BAB I

PENDAHULUAN

1. 1. Latar Belakang Masalah

Steganography (*covered writing*) didefinisikan sebagai ilmu dan seni untuk menyembunyikan pesan rahasia (*hiding message*) sedemikian rupa, sehingga keberadaan (*eksistensi*) pesan tidak terdeteksi oleh indera manusia [1]. *Steganography* di dunia *modern* biasanya mengacu pada data, informasi atau suatu arsip yang telah disembunyikan ke dalam suatu media teks, citra digital, audio, atau video.

Teknik *Dynamic Cell Spreading* merupakan salah satu teknik *steganography*. Teknik ini menggunakan metode *Least Significant Bit* (LSB) pada proses penyisipannya. Teknik *Dynamic Cell Spreading* dinilai lebih cepat dalam melakukan proses penyisipan dan ekstraksi, karena menggunakan *memory buffer* sebagai media perantaranya [2].

File *steganography* biasanya disebarkan melalui media internet, sehingga aspek keamanannya harus dipertimbangkan. *Steganography* biasanya digabungkan dengan *cryptography*, sehingga pesan rahasia yang disembunyikan menjadi lebih aman. Penyebaran informasi di media internet sangat rentan terhadap serangan. Informasi rahasia dapat diungkap atau dirubah oleh para oknum yang tidak bertanggungjawab. Ancaman ini mungkin masih ada walaupun informasi tersebut sudah terenkripsi [3]. Perubahan itulah yang menjadi permasalahan besar bagi orang yang menerima informasi tersebut. Apabila

“jangan” telah berubah menjadi “tidak” atau “1000” telah berubah menjadi “10000”, hal tersebut tentunya dapat merugikan pihak penerima, sehingga jaminan keaslian suatu data sangat diperlukan.

Pada beberapa kasus, seringkali otentikasi yang diperlukan, tetapi kerahasiaan data tidak. Maksudnya, data tidak perlu dienkripsikan, sebab yang dibutuhkan hanya otentikasi saja [1]. *Digital Signature Algorithm* (DSA) menawarkan pembentukan *signature* yang dapat menyelesaikan masalah *non-repudiation*. Karena DSA tidak dapat digunakan untuk enkripsi melainkan dispesifikasikan khusus untuk otentikasi. DSA merupakan bakuan (*standard*) untuk *digital signature* yang dinamakan *Digital Signature Standard* (DSS) dan dipublikasikan oleh *The National Institue of Standard and Technology* (NIST) pada bulan agustus 1991 [4].

Berdasarkan pengamatan, belum ada penelitian yang menggabungkan *steganography* dengan *digital signature*. Dengan adanya penelitian tersebut, penggabungan *steganography* dan *digital signature* diyakini dapat menutupi kelemahan-kelemahan baik dari segi *steganography* maupun *digital signature*. Oleh karena itu diperlukannya penelitian yang dapat membuktikan kelebihan dan kekurangan penggabungan *steganography* dan *digital signature*.

1. 2. Perumusan Masalah

Berdasarkan latar belakang masalah yang dihadapi, perumusan masalah yang didapat dari skripsi ini adalah :

Bagaimana membangun perangkat lunak steganografi menggunakan teknik *Dynamic Cell Spreading* (DCS) dan *Digital Signature Algorithm* (DSA) sebagai keamanan data.

1. 3. Maksud dan Tujuan

Berdasarkan latar belakang masalah, maka maksud dari penulisan skripsi ini adalah untuk membangun perangkat lunak steganografi menggunakan teknik *Dynamic Cell Spreading* (DCS) dan *Digital Signature Algorithm* (DSA) untuk keamanan datanya.

Tujuan yang akan dicapai dalam penulisan skripsi ini adalah :

1. Membuktikan kelebihan dan kekurangan penggabungan *steganography* dengan *digital signature*.
2. Melakukan uji coba performansi pada teknik DCS dan DSA.
3. Melakukan pengukuran kualitas file multimedia setelah disisipkan file rahasia untuk mengetahui kinerja perangkat lunak.

