BAB 1. PENDAHULUAN

1.1. Latar belakang

Perkembangan teknologi yang begitu pesat mempengaruhi gaya hidup manusia terutama dalam berkomunikasi. Saat ini komunikasi tidak hanya bisa dilakukan secara langsung melainkan dapat dilakukan dengan cara daring dengan memanfaatkan internet. Jumlah pengguna internet di Indonesia mengalami peningkatan selama kurun waktu 2016 sampai 2020. Menurut Badan Pusat Statistik (2016) persentase penduduk yang menggunakan internet sekitar 25,37 persen dan mengalami peningkatan menjadi 53,73 persen pada tahun 2020. Berdasarkan angka tersebut menunjukkan pertukaran informasi melalui internet terus mengalami peningkatan. Mudahnya pertukaran informasi melalui internet tersebut membawa dampak positif karena dapat memudahkan manusia untuk bertukar informasi secara cepat. Namun disisi lain komunikasi secara daring juga membawa dampak negatif karena dengan berkembangya teknologi maka berkembang pula kejahatan dunia maya dan pengiriman pesan atau informasi semakin rentan terhadap penyadapan.

Pada beberapa kondisi pesan atau informasi yang akan dikirimkan bersifat rahasia, misalnya pin ATM, kata sandi dan lain sebagainya sehingga hanya pihak pengirim dan penerima yang boleh mengetahuinya. Oleh karena itu keamanan informasi perlu dijaga untuk menghindari pencurian dan penyalahgunaan data oleh pihak yang tidak bertanggung jawab. Untuk mengatasi situasi tersebut diperlukan suatu aplikasi yang dapat mengamankan pesan dengan mengacaknya menjadi karakter yang sulit dimengerti kemudian menyembunyikan pesan tersebut kedalam media yang dapat diakses oleh setiap orang. Teknik yang dapat digunakan untuk mengacak dan menyembunyikan pesan kedalam media lain yaitu kriptografi dan steganografi.

Kriptografi adalah cara untuk mengacak pesan atau informasi menjadi karakter acak yang tidak dapat dipahami artinya. Algoritma *Rivest Shamir Adleman* atau dikenal dengan RSA adalah salah satu jenis kriptografi asimetris yang dipublikasikan oleh Len Adleman, Ron Rivest dan Adi Shamir pada tahun 1978.

Enkripsi ini memanfaatkan sepasang kunci yaitu kunci public dan kuncin privat untuk mengamankan pesan. Namun teknik ini dapat menimbulkan kecurigaan dan membuat pihak luar melakukan serangan untuk mengetahui isi dari pesan. Oleh karena itu dibutuhkan teknik lain yang dapat menyembunyikan pesan terenkripsi agar tidak menimbulkan kecurigaan pihak ketiga. Teknik tersebut adalah steganografi.

Steganografi adalah ilmu dan seni menyembunyikan informasi dalam bagian informasi lainnya (Bhargava dan Mukhija, 2019). Dalam melakukan steganografi metode *Least Significant Bit* (LSB) merupakan metode yang paling banyak digunakan. Berdasarkan media penampung atau *cover object*, citra digital merupakan media yang paling sering digunakan karena manusia sering menggunakan citra untuk berbagi informasi selain itu ukuran citra relatif lebih kecil dibanding audio dan video. Metode LSB menyembunyikan pesan dalam bit terendah yang tidak berpengaruh dalam penyusunan warna di setiap pixel pada citra digital.

Penelitian tentang keamanan pesan informasi dengan menggabungkan metode kriptografi dan steganografi sebelumnya pernah dilakukan pada tahun 2018 dengan judul penelitian "Teknik Penyembunyian dan Enkripsi Pesan pada Citra Digital dengan Kombinasi Metode LSB dan RSA". Hasil dari penelitian tersebut menunjukkan adanya peningkatan keamanan dan kualitas gambar terjaga dilihat dari nilai MSE 0.1232dB dan PSNR 57.2258dB (Handoyo et al., 2018).

