**JURUSAN TEKNIK INFORMATIKA**

**FAKULTAS TEKNOLOGI INFORMASI**

**INSTITUT TEKNOLOGI SEPULUH NOPEMBER**

**USULAN TUGAS AKHIR**

# **IDENTITAS PENGUSUL**

**Nama : Arya Widyadhana**

**NRP : 5108100177**

**Dosen Wali : Ir. Muhammad Husni, M.Kom**

1. **JUDUL TUGAS AKHIR**

**2.1. Judul dalam Bahasa Indonesia:**

*“Pembagian Citra Rahasia Dengan Menggunakan Otentikasi Berantai dan Penyisipan Secara Dinamis”*

**2.2. Judul dalam Bahasa Inggris:**

*“Secret Image Sharing With Authentication-Chaining and Dynamic Embedding”*

1. **LATAR BELAKANG**

Pembagian dan penyembunyian data di dalam file citra memiliki dua permasalahan dasar yang harus diperhatikan. Pertama, kualitas dari citra stego dan kedua, besarnya ukuran citra stego. Bagaimana caranya agar kualitas citra stego tidak berbeda jauh dengan citra kamuflase agar tidak mengundang kecurigaan orang lain dan bagaimana caranya agar ukuran citra stego tidak besar sekali sehingga pengiriman dan penyimpanan citra stego mudah dilakukan.

Dari sisi keamanan, masalah yang muncul pada pembagian dan penyembunyian data di dalam file citra adalah bagaimana caranya agar citra stego tidak mudah dirusak orang yang tidak berhak. Pada metode-metode yang telah dikemukakan oleh beberapa ilmuwan, masalah ini diatasi dengan cara digunakannya suatu bit otentikasi pada setiap blok-blok piksel pada citra kamuflase.

Metode-metode pembagian suatu citra rahasia yang didasarkan pada teori Shamir Secret Sharing yang selama ini dikemukakan oleh beberapa ilmuwan memiliki suatu permasalahan besar yang sama pada hasil akhir yaitu file citra stego yang memiliki ukuran relatif besar dan kualitas citra stego yang kurang bagus. Hal-hal ini terjadi karena penyisipan dilakukan dengan cara statis.

1. **TUJUAN TUGAS AKHIR**

Dikembangkannya suatu metode penyisipan dinamis adalah untuk mengatasi masalah yang muncul pada penyisipan statis yaitu dipatoknya ukuran blok-blok piksel untuk penyisipan dari citra kamuflase yang menyebabkan ukuran citra stego besar dan kualitas visual citra stego menurun.

1. **PERMASALAHAN**

Permasalahan yang muncul adalah adakah cara atau metode yang dapat mengatasi masalah ukuran citra stego yang terlalu besar dan kualitas visual yang tidak tentu dari metode penyisipan statis? Jika dilihat dan diteliti masalah pada penyisipan statis adalah ukuran blok-blok piksel citra kamuflase yang telah dipatok. Ini menyebabkan penyisipan tidak fleksibel dalam arti jumlah bit yang disisipkan pada setiap blok tidak bisa berubah mengikuti ukuran citra rahasia dan citra kamuflase sehingga ukuran citra stego bisa jadi sangat besar dan juga tidak meratanya penyisipan pada citra kamuflase sehingga menurunkan kualitas visual dari citra stego yang dihasilkan

1. **BATASAN MASALAH**

Permasalahan yang dibahas dalam tugas akhir ini dibatasi sebagai berikut:

* + - 1. Citra digital yang digunakan hanya yang *8-bit gray scale.*
      2. Implementasi tugas akhir ini menggunakan bahasa pemrograman Java.

1. **RINGKASAN TUGAS AKHIR**

Sebuah citra digital rahasia yang menyimpan sebuah pesan rahasia akan disebarkan ke sekelompok orang. Citra rahasia tersebut akan disisipkan ke dalam file citra kamuflase agar orang lain diluar kelompok tersebut tidak mengetahui citra rahasia tersebut. Untuk alasan keamanan, file citra digital rahasia tersebut di pecah-pecah dan setiap orang dari kelompok tersebut mendapat satu bagian dari pecahan file citra digital rahasia yang disebarkan. Untuk dapat melihat file citra digital rahasia yang orisinil diperlukan sedikitnya *k*-pecahan dari file citra digital rahasia yang dipegang oleh anggota kelompok tersebut.