1. 4. Batasan Masalah

Dalam menyelesaikan Skripsi ini, pembahasan yang dibahas hanya mencakup pada :

1. File *parent* hanya bisa menggunakan dokumen audio, dokumen gambar dan dokumen video.
2. Format file *parent* yang digunakan terbagi menjadi :
   a. Dokumen Gambar : bmp, gif, jpg dan jpeg.
   b. Dokumen Audio : mp3 dan wav.
   c. Dokumen Video : mp4, avi, flv, mkv dan 3gp.
3. File *child* yang akan disisipkan tidak hanya sebatas dokumen teks saja, tetapi bisa juga menggunakan dokumen suara, gambar dan video.
4. Format file *child* yang akan disisipkan terbagi menjadi :
   a. Dokumen Teks : txt, rtf, doc, docx, ppt, pptx, xls, xlsx dan pdf.
   b. Dokumen Gambar : bmp, gif, jpg dan jpeg.
   c. Dokumen Audio : mp3 dan wav.
   d. Dokumen Video : mp4, flv dan 3gp.
5. Ukuran file *parent* harus lebih besar dari ukuran dokumen rahasia, minimal 8x lebih besar dari file *child*.
6. Basis aplikasi yang digunakan adalah berbasis desktop. Karena apabila ukuran file *parent* sangat besar, maka dibutuhkan *resource hardware* yang sangat besar pula.

1. 5. Metodologi Penelitian

Metodologi penelitian yang digunakan dalam penulisan skripsi ini menggunakan metode analisis deskriptif yang akan dijelaskan sebagai berikut:

1. Metode pengumpulan data

Metode pengumpulan data yang digunakan dalam skripsi ini adalah sebagai berikut :

a. Studi Literatur.

Metode pengumpulan data yang digunakan dalam penelitian ini adalah studi pustaka yang merupakan pengumpulan data dengan cara mengumpulkan literatur-literatur dari perpustakaan yang bersumber dari buku-buku, jurnal ilmiah, situs-situs di internet, *paper* dan bacaan-bacaan yang ada kaitannya dengan judul penelitian. Pada tahap ini akan dilakukan eksplorasi literatur dan pustaka mengenai steganografi pada dokumen *digital*, format dokumen *digital*, teknik *Dynamic Cell Spreading* (DCS), metode *Least Significant Bit* (LSB), *Digital Signature Algorithm* (DSA) dan fungsi *hash SHA.*

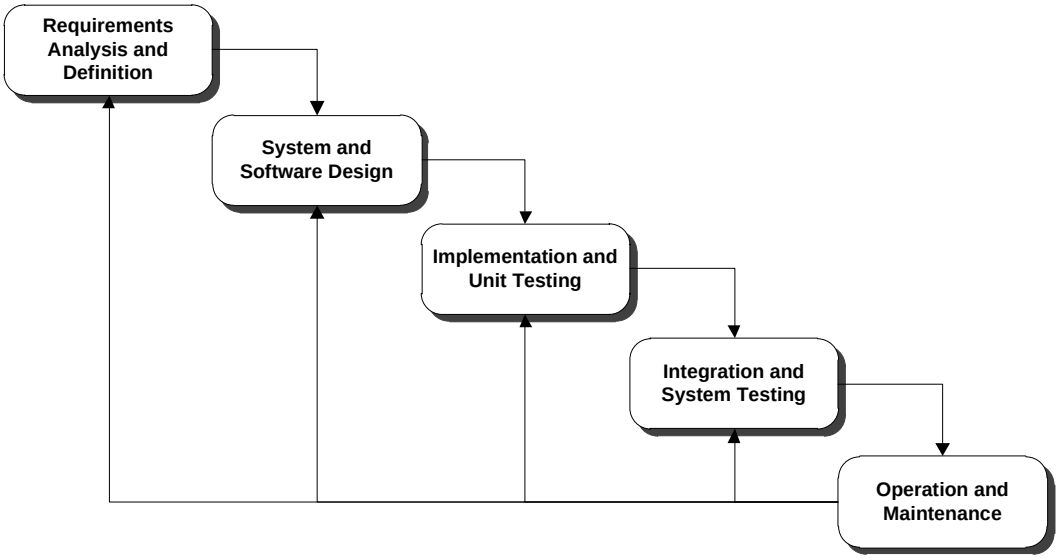
2. Metode Pembangunan Perangkat Lunak.

