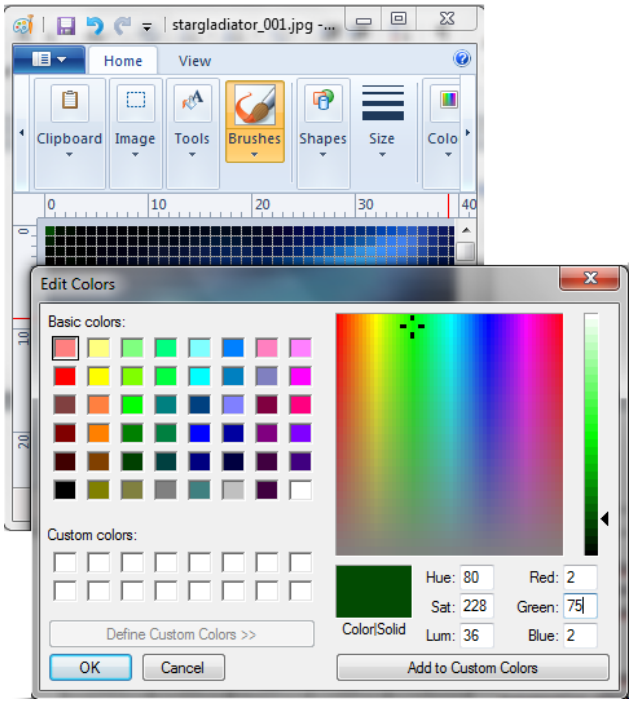
2. Kita membuat daftar di piksel mana saja karakter akan disembunyikan (opsional, memudahkan kita untuk mengecek urutan karakter, sehingga pada pesan yang kita sembunyikan tidak ada kesalahan urutan atau kesalahan penempatan karakter pada piksel).

Koordinat Pixel	Nilai Komponen RGB			Urutan Karakter
	R	G	**B**	
0,0	2	75	2	K
2,2	3	111	4	o
5,6	2	100	2	d
7,8	3	101	3	e
10,11	5	58	8	:
15,19	23	32	21	Spasi
38,40	12	49	20	1
50,60	24	50	38	2
74,98	25	51	3	3
99,101	101	52	66	4
200,167	34	10	3	Enter
234,170	16	66	20	B
250,190	37	101	30	e
287,220	53	115	38	s
340,258	40	111	22	o
380,280	20	107	30	k
400,310	20	32	20	spasi
420,330	20	112	17	p
440,347	40	97	51	a
480, 398	30	103	15	g
510,413	20	105	21	i
530,434	25	44	22	,
555,456	15	32	21	spasi
570,477	21	108	21	l
591,498	21	97	2	a
612,500	11	112	3	p
623,503	17	111	20	o
640,523	26	114	25	r
666,548	14	107	22	k
680,570	20	97	23	a
700,593	30	110	6	n
730,599	14	32	5	spasi
744,604	26	115	13	s
770,617	11	101	6	e
781,623	18	109	11	m
799,634	101	117	15	u
810,649	13	97	18	a
823,667	22	32	16	spasi
845,683	22	107	11	k
867,694	21	101	5	e
888,699	13	106	4	j
901,703	22	97	4	a
923,707	24	100	4	d
947,711	2	105	6	i
949,717	5	97	21	a
954,738	13	110	7	n
967,745	11	32	4	spasi
978,749	11	100	6	d
989,755	10	105	4	i
999,759	12	32	2	spasi
1011,761	9	84	6	T
1020,767	4	75	1	K
1024,768	6	80	14	P

Tabel 2 Daftar piksel dari citra digital beserta dengan nilai dari komponen yang akan diubah (mengandung pesan yang tercantum di atas)

