BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil implementasi, pengujian, dan analisis yang telah dilakukan terhadap metode steganografi *Adaptive* LSB *Matching* pada domain DCT, Peneliti dapat menarik kesimpulan sebagai berikut.

Kinerja Kualitas Visual (*Imperceptibility*) Kinerja metode *Adaptive LSB Matching* pada citra JPEG terbukti lebih unggul dalam mempertahankan kualitas visual dibandingkan metode DCT Standar. Berdasarkan hasil pengujian, metode usulan mampu menghasilkan rata-rata nilai *Peak Signal-to-Noise Ratio* (PSNR) yang lebih tinggi dan stabil, bahkan pada beban pesan maksimum sekalipun. Hal ini menunjukkan bahwa strategi penyisipan pada area frekuensi dengan energi stabil lebih efektif dalam meredam distorsi visual, sehingga citra stego tetap berada di atas ambang batas perseptual manusia dan sulit dibedakan dari citra aslinya.

Efektivitas Resistensi Deteksi Statistik Penerapan teknik modifikasi nilai koefisien pada frekuensi rendah-menengah terbukti sangat efektif dalam meminimalkan deteksi statistik berbasis analisis entropi. Metode usulan berhasil menekan nilai Selisih Entropi hingga mencapai tingkat yang sangat minimal, yang mengindikasikan bahwa distribusi histogram citra stego sangat identik dengan citra asli. Stabilitas statistik ini membuktikan bahwa mekanisme adaptif mampu menyamarkan jejak penyisipan secara signifikan, sehingga memiliki tingkat keamanan yang lebih tinggi terhadap serangan steganalisis dibandingkan metode konvensional.

Secara keseluruhan, penelitian ini menyimpulkan bahwa integrasi algoritma *Adaptive* LSB *Matching* pada posisi koefisien DCT yang strategis berhasil memberikan solusi keseimbangan yang optimal antara *fidelity* dan keamanan statistik. Metode ini terbukti mampu menyamarkan jejak penyisipan sebagai variasi *luminance* alami citra, sehingga menawarkan solusi komunikasi rahasia yang tangguh dan layak dipertimbangkan sebagai alternatif pengganti metode steganografi konvensional pada citra JPEG.

5.2 Saran

Penelitian ini telah berhasil membuktikan konsep *Proof of Concept* peningkatan keamanan steganografi DCT. Namun, terdapat beberapa keterbatasan yang dapat diperbaiki atau dikembangkan pada penelitian selanjutnya. Berdasarkan pengalaman selama proses penelitian, Peneliti memberikan saran-saran sebagai berikut:

1. Peningkatan Kapasitas Pesan (*High Capacity Payload*) Pada penelitian ini, beban pesan dibatasi hingga 144 bit untuk memvalidasi stabilitas entropi. Penelitian selanjutnya disarankan untuk menguji batas jenuh (*saturation point*) metode ini dengan menyisipkan pesan yang jauh lebih besar (ribuan bit) untuk mengetahui pada titik mana kualitas visual dan statistik mulai menurun secara signifikan.
2. Implementasi pada Citra Berwarna (RGB) Penelitian ini membatasi objek pada citra *grayscale* (kanal tunggal). Pengembangan selanjutnya dapat menerapkan algoritma ini pada citra berwarna (RGB atau *YCbCr*) untuk memanfaatkan redundansi data pada kanal warna (*krominans*) yang mungkin menawarkan kapasitas penyisipan lebih besar dengan dampak visual yang lebih minim.
3. Pengujian Ketahanan (*Robustness*) fokus penelitian ini adalah pada aspek *imperceptibility* dan keamanan statistik (entropi). Peneliti menyarankan agar penelitian mendatang menguji ketahanan (*robustness*) metode ini terhadap serangan aktif, seperti *cropping*, *scaling*, penambahan *noise*, atau kompresi JPEG berulang dengan faktor kualitas yang bervariasi.
4. Kombinasi dengan Kriptografi untuk meningkatkan keamanan isi pesan, disarankan untuk mengombinasikan metode steganografi ini dengan algoritma kriptografi (seperti AES atau RSA). Pesan sebaiknya dienkripsi terlebih dahulu menjadi *cipher text* sebelum disisipkan ke dalam citra, sehingga memberikan lapisan keamanan ganda (*double layer security*).

Dengan mempertimbangkan rekomendasi pengembangan di atas, diharapkan penelitian selanjutnya dapat memperluas cakupan implementasi metode ini agar tidak hanya aman dari sisi statistik, tetapi juga tangguh menghadapi berbagai manipulasi sinyal digital, sehingga dapat diterapkan secara lebih luas dalam sistem keamanan informasi yang kompleks.