BAB 1 PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi berperan penting sebagai sarana yang efisien dalam menciptakan serta meluaskan akses informasi, melalui pemanfaatan teknologi komputer dalam konteks bisnis. Oleh karena itu, komputer merupakan hal yang dibutuhkan manusia dan berperan penting dalam berbagai macam manfaat. Salah satunya yaitu, dapat digunakan oleh banyak ahli untuk mengakses komputer bertukar file, kirim *email*, namun komputer tidak hanya sebatas melakukan hal tersebut. Komputer mampu menghasilkan sistem informasi secara global yang mempercepat pertukaran informasi global [1].

Perkembangan teknologi informasi, ditandai dengan 5,4 miliar pengguna internet global pada 2023 telah mempercepat pertukaran informasi [2]. Di Indonesia, transformasi digital juga terasa signifikan, terutama dalam mendukung sektor pemerintahan, kesehatan, dan ekonomi. Namun, di balik kemajuan ini, ancaman keamanan data menjadi tantangan besar yang mengintai, baik bagi individu, organisasi, maupun negara, karena data yang tidak terlindungi dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab.

Kini, ancaman siber semakin kompleks, dengan serangan seperti *phishing*, *ransomware*, dan *data breach* yang merugikan berbagai pihak. Berdasarkan laporan Badan Siber dan Sandi Negara (BSSN), sektor administrasi pemerintahan menjadi target utama serangan siber di Indonesia diikuti oleh sektor keuangan dan energi sepanjang tahun 2023 [3]. KumparanTECH juga menyoroti bahwa serangan siber di Indonesia pada semester pertama 2024 didominasi oleh pelaku dari dalam negeri [4]. Fenomena ini ditunjukkan pada Gambar 1.1, yang menggambarkan bahwa ancaman tidak hanya berasal dari luar, tetapi juga dari dalam negeri sendiri. Ancaman siber juga diperkirakan akan semakin berbahaya kedepannya [5].

Gambar 1. 1 Distribusi Sumber Serangan Siber ke Indonesia pada Semester Pertama 2024 [4].

Salah satu teknik pengamanan data yang sering digunakan adalah kriptografi dan steganografi. Perlindungan dari steganografi bisa lebih kuat dengan menambahkan teknik enkripsi kriptografi sebelum menyembunyikan pesan di dalam gambar [6]. Kriptografi merupakan suatu ilmu yang mempelajari teknik matematika yang berkaitan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Namun tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi [1]. Enkripsi merupakan salah satu solusi atau metode keamanan data terbaik untuk menjaga kerahasiaan dan keandalan data, serta dapat meningkatkan keamanan data atau informasi [7]. Steganografi, di sisi lain, menyembunyikan data dalam media seperti gambar atau audio, sehingga keberadaan data tersebut tidak terdeteksi oleh pihak yang tidak berwenang [8]. Penelitian terdahulu, seperti yang dilakukan oleh Hermawan dan Ujianto, menunjukkan bahwa kombinasi kriptografi dapat meningkatkan efisiensi dan keamanan data [9], sementara Mido dan Ujianto mengungkapkan potensi steganografi dalam menyembunyikan informasi tanpa mengubah kualitas media secara signifikan [6]. Namun, pendekatan sebelumnya sering kali hanya menggunakan salah satu teknik, sehingga keamanan yang dihasilkan belum maksimal.

