IMPLEMENTASI STEGANOGRAFI MENGGUNAKAN METODE *BIT PLANE COMPLEXITY SEGMENTATION* PADA CITRA DIGITAL

Yuri Arianto[1], Rizky Ardiansyah[2], Rachmad Jibril Al Kautsar[3]

[1,2,3] Program Studi Teknik Informatika, Jurusan Teknologi Informasi, Politeknik Negeri Malang
[1] yuri@polinema.ac.id, [2] rizky.computerscience@gmail.com, [3] jibril.rachmad@gmail.com

Abstrak

Keamanan informasi dapat berupa menyembunyikan atau mengubah informasi. Dalam penelitian ini diterapkan cara mengamankan informasi dengan menyembunyikan informasi kedalam sebuah wadah seperti image, vidio dan audio, Teknik ini disebut Steganografi. Pada steganografi terdapat banyak metode yang dapat digunakan, kali ini Peneliti menggunakan metode Bit Plane Complexity Segmentation (BPCS). Pada metode BPCS informasi atau pesan disisipkan pada daerah bit plane yang mengandung noise. Metode ini memanfaatkan pengelihatan manusia yang tidak dapat melihat perubahan biner pada gambar. Pada penelitian ini Cover image yang digunakan adalah citra dengan format JPG, PNG, dan BMP. Sedangkan pesan yang disimpan kedalam citra berupa file dengan format .txt dan .docx. Proses pengujian dilakukan dengan menyisipkan file kedalam beberapa Cover image menggunakan aplikasi yang telah dibangun. Hasil pengujian menghasilkan stego image dengan nilai rata-rata PSNR antara 22 - 25 dB. Sedangkan rata-rata penyisipan pesan sebesar 40%. Penerapan teknik steganografi bermanfaat untuk menyembunyikan pesan dalam suatu media tanpa terdeteksi oleh pengelihatan manusia secara kasat mata.

Kata kunci : steganografi, *bit plane complexity segmentation*, citra digital.

1. Pendahuluan

Semakin canggihnya teknologi menimbulkan mudahnya informasi yang kita miliki untuk jatuh kepada pihak yang tidak berhak. Untuk mengurangi dan mencegah terjadinya hal tersebut, terdapat beberapa teknik yang yang mampu menyamarkan pesan pada suatu media, salah satu teknik tersebut dinamakan Steganografi.

Steganografi merupakan salah satu metode yang dapat digunakan untuk mengamankan informasi. Steganografi berbeda dengan kriptografi atau metode keamanan informasi lainnya, metode ini yaitu menyembunyikan informasi atau pesan kedalam media lain seperti citra digital, teks, suara atau video sehingga tidak menimbulkan kecurigaan orang lain. Steganografi membutuhkan dua properti, yaitu informasi dan media penampung. Media penampung yang banyak digunakan untuk menyembunyikan informasi yaitu citra digital. penyisipan informasi pada media citra digital dilakukan pada bit – bit pixel yang terdapat pada citra.

Penggunaan citra digital sebagai media penampung mempunyai kelebihan karena indera penglihatan manusia memiliki keterbatasan terhadap warna, sehingga dengan keterbatasan tersebut manusia sulit membedakan citra digital yang asli dengan citra digital yang telah disisipi pesan rahasia.

Steganografi mempunyai banyak metode yang dapat digunakan. Metode - metode yang digunakan dalam pembuatan steganografi mempunyai kriteria - kriteria yaitu kapasitas media penampung menyimpan informasi (payload capacity), kualitas media penampung yang telah disisipi pesan (fidelity), ketahanan terhadap manipulasi (robustness) dan tidak menimbulkan kecurigaan pada media penampung yang telah disisipi pesan (Unsuspicious file). Kriteria - kriteria ini harus dipenuhi oleh metode yang digunakan dalam pembuatan steganografi, agar media yang menampung informasi tidak menimbulkan kecurigaan. Namun dari kriteria - kriteria tersebut, steganografi tidak memastikan keamanan terhadap informasi yang tersembunyi pada media penampung. Sehingga jika media penampung dapat diungkap oleh orang yang tidak bertanggung jawab, maka informasi yang tersembunyi akan langsung diketahui.

