

Implementasi Steganografi dengan Metode *Bit-Plane Complexity Segmentation (BPCS)* untuk Dokumen Citra Terkompresi

Arya Widyanarko - 13504030

Program Studi Teknik Informatika, Institut Teknologi Bandung, Jl. Ganesha 10 Bandung

Email: if14030@students.if.itb.ac.id

Abstract – Steganografi adalah suatu teknik untuk menyembunyikan suatu informasi yang rahasia atau sensitif tanpa terlihat agar tidak terlihat seperti semestinya. Data rahasia disembunyikan dengan cara disisipkan pada suatu media tertentu sehingga tidak terlihat bahwa dalam media tersebut disembunyikan suatu informasi. *Bit-Plane Complexity Segmentation (BPCS)* adalah salah satu metode steganografi, dimana metode ini memiliki kapasitas penyisipan pesan yang relatif besar jika dibandingkan dengan metode lain seperti *Least Significant Bit*. Pada makalah ini, dikembangkan sebuah perangkat lunak *Secret-Postcard* yang mengaplikasikan steganografi dengan metode *BPCS* dengan media citra terkompresi (*compressed image*). Selain itu dilakukan pengujian hasil implementasi *BPCS* pada citra terkompresi ini. Sebelum melakukan implementasi perangkat lunak, dilakukan analisis kecocokan metode ini dengan media citra terkompresi. Analisis dilakukan pada tiga format citra terkompresi, yaitu *JPEG (Joint Photograph Expert Graphics)*, *GIF (Graphics Interchange Format)* dan *PNG (Portable Network Graphics)*. Implementasi dan pengujian dilakukan pada satu format gambar yang dianggap paling sesuai dengan *BPCS*.

Kata kunci: *Steganography, Bit-Plane Complexity Segmentation, Compressed Image, Portable Network Graphics.*

1. PENDAHULUAN

Internet saat ini telah menjadi bagian yang sangat penting bagi infrastruktur komunikasi di dunia. Pertukaran informasi melalui internet memiliki banyak kelebihan dibandingkan dengan media komunikasi lainnya, terutama dari segi kecepatannya. Namun informasi yang dikirimkan melalui internet tidak dapat dijamin keamanannya. Penyesuaian terhadap informasi rahasia sering terjadi pada media komunikasi ini. Saluran yang digunakan internet pada umumnya bukan merupakan saluran yang aman. Saluran yang aman sebenarnya tersedia, namun kecepatan koneksi menggunakan saluran yang aman ini cenderung lambat.

Terdapat beberapa usaha untuk menangani masalah keamanan data rahasia yang dikirimkan melalui internet, diantaranya adalah menggunakan teknik

kriptografi dan steganografi. Steganografi adalah teknik menyembunyikan data rahasia ke dalam data lainnya sehingga perubahan yang terjadi tidak terlihat mencurigakan.

Pada makalah ini dibahas mengenai steganografi dengan metode *Bit-Plane Complexity Segmentation* dengan media citra terkompresi. Metode *BPCS* ini diperkenalkan oleh Eiji Kawaguchi dan R. O. Eason pada tahun 1997 [KAW97]. Metode *BPCS* ini memanfaatkan perhitungan kompleksitas pada tiap *bit-plane* dalam menyelipkan informasi rahasia [KAW97]. Kelebihan metode ini jika diterapkan pada dokumen citra dengan format *bitmap* adalah memiliki kapasitas penyisipan data rahasia yang lebih besar dibanding metode lain. Sejauh ini metode *BPCS* baru diterapkan pada dokumen citra dengan format *bitmap*, tidak pada dokumen citra terkompresi.

2. CITRA DIJITAL

Citra digital memiliki informasi berupa gambar dan terdiri dari elemen terkecil yaitu piksel. Citra digital direpresentasikan dalam bentuk matriks 2 dimensi yang setiap elemen merepresentasikan piksel pada gambar.

2.1. Warna pada Citra Digital

Terdapat beberapa jenis pewarnaan pada citra digital yaitu *duotone* (dua warna), *grayscale* dan citra berwarna. Citra berwarna dapat memiliki sistem pewarnaan *RGB, indexed color* atau *256 color*.

