

Analisis Kapasitas Dan *Imperceptibility* Proses Penyisipan Pesan Pada Citra Menggunakan LWT dan Metode BPCS

Malahayati

Universitas Islam Negeri Ar-Raniry Banda Aceh
Email : malaoemar2701@gmail.com

Abstrak

Salah satu cara untuk melindungi pesan rahasia dari orang yang tidak berhak mengaksesnya yaitu dengan cara menyisipkan pesan rahasia pada suatu wadah penampung, misalnya citra. Penelitian ini akan mengevaluasi kapasitas pesan rahasia yang dapat ditampung oleh citra, serta tingkat *imperceptibility* citra yang telah mengandung pesan rahasia. Pesan rahasia akan disisipkan pada daerah koefisien wavelet yaitu koefisien aproksimasi (LL) yang diperoleh dengan melakukan Lifting Wavelet Transform (LWT). Metode yang digunakan untuk menyisipkan bit-bit pesan ke dalam piksel citra yaitu metode Bit-Plane Complexity Segmentation (BPCS). Hasil yang diperoleh pada penelitian ini, citra yang memiliki noise-like tinggi akan memiliki kapasitas yang banyak, akan tetapi tingkat *imperceptibility* yang kurang.

Kata kunci: Lifting Wavelet Transform, Segmentasi Bit-Plane Complexity, citra

Abstract

The way to protect the secret messages from unauthorized people is by inserting a secret message in a container, for example, images. This study will evaluate the capacity of secret messages that can be accommodated by images, as well as the level of *imperceptibility* of images that already contain secret messages. The secret message will be inserted in the wavelet coefficient region, which is the approximation coefficient (LL) obtained by performing Lifting Wavelet Transform (LWT). The method used to insert message bits into image pixels is the Bit-Plane Complexity Segmentation (BPCS) method. The results obtained in this study, images that have high noise-like will have a lot of capacity, but lacking the level of *imperceptibility*.

keywords: Lifting Wavelet Transform, Bit-Plane Complexity Segmentation, citra

1. Pendahuluan

Seiring dengan perkembangan teknologi, kejahatan yang memanfaatkan teknologi dan informasi juga turut berkembang. Dengan berbagai teknik banyak yang mencoba untuk mengakses data/pesan yang bukan haknya. Oleh karena itu, perlu diciptakan suatu teknik pengamanan untuk melindungi informasi dari orang yang tidak berhak tersebut. Salah satu teknik pengamanan informasi adalah steganografi. Steganografi merupakan teknik penyisipan pesan rahasia pada media penampung dengan maksud orang yang tidak berhak memiliki pesan tersebut tidak menyadari keberadaan dari pesan yang disisipkan. Salah satu metoda steganografi yaitu dengan cara menyisipkan pesan rahasia ke dalam media penampung citra.

Terdapat beberapa hal yang harus diperhatikan pada teknik steganografi dengan media penampung citra, dua diantaranya adalah kapasitas penyisipan dan *imperceptibility* citra yang telah disisip pesan (Eloff, Morkel, Olivier, 2005 dan Bateman, Schaathun, 2008). Kapasitas penyisipan artinya kemampuan suatu citra dalam menampung data yang akan disisipkan, sedangkan *imperceptibility* artinya keberadaan pesan tidak dapat dipersepsi oleh panca indra. Pada penelitian yang dilakukan oleh Silvia Torres-Maya, Mariko Nakano-Miyatake dan Hector Perez-Meana pada tahun 2006, dijelaskan bahwa pesan rahasia disisipkan pada citra, yaitu di daerah *bit-plane* koefisien wavelet yang diperoleh dengan melakukan *Integer Wavelet Transform* (IWT) pada citra tersebut. Sedangkan proses pergantian bit pesan dengan bit pada citra dilakukan pada daerah *bit-plane* citra yang kompleks, yang diperoleh dengan menggunakan metode BPCS dengan ketetapan nilai *threshold* =0,3. Tujuannya untuk mendapatkan kapasitas penyisipan dan *imperceptibility* yang tinggi. Namun pada penelitian yang dilakukan oleh Seed Sarreshtedari dan shahrokh Ghaemmaghmi pada tahun 2010, mengungkapkan bahwa untuk mendapatkan kapasitas penyisipan dan *imperceptibility* yang tinggi, proses penyisipan menggunakan metode BPCS serta menggunakan *random seed* untuk menentukan blok yang akan disisipi bit pesan. Selain itu, proses penyisipan pada penelitian ini hanya menggantikan bit citra pada posisi LSB sebesar bit pesan yang akan disisip.

