# IMPLEMENTASI STEGANOGRAFI PADA CITRA DIGITAL DENGAN METODE BIT-PLANE COMPLEXITY SEGMENTATION

**Viktorius Dedy Kurniawan Budianto[1], Tjokorda Agung Budi Wirayuda[2], Ade Romadhony[3]**

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

**Abstrak**

**Steganografi adalah teknik 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. BPCS memanfaatkan karakteristik dari human vision yang tidak melihat informasi visual dalam area yang mengandung noise dalam sebuah citra. BPCS memanfaatkan perhitungan kompleksitas pada tiap bit-plane dalam menyelipkan informasi rahasia.**

**Hasil akhir yang diperoleh dalam Tugas Akhir ini adalah steganografi BPCS pada citra digital BMP mampu menampung data rahasia lebih dari 50% dari ukuran citra cover. Kualitas citra steganografi yang dihasilkan metode BPCS ini pun masih baik ketika disisipkan data rahasia hingga 50% dari ukuran citra cover. Hal ini bisa dilihat dari nilai PSNR yang diatas 30. Namun metode ini memiliki kelemahan terhadap serangan. Tidak ada yang memiliki nilai BER dibawah 20% ketika diberi serangan seperti kompresi, noise, resize, dan rotasi.**

**Kata Kunci : Steganografi, Bit-Plane Complexity Segmentation, BMP**

**Abstract**

**Steganography is the technique of hiding a secret or sensitive information without seeming to not look like it should be. Secret data hidden by inserted in a particular medium so it does not appear that the media hide the information.**

**Bit-Plane Complexity Segmentation (BPCS) is one method of steganography, where this method has the capacity of a relatively large insertion of messages. BPCS utilize the characteristics of human vision does not see the visual information in areas that contain noise within an image. BPCS harness the complexity of the calculations on each bit-plane in the slip confidential information.**

**Final results obtained in this thesis is the BPCS steganography in digital images of BMP is able to accommodate the confidential data of more than 50% of the size of the cover image. The quality of images generated by BPCS steganography method is still good when confidential data inserted up to 50% of the size of the cover image. This can be seen from the PSNR values above 30. However, this method has a weakness against attacks. No one has the BER values below 20% when given the attacks such as compression, noise, resize, and rotation.**

**Keywords : Steganography, Bit-Plane Complexity Segmentation, BMP**

# 1. Pendahuluan

## 1.1 Latar Belakang

Pertukaran informasi di Internet telah menjadi bagian yang penting dalam perkembangan teknologi informasi di seluruh dunia. Hal tersebut dikarenakan media Internet memiliki banyak kelebihan dibandingkan dengan media komunikasi lainnya. Misalnya, akses kecepatan yang tinggi sehingga proses transfer data menjadi lebih cepat. Namun, sesungguhnya media internet bukanlah media yang aman untuk pertukaran informasi. Seseorang bisa saja menyadap aliran pengiriman data penting melalui email atau transaksi online.

Terdapat beberapa cara yang dapat digunakan untuk menjaga keamanan dan kerahasiaan data, diantaranya dengan menggunakan teknik Kriptografi dan Steganografi. Kriptografi adalah ilmu yang mempelajari mengenai teknik pengubahan pesan untuk membuat pesan tersebut aman dan tahan dari serangan [03]. Steganografi (*steganography*) adalah ilmu dan seni menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui [09]. Keuntungan steganografi dibandingkan dengan kriptografi adalah bahwa pesan yang dikirim tidak menarik perhatian sehingga media penampung yang membawa pesan tidak menimbulkan kecurigaan bagi pihak ketiga. Ini berbeda dengan kriptografi dimana *ciphertext* menimbulkan kecurigaan bahwa pesan tersebut merupakan pesan rahasia.[09]

Pada umumnya, steganografi menggunakan media digital sebagai wadah penampung, misalnya citra, suara (audio), teks, dan video [01]. Data rahasia yang disembunyikan juga dapat berupa citra, suara, teks, atau video [01]. Pada Tugas Akhir ini, wadah penampung yang digunakan adalah citra digital. Ada beberapa metode yang dapat digunakan untuk steganografi pada citra digital, antara lain: *Least Significant Bit (LSB), Spread Spectrum Steganography* dan *Bit-Plane Complexity Segmentation (BPCS)*.