Metode analisis data dalam pembuatan perangkat lunak menggunakan paradigm perangkat lunak secara *waterfall*, yang meliputi beberapa proses berikut:

Berikut ini akan dijelaskan mengenai tahap-tahap pembangunan sistem dengan menggunakan paradigma *waterfall* [Gambar 1.1].

a. Requirements Analysis and Definition

Tahap ini merupakan bagian dari kegiatan sistem yang terbesar dalam pengerjaan suatu proyek. Pada tahap ini dilakukan analisa terhadap permasalahan dan menetapkan berbagai kebutuhan yang diperlukan dalam pembangunan atau pengembangan suatu perangkat lunak.



Gambar 1.1 Metode Waterfall [5]

b. System and Software Design

Tahap menerjemahkan kebutuhan-kebutuhan yang dianalisis ke dalam bentuk yang mudah dimengerti. Sehingga didapat jelas fungsi dan kebutuhan yang diinginkan dari pembangunan atau pengembangan perangkat lunak tersebut. Langkah selanjutnya yang dilakukan adalah merancang tampilan perangkat lunak agar mudah dimengerti oleh pengguna sesuai dengan fungsi dan kebutuhan perangkat lunak tersebut.

c. Implementation and unit testing

Tahap penerjemahan data atau pemecahan masalah yang telah dirancang kedalam suatu bahasa pemrograman tertentu. Sehingga dihasilkan sebuah

perangkat lunak yang sesuai dengan kebutuhan pengguna. Setiap fungsional yang ada pada perangkat lunak tersebut dilakukan uji kelayakan, sehingga perangkat lunak tersebut dapat berjalan dengan baik.

d. Integration and System Testing

Pada tahap ini, dilakukan penyempurnaan terhadap perangkat lunak secara keseluruhan agar dapat berjalan sesuai dengan kebutuhan. Pengujian perangkat lunak terhadap data nyata perlu dilakukan untuk memastikan kelayakan dari perangkat lunak tersebut.

e. Operation and Maintenance

Tahap akhir dimana suatu perangkat lunak yang sudah selesai dapat dioperasikan langsung oleh pengguna. Tahap *maintenance* perlu dilakukan untuk disesuaikan apabila ada perubahan sesuai dengan permintaan pengguna.

1. 6. Sistematika Penulisan

Sistematika penulisan skripsi ini disusun untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penulisan tugas akhir ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini akan menguraikan tentang latar belakang permasalahan, merumuskan inti permasalahan yang dihadapi, menentukan maksud dan tujuan skripsi, batasan masalah, metodologi penelitian yang digunakan serta sistematika penulisan..

BAB II LANDASAN TEORI

Bab ini membahas berbagai konsep dasar dan teori-teori yang berkaitan dengan topik skripsi yang dilakukan dan hal-hal yang berguna dalam proses analisis permasalahan.

BAB III ANALISIS MASALAH DAN PERANCANGAN SISTEM

Bab ini membahas mengenai sub-sub sistem yang diuraikan dari system utama dengan tujuan untuk mengetahui dan mengefektifkan cara kerja dan interaksi dari tiap sub system dalam fungsinya untuk mencapai tujuan system utama. Didalamnya terdapat analisis terhadap proses pembentukan sepasang kunci, proses pembangkitan *Digital Signature*, proses verifikasi *Digital Signature*, proses *embedding* dan proses *ekstrakting.* Selain itu terdapat juga kebutuhan fungsional dan *non*-fungsional dari sistem, perancangan antarmuka untuk aplikasi yang akan dibangun sesuai dengan hasil analisis yang telah dibuat.

BAB IV PENGUJIAN DAN IMPLEMENTASI SISTEM

Bab ini membahas tentang penerapan dari rancangan perangkat lunak sebelumnya ke dalam bahasa pemrograman tertentu dan pengujian terhadap perangkat lunak apakah telah benar dan sesuai seperti yang diharapkan.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi tentang kebenaran hipotesis yang diajukan pada batasan masalah berdasarkan hasil penelitian yang telah dilakukan dan masukan-masukan yang dapat digunakan untuk pengembangan perangkat lunak selanjutnya.