ANALISIS EVALUASI KINERJA QUALITY & DIFFERENTIAL ANALYSIS PADA FILE GAMBAR MENGGUNAKAN ALGORITMA AES-CBC

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

M. ALFAHRI SOLEHAN

21.83.0679

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

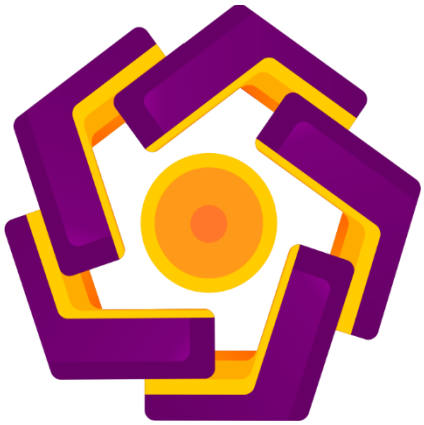
2025

ANALISIS EVALUASI KINERJA QUALITY & DIFFERENTIAL ANALYSIS PADA FILE GAMBAR MENGGUNAKAN ALGORITMA AES-CBC

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer



disusun oleh

M. ALFAHRI SOLEHAN

21.83.0679

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS EVALUASI KINERJA QUALITY & DIFFERENTIAL ANALYSIS PADA FILE GAMBAR MENGGUNAKAN ALGORITMA AES-CBC

yang disusun dan diajukan oleh

M. Alfahri Solehan

21.83.0679

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 26 Mei 2025

Dosen Pembimbing,

Dr. Dony Ariyus, S.S., M.Kom.

NIK. 190302128

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS EVALUASI KINERJA QUALITY & DIFFERENTIAL ANALYSIS PADA FILE GAMBAR MENGGUNAKAN ALGORITMA AES-CBC

yang disusun dan diajukan oleh

M. Alfahri Solehan

21.83.0679

Telah dipertahankan di depan Dewan Penguji
pada tanggal 26 Mei 2025

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Muhammad Koprawi, S.Kom., M.Eng **NIK. 190302454**	
Wahid Miftahul Ashari, S.Kom., M.T **NIK. 190302452**	
Dr. Dony Ariyus, S.S., M.Kom. **NIK. 190302128**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 26 Mei 2025

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, S.Kom., M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : M. Alfahri Solehan
NIM : 21.83.0679

Menyatakan bahwa Skripsi dengan judul berikut:

Analisis Evaluasi Kinerja Quality & Differential Analysis Pada File Gambar Menggunakan Algoritma AES-CBC

Dosen Pembimbing : Dr. Dony Ariyus, S.S., M.Kom.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 21 Mei 2025

Yang Menyatakan.

M. Alfahri Solehan

HALAMAN PERSEMBAHAN

Segala puji syukur penulis panjatkan ke hadirat Allah Subhanahu wa Ta'ala atas limpahan rahmat, hidayah, dan karunia-Nya, sehingga skripsi ini dapat diselesaikan dengan sebaik-baiknya. Dengan segala kerendahan hati, karya ini penulis persembahkan untuk:

1. **Ayah dan Ibu tercinta**, Bapak Syahroni dan Ibu Sriyati, yang tidak pernah berhenti memberikan doa, dukungan, pengorbanan, serta cinta yang tulus dalam setiap langkah perjalanan hidup penulis. Terima kasih atas segala jerih payah yang telah diberikan demi masa depan anakmu.
2. **Bapak Dony Ariyus, M.Kom**, selaku dosen pembimbing, yang dengan sabar dan penuh dedikasi telah membimbing penulis dalam proses penyusunan skripsi ini hingga terselesaikan.
3. **Teman-teman dan sahabat seperjuangan**, yang telah menjadi bagian penting dalam perjalanan perkuliahan, baik dalam suka maupun duka. Terima kasih atas kebersamaan, dukungan, dan semangat yang tak ternilai selama masa studi ini.

Semoga karya sederhana ini dapat menjadi awal dari kontribusi penulis dalam bidang ilmu pengetahuan serta memberikan manfaat bagi pihak yang membutuhkan.

.

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah Subhanahu wa Ta'ala, atas rahmat, hidayah, serta inayah-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul **"Analisis Evaluasi Kinerja Quality & Differential Analysis pada File Gambar Menggunakan Algoritma AES-CBC."**

Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata 1 pada Program Studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta. Dalam proses penyusunan skripsi ini, penulis mendapat banyak dukungan, arahan, dan bantuan dari berbagai pihak, baik secara moral maupun materiil. Oleh karena itu, penulis menyampaikan terima kasih dan penghargaan yang sebesar-besarnya kepada:

1. Ayah dan Ibu tercinta yang selalu memberikan doa, kasih sayang, serta dukungan moril dan spiritual yang tidak pernah putus.
2. Bapak Prof. Dr. M. Suyanto, M.M., selaku Rektor Universitas Amikom Yogyakarta.
3. Ibu Prof. Dr. Kusrini, S.Kom., M.Kom., selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
4. Bapak Dr. Dony Ariyus, S.S., M.Kom., selaku Ketua Program Studi Teknik Komputer sekaligus Dosen Pembimbing yang telah dengan sabar memberikan arahan, masukan, serta bimbingan kepada penulis dalam menyelesaikan skripsi ini.
5. Seluruh dosen dan staf di Universitas Amikom Yogyakarta yang telah memberikan ilmu dan pelayanan terbaik selama masa studi.
6. Teman-teman dan semua pihak yang turut membantu dan memberikan semangat hingga skripsi ini dapat terselesaikan.

Yogyakarta, 07 Mei 2025

M. Alfahri Solehan

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR KODE PROGRAM

DAFTAR LAMPIRAN

INTISARI

Penelitian ini mengeksplorasi pendekatan Quality dan Differential Analysis untuk menilai kinerja algoritma AES-Cipher Block Chaining (AES-CBC) pada enkripsi gambar. Algoritma AES-CBC dipilih karena kemampuannya dalam mengenkripsi data gambar secara aman dan efisien. Penelitian ini berfokus pada implementasi AES-CBC untuk mengenkripsi dan mendekripsi gambar color dan grayscale berukuran 512 x 512 piksel, dengan tujuan mengimplementasikan algoritma tersebut dan mengevaluasi hasil enkripsi dan dekripsi menggunakan metrik Quality dan Differential.

Metode yang digunakan dalam penelitian ini melibatkan proses enkripsi dan dekripsi menggunakan AES-CBC pada gambar dengan ukuran dan tipe yang berbeda. Evaluasi dilakukan dengan menggunakan metrik kualitas seperti Mean Squared Error (MSE), Root Mean Squared Error (RMSE), Peak Signal-to-Noise Ratio (PSNR), dan Structural Similarity Index (SSIM) untuk menilai kualitas enkripsi dan dekripsi. Selain itu, metrik efisiensi diferensial seperti Number of Changing Pixels Rate (NPCR), Unified Average Changing Intensity (UACI), dan Correlation Coefficient (CC) digunakan untuk mengukur perubahan diferensial dan pengacakan piksel.

Hasil penelitian menunjukkan nilai MSE dan RMSE pada nilai 0, PSNR melebihi 30db, serta SSIM mencapai 1, mencerminkan kualitas dekripsi yang sangat baik. Nilai NPCR dan UACI mencapai persentase ideal, menunjukkan kemampuan algoritma menangani perubahan diferensial, sementara CC antara gambar asli dan terenkripsi mencapai nol, membuktikan pengacakan piksel yang efektif. Penelitian ini memberikan wawasan tentang efektivitas AES-CBC dalam mengamankan file gambar dan mendukung pengembangan metode enkripsi yang lebih aman di masa depan.

Kata kunci: AES-CBC, Enkripsi Gambar, Quality & Differential Analysis, Keamanan Data Citra, Evaluasi Kinerja.

ABSTRACT

This study explores the use of Quality and Differential Analysis approaches to evaluate the performance of the AES-Cipher Block Chaining (AES-CBC) algorithm in image encryption. AES-CBC was chosen for its capability to securely and efficiently encrypt image data. The research focuses on the implementation of AES-CBC to encrypt and decrypt both color and grayscale images with a resolution of 512 x 512 pixels, aiming to implement the algorithm and assess the encryption and decryption results using Quality and Differential metrics.

The methodology involves encrypting and decrypting images of various types and sizes using the AES-CBC algorithm. The evaluation is conducted using quality metrics such as Mean Squared Error (MSE), Root Mean Squared Error (RMSE), Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity Index (SSIM) to assess the quality of encryption and decryption. Additionally, differential efficiency metrics such as Number of Changing Pixels Rate (NPCR), Unified Average Changing Intensity (UACI), and Correlation Coefficient (CC) are used to measure differential changes and pixel randomness.

The results show MSE and RMSE values of 0, PSNR exceeding 30 dB, and an SSIM score of 1, reflecting excellent decryption quality. The NPCR and UACI values reach ideal percentages, indicating the algorithm's ability to handle differential changes, while the CC between the original and encrypted images reaches zero, demonstrating effective pixel randomization. This study provides insights into the effectiveness of AES-CBC in securing image files and supports the development of more secure encryption methods in the future.

Keyword: *AES-CBC, image encryption, Quality & Differential Analysis, Image Data Security, Performance Evaluation*