Metode Bit Plane Complexity Segmentation (BPCS) merupakan salah satu metode yang dapat digunakan dalam pembuatan steganografi. Metode ini adalah pengembangan dari metode Least Significant Bit (LSB). Metode ini menawarkan kapasitas penyimpanan pesan yang lebih besar, dengan kualitas citra yang lebih baik daripada metode LSB.

2. Tinjauan Pustaka

2.1 Steganografi

Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya citra, suara, teks, dan video. Data rahasia yang disembunyikan juga dapat berupa citra, suara, teks, atau video. Steganografi dapat dipandang sebagai kelanjutan kriptografi. Jika pada kriptografi, data yang telah disandikan (*ciphertext*) tetap tersedia, maka dengan steganografi *cipherteks* dapat disembunyikan sehingga pihak ketiga tidak mengetahui keberadaannya.

Di negara-negara yang melakukan penyensoran informasi, steganografi sering digunakan untuk menyembunyikan pesan-pesan melalui gambar (*images*), video, atau suara (*audio*) Khaire, S. (2010).

2.2 Bit Plane Complexity Segmentataion

Bit plane complexity segmentation (BPCS) adalah salah satu teknik steganografi yang diperkenalkan oleh Eiji Kawaguchi dan R. O. Eason pada tahun 1997, untuk mengatasi kekurangan teknik steganografi tradisional seperti teknik *Least Significant Bit (LSB), Transform embedding technique, Perceptual masking technique*. Teknik tradisional ini membatasi kapasitas data yang dapat disembunyikan dan hanya dapat menyembunyikan hingga 10 - 15% dari jumlah besarnya media penampung. Sedangkan *Bit plane complexity segmentation* dapat menampung pesan hampir 50% dari jumlah besarnya media penampung. Hal ini terjadi karena penyisipan dilakukan tidak hanya pada *least significant bit*, tapi pada seluruh *bit-plane* termasuk pada *most significant bit.* Sedangkan untuk citra hasil steganografi terlihat sama seperti citra aslinya, tidak terlihat perbedaannya secara visual.

Pada BPCS dokumen citra dibagi menjadi segmen-segmen dengan ukura 8x8 piksel. Pada dokumen citra 8-*bit*, setiap satu segmen akan memiliki 8 buah *bitplane* yang merepresentasikan piksel-piksel dari setiap *bit* tersebut. Proses pembagian segmen 8x8 menjadi 8 buah *bit-plane* disebut proses *bit plane slicing*. pada BPCS, proses penyisipan dilakukan pada *bit-plane* dengan sistem CGC (*Canonocal Gray Code*) karena proses *bit slicing* pada CGC cenderung lebih baik dibandingkan pada PBC (*Pure Binary Code*). Proses penyisipan data dilakukan pada segmen yang memiliki kompleksitas yang tinggi atau disebut juga sebagai *noise-like region.*

PBC merupakan sandi yang digunakan untuk menyajikan setiap digit dalam bilangan desimal dengan ekuivalen binernya. CGC termasuk sandi dengan perubahan minimum yang berarti setiap bilangannya hanya berbeda satu bit dari bilangan sebelumnya. Pada CGC penyisipan pesan menggunakan LSB dan MSB (*Most Significant Bit)* citra hasil steganografi dan citra aslinya tidak terlihat perbedaan secara visual.

Bit Plane Slicing adalah operasi pemisahan gambar ke *bit-plane* penyusunnya. Pixel adalah nomor digital terdiri dari bit. Dalam gambar 8-bit, intensitas setiap pixel diwakili oleh 8-bit. 8-bit image terdiri dari delapan 1-bit plane dari bit plane '0' (LSB) ke bit-plane '7' (MSB). Plane '0' berisi bit urutan terendah dari semua piksel dalam gambar sementara plane '7' berisi bit lebih tinggi. *Bit Plane Slicing* berguna untuk kompresi gambar. Sebagai contoh, misalkan ada citra P dengan kedalaman n-*bit*, dapat ditunjukkan P = (P1, P2… Pn). Pi merupakan *bit plane* ke-i, dengan i = 1, 2, …, n. Jika citra P terdiri dari 3 warna, *red, green, blue,* maka dapat ditunjukkan P = (PR1, PR2, …, PRn, PG1, PG2, …, PGn, PB1, PB2, …, PBn) dengan PRi adalah *bit-plane* ke-i untuk *red*, PGi adalah *bit-plane* ke-i untuk *green*, dan PBi adalah *bit-plane* ke-i untuk *blue.*

