Studi analisis dan perbandingan teknik steganografi citra pada domain spasial, domain frekuensi, dan domain kompresi

Fadhil Muhtadin - 13510070
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13510070@std.stei.itb.ac.id

***Abstrak*—Steganografi adalah ilmu menyembunyikan pesan sehingga orang lain tidak dapat melihatnya. Seiring dengan berkembangnya teknologi informasi, kebutuhan akan metode atau media untuk mengirimkan pesan secara aman mulai bertambah. Ada banyak cara untuk melakukannya, seperti melakukan enkripsi pada pesan atau steganografi yang menyembunyikannya di dalam pesan lain agar tidak dapat terdeteksi. Steganografi sendiri sudah ada sejak lama, mulai dari masa peradaban yunani. Pada era digital sekarang ini, metode steganografi mulai merambah ranah digital. Pada steganografi digital, data digital berupa file digital yang direpresentasikan dalam kode biner dapat disisipkan pada file digital lainnya sebelum kemudian dikirim, agar penyadap pesan tidak dapat mendeteksi adanya pesan rahasia dalam file yang dikirim tersebut. File digital ini ada berbagai macam, dapat berupa file text, dokumen, gambar, audio, maupun video. Pada makalah ini, yang menjadi fokus adalah teknik-teknik yang digunakan dalam steganografi pada citra digital.**

***Kata kunci*—steganografi citra, domain spasial, domain frekuensi, domain kompresi.**

I. PENDAHULUAN

Kata Steganografi berasal dari bahasa yunani yakni *steganos* yang artinya tertutupi atau terproteksi, dan *graphei* yang artinya tulisan. Steganografi adalah seni dan ilmu menulis pesan rahasia sehingga tidak ada siapapun kecuali pengirim pesan dan orang yang dituju yang dapat mendeteksi adanya pesan tersebut, sebuah metode sekuriti lewat penyembunyian. Keunggulan penggunaan steganografi dibandingkan kriptografi adalah psean rahasia tersebut tidak mengundang perhatian sama sekali. Walaupun kita dapat mengenkripsi pesan rahasia yang sulit dipecahkan, bila terlihat bahwa pesan tersebut merupakan pesan yang terenkripsi, maka orang lain akan curiga dengan pesan tersebut. Sehingga upaya untuk memecahkan kode pesan tersebut dapat dilakukan, atau bahkan pesan tersebut tidak boleh dikirimkan sama sekali. Pada praktiknya, kebanyakan yang dilakukan adalah penggabungan kedua metode tersebut, sehingga jika pesan rahasia dapat dideteksi keberadaannya, pesan tersebut dalam keadaan terenkripsi sehingga sangat sulit bagi penyadap untuk mendapatkan pesan aslinya.

Steganografi sendiri sudah dilakukan sejak zaman dahulu. Penggunaan pertama kali dilakukan oleh bangsa yunani pada tahun 440 sebelum masehi dengan menuliskannya pada lapisan kayu yang kemudian dilapisi oleh lilin. Histiaeus juga pernah melakukannya dengan menuliskan pesan pada kepala budak-budak yang dicukur gundul. Setelah rambutnya tumbuh kembali baru budak-budak tersebut dikirimkan ke tujuan. Pada sekitar tahun 100 masehi, tulisan dengan menggunakan tinta transparan mulia digunakan. Getah dari tumbuhan *Thythimallus* digunakan sebagai tinta tarnsparan yang hanya dapat dilihat jika dipanaskan hingga berwarna coklat. Pada perang dunia 2, teks panjang digunakan untuk mengkamuflase pesan rahasia. Demikian banyaknya metode steganografi yang digunakan sebelum merambah ke ranah digital.

Dengan berkembangnya teknologi komputer digital, teknik-teknik steganografi modern mulai digunakan. Pada intinya, steganografi digital melakukan penyisipan bit-bit pesan rahasia kedalam bit-bit pesan *cover*. Sehingga metode ini dapat diaplikasikan ke dalam berbagai jenis file digital, karena pada dasarnya semua file digital dapat direpresentasikan menggunakan bit-bit biner.

