

BAB V KESIMPULAN, IMPLIKASI, DAN REKOMENDASI

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan penulis mengenai “Implementasi Algoritma Kriptografi *Serpent* dan Steganografi LSB untuk Pengamanan Data Teks Berbasis Aplikasi Android”, dapat diambil beberapa kesimpulan sebagai berikut:

1. Implementasi algoritma enkripsi *Serpent* dalam aplikasi Android menunjukkan hasil yang positif, dengan *ciphertext* yang dihasilkan memiliki nilai korelasi Pearson rata-rata $-0,047388859$ yang mengindikasikan korelasi sangat lemah dengan *plaintext*. Selain itu, berdasarkan estimasi perhitungan waktu serangan *bruteforce* terhadap panjang kunci 256-bit *Serpent*, bahkan dengan 8 miliar mesin yang bekerja secara bersamaan diperlukan waktu sekitar $3,64 \times 10^{58}$ tahun. Hal ini menunjukkan bahwa algoritma *Serpent* memiliki tingkat *robustness* yang sangat tinggi terhadap serangan *bruteforce* dan efektif dalam menyamarkan pesan teks dan mencegah pihak ketiga yang tidak bertanggung jawab untuk mendapatkan data asli.
2. Penggunaan teknik steganografi LSB untuk menyisipkan data ke dalam gambar menunjukkan hasil yang memuaskan. Hasil pengujian dengan menyisipkan data dengan data sebesar 32 *byte* karakter pada gambar menunjukkan nilai rata-rata MSE 0.00574 dan nilai rata-rata PSNR 70.6074 dB, yang mengindikasikan bahwa kualitas gambar tetap baik. Pengujian pada gambar kecil dengan menyisipkan besar data maksimum yang dapat disisipkan pada gambar menunjukkan nilai MSE di kisaran 2.4 sampai 2.6 dan nilai PSNR di kisaran 44 dB sampai 43 dB. Meskipun nilai MSE lebih tinggi dan PSNR lebih rendah pada pengujian ini, perubahan pada gambar tetap sulit dilihat oleh mata manusia. Selain itu, hasil pengujian korelasi *ciphertext* dan *plaintext* dengan korelasi Pearson memiliki nilai yang mendekati nol menunjukkan bahwa *ciphertext* memiliki tingkat korelasi sangat lemah. Integrasi teknik steganografi LSB ke dalam aplikasi ini

terbukti meningkatkan keamanan data teks yang telah dienkripsi dengan algoritma *Serpent*. Data yang disembunyikan tetap terjaga dan sulit dideteksi, menandakan bahwa teknik steganografi LSB tetap efektif dalam menyembunyikan data.

3. Pengembangan aplikasi Android yang mengimplementasikan algoritma enkripsi *Serpent* dan teknik steganografi LSB berhasil terlaksanakan dengan menggunakan metode pengembangan aplikasi *Agile*. Sementara untuk metode penelitian yang digunakan adalah metode penelitian *Design and Development* atau D&D. Pengujian terhadap aplikasi dilakukan dengan menggunakan metode pengujian *black box*. Hasil yang didapatkan menunjukkan bahwa seluruh fitur pada aplikasi berfungsi dengan baik sesuai dengan spesifikasi dan kebutuhan fungsionalitas yang diharapkan oleh penulis.

5.2 Implikasi

Penelitian ini memiliki beberapa implikasi penting yang dapat diterapkan dalam berbagai situasi. Pertama, aplikasi Android implementasi algoritma kriptografi *Serpent* dan teknik steganografi LSB dapat meningkatkan keamanan data teks secara signifikan. Dengan ini dapat mengurangi risiko data sensitif terbaca oleh pihak ketiga yang tidak bertanggung jawab, sehingga dapat memberikan perlindungan tambahan bagi data yang akan dikirimkan. Ini menunjukkan bahwa aplikasi ini dapat digunakan di berbagai sektor industri yang membutuhkan keamanan data, seperti perbankan, bidang kesehatan, atau pemerintahan. Sektor-sektor ini dapat menggunakan aplikasi untuk mengamankan data sensitif jika ingin mengirimkan data tersebut dan tidak jatuh ke tangan yang salah.

Selain itu, penelitian ini membuka peluang bagi penelitian lebih lanjut pada bidang keamanan data. Penelitian ini dapat menjadi dasar bagi pengembangan aplikasi keamanan data lainnya yang lebih canggih dan kompleks. Penelitian lanjut dapat mengeksplorasi peningkatan algoritma kriptografi dan teknik steganografi yang digunakan.

5.3 Rekomendasi

Berdasarkan hasil penelitian dan kesimpulan yang telah diambil, berikut adalah beberapa rekomendasi yang penulis sampaikan untuk pengembangan selanjutnya:

1. Diperlukan pengujian lebih lanjut dengan menguji aplikasi di berbagai perangkat yang berbeda untuk memastikan kompatibilitas dan performa yang konsisten di semua perangkat.
2. Mempertimbangkan penggunaan teknik steganografi *noiseless* yang dapat menghilangkan *noise* yang ditambahkan kepada gambar, sehingga data tidak akan mempengaruhi kualitas gambar.
3. Menggunakan algoritma *Serpent* yang sudah di ditingkatkan untuk mengefisienkan waktu proses enkripsi dan dekripsi data tanpa mengurangi keamanan data.