

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Bedasarkan rumusan masalah serta hasil dan pembahasan, berikut kesimpulan yang diperoleh dari penelitian ini :

1. Implementasi gabungan kriptografi ElGamal dan steganografi *Least Significant Bit* (LSB) dengan *Blum Blum Shub* (BBS) terdiri dari enam tahap utama: pembangkitan kunci, enkripsi, *embedding*, ekstraksi, dekripsi, dan cek kualitas gambar. Tahap pertama adalah pembangkitan kunci ElGamal. Tahap kedua adalah enkripsi pesan menggunakan algoritma ElGamal. Tahap ketiga adalah *embedding* pesan terenkripsi ke dalam citra RGB menggunakan teknik LSB dan BBS. Tahap keempat adalah ekstraksi pesan dari *stego-image* menggunakan teknik yang sama. Tahap kelima adalah dekripsi pesan menggunakan algoritma ElGamal. Terakhir, tahap cek kualitas gambar dilakukan untuk memastikan kualitas *stego-image* yang dihasilkan tetap tinggi.
2. Pembuatan program aplikasi dari hasil penggabungan algoritma kriptografi ElGamal dan steganografi LSB BBS ini dikonstruksi menggunakan *Graphical User Interface* (GUI) dalam bahasa pemrograman *Python*. Program ini memiliki beberapa tab yang memisahkan fungsionalitasnya, yaitu pembangkitan kunci ElGamal, enkripsi menggunakan algoritma ElGamal, dekripsi menggunakan algoritma ElGamal, *embedding* menggunakan *Least Significant Bit*, ekstraksi menggunakan *Least Significant Bit*, dan cek kualitas gambar. Pengguna dapat dengan mudah mengakses dan menjalankan setiap fungsi dari aplikasi ini melalui antarmuka yang *user-friendly*.
3. Validasi program dilakukan menggunakan parameter *Peak Signal to Noise*

Ratio (PSNR) untuk menilai kualitas *stego-image*. Nilai PSNR yang tinggi mengindikasikan bahwa kualitas gambar setelah penyisipan pesan tetap terjaga. Hasil pengujian menunjukkan bahwa implementasi kriptografi ElGamal dan steganografi kombinasi LSB dan BBS dalam aplikasi ini dapat menghasilkan *stego-image* dengan kualitas yang sangat baik, menjaga kerahasiaan pesan, serta memberikan perlindungan yang kuat terhadap upaya kriptanalisis. Validasi menggunakan PSNR menunjukkan bahwa metode ini efektif untuk penyisipan pesan rahasia dalam gambar tanpa mengurangi kualitas visual gambar secara signifikan.

5.2 Saran

Setelah melakukan penelitian mengenai implementasi kriptografi ElGamal dan steganografi kombinasi *Least Significant Bit* dan *Blum Blum Shub* untuk pengamanan pesan rahasia dalam gambar, terdapat beberapa saran untuk dikembangkan pada penelitian selanjutnya, yaitu:

1. Menggunakan metode steganografi lain seperti *Discrete Cosine Transform*(DCT), *Discrete Wavelet Transform* (DWT), dan *Bit-Plane Complexity Segmentation* (BPCS) .
2. Menggunakan metode PRNG lain seperti *Park-Miller generator*, *Lagged Fibonacci generator*, *Mersenne Twister*, *Permuted Congruential Generator* dan WELL.