Berdasarkan latar belakang dan penelitian sebelumnya maka pada penelitian ini akan dievaluasi kapasitas penyisipan pesan pada citra dan tingkat *imperceptibility* citra yang telah disisip pesan (citra stego) dengan menggunakan LWT serta penerapan metode BPCS, Pada penelitian ini bit pesan akan disisipkan pada seluruh bit citra yang merupakan daerah *noise-like*. Untuk mendapatkan daerah *noise-like* yang efektif, nilai *threshold* yang digunakan pada penelitian ini adalah 0,3 dan 0,4.

2. Tinjauan Pustaka

Pada bagian ini akan dijelaskan citra digital, steganografi, Lifting Wavelet Transform (LWT) dan *Bit-Plane Complexity Segmentation* (BPCS).

a. Citra Digital

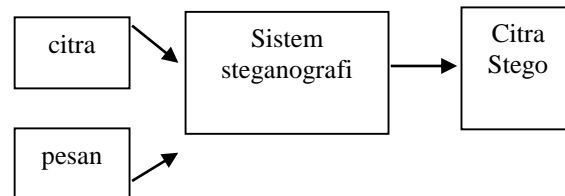
Citra digital merupakan kumpulan piksel-piksel yang membentuk sebuah gambar yang dapat dilihat oleh mata manusia. Pada citra digital, data direpresentasikan dalam bentuk matriks. Suatu matriks terdapat indeks baris (m) dan indeks kolom (n) untuk menyatakan suatu titik pada citra tersebut. Perpotongan m,n disebut juga elemen gambar/piksel. Nilai piksel menyatakan tingkat intensitas dari citra tersebut (Blackledge, 2005). Gambar 1. Merupakan citra digital yang dinyatakan dengan matriks berukuran $M \times N$, dengan M menyatakan baris dan N menyatakan kolom.

$$f(m,n) = \begin{pmatrix} f(0,0) & f(0,1) & f(0,2) & \dots & f(0,N-1) \\ f(1,0) & f(1,1) & f(1,2) & \dots & f(1,N-1) \\ f(2,0) & f(2,1) & f(2,2) & \dots & f(2,N-1) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ f(M-1,0) & f(M-1,1) & f(M-1,2) & \dots & f(M-1,N-1) \end{pmatrix}$$

Gambar 1. Representasi citra digital dalam bentuk matriks (Jahne, 2005)

b. Steganografi

Steganografi merupakan suatu cara menyembunyikan pesan, sehingga keberadaan pesan tersebut tidak diketahui. Pesan yang digunakan berupa citra, suara teks atau video. Sedangkan media penampung juga dapat digunakan citra, suara, teks atau video (Cole, 2003). Gambar 2. Merupakan ilustrasi teknik steganografi dengan media penampung citra.



Gambar 2. Ilustrasi steganografi

Berdasarkan metode pemrosesannya, steganografi dapat digolongkan menjadi dua bagian, pada domain spasial dan domain transformasi. Proses penyisipan pada domain spasial yaitu dengan mengubah nilai piksel pada citra asli, sedangkan proses penyisipan pada domain transformasi seperti *Fast Fourier Transform (FFT)*, *Discrete Cosine Transform (DCT)* dan *Wavelet Transform* dilakukan dengan merubah koefisien transformasinya.

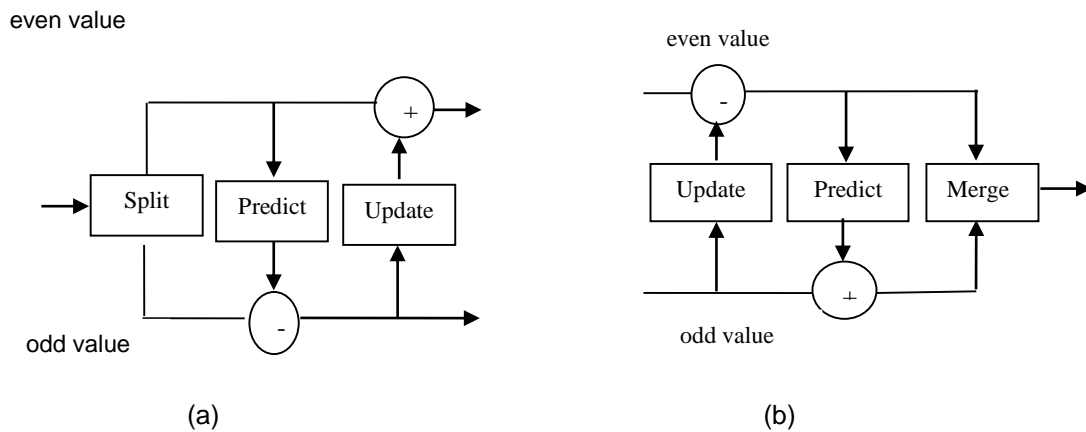
c. Lifting Wavelet Transform (LWT)