Steganografi digital memiliki banyak ragam aplikasi. Mulai dari organisasi atau badan kemanan suatu negara yang membutuhkan cara untuk mensirkulasikan pesan secara aman, watermarking untuk perlindungan properti intelektual, penyisipan data pasien pada gambar medikal untuk mengurangi waktu transmisi pesan, sampai penggunaannya pada beberapa printer modern.

Pada makalah ini, fokus kita adalah metode steganografi pada citra digital. Steganografi pada citra berupaya menyisipkan pesan rahasia dalam sebuah *cover image* sehingga gambar yang sudah disusupi pesan tidak terlihat berbeda dari gambar aslinya. Pesan tersebut dapat berupa text maupun gambar lainnya. Steganografi citra menjadi salah satu cara favorit, karena pada file gambar terdapat banyak bit-bit redundan yang dapat dipakai sebagai tempat menyisipkan pesan sehingga gambar tidak banyak berubah. File video dan audio juga memiliki

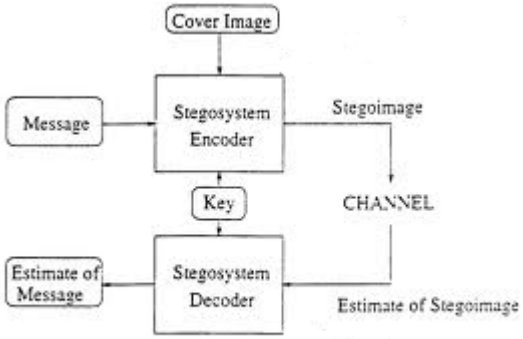
banyak bit redundan, namun karena ukurannya yang besar, maka file gambar menjadi lebih disukai.

Pada steganografi digital yang akan kita bahas, terdapat tiga macam metode, yakni metode yang menggunakan domain spasial, domain frekuensi, dan domain kompresi. Kita akan membahas perbandingan di antara ketiga metode tersebut.

II. Dasar Teori

A. Skema Steganografi

Secara umum, skema metode stganografi citra adalah sebagai berikut



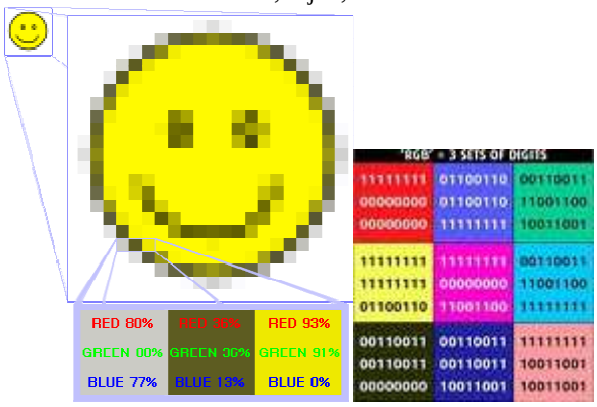
Gambar 1 – Skema Steganografi citra

Pertama, gambar yang akan menjadi cover image dipilih sesuai ukuran yang kira-kira mencukupi untuk menyimpan pesan rahasia. Lalu encoder menyisipkan bit-bit pesan ke dalam cover image sesuai teknik algoritma steganografi yang digunakan. Pesan ini dapat dienkripsi terlebih dahulu sebelumnya. Peletakan bit-bit tempat pesan disisipkan dapat dilakukan secara sekuensial maupun secara acak agar lebih aman. Jika dilakukan secara acak, peletakan bit-bit tersebut ditentukan oleh kunci yang dimasukkan pengguna. Kunci inilah yang nanti dapat dipakai oleh penerima pesan untuk mengekstrak pesan dari gambar. File gambar yang telah disisipi ini disebut sebagai stego-image dan file inilah yang dikirim ke penerima.