Implementasi pada Tugas Akhir ini menggunakan metode Bit-Plane Complexity Segmentation (BPCS) terhadap citra digital dengan format *BMP*. Metode BPCS ini diperkenalkan oleh Eiji Kawaguchi dan R.O. Eason pada tahun 1997 [06]. BPCS memanfaatkan karakteristik dari *human vision* yang tidak melihat informasi visual dalam area yang mengandung noise dalam sebuah citra. BPCS memanfaatkan perhitungan kompleksitas pada tiap bit-plane dalam menyelipkan informasi rahasia. Kelebihan metode BPCS ini jika diterapkan pada citra digital adalah memiliki kapasitas penyisipan data rahasia mencapai 50% dari kapasitas wadah penampungnya [06]. *BMP* menangani file grafik dalam sistem operasi Microsoft Windows. File *BMP* tidak dikompresi, sehingga memiliki ukuran yang besar. Kelebihan *BMP* adalah kesederhanaan, penerimaan luas, dan digunakan dalam program Windows.

## 1.2 Perumusan Masalah

Berdasarkan latar belakang di atas, permasalahan yang diteliti dan dijabarkan pada Tugas Akhir ini adalah

1. Bagaimana menerapkan steganografi dengan metode BPCS pada citra digital dengan format *BMP*. Menurut teori metode BPCS ini memiliki kapasitas penyisipan data rahasia mencapai 50% dari kapasitas wadah penampungnya.
2. Bagaimana kualitas citra steganografi pada metode BPCS.
3. Bagaimana ketahanan terhadap serangan pada citra steganografi.

Sedangkan batasan masalah dalam menyelesaikan Tugas Akhir ini, antara lain:

1. Format citra digital yang akan disisipi data rahasia adalah *BMP* 24 bit RGB dengan resolusi 512 × 512 pixel.
2. Besarnya threshold untuk steganografi adalah 0.1, 0.2, 0.3, 0.4, dan 0.5
3. *Block Bit-Plane* berukuran 8 × 8 pixel, 32 × 32 pixel, dan 256 × 256 pixel.
4. Media digital yang menjadi data rahasia berupa teks, citra, audio, dan video.
5. File map yang berisi informasi letak data rahasia disembunyikan, tidak disisipkan pada citra steganografi.
6. Serangan terhadap citra steganografi berupa kompresi jpg, resize 50%, noise Gaussian 12.5%, dan rotasi $15^0$

## 1.3 Tujuan

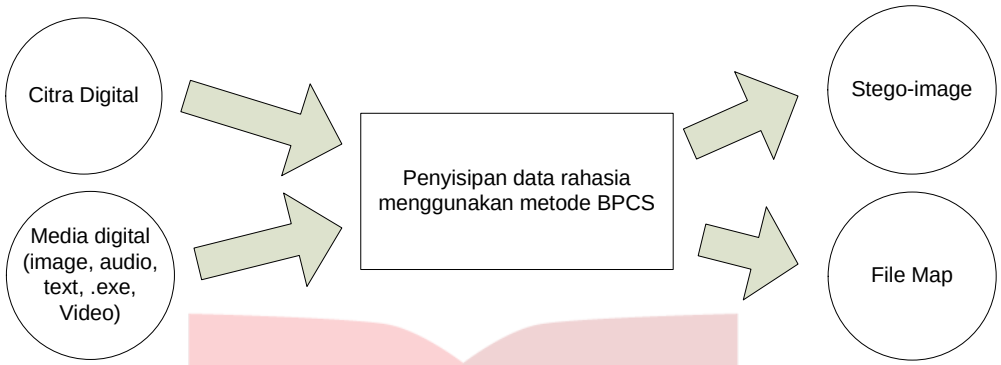
Tujuan dari penelitian Tugas Akhir ini:

1. Memahami steganografi dengan menggunakan metode BPCS.
2. Membangun perangkat lunak yang merupakan implementasi dari metode BPCS untuk menyisipkan dan meng-ekstraksi suatu data rahasia pada citra digital.
3. Mengetahui pengaruh *threshold* (batas yang ditentukan sebagai batas kompleksitas untuk memisahkan antara *informative region* dengan *noise-like region*) terhadap kapisitas penyisipan data rahasia dan kualitas citra steganografi (citra yang telah disisipkan data rahasia).
4. Mengetahui tingkat ketahanan citra steganografi terhadap serangan.

