BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilaksanakan dengan menerapkan Algoritma-CBC (Cipher Block Chaining) pada file gambar dan mengevaluasi kinerjanya, beberapa kesimpulan yang dapat diambil adalah sebagai berikut:

1. Algoritma AES-CBC berhasil diimplementasikan pada file gambar dengan hasil yang menunjukkan perubahan visual signifikan pada gambar yang terenkripsi. Proses enkripsi dan dekripsi berjalan sesuai dengan yang diharapkan, menjaga integritas data pada gambar yang diolah.
2. Evaluasi kualitas citra menunjukkan hasil yang sangat baik. Gambar hasil dekripsi memiliki nilai rata-rata MSE sebesar 19.899,61 dan RMSE sebesar 145,83, menunjukkan tingkat kesalahan yang sangat kecil. Nilai PSNR rata-rata mencapai 100 dB dan SSIM sebesar 1,0, yang mengindikasikan bahwa kualitas gambar terdekripsi hampir identik dengan gambar aslinya. Ini menunjukkan bahwa Algoritma AES-CBC mampu menjaga kualitas gambar secara optimal setelah proses enkripsi dan dekripsi.
3. Pengujian NPCR dan UACI berdasarkan nilai yang ditunjukkan oleh rata-rata NPCR sebesar 100% dan UACI sebesar 49,61%,yang berarti algoritma ini memiliki tingkat resistensi yang baik terhadap serangan diferensial. Hal ini menunjukkan bahwa AES mode CBC cukup aman dalam menghadapi perubahan kecil pada data input yang dapat mengakibatkan perbedaan besar pada output enkripsi.
4. Hasil pengujian korelasi antar-piksel (CC) dengan nilai rata-rata CC sebesar –0,0001, menunjukkan bahwa AES mode CBC mampu mengurangi korelasi antar-piksel pada gambar terenkripsi, sehingga meningkatkan tingkat keamanan citra data gambar.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, beberapa saran berikut diajukan sebagai masukan untuk pengembangan penelitian di masa mendatang:

1. Disarankan untuk membandingkan kinerja Algoritma AES-CBC dengan algoritma kriptografi lainnya, seperti AES-ECB, AES-CFB, AES-OFB atau mode enkripsi lainnya, untuk mengevaluasi apakah ada metode yang lebih efisien atau aman.
2. Penerapan Algoritma AES-CBC pada jenis file lain seperti audio atau video dapat dilakukan untuk melihat kinerjanya pada media yang berbeda dan mengevaluasi keamanannya dalam konteks yang lebih luas.
3. Penelitian masa depan bisa mengintegrasikan teknik steganografi dengan kriptografi untuk meningkatkan keamanan data yang disembunyikan di dalam file gambar, sehingga menghasilkan sistem keamanan data yang lebih kompleks dan sulit ditembus.

.