B. Domain Spasial

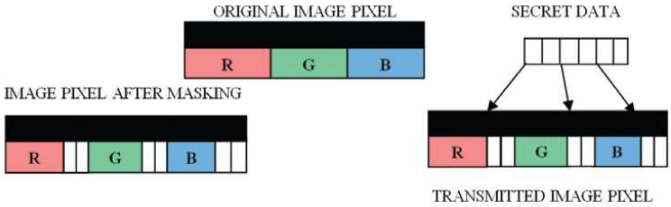
Sebuah file gambar digital terdiri atas pixel-pixel. Sebuah pixel adalah titik fisik atau elemen terkecil dari sebuah file gambar. Pada sistem pewarnaan digital, sebuah warna pada umumnya direpresentasikan oleh 3 atau 4 komponen yakni merah, hijau, dan biru (RGB) atau cyan, magenta, yellow, black (CMYK). Pada layar komputer, skema yang digunakan adalah sistem warna RGB.

Pada sistem RGB, tiap warna pixel direpresentasikan oleh komponen warna merah, hijau, dan biru. Ukuran bit yang digunakan dalam pixel bergantung format yang digunakan. Ukuran ini diukur dalam bit per pixel (bpp). Satu bpp artinya tiap pixel memiliki 1 bit. Pada umumnya format yang digunakan adalah 24 bpp dimana 1 pixel memiliki 3 byte, yang masing-masing byte menyatakan nilai intensitas warna merah, hijau, dan biru.



Gambar 2 – Contoh pixel pada sebuah file citra dan representasi warna pixel dalam 24bit

Pada domain spasial, file citra pertama didekomposisi menjadi bidang bit representasi dari tiap-tiap pixelnya dan *Least Significant bit* (LSB) dari tiap pixel diganti menjadi bit-bit pesan rahasia.



Gambar 3 – Metode steganografi domain spasial

Metode ini memanfaatkan kelemahan indra pengelihatan manusia dalam mengemati perubahan sedikit pada gambar. Karena yang diubah hanyalah LSB, maka gambar tersebut secara visual tidak mengalami banyak perubahan sehingga tidak dapat dideteksi oleh indra manusia.

C. Domain Frekuensi

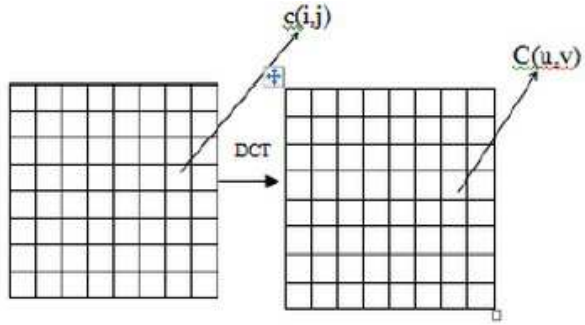
Penemuan metode LSB merupakan suatu pencapaian yang cukup luar biasa. Namun, seperti yang terjadi pada ilmu kriptografi yang melahirkan ilmu kriptoanalisis, pada steganografi juga berkembang ilmu steganalisis beriringan dengan munculnya sebuah metode steganografi yang baru. Metode LSB diatas kurang aman terhadap serangan, sehingga diperlukan metode yang lebih *robust*. Akhirnya ditemukanlah metode penyisipan pada domain frekuensi.

Pada umumnya, file citra digital berbentuk file yang terkompresi. Kompresi dilakukan agar bit-bit redundan pada file dapat dikurangi dan ukuran file dapat diperkecil secara drastis agara tidak menmakan space memory.

Domain frekuensi adalah domain analisis fungsi matematis atau sinyal terhadap frekuensi (dibandingkan pada domain spasial yang mengguanakan ruang atau

waktu). Metode penyisipan pada domain frekuensi berupaya agar bit-bit pesan disisipkan pada bit-bit yang signifikan pada file, sehingga saat kompresi dilakukan, kerusakan pada bit-bit pesan dapat dikurangi.

Pada salah satu tipe file gambar digital yang sering digunakan, yakni file JPEG, kompresi yang dilakukan berbasiska metode Discrete Cosine Transformation (DCT). DCT adalah transformasi yang mengekspresikan sejumlah data points sebagai jumlah dari fungsi cosine yang berosilasi pada frekuensi yang berbeda. Metode DCT menggunakan koefisian DCT untuk mentransformasi gambar dari domain spasial ke dalam domain frekuensi.