Pada citra digital dengan pewarnaan *duotone*, warna pada piksel hanya memiliki 2 kemungkinan warna, pada umumnya hitam-putih. Dengan penggunaan warna 1-bit, maka kualitas gambar pada citra digital tidak begitu bagus. Pewarnaan *grayscale* memiliki kualitas lebih baik. Pada *grayscale*, warna yang tersedia hanyalah warna-warna yang ada diantara hitam dan putih, meliputi warna abu-abu yang beragam.

Citra *RGB* adalah yang paling populer saat ini, dimana setiap piksel direpresentasikan dengan intensitas warna merah, hijau dan biru. Citra *indexed color* hanya memiliki 256 warna yang telah didefinisikan pada tabel warna, namun memiliki ukuran *file* yang lebih kecil.

2.2. Kompresi pada Citra Dijital

Konsep kompresi pada citra digital sama dengan kompresi pada umumnya. Pada kompresi citra digital, sebuah bit-bit citra digital yang dikompresi harus dapat didekompresi sehingga menghasilkan bit-bit piksel yang membentuk gambar seperti semula. Piksel tersebut bisa persis sama atau terjadi perubahan sedikit, bergantung pada teknik kompresi yang digunakan, teknik tersebut termasuk teknik kompresi yang *lossy* atau *lossless*.

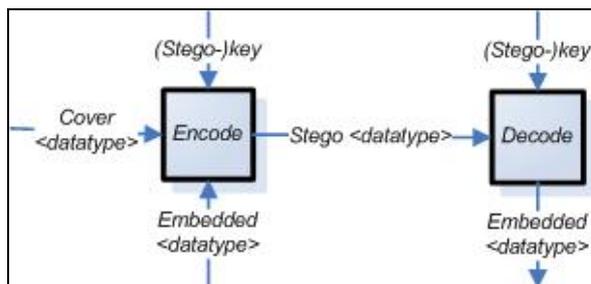
Pada teknik kompresi *lossless*, jika sebuah dokumen citra tidak terkompresi dikompresi dengan teknik kompresi *lossless* dan diexpand kembali, maka akan menghasilkan bit-bit asli yang persis sama dengan bit-bit sebelum dilakukan kompresi [MIA99]. *GIF* dan *PNG* termasuk kepada format dokumen citra yang *lossless*.

Teknik kompresi yang *lossy* digunakan oleh format *JPEG* yang dikompresi dengan *Discrete Cosine Transform (DCT)*. Dengan menggunakan teknik kompresi *lossy*, maka gambar yang dihasilkan mendekati bit-bit asli namun dilakukan perubahan sehingga tidak tepat sama dengan bit-bit yang ada pada gambar asli namun sangat mirip [MIA99]. Kelebihan dari teknik kompresi yang *lossy* adalah bahwa teknik kompresi ini menghasilkan hasil kompresi yang berukuran lebih kecil.

3. STEGANOGRAFI

Steganografi adalah teknik menyembunyikan suatu informasi yang rahasia atau sensitif pada suatu media perantara agar tidak terlihat seperti semestinya [MAN06]. Steganografi telah digunakan oleh manusia sejak zaman dahulu. Terdapat teknik steganografi klasik yang digunakan pada zaman dahulu dan teknik steganografi modern yang digunakan zaman sekarang dan lebih berorientasi pada dunia *digital*. Menurut catatan sejarah, teknik steganografi telah diterapkan semenjak tahun 484SM hingga serangan 11 September oleh teroris [BAK07].

Seiring berjalannya waktu memasuki era digital, maka teknik steganografi modern pun turut berkembang. Pada teknik steganografi modern, media penyisipan pada umumnya merupakan arsip multimedia seperti dokumen citra (*image*), suara (*audio*), atau *video*.



Gambar 1. Proses Steganografi Modern

4. BIT-PLANE COMPLEXITY SEGMENTATION

Bit-plane complexity segmentation (BPCS) adalah salah satu teknik steganografi yang diperkenalkan oleh Eiji Kawaguchi dan R. O. Eason pada tahun 1997 [KAW97]. Pada *BPCS* dokumen citra dibagi menjadi segmen-segmen dengan ukuran 8x8 piksel setiap segmennya [KAW99]. Pada dokumen citra 8-bit, setiap satu segmen akan memiliki 8 buah *bit-plane* yang merepresentasikan piksel-piksel dari setiap bit tersebut. Proses penyisipan data dilakukan pada segmen yang memiliki kompleksitas yang tinggi. Segmen yang memiliki kompleksitas tinggi ini disebut *noise-like regions*. Pada segmen-segmen ini penyisipan dilakukan tidak hanya pada *least significant bit*, tapi pada seluruh *bit-plane*.