Algoritma yang digunakan adalah algoritma *Shamir Secret Sharing Scheme* yaitu sebuah skema (*k, n*) yang dikemukakan oleh Shamir pada tahun 1979. Jika dalam kelompok terdapat *n*-orang dan untuk dapat merangkai pesan rahasia, yang telah dipecah kepada *n*-orang dalam kelompok tersebut, dibutuhkan *k*-pecahan maka digunakan suatu (*k* - 1) polinomial sebagai berikut:

dimana *y* adalah sebuah integer rahasia yang akan disebarkan dan *m1, m2, …, dan mk* adalah integer acak.

Dalam kasus pembagian citra digital rahasia ini, *y* adalah nilai setiap piksel dari citra rahasia, *x* adalah nilai piksel pertama dari citra yang digunakan sebagai kamuflase, dan nilai *k* adalah 2, 3, atau 4.

Secara keseluruhan metode otentikasi berantai dan penyisipan dinamis dapat digambarkan sebagai berikut:



**Proses Penyisipan Dinamis**

Setiap piksel dari citra rahasia dianggap sebagai suatu rahasia tersendiri sehingga piksel-piksel tersebut disisipkan satu-satu ke dalam citra kamuflase. Metode ini menggunakan bit otentikasi untuk setiap piksel. Piksel-piksel ini disisipkan ke blok-blok piksel pada citra kamuflase.

Pertama, bit-bit, yang terdiri dari setiap piksel citra rahasia dan bit otentikasi, sebanyak *l* dihitung jumlah bitnya . Kemudian banyaknya piksel dalam satu blok (*BS*) pada citra kamuflase (*CI*) dihitung dengan cara:

Kedua, jumlah bit yang akan disisipkan (*Nb*) pada setiap blok dihitung. Pada setiap D*i* jumlah bit berjumlah 8 + *m* bit otentikasi dimana *m* bernilai 1, 2, atau 3.

Dalam satu blok piksel sudah pasti bit digunakan untuk penyisipan tetapi jika *Nb* bukan sebuah integer maka dalam piksel terakhir dari blok tersebut bit yang digunakan untuk penyisipan adalah . Maka bit yang digunakan untuk setiap piksel *Bi* pada *B* yang dilambangkan adalah sebanyak:

Dari semua perhitungan ini didapatkan untuk setiap *Di* jumlah bitnya berapa, jumlah piksel setiap blok pada citra kamuflase untuk penyisipan, dan berapa bit yang disisipkan pada setiap piksel pada setiap blok.

**Proses Otentikasi Berantai**

Untuk memastikan suatu citra stego (citra kamuflase yang sudah di sisipkan citra rahasia) tidak dirusak oleh orang, digunakan suatu data otentikasi di dalam setiap blok dari citra stego. Semakin besar data otentikasi yang digunakan, semakin besar pula kesempatan terdeteksinya suatu perusakan citra stego. Tetapi semakin besar data otentikasi yang digunakan, semakin jelek kualitas dari citra stego.

Tujuan dari otentikasi berantai ini adalah memperkecil probabilitas dari perusakan, yang dari metode-metode sebelumnya menjadi . Proses ini menghasilkan 2 bit otentikasi dan untuk setiap blok pada citra stego () yang mengacu pada blok pada citra kamuflase (*B*).

Misalkan = adalah blok ke *j* dari dan misalkan adalah bit-bit yang akan disisipkan ke dalam blok . Maka bit otentikasi dari yang dilambangkan dihitung dengan sebuah *hash function* sebagai berikut:

dimana adalah jumlah bit yang masih orisinil dari . adalah sebuah *all-zero vector*. *Key k* dari *hash function* *Hk* harus dibagikan menggunakan skema Shamir (*k, n*).