Gambar 4 – Transformasi domain spasial ke domain frekuensi dengan DCT

Rumus umum DCT untuk data 1 dimensi (N data item) adalah sebagai berikut:

$$C(u) = a(u)\sum_{x=0}^{N-1} f(x)\cos[\frac{(2x+1)u\pi}{2N}]$$

Sedangkan rumus untuk 2 dimensi (Gambar NxM) adalah sebagai berikut:

$$C(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos[\frac{(2x+1)u\pi}{2N}]\cos[\frac{(2y+1)v\pi}{2N}]$$

Pada rumus ini, c(i,j) adalah intensitas warna pixel pada baris i dan kolom j. C(u,v) adalah koefisien DCT pada baris u dan kolom v pada matrix DCT. Kompresi dapat dicapai karena nilai pada matrix bagian kanan bawah merepresentasikan frekuensi yang tinggi dan cukup kecil untuk dapat diabaikan tanpa mendistorsi gambar.

Pada steganografi, DCT digunakan dengan metode seperti berikut:

i. File gambar dipecah menjadi 8x8 blok pixel
ii. Dari kiri ke kanan, atas ke bawah, DCT diaplikasikan pada tiap blok
iii. Tiap blok dikompresi menggunakan tabel kuantisasi menjadi DCT koefisien dan bit-bit pesan disisipkan ke dalam DCT koefisien tersebut.

D. Domain Kompresi

Pada perkembangan terakhir, para ahli mulai mengembangkan cara baru untuk steganografi yang menggunakan domain kompresi. Metode dengan domain kompresi berusaha untuk menyisipkan bit-bit pesan rahasia langsung ke dalam bit-bit file gambar yang telah terkompresi.

Salah satu metode yang diajukan adalah metode menggunakan *Block Truncation Coding* (BTC). Teknik ini berupaya memanipulasi bitmap yang dihasilkan dari *Block Truncation Coding.* Pada fase encoding dari BTC, file gambar pertama-tama dibagi menjadi blok-blok nxn pixel yang tidak saling overlap. Untuk tiap blok, nilai rata-rata pixel dikalkulasi. Semua pixel dalam blok dibagi ke dalam 2 grup, grup pertama adalah pixel yang nilainya lebih besar dari nilai rata-rata, sedangkan grup kedua adalah pixel yang nilainya lebih kecil dari atau sama dengan nilai rata-rata. Sebuah bitmap dengan ukuran yang sama dengan blok tersebut digunakan untuk menyimpan hasil kompresi BTC. Bit pada bitmap diset menjadi 1 jika termasuk dalam grup pertama dan diset menjadi 0 jika termasuk dalam grup kedua. Kemudian nilai rata-rata bit pixel pada grup pertama dan kedua dihitung dan digunakan untuk mengkompresi gambar asli menjadi bitmap dengan 2 level kuantisasi. Metode steganografi domain kompresi kemudian menyisipkan bit-bitpesan rahasia ke dalam bitmap blok yang bersangkutan.

E. Ukuran Performansi

Pada umumnya ukuran performansi sebuah metode steganografi dapat diukur dengan parameter-parameter dibawah ini:

Kapasitas penyisipan, yakni seberapa besar file atau pesan yang dapat disisipkan tanpa terlalu mendistorsi fila gambar asli.

Transparansi Persepsi, yaitu apakah file stego-image yang dihasilkan tidak jauh berbeda dari file gambar aslinya. Parameter ini biasanya diukur menggunakan *Peak Signal to Noise Ratio* (PSNR) yakni arameter pengukuran distorsi sebuah file citra. Rumus PSNR diberikan dibawah

$$PSNR = 20\log_{10}(\frac{MAX_I}{\sqrt{MSE}})$$

Dimana MAX adalah nilai maksimum yang mungkin untuk sebuah pixel gambar. MSE adalah *Mean Square Error* yang rumusnya adalah sebagai berikut

$$\frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j)-K(i,j)]^2$$

I adalah pixel gambar asli berukuran mxn sedangkan K adalah pixel stego-image.