Untuk mengatasi keterbatasan tersebut, penelitian ini mengusulkan solusi yang menggabungkan kriptografi dan steganografi untuk menciptakan sistem keamanan data yang lebih kuat. Pendekatan ini menggunakan algoritma *Advanced Encryption Standard* (AES), *Rivest Shamir Adleman* (RSA), dan metode *Least Significant Bit* (LSB). AES adalah algoritma kriptografi simetris yang menggunakan kunci dengan panjang tertentu dalam penelitian ini 256-bit untuk mengenkripsi data dalam blok berukuran 128-bit, dikenal karena kecepatan dan ketahanannya terhadap serangan seperti *brute force* [10]. Algoritma dalam penelitian ini bekerja dengan mode operasi *Cipher Block Chaining* (CBC), di mana setiap blok data dienkripsi dengan menggabungkannya dengan blok sebelumnya, meningkatkan keacakan hasil enkripsi. RSA adalah algoritma kriptografi asimetris yang memanfaatkan pasangan kunci publik dan privat dalam penelitian ini menggunakan kunci 2048-bit untuk mengamankan distribusi kunci dan memastikan hanya pihak yang berwenang yang dapat mengakses data [11]. RSA bekerja dengan memanfaatkan prinsip matematika bilangan prima besar, di mana kunci publik digunakan untuk enkripsi dan kunci privat untuk dekripsi, memberikan keamanan tambahan dalam pengiriman kunci. Sementara itu, metode LSB menyisipkan data ke dalam bit paling tidak signifikan dari piksel gambar berwarna RGB, memungkinkan penyembunyian informasi tanpa mengubah tampilan visual gambar secara nyata, karena perubahan pada bit tersebut hanya menghasilkan perbedaan warna yang sangat kecil misalnya, dari nilai 255 menjadi 254 pada saluran warna [6]. Pendekatan ini dipilih karena memberikan keamanan berlapis. Enkripsi AES-256 dan RSA-2048 memastikan data tidak dapat dibaca tanpa kunci, dan steganografi menyembunyikan keberadaan data tersebut, menjadikannya solusi yang lebih aman dibandingkan metode yang hanya menggunakan salah satu teknik.

Metode LSB dipilih untuk steganografi dalam penelitian ini karena kelebihannya dalam proses penyisipan dan ekstraksi yang cepat serta nilai MSE kecil dan PSNR besar, yang mendukung efisiensi dan ketahanan kualitas citra [8]. Berdasarkan analisis penelitian, LSB menawarkan penyisipan data dengan

perubahan minimal pada citra, menjaga resolusi dan ukuran citra tetap sama sebelum serta sesudah penyisipan, yang selaras dengan efisiensi AES. Dibandingkan dengan Discrete Wavelet Transform (DWT), yang membutuhkan waktu lama dalam pemrosesan dan kualitas citra dipengaruhi oleh jumlah karakter pesan, LSB menyediakan keunggulan dalam kecepatan dan konsistensi resolusi. Selain itu, dibandingkan dengan Bit Plane Complexity Segmentation (BPCS), yang memiliki waktu penyisipan lambat dan menyebabkan perubahan ukuran file citra, LSB menawarkan kecepatan lebih baik dan ukuran file yang stabil, mendukung ketahanan visual. Meskipun LSB memiliki kelemahan seperti tingkat ketahanan pesan yang buruk terhadap perubahan kontras dan kerentanan terhadap serangan pemrosesan gambar, metode ini tetap dipilih karena kelebihannya dapat ditingkatkan dengan pengembangan Enhanced LSB untuk meningkatkan ketahanan terhadap analisis keamanan [8].

Sistem yang diusulkan melibatkan proses di mana pesan rahasia dalam format teks (*.txt) dienkripsi menggunakan AES-256 dalam mode CBC, kemudian kunci AES dienkripsi dengan RSA-2048 menggunakan kunci publik. Data terenkripsi ini disembunyikan dalam gambar berwarna RGB (*.png) menggunakan metode LSB, menghasilkan gambar stego yang tampak identik dengan gambar asli. Untuk mendekripsi, data diekstrak dari gambar, kunci AES didekripsi dengan kunci privat RSA, dan pesan asli diperoleh kembali menggunakan kunci AES. Pemilihan format teks (*.txt) sebagai subjek dilakukan karena sederhana untuk diolah dan dienkripsi, sementara format gambar PNG dipilih sebagai objek karena sifatnya yang lossless, memastikan integritas data LSB, berbeda dengan format JPEG yang dapat merusak data akibat kompresi lossy [6], [12]. Sistem ini dievaluasi melalui metrik seperti *Mean Squared Error* (MSE), *Peak Signal to Noise Ratio* (PSNR), waktu eksekusi, penggunaan memori, dan ukuran berkas, untuk memastikan keamanan sekaligus efisiensi.

Berdasarkan permasalahan, latar belakang, serta metode penyelesaian di atas, maka dilakukanlah penelitian dengan judul "**Implementasi Algoritma**

AES-256 Dan RSA Dalam Steganografi Gambar Berwarna Dengan Metode LSB Untuk Meningkatkan Keamanan Data".

