BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Seiring dengan perkembangan zaman, teknologi informasi dan komunikasi juga berkembang dengan pesat sehingga menjadi salah satu teknologi yang banyak digunakan dalam kehidupan sehari-hari, perkembangan teknologi informasi dan komunikasi ini membawa banyak manfaat dan keuntungan yang didapat dalam berbagai bidang industri. Dengan kemajuan teknologi informasi, internet sudah menjadi bagian yang sangat penting bagi masyarakat modern. Internet merupakan sekumpulan jaringan komputer yang terhubung dengan berbagai situs pemerintah, instansi, grup, maupun perorangan dengan tujuan memberikan informasi terhadap pengguna (Handoyo dkk., 2018). Selain membawakan banyak manfaat dan keuntungan, terdapat kerugian yang dapat diakibatkan pihak-pihak yang tidak bertanggung jawab di internet, seperti pencurian data penting, berbagai situs di *hack*, dan data sensitif pribadi disadap. Data teks, sebagai salah satu bentuk informasi yang paling umum di internet sehingga data teks ini menjadi sasaran empuk untuk bagi pihak-pihak yang tidak bertanggung jawab di internet. Salah satu kasus kerugian dari aksi pihak-pihak yang tidak bertanggung jawab adalah pada kasus pembajakan aplikasi percakapan WhatsApp milik direktur utama PT Tempo Inti Media Tbk, Toriq Hadad (Wildasyah, 2019). Oleh karena itu, perlu adanya langkah-langkah keamanan yang kuat untuk melindungi data pribadi.

Keamanan merupakan salah satu faktor utama di dalam dunia teknologi informasi dan komunikasi. Banyak perusahaan, instansi, ataupun organisasi memiliki informasi yang bersifat rahasia, dalam penyebaran informasi yang bersifat pribadi dan rahasia biasanya lebih cenderung mengalami serangan dari pihak ketiga, sehingga keamanan pengiriman data atau informasi rahasia harus lebih ditingkatkan (Mulyono dkk., 2018). Terdapat beberapa metode yang dapat digunakan untuk mengamankan informasi, pertama dengan menggunakan metode steganografi pesan akan di sembunyikan dalam media data lain contohnya berupa gambar, dengan menyembunyikan pesan di dalam media lain maka pihak-pihak tidak bertanggung jawab akan terkecoh dengan tampilannya seakan-akan data tersebut hanyalah data gambar biasa (Prasetya dkk., 2023). Selain itu metode kedua

adalah kriptografi, metode ini mengubah makna pesan sehingga tidak dapat terbaca atau tidak ada maknanya dengan menggunakan berbagai perhitungan matematika (Mulyono dkk., 2018).

Penelitian sebelumnya yang dilakukan oleh Fitri Yanti dan Khari Budayawan (2023) menggabungkan steganografi *Least Significant Bit* (LSB) dengan *Vigenere cipher* untuk pengaman pesan teks pada aplikasi desktop. Hasil yang didapatkan dari penelitian tersebut menunjukkan bahwa *stego image* yang dihasilkan sulit dibedakan dengan mata telanjang dan teknik LSB dinilai baik untuk menyisipkan pesan ke dalam citra (Yanti & Budayawan, 2023)

Selain itu, penelitian yang dilakukan oleh Pradhipta Ramadhinara H., M. Khoirul Anam, dan Danna Saputra (2015) menggunakan teknik steganografi LSB untuk menyisipkan pesan ke dalam citra dengan tambahan algoritma enkripsi *Serpent* pada data teks untuk meningkatkan keamanan data. Implementasi ini dilakukan pada aplikasi desktop dengan menggunakan bahasa pemrograman *Java,* hasil yang di dapat menunjukkan bahwa penggunaan steganografi LSB dan algoritma enkripsi *Serpent* efektif dalam menyembunyikan pesan dan melindungi data dari pihak ketiga yang tidak bertanggung jawab Ramadhinara dkk. (2015)

Penelitian lainnya yang dilakukan oleh Bayu Rizki R., R. Rumani M., dan Muhammad Nasrun (2015) membandingkan algoritma kriptografi *Serpent* dan AES untuk enkripsi pesan teks SMS di perangkat Android. Hasil penelitiannya menunjukkan bahwa algoritma AES lebih efisien dibandingkan *Serpent* dalam hal waktu saat proses dekripsi, lalu *Serpent* menunjukkan hasil *avalanche effect* yang lebih baik, *avalanche effect* merupakan perubahan signifikan pada *output* saat ada perubahan kecil pada *input* (Rizki dkk., 2015).