4.1. Kompleksitas Gambar Biner

Kompleksitas gambar biner adalah suatu parameter kerumitan dari suatu gambar biner. Pada makalah ini, ukuran kompleksitas yang akan digunakan adalah *black-and-white border image complexity*. Perubahan warna hitam dan putih dalam gambar biner adalah ukuran yang baik untuk menghitung nilai kompleksitas. Jika perubahan warna yang terjadi banyak, maka gambar tersebut memiliki tingkat kompleksitas tinggi. Jika sebaliknya, maka gambar tersebut merupakan gambar yang simpel [KAW97]. Perubahan warna hitam-putih adalah jumlah dari perubahan warna yang terjadi pada setiap baris dan kolom dalam gambar. Sebagai contoh, sebuah piksel hitam yang dikelilingi piksel putih memiliki nilai perubahan warna 4.

Dengan α sebagai nilai kompleksitas, maka rumus penghitungan kompleksitas yang akan digunakan adalah [KAW97]:

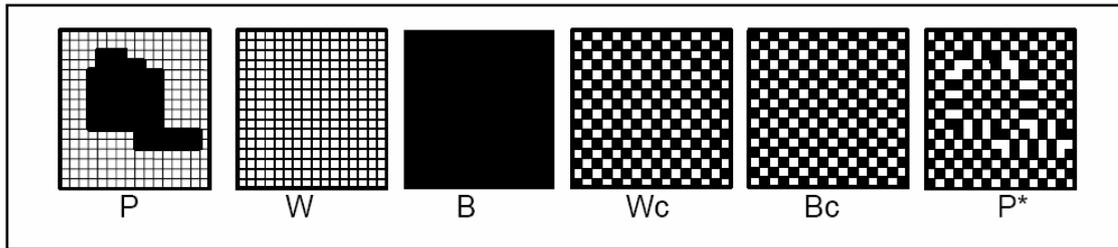
$$\alpha = \frac{k}{n} \quad \dots (1)$$

Dengan k adalah jumlah perubahan warna hitam-putih dan n adalah kemungkinan maksimal perubahan warna dalam gambar.

4.2. Konjugasi dari Gambar Biner

Konjugasi dari suatu gambar biner P adalah sebuah gambar biner lainnya yang memiliki nilai kompleksitas sebesar satu dikurangi nilai kompleksitas P . Dari Gambar 1 dapat dilihat bahwa P adalah gambar yang memiliki piksel *background* dengan pola W dan piksel *foreground* dengan pola B . P^* yang merupakan konjugasi dari P memiliki spesifikasi sebagai berikut [KAW97]:

- 1) Memiliki bentuk area *foreground* sama dengan P .
- 2) Memiliki pola area *foreground* sama dengan pola Bc .
- 3) Memiliki pola area *background* sama dengan pola Wc .



Gambar 2. Konjugasi pada Gambar Biner

Untuk membangun sebuah konjugasi P^* dari sebuah gambar P , dapat dilakukan dengan rumus berikut, dimana “ \oplus ” menandakan operasi *exclusive OR*.

$$P^* = P \oplus Wc \quad \dots(2)$$

$$(P^*)^* = P \quad \dots(3)$$

$$P^* \neq P \quad \dots(4)$$

Jika $\alpha(P)$ adalah kompleksitas dari P , maka:

$$\alpha(P^*) = 1 - \alpha(P) \quad \dots(5)$$

4.3. Informative Region dan Noise-Like Region

Informative image berarti gambar yang simpel, sementara *noise-like region* berarti gambar yang kompleks. Hal ini hanya berlaku pada kasus dimana sebuah gambar biner merupakan bagian dari sebuah gambar yang natural [KAW97].

Kompleksitas sebuah area *bit-plane* adalah parameter yang digunakan dalam menentukan sebuah *bit-plane* merupakan *informative* atau *noise-like region*. Parameter kompleksitas ini dibatasi oleh nilai *threshold* (α_0).

