BAB I
PENDAHULUAN

1.1 Latar Belakang

Komunikasi digital di era sekarang memerlukan keamanan data yang kuat dan tidak terdeteksi. Steganografi berbasis Least Significant Bit (LSB) merupakan teknik yang populer untuk melindungi kerahasiaan data agar keberadaannya sulit dikenali pihak tidak berwenang[1]. Metode ini sering dipilih karena kemampuannya untuk mempertahankan tampilan media asli tanpa menimbulkan perubahan yang signifikan. Meskipun memiliki keunggulan dalam penyamarkan data rahasia, steganografi berbasis Least Significant Bit (LSB) seringkali menghadapi dilema yang signifikan antara kapasitas muatan, kualitas gambar, dan keamanan [2]. Peningkatan kapasitas penyisipan pada LSB dapat secara tidak langsung menurunkan kualitas gambar steganografi dan meningkatkan resiko steganalisis[3]. Selain itu, metode LSB tradisional masih menggunakan pola penyisipan secara sekuensial dan deterministik yang dapat menghasilkan suatu pola yang bisa diprediksi dan dideteksi oleh steganalisis modern. Ketika proses penyembunyian ini terbongkar, maka data rahasia dapat langsung diambil karena tidak memiliki perlindungan berupa enkripsi.

Beberapa upaya telah dilakukan untuk mengatasi masalah ini, penggabungan steganografi dengan enkripsi AES-GCM telah terbukti mampu memberikan perlindungan berlapis pada data rahasia [4]. Di sisi lain, penelitian lain menggabungkan steganografi dengan kompresi Huffman untuk memperkecil ukuran data sebelum di sisipkan sehingga dapat meningkatkan kapasitas tanpa mengurangi kualitas gambar steganografi [2]. Sementara itu, teknik pengacakan berbasis pohon Adelson-Velsky and Landis (AVL) juga diusulkan untuk mengurangi pola deterministik pada metode LSB konvensional [5]. Namun pendekatan ini ditemukan kurang efisien karena menimbulkan *overhead* waktu sebesar O(log N) untuk setiap pixel yang disisipkan. Selain itu, kompleksitas ruang sebesar O(N) yang diperlukan untuk menyimpan informasi struktural di setiap n*ode* membutuhkan memori komputasi yang tinggi. Ketergantungan metode ini pada satu kanal warna tertentu juga menurunkan kapasitas penyisipan.

Berdasarkan masalah tersebut, penelitian ini mengusulkan modal steganografi LSB hibrida yang mengintegrasikan tiga komponen utama yaitu kompresi lossless *Lempel Ziv Welch* (LZW), enkripsi terotentikasi AES-GCM, serta generator acak kriptografi Ascon-XOF sebagai kontribusi kebaruan. Penggunaan *Lempel Ziv Welch* (LZW) dipilih karena

merupakan metode kompresi lossless berbasis kamus yang mampu mengurangi ukuran data dengan memanfaatkan pola data yang berulang dan menggantinya dengan kode yang lebih pendek [6][7]. Hal tersebut secara tidak langsung dapat meningkatkan kapasitas pada citra digital tanpa mengurangi kualitas citra, sehingga sesuai untuk proses penyembunyian data berukuran besar. Sementara itu, AES-GCM digunakan untuk menjamin keamanan dan integritas data. Mode GCM ini secara spesifik memastikan data tidak hanya terenkripsi, tetapi juga terlindungi dari modifikasi pihak yang tidak berwenang, dimana jika terjadi perubahan pada data tersembunyi, maka proses dekripsi akan dibatalkan sehingga integritas data rahasia tetap terjamin. Namun, selain perlindungan isi data, steganografi juga memerlukan teknik penyisipan yang tidak berpola agar tidak mudah dideteksi oleh steganalisis. Ascon-XOF mampu mengatasi kelemahan pendekatan berbasis pohon AVL karena dapat menghasilkan urutan acak lebih cepat, tidak memerlukan struktur data kompleks, dan tidak membentuk pola teratur yang mudah diprediksi. Dengan keunggulan tersebut, kami menggunakan Ascon-XOF sebagai generator acak kriptografi, yang telah ditetapkan sebagai standard oleh NIST [8]. Keamanan algoritma ini juga sudah teruji, dimana hasil penelitian menunjukkan bahwa meskipun dilakukan serangan *preimage* pada varian 2-*round*, kompleksitas yang dibutuhkan tetap sangat tinggi yaitu mencapai 2^{97}, sehingga tidak membahayakan keamanan Ascon-XOF pada 12-*round* penuh [9]. Oleh karena itu, penelitian ini bertujuan untuk merancang dan mengimplementasikan sebuah model steganografi LSB hibrida yang aman, efisien, dan memiliki kapasitas tinggi dengan mengintegrasikan ketiga teknologi tersebut. Maka berdasarkan uraian di atas, dilakukan penulisan tugas akhir dengan judul **"PENERAPAN KEAMANAN MENGGUNAKAN KOMPRESI LZW DAN ENKRIPSI AES-256-GCM DENGAN ASCON-XOF128 SEBAGAI GENERATOR ACAK PADA STEGANOGRAFI LSB".**

