BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Perkembangan teknologi informasi berkembang begitu pesat dan semakin memudahkan penggunanya dalam berkomunikasi melalui berbagai macam media. Komunikasi yang pada dasar nya melibatkan minimal dua objek yang saling mengirim ataupun menerima pesan yang memanfaatkan teknologi informasi rentan terhadap kejahatan yang merujuk pada memanipulasi pesan dengan cara memanfaatkan celah keamaanan.

Keamanan dari suatu pesan adalah suatu aspek terpenting dari informasi. Berhubungan dengan pentingnya informasi, pihak pengirim mempertanyakan keaslian informasi tersebut, apakah masih murni atau sudah merupakan informasi yang telah dikelola oleh pihak yang tidak berkepentingan. Karena kerahasiaan suatu informasi akan hilang jika telah diakses oleh pihak yang tidak memiliki kepentingan terhadap informasi tersebut, ditambah maraknya tidakan phishing pada pencurian data pada beberapa *platform* email maka dengan ditingkatkannya keamanan pada email diharapkan pesan tidak mudah jatuh kepada pihak-pihak yang tidak memiliki kepentingan.

Banyaknya model dari keamanan data yang telah dikembangkan salah satunya adalah algoritma steganografi least significant bit (LSB) dan algoritma kriptografi vigenere cipher. Dimana algoritma LSB ini paling sederhana, cepat dalam proses

UNIVERSITAS ISLAM NEGERI
SUNAN GUNUNG DJATI

penyisipan dan ektraksi pesan, serta mempunyai kapasitas penyisipan yang cukup besar dibandngkan algoritma pada umumnya serta kualitas citra hasil yang cukup baik.[1] Algoritma LSB merupakan metode yang menerapkan teknik substitusi. Metode LSB menyembunyikan data rahasia ke dalam piksel-piksel yang tidak signifikan (least significant pixel) dari stegomedium.[2]

Algoritma vigenere cipher merupakan algoritma yang tangguh, teks yang telah dienkripsi menggunakan algoritma vigenere cipher akan sulit didapatkan hasil dekripsinya tanpa mengunakan kuncinya. Viginere cipher memiliki table standart vigenere dalam mengenkripsi sebuah pesan. Tabel vigenere standar yang digunakan adalah table huruf 26 alfabetik, yang dimulai dari huruf A sampai dengan huruf Z. Kunci vigenere cipher digunakan secara berulang sebanyak pesan yang dienkripsi. Semakin unik huruf alfabetik yannf digunakan sebagai key atau kunci, maka akan semakin kuat keamanan dari algoritma vigenere cipher.[3]

Algoritma steganografi memiliki tujuan dan fungsi untuk menyembunyikan pesan kedalam media citra, untuk meningkatkan keamanan pesan dapat digunakan kombinasi antara kriprografi dengan steganografi karena steganografi memiliki alur yang searah dengan kriptografi, dimana kriptografi sendiri memiliki bentuk untuk memberikan beberapa samaran dari sebuah pesan melalui media digital, dengan demikian data yang berbentuk teks dapat disisipkan kedalam sebuah gambar ataupun video, atau dengan kata lain plaintext dienkripsi terlebih dahulu, kemudian ciphertext disisipkan didalam media lain, sehinga pihak-pihak yang tidak memiliki kepentingan tidak menyadari keberadaan pesan yang telah disembunyikan.

UNIVERSITAS ISLAM NEGERI
SUNAN GUNUNG DJATI

1.2. Perumusan Masalah

Berdasarkan latar belakang tersebut dapat disimpulkan rumusan masalah sebagai berikut :

1. Bagaimana menerapkan algoritma vigenere cipher untuk mengenkripsi pesan?
2. Bagaimana mengimplementasikan algoritma least significant bit untuk menyembuyikan ciphertext yang telah di enkripsi oleh algoritma vigenere cipher kedalam media citra digital?
3. Bagaimana kinerja Algoritma vigenere cipher dan least significant bit?

1.3. Tujuan Penelitian

Tujuan Adapun tujuan penelitian ini adalah :

1. Menerapkan algoritma *vigenere cipher* untuk mengenkripsi pesan.
2. Menerapkan algoritma *least significant bit* untuk menyembunyikan *ciphertext*.
3. Mengetahui kinerja algoritma *vigenere cipher* dan *least significant bit*.

UNIVERSITAS ISLAM NEGERI
SUNAN GUNUNG DJATI
BANDUNG

1.4. Manfaat Penelitian

Manfaat dari penelitian ini yaitu menghasilkan sebuah sistem yang dapat meningkatkan keamanan pesan, agar pesan tidak mudah jatuh kepada pihak yang tidak berkepentingan. Sistem ini dikembangkan dengan menggunakan teknik steganografi dan kriptografi menggunakan metode Least Significant Bit untuk menyisipkan pesan kedalam media citra digital dan Vigener cipher untuk mengenkripsi pesan. Dengan harapan sistem ini dapat meningkatkan keamanan dengan lebih baik, sehingga pesan

tidak mudah terbaca serta kerahasiaan pesan yang lebih terjaga, dengan demikian keamanan pesan akan jauh lebih baik.

