

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Bertukar informasi digital memanfaatkan internet sangat berisiko mengalami pencurian lalu diubah sedemikian rupa lalu disebarluaskan kembali[1]. Semakin banyak serangan yang bisa terjadi dalam proses pertukaran data menyebabkan dibutuhkan suatu metode agar dapat meningkatkan keamanan informasi. Salah satu metode yang dapat digunakan yaitu teknik steganografi. Steganografi adalah suatu teknik menyisipkan pesan ke dalam suatu media[1], dimana pesan yang akan dikirimkan tidak diubah bentuknya, melainkan disisipkan pada sebuah media lain (*cover-image*) seperti gambar atau citra, video, dan suara. Media yang telah disisipi pesan rahasia (*stego-image*) kemudian dikirim kepada penerima tanpa menimbulkan kecurigaan dari pihak luar, karena perbedaan dari media asli (*cover-image*) dengan media yang telah disisipi pesan rahasia (*stego-image*) tidak kasat mata. Steganografi pada masa kini dilakukan pada media digital berupa citra, audio, maupun video.

Metode *Spread Spectrum* merupakan salah satu metode yang dapat digunakan dalam pembuatan steganografi. Metode tersebut dibagi menjadi dua proses utama, yaitu proses *encode* dan *decode*. Pada proses *encode* dilakukan operasi penyisipan pesan ke dalam *cover-image*. Sedangkan proses *decode* dilakukan proses ekstraksi pesan dan kemudian dikembalikan menjadi pesan awal[2]. Namun sebuah pesan yang disisipkan menggunakan metode *Spread Spectrum* mempunyai permasalahan pada keamanan pesan dan dapat dengan mudah dibongkar pihak ketiga karena hanya butuh tahapan proses ekstraksi dari *Spread Spectrum*[1]. Pada penelitian [1] terdapat aplikasi steganografi *Spread Spectrum*, namun dalam penelitian tersebut disebutkan jika pesan yang disisipkan ke gambar hanya berupa file pesan tanpa enkripsi. Dengan begitu, pihak manapun akan mudah membongkar isi pesan dengan hanya menerapkan algoritma ekstraksi *Spread Spectrum*. Begitu pun dengan penelitian [3] di mana keberadaan pesan teks dapat dengan mudah diekstraksi oleh pihak manapun.

Untuk menambah tingkat keamanan dari informasi yang akan disisipkan kedalam citra, steganografi dapat dikombinasikan dengan kriptografi sehingga pesan yang disisipkan akan lebih sulit untuk dibaca pihak ketiga. Namun keberadaan kriptografi tidak boleh mempengaruhi kualitas citra, citra stego yang baik harus mempunyai nilai *Peak Signal to Noise Ratio* (PSNR) minimal 40db[4]. Dipilihlah teknik kriptografi *Affine Cipher* sebagai upaya optimalisasi keamanan steganografi ini. Kriptografi adalah ilmu yang berdasarkan pada teknik matematika yang erat kaitanya dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas [5]. Sedangkan *Affine Cipher* adalah algoritma kriptografi yang dikembangkan dari metode *Caesar Cipher* [6]. Algoritma ini merupakan contoh dari kriptografi pertukaran monoalfabet. Algoritma ini bekerja dengan cara menukar setiap karakter pesan yang disisipkan dengan karakter lain, bisa berupa alfabet, angka, ataupun karakter spesial. Penukaran ini dinamakan *affine transformation* [6].

Berdasarkan hal yang telah diuraikan di atas, maka dalam penelitian ini akan dibangun sebuah sistem steganografi *Spread Spectrum* yang dipadukan dengan *Affine Cipher* sebagai upaya optimalisasi keamanan pesan, optimalisasi ini juga diharapkan tetap bisa menjaga integritas parameter dari steganografi seperti *imperceptibility*, *fidelity*, *robustness*, dan *recovery* [7].

