BAB 1
PENDAHULUAN

1.1. Latar Belakang Masalah

Berdasarkan sejarah panjang mengenai metode kerahasiaan informasi, tujuan utama dari kegiatan tersebut adalah melindungi informasi agar tidak dapat dideteksi oleh pihak yang tidak berkepentingan. Seiring perkembangan teknologi, metode steganografi digunakan pula untuk aktivitas-aktivitas pengabsahan sebuah dokumen. Sistem kearsipan paling banyak menggunakan metode ini. Penggunaan steganografi merupakan teknologi yang sangat bermanfaat dalam pengamanan dokumen. Steganografi berbeda dengan kriptografi atau metode keamanan informasi lainnya, steganografi 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 karna indra pengelihatan manusia memiliki keterbatasan tersebut manusia sulit membedakan citra digital yang asli dengan citra 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 *Random Pixel Positioning (RPP)* merupakan salah satu metode yang dapat digunakan dalam pembuatan steganografi. Dari beberapa metode steganografi yang digunakan antara lain metode *Random Pixel Positioning (RPP).* metode tersebut yaitu merubah file gambar maupun file sisipan ke dalam bentuk bit dan menyisipkan bit-bit dari file sisipan tersebut ke dalam bit-bit pada file gambar. *Random pixel positioning (RPP*) merupakan pengembangan dari metode LSB yakni dengan mengacak posisi bit-bit tersebut dalam bit-bit gambar sehingga tidak mudah dilacak. Salah satu enkripsi yang dapat digunakan yaitu algoritma *Advanced Encryption Standard(AES)* adalah *blockchiptertext* yang dapat mengenkripsi *(encipher)* dan dekripsi *(decipher)* yaitu mengubah pesan asli *(plaintext)* menjadi pesan dalam bentuk tersandi *(ciphertext).* Proses enkripsi akan menghasilkan data tersandi dan hanya dibuka atau dibaca oleh pihak penerima yang memiliki kinci *(key)* sedangkan proses dekripsi adalah mengembalikan data tersandi menjadi bentuk data asli. Baik teknik kriptografi dan steganografi sama-sama memiliki kekurangan, oleh karena itu menggabungkan kedua teknik enkripsi ini dimaksudkan akan menambah tingkat keamanan pada saat pertukaran data menyisipkan pesan rahasia bahkan untuk mengklaim autentifikasi dari suatu media citra digital yang dibuat.

Berdasarkan uraian tersebut, maka pada tugas akhir ini akan dilakukan **"PEMBANGUNAN APLIKASI STEGANOGRAFI PADA CITRA DIGITAL MENGGUNAKAN METODE *RANDOM PIXEL POSITIONING (RPP)* DAN ALGORITMA *ADVANCED ENCRYPTION STANDARD (AES)256*BIT UNTUK KEAMANAN DATA"** agar data yang bersifat rahasia aman dan tidak mudah dilihat oleh pihak ketiga.

1.2. Rumusan Masalah

Metode dan algoritma yang digunakan untuk menyisipkan pesan pada citra digital, maka pada permasalahan ini adalah bagaimana pesan yang disisipkan harus tidak terlihat jelas oleh kasat mata, dan juga harus menjaga keutuhan pesan yang

disisipkan dengan metode *random pixel positioning* dan algoritma *advanced encryption standard.*

Perumusan masalah dapat dilihat melalui point-point berikut ini

1. Bagaimana cara penyisipan pesan ke citra digital menggunakan metode dan algoritma yang digunakan ?
2. Bagaimana cara mendapatkan *pixel-pixel* yang telah disisipi pesan sehingga pesan dapat di-ekstrak kembali ?.

1.3. Maksud dan Tujuan

Berdasarkan permasalahan yang diteliti, maka maksud dari penulisan tugas akhir ini adalah untuk membangun aplikasi steganografi pada citra digital menggunakan metode *Random Pixel Positioning (RPP)* dan algoritma *advanced encryption standard (AES)256 bits* untuk keamanan data.

Tujuan yang akan dicapai dalam penelitian ini adalah:

1. Melakukan pengujian terhadap keamanan pesan menggunakan aplikasi *steganalysis* yaitu *StegSpy2.1*
2. Untuk mengetahui besar pesan yang dapat disembunyikan kedalam citra digital menggunakan metode *random pixel positioning (RPP).*
3. Untuk mengetahui kualitas citra yang telah disisipi pesan menggunakan metode *random pixel positioning (RPP).*
4. Untuk mengetahui ketahanan pesan pada citra yang telah disisipi pesan.

1.4. Batasan Masalah

Batasan masalah yang ditentukan pada pembangunan aplikasi steganografi menggunakan metode *Random Pixel Positioning (RPP)* dan algoritma *advanced encryption standard (AES)256* untuk keamanan data ini adalah sebagai berikut :

1. Media penampug 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 dengan jenis yaitu:
   a. Pesan teks : *.txt, *.doc, *.docx, *.pdf dan *.xls
   b. Pesan gambar : *.bmp *.png dan *.jpg.