Sebuah *bit-plane* tergolong sebagai *informative region* apabila memiliki nilai kompleksitas yang lebih kecil dibandingkan *threshold* ($\alpha \leq \alpha_0$) dan sebaliknya akan dianggap sebagai *noise-like region*. Pada tugas akhir ini, nilai α_0 yang digunakan beragam, yaitu diantara 0,1 hingga 0,5.

4.4. Algoritma BPCS

Berikut adalah langkah-langkah yang dilakukan pada algoritma *BPCS* saat menyisipkan data [KAW99]:

- 1) Mengubah *cover image* dari sistem *PBC* menjadi sistem *CGC*. Sebelumnya, gambar tersebut di-slice terlebih dahulu menjadi *bit-plane*. Setiap *bit-plane* mewakili bit dari setiap piksel.
- 2) Segmentasi setiap *bit-plane* pada *cover image* menjadi *informative* dan *noise like region* dengan menggunakan nilai batas/*threshold* (α_0).
- 3) Bagi setiap byte pada data rahasia menjadi blok-blok.
- 4) Jika blok(S) tidak lebih kompleks dibandingkan dengan nilai batas, maka lakukan konjugasi terhadap S untuk mendapatkan S^* yang lebih kompleks.
- 5) Sisipkan setiap blok data rahasia ke *bit-plane* yang merupakan *noise-like region*. Kemudian simpan data konjugasi pada “*conjugation map*”.
- 6) Sisipkan juga pemetaan konjugasi yang telah dibuat.

- 7) Ubah *stego-image* dari sistem *CGC* menjadi sistem *PBC*.

Proses ekstraksi data rahasia dapat dilakukan dengan menerapkan langkah-langkah penyisipan secara terbalik.

5. ANALISIS

Dokumen citra yang banyak beredar saat ini sebagian besar merupakan dokumen citra terkompresi. Terdapat banyak format dokumen citra terkompresi, diantaranya *JPEG*, *GIF*, *PNG* dan *TIFF*. Namun dari sekian banyak format dokumen citra terkompresi, hanya format *JPEG*, *GIF* dan *PNG* yang akan dianalisis lebih dalam karena ketiganya merupakan format yang paling umum dan paling sering digunakan.

Ketiga format ini memiliki ciri khas masing-masing yang membedakan antara satu dan lainnya, dilihat dari teknik kompresi yang digunakan, jumlah dan jenis warna yang digunakan dan sifat kompresinya.

	JPEG	GIF	PNG
Teknik Kompresi	Huffman, DCT	LZW	Deflate
Lossy atau Lossless	Lossy	Lossless	Lossless
Warna	RGB, grayscale	Indexed color	Indexed color, grayscale, RGB
Warna Transparan	Tidak	Ya	Ya

Tabel 1. Perbandingan Citra *JPEG*, *GIF* dan *PNG*

5.1. Analisis Kecocokan BPCS dengan citra JPEG

Format *JPEG* dapat menggunakan *huffman coding* ataupun *DCT*. Yang membedakan keduanya adalah *DCT* merupakan kompresi yang *lossy*, sementara *huffman coding* merupakan kompresi yang *lossless*.

Pada *JPEG huffman coding*, algoritma *huffman* yang digunakan merupakan teknik kompresi yang *lossless*, sehingga jika dilakukan dekompresi, bit-bit gambar yang sesungguhnya akan didapatkan [MIA99]. Dengan bit-bit tersebut, maka proses pembuatan gambar biner dari bit-bit dari piksel tersebut akan dapat dilakukan dengan akurat tanpa adanya perubahan nilai bit. Maka algoritma *BPCS* dapat diterapkan pada *JPEG huffman coding*.

Permasalahan yang muncul jika yang digunakan adalah teknik *DCT*. Teknik *DCT* merupakan teknik kompresi yang *lossy* [SAL07]. Teknik kompresi ini dapat memampatkan data hingga sekecil mungkin, namun dengan melakukan perubahan pada nilai-nilai bit data. Data yang berubah adalah nilai intensitas warna pada piksel, namun tidak terlalu signifikan dan tidak terlihat jelas menggunakan mata manusia.