1.2 Rumusan Masalah

Dari latar belakang di atas maka didapat berupa rumusan masalah sebagai berikut;

1. Bagaimana mengimplementasikan kombinasi algoritma steganografi *Spread Spectrum* dan kriptografi *Affine Cipher*
2. Bagaimana mengoptimalkan keamanan dan kualitas citra steganografi yang merujuk pada parameter kriptografi dan steganografi.

1.3 Maksud dan Tujuan

1.3.1 Maksud

Adapun maksud dari penelitian yang hendak dilakukan adalah menerapkan steganografi *Spread Spectrum* dan kriptografi *Affine Cipher*.

1.3.2 Tujuan

Untuk tujuan dari penelitian yang akan dilakukan adalah sebagai berikut:

1. Menghasilkan kualitas steganografi yang baik dengan melalui 4 pengujian kriteria steganografi yaitu *imperceptibility*, *fidelity*, *robustness*, dan *recovery*.
2. Mengoptimalkan keamanan pesan steganografi *Spread Spectrum* dengan *Affine Cipher* yang merujuk pada 4 kriteria keamanan kriptografi yaitu *confidentiality*, *integrity*, *availability*, dan *access control*.

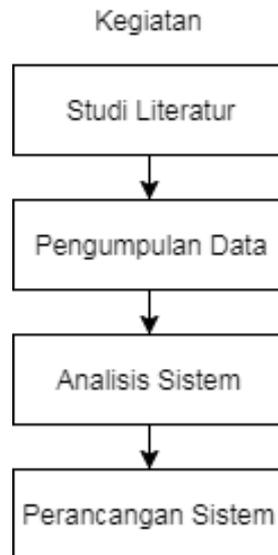
1.4 Batasan Masalah

Dalam penelitian ini terdapat beberapa batasan masalah yang harapannya dapat mempersempit masalah yang terlalu luas, diantaranya;

1. Melakukan penyisipan pesan teks dan ekstraksi pesan teks yang disisipkan ke dalam gambar.
2. Terdapat satu metode steganografi yaitu metode *Spread Spectrum*.
3. Terdapat satu metode keamanan algoritma yaitu teknik kriptografi *Affine Cipher*.
4. Menggunakan software MatLab untuk membantu analisis dan perancangan sistem.
5. Pesan yang disisipkan ke dalam gambar hanya berupa pesan teks.
6. Gambar sebagai media penyisipan pesan (*cover-image*) berformat JPG dan PNG.

1.5 Metode Penelitian

Adapun metode penelitian yang digunakan dalam penelitian ini adalah metode penelitian kuantitatif. Penelitian kuantitatif adalah suatu proses menemukan pengetahuan yang menggunakan data berupa angka sebagai alat menganalisis keterangan mengenai apa yang ingin diketahui [2].



Gambar 1.1 Kerangka Kerja Penelitian

Berdasarkan kerangka kerja penelitian yang telah digambarkan di atas, maka dapat diuraikan pembahasan masing-masing tahap dalam penelitian adalah sebagai berikut :

1. Studi Literatur

Pada tahap ini dilakukan pencarian landasan-landasan teori mengenai *Spread Spectrum* dan *Affine Cipher* yang diperoleh dari berbagai jurnal penelitian dan internet untuk melengkapi perbendaharaan konsep dan teori, sehingga memiliki landasan dan keilmuan yang baik dan sesuai.

2. Pengumpulan Data

Pada tahap ini dilakukan proses pengumpulan data dengan metode observasi untuk melakukan pengamatan dan analisa terhadap proses pembangunan sistem yang terdahulu.

3. Analisis Sistem

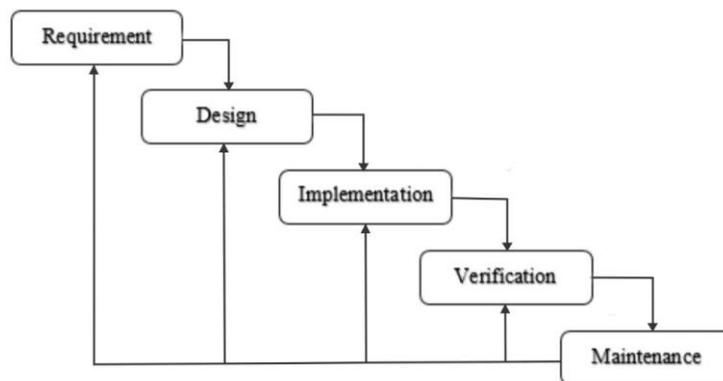
Pada tahap ini dilakukan identifikasi masalah pada sistem yang sedang berjalan. Dengan demikian, diharapkan penelitian ini dapat menemukan solusi dari permasalahan yang ada.