Pada tahun 2019 juga terdapat penelitian dengan judul "Hide Image And Text Using Lsb, Dwt And Rsa Based On Image Steganography". Penelitian tersebut menghasilkan kesimpulan bahwa penggabungan metode LSB, DWT dan RSA dengan media penampung citra *grayscale* dapat meningkatkan keamanan data dengan nilai PSNR sebesar 71.2145dB (Bhargava & Mukhija, 2019).

Selain penelitian diatas tahun 2021 juga dilakukan penelitian pengamanan data dengan judul "Implementasi Steganografi Image Processing Dan Enkripsi Aes Menggunakan Openstego". Pada penelitian tersebut menggabungkan staganografi LSB dan kriptografi simetris AES dengan media penampung pesan citra digital

berwarna. Hasil dari penelitian tersebut yaitu semakin besar ukuran gambar semakin baik nilai PSNR untuk ukuran pesan yang sama (Laksmiati, 2021).

Berdasarkan latar belakang diatas maka dapat disimpulkan bahwa pembuatan sistem pengamanan pesan masih bisa dikembangkan dengan membangun sistem berbasis website agar lebih mudah digunakan dan pada media penampung pesan menggunakan citra digital berwarna yang umum digunakan. Maka peneliti mengusulkan pengembangan penelitian dengan menggabungkan algoritma steganografi LSB (*Least Significant Bit*) dan algoritma kriptografi RSA (*Rivest Shamir Adleman*). Penelitian ini akan diberi judul "Keamanan pesan teks menggunakan teknik steganografi dan kriptografi pada citra digital berwarna dengan metode *Least Significant Bit* dan *Rivest Shamir Adleman*".

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan diatas maka yang menjadi perumusan masalah dalam penelitian ini adalah:

1. Bagaimana implementasi algoritma steganografi *Least Significant Bit* (LSB) dan kriptografi *Rivest Shamir Adleman* (RSA) dalam mengamankan informasi melalui media citra digital?
2. Bagaimana perbedaan kualitas gambar penampung pesan sebelum dan sesudah dilakukan steganografi LSB berdasarkan nilai PSNR dan MSE?
3. Bagaimana perbedaan *stego image* sebelum dan sesudah dikirim melalui whatsapp dan telegram?

1.3. Batasan Masalah

Batasan masalah pada penelitian ini yaitu :

1. Aplikasi yang dibagun merupakan aplikasi berbasis website menggunakan bahasa pemrograman PHP.
2. Untuk mengetahui perbedaan kualitas citra digital berwarna sebelum dan sesudah disisipkan pesan teks berdasarkan nilai MSE dan PSNR.
3. Citra digital yang digunakan adalah citra berwarna dengan format PNG dan BMP.
4. Pesan rahasia yang disisipkan berupa teks.

5. Aplikasi untuk melakukan uji coba pengiriman yaitu whatsapp dan telegram.

1.4. Tujuan

Berdasarkan rumusan masalah yang telah dijelaskan, maka tujuan dari penelitian ini adalah:

1. Mengimplementasikan metode LSB dan RSA dalam membangun sistem pengamanan informasi berupa teks dengan melakukan enkripsi dan disimpan pada media lain berupa citra digital.
2. Mengetahui perbedaan kualitas gambar sebelum dan sesudah dilakukan steganografi LSB.
3. Untuk mengetahui perbedaan *stego image* sebelum dan sesudah dilakukan uji coba pengiriman melalui aplikasi whatsapp dan telegram.

1.5. Manfaat

Manfaat yang diharapkan dari penelitian implementasi Keamanan pesan teks menggunakan teknik steganografi dan kriptografi pada citra digital berwarna dengan metode LSB dan RSA bagi pengguna adalah menghasilkan aplikasi yang dapat mengamankan informasi rahasia berupa teks kedalam media gambar sehingga tidak menimbulkan kecurigaan kepada pihak ketiga. Selain itu, manfaat bagi penulis yaitu mengetahui pengaruh dari teknik steganografi dan kriptografi terhadap kualitas gambar penampung informasi rahasia dengan mengimplementasikan metode dan teori yang telah dipelajari.