Permasalahan timbul karena perubahan nilai bit pada dokumen *JPEG* dapat merusak isi pesan yang disisipkan dengan menggunakan *BPCS*. Setelah melakukan penyisipan pesan dengan menggunakan *BPCS*, terjadi perubahan bit-bit saat melakukan kompresi dengan *DCT*. Dengan adanya perubahan tersebut, maka proses ekstraksi pesan tersebut akan mengalami masalah karena representasi piksel dalam bentuk bit yang telah berubah saat dekomposisi dilakukan sebelum proses ekstraksi tersebut.

Teknik *BPCS* dapat diterapkan dengan baik pada citra digital terkompresi yang *lossless*, namun tidak dengan kompresi *lossy*. Teknik ini kurang cocok jika diimplementasikan pada dokumen citra terkompresi dengan format *JPEG*.

5.2. Analisis Kecocokan *BPCS* dengan citra *GIF*

Graphics Interchange Format yang dikembangkan oleh compuserve adalah format citra terkompresi yang menggunakan algoritma kompresi *LZW*. Kompresi *LZW* ini merupakan jenis kompresi yang *lossless* [SAY03]. Seperti yang telah dibahas sebelumnya, *BPCS* dapat diterapkan dengan baik jika diterapkan pada citra digital dengan kompresi yang *lossless*. Artinya pada dokumen *GIF*, penerapan *BPCS* pada penyisipan pesan tidak akan mengakibatkan kerusakan pesan seperti pada *JPEG* dengan *DCT* yang *lossy*.

Masalah pada *GIF* muncul karena format ini hanya mendukung penggunaan *indexed color* ini. Dokumen *GIF* tidak menggunakan warna *RGB* yang membaca bit sebagai representasi piksel dalam bentuk intensitas warna masing-masing. Penggunaan *indexed color* artinya bahwa setiap dokumen *GIF* pasti memiliki tabel warna yang berjumlah maksimal 256 [MIA99].

Perubahan 1 buah *LSB* pada penggunaan tabel warna bisa saja menyebabkan perubahan warna yang cukup jauh, apalagi perubahan pointer ke tabel warna yang cukup besar. Hal ini memperbesar kemungkinan rusaknya *stego-image*. Dengan menggunakan teknik *BPCS*, akar masalah ini tidak dapat diabaikan begitu saja. Yang dimainkan pada teknik ini adalah penipuan mata dengan intensitas warna pada segmen gambar yang dianggap kompleks. Perubahan bit yang dilakukan pada *BPCS* tidak hanya pada *LSB*, tetapi bisa jadi perubahan tersebut terjadi pada *MSB*. Karena itu, jika nilai indeks berubah terlalu jauh maka bisa jadi warna piksel berubah drastis, karena perubahan satu indeks saja bisa merubah warna cukup drastis.

Dengan demikian, maka *BPCS* dapat diterapkan dengan baik tanpa ada kerusakan pesan pada dokumen *GIF*, namun berpeluang besar menyebabkan kerusakan gambar karena perubahan drastis yang terjadi antara *cover image* dan *stego-image*.

5.3. Analisis Kecocokan *BPCS* dengan citra *PNG*

Portable Network Graphics merupakan format yang paling terakhir dikembangkan dibandingkan *GIF* dan *JPEG* [ROE99]. Pengembangannya ditujukan untuk dapat menggantikan peranan format *GIF*. Teknik kompresi *deflate* dengan menggunakan algoritma *LZ77* dan *huffman* yang digunakan *PNG* merupakan teknik kompresi yang *lossless* [SAY03].

Format *PNG* mendukung jenis pewarnaan yang sangat beragam karena dapat menampung piksel dengan warna *RGB*, *grayscale* serta *indexed color* [MIA99]. Penerapan *BPCS* pada format ini tentunya tidak akan memiliki masalah besar dilihat dari aspek perubahan gambar sebelum dan sesudah penyisipan karena mendukung penggunaan warna *RGB*.

