**JURUSAN TEKNIK INFORMATIKA**

**FAKULTAS TEKNOLOGI INFORMASI**

**INSTITUT TEKNOLOGI SEPULUH NOPEMBER**

**USULAN TUGAS AKHIR**

# **IDENTITAS PENGUSUL**

Nama : **Tegar Meda Rahman**

NRP : **5108100019**

Dosen Wali : **Yudhi Purwananto,S.Kom. M.Kom**

1. **JUDUL TUGAS AKHIR**

**Implementasi Kriptografi dan Steganografi Pada Media Gambar dengan Menggunakan Metode Blowfish dan GifShuffle**

1. **LATAR BELAKANG**

Saat ini komunikasi merupakan salah satu hal terpenting dalam kehidupan. Tidak hanya manusia tetapi semua makhluk hidup juga saling berkomunikasi satu dengan lainya dengan caranya sendiri. Pada era informasi seperti sekarang, komunikasi merupakan hal yang sangat penting. Ada saat dimana suatu informasi tersebut bersifat rahasia sehingga tidak boleh ada orang lain yang mengetahui informasi selain orang yang dituju. Oleh karena itu metode komunikasi yang digunakan harus dibuat sedemikian rupa sehingga tidak ada orang lain selain orang yang di tuju mengetahui tentang informasi tersebut [1].

Maka dari itu lahirlah sebuah metode kriptografi yaitu sebuah metode untuk mengolah informasi dengan algoritma tertentu sehingga informasi menjadi samar dan sulit dipahami maknanya. Tetapi dengan semakin berkembangnya teknologi semakin berkembang juga kemampuan untuk memecahkan kriptografi yang disebut dengan kriptanalisis. Sehingga pengamanan suatu informasi yang bersifat sangat penting juga harus berkembang[2].

Steganografi merupakan suatu seni menyembunyikan informasi pada suatu media. Media yang digunakan bisa berupa gambar, suara ataupun video. Sehingga jika seseorang ingin mengirim pesan kepada orang lain, tidak akan ada orang lain yang menyadari jika dalam media tersebut terdapat pesan rahasia.

Oleh karena itu pada tugas akhir ini dibuat sebuah implementasi yang membuat steganografi teks pada media gambar. Metode enkripsi yang digunakan adalah metode Blowfish yaitu merupakan algoritma kunci simetrik cipher blok yang dirancang pada tahun 1993 oleh Bruce Schneider untuk menggantikan DES (Data Encryption Standard), dan metode GifShuffle yaitu sebuah algortima steganografi yang digunakan untuk menyembunyikan pesan dalam berkas citra dengan format GIF. Algoritma GifShuffle intinya memanfaatkan header file GIF yang menyimpan palet warna sebagai media penyisipan pesan.

1. **RUMUSAN MASALAH**

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

1. Bagaimana membuat program kriptografi dengan menggunakan Metode Blowfish kemudian menyisipkan pesan yang telah di enkripsi tersebut ke dalam sebuah image dengan menggunakan Metode GifShuffle.
2. Bagaimana membuat program yang mampu melakukan Dekripsi dari file yang telah di Enkripsi dengan menggunakan Metode Blowfish dan GifShuffle.
3. **BATASAN MASALAH**

Permasalahan yang diangkat dalam tugas akhir ini dapat dipaparkan sebagai berikut :

1. Metode Kriptografi yang digunakan adalah metode Blowfish.
2. Metode Steganografi yang digunakan adalah metode GifShuffle.
3. File media steganografi adalah file image berformat gif.
4. File yang akan di enkripsi adalah plain text (.txt)
5. Ukuran maksimal file yang akan di enkripsi 1675 bit.
6. Bahasa pemrograman yang digunakan adalah Java.
7. **TUJUAN TUGAS AKHIR**

Tujuan dari Tugas Akhir ini adalah untuk menghasilkan sebuah implementasi penyembunyian informasi teks ke media gambar yaitu menyisipkan suatu pesan rahasia pada media image. Implementasi ini memanfaatkan metode Blowfish untuk mengenkripsi dan dekripsi pesan dan metode GifShuffle untuk menyisipkan hasil enkripsi ke dalam image dengan format GIF.

