BAB I

PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi informasi saat ini telah menjadi bagian penting dalam kehidupan masyarakat modern. Salah satu inovasi yang paling berpengaruh adalah internet, yang memungkinkan penyebaran dan pertukaran informasi secara cepat dan luas (Ali Fitriani, 2020). Namun, kemudahan akses internet juga menimbulkan tantangan baru, khususnya dalam hal keamanan dan privasi data. Informasi yang dikirimkan melalui jaringan internet berisiko disadap atau dicuri oleh pihak-pihak yang tidak bertanggung jawab (Darwis & Pasaribu Octaviansyah, 2020). Oleh karena itu, pengamanan data menjadi kebutuhan penting bagi individu, perusahaan, maupun organisasi untuk melindungi informasi sensitif dari ancaman pihak ketiga (Wijayanti & Romadlon, 2022).

Salah satu metode pengamanan data adalah steganografi, yaitu teknik menyembunyikan pesan di dalam media lain seperti citra, audio, atau video, sehingga keberadaan pesan tersebut tidak mudah terdeteksi. Meskipun steganografi efektif dalam menyembunyikan keberadaan informasi, metode ini memiliki kelemahan, terutama terhadap serangan steganalisis. Steganalisis adalah teknik analisis statistik atau algoritmik yang mampu mendeteksi adanya data tersembunyi di dalam suatu media (Munir, 2019). Oleh karena itu, penggunaan steganografi saja belum cukup untuk menjamin keamanan data secara menyeluruh.

Untuk mengatasi kelemahan tersebut, steganografi perlu dikombinasikan dengan metode kriptografi. Kriptografi berperan untuk mengenkripsi isi pesan sebelum disisipkan ke dalam media steganografi. Dengan demikian, meskipun pesan tersembunyi berhasil ditemukan, isi pesan tetap tidak dapat dibaca tanpa kunci dekripsi yang sesuai (Alanzy et al., 2023). Kombinasi antara steganografi dan kriptografi dapat meningkatkan keamanan komunikasi digital, karena menggabungkan penyembunyian keberadaan pesan dan pengacakan isi pesan.

Penelitian yang dilakukan oleh (Jacinto et al., 2022) mengusulkan metode pengaman file yang menggabungkan steganografi LSB dan kriptografi AES mode CBC. Metode yang diajukan melibatkan enkripsi pesan teks menggunakan algoritma AES-CBC, kemudian menyisipkannya ke dalam citra pembawa format BMP menggunakan teknik LSB yang telah ditingkatkan dengan pemilihan area kontras rendah berdasarkan analisis statistik citra. Area kontras rendah ini dipilih karena cenderung sulit dideteksi oleh mata manusia dan teknik steganalisis. Hasil implementasi menunjukkan bahwa pendekatan ini menciptakan tiga lapisan keamanan, menjadikan informasi sulit untuk diakses tanpa pengetahuan tentang kunci enkripsi serta parameter statistik yang digunakan untuk menyisipkan pesan. Meskipun demikian, apabila kunci AES didapatkan oleh pihak lain maka data dapat didekripsi dengan mudah dikarenakan algoritma AES menggunakan kunci yang sama dalam proses enkripsi dan dekripsi, dan mode AES-CBC juga tidak aman terhadap serangan manipulasi *ciphertext* karena tidak memiliki mekanisme autentikasi bawaan.

Penelitian lainnya yang dilakukan oleh (Ali Fitriani, 2020), menggabungkan kriptografi RSA dengan steganografi LSB. Pada penelitian yang dilakukan oleh Ali Fitriani, pesan rahasia dienkripsi menggunakan algoritma RSA (dengan kunci publik), kemudian menanamkan *ciphertext* RSA ke dalam citra menggunakan steganografi LSB. RSA memberikan keamanan kriptografi yang sangat kuat karena tanpa kunci privat, dekripsi sangat sulit dilakukan. Namun demikian, RSA secara komputasi tidak dirancang untuk mengenkripsi data berukuran besar. Akibatnya, pendekatan ini kurang efisien jika pesan yang disembunyikan berkapasitas besar, karena pesan harus dipecah menjadi potongan kecil yang dienkripsi satu per satu. Dengan kata lain, gabungan RSA dan LSB cocok untuk pesan pendek tetapi tidak optimal untuk data yang besar.