Sementara itu, kompleksitas citra biner adalah suatu parameter kerumitan dari suatu citra biner. Perubahan warna hitam dan putih dalam gambar biner pada setiap baris dan kolom secara horizontal (kiri ke kanan) dan vertical (atas ke bawah) 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 *simple*. Kompleksitas gambar dilambangkan dengan ‘α’ dan diberikan persamaan.

$$\alpha = \frac{k}{2\ x\ 2^n\ x\ (2^n - 1)} \qquad (1)$$

Dimana ‘k’ adalah perubahan warna hitam-putih dan α adalah nilai kompleksitas. Untuk sebuah citra biner persegi dengan ukuran 2nx2n, kemungkinan maksimal perubahan warna adalah 2*2n*(2n-1) dan kemungkinan minimum perubahan warnanya adalah 0, diperoleh untuk gambar semua hitam atau semua putih.

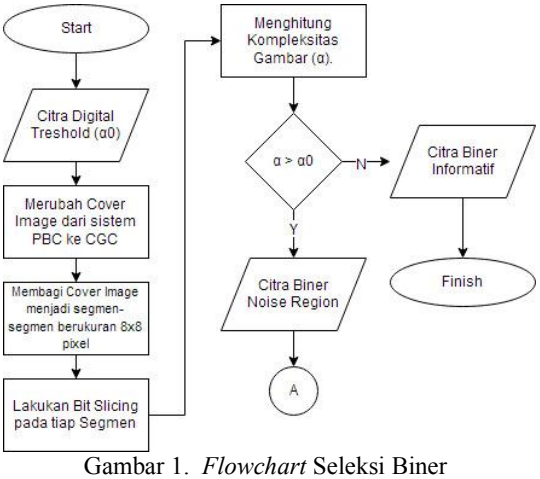
Kompleksitas sebuah area *bit-plane* adalah parameter yang digunakan dalam menentukan sebuah *bit-plane* merupakan *informative* atau *noise-like region.* Parameter kompleksitas ini harus memiliki batas yang berupakan pemisah keduanya yang disebut *threshold* (α0). Sebuah *bit-plane* tergolong sebagai *informative region* apabila memiliki nilai kompleksitas yang lebih kecil dibandingkan dengan nilai *threshold* ($\alpha < \alpha 0$) dan apabila memiliki nilai kompleksitas yang lebih besar dibandingkan dengan nilai *threshold* ($\alpha \geq \alpha 0$) akan dianggap sebagai *noiselike region* Dewim, S., dkk (2012).

2.3 Citra Digital

Citra digital adalah gambar dua dimensi yang bisa ditampilkan pada layar komputer sebagai himpunan/ diskrit nilai digital yang disebut pixel. Dalam tinjauan matematis, citra merupakan fungsi kontinu dari intensitas cahaya pada bidang dua dimensi. Citra digital adalah citra f(x,y) dimana dilakukan diskritisasi koordinat sampling/ spasial dan diskritisasi tingkat kwantisasi (kabuan/ kecemerlangannya). Citra digital merupakan fungsi intensitas cahaya f(x,y), dimana nilai x dan nilai y adalah koordinat spasial. Nilai fungsi tersebut di setiap titik (x,y) merupakan tingkat kecemerlangan citra pada titik tersebut. Citra digital merupakan suatu matriks dimana indeks baris dan kolomnya menyatakan suatu titik pada citra tersebut dan elemen matriksnya menyatakan tingkat keabuan pada titik tersebut. Format citra digital yaitu matriks yang berukuran N (baris) x M (kolom) Madenda, S. (2015).