4. Pengembangan Sistem

Pada Tahap ini dilakukan pengembangan sistem dengan menggunakan model waterfall.

1.6 Metode Pembangunan Perangkat Lunak

Dalam membangun sistem perangkat lunak dilakukan sebuah paradigma pembangunan perangkat lunak dengan metode waterfall, yang meliputi tahapan sebagai berikut:



Gambar 1.2 Alur Proses Waterfall

Tahapan Metode *Waterfall*

Dalam pengembangannya metode *waterfall* memiliki beberapa tahapan yang berurut yaitu: *requirement* (analisis kebutuhan), *design system* (desain sistem), *Coding* (pengkodean) & *Testing* (pengujian), Penerapan Program, pemeliharaan. Tahapan tahapan dari metode *waterfall* adalah sebagai berikut :

1. *Requirement Analysis*

Tahap ini pengembang sistem diwajibkan memahami perangkat lunak yang diharapkan dan batasan perangkat lunak tersebut. Informasi ini bisa dapat

diperoleh melalui wawancara, diskusi, atau survei langsung. Informasi dianalisis untuk mendapatkan data yang dibutuhkan.

2. *System Design*

Spesifikasi kebutuhan dari tahapan sebelumnya akan mulai dipelajari disini dan desain sistem dibangun. Desain Sistem membantu untuk menentukan perangkat keras (*hardware*) dan sistem persyaratan dan juga membantu dalam mendefinisikan arsitektur sistem secara keseluruhan.

3. *Implementation*

Dalam tahap ini, sistem pertama kali dikembangkan di program kecil yang biasa disebut *unit*. Setiap *unit* dikembangkan dan diuji untuk fungsionalitas yang disebut sebagai *unit testing*.

4. *Integration & Testing*

Seluruh *unit* yang dikembangkan dalam tahap implementasi diintegrasikan ke dalam sistem setelah dilakukannya pengujian pada masing-masing *unit*. Setelah itu seluruh sistem diuji untuk mengecek setiap kegagalan maupun kesalahan.

5. *Operation & Maintenance*

Tahap ini adalah tahap akhir dalam model waterfall. Perangkat lunak yang sudah jadi, dijalankan serta dilakukan pemeliharaan. Pemeliharaan termasuk dalam memperbaiki kesalahan yang tidak ditemukan pada langkah sebelumnya.

1.7 Sistematika Penulisan

BAB 1 PENDAHULUAN

Bab ini akan membahas mengenai latar belakang masalah, perumusan masalah, maksud dan tujuan, batasan masalah, metodologi penelitian yang digunakan, serta sistematika penulisan.

BAB 2 LANDASAN TEORI

Membahas berbagai konsep dasar dan teori-teori yang berkaitan dengan topik penelitian yang dilakukan dan hal-hal yang berguna dalam proses analisis permasalahan.

BAB 3 ANALISIS DAN PERANCANGAN

Membahas tentang hasil pencarian data, analisis masalah, analisis kebutuhan, analisis proses, dan perancangan sistem yang dibangun.

BAB 4 IMPLEMENTASI DAN PENGUJIAN

Implementasi dari apa yang telah dijabarkan dan dianalisis di bab sebelumnya. Pengujian yang menunjukkan jika perangkat lunak sudah siap digunakan.

BAB 5 KESIMPULAN DAN SARAN

Berisi kesimpulan terkait dari penelitian ini yang mengambil tema tentang steganografi dan kriptografi. Disini juga dijelaskan soal keberhasilannya menjalankan penelitian ini. Ada pula saran untuk menjadikan penelitian ini lebih baik lagi kedepannya.

