BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era digital sekarang ini yang terus berkembang, pengiriman pesan rahasia telah menjadi bagian integral dari komunikasi sehari-hari. Namun, kekhawatiran terkait keamanan semakin meningkat seiring dengan rentangnya sistem pengiriman pesan saat ini terhadap pencurian data. Hal ini juga dijelaskan pada penelitian yang dilakukan oleh Gurning (2020) mengatakan pengiriman pesan sekarang ini rentang terhadap pencurian data karena tingkat keamanan yang rendah dan datanya muda dipecahkan. Tingkat keamanan yang rendah dan kerentanannya ini yang menciptakan celah memungkinkan pihak yang tidak berwenang untuk mengakses dan mencuri informasi yang seharusnya bersifat rahasia.

Dalam hal ini perlu adanya inovasi dan peningkatan pada sistem keamanan data. Solusi-solusi baru yang menggabungkan enkripsi tingkat tinggi, otentikasi ganda, dan teknologi keamanan terbaru menjadi krusial untuk menjaga kerahasian pesan sepanjang perjalanan pengiriman. Dengan meningkatkan keamanan pengirim pesan rahasia membuat berkomunikasi tanpa khawatir terhadap potensi ancaman keamanan yang dapat mengakibatkan pencurian data dan pelanggaran privasi yang merugikan. Menurut Arif dan Nurokhman (2023) tentang meningkatkan keamanan informasi, sistem keamanan data perlu diperhatikan dan harus dijaga kerahasiaannya agar pesan yang ingin dikirim ke penerima dapat dirahasiakan dengan menerapkan ilmu yang mempelajari privasi data atau informasi yaitu kriptografi.

Dengan penerapan kriptografi dapat digunakan untuk menjaga keamanan pesan yang dikirim dari suatu tempat ke tempat yang lain, pesan asli yang dikirim dengan teknik kriptografi (*plaintext*) sudah diubah atau dienkripsi dengan suatu kunci menjadi suatu informasi acak yang tidak bermakna (*ciphertext*). Kunci hanya diketahui oleh pengirim dan penerima, dari kunci ini penerima dapat mengubah text terenkripsi (*ciphertext*) kembali ke bentuk aslinya (*plaintext*). Dengan cara ini individu yang tidak memiliki otoritas untuk mengakses pesan tersebut tidak dapat

mengetahui isi pesan sebenarnya, melainkan hanya melihat rangkaian teks acak (Putri dkk,. 2021). Namun karena sifatnya yang bersifat acak, muncul kekhawatiran terkait pesan yang dikirim yang dapat menimbulkan kecurigaan. Dikarenakan pesan tersebut terlihat tanpa makna yang jelas dapat terjadi kemungkinan pihak luar melakukan sabotase dengan maksud agar penerima tidak dapat memperoleh pesan secara lengkap. Untuk mengatasi tantangan ini, dapat diterapkan pendekatan lain yaitu Steganografi yang menjadi lebih efektif dalam mengurangi kecurigaan karena pesan yang terenkripsi akan disisipkan atau disembunyikan ke dalam citra.

Penerapan steganografi pada masa kini umumnya memanfaatkan media digital, khususnya citra digital sebagai wadah untuk menyembunyikan pesan. Proses utamanya adalah menyisipkan informasi ke dalam sebuah gambar (*cover image*) dengan tujuan agar pihak lain tidak sadar adanya daa tersembunyi tersebut. Selanjutnya steganografi membuat citra stego (*stegno image*) yang memiliki penampilan yang serupa dengan bentuk aslinya. Penampilan serupa ini yang memungkinkan mata seseorang tidak dapat membedakan gambar asli yang tidak memiliki pesan didalamnya dengan gambar stego yang memiliki pesan didalamnya (Widyawati, 2019).