3. Pembahasan

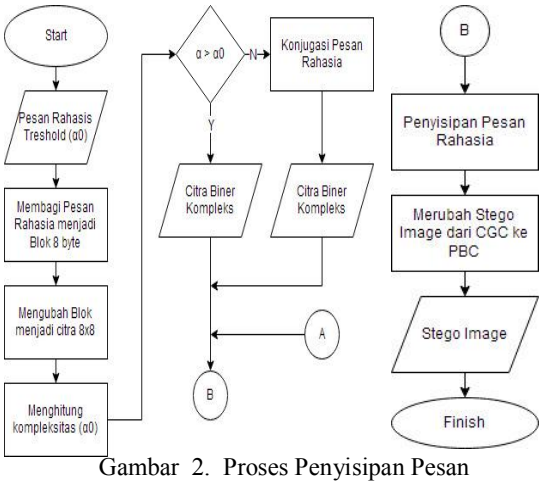
Pada steganografi BPCS terdapat beberapa proses yaitu proses seleksi biner citra digital, proses penyisipan pesan, dan proses ekstraksi pesan. *Flowchart* seleksi biner dapat dilihat pada Gambar 1.



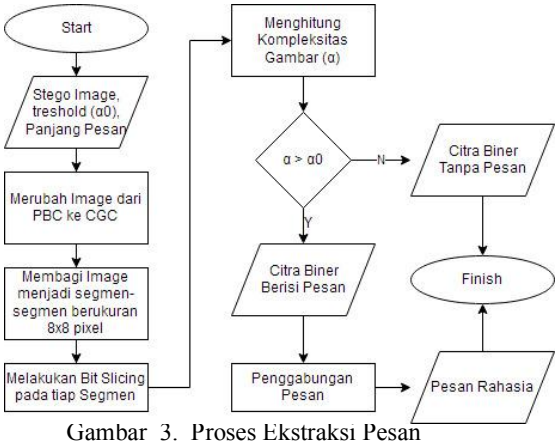
Gambar 1. *Flowchart* Seleksi Biner

Setelah citra diseleksi biner selanjutnya pesan akan dirubah kedalam bentuk blok dengan ukuran 8x8 kemudian akan disisipkan kedalam citra. Proses penyisipan pesan dapat dilihat pada Gambar 2.

Setelah pesan disisipkan kedalam citra citra akan dikirimkan ke penerima pesan. Penerima pesan akan mengekstrak pesan dari dalam citra untuk melihat isi pesan yang diterimanya. Proses ekstraksi pesan dapat dilihat pada Gambar 3.



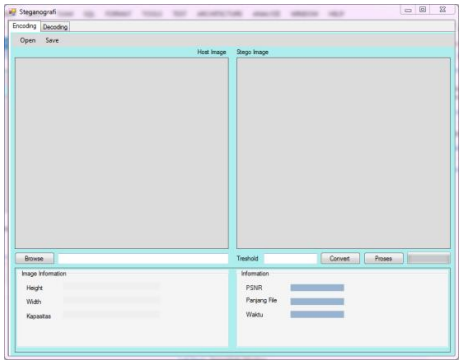
Gambar 2. Proses Penyisipan Pesan



Gambar 3. Proses Ekstraksi Pesan

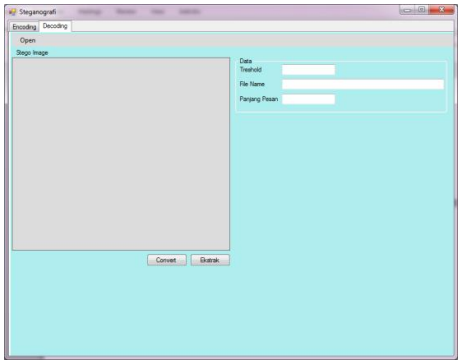
4. Implementasi

Pada penelitian ini aplikasi steganografi dibuat menggunakan Visual Studio dengan bahasa pemrograman c#. Pada aplikasi yang dibuat terdapat 2 halaman yaitu halaman *encoding* dan halaman d*ecoding*. Pada halaman e*ncoding* pengguna dapat melakukan proses penyisipan pesan kedalam citra. Tampilan halaman *encoding* dapat dilihat pada Gambar 4.