Kemungkinan terburuk yang dapat terjadi adalah jika pewarnaan yang digunakan adalah *indexed color*. Kemungkinan tersebut hanya berkaitan dengan hasil keluaran proses penyisipan yang dikhawatirkan berupa gambar yang rusak. Hal ini dapat ditangani dengan melakukan konversi pewarnaan menjadi *RGB* ketika melakukan penyisipan. Kemungkinan hilang atau rusaknya pesan rahasia tidak ada pada penerapan *BPCS* pada *PNG*. Hal tersebut cukup jelas mengingat teknik kompresi yang digunakan pada *PNG* merupakan kompresi yang *lossless*.

Dengan demikian, maka *BPCS* dapat diterapkan dengan baik pada citra digital dengan format *PNG* tanpa adanya kerusakan pesan dan hanya kemungkinan kecil menghasilkan *stego-image* yang agak terlihat rusak jika menggunakan *indexed color*. Format ini cocok dengan teknik *BPCS*.

5.4. Format Citra Terkompresi yang Digunakan dalam Implementasi

Pada proses analisis yang telah dilakukan, dibahas kecocokan masing-masing format citra *JPEG*, *GIF* dan *PNG* dengan teknik *BPCS*. Kecocokan tersebut dilihat dari aspek kekuatan penyimpanan, yaitu kemampuan menyimpan pesan tanpa adanya kerusakan dan aspek keamanan, yaitu hasil *stego-image* yang dihasilkan tidak rusak dan mencurigakan bahwa ada pesan yang tersimpan didalamnya.

Tabel 2 menunjukkan perbandingan kecocokan ketiga format citra terkompresi yang dianalisis dengan *BPCS*. Format *PNG* merupakan format yang paling cocok dengan *BPCS*. Karena itu pada implementasi *BPCS* pada makalah ini, format *PNG* yang dipilih untuk digunakan.

Aspek	JPEG	GIF	PNG
Ada bit yang hilang pada proses kompresi	Ya	Tidak	Tidak
Pesan rahasia terjaga tanpa kerusakan	Tidak	Ya	Ya
Mendukung RGB atau indexed color	RGB	Indexed Color	Keduanya
Kemungkinan kerusakan pada stego-image	Tidak	Ya	Tidak
Kecocokan dengan BPCS (skala 0-5)	3	2,5	4,5

Tabel 2. Hasil Analisis Kecocokan BPCS dengan JPEG, GIF dan PNG

5.5. Penerapan BPCS pada Citra PNG

Pada proses penyisipan, perlu dilakukan dekompresi terlebih dahulu terhadap citra PNG sebelum melakukan penyisipan pesan. Setelah melakukan penyisipan pesan, citra kembali dikompresi dengan teknik *deflate* untuk menghasilkan citra PNG keluaran.

Pada proses ekstraksi, dilakukan dekompresi terhadap citra PNG untuk mendapatkan intensitas warna setiap piksel. Kemudian pesan langsung diekstraksi dari data piksel tersebut dan diproses dengan menggunakan peta konjugasi untuk menghasilkan pesan yang sama persis dengan pesan sebelum disisipkan.

Perubahan ukuran citra PNG setelah proses penyisipan sangat mungkin terjadi karena adanya perubahan nilai bit karena penyisipan bit pesan. Ukuran citra dapat membesar maupun mengecil karena perubahan nilai bit ini akan mempengaruhi proses kompresi setelah penyisipan.

6. HASIL DAN PENGUJIAN

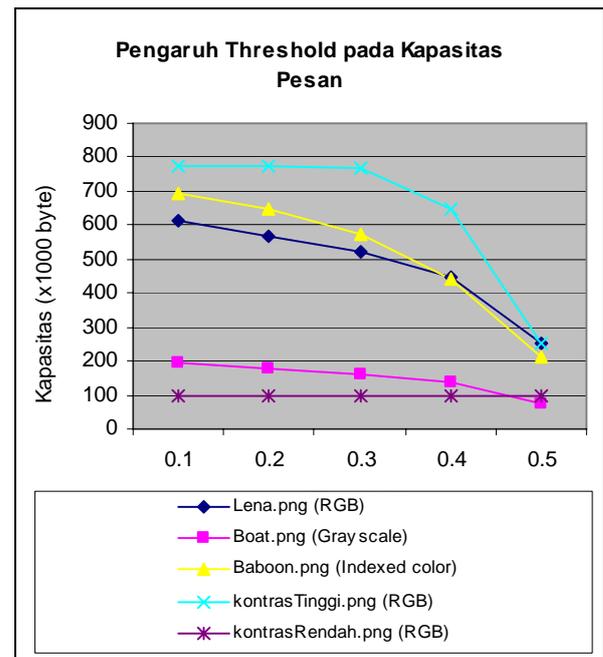
Perangkat lunak Secret-Postcard berhasil dibangun untuk mengimplementasikan metode BPCS pada citra PNG. Pengujian dilakukan terhadap perangkat lunak ini dengan 3 kriteria pengujian yaitu kebenaran program (fungsionalitas perangkat lunak), pengaruh *threshold* pada kapasitas penyisipan dan pengujian nilai PSNR sebagai parameter kualitas *stego-image*.



