ABSTRAK

Penelitian ini menyelidiki perbandingan mode *Galois Counter Mode, Output Feedback,* dan *Cipher Feedback* pada algoritma AES terkait kecepatan enkripsi dan keamanan gambar RGB. Penelitian ini bertujuan untuk menemukan mode yang memiliki keseimbangan antara kecepatan dan tingkat keamanan antara *Galois Counter Mode* ,*Output Feedback* (OFB) dan *Cipher Feedback* (CFB), dalam konteks enkripsi gambar. Tujuan utamanya termasuk mengevaluasi kecepatan enkripsi dan tingkat keamanan AES. Selain itu, penelitian ini membandingkan kinerja GCM, OFB, dan CFB untuk menentukan pendekatan yang optimal untuk enkripsi gambar yang aman dan efisien. Metodologi penelitian melibatkan beberapa langkah: Pengumpulan Data, Pembagian Piksel, Inisialisasi, Enkripsi, dan Pengujian. Gambar dari situs web Unsplash digunakan sebagai data masukan. Gambar-gambar tersebut dibagi menjadi enam bagian yang sama untuk meningkatkan kecepatan enkripsi melalui pemrosesan paralel. Kunci enkripsi AES dibuat, dan nonce unik digunakan untuk setiap proses enkripsi. Algoritme AES-GCM, AES-OFB, dan AES-CFB diimplementasikan, dengan proses enkripsi dijalankan secara paralel untuk bagian gambar yang dibagi. Hasil enkripsi dievaluasi dengan menggunakan metrik NPCR (*Number of Pixel Changing Rate*) dan UACI (*Unified Average Changing Intensity*) untuk mengukur sensitivitas dan distorsi.

Hasil pengujian menunjukkan bahwa ketiga mode tersebut memiliki kecepatan enkripsi yang serupa dan menghasilkan nilai Number of Pixel Change Rate (NPCR) yang sangat tinggi, rata-rata mencapai 99,61%. Nilai ini menunjukkan bahwa ketiga metode secara efektif menyamarkan gambar asli melalui perubahan pixel yang signifikan. Selain itu, pengujian Unified Average Changing Intensity (UACI) mengungkapkan konsistensi tinggi dalam variasi perubahan intensitas pixel, dengan nilai UACI berkisar antara 29,55% hingga 39,22%. Hasil penelitian juga menunjukkan bahwa semua mode enkripsi mampu menjaga kesesuaian pixel antara gambar asli dan gambar yang didekripsi, menunjukkan bahwa proses enkripsi-dekripsi bersifat lossless. Secara keseluruhan, ketiga mode enkripsi terbukti sangat efektif dan reliabel dalam melindungi integritas dan keamanan data gambar tanpa kehilangan informasi.

Penelitian ini menegaskan bahwa GCM, OFB, dan CFB semuanya adalah pilihan yang efektif dan andal untuk enkripsi citra, dengan GCM sebagai pilihan terbaik untuk kebutuhan