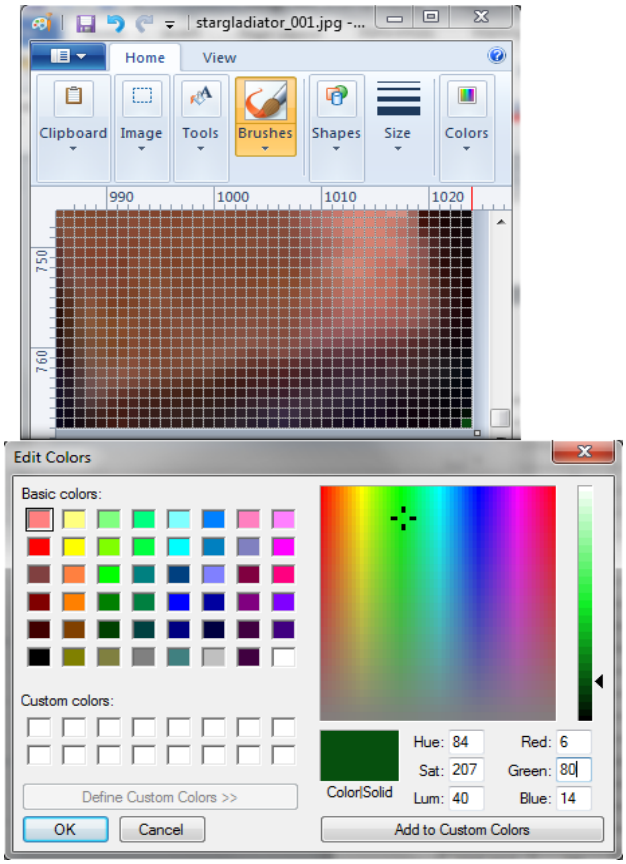
Untuk membuat daftar di atas diperlukan tabel ASCII, boleh yang extended atau standar asalkan tidak menggunakan karakter yang ada di luar tabel ASCII tersebut.

3. Setelah kita membuat daftar piksel-piksel yang akan disisipi karakter, kita melakukan penggantian nilai-nilai komponen pada tiap piksel sesuai dengan daftar yang kita buat tadi, mulai dari karakter pertama, kedua sampai karakter terakhir.



Gambar 11 Pengubahan piksel untuk karakter pertama pada citra digital.

Proses penggantian piksel dilakukan terus sampai pada karakter terakhir.



Gambar 12 Pengubahan piksel untuk karakter terakhir pada citra digital.

4. Setelah penggantian piksel mencapai karakter terakhir, maka steganografi pesan di atas selesai dilakukan. Kita akan mendapatkan sebuah citra digital yang sudah terdapat pesan rahasia di dalamnya.

Gambar 13 Citra Digital yang sudah disisipi pesan rahasia

V. ANALISIS METODE DAN IMPLEMENTASI

Dari metode dan hasil implementasi di atas bisa dilakukan analisis terhadap kelebihan dan kelemahan dari steganografi citra digital dengan menggunakan metode di atas.

Kelemahan:

- Semakin panjang pesan yang disembunyikan maka waktu yang dibutuhkan untuk melakukan steganografi dan melakukan dekripsi pesan rahasia pada citra digital tersebut akan menjadi semakin lama. Ini disebabkan karena metode ini merupakan metode manual. Untuk mengatasi masalah ini bisa dibuat program yang bisa mengakses sejumlah piksel secara langsung pada citra digital dan mengganti nilai-nilai komponennya.
- Pesan mudah didekripsi apabila sudah konsep akan metode tersebut sudah diketahui karena tidak membutuhkan kakas atau program yang bermacam-macam.
- Faktor presisi sangatlah berpengaruh saat melakukan penggantian piksel-piksel secara manual. Karena kesalahan penggantian piksel-piksel yang ada akan berdampak pada pesan yang akan disembunyikan menjadi aneh atau malah menjadi pesan yang tidak bermakna. Hal ini juga berlaku saat melakukan dekripsi.
- Citra digital akan menjadi sangat aneh ketika melakukan steganografi tersebut pada citra-citra digital yang mempunyai resolusi yang sangat kecil. Ini membuat perbedaan warna yang sangat diskrit sehingga citra digital menjadi tidak lazim dan menimbulkan kecurigaan akan adanya pesan rahasia di dalamnya.
- Pada model warna RGB perujukan piksel selanjutnya

tidak terlalu dinamis karena hanya terdiri dari tiga komponen saja.

