

BAB I PENDAHULUAN

1.1 Latar Belakang

Hanya dua faktor yang sangat penting untuk sistem informasi saat ini adalah keamanan dan integritas data. Hal ini disebabkan oleh pertumbuhan teknologi berbasis pengetahuan saat ini, yang memungkinkan munculnya alat-alat baru yang terutama digunakan oleh institusi terkait untuk memastikan keamanan sistem informasi tersebut. Ironisnya, teknik yang digunakan untuk mengenkripsi data untuk penyimpanan biasanya lebih kompleks daripada teknik yang digunakan untuk mengenkripsi data untuk transmisi. Oleh karena itu, perlu dibuat sistem perlindungan data yang dapat melindungi informasi sensitif melalui enkripsi data, sehingga menyulitkan pihak yang tidak dapat dipercaya untuk mengakses dan mendekodekannya.

Setiap aktivitas yang membahayakan privasi seseorang dapat diartikan sebagai sarana untuk mengakses, mentransfer, atau menyimpan data pribadi mereka tanpa sepengetahuan mereka. Istilah "kejahatan dunia maya" mengacu pada jenis kejahatan kekerasan yang memungkinkan penggunaan internet atau perangkat elektronik lainnya untuk melakukan kejahatan kekerasan. Islam tidak salah lagi menekankan pentingnya melindungi privasi individu sebagaimana dinyatakan dalam Al-Qur'an Surah An-Nur ayat 27 yang berbunyi :

يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّى تَسْتَأْنِسُوا
وَتُسَلِّمُوا عَلَىٰ أَهْلِهَا ذَلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُونَ

Yang artinya : “Wahai orang-orang yang beriman! Janganlah kamu memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. Yang demikian itu lebih baik bagimu, agar kamu selalu ingat”. Ayat tersebut menjelaskan pentingnya dalam menjaga suatu privasi dimana pada penelitian ini yang menjadi privasi adalah sebuah pesan yang bersifat rahasia.

Untuk itu akan diterapkan suatu teknik yang dapat digunakan dalam meningkatkan keamanan sebuah pesan.

Kriptografi dan steganografi adalah dua metode keamanan data yang terkenal. Kriptologi adalah studi tentang bagaimana menganalisis informasi secara non-artistik dengan menggunakan data, informasi, atau sumber lain sebagai bukti. Enkripsi dan dekripsi adalah dua proses utama dalam sebuah citra kriptografi. Dekripsi adalah proses perubahan ciphertext kembali menjadi plaintext, sedangkan enkripsi adalah perubahan plaintext menjadi ciphertext. Dekripsi adalah proses membalikkan proses enkripsi dan mengubah data terenkripsi kembali menjadi plaintext. Steganografi adalah teknik yang digunakan untuk menjamin kerahasiaan suatu pesan. Dengan menempatkan informasi tersembunyi dalam file sampel, steganografi mempertahankan statusnya sebagai bentuk media yang sah sehingga tampak seperti teks biasa. Hanya mereka yang mau memahami makna dari pesan yang bersangkutan yang boleh membaca pesan yang telah ditulis.

Dalam penelitian ini algoritma kriptografi dan steganografi yang digunakan oleh peneliti adalah algoritma *Beaufort* dan *LSB2bit*. Algoritma *Beaufort* adalah satu-satunya variasi paling umum dari metode sandi *Vigenère*, yang menggunakan jenis skrip klasik tertentu. Di *Beaufort*, definisi *K* ditulis sebagai $K = k_1 \dots k_d$. Dimana k_i diturunkan dari angka yang sama dengan pergeseran abjad *I* sebagai cipher *Vigenere*. Algoritma *LSB* bukanlah prosedur yang sangat rumit, dan penyimpanan pesan dalam gambar juga sangat besar, sehingga Anda dapat memasukkan data. Metode tersebut mengandalkan bilangan biner yaitu 0 dan 1 untuk mempercepat proses implementasi. Selain itu, metode ini hanya membutuhkan satu bit, dan ini sangat penting karena stego image atau media yang diperoleh hampir sama dengan steganografi yang digunakan sebelumnya karena hanya tersisa satu bit yang perlu dilindungi.

Penggunaan kedua algoritma tersebut bertujuan untuk mengamankan pesan sebelum di sisipkan ke dalam citra sehingga pesan yang akan disisipkan akan memiliki tingkat keamanan yang lebih baik. Berdasarkan latar belakang diatas, pada penelitian ini akan dibangun sebuah aplikasi untuk mengamankan pesan yang terdapat pada sebuah *file text* dengan cara melakukan enkripsi terhadap pesan yang

selanjutnya akan disembunyikan pada sebuah citra, oleh karena itu dalam penelitian ini akan diambil sebuah judul “**Kombinasi Algoritma Beaufort Cipher dan LSB2bit Untuk Keamanan File Text**”.

1.2 Rumusan Masalah

Berikut adalah rumusan masalah yang akan dipecahkan melalui penelitian ini, antara lain :

- a. Bagaimana mengamankan data pesan teks dan menyisipkannya ke dalam sebuah citra ?
- b. Bagaimana proses penggunaan algoritma beaufort dan LSB2bit dalam sebuah aplikasi ?
- c. Bagaimana membangun sebuah aplikasi berbasis android untuk digunakan pada perangkat *mobile* ?

1.3 Batasan Masalah

Ada beberapa batasan permasalahan dalam penulisan penelitian ini, antara lain :

- a. Aplikasi yang akan dibangun pada penelitian ini akan digunakan untuk enkripsi pesan yang terdapat pada *file text* dan menyisipkannya pada citra.
- b. Citra yang digunakan untuk penyisipan pesan adalah citra digital dengan ekstensi .jpeg/.jpg, .png dan .bmp.
- c. Pesan yang akan disisipkan pada citra berasal dari teks yang terdapat pada *file text* dengan ekstensi .txt.
- d. Proses enkripsi dilakukan menggunakan algoritma beaufort cipher dan proses penyisipan dilakukan menggunakan algoritma LSB2bit.
- e. Sistem akan dibangun menggunakan perangkat lunak Android Studio dan akan digunakan pada *smartphone* Android.
- f. Bahasa pemrograman yang akan digunakan dalam membangun sistem adalah Java.

1.4 Tujuan Penelitian

Tujuan dari pelaksanaan penelitian ini dapat disimpulkan menjadi poin sebagai berikut :

- a. Mengamankan dan menyisipkan pesan yang terdapat pada file text ke dalam sebuah citra.
- b. Menggunakan algoritma beaufort dan algoritma LSB2bit untuk mengamankan pesan.
- c. Membangun aplikasi berbasis android untuk mengamankan dan menyisipkan pesan ke dalam citra.

1.5 Manfaat Penelitian

Yang menjadi manfaat dari pelaksanaan penelitian ini dapat dilihat sebagai berikut :

- a. Aplikasi yang dihasilkan dapat dijadikan sebuah media untuk mengamankan dan menyisipkan pesan ke dalam citra
- b. Dengan kombinasi algoritma beaufort cipher dan LSB2bit akan dihasilkan sebuah sistem yang lebih baik dalam mengamankan pesan.
- c. Aplikasi berbasis android dapat mempermudah pengguna dalam menggunakan aplikasi secara *mobile*.