1.2 Rumusan Masalah

Berdasarkan Latar Belakang diatas berikut adalah rumusan masalah yang ditemukan:

1. Kapasitas penyisipan data rahasia pada citra steganografi LSB masih terbatas, sehingga sulit untuk menyimpan data dalam jumlah besar tanpa menurunkan kualitas citra.
2. Data yang disisipkan dalam citra steganografi LSB berisiko dimodifikasi atau terbongkar, sehingga keamanan dan integritas data tidak terjamin.

1.3 Tujuan

Tujuan dari tugas akhir ini adalah:

1. Mengimplementasikan algoritma kompresi LZW untuk mengurangi ukuran data rahasia sebelum proses penyisipan untuk mengoptimalkan kapasitas penyimpanan data rahasia tanpa menurunkan kualitas visual citra penampung.
2. Mengimplementasikan algoritma enkripsi AES-GCM untuk menjamin aspek kerahasiaan dan integritas data rahasia dari upaya akses dan modifikasi pihak tidak berwenang.

1.4 Manfaat

Hasil dari penelitian ini diharapkan memberikan manfaat sebagai berikut:

1. Memungkinkan penyimpanan data rahasia dengan kapasitas yang lebih besar tanpa merusak kualitas visual citra penampung secara signifikan.
2. Pengguna dapat menyimpan data rahasia tanpa khawatir terbaca pihak lain.

1.5 Ruang Lingkup

Ruang lingkup dari tugas akhir ini, antara lain:

1. Citra sampul berupa gambar RGB 24bit berformat BMP atau PNG.
2. Data rahasia yang disisipkan berupa teks input secara langsung, disesuaikan dengan kapasitas penyisipan yang tersedia pada citra sampul.
3. Pemilihan pixel dan urutan channel warna dipilih berdasarkan generator acak kriptografi Ascon XOF128.
4. Jumlah bit sisip adalah 2, 3, dan 4 bit, dipilih berdasarkan generator acak kriptografi Ascon XOF128.
5. Pengujian kapasitas dilakukan dengan menghitung seberapa besar data rahasia yang dapat disisipkan pada citra sampul.
6. Pengujian kualitas citra hasil penyisipan (*stego-image*) diukur menggunakan metode *Mean Square Error* (MSE), *Peak Signal-to-Noise Ratio* (PSNR), dan *Structural Similarity Index* (SSIM).
7. Pengujian ini dilakukan dengan mensimulasikan manipulasi data menggunakan metode *Bit Flipping Attack*. Pengujian ini bertujuan untuk memastikan bahwa setiap perubahan pada data dapat dideteksi, sehingga kerahasiaan dan integritas data rahasia tetap terjaga dari modifikasi yang tidak sah.
8. Pengujian terhadap steganalisis dilakukan dengan *Chi-Square Attack* untuk mendeteksi keberadaan data tersembunyi dalam citra.
9. Aplikasi tidak menggunakan penerapan database seperti *MySQL* atau sejenisnya.