## 1.4 Metodologi Penyelesaian Masalah

Metedologi yang digunakan dalam menyelesaikan Tugas Akhir ini adalah:

1. Study Literatur
   Tahap ini bertujuan untuk mengumpulkan bahan-bahan, dan mendapatkan referensi yang jelas dan dasar teori yang kuat mengenai steganografi dengan metode *Bit-Plane Complexity Segmentation* pada citra digital serta referensi Java yang digunakan sebagai bahasa pemrograman untuk membangun aplikasi steganografi.
2. Analisis dan Design
   Tahap ini meliputi analisis kebutuhan untuk merancang sebuah sistem steganografi pada citra digital. Deskripsi sistem baik proses penyisipan maupun ekstraksi data rahasia dapat dilihat pada gambar berikut:




*Gambar 1-1. Proses Penyisipan Data Rahasia.*


*Gambar 1-2. Proses Ekstraksi Data Rahasia.*

3. Implementasi
   Tahap ini meliputi pembangunan sistem yang telah dirancang pada tahap sebelumnya. Pada tahap ini diimplementasikan perancangan yang telah dilakukan menjadi sebuah sistem dengan menggunakan bahasa pemrograman Java.
4. Pengujian dan Analisis Hasil
   Pada tahap ini dilakukan pengujian terhadap sistem yang telah dibangun dan sekaligus melakukan analisis terhadap hasil dari sistem**.** Beberapa pengujian yang dilakukan, antara lain:
   a. *Fidelity*, *robustness*, dan *recovery* pada stego-image yang telah dikompresi ke berbagai format image jpeg, gif, dan png.
   b. Pengaruh *threshold* pada kapasitas maksimal data rahasia yang dapat disisipkan ke dalam citra digital menggunakan metode BPCS.
   c. Kualitas stego-image setelah disisipi data rahasia dengan membandingkan antara stego-image dan image sebelum mengalami proses penyisipan data rahasia. Pembandingan dilakukan dengan cara penampilan visual dan PNSR (*Peak Signal to Noise Ratio*).
   d. Ketahanan citra steganografi terhadap serangan. Pembandingan dilakukan dengan BER (*Bit Error Rate*).

5. Pembuatan Laporan
   Pada tahap ini, dilakukan penyusunan laporan Tugas Akhir dan pengumpulan dokumentasi dengan mengikuti kaidah penulisan yang benar dan sesuai dengan ketentuan-ketentuan atau sistematika yang telah ditetapkan oleh institusi.

Telkom University

# 5. Kesimpulan dan Saran

## 5.1 Kesimpulan

Berdasarkan hasil pengujian dan analisis yang telah dilakukan, dapat diambil beberapa kesimpulan sebagai berikut:

