**JURUSAN TEKNIK INFORMATIKA**

**FAKULTAS TEKNOLOGI INFORMASI**

**INSTITUT TEKNOLOGI SEPULUH NOPEMBER**

**USULAN TUGAS AKHIR**

# **IDENTITAS PENGUSUL**

Nama : **Muhammad Holil**

NRP : **5108 100 704**

Dosen Wali :  **Bilqis Amaliah, S.Kom., M.Kom.**

1. **JUDUL TUGAS AKHIR**

**Aplikasi *Chat* pada Media Gambar dengan Steganografi Menggunakan Metode *Four-pixel Differencing* dan Modifikasi Substitusi *Least Significant Bit* (LSB).**

1. **LATAR BELAKANG**

Perkembangan media digital yang pesat dan penggunaannya yang meliputi berbagai bidang menimbulkan tuntutan yang semakin besar untuk menciptakan suatu sistem penyampaian informasi yang terjamin keamanannya. Salah satunya adalah dengan steganografi. Steganografi merupakan suatu metode untuk menyisipkan informasi rahasia dalam suatu objek gambar atau media lain. Dengan steganografi, informasi disembunyikan sedemikian rupa sehingga tidak diketahui keberadaannya yang dikenal dengan istilah informasi hiding.

Metode steganografi yang paling terkenal adalah substitusi *Least Significant Bit* (LSB), yang menanamkan data dengan mengganti pixel k LSB dengan k bits rahasia secara langsung. Manusia hanya memiliki kepekaan terhadap perubahan pixel pada daerah yang *smooth* namun sebaliknya tidak peka terhadap perubahan yang ada pada area *edges.* Namun metode yang digunakan pada umumnya mempunyai kekurangan yakni pada sisi kapasitas data yang akan ditempelkan.

Oleh karena itu, pada tugas akhir ini dibuat sebuah aplikasi *chat* yang mampu menyembunyikan pesan kedalam sebuah gambar. aplikasi ini akan menerapkan teknik steganografi pada media gambar menggunakan metode *Four-pixel differencing*  dan metode modifikasi substitusi LSB, metode ini dipilih karena memiliki kapasitas penempelan data yang besar serta minimnya kemungkinan kerusakan gambar dari proses penempelan data. *Four-pixel differencing* akan menghitung rata-rata dari tiga nilai yang berbeda, kemudian hasil dari penghitungan ini dimanfaatkan untuk membedakan area *edges* dan area *smooth,*dan untuk menentukan banyaknya bit yang akan ditanamkan dalam blok. penanaman *secret bit* kedalam masing-masing pixel di dalam blok menggunakan subsitusi *Least Significant Bit* (LSB). Kemudian *Readjustment* akan dilakukan untuk meminimalisasi distorsi yang dihasilkan dari proses penanaman data. *Stego image* inilah yang nantinya akan dikirimkan.

1. **RUMUSAN MASALAH**

Rumusan masalah yang diangkat dalam Tugas Akhir ini dapat dipaparkan sebagai berikut :

* Bagaimana cara untuk mendapatkan kapasitas penanaman data yang besar dengan meminimalisasi distorsi pada *stego image*.
* Bagaimana cara menanamkan dan mengekstrak pesan menggunakan metode modifikasi substitusi *Least Significant Bit* (LSB).
* Bagaimana membuat aplikasi *chat* dengan steganografi menggunakan metode *Four-pixel Differencing* dan Modifikasi Substitusi *Least Significant Bit* (LSB).

1. **BATASAN MASALAH**

Permasalahan yang dibahas dalam Tugas Akhir ini memiliki beberapa batasan, diantaranya sebagai berikut:

