BAB I
PENDAHULUAN

I.1 Latar Belakang Masalah

Steganografi merupakan salah satu metode yang dapat digunakan untuk mengamankan informasi. Steganografi berbeda dengan kriptografi atau metode keamanan informasi lainnya, metode ini yaitu menyembunyikan informasi atau pesan kedalam media lain seperti citra digital, teks, suara atau video sehingga tidak menimbulkan kecurigaan orang lain. Steganografi membutuhkan dua properti, yaitu informasi dan media penampung[4]. Media penampung yang banyak digunakan untuk menyembunyikan informasi yaitu citra digital. penyisipan informasi pada media citra digital dilakukan pada bit – bit pixel yang terdapat pada citra. Penggunaan citra digital sebagai media penampung mempunyai kelebihan karena indera penglihatan manusia memiliki keterbatasan terhadap warna, sehingga dengan keterbatasan tersebut manusia sulit membedakan citra digital yang asli dengan citra digital yang telah disisipi pesan rahasia.

Steganografi mempunyai banyak metode yang dapat digunakan, namun metode yang banyak digunakan saat ini masih mempunyai kekurangan dalam hal kualitas, kapasitas, dan ketahanan[3]. Metode – metode yang digunakan dalam pembuatan steganografi mempunyai kriteria – kriteria yaitu kapasitas media penampung menyimpan informasi (*payload capacity*), kualitas media penampung yang telah disisipi pesan (*fidelity*), ketahanan terhadap manipulasi (*robustness*) dan tidak menimbulkan kecurigaan pada media penampung yang telah disisipi pesan (*Unsuspicious file*)[2]. Kriteria – kriteria ini harus dipenuhi oleh metode yang digunakan dalam pembuatan steganografi, agar media yang menampung informasi tidak menimbulkan kecurigaan. Namun dari kriteria – kriteria tersebut, steganografi tidak memastikan keamanan terhadap informasi yang tersembunyi pada media penampung. Sehingga jika media penampung dapat diungkap oleh orang yang tidak bertanggung jawab, maka informasi yang tersembunyi akan langsung diketahui.

Metode *pixel value differencing (PVD)* merupakan salah satu metode yang dapat digunakan dalam pembuatan steganografi. Metode ini menawarkan kapasitas penyimpanan pesan yang lebih besar, dengan kualitas citra yang lebih baik dibandingkan dengan metode lain[10]. Untuk menambah tingkat keamanan dari informasi yang akan disisipkan kedalam citra, steganografi dapat dikombinasikan dengan enkripsi, sehingga informasi yang disisipkan tidak akan mudah dibaca oleh orang yang tidak bertanggung jawab. Salah satu enkripsi yang dapat digunakan yaitu algoritma *rijndael* yang merupakan algoritma yang digunakan untuk standar kriptografi *Advanced Encryption Standard* (AES).

Berdasarkan uraian tersebut, maka pada tugas akhir ini akan dilakukan **"PEMBANGUNAN APLIKASI STEGANOGRAFI PADA CITRA DIGITAL MENGGUNAKAN METODE *PIXEL VALUE DIFFERENCING (PVD)* DAN ALGORITMA *RIJNDAEL* UNTUK KEAMANAN DATA"**.

I.2 Rumusan Masalah

Berdasarkan pada latar belakang yang telah diuraikan, perumusan masalah yang didapat pada tugas akhir ini adalah bagaimana membangun aplikasi steganografi menggunakan metode *pixel value differencing (PVD)* dan algoritma *rijndael* pada citra digital.

I.3 Maksud dan Tujuan

Berdasarkan permasalahan yang telah diuraikan, maka maksud dari penulisan tugas akhir ini adalah untuk membangun aplikasi steganografi pada citra digital menggunakan metode *pixel value differencing (PVD)* dan algoritma *rijndael* untuk keamanan data.

Tujuan yang akan dicapai dalam penelitian ini adalah :

1. Untuk mengimplementasikan penyembunyian pesan atau informasi kedalam citra digital menggunakan metode *pixel value differencing (PVD)* dan algoritma *rijndael.*
2. Untuk mengetahui performansi pada metode *pixel value differencing (PVD).*

3. Untuk mengetahui besar pesan yang dapat disembunyikan kedalam citra digital menggunakan metode *pixel value differencing (PVD).*
4. Untuk mengetahui kualitas citra yang telah disisipi pesan menggunakan metode *pixel value differencing (PVD).*
5. Untuk mengetahui ketahanan pesan pada citra yang telah disisipi pesan.

I.4 Batasan Masalah

Batasan masalah yang ditentukan pada pembangunan aplikasi steganografi menggunakan metode *pixel value differencing (PVD)* dan algoritma *rijndael* untuk keamanan data ini adalah sebagai berikut :

1. Media penampung pesan hanya file citra berformat *.bmp, *.png, *.gif dan *.jpg.
2. Pesan yang akan disisipkan kedalam citra tidak hanya file teks saja, tapi juga dapat berupa gambar, suara dan jenis file lainnya dengan format yaitu:
   a. Pesan teks : *.txt, *.doc, *.docx, *.pdf dan *.xls
   b. Pesan gambar : *.bmp, *.png, *.gif dan *.jpg.
   c. Pesan suara : *.mp3 dan *.wav
   d. Pesan kompresi : *.rar dan *.zip
3. Dua pesan dapat disisipkan kedalam citra.
4. Menggunakan algoritma *rijndael* 128bit untuk enkripsi pesan yang akan disisipkan kedalam citra.
5. Hal – hal yang akan diujikan pada aplikasi yang dibangun yaitu:
   a. Besar pesan yang dapat disembunyikan kedalam citra.
   b. Performansi pada metode *pixel value differencing (PVD)*.
   c. Kualitas citra yang telah disisipi pesan yang dinyatakan dalam *PSNR*.
   d. Ketahanan pesan pada citra yang telah disisipi pesan (*robustness*).
6. Aplikasi yang dibangun berbasis desktop.
7. Perangkat lunak yang digunakan untuk pembangunan aplikasi yaitu :
   a. Sistem operasi yang digunakan yaitu windows.
   b. Pengkodean dan desain aplikasi menggunakan Java NetBeans7.

I.5 Metodologi Penelitian

Metodologi penelitian yang digunakan dalam penulisan tugas akhir ini menggunakan metode analisis deskriptif yang yang terdiri dari dua metode yaitu metode pengumpulan data, dan metode pembangunan perangkat lunak.

I.5.1 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam penelitian ini adalah menggunakan metode studi literatur. Studi literatur merupakan pengumpulan data dengan cara mengumpulkan literatur, jurnal, *paper* dan bacaan – bacaan yang ada kaitannya dengan judul penelitian. Data yang akan dikumpulkan dari literatur dan pustaka yaitu mengenai steganografi pada citra digital, metode steganografi *pixel value differencing* (PVD) dan algoritma kriptografi *rijndael*.

I.5.2 Metode Pembangunan Perangkat Lunak

Metode pembangunan perangkat lunak ini menggunakan metode *waterfall* seperti pada gambar I.1 yang terdiri dari beberapa tahap, yaitu:

1. *Requirement*

   Requirement merupakan tahapan analisis terhadap apa saja yang dibutuhkan oleh sistem yang akan dibangun. Analisis yang dilakukan meliputi analisis pengguna dan kebutuhan sistem.

2. *Design*

   Design merupakan tahap melakukan perancangan terhadap keseluruhan sistem. Perancangan yang dilakukan yaitu perancangan antarmuka dari sistem yang dibangun.

3. *Implementation*

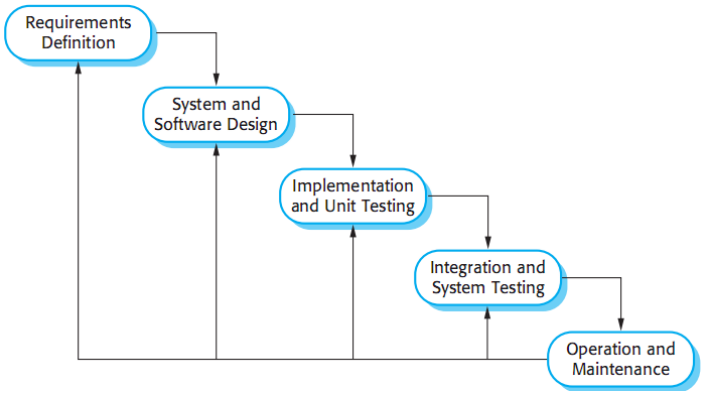
   Implementation merupakan tahap merubah perancangan dan analisis yang dilakukan sebelumnya kedalam kode pemrograman yang digunakan. Tahap ini juga dilakukan *unit testing* untuk mengetahui apakah telah sesuai dengan kebutuhan sistem.

4. *Testing*

   Testing merupakan tahap dimana sistem yang telah dikodekan dilakukan pengujian. Pengujian ini dilakukan untuk mengetahui apakah terdapat kesalahan pada sistem yang telah dikodekan pada tahap *implementation* atau tidak.

5. *Maintenance*

   Maintenance merupakan tahap perawatan jika terjadi kesalahan pada sistem. Perawatan yang dilakukan yaitu mengkoreksi jika terjadi kesalahan, menambah fungsionalitas dan *requirement* sistem.



Gambar I.1 Metode *Waterfall*[7]

I.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 menguraikan tentang latar belakang permasalahan, merumuskan inti permasalahan yang dihadapi, menentukan tujuan dan kegunaan penelitian, yang kemudian diikuti dengan pembatasan masalah, serta sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini membahas berbagai konsep dasar dan teori-teori yang berkaitan dengan topik penelitian yang dilakukan dan hal-hal yang berguna dalam proses analisis permasalahan serta tinjauan terhadap penelitian-penelitian serupa yang telah pernah dilakukan sebelumnya termasuk sintesisnya.

BAB III ANALISIS MASALAH DAN PERANCANGAN SISTEM

Bab ini membahas mengenai sub-sub sistem yang diuraikan dari sistem utama dengan tujuan untuk mengetahui cara kerja dan interaksi dari tiap sub sistem dalam fungsinya untuk mencapai tujuan sistem. Didalamnya terdapat analisis terhadap proses penjadwalan kunci, proses enkripsi, proses dekripsi,

proses penyisipan dan proses ekstraksi, selain itu terdapat juga kebutuhan fungsional dan nonfungsional 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 implementasi dari aplikasi yang dibangun. Implementasi dilakukan berdasarkan analisis dan perancangan yang telah dilakukan, kedalam bahasa pemrograman tertentu. Hasil dari implementasi, kemudian dilakukan pengujian apakah aplikasi telah sesuai seperti yang diharapkan.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi tentang kesimpulan berdasarkan hasil penelitian yang telah dilakukan dan masukan-masukan yang dapat digunakan untuk pengembangan perangkat lunak selanjutnya.