Kelebihan:

- Ketika steganografi dilakukan pada citra digital dengan resolusi tinggi, maka citra yang dihasilkan tidak akanberbeda dengan citra aslinya (sangat mirip dengan aslinya), hal ini terlihat dari hasil implementasi, kecuali citra digital tersebut diperbesar sampai berlipat-lipat.
- Sulit untuk dipecahkan,bila tidak mengetahui metodenya, kecuali orang yang bersangkutan melakukan pelacakan semua kombinasi secara bruteforce pada semua piksel yang ada.
- Tingkat kecurigaan atas adanya pesan rahasia pada citra digital sangatlah kecil.
- Metode ini tidak membutuhkan keahliah khusus, sehingga orang awam-pun bisa melakukan implementasi metode steganografi ini.

Selain kelebihan dan kelemahan dari steganografi di atas, dapat diambil juga beberapa hal penting, yaitu:

- Besar-kecilnya resolusi citra digital berpengaruh pada tingkat kecurigaan akan adanya pesan rahasia pada citra digital tersebut (citra digital terlihat lazim atau tidak)
- Panjang-pendeknya pesan akan mempengaruhi waktu yang dilakukan untuk melakukan steganografi dan dekripsi (kecuali digunakan program khusus).
- Semakin kaya warna yang ada pada citra digital juga mempengaruhi seberapa lazim gambar tersebut ketika sudah disisipi pesan rahasia.
- Agar peletakan lebih dinamis, model warna CMYK dapat menjadi alternatif dalam melakukan steganografi dengan metode pada makalah ini.
- Untuk menambahkan kesulitan dalam melakukan dekripsi, dalam melakukan peletakan karakter awal dan karakter akhir pada piksel citra digital dapat dilakukan dengan mekanisme tertentu, misalnya dengan sandi atau kode tertentu yang dipisah pemberiaanya dengan citra digital yang telah disisipi pesan (embedded image).
- Piksel terakhir juga bisa digunakan untuk mengulang proses steganografi untuk karakter selanjutnya apabila pesan yang ada terlalu panjang diletakkan pada citra digital.
- Untuk mendapatkan presisi yang lebih saat melakukan pengubahan piksel, kita dapat menggunakan kakas yang lebih bagus seperti Adobe Photoshop.

V. KESIMPULAN

Dari hasil analisis di atas dapat diambil beberapa kesimpulan, yaitu:

- Dengan menggunakan pengubahan piksel secara manual pada citra digital, kita bisa melakukan steganografi pesan teks dengan menyisipkan karakter yang ada pada nilai komponen-komponen penyusun dari piksel citra digital.
- Metode steganografi pada makalah ini mudah dipelajari, sehingga orang awam-pun tidak terlalu sulit dalam memahaminya.
- Dengan menggunakan kakas (image editor) yang cukup umum digunakan pada masyarakat, metode ini bisa diimplementasikan sehingga orang yang ingin mengimplementasikan metode ini tidak perlu belajar akan kakas tertentu dari awal.
- Pengembangan metode ini masih bisa dilakukan lebih lanjut lagi mengingat banyaknya eksplorasi yang bisa dilakukan terhadap komponen-komponen citra digital yang ada.

REFERENSI

[1] Munir, Rinaldi, “Watermarking”, slide kuliah IF3058 Steganografi, hal. 1-27.

[2] http://en.wikipedia.org/wiki/CMYK_color_model diakses pada Minggu, 20 Maret 2011.

[3] http://en.wikipedia.org/wiki/Digital_image diakses pada Jum'at, 18 Maret 2011.

[4] http://en.wikipedia.org/wiki/Pixel diakses pada Jum'at, 18 Maret 2011.

[5] http://en.wikipedia.org/wiki/Raster_graphics diakses pada Jum'at, 18 Maret 2011.

[6] http://en.wikipedia.org/wiki/RGB_color_model pada Minggu, 20 Maret 2011.

[7] http://en.wikipedia.org/wiki/RGB_color_space diakses pada Minggu, 20 Maret 2011.

[8] http://id.wikipedia.org/wiki/Piksel diakses pada Minggu, 20 Maret 2011.

[9] http://en.wikipedia.org/wiki/Piksel diakses pada Minggu, 20 Maret 2011.

[10] http://en.wikipedia.org/wiki/Piksel diakses pada Minggu, 20 Maret 2011.

[11] http://www.mahamerubali.com/desain_grafik/format_grafik_rgb_-_cmyk.html diakses pada Minggu, 20 Maret 2011.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 23 Maret 2011

ttd

Aridarsyah Eka Putra
13507058