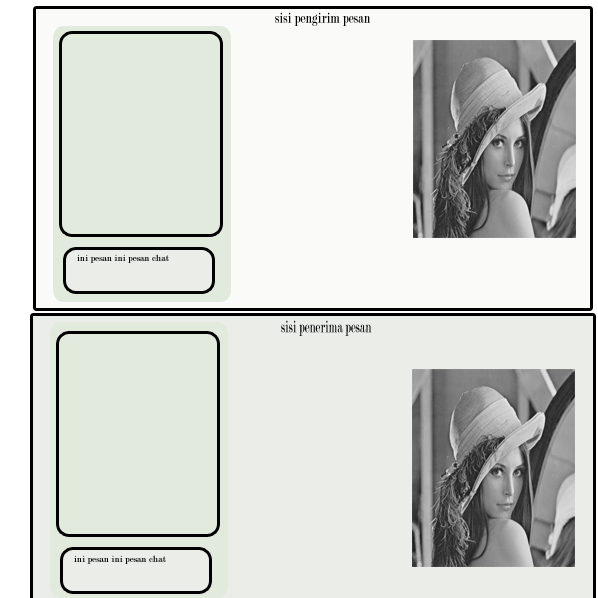
* + - 1. Menggunakan bahasa pemrograman Java.
      2. Media gambar asli (*cover image*) yang digunakan adalah gambar *grayscale* dengan format Bitmap.
      3. Format gambar yang sudah ditanami pesan (*stego image*) adalah Bitmap
      4. Algoritma yang digunakan adalah *Four-pixel Differencing* dan Modifikasi Substitusi *Least Significant Bit* (LSB)

1. **TUJUAN TUGAS AKHIR**

Tujuan pembuatan tugas akhir ini adalah untuk menghasilkan sebuah aplikasi *chat* yang menyembunyikan pesan ke media gambar menggunakan metode *Four-pixel Differencing* dan Modifikasi Substitusi *Least Significant Bit* (LSB). Metode mampu menghasilkan kapasitas *embed* data yang lebih besar serta menghasilkan *stego image* yang minim distorsi.

1. **RINGKASAN TUGAS AKHIR**

Dalam tugas akhir ini penulis mengusulkan aplikasi *chat* yang melakukan proses *embed* data berupa pesan kepada sebuah gambar *grayscale* dengan menggunakan metode *Four-pixel* *Differencing* dan Modifikasi Substitusi LSB. Setiap pesan yang akan dikirimkan oleh pengirim akan ditanamkan pada sebuah gambar, gambar inilah yang akan dikirimkan pada sisi penerima. Gambar yang sudah diterima oleh user akan diekstrak sehingga pesan yang terdapat di dalam gambar dapat terbaca oleh penerima pesan. Detail proses dari aplikasi dapat dilihat pada Gambar 1



Gambar 1. Detail proses aplikasi

Pesan ditanamkan ke sebuah gambar

Gambar yang sudah ditanami pesan dikirimkan ke penerima pesan

gambar yang diterima akan diekstrak, sehingga penerima dapat membaca pesan asli dari gambar yang dikirimkan

Sebelum menanamkan pesan pada gambar Aplikasi ini akan menghitung nilai rata-rata dari tiga pixel dari *cover image* yang kemudian nilai rata-rata ini akan dibagi menjadi dual level yang berbeda yakni level rendah dan level tinggi. Pixel yang berlokasi di blok akan ditanami k-bit dengan menggunakan metode modifikasi substitusi LSB, dimana nilai k ditentukan oleh level dimana nilai rata-rata dari tiga pixel berada. Level yang rendah akan menggunakan nilai yang lebih kecil kl, sedangkan level yang tinggi akan menggunakan nilai kh. distorsi pada gambar dapat diminimalisasi dengan melakukan proses *readjustment* dimana pada saat yang bersamaan menjamin level yang sama dimana nilai rata-rata berada sebelum dan sesudah proses *embedding*.

Semua pixel pada *cover image* adalah 256 *gray values*. Gambar asli (*Cover image)* akan dibagi menjadi *non-overlapping four pixel block*. Untuk setiap blok mempunyai empat *neighboring pixel* (pij, pij+1, pi+1j, pi+1j+1) dan *gray value-*nya adalah y0, y1, y2, y3 berturut-turut. Detail dari setiap langkah proses *embedding* sebagai berikut.