Robustness, yakni seberapa tangguh metode penyisipan terhadap berbagai macam transformasi gambar seperti crop, rotasi, dan kompresi.

Kompleksitas komputasi, yaitu seberapa efisien algoritma penyisipan efisien terhadap waktu dan ruang memori.

III. PEMBAHASAN

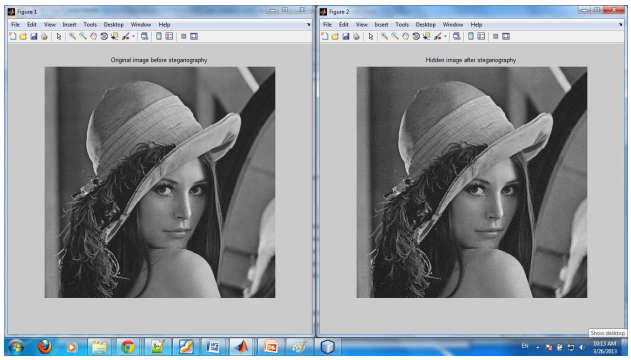
A. Metode Pengujian

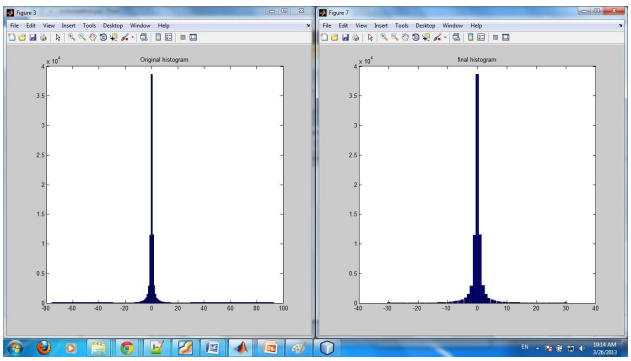
Pengujian dilakukan menggunakan kode MATLAB yang dapat diunduh. Gambar yang digunakan adalah 2 buah gambar grayscale, yakni lena.bmp dan rose.jpg.

Untuk parameternya digunakan PSNR sebagai parameter utama. Kode untuk menghitung PSNR adalah sebagai berikut

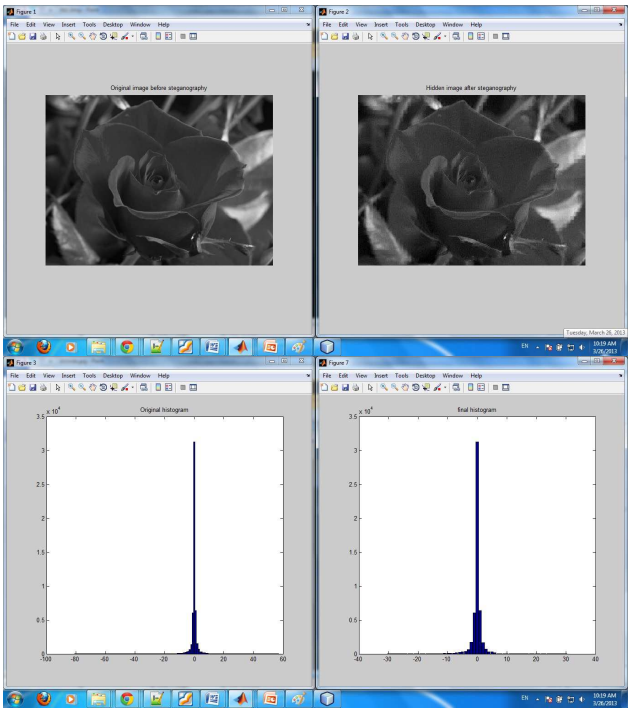
```
function PSNR(A,B)


if A == B
   error('Images are identical:
PSNR has infinite value')
end

max2_A = max(max(A));
max2_B = max(max(B));
min2_A = min(min(A));
min2_B = min(min(B));

if max2_A > 1 || max2_B > 1 ||
min2_A < 0 || min2_B < 0
   error('input matrices must
have values in the interval
[0,1]')
end

error_diff = A - B;
decibels =
20*log10(1/(sqrt(mean(mean(error_
diff.^2)))));
disp(sprintf('PSNR = +%5.2f
dB',decibels))
```

Berikut contoh hasil pengujian terhadap algoritma DCT.