LWT adalah salah satu bagian dari *Discrete Wavelet Transform (DWT)* yang diperkenalkan pada tahun 1996 oleh Wim Sweldens. LWT merupakan generasi kedua DWT (Sweldens, 1996). Pada DWT dilakukan proses beberapa filter secara terpisah, sedangkan dengan LWT operasi proses dibagi dan diproses secara bersamaan dan tidak memerlukan *array* sementara dalam proses kalkulasi (*in-place computation*) sehingga implementasi *lifting scheme* lebih cepat dari pada implementasi wavelet klasik.

Tiga langkah forward LWT adalah:

1. *Split*, yaitu pembagian data menjadi dua, elemen-elemen berindeks ganjil dan elemen-elemen berindeks genap,
2. *Predict*, yaitu prediksi elemen ganjil dari elemen genap, dan
3. *Update*, yaitu lanjutan dari fase predict untuk menentukan nilai elemen genap.

Di sisi lain, langkah *inverse LWT (ILWT)* merupakan kebalikan dari *forward LWT*, yaitu *undo update*, *undo predict*, dan *merge (Chen)*.



Gambar 3. Skema LWT (a) maju (b) balik

d. Bit-Plane Complexity Segmentation (BPCS)

BPCS merupakan teknik steganografi yang diperkenalkan Eiji Kawaguchi dan Richard O.Eason pada tahun 1998. Proses penyisipan dengan metode BPCS memiliki kapasitas yang besar (Kawaguchi dan Eason, 1998).

Berikut langkah-langkah yang dilakukan pada penyisipan data menggunakan metode BPCS:

1. Mengubah citra dari sistem *Pure Binary Code (PBC)* menjadi sistem *Canonical Gray Code (CGC)*. Konsep perubahan PBC menjadi CGC menggunakan persamaan (1) dan (2).

$$g_1 = b_1 \dots\dots\dots(1)$$

$$g_i = b_{i-1} \oplus b_i \quad ; \quad i > 1 \dots\dots\dots(2)$$

2. Selanjutnya citra di- *slice* menjadi *bit-plane*. Setiap *bit-plane* mewakili bit dari setiap piksel. Hitung kompleksitas (α) setiap *bit-plane* citra. Dengan menggunakan nilai batas/*threshold* $\alpha_0 = 0,3$, setiap *bit-plane* yang memiliki $\alpha \geq \alpha_0$ merupakan daerah *noise-like* dan *bit-plane* yang memiliki $\alpha < \alpha_0$ merupakan daerah *informative*. Nilai α dapat dihitung menggunakan persamaan (3)

$$\alpha = k/n \dots\dots\dots(3)$$

Dengan k =jumlah perubahan warna hitam-putih pada setiap *bit-plane* dan n kemungkinan maksimal perubahan warna hitam-putih. Untuk sebuah citra biner persegi dengan ukuran $2^N \times 2^N$, maka n adalah $2 * 2^N * (2^N - 1)$.

3. Kelompokkan byte-byte pesan menjadi rangkaian blok pesan rahasia.
4. Jika blok pesan (S) kurang kompleks dibandingkan dengan nilai batas, maka lakukan konjugasi terhadap S untuk mendapatkan S^* yang lebih kompleks. Proses konjugasi dapat dilakukan dengan meng-XOR blok pesan yang tidak kompleks dengan blok W_c . Gambar 4. Merupakan blok matriks W_c

$$W_c = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Gambar 4. Blok Peta Konjugasi

5. Sisipkan setiap blok pesan rahasia ke *bit-plane* yang merupakan daerah *noise-like*. Jika blok S dikonjugasi, maka simpan pada "*conjugation map*".
6. Sisipkan juga *conjugation map* seperti yang dilakukan pada blok pesan rahasia.
7. Ubah citra stego dari sistem CGC menjadi sistem PBC menggunakan persamaan (4) dan (5).