1. Hitung rata-rata nilai D. mengunakan rumus berikut

ymin =min{y0, y1, y2,y3}

1. Metode ini secara *adaptive* akan menanamkan pesan menggunakan dua level (level rendah dan level tinggi), nilai batas T digunakan untuk membagi nilai dari D menjadi dua level. Jika D≤T, maka D termasuk level yang rendah dan k=kl namun jika sebaliknya, D akan termasuk ke level tinggi sehingga nilai k=kh, untuk menyukseskan prosedur r*eadjusting* maka nilai T dan k harus bernilai

2kl ≤T≤2kh dan 1≤kl,kh≤5.

1. Periksa blok mana yang merupakan “*Error Block*”. *Error block* adalah kondisi dimana D≤T dan ymax-ymin › 2T+2 .ymax=max{y0,y1,y2,y3} *Error Block* ini tidak boleh digunakan untuk proses *embed* data.
2. Ubah yi menjadi yi′ dengan menggunakan k-bit substitusi LSB biasa (0≤i≤3) secara berurutan.
3. Gunakan k-bit modifikasi substitusi LSB untuk yi′ sehingga menghasilkan yi′′ (0≤i≤3) secara berurutan.
4. Langkah berikut ini disebut “*readjusting* *procedure*”. kemudian cari sehingga

* dan D berada di level yang sama, dimana

.

* *Block* *stego* final adalah dan tidak termasuk kedalam *“Error Block”*.
* Nilai dari diminimalkan.

Setelah pergantian (y0, y1, y2,y3) menjadi di dalam blok maka proses penyembunyian 4k-bit *secret data* telah sukses. Ulangi langkah 1-6 sampai semua *secret data* telah ditanamkan ke dalam *cover image*. Sebagai contoh jika kita mempunyai empat nilai *neighboring pixel* (139,146,137,142), dan *secret data*-nya adalah 000111111101. Kita asumsikan nilai T=5,kl =2 dan kh=3. Sehingga kita mendapatkan nilai , kemudian yi(0≤i≤3) ditanami 3-bit menggunakan LSB biasa sehingga nilai y0′=136, y1′=151, y2′=143, y3′=141. Setelah itu gunakan metode modifikasi substitusi LSB sehingga y0′′=136, y1′′=143, y2′′=135, y3′′=141. Setelah proses readjustment dilakukan makan akan menghasilkan. setelah pesan berhasil ditanamkan ke *cover image* maka aplikasi akan mengirimkan *stego image* ini menggantikan pesan *chat* yang dikirimkan oleh pengguna.

pada proses ekstraksi, *stego image* akan di partisi menjadi *four-pixel blocks* yang hampir sama seperti ketika proses *embed* data. Untuk masing-masing blok (pij, pij+1, pi+1j, pi+1j+1) proses berikut ini akan dilakukan unuk melakukan ekstraksi *secret data.*

1. Hitung nilai D seperti pada proses *embed* data.
2. Nilai *threshold* T layaknya pada proses *embed* data digunakan untuk menentukan keberadaan D berada di level rendah k=kl atau berada dilevel yang tinggi k=kh.
3. Periksa blok mana yang merupakan “*Error Block*” jika bukan ekstrak 4k-bit *secret data* dari k-bit LSB dari yi(0≤i≤3).kalau tidak *restart* dari langkah 1.

Contoh jika diketahui (136,151,135,141) ,T=5, D= berada di “level tinggi” sehingga k=kh=3. Ekstrak 3-bit LSB dari yi(0≤i≤3) secara berurutan , sehingga diperoleh *secret data* berupa 000111111101, Secret data inilah yang nantinya akan diterima pengguna.

1. **METODOLOGI**

Ada beberapa tahap dalam proses pengerjaan tugas akhir ini. Berikut adalah tahap-tahap dalam pembuatannya.

* + - * 1. **Studi Literatur**

Tahap ini merupakan tahap pengumpulan informasi yang diperlukan untuk pengerjaan tugas akhir sekaligus mempelajarinya. Mulai dari pengumpulan literatur, diskusi, perancangaan dan implementasi yang terkait dengan metode steganografi dengan metode *Least Significant Bit, Four-pixel Differencing*, serta pemrograman java terutama fungsi-fungsi dan metode untuk mengolah gambar.