Gambar 5 – Gambar lena sebelum disisipkan (kiri) dan setelah disisipkan (kanan) beserta histogramnya



Gambar 6 - Gambar rose sebelum disisipkan (kiri) dan setelah disisipkan (kanan) beserta histogramnya

Terlihat dari histogramnya terdapat sedikit perbedaan antara gambar yang belum disisipi dengan yang sudah. Ini menyatakan bahwa algoritma DCT yang dipakai masih menghasilkan sedikit distorsi.

B. Hasil Pengujian

Gambar	Metode	PSNR
lena	LSB	57.14
	DCT	43.21
	BTC	39.91
rose	LSB	59.57
	DCT	46.43
	BTC	42.17

Dilihat dari tabel diatas, terlihat bahwa kualitas PSNR

yang lebih baik ada pada metode yang menggunakan domain spasial ketimbang domain transformasi. Ini terjadi karen pada domain spasial, bit-bit pesan langsung disisipkan pada Least Significant Bit sedangkan pada domain transformasi seperti domain frekuensi dan kompresi menggunakan bit-bit yang cukup signifikan. Namun trade-off yang didapatkan adalah bahwa metode spasial tidak *robust* terhadap metode domain transformasi.

IV. KESIMPULAN

Jika diibandingkan antara metode steganografi domain spasial, frekuensi dan kompresi, masing-masing metode memiliki keunggulannya masing-masing.

Metode dengan domain spasial pada umumnya memiliki kapasitas penyisipan yang besar karena yang dimanipulasi adalah bit-bit gambar secara langsung tanpa kompresi. Namun, metode ini dianggap kurang aman karena rentan terhadap transformasi file citra seperti kompresi dan rotasi. Hal ini dikarenakan bit-bit pesan disisipkan hanya pada LSB dari citra secara langsung yang sangat mungkin merupakan bit-bit redundan yang dapat rusak oleh transformasi.

Metode yang menggunakan domain transformasi seperti domain frekuensi dan domain kompresi pada umumnya lebih *robust* terhadap tarnsformasi karen bit-bit pesan disimpan ke dalam bit-bit file citra yang signifikan, namun trade-offnya adalah kapasitas penyisipan yang berkurang dibandingkan metode domain spasial.

Secara umum pula dapat dikatakan bahwa terdapat tarde-off antara kualitas stego-image terhadap kapasitas penyisipan. Kita dapat menyisipkan pesan yang lebih besar namun dengan risiko kualitas stego-image tidak terlalu baik, dengan artian file stego-image yang dihasilkan sangat terdistorsi dari file citra aslinya sehingga mudah dideteksi dengan teknik stegoanalisis yang menggunakan parameter seperti *Peak Signal to Noise Ratio*.

Akhir kata, steganografi merupakan alat yang cukup handal dalam mengirimkan pesan rahasia. Dengan demikian banyak pula risiko teknologi ini digunakan untuk tujuan yang tidak baik. Seperti contohnya penggunaannya oleh jaringan teroris untuk saling bertukar pesan rahasia. Maka dari itu, sebaiknya kita yang memahami teknologi tersebut tidak menyalahgunakannya.

DAFTAR REFERENSI

[1] Anu, Rekha, Praveen, “Digital Image Steganography”, India: Gurgaon College of Engineering, 2011.

[2] Hardik Patel, “*Steganography Techniques Based On DCT Coefficients*”. International Journal of Engineering Research and Application, 2012.

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, 25 Maret 2013

ttd

Fadhil Muhtadin
13510070