$$b1 = b1 \dots\dots\dots(4)$$

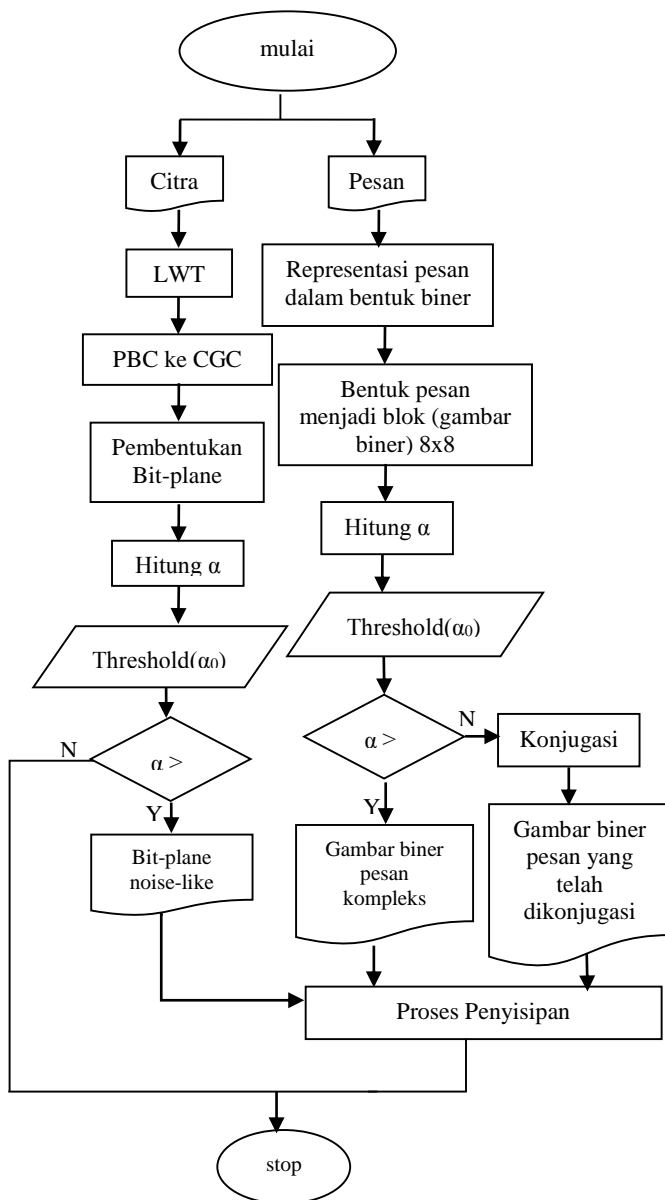
$$bi = gi \oplus bi-1 \quad ; i > 1 \dots\dots(5)$$

3. Metodologi Penelitian

Pada penelitian ini akan digunakan media penampung citra dan pesan rahasia berupa teks. Adapun citra yang digunakan adalah citra grayscale lena_gray.tiff 512 x 512 dan danau_gray.tiff 512 x 512. Sedangkan pesan rahasia yang digunakan pada penelitian ini adalah teks "penelitian ini". Nilai *threshold* yang digunakan pada penelitian ini adalah 0,3 dan 0,4.

a. Langkah-langkah penelitian

Adapun langkah penelitian ini seperti terlihat pada Gambar 5.



Gambar 5. Diagram alur penelitian

b. Evaluasi Penelitian

Pada penelitian ini dilakukan evaluasi *Peak Signal to Noise Ratio (PSNR)* antara citra asli dan citra stego serta evaluasi kapasitas citra yang dapat disisipi pesan.

1. *PSNR*

PSNR digunakan untuk menghitung *imperceptibility* dari citra stego. Dengan asumsi $C(i,j)$ adalah citra asli dan $S(i,j)$ adalah citra stego. *PSNR* dapat dihitung menggunakan persamaan (6)

$$PSNR = 10 \log_{10} \frac{m^2}{MSE} \text{ db} \dots \dots \dots (6)$$

Dimana

$$MSE = \frac{1}{[NxN]^2} \sum_{i=1}^N \sum_{j=1}^N [C(ij) - S(ij)]^2 \dots\dots(7)$$

2. Menghitung kapasitas

Kapasitas pada teknik steganografi merupakan jumlah bit maksimum yang dapat disisip. Pada penelitian ini media penampung yang digunakan citra, sehingga kapasitas dapat diukur dengan bit per piksel (bpp). Bpp dapat dihitung menggunakan persamaan (8).

$$bpp = \frac{hidden\ bits}{Numpix(Ic)} \dots\dots\dots(8)$$

4. Hasil dan Pembahasan

Setelah dilakukan penelitian diperoleh citra yang telah disisip pesan (citra stego). Perbandingan citra stego dengan citra asli dapat dilihat pada Gambar 6(a), 6(b) dan 6(c).