* + - * 1. **Perancangan Sistem**

Pada tahap ini dilakukan analisis awal dan pendefinisian kebutuhan sistem untuk mengetahui masalah yang sedang dihadapi. Dari proses tersebut selanjutnya dirumuskan rancangan sistem yang dapat memberi pemecahan masalah tersebut.

* + - * 1. **Implementasi**

Pada tahap ini dilakukan pembuatan atau pengembangan sistem yang merupakan implementasi dari rancangan yang telah dibuat sebelumnya.

* + - * 1. **Uji Coba dan Evaluasi**

Pada tahap ini akan dilakukan pengujian fungsional serta performa terhadap aplikasi *chat* menggunakan data atau skenario yang telah dipersiapkan sebelumnya. Uji coba dan evaluasi perangkat dilakukan untuk mencari masalah yang mungkin timbul, mengevaluasi jalannya program, dan mengadakan perbaikan jika ada kekurangan.

* + - * 1. **Penyusunan Buku Tugas Akhir**

Pada tahap ini disusun laporan tugas akhir sebagai dokumentasi pelaksanaan tugas akhir, yang mencakup seluruh konsep, teori, implementasi, serta hasil yang telah dikerjakan. Laporan tugas akhir ini akan dibagi menjadi beberapa bab sebagai berikut.

1. Bab I. Pendahuluan yang berisi latar belakang, permasalahan, tujuan, batasan permasalahan, metodologi, dan sistematika penulisan.
2. Bab II. Landasan Teori mencakup dasar ilmu yang mendukung pembahasan tugas akhir ini.
3. Bab III. Desain Aplikasi.
4. Bab IV. Implementasi Aplikasi yang telah dibuat akan dilakukan pembuatan aplikasi yang dibangun dengan komponen-komponen yang telah ada yang sesuai dengan permasalahan dan batasannya yang telah dijabarkan pada bab pertama.
5. Bab V. Uji Coba dan Analisis Hasil akan dilakukan uji coba berdasarkan parameter-parameter yang ditetapkan dan dilakukan analisis terhadap hasil uji coba tersebut.
6. Bab VI. Penutup yang berisi simpulan yang dapat diambil dari tugas akhir ini beserta saran untuk pengembangan selanjutnya.
7. **JADWAL PEMBUATAN TUGAS AKHIR**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Kegiatan** | **Bulan** | | | | | | | | | | | | | | | | | | | |
| **Pebruari** | | | | **Maret** | | | | **April** | | | | **Mei** | | | | **Juni** | | | |
| 1 | Studi Literatur |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2 | Perencanaan Perangkat Lunak |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3 | Implementasi |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 | Uji Coba dan Evaluasi |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5 | Penyusunan Buku Tugas Akhir |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

1. **DAFTAR PUSTAKA**

[1] Chan, C.-k., & Cheng, L. (2004). Hiding data in images by simple LSB substitution. *Elsevier* .

[2] Liao, X., Wen, Q.-y., & Zhang, J. (2011). A steganographic method for digital images with four-pixel differencing. *elsevier* .

[3] Tjong, A. (2008, september 22). *Steganografi : 2. LSB (Least Significant Bit)*. diakses maret 5, 2012, dari Andreas Tjong Spreading knowledge: http://andreastjong.wordpress.com/2008/09/22/steganografi-2-lsb-least-significant-bit/

[4] Katzenbeisser, S., & A.P. Petitcolas, F. (2000). Information Hiding Techniques for Steganography and Digital Watermarking. ARTECH HOUSE, INC.

[5] J. Cox, I., L. Miller, M., A. Bloom, J., Fridrich, J., & Kalker, T. (2008). Digital Watermarking and Steganography Second Edition. Elsevier.

**LEMBAR PENGESAHAN**

###### **Surabaya, 16 Maret 2012**

|  |  |
| --- | --- |
| Menyetujui,  Dosen Pembimbing I  Ir. Muchammad Husni, M.Kom.  NIP.- | Menyetujui,  Dosen Pembimbing II  **Baskoro Adi Pratomo, S.Kom, M.Kom.**  NIP.- |
|  |  |