1. Kapasitas penyisipan pesan dengan metode BPCS pada citra *BMP* cukup besar mencapai lebih dari 50% dari ukuran citra cover. Kapasitas penyisipan dipengaruhi oleh jumlah edge sebuah citra, semakin banyak jumlah edge (memiliki nilai kompleksitas yang tinggi), maka kapasitas penyisipan semakin besar.
2. Kualitas citra steganografi pada metode BPCS, dipengaruhi oleh beberapa faktor berikut:
   a. *Threshold*. Semakin besar nilai *threshold*, maka semakin baik kualitas citra steganografi yang dihasilkan (nilai PSNR meningkat). Namun apabila menggunakan cara penyisipan dilakukan pada blok *bit-plane* dengan kompleksitas tertinggi, maka *threshold* tidak berpengaruh terhadap kualitas citra steganografi (nilai PSNR cenderung sama) dan dengan menggunakan cara penyisipan ini dapat meningkatkan kualitas citra steganografi.
   b. Ukuran blok *bit-plane*. Semakin besar ukuran blok *bit-plane* yang digunakan, maka semakin baik kualitas citra steganografi yang dihasilkan.
   c. Ukuran data rahasia maksimum yang dapat disisipkan untuk mendapatkan kualitas citra steganografi yang baik adalah 50% dari ukuran citra cover.
3. Metode BPCS pada citra *BMP* memiliki kelemahan terhadap serangan baik kompresi, *noise*, *resize*, dan rotasi. Data rahasia output dari proses ekstraksi citra steganografi yang telah diberi serangan selalu mengalami kerusakan mencapai lebih dari 40%. Walaupun metode ini telah dimodifikasi dengan penyisipan data rahasia hanya dilakukan pada awal tiap bit RGB, namun kerusakan terhadap serangan masih tinggi. Hanya ketahanan serangan kompresi, *noise*, dan rotasi yang mengalami peningkatan. Dengan peningkatan ketahanan terbesar pada serangan *noise* walaupun masih diatas nilai toleransi kerusakan (20%).
4. Metode BPCS tidak dapat dikatakan sebagai salah satu metode pada steganografi, karena salah satu syarat (*Robustness*) tidak terpenuhi. Metode BPCS ini lebih cocok dikatakan sebagai metode dari *fragile watermarking*, dengan cara penyisipan yang dilakukan pada blok *bit-plane* yang memiliki nilai kompleksitas tertinggi, karena memiliki tingkat kerusakan tertinggi.

## 5.2 Saran

Hasil evaluasi dan analisa terhadap steganografi pada citra digital dengan metode *Bit-Plane Complexity Segmentation* (BPCS) menunjukkan bahwa sistem masih dapat dikembangkan. Beberapa saran pengembangan yang bisa dilakukan yaitu:

1. Perlu adanya analisis lebih lanjut dan implementasi metode BPCS pada citra terkompresi. Analisis yang diperlukan misalnya penanganan *DCT* pada kompresi *JPG* untuk menangani kerusakan data rahasia.
2. Perlu dilakukan analisis penerapan metode BPCS pada dokumen multimedia lain, seperti video. Video memiliki kemiripan dengan citra karena video terdiri *frame*, dimana *frame* tersebut merupakan citra.

# Daftar Pustaka


[01] Angraini; Ema Utami. (2007). *ANALISIS PENYISIPAN DATA PADA CITRA BITMAP MENGGUNAKAN METODE BIT PLANE COMPLEXCITY SEGMENTATION*. (Online). Tersedia di: http://digilib.unsri.ac.id/download/ [20 Oktober 2009]

[02] Cole, Eric. 2003. *Hiding in Plainsight : Steganography and the Art of Covert Communication*. Wiley Publishing,Inc.

[03] Forouzan, Behrouz. 2008. Cryptography and Network Security, McGraw-Hill

[04] Johnson, Neil F. Jajodia, Sushil. 1998. *Exploring Steganography: Seeing The Unseen*. IEEE

[05] Kawaguchi, Eiji. 1999. *A Research on Bit-Plane Complexity Segmentation Based Steganography*, Kyushu Institute of Technology

[06] Kawaguchi, Eiji & R. O. Eason. 1997. *Principle and Application of BPCS Steganography*. Kyushu Institute of Technology

[07] Krenn, Robert. 2004. *Steganography and Steganalysis: Chapter 1*

[08] Munir, Rinaldi. 2006. *Kriptografi*. Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung

[09] Penulis. (2009). Steganografi. (Online). Tersedia di: http://www.ittelkom.ac.id/library/index.php?view=article&catid=20%3Ainformatika&id=595%3Asteganografi&option=com_ content&Itemid=15 [20 Oktober 2009]

[10] Technical Advisory Service for Images. (2005). *The Digital Image*. Tersedia di: http://www.tasi.ac.uk [11 April 2010]

[11] Fahmi. 200_. *STUDI DAN IMPLEMENTASI WATERMARKING CITRA DIGITAL DENGAN MENGGUNAKAN FUNGSI HASH*. Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung

[12] Munir, Rinaldi. 2006. *Sekilas Image Watermarking untuk Memproteksi Citra Digital dan Aplikasinya pada Citra Medis.* Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung

[13] Baldman, A. 2003. *Bit Error Ratio Testing: How Many Bits are Enough?*. New Hampshire: InterOperability Laboratory, University of New Hampshire