1. **MANFAAT TUGAS AKHIR**

Manfaat yang diharapkan dari Tugas Akhir ini adalah dapat memberikan keamanan bagi pengirim pesan dengan melakukan enkripsi kemudian menyisipkan pada image sehingga pesan tidak akan diketahui oleh orang lain dengan mudah, orang lain tidak akan mengira jika di dalam sebuah image yang dikirim oleh pengirim berisi sebuah pesan rahasia, sehingga pesan akan tersampaikan dengan aman kepada si penerima yang dituju.

1. **RINGKASAN TUGAS AKHIR**

Implementasi Kriptografi dan Steganografi Pada Media Gambar dengan Menggunakan Metode Blowfish dan GifShuffle secara garis besar akan dijelaskan seperti gambar dibawah :

Algoritma Blowfish adalah algoritma kunci simetrik cipher blok yang dirancang pada tahun 1993 oleh Bruce Schneider untuk menggantikan DES (*Data Encyption Standard*). Algoritma Blowfish dibuat untuk digunakan pada komputer yang mempunyai microprosesor besar (32-bit keatas dengan cache data yang besar). Blowfish merupakan blok cipher 64-bit dengan panjang kunci variabel. Algoritma ini terdiri dari dua bagian yaitiu *key expansion* dan enkripsi data. *Key expansion* berfungsi merubah kunci (Minimum 32-bit, maksimum 448 bit) menjadi beberapa *array* *subkey* dengan total 4168 *byte.* Enkripsi data terdiri dari iterasi fungsi sederhana sebanyak 16 kali putaran. Setiap putaran terdiri dari permutasi kunci-dependent. Semua operasi adalah penambahan dan XOR pada variable 32-bit. Operasi tambahan lainya hanyalah empat penelusuran tebel array berindeks untuk setiap putaran. Pada proses dekripsi dilakukan dengan urutan yang sama persis dengan proses enkripsi, hanya saja dilakukan dengan urutan yang terbalik [2].

Algoritma GifShuffle adalah sebuah Algoritma Steganografi yang digunakan untuk menyembunyikan pesan dalam berkas citra dengan format GIF. Algoritma GifShuffle pada intinya memanfaatkan header file GIF yang menyimpan palet warna sebagai media penyisipan pesan. Dalam algoritma ini tidak terjadi perubahan apapun dalam data berkas dengan format GIF. Algoritma GifShuffle memanfaatkan penukaran posisi ke 256 palet warna dalam berkas citra berformat GIF. Dengan dilakukanya penukaran posisi maka akan diperoleh sebuah informasi berkaitan dengan perbedaan posisi dengan posisi awal. Karena berkas dengan format GIF mengandung 256 palet warna maka dapat disimpulkan bahwa total penyimpanan maksimum dari format ini adalah 1675 bit [1].

Proses enkripsi :

Output

Steganografi

*Chipertext*

Enkripsi

Pesan

Gambar 1 proses enkripsi

Ada sebuah pesan berupa teks akan di enkripsi menggunakan algoritma Blowfish yang akan menghasilkan sebuah *chipertext*, kemudian *chipertext* akan disisipkan pada sebuah image berformat GIF dengan menggunakan metode GifShuffle output yang dihasilkan pada proses enkripsi adalah sebuah image berformat GIF yang berisikan suatu pesan yang telah di enkripsi.

Proses Dekripsi :

Pesan

Dekripsi

*Chipertext*

Steganografi

Output

Gambar 2 proses dekripsi

jika ingin mengetahui pesan yang disisipkan pada image maka harus di dekripsi terlebih dahulu dengan cara seperti pada gambar di atas. Dari hasil enkripsi akan diproses dengan menggunakan metode GifShuffle dari proses tersebut akan diperoleh sebuah *chipertext* kemudian dari *chipertext* tersebut akan di dekripsi menggunakan metode Blowfish. Hasilnya adalah sebuah pesan yang sama sebelum proses enkripsi.