Gambar 3. Contoh Hasil Uji Penyisipan

Pada kriteria pengujian yang pertama, perangkat lunak Secret-Postcard telah berhasil mengimplementasikan seluruh kebutuhan perangkat lunak dalam hal fungsionalitas yaitu melakukan penyisipan, ekstraksi dan penanganan *error*. Gambar 3 menunjukkan hasil penyisipan pada citra Lena.png (703 KB) dengan pesan sebesar 224 KB.

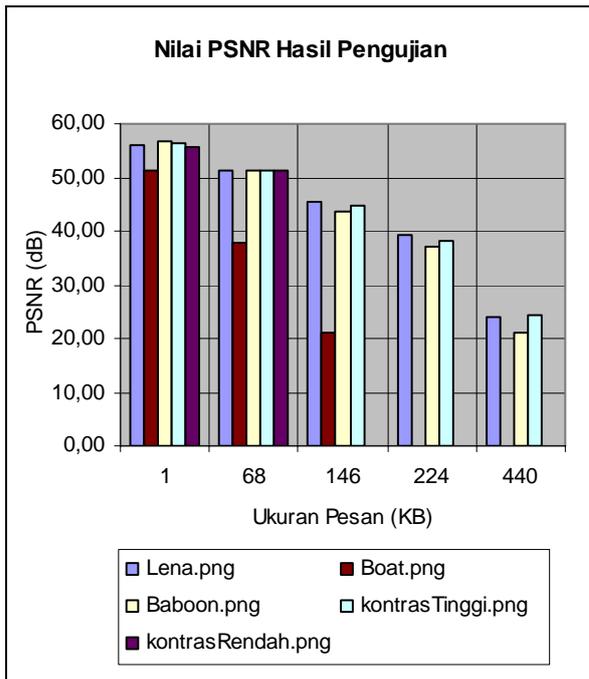
Pada kriteria pengujian kedua, dilakukan pengujian kapasitas dengan nilai *threshold* berbeda-beda pada 5 buah citra PNG berukuran 512x512 piksel.



Gambar 4. Grafik Pengaruh *Threshold* pada kapasitas

Dari gambar 4 terlihat bahwa gambar dengan kontras yang tinggi dan rendah memiliki perubahan kapasitas yang mencolok. Ini artinya bahwa gambar dengan kontras yang tinggi dapat menyimpan pesan dengan kapasitas yang lebih besar karena sebagian besar segmen pada gambar tersebut adalah *noise-like region*. Lain halnya dengan citra dengan kontras yang rendah. Pada citra dengan kontras yang rendah, kapasitas penyisipan tidak berubah pada semua *threshold*. Hal ini disebabkan jumlah segmen *noise-like region* pada gambar sangat sedikit, sehingga kapasitas penyisipan pesan tidak jauh berbeda dengan menggunakan metode LSB.

Dari grafik, dapat dilihat bahwa nilai perubahan terbesar kapasitas adalah pada saat *threshold* diantara 0,4 dan 0,5. Ini artinya pada perubahan *threshold* antara 0,4 dan 0,5 banyak daerah gambar biner yang tidak kompleks pada *threshold* 0,5 menjadi kompleks pada *threshold* 0,4. Karena itu, untuk menjaga kualitas *stego-image* yang dihasilkan, nilai *threshold* yang baik digunakan adalah 0,5. Jika membutuhkan kapasitas yang lebih besar, lebih baik menggunakan nilai *threshold* 0,3 atau 0,4.



