BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan rumusan masalah serta hasil dan pembahasan, kesimpulan penelitian ini diperoleh sebagai berikut.

1. Kriptografi gambar menggunakan mode operasi *Counter* RAES yang dimodifikasi dilakukan dengan menerapkan enkripsi RAES yang dimodifikasi dalam mode operasi *Counter* pada blok-blok hasil partisi warna utama penyusun gambar. Pada mode operasi ini, *counter* awal diperoleh dengan menerapkan suatu fungsi pada kunci untuk menyamarkan hubungan antara kunci dan *counter* awal. *Counter* selanjutnya diperoleh dengan menerapkan fungsi penambahan standar. Modifikasi RAES terletak pada penggunaan *rail-fence chiper* yang dioptimalkan dan pengelolaan kunci *rail-fence chiper*. *Rail-fence chiper* yang dioptimalkan membuat algoritma enkripsi RAES menjadi lebih efisien. Pengelolaan kunci membuat kunci *rail-fence chiper* yang sebenarnya menjadi tersamarkan dan membuat semua kunci yang mungkin di RAES dapat digunakan.
2. Program aplikasi kriptografi gambar menggunakan mode operasi *Counter* RAES yang dimodifikasi dibuat menggunakan Python dan beberapa *library*. Program aplikasi ini terdiri dari halaman utama dan halaman Tentang. Halaman utama digunakan untuk melakukan kriptografi gambar menggunakan mode operasi *Counter* RAES yang dimodifikasi serta menyimpan gambar hasil kriptografi tersebut. Halaman Tentang yang memuat informasi singkat terkait program aplikasi dapat diakses dari halaman utama.

5.2 Saran

1. Penelitian ini hanya membahas terkait implemantasi algoritma kriptografi pada gambar. Penelian selanjutnya dapat mencoba melakukan penelitian terkait analisis keamanan kriptografi gambar menggunakan mode operasi *Counter* RAES yang dimodifikasi.
2. Pada penelitian ini, algoritma kriptografi diterapkan pada pesan berupa gambar RGB. Penelitian selanjutnya dapat mencoba menerapkan algoritma

kriptografi ini pada bentuk pesan yang lain, diantaranya gambar RGBa, audio, dan video.

3. Pada penelitian ini, program aplikasi dikonstruksi menggunakan Python untuk memberikan gambaran cara algoritma kriptografi gambar diterapkan. Penelitian selanjutnya dapat mencoba menerapkan algoritma kriptografi ini pada teknologi dan kasus yang lebih spesifik. Contoh teknologi yang dapat digunakan adalah Android.
4. Pada penelitian ini, mode operasi yang digunakan adalah mode operasi *Counter*. Penelitian selanjutnya dapat mencoba menerapkan mode operasi *Galois Counter Mode*. Mode operasi ini tidak hanya menghadirkan keamanan berupa kerahasiaan, tapi juga autentifikasi.
5. Pada penelitian ini, lapangan galois digunakan untuk memilih *counter* awal. Penelitian selanjutnya dapat menerapkan lapangan galois untuk pembangkitan bilangan acak.