Gambar 4. Tampilan Halaman *Encoding*

Pada halaman *decoding* pengguna dapat melakukan proses ekstraksi pesan untuk mengambil pesan yang terdapat dalam citra. Tampilan halaman *decoding* dapat dilihat pada Gambar 5.



Gambar 5. Tampilan Halaman *Decoding*

5. Pengujian

Pengujian terhadap kualitas Citra hasil steganografi dan lama proses penyisipan berdasarkan besar pesan yang disisipkan. Pesan yang digunakan dalam pengujian yaitu :

- Pemilik.txt : 49 byte
- Informasi.docx : 12636 byte

Kemudian berikut adalah Cover Image yang digunakan dan Stego Image yang telah berisi pesan. Hasil pengujian penyisipan dapat dilihat pada Tabel 1 :

Tabel 1. Pengujian Penyisipan

No	Pesan	Citra Awal	Citra Hasil
1	Informasi		
2	Pemilik		
3	Informasi		
4	Pemilik		

Pada hasil penyisipan pada Tabel 2 masing-masing citra diberi nama sesuai dengan nomor Citra 1 dan Citra 2 berukuran 225 x 225 Pixel dengan format JPG, Citra 3 dan Citra 4 berukuran 500 x 354 Pixel dengan format BMP. Selanjutnya akan dihitung nilai PSNR dan waktu yang diperlukan untuk proses penyisipan.

Tabel 2. Hasil Perbandingan Penyisipan

No	Pesan	Citra	PSNR	Waktu
1	Pemilik.txt	cLena.jpg	25,21	8,02
		cRumah.bmp	24,32	28,12
2	Informasi.docx	cLena.jpg	24,72	7,84
		cRumah.bmp	23,81	26,97

Dari tabel 1 dapat ditarik kesimpulan bahwa semakin besar ukuran Pesan Rahasia yang disisipkan maka semakin kecil nilai PSNR yang didapat. Sedangkan untuk waktu proses semakin besar ukuran Cover Image maka semakin lama waktu yang dibutuhkan untuk proses penyisipan. Rata-rata nilai PSNR dari tabel diatas termasuk rendah, hal ini menunjukkan bahwa kualitas Stego Image tidak begitu bagus. Akan tetapi perbedaan antara Cover Image dan Stego Image tidak terlihat secara kasat mata.

6. Kesimpulan

Beberapa hal yang dapat disimpulkan dari penelitian ini :

1. Penyisipan pesan dengan menggunakan metode BPCS memiliki nilai PSNR yang relatif rendah dengan nilai rata – rata 22 dB tetapi perbedaan tidak terlihat secara kasat mata.
2. Lamanya waktu proses penyisipan berbanding lurus dengan besarnya ukuran citra yang digunakan sebagai wadah.
3. Untuk mendapatkan hasil citra yang baik digunakan nilai treshold diatas 0,3.
4. Untuk mendapatkan kapasitas penyimpanan pesan yang besar digunakan nilai treshold dibawah 0,3.
5. Jika ukuran pesan yang akan disisipkan kedalam citra melebihi kapasitas penampungan maka pesan tidak dapat disisipkan kedalam citra.

Daftar Pustaka:

Dewim, S., Wibowo, A., dan Rachmawati Heni. (2012): *Analisis Perbandingan Steganografi pada Citra Digital GIF dan TIFFdengan Metode BPCS.*

Ibrahim, R., dan Suk Kuan, T. (2011): *Steganography Algorithm to Hide Secret Message inside an Image.*

Khaire, S. (2010): *Review : Steganography – Bit PlaneComplexity Segmentation (BPCS) Technique.*

Kawagichi, E., dan Eason, R. Tanpa Tahun. *Principle and applications of BPCS-Steganography*

Madenda Sarifudin, "Pengolahan Citra dan Vidio Digital", Jakarta, Erlangga, 2015.