BAB V
KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan penelitian ini, pengujian dan analisis terhadap sistem, maka didapatkan kesimpulan sebagai berikut:

1. Metode AES 128 *bits* dapat diimplementasikan untuk proses enkripsi dan proses dekripsi pada video MPEG-2 dengan beberapa proses yang dilakukan yaitu:
   a. Melakukan proses ekstraksi video menjadi *frame* dahulu
   b. Melakukan konversi *frame* menjadi blok data dari *frame* asli setiap sebesar 128 *bits* atau 16 piksel sampai dengan ukuran maksimum *frame* asli tersebut.
   c. Input kunci AES 128 *bits.*
   d. Hitung kunci AES 128 *bits* dengan fungsi *hash* SHA-256.
   e. Jika dilakukan proses enkripsi maka inisialisasi pada blok data *frame* asli per 16 piksel dan jika dilakukan pada proses dekripsi makak inisialisasi pada blok data *frame* enkripsi per 16 piksel.
2. Metode SHA-256 terbukti dapat meningkatkan kompleksitas kunci pada AES 128 *bits* terlihat dari hasil uji *Randomness Test* bahwa kunci pada AES 128 *bits* yang menggunakan SHA-256 telah lolos semua tes uji sedangkan yang tidak menggunakan SHA-256 pada tahap Uji Poker gagal dan Uji Run *gagal*.
3. Hasil Uji Faktor *Fidelity*
   a. Berdasarkan evaluasi hasil pengujian *frame* asli dan *frame* enkripsi dari total empat dataset *frame* awal, tengah dan akhir dari masing-masing video, dua dari video yang diuji menghasilkan nilai PSNR pada kriptografi yang ideal yaitu di bawah 30 dB dengan nilai terbaik sebesar 27.8639 dB. Sedangkan untuk nilai MSE semua dataset *frame* yang diuji menghasilkan nilai MSE yang ideal yaitu diatas 30 yang berarti tingkat keacakan semakin error dan dengan nilai MSE terbaik sebesar 107.1931.
   b. Sedangkan berdasarkan evaluasi hasil pengujian *frame* asli dan *frame* dekripsi dari total empat dataset *frame* awal, tengah dan akhir dari masing-masing video, semua dataset *frame* yang diuji memiliki hasil PSNR yang ideal yaitu diatas 30 dB dengan nilai terbaik sebesar 43.3967. Sedangkan untuk nilai MSE juga memiliki hasil yang ideal yaitu di bawah 30 dengan nilai MSE terbaik sebesar 3.0148.

5.2. Saran

Dalam pelaksanaan penelitian, penulis menyadari bahwa banyak kekurangan di dalam penelitian ini. Oleh karena itu penulis menyampaikan beberapa saran akar penelitian yang akan dilakukan mengenai pembahasan yang serupa dengan penelitian ini dapat menjadi lebih baik. Beberapa saran penulis untuk penelitian selanjutnya, antara lain sebagai berikut:

a. Sistem yang dihasilkan saat ini memiliki beberapa keterbatasan, salah satunya adalah hanya bisa melakukan proses enkripsi pada sebagian *frame* video, karena proses enkripsi yang masih cukup lama dalam proses enkripsi semua *frame* yang ada pada video maka diharapkan untuk penelitian selanjutnya dapat mengimplementasikan algoritma yang dapat melakukan proses enkripsi dan dekripsi dengan baik dan diimplementasikan pada semua *frame* dalam video agar lebih aman dan dengen waktu yang efisien juga.
b. Pada penelitian ini format video yang digunakan hanya dalam bentuk MPEG-2 dan tidak terdapat validasinya, diharapkan untuk penelitian selanjutnya format video dapat beragam seperti .AVI, .MP4 dan format video kompresi lainnya.
c. Sistem saat ini belum memiliki tampilan yang memadai karena keterbatasan pada GUI matlab, maka diharapkan pada penelitian selanjutnya dapat membuat tampilan dari aplikasi menjadi lebih baik dengan bahasa pemrograman yang lainnya.
d. Pada pembuatan penelitian selanjutnya dapat membuat dengan bahasa pemrograman lainnya selain Matlab, yaitu dalam java, bahasa R, phyton dan lain-lainnya