1. **METODOLOGI**

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

1. **Pemahaman Sistem dan Studi Literatur**

Tahap ini merupakan tahap pengumpulan informasi yang diperlukan untuk pengerjaan tugas akhir sekaligus mempelajari konsep dan teknologi yang akan digunakan. Proses pada tahap ini meliputi pengumpulan referensi dan dokumentasi dari internet, diskusi dan pemahaman topic tugas akhir, diantaranya tentang :

1. Proses enkripsi dan dekripsi pada metode kriptografi, terutama pada algoritma Blowfish.
2. Pemrograman Java, terutama fungsi-fungsi dan metode untuk mengolah gambar.
3. Proses enkripsi dan dekripsi pada algoritma GifShuffle dan implementasinya terhadap pengolahan gambar.
4. **Perancangan Sistem**

Tahap ini meliputi perancangan sistem berdasarkan studi literatur dan pembelajaran konsep teknologi dari perangkat lunak yang ada. Tahap ini merupakan tahap yang paling penting dimana bentuk awal aplikasi yang akan diimplementasikan didefinisikan. Pada tahapan ini dilakukan perancangan tentang tampilan GUI dari program. Dan juga dirancang tentang OOP dari implementasi metode Blowfish dan GifShuffle.

1. **Implementasi**

Pada tahap ini dilakukan implementasi rancangan system aplikasi yang telah dibuat. Aplikasi dibangun dengan berpedoman pada konsep-konsep yang sudah ditentukan pada tahap sebelumnya

1. **Uji Coba dan Evaluasi**

Pada tahap iniaplikasi akan diuji setelah selesai diimplemetasikan menggunakan skenario yang sudah dipersiapkan. Pengujian dan evaluasi akan dilakukan dengan melihat kesesuaian dengan perencanaan. Dengan melakukan pengujian dan evaluasi dimaksudkan juga untuk menjalannya program, mencari masalah yang mungkin timbul dan mengadakan perbaikan jika terdapat kesalahan.

1. **Penyusunan Laporan 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

Pendahuluan yang berisi latar belakang, permasalahan, tujuan, batasan permasalahan, metodologi, dan sistematika penulisan.

1. Bab II. Landasan Teori

mencakup dasar ilmu yang mendukung pembahasan tugas akhir ini.

1. Bab III. Disain Aplikasi.

Bab ini berisi mengenai desain sistem, Flowchart dan desain antarmuka yang akan dibuat. Yaitu berupa aplikasi kriptografi dan steganografi yang menggunakan metode Blowfish dan GifShuffle.

1. 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.

1. Bab V. Uji Coba dan Analisis Hasil akan dilakukan uji coba berdasarkan parameter-parameter yang ditetapkan dandilakukan analisis terhadap hasil uji coba tersebut.
2. Bab VI.Penutup yang berisi simpulan yang dapat diambil dari tugas akhir ini beserta saran untuk pengembangan selanjutnya.

1. **JADWAL PEMBUATAN TUGAS AKHIR**

Berikut merupakan jadwal pengerjaan tugas akhir ini:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Tahapan** | **Bulan** | | | | | | | | | | | | | | | |
| **1** | | | | **2** | | | | **3** | | | | **4** | | | |
| Studi Kepustakaan |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Disain Sistem |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Implementasi |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Uji Coba dan Evaluasi |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Penyusunan Laporan Tugas Akhir |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

1. **DAFTAR PUSTAKA**
2. Penalosa, R. A. (2010). Steganografi Pada Citra dengan Format GIF menggunkan Algoritma GifShuffle.

2. Sutanto, C. A. (2010). Penggunaan Algoritma Blowfish dalam Kriptografi.

**LEMBAR PENGESAHAN**

###### Surabaya, 24 Februari 2012

Menyetujui,

|  |  |
| --- | --- |
| Dosen Pembimbing I,  **Ary Mazharuddin S., S.Kom., M.Comp.Sc.**  NIP. 19810620 200501 1 003 | Dosen Pembimbing II,  **Hudan Studiawan, S. Kom, M. Kom.**  NIP - |