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Seberapa efektif algoritma AES-256 dengan mode *Cipher Block Chaining* (CBC) dan algoritma RSA-2048 dalam mengenkripsi kunci AES dalam mengenkripsi data teks untuk mencegah akses tidak sah ?
2. Seberapa baik metode steganografi Least Significant Bit (LSB) dalam menyembunyikan data terenkripsi pada gambar berwarna format PNG tanpa mengubah kualitas visual ?
3. Bagaimana efisiensi sistem kombinasi AES-256, RSA-2048, dan LSB dalam hal waktu eksekusi dan penggunaan memori untuk pengamanan data teks ?

1.3 Pertanyaan Penelitian

Berdasarkan rumusan masalah yang telah diuraikan, pertanyaan penelitian dalam penelitian ini adalah sebagai berikut:

1. Bagaimana mengamankan data teks dari akses tidak sah menggunakan kombinasi algoritma AES-256 dengan mode *Cipher Block Chaining* (CBC) dan algoritma RSA-2048 untuk enkripsi kunci AES?
2. Bagaimana menyembunyikan data terenkripsi pada gambar berwarna (*.png) menggunakan metode steganografi *Least Significant Bit* (LSB) dan mengevaluasi kualitas visualnya melalui *Mean Squared Error* (MSE) dan *Peak Signal-to-Noise Ratio* (PSNR)?
3. Bagaimana mengevaluasi efisiensi sistem kombinasi AES-256, RSA-2048, dan LSB dalam hal waktu eksekusi dan penggunaan memori untuk pengamanan data teks?

1.4 Batasan Masalah

Berdasarkan rumusan masalah dan pertanyaan penelitian, batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Data yang diproses berupa teks (*.txt).
2. Proses enkripsi menggunakan algoritma AES-256 dengan mode *Cipher Block Chaining* (CBC) dan algoritma RSA-2048 untuk enkripsi kunci AES.
3. Media penyisipan data adalah gambar berwarna (*.png).
4. Proses penyisipan data menggunakan metode steganografi *Least Significant Bit* (LSB), dengan evaluasi kualitas visual melalui *Mean Squared Error* (MSE) dan *Peak Signal-to-Noise Ratio* (PSNR), serta efisiensi melalui waktu eksekusi dan penggunaan memori.

1.5 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah diuraikan, penelitian ini bertujuan untuk :

1. Mengimplementasikan kombinasi algoritma AES-256 dengan mode *Cipher Block Chaining* (CBC) dan algoritma RSA-2048 untuk enkripsi kunci AES guna mengamankan data teks dalam format *.txt dari akses tidak sah.
2. Mengimplementasikan metode steganografi *Least Significant Bit* (LSB) untuk menyembunyikan data terenkripsi pada gambar berwarna format *.png, dengan evaluasi kualitas visual melalui *Mean Squared Error* (MSE) dan *Peak Signal-to-Noise Ratio* (PSNR).
3. Mengevaluasi efisiensi sistem kombinasi AES-256, RSA-2048, dan LSB dalam hal waktu eksekusi dan penggunaan memori untuk pengamanan data teks.

1.6 Manfaat Penelitian

Penelitian ini memberikan beberapa manfaat penting, yaitu :

1. Menyediakan solusi keamanan data teks yang efektif melalui kombinasi AES-256 dan RSA-2048, melindungi informasi sensitif dari ancaman siber seperti *phishing* dan *data breach*.
2. Menghasilkan teknik steganografi LSB yang menjaga kualitas visual gambar PNG, mendukung aplikasi multimedia dengan keamanan tinggi.
3. Berkontribusi pada pengembangan ilmu kriptografi dan steganografi.

1.7 Metode Penelitian

Metode penelitian ini menguraikan pendekatan sistematis untuk mencapai tujuan penelitian, meliputi Identifikasi Masalah dan Pemahaman Kriptografi, Studi Literatur, Mencari Data, Analisis dan Implementasi Kriptografi, Analisis dan Implementasi Teknik Steganografi, Penyusunan Hasil Analisis dan Pembahasan Temuan, serta Kesimpulan. Tahapan ini akan dijelaskan lebih lanjut di Bab 3.3.