1. **METODOLOGI**

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

1. **Studi literatur**

Tahap ini merupakan tahap pengumpulan informasi dan pustaka yang diperlukan untuk pengerjaan tugas akhir dan tahap mempelajari informasi dan pustaka yang dikumpulkan. Hal yang dilakukan pada tahap ini adalah pengumpulan literatur, membaca dan memahami literatur, dan diskusi dengan orang yang mengerti tentang topik yang diangkat dalam tugas akhir. Topik yang harus dipahami pada tugas akhir ini meliputi:

* + - 1. Format Citra Digital
      2. *Steganography* pada Citra Digital
      3. Algoritma *Shamir’s Secret Sharing*

1. **Analisis dan Perancangan Sistem**

Pada tahap ini dilakukan perancangan sistem dengan menggunakan pemahaman yang didapat pada tahap studi literatur. Tahap ini merupakan tahap yang paling penting pada bentuk awal atau prototipe yang akan diimplementasikan. Hal yang dilakukan pada tahap ini adalah menganalisis kebutuhan sistem, algoritma yang digunakan, dan proses-proses yang dilakukan selama pembuatan sistem. Dari semua proses tersebut, dihasilkan suatu rancangan sistem.

1. **Implementasi**

Pada tahap ini dilakukan implementasi rancangan sistem yang telah dibuat. Tahapan ini merealisasikan apa yang dihasilkan pada tahapan sebelumnya sehingga menjadi sebuah perangkat lunak yang sesuai dengan apa yang telah direncanakan.

1. **Uji coba dan evaluasi**

Pada tahap ini akan diuji perangkat lunak yang telah selesai diimplemetasikan. Pengujian dan evaluasi akan dilakukan dengan melihat kebenaran data yang dihasilkan perangkat lunak tersebut dan kecepatan algoritma yang diimplementasikan.

1. **Penyusunan laporan tugas akhir**

Pada tahap ini laporan tugas akhir disusun 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 yang berisi dasar ilmu yang mendukung pembahasan dan topic dari tugas akhir ini.
3. Bab III. Desain Perangkat Lunak yang berisi analisis dan desain tentang perangkat lunak yang akan dibuat sesuai dengan permasalahan dan batasan permasalahan yang dicantumkan pada Bab I.
4. Bab IV. Implementasi Perangkat Lunak yang berisi penjelasan tentang hasil implementasi perangkat lunak yang sesuai dengan rancangan yang dibuat pada Bab III.
5. Bab V. Uji Coba dan Evaluasi yang berisi data-data hasil uji coba yang dilakukan kepada perangkat lunak yang telah diimplementasikan yang sesuai dengan Bab IV.
6. Bab VI.Penutup yang berisi simpulan yang dapat diambil dari tugas akhir ini beserta saran untuk pengembangan selanjutnya
7. **JADWAL PEMBUATAN TUGAS AKHIR**

Tugas akhir ini diharapkan dapat dikerjakan berdasarkan jadwal sebagai berikut.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No** | **Tahapan** | **Bulan** | | | | | | | | | |
| **Februari 2012** | | **Maret 2012** | | **April 2012** | | **Mei 2012** | | **Juni 2012** | |
| 1 | Studi Kepustakaan |  |  |  |  |  |  |  |  |  |  |
| 2 | Analisis dan Perancangan Sistem |  |  |  |  |  |  |  |  |  |  |
| 3 | Implementasi |  |  |  |  |  |  |  |  |  |  |
| 4 | Uji Coba dan Evaluasi |  |  |  |  |  |  |  |  |  |  |
| 5 | Penyusunan Laporan Tugas Akhir |  |  |  |  |  |  |  |  |  |  |

1. **DAFTAR PUSTAKA**
2. http://www.sciencedirect.com/
3. Eslami, Z., Ahmadabadi, J.Z., 2011, Secret Image Sharing with Authentication-Chaining and Dynamic Embedding.
4. Lin, C-C., Tsai, W-H., 2004, Secret Image Sharing with Steganography and Authentication.
5. Chan, C-K., Cheng, L.M., 2003, Hiding Data in Images by Simple LSB Substitution.

**LEMBAR PENGESAHAN**

###### Surabaya, 11 Maret 2011

Menyetujui,

|  |  |
| --- | --- |
| Dosen Pembimbing I, | Dosen Pembimbing II,  **Rully Soelaiman**  NIP |