Berdasarkan hasil penelitian sebelumnya, maka penelitian ini akan mencoba untuk mengombinasikan enkripsi AES dan RSA untuk mengamankan file hasil steganografi LSB. Mode enkripsi AES yang digunakan pada penelitian ini adalah AES-GCM (Galois/Counter Mode). AES-GCM adalah mode operasi AES yang menghasilkan enkripsi terautentikasi, yang menyediakan kerahasiaan sekaligus keutuhan data. Dengan autentikasi bawaan dalam bentuk tag, AES-GCM tahan terhadap modifikasi *ciphertext*. Sementara itu, RSA dengan kunci 4096-bit menyediakan lapisan keamanan asimetris yang sangat kuat untuk pertukaran kunci simetris dan juga tahan akan modifikasi *ciphertext*. Gabungan ini menyatukan kelebihan kriptografi simetris (enkripsi cepat dan efisien) dan asimetris (keamanan kunci publik), sehingga mengatasi celah keamanan sebelumnya.

1.2. Rumusan Masalah

Merujuk pada latar belakang yang telah dipaparkan sebelumnya, maka rumusan masalah pada penelitian ini adalah, bagaimana pengaruh gabungan algoritma enkripsi AES-GCM 256 bit dan RSA 4096 bit dalam meningkatkan keamanan steganografi LSB?

1.3. Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah meningkatkan keamanan Steganografi LSB dengan menggunakan gabungan algoritma kriptografi AES-GCM 256 bit dan RSA 4096 bit.

1.4. Batasan Masalah

Adapun batasan masalah dari penelitian yang akan dilakukan, yaitu:

1. Penelitian ini akan berfokus pada pengamanan pesan teks atau file yang akan disisipkan dalam citra menggunakan gabungan antara teknik enkripsi dan steganografi.
2. Algoritma Enkripsi yang akan digunakan dalam penelitian ini adalah Algoritma AES-GCM 256 bit dan Algoritma RSA 4096 bit.
3. Metode Steganografi yang akan digunakan dalam penelitian ini adalah Metode Steganografi *Least Significant Bit* (LSB)
4. Penggunaan citra dalam penelitian ini terbatas pada format citra digital PNG RGB 24 bit.

1.5. Manfaat Penelitian

Adapun manfaat yang diperoleh dari penelitian yang akan dilakukan, yaitu:

1. Memberikan wawasan tentang penggunaan algoritma AES-GCM 256 bit dan algoritma RSA 4096 bit untuk meningkatkan keamanan steganografi LSB.
2. Menyediakan panduan implementasi terkait teknis penggunaan algoritma AES-GCM 256 bit dan RSA 4096 bit untuk meningkatkan keamanan steganografi LSB.
3. Meningkatkan pemahaman tentang potensi keamanan dan aplikasi praktis teknik ini dalam berbagai konteks, termasuk penyimpanan data sensitif dan aplikasi keamanan informasi lainnya.

Penelitian ini diharapkan akan menjadi kontribusi yang berharga dalam mengatasi tantangan keamanan informasi di era digital yang terus berkembang.

1.6. Sistematika Penulisan

Sistematika penulisan penelitian ini disusun sebagai gambaran umum untuk memudahkan dalam memahami penelitian dilakukan sehingga membantu dalam pembuatan laporan. Secara garis besar, sistematika penulisan pada penelitian ini sebagai berikut:

BAB I PENDAHULUAN

Bab ini menjelaskan mengenai latar belakang, rumusan masalah, tujuan penelitian, Batasan masalah, manfaat penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini menjelaskan teori – teori yang digunakan sebagai suatu landasan penelitian yang digunakan untuk menyelesaikan permasalahan yang dibuat pada penelitian ini, bahasan dalam penelitian tentang algoritma kriptografi dan steganografi beserta metode - metode yang akan digunakan

BAB III METODOLOGI PENELITIAN

Bab ini berisi penjelasan metode yang akan digunakan dalam penelitian serta dalam pada bab ini berisi juga penjelasan mengenai rancangan dan kebutuhan dalam penelitian ini

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi tentang hasil dari implementasi penelitian dan pembuatan sistem yang sudah dilakukan berdasarkan pada perancangan yang di buat pada bab sebelumnya dan bab ini membahas hasil pengujian untuk mengetahui hasil apakah sistem berhasil atau tidak

BAB V KESIMPULAN DAN SARAN

Bab ini akan menjelaskan sebuah kesimpulan dari penelitian yang sudah dilakukan dan akan diberikan juga saran untuk mengetahui kekurangan dalam penelitian sehingga dapat dikembangkan lagi