1.5. Batasan Masalah

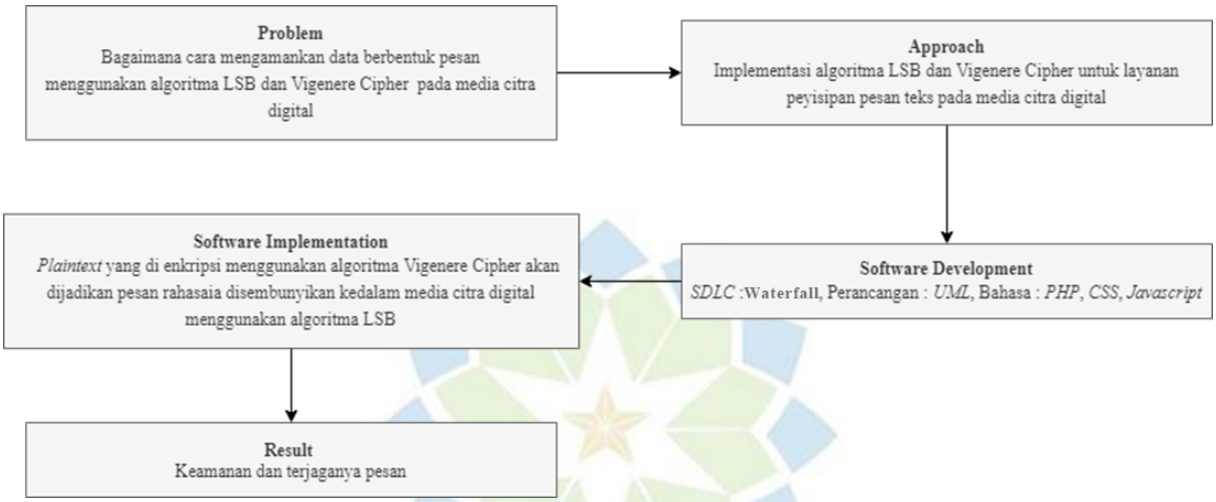
Banyaknya perkembangan dan pembahasan ini dapat ditentukan dalam permasalahan di atas, dalam batasan-batasan mengenai permasalahan apa yang akan diselesaikan dalam peneliltian ini. Adapun batasan-batasan tersebut diantaranya:

1. Penyisipan pesan taks kedalam media citra digital pada penelitian ini dibatasi menggunakan algoritma least significant bit.
2. Teks yang dienkripsi dibatasi menggunakan algoritma vigenere cipher sebelum disisipkan kedalam media citra digital.
3. Pengiriman pesan dibatasi manggunakan *library* PHPMailer.
4. Jumlah karakter teks maksimal yang disisipkan kedalam media citra digital sebanyak 5000 karakter.
5. Format gambar yang dapat dienkripsi meliputi jpg.

SUNAN GUNUNG DJATI
BANDUNG

1.6. Kerangka Pemikiran

Adapun kerangka pemikiran dari Aplikasi ini yang di gambarkan pada Gambar 1.1 kerangaka pemikiran.



Gambar 1. 1 Kerangka Pemikiran

1.7.Metodologi Penelitian

1.7.1 Metodologi Penelitian

Metode yang digunakan untuk mengumpulkan data yaitu dengan menggunakan sebuah metode penelitian deskriptif, menggunakan metode penelitian yang memiliki tujuan untuk menggambarkan permasalahan secara lengkap dan objektif . Adapun metode yang digunakan dalam pengumpulan data tersebut diataranya:

1. Wawancara merupakan cara untuk mendapatkan sebuah informasi melalui penelitian langsung terhadap narasumber. Dalam hal ini narasumber merupakan seseorang yang ahli dalam bidang penelitian yang berkaitan.

2. Observasi, yaitu mengamati objek penelitian secara langsung agar mendapatkan data-data yang dibutuhkan.
3. Studi Literatur, yaitu untuk mendapatkan data secara tertulis yang didapat dari kajian secara literature, studi ilmiah dan laporan penelitian yang terkait dengan bidang studi yang diteliti.

1.7.2 Metodelogi Pengembangan

Tahapan-tahapan yang digunakan dalam pengembangan sistem adalah dengan model Waterfall. Model waterfall merupakan suatu metode yang dikenal sebagai model air terjun karena dalam proses membangun sistem, pengembang harus menyelesaikan fase saat ini sebelum melanjutkan fase yang berikutnya [8].

Adapun tahapan-tahapan dalam pengembangan sistem otorisai user dengan menggunakan metode waterfall ini dapat dijelaskan sebagai berikut:

1. Requirements Specification

Merupakan tahap awal dalam model waterfall yang bertujuan untuk menganalisa semua kebutuhan yang diperlukan dalam pembangunan proyek tugas akhir ini. Dalam pembangunan sistem otorisasi ini dijelaskan mengenai hardware dan software yang dibutuhkan.

2. Design

Tahap design merupakan tahap perancangan desain, pada tahap ini desain sistem otorisasi dirancang mulai dari perancangan desain user interface sampai dengan perancangan alur program sistem otorisasi ini.