Gambar 6. (a) Citra danau_gray asli
(b) Citra danau stego,th=0,3
(c) Citra danau stego,th=0,4

Berdasarkan Gambar 6 dapat dilihat bahwa proses penyisipan telah berhasil dilakukan, dengan citra stego dan citra asli tidak dapat dibedakan secara mata manusia. Hal ini menunjukkan keberadaan pesan tidak dapat dipersepsi secara mata manusia. Sedangkan hasil evaluasi kapasitas dan *imperceptibility* (PSNR) dapat dilihat pada Tabel 1.

Tabel 1. Hasil penelitian

Citra	Thres-hold	Jumlah noise-like	Kapasitas (bpp)	PSNR (dB)
Danau_gray.tiff (512x512)	0,3	4213	4,11	50,7
	0,4	3262	3,19	51,3

Berdasarkan Tabel 1. terlihat bahwa perubahan nilai *threshold* mempengaruhi jumlah *noise-like* yang mana dapat mempengaruhi kapasitas dan *imperceptibility* citra. Citra yang menggunakan *threshold* 0,3 memiliki jumlah *noise-like* lebih tinggi dibandingkan dengan citra yang menggunakan *threshold* 0,4. Sehingga citra yang menggunakan *threshold* 0,3 akan memiliki kapasitas lebih banyak dibandingkan dengan citra yang menggunakan *threshold* 0,4. Namun hal ini berbanding terbalik dalam hal *imperceptibility*. Citra yang menggunakan *threshold* 0,3 memiliki tingkat *imperceptibility* (PSNR) lebih buruk dibandingkan dengan citra yang menggunakan *threshold* 0,4.

Berdasarkan penelitian secara keseluruhan proses penyisipan pesan pada citra, sebaiknya pada citra yang memiliki *noise-like* tinggi. Artinya pada citra *noise-like* tinggi akan memiliki kompleksitas atau perubahan warna yang tinggi pula.

5. Kesimpulan dan Saran

a. Kesimpulan

Setelah dilakukan penelitian diperoleh kesimpulan bahwa penyisipan pesan pada citra menggunakan LWT dan metode BPCS berhasil dilakukan. Selain itu, penggunaan citra dengan *noise-like* tinggi serta penetapan nilai *threshold* 0,4 akan menghasilkan citra stego dengan *imperceptibility* tinggi (terjaga kualitasnya) serta dapat membatasi ukuran pesan pada batas kerusakan yang tidak terlihat oleh mata.

b. Saran

Berdasarkan hasil penelitian di atas, maka disarankan perlu adanya penelitian lanjutan dengan media penyimpanan citra warna serta menggunakan jenis transformasi dan penggunaan metode penyimpanan lainnya.

REFERENSI

- Bernd Jahne. (2005). *Digital Image Processing*, 6th ed. Germany: springer
- Eric Cole. (2003). *Hiding in Plain Sight: Steganography and the Art of Covert Communication*. Carol Long, Ed, Canada: Bob Ipsen
- Eiji Kawaguchi, Richard O. Eason. (1998). *Principle and Application of BPCS-Steganography*.
- Jonathan M. Blackledge. (2005). *Digital Image Processing (Mathematical and Computational Methods)*. England:Horwood.
- J. H. P. Eloff, T. Morkel, M. S. Olivier. (2005). An Overview of Image Steganography. *Proceeding of the Fifth Annual Information Security South Africa Conference (ISSA)*, pp.1-12, South Africa.
- Philip Bateman, Dr. Hans Georg Schaathun. (2008). *Image Steganography and Steganalysis*. Departement of Computing Faculty of Engineering and Physical Science University of Surrey, Master Thesis, United Kingdom.
- Silvia Torres-Maya, Mariko Nakano-Miyatake dan Hector Perez-Meana. (2006). An Image Steganography System Based on BPCS and IWT. *Proceeding IEEE-CONIELECOMP*.
- Seed Sarreshtedari, shahrokh Ghaemmaghmi. (2010). High Capacity Image Steganography in wavelet Domain. *Proceeding IEEE-CCNC*.
- Wim Sweldens. (1996). The Lifting Scheme: A Construction of Second Generation Wavelets. *SIAM Journal on Mathematical Analysis*.