BAB I

PENDAHULUAN

1.1 Latar Belakang Penelitian

Aset terpenting yang paling dilindungi di zaman digital ini salah satunya adalah data. Banyak kemungkinan suatu data yang disimpan oleh seseorang dapat dicuri dan disalahgunakan oleh pihak yang tidak berwenang dan oknum yang sangat merugikan. Fenomena saat ini tidak dapat disangkal bahwa alamat email dan password pengguna di negara Indonesia yang bocor di internet tembus 3,2 Miliar secara keseluruhan kredensial dibanding tahun 2017 yang hanya mencapai 1,7 Miliar [1]. Ditambah kabar terbaru lagi yang sangat fenomenal di tahun 2022 ini, kasus Hacker Bjorka yang berhasil meretas data pelanggan Indihome, data registrasi SIM Card, data rahasia presiden dan data-data tokoh pejabat pemerintahan Indonesia yang terumbar data-datanya di situs internet [2].

Saat ini berbagai platform dan aplikasi banyak yang menerapkan berbagai jenis pengamanan data, misalnya *end to end encryption* pada fitur *chat* dan perbankan. Dengan model pengamanan data ini membuat hanya pihak penerima dan pengirim yang bisa membaca keaslian data. Dan jenis pengamanan data lainya seperti kriptografi dan steganografi yang sampai saat ini banyak penelitian dan pengembangan dari tahun ke tahun.

Peningkatan dan perkembangan terjadi pada berbagai algoritma kriptografi yang mana Vigenere Cipher paling banyak mengalami evolusi. Salah satu pengembangannya adalah dengan membuat kombinasi Vigenere Cipher dengan 1 algoritma lain yang di mana rata-rata hanya melakukan 2 kombinasi algoritma dalam pengembangan penelitiannya. Sementara itu, jika proses enkripsi semakin banyak maka proses pemecahan sandi akan lebih sulit dilakukan dan semakin aman dalam merahasiakan informasi [3].

Algoritma Vigenere Cipher merupakan algoritma yang kuat, jika teks yang dienkripsi dengan algoritma Vigenere Cipher tidak digunakan maka akan sulit untuk mendapatkan hasil dekripsi. Viginere Cipher memiliki tabel Vigenere standar saat mengenkripsi pesan. Tabel Vigenere standar yang digunakan adalah alfabet 26

huruf, dari huruf A sampai huruf Z. Kunci Vigenere Cipher digunakan secara berulang sebanyak pesan yang dienkripsi. Semakin unik huruf alfabetik yang digunakan sebagai key atau kunci, maka akan semakin kuat keamanan dari algoritma Vigenere Cipher [4]. Vigenere Cipher berfungsi untuk mengenkripsi data pesan sehingga menjadi kode enkripsi yang tidak dipahami.

Rivest Code 4 merupakan salah satu jenis stream Cipher, yaitu memproses unit atau input data pada satu saat. Unit atau data pada umumnya sebuah byte atau bahkan kadang kadang Bit (byte dalam hal RC4). Panjang kunci yang digunakan 1 sampai 256 byte algoritma kriptografi ini sederhana dan mudah diimplementasikan dengan kecepatan proses enkripsi dan dekripsi yang terbilang cukup cepat [5]. Rives Code 4 berfungsi untuk mengenkripsi data pesan menjadi kode *hexadecimal* yang mana hal ini merupakan kode yang sulit untuk dipecahkan.

Kombinasi Vigenere Cipher dan RC4 merupakan kombinasi algoritma kriptografi yang memiliki kinerja bagus yaitu dengan mendekripsikan setiap huruf dengan kunci yang berbeda serta panjang kunci yang digunakan mencapai 256 byte. Dengan menggabungkan dua metode akan mempersempit kemungkinan kebocoran data enkripsi sehingga data menjadi lebih aman [6].

Algoritma LSB adalah yang paling sederhana, dan cepat dalam proses penyisipan dan ekstraksi pesan. Dibandingkan dengan algoritma umum, memiliki kapasitas penyisipan yang cukup besar, dan kualitas gambar yang dihasilkan cukup baik [7]. Algoritma LSB adalah metode penerapan teknik penyembunyian. Metode LSB menyembunyikan data rahasia ke dalam piksel paling tidak signifikan dari stegomedium [8]. Algoritma steganografi LSB memiliki tujuan dan fungsi untuk menyembunyikan pesan ke dalam media citra, untuk meningkatkan keamanan pesan dapat digunakan kombinasi antara kriptografi 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 ke dalam sebuah gambar ataupun video, atau dengan kata lain plaintext dienkripsi terlebih dahulu, kemudian ciphertext disisipkan di dalam media lain, sehingga pihak-pihak yang tidak memiliki kepentingan tidak menyadari keberadaan pesan yang telah disembunyikan.

Problematika implementasi LSB, Vigenere Cipher, dan Rivest Code 4 hanya bisa mengenkripsi data berbentuk teks. Oleh karena itu data berbentuk file perlu dikonversi menjadi data berbentuk teks agar bisa diimplementasikan. Base64 akan menyempurnakan implementasi kombinasi algoritma LSB, Vigenere Cipher dan Rivest Code 4 terhadap data berbentuk file. Base64 memiliki salah satu kegunaan dalam mengonversi data berbentuk file menuju data berbentuk teks [9].

Penelitian ini akan mengombinasikan 3 algoritma antara lain steganografi Least Significant Bit (LSB), algoritma kriptografi Vigenere Cipher dan algoritma kriptografi Rivest Code 4. Algoritma Vigenere Cipher dan Rivest Code 4 akan digunakan sebagai kombinasi pengamanan enkripsi data sehingga menjadi 2 lapis enkripsi dan algoritma Least Significant Bit (LSB) akan menyembunyikan hasil enkripsi tersebut ke dalam gambar sehingga sulit ditebak keberadaannya dan sulit untuk mendekripsikannya.

1.2 Perumusan Masalah Penelitian

Adapun rumusan masalah dari penelitian ini adalah sebagai berikut:

1. Bagaimana implementasi algoritma Least Significant Bit yang berfungsi untuk menyembunyikan pesan rahasia yang telah dienkripsi oleh kombinasi algoritma Vigenere Cipher dan Rivest Code 4 di dalam media citra digital terhadap pengamanan pesan rahasia?
2. Bagaimana kinerja aplikasi terhadap algoritma Least Significant Bit dan kombinasi Vigenere Cipher dengan Rivest Code 4 untuk pengamanan pesan rahasia berbasis citra digital?

1.3 Tujuan Penelitian

Tujuan dilakukannya penelitian ini adalah sebagai berikut:

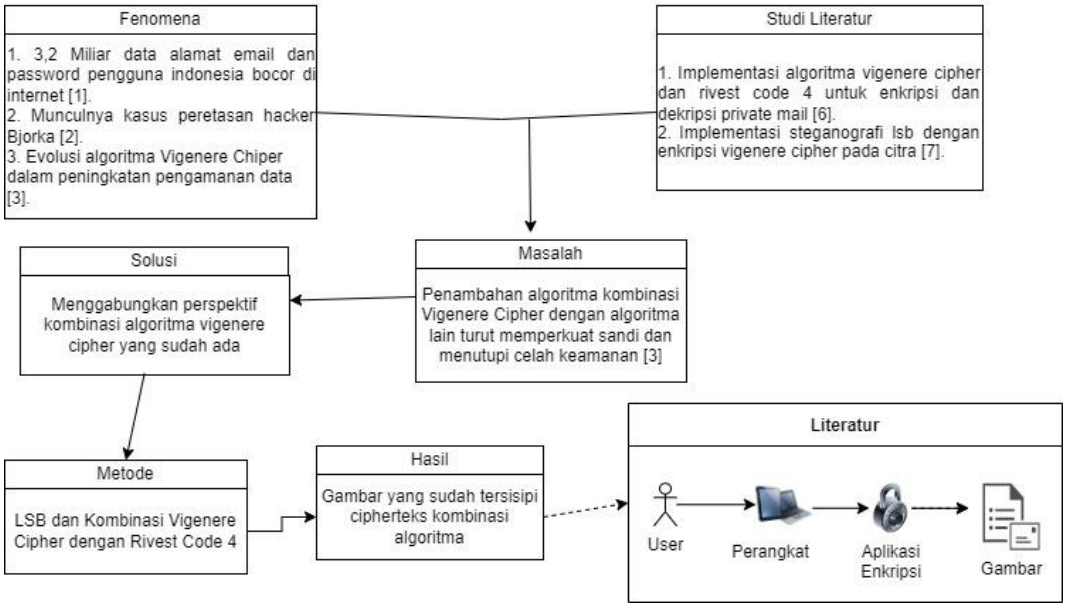
1. Menerapkan algoritma Least Significant Bit yang berfungsi untuk menyembunyikan pesan rahasia yang telah dienkripsi oleh kombinasi algoritma Vigenere Cipher dan Rivest Code 4 di dalam media citra digital terhadap pengamanan pesan rahasia.
2. Mengetahui kinerja aplikasi terhadap implementasi algoritma Least Significant Bit dan kombinasi Vigenere Cipher dengan Rivest Code 4 untuk pengamanan pesan rahasia berbasis citra digital.

1.4 Batasan Masalah Penelitian

Untuk membatasi pembahasan agar tidak keluar dari topik penelitian, maka dibutuhkan batasan masalah. Adapun batasan-batasan masalah yang diterapkan sebagai berikut:

1. Pesan teks yang dienkripsi dibatasi dengan kombinasi algoritma Vigenere Cipher dan Rivest Code 4 untuk disisipkan di dalam media citra digital.
2. Penyisipan pesan text ke dalam media citra digital ini menggunakan algoritma Least Significant Bit dengan penyisipan 1 bit terakhir *binary blue* pada setiap pixel gambar.
3. Maksimal karakter teks yang dienkripsi adalah sebanyak 1 juta karakter
4. File yang bisa dikonversi menjadi byte array teks dan sebaliknya merupakan jenis format RAR, PDF, MP3 dan MP4.
5. Jenis format gambar untuk dijadikan cover steganografi adalah berformat .jpg .

1.5 Kerangka Pemikiran Penelitian



Gambar 1. 1 Kerangka Pemikiran

Kriptografi merupakan ilmu serta seni untuk melindungi keamanan pesan kala pesan dikirim dari suatu tempat ke tempat lain [9]. Pesan yang dirahasiakan dinamakan plaintext, sebaliknya pesan hasil penyandian disebut ciphertext.

Enkripsi atau disebut juga proses penyandian plaintext jadi ciphertext sedangkan proses membalikkan ciphertext jadi plaintext asalnya disebut dekripsi.

Enkripsi kriptografi menimbulkan banyak kecurigaan oleh siapapun. Sehingga bisa jadi orang luar akan mencari cara untuk memecahkan enkripsi tersebut. Oleh karena itu dibuatkanlah Steganografi untuk menyembunyikan enkripsi, sehingga orang biasa tidak akan mencurigai dan melakukan tindakan pemecahan enkripsi karena rasa penasaran tersebut. Hal ini akan berbeda situasinya jika orang tersebut adalah kriptanalis. Ia bisa melakukan pemecahan enkripsi pesan walaupun tersembunyi di media apapun jika algoritma enkripsinya lemah dan diketahui olehnya. Oleh karena itu perlu ada penguatan keamanan pesan agar tidak terbongkar dengan mudah. Kombinasi algoritma enkripsi merupakan salah satu solusi dalam menangani kerentanan ini. Dengan adanya kombinasi ini, diharapkan menyulitkan dan memperumit kriptanalis dalam membongkar pesan yang sudah menjadi 2 lapis enkripsi karena kombinasi algoritma tersebut.

1.6 Sistematika Penulisan

Peraturan sistematika penulisan tugas akhir di jurusan Teknik Informatika UIN Sunan Gunung Djati Bandung telah menetapkan dalam peraturan barunya bahwa sistematika penulisan tugas akhir mahasiswa terbagi menjadi lima bagian [10]. Sistematika penulisan tersebut antara lain:

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 penelitian, rumusan masalah penelitian, tujuan penelitian, batasan masalah penelitian, kerangka pemikiran penelitian, dan sistematika penulisan.

BAB II KAJIAN LITERATUR

Bab II adalah Kajian Literatur yang membahas perihal perkembangan paling mutakhir dalam global keilmuan dan penelitian atau seringkali identik dengan state of the art asal teori yang sedang dikaji dan kedudukan masalah penelitian dalam bidang informatika yang sedang diteliti.

BAB III METODOLOGI PENELITIAN

Bab III mendekripsikan langkah-langkah dan teknik yang dilakukan pada penelitian, lazimnya dijelaskan secara kronologis serta sistematis. Mayoritas metode penelitian mengacu pada model proses pengembangan software yg ada, atau contoh model lain yang cocok dengan kebutuhan serta ciri penelitian yang dilakukan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini peneliti memaparkan 2 hal utama. Pertama pemaparan perihal temuan atau hasil penelitian berdasarkan tahapan penelitian yang dilakukan. Peneliti mampu memaparkan penelitiannya yang akan terjadi dalam bentuk kualitatif atau kuantitatif sesuai hasil pengelolaan dan analisis data. Pemaparan hasil penelitian disesuaikan dengan urutan rumusan masalah penelitian. Kedua pembahasan hasil atau temuan penelitian untuk menjawab rumusan penelitian. Pola tematik disarankan untuk memudahkan pembahasan hasil penelitian, di mana setiap temuan dibahas secara langsung sebelum membahas ke temuan selanjutnya.

BAB V SIMPULAN DAN SARAN

Penulisan simpulan dijelaskan dengan cara uraian padat lebih baik daripada dengan cara butir demi butir. Simpulan harus bisa menjawab rumusan masalah. Selain itu, simpulan tak mencantumkan lagi angka-angka kuantitatif termasuk angka-angka yang merupakan poin hasil pengujian. Dalam tawaran penelitian selanjutnya, usahakan saran atau rekomendasi dipusatkan di dua atau 3 hal yang paling utama dalam penelitian. Alangkah baiknya jika penulis menyarankan penelitian yang satu tahap lebih baik dari penelitiannya sendiri.