Gambar 5. Grafik Nilai PSNR Pengujian

Gambar 5 menunjukkan grafik hasil pengujian kualitas *stego-image*. Dari grafik tersebut terlihat bahwa hasil penyisipan mengeluarkan *stego-image* yang memiliki kualitas baik hingga ukuran tertentu. Pada ukuran pesan yang sudah terlalu besar, kualitas gambar akan semakin menurun. Hal ini telah diperkirakan sebelumnya, karena untuk bisa menyisipkan pesan yang besarnya hingga 70%-80% dari *vessel image* pasti diimbangi dengan adanya kerusakan pada citra keluaran.

Dari hasil analisis pengujian ini, untuk melakukan penyisipan pesan dengan metode *BPCS* dengan citra keluaran yang terjaga kualitasnya, maka lebih baik gunakan nilai *threshold* 0,5. Selain itu, jenis dokumen pesan yang disisipkan tidak memberikan pengaruh tertentu terhadap *stego-image*. Hal ini dibuktikan dengan penggunaan jenis dokumen pesan yang beragam pada pengujian.

7. KESIMPULAN

Kesimpulan yang dapat ditarik dari pembahasan dalam makalah ini yaitu:

- 1) Steganografi dengan metode *BPCS* dapat diterapkan pada citra terkompresi tanpa adanya modifikasi pada proses utama penyisipan dan ekstraksi pesan.
- 2) Citra terkompresi *PNG* adalah format citra terkompresi yang paling cocok untuk penerapan steganografi dengan metode *BPCS* dibandingkan dengan format *GIF* dan *JPEG*.
- 3) Perangkat lunak yang mengimplementasikan steganografi dengan metode *BPCS* pada citra *PNG* berhasil dibangun.

- 4) Kapasitas maksimal penyisipan pesan pada citra *PNG* dengan menggunakan metode *BPCS* sangat besar. Kapasitas maksimal yang sangat besar ini dipengaruhi oleh dua hal, yaitu penggunaan metode *BPCS* yang merupakan metode steganografi yang memiliki kapasitas penyisipan lebih besar dibandingkan dengan metode lain dan penggunaan citra terkompresi sehingga ukuran citra lebih kecil dibandingkan dengan citra tidak terkompresi.
- 5) Pengujian nilai PSNR menunjukkan bahwa semakin besar pesan yang disisipkan, kualitas *stego-image* yang dihasilkan semakin buruk.

DAFTAR REFERENSI

- [BAK07] Bakshi, Nishesh, *Steganography*, Syracuse University, 2007.
- [BOU96] Boutell, Thomas, *PNG (Portable Network Graphics) Specification Version 1.0*, Massachusetts Institute of Technology, 1996.
- [BRO03] Brown, Adrian, *Image Compression*, The National archive, 2003.
- [FOR08] Forouzan, Behrouz, *Cryptography and Network Security*, McGraw-Hill, 2008.
- [GUA01] Guan, Ling. Kung, Sun-Yuan. Larsen, Jan, *Multimedia Image and Video Processing*, CRC Press, 2001.
- [KAW97] E. Kawaguchi, R. O. Eason. *Principle and Application of BPCS Steganography*, 1997.
- [KAW99] Kawaguchi, Eiji, *A Research on Bit-Plane Complexity Segmentation Based Steganography*, Kyushu Institute of Technology, 1999.
- [LYN02] Lynch and Horton, *Graphic: Color Displays*, 2002.
URL : <http://webstyleguide.com/graphics/displays.html>
Tanggal akses 2 Maret 2008.
- [MAN06] Mangarae, Aelphaeis, *Steganography FAQ*, Zone-H.Org, 2006.
- [MIA99] Miano, John, *Compressed Image File Format JPEG, PNG, GIF, XBM, BMP*, Addison Wesley Longman, Inc., 1999.
- [ROE99] Roelofs, Greg, *PNG: The Definitive Guide*, O'Reilly & Associates Inc., 1999.
- [SAL07] Salomon, David, *Data Compression The Complete Reference Fourth Edition*, Springer-Verlag London Limited, 2007.
- [SAY03] Sayood, Khalid, *Lossless Compression Handbook*, Academic Press, 2003.
- [SIM84] G. Simmons. "The Prisoner's Problem and the Subliminal Channel", *Advances in Cryptology: Proceedings of CRYPTO '83*, 1984.