Pada penelitian sebelumnya pernah dilakukan oleh Budiman (2023) mengatakan bahwa menggunakan kriptografi saja tidak cukup untuk melindungi pesan, perlu adanya kombinasi salah satunya metode untuk menggabungkan kriptografi adalah steganografi. Penelitian ini juga menjelaskan steganografi memiliki keterkaitan dengan kriptografi, karena tujuannya adalah menyembunyikan pesan rahasia melalui suatu media. Algoritma steganografi yang biasa digunakan adalah *Least Significant Bit* (LSB). Metode *Least Significant Bit* (LSB) merupakan metode yang sederhana karena hanya mengubah nilai bit terakhir dalam sebuah pesan dengan bit pesan yang disisipkan. Penggunaan algoritma *Least Significant Bit* (LSB) dalam enkripsi memberikan keamanan tanpa menimbulkan kecurigaan, karena LSB mampu menyimpan informasi tanpa mengubah ukuran atau kontennya (Ratama dan Munawaroh, 2022). Meskipun metode LSB dikenal sederhana dan muda, namun metode ini menjadi rentan terhadap potensi serangan jika tidak dikombinasikan dengan algoritma lainnya. Pada penelitian yang

dilakukan oleh Megantara (2019) pengujian telah dilakukan dengan menggunakan kombinasi algoritma *Hill Cipher* untuk melakukan enkripsi pada pesan dan algoritma LSB untuk menyembunyikan pesan ke dalam citra. Hasil dari uji coba penelitian ini meningkatkan keamanan dengan tetap mempertahankan kualitas citra yang baik.

Syahputra, dkk (2021) juga melakukan penelitian dengan kombinasi algoritma *Atbash Cipher* dan Algoritma Transposisi Segitiga dalam skema super enkripsi. Dengan teknik kombinasi antara dua algoritma kriptografi ini mendapatkan *ciphertext* yang lebih kuat dan sulit untuk dipecahkan, selain itu juga untuk mengatasi kelemahan penggunaan *ciphertext* tunggal yang cenderung lemah. Untuk menggabungkan kedua algoritma kriptografi ini yaitu dengan cara mengenkripsi pesan menggunakan *Atbash Cipher* terlebih dahulu, menghasilkan pesan terenkripsi yang disebut *ciphertext*. Selanjutnya, pesan tersebut dienkripsi kembali menggunakan teknik Transposisi Segitiga. Proses dekripsi *ciphertext* melibatkan langkah awal dekripsi dengan teknik Transposisi Segitiga, diikuti dengan dekripsi menggunakan algoritma *Atbash Cipher*. Dengan demikian, *ciphertext* dapat dikembalikan ke bentuk file aslinya.

Dari latar belakang permasalahan diatas, peneliti mencoba melakukan penelitian untuk menutupi kelemahan penggunaan *ciphertext* tunggal dengan menggunakan teknik kombinasi *Atbash Cipher* dan *Hill Cipher* sebagai super enkripsi. *Atbash Cipher* memiliki kelebihan yaitu menyajikan enkripsi yang sederhana dan cepat, tidak memakan banyak sumber daya. Namun, *Atbash* memiliki kelemahan, terutama dalam menyandikan huruf "A" yang selalu diubah menjadi "Z" dan sebaliknya. Kelemahan ini dapat dimanfaatkan oleh penyerang yang mudah menyadari pola ini. Dengan mengabungkan algoritma *Hill Cipher* dapat menutupi kelemahan dari *Atbash Cipher*, memberikan lapisan keamanan tambahan dan kompleksitas. Penggunaan matriks kunci memberikan variasi lebih besar dalam mengenkripsi pesan dan dapat memyembunyikan pola-pola sederhana pada *Atbash Cipher*. Kombinasi ini dapat diperkuat dengan menerapkan LSB untuk menyembunyikan atau menyisipkan pesan ke dalam citra tanpa mengubah tampilan visualnya. Dengan demikian kombinasi ini menciptakan perlindungan pesan

rahasia yang lebih kuat dari serangan dengan memanfaatkan keunggulan masing-masing algoritma.