UNIVERSITAS ISLAM NEGERI SUNAN GUNUNG DJATI BANDUNG

3. Implementation

Tahap ini adalah proses pengerjaan sistem dengan menerapkan kode program (Encoding) berdasarkan hasil perancangan desain yang telah dilakukan pada tahap sebelumnya kedalam bahasa pemrograman. Pada tahap inilah desain sistem otorisasi yang telah dirancang diimplementasikan sehingga rancangan sebelumnya menjadi suatu model program.

4. Testing

Tahap ini merupakan pengujian yang dilakukan oleh individu atau kelompok penguji (Unit Testing) terhadap seluruh sistem yang telah dibangun

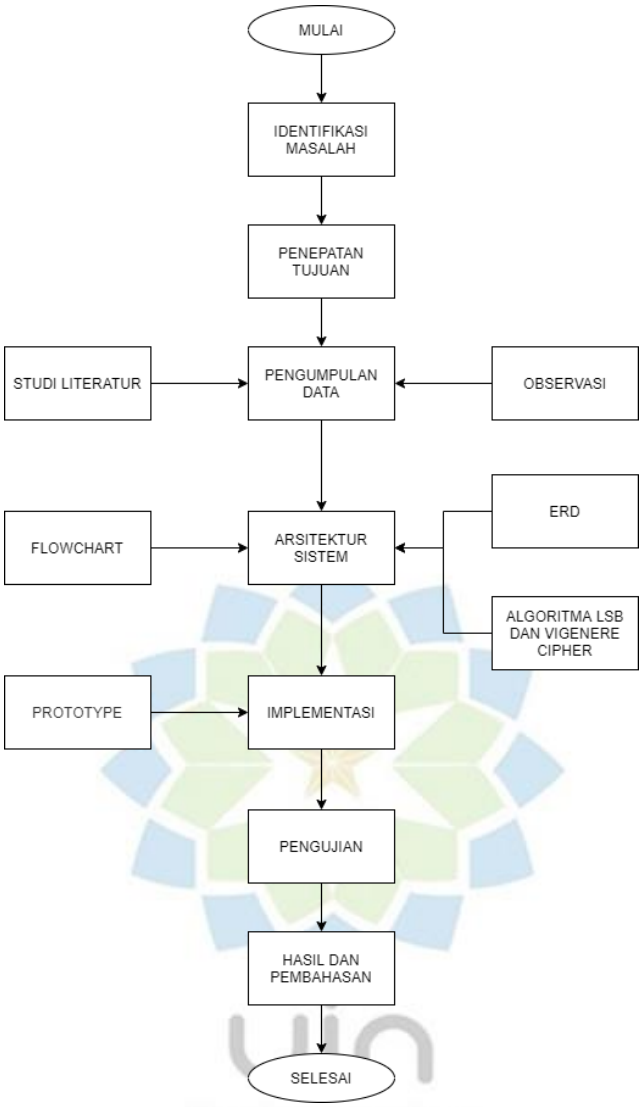
5. Devloyment and Maintenance

Tahapan ini adalah tahap terakhir dari model waterfall yaitu menjalankan sistem yang telah dibangun, memperbaiki bug dan dilakukan pemeliharaan secara berkala

1.7.3. Alur Penelitian

UNIVERSITAS ISLAM NEGERI
SUNAN GUNUNG DJATI
BANDUNG

Berikut alur penelitian dari Aplikasi ini yang digambarkan pada Gambar 1.2 alur penelitian.



Gambar 1. 2 Alur Penelitian

UNIVERSITAS ISLAM NEGERI
SUNAN GUNUNG DJATI
BANDUNG

1.8.Sistematika Penulisan

Laporan tugas akhir terbagi ke dalam lima bab tersusun secara sistematika sebagai berikut ini:

BAB I PENDAHULUAN

Bab I ialah bab yang menjadi gambaran mengenai permasalahan – permasalahan yang akan dibahas pada bab berikutnya. Bab I ini terdiri pada beberapa

pokok bahasan latar belakang, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian dan sistematika penulisan.

BAB II STUDI PUSTAKA

Pada Bab II dijelaskan mengenai teori yang berkaitan pada penelitian serta proses perancangan dan implementasi system. Pada bab II juga berisikan State of The Art atau pemaparan mengenai penelitian – penelitian para terdahulu yang memiliki kaitan dengan penelitian yang akan penulis lakukan.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab III menjelaskan mengenai pembahasan analisis serta perancangan sistem yang dibangun berdasarkan permasalahan yang sudah dirumuskan pada bab II.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Bab IV ialah pembahasan terhadap kebutuhan system yang dikembangkan serta implementasi pengembangan system, spesifikasi system dan juga pengujian.

UNIVERSITAS ISLAM NEGERI
SUNAN GUNUNG DJATI
BANDUNG

BAB V KESIMPULAN DAN SARAN

Bab V kesimpulan dan saran membahas mengenai rincian kesimpulan dari hasil penelitian serta memuat saran untuk kajian lanjutan yang berketerkaitan dengan penelitian yang dilakukan.