3. Menggunakan algoritma *advanced encryption standard (AES)256bits* untuk enkripsi pesan yang akan disisipkan kedalam citra.
4. Hal – hal yang akan diujikan pada aplikasi yang dibangun yaitu:
   a. Besar pesan yang dapat disembunyikan kedalam citra
   b. Kualitas citra yang telah disisipi pesan yang dinyatakan dalam *PSNR*.
   c. Ketahanan terhadap manipulasi citra yang telah disisipi pesan (*robustness*).
5. Aplikasi yang dibangun berbasis desktop.
6. Perangkat lunak yang digunakan untuk pembangunan aplikasi yaitu :
   a. Sistem operasi yang digunakan yaitu windows.
   b. Pengkodean dan desain aplikasi menggunakan Java NetBeans7.

1.5. Metodologi Penelitian

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

1.5.1. Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam penulisan tugas akhir 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 *random pixel positioning (RPP) dan algoritma Advanced encryption standard (AES)256bits.*

1.5.2. Metode pembangunan perangkat lunak

Metode pembangunan perangkat lunak ini menggunakan metode *waterfall* seperti pada gambar 1.1 yang terdiri dari beberapa tahap, yaitu:

1. *Requirement Definition*

   Requirement Definition merupakan tahapan analis terhadap apa saja yang dibutuhkan oleh system yang akan di bangun. Analis yang dilakukan meliputi analis pengguna kebutuhan system.

2. *System and Software Design*

   System and Software Design merupakan tahap melakukan perancangan terhadap keseluruhan sistem perancangan yang dilakukan yaitu perancangan antar muka dari sistem yang dibangun.

3. *Implementation and Unit Testing*

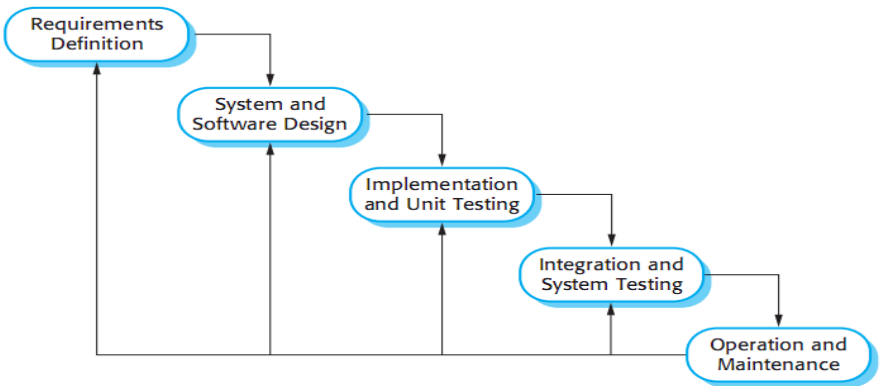
   Implementation and Unit Testing merupakan tahap merubah perancangan dan analis yang dilakukan sebelumnya kedalam kode pemograman yang digunakan. Tahap ini juga dilakukan *unit testing* untuk mengetahui apakah telah sesuai dengan kebutuhan sistem.

4. *Integrasi and System Testing*

   Integrasi and System Testing merupakan 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. *Operation and Maintenance*

   Operation and Maintenance merupakan tahap perawatan jika terjadi kesalahan pada system merawatan yang dilakukan yaitu pengkoreksi jika terjadi kesalahan, menambah fungsionalitas dan *requiretment* sistem.



Gambar 1. 1 Metode Waterfall [1]

1.6. Sistematika Penulisan

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

BAB 1. PENDAHULUAN

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

BAB 2. 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 3. ANALISIS DAN PERANCANGAN SISTEM

Bab ini membahas mengenai sub-sub sistem yang di uraikan dari sistem utama dengan tujuan untuk mengetahui cara kerja dan interaksi dari tiap sub sistem dalam fungsinya untuk mencapai tujuan sistem. Didalamnya terdapat analis terhadap proses penjadwalan kunci, proses enkripsi, proses dekripsi, proses penyisipan dan proses ekstrasi, selain itu terdapat juga kebutuhan fungsional dan nonfungsional dari sistem, perancangan antar muka untuk aplikasi yang akan dibangun sesuai dengan hasil analis yang telah dibuat.

BAB 4. IMPLEMENTASI DAN PENGUJIAN

Bab ini membahas tentang implementasi dari aplikasi yang dibangun. Implementasi dilakukan berdasarkan analis dan perancangan yang telah dilakukan, kedalam bahasa pemograman tertentu. Hasil dari implementasi, kemudian dilakukan, kedalam bahasa pemograman tertentu. Hasil dari implementasi, kemudian dilakukan pengujian apakah aplikasi telah sesuai seperti yang diharapkan.

BAB 5. KESIMPULAN DAN SARAN

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