1.2 Rumusan Masalah

Berdasarkan latar belakang sebelumnya, maka disimpulkan rumusan masalah yang harus diselesaikan pada penelitian ini yaitu bagaimana efektifitas penggabungan Kriptografi (*Atbash Cipher* dan *Hill Cipher*) dengan Steganografi (LSB) dalam meyembunyikan pesan?

1.3 Batasan Masalah

Adapun batasan masalah ini dalam penelitian ini untuk membuat penelitian ini tidak keluar dan tidak menyimpang dari yang diteliti, serta dari faktor keterbatasan yang dimiliki terutama dalam hal pengetahuan, biaya, waktu dan sebagainya. Maka penulis membatasi masalah sebagai berikut:

1. Data yang digunakan pada proses mensyisipkan pesan ke steganografi *Least-Significant Bit* (LSB) adalah citra warna "*color image*" berformat (*.jpg), (*.jpeg), dan (*.png) dengan ukuran file yang berbeda-beda, maksimal ukuran citra 2Mb.
2. Pesan yang akan disisipkan hanya berupa tipe data "*string*" dengan panjang karakter maksimal 250 kata dan menggunakan format kalimat UTF-8.
3. Penyisipan pesan pada citra menggunakan Algorititma *Atbash Cipher* dan *Hill Cipher* menggunakan bahasa pemograman Python.
4. Kunci Matrik *Hill Cipher* yang digunakan adalah Kunci Matrik 3 x 3.

1.4 Tujuan Penelitian

Seiring dengan latar belakang dan rumusan masalah di atas, penelitian ini bertujuan untuk menjadikan Steganografi sebagai pengiriman pesan rahasia yang aman dengan mengimplementasi kombinasi *Atbash Cipher* dengan *Hill Cipher* sebagai super enkripsi dengan *Least Significant Bit* (LSB) pada citra.

1.5 Manfaat Penelitian

Adapun manfaat penelitian ini dengan mengkombinasikan *Atbash Cipher*, *Hill Cipher*, dan Steganografi LSB pada citra, diharapkan dapat meningkatkan tingkat keamanan dalam pengiriman pesan rahasia dan memberikan perlindungan lebih baik terhadap potensi ancaman keamanan dan pencurian data. Menambah wawasan bidang keamanan informasi dengan menggabungkan dua metode kriptografi (*Atbash Cipher* dan *Hill Cipher*) sebagai super enkripsi dan steganografi LSB dalam konteks penyisipan pesan ke dalam citra, serta sebagai solusi bagi pihak pihak yang menggunakan teknologi informasi dan komunikasi untuk dapat melakukan pengiriman pesan dengan aman.

1.6 Sistematika Penulisan

Penulisan skripsi penelitian ini diatur dengan suatu format yang terstruktur dan sistematis. Struktur penulisan yang digunakan untuk skripsi penelitian ini adalah sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini menjelaskan tentang latar belakang, perumusan masalah, Batasan masalah, tujuan dari penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II KAJIAN LITERATUR

Pada bab ini menjelaskan penelitian-penelitian sebelumnya, kosep dan teori yang telah digunakan dalam studi kasus dan metode yang sama.

BAB III METODOLOGI PENELITIAN

Pada bab ini menjelaskan tentang kerangka penelitian, waktu dan alat yang digunakan saat mengumpulkan data, perangkat yang digunakan untuk melakuakn penelitian, serta analisis, perancangan dan implementasi.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini menjelaskan tentang proses pengujian dam pembahasan terkait hasil yang didapatkan dari penelitian yang dilakukan.

BAB V PENUTUP

Pada bab ini menjelaskan tentang kesimpulan dan saran dari hasil penelitian.

DAFTAR PUSTAKA

Pada bab ini berisi referensi yang digunakan sebagai landasan dan sumber data sekunder dalam penyusunan kajian literatur pada penelitian ini.