Dalam penelitian ini penulis menggunakan algoritma kriptografi *Serpent* dan steganografi *Least Significant Bit* (LSB). Algoritma enkripsi kriptografi *Serpent* merupakan algoritma *cipher* blok, *cipher* blok beroperasi dalam bentuk rangkaian bit yang dibagi-bagi menjadi blok-blok dengan Panjang bitnya sudah ditentukan sebelumnya (Putri, 2010). Algoritma enkripsi *Serpent* di desain dengan dua kali lebih banyak putaran sebagai asuransi analisis penemuan masa depan dalam kriptografi (Izevbizua, 2015). Walaupun algoritma enkripsi *Serpent* sudah sangat kuat dan sulit untuk di dekripsi, jika pihak-pihak tidak bertanggung jawab

menemukan pesan *ciphertext* hasil enkripsi tetap saja akan menimbulkan kecurigaan sehingga mendorongnya aksi peretasan oleh pihak-pihak tidak bertanggung jawab. Maka dari itu, dilakukan tahap steganografi agar tidak menimbulkan kecurigaan dan pihak tidak bertanggung jawab tidak akan mengetahui bahwa ada pesan rahasia yang dikirim. Metode steganografi yang digunakan dalam penelitian ini yaitu metode *Least Significant Bit* (LSB). LSB melakukan perubahan pada bit terakhir dari setiap piksel atau bit yang paling tidak signifikan dengan bit dari data teks yang akan di sembunyikan pada gambar. LSB digunakan dikarenakan dengan menggunakan metode LSB jika informasi yang disembunyikan pada gambar sedikit maupun banyak tidak akan mempengaruhi segi kualitas gambar, sehingga tidak terlihat perubahan kualitas secara kasat mata (Lutfi & Rosihan, 2018). Diharapkan implementasi penggabungan metode enkripsi *Serpent* dan steganografi LSB dapat meningkatkan keamanan pesan.

Keunikan dari penelitian ini terletak pada pengembangan aplikasi Android yang menggabungkan metode kriptografi *Serpent* dan steganografi LSB untuk pengamanan data teks. Berbeda dengan penelitian sebelumnya yang berfokus pada aplikasi desktop, penelitian ini juga melakukan pengujian *robustness* yang mendalam menggunakan MSE, PSNR, Korelasi Pearson, dan pengujian kasat mata. Dengan demikian, penelitian ini memberikan kontribusi baru dalam konteks pengamanan data teks pada platform *mobile*, serta memberikan metode pengujian yang lebih komprehensif untuk memastikan keamanan dan efektivitas solusi yang diusulkan.

1.2 Rumusan Masalah Penelitian

Berdasarkan paparan latar belakang sebelumnya, peneliti merumuskan beberapa rumusan masalah yaitu:

1. Berapa besar *robustness* keamanan data teks dengan menggunakan algoritma kriptografi *Serpent*?
2. Bagaimana steganografi LSB dapat diintegrasikan untuk mengamankan data teks yang telah dienkripsi dengan algoritma kriptografi *Serpent*?
3. Bagaimana merancang aplikasi Android yang mengimplementasikan algoritma enkripsi *Serpent* dan teknik steganografi LSB guna meningkatkan keamanan data teks?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah penelitian sebelumnya, maka tujuan dari penelitian ini yaitu:

1. Mengetahui seberapa besar *robustness* dalam keamanan data yang dihasilkan dari implementasi algoritma kriptografi *Serpent*.
2. Mengetahui bagaimana metode steganografi LSB dapat digunakan dalam algoritma ini untuk meningkatkan keamanan data teks yang telah dienkripsi dengan algoritma kriptografi *Serpent*.
3. Mengetahui bagaimana merancang aplikasi Android yang mengimplementasikan algoritma enkripsi *Serpent* dan teknik steganografi LSB guna meningkatkan keamanan data teks.

1.4 Batasan Penelitian

Berdasarkan tujuan penelitian di atas, maka batasan masalah dari penelitian ini yaitu:

1. Aplikasi yang dikembangkan khusus untuk platform Android.
2. Aplikasi tidak terkoneksi ke internet dan tidak menggunakan *database*, sehingga semua proses enkripsi, dekripsi, *embedding* data, dan ekstrak data teks dilakukan secara lokal.
3. Media yang diamankan difokuskan pada data teks.
4. Hanya format gambar PNG dan JPEG yang digunakan dalam penelitian ini
5. Metode yang digunakan dalam penelitian ini adalah kriptografi dengan algoritma *Serpent* dan steganografi dengan menggunakan teknik *Least Significant Bit* (LSB).
6. Jumlah karakter yang akan disisipkan tidak bisa melebihi batas maksimum karakter yang dapat ditampung oleh gambar.

1.5 Manfaat Penelitian

Berdasarkan tujuan Penelitian yang telah dipaparkan sebelumnya, Penelitian ini diharapkan bermanfaat bagi perkembangan teknologi terutama dalam bidang *cybersecurity* dan keamanan data.

1.5.1. Manfaat Teoritis

1. Penelitian ini diharapkan memberikan referensi baru teruntuk Penelitian selanjutnya dengan tema atau topik penelitian yang sama dengan harapan penelitian ini dapat dikaji lebih baik lagi selanjutnya.
2. Penelitian ini diharapkan memberikan inovasi baru yaitu menggabungkan dua metode keamanan data yaitu kriptografi *Serpent* dan steganografi LSB dengan *robustness* yang lebih tinggi dibanding dengan menggunakan satu metode saja.

1.5.2. Manfaat Praktis

1. Bagi pengguna, aplikasi ini bermanfaat jika pengguna ingin memberikan informasi pesan yang bersifat rahasia, pesan yang terkirim akan di enkripsi lalu di bungkus dengan gambar sehingga terlihat sebagai gambar biasa saja.
2. Bagi peneliti, dapat menerapkan semua pengetahuan yang diperoleh selama studi perkuliahan dan juga pengetahuan yang didapatkan selama mengikuti program MSIB, juga dapat berkontribusi dalam pengembangan kriptografi.

1.6 Struktur Organisasi Skripsi

Berdasarkan pada Peraturan Rektor UPI (Universitas Pendidikan Indonesia) Nomor.7867/UN40/HK/2021 tentang Pedoman penulisan Karya Ilmiah Universitas Pendidikan Indonesia Tahun Akademik 2021. Sistematika penulisan karya ilmiah ini terdiri atas 5 bagian, yaitu pendahuluan, kajian pustaka, metode penelitian, temuan dan pembahasan, serta simpulan, implikasi, dan rekomendasi. Adapun detail setiap bagiannya sebagai berikut:

1. **PENDAHULUAN**

   Pada bab ini penulis membahas latar belakang penelitian, mengidentifikasi permasalahan yang akan diselesaikan, merincikan tujuan, menentukan batasan pada penelitian yang dilakukan serta manfaat penelitian dari penelitian yang dilakukan. Selain itu struktur organisasi dijelaskan agar memberikan gambaran terhadap arah penulisan.

2. **KAJIAN PUSTAKA**

Pada bab ini, penulis membahas mengenai kajian teoritis dari penelitian, Fokus utama dari bab ini adalah pemahaman mengenai algoritma kriptografi *Serpent*, teknik steganografi *Least Significant Bit* (LSB), dan platform Android sebagai platform utama pengembangan aplikasi. Selain itu kerangka pemikiran dan hipotesis penelitian akan dirincikan pada bab ini, yang akan memberikan landasan kokoh untuk penelitian yang dilakukan.

3. METODE PENELITIAN

Pada bab ini, penulis membahas mengenai metode penelitian yang digunakan dalam penelitian ini serta objek penelitian. Pendekatan yang digunakan adalah *Design and Development* (D&D) yang memberikan kerangka kerja sistematis dan berulang untuk pengembangan dan evaluasi solusi desain. Penelitian ini mencakup enam tahapan utama yang disesuaikan dengan metodologi D&D: Analisis, Perancangan Sistem, Pengembangan, Pengujian, Evaluasi, dan Pelaporan. Setiap tahapan dirincikan dengan kegiatan spesifik, teknik pengumpulan data, dan teknik analisis data yang digunakan untuk mencapai tujuan penelitian.

4. TEMUAN DAN PEMBAHASAN

Pada bab ini membahas hasil temuan dari penelitian, mencakup presentasi data, analisis mendalam, dan interpretasi hasil. Pembahasan melibatkan perbandingan dengan literatur terkait, analisis implikasi hasil, serta pengidentifikasian kelemahan penelitian.

5. SIMPULAN, IMPLIKASI, DAN REKOMENDASI

Pada bab ini, penulis membahas penutup laporan. Simpulan memberikan ringkasan temuan penting dan jawaban terhadap pertanyaan penelitian, menyoroti keefektifan dan efisiensi metode yang digunakan dalam penelitian ini. Implikasi membahas dampak temuan terhadap teori keamanan data dan praktik pengembangan aplikasi pengamanan data teks. Rekomendasi diberikan untuk penelitian selanjutnya dan penerapan hasil temuan dalam konteks praktis, termasuk saran untuk pengembangan lebih lanjut dari metode gabungan kriptografi *Serpent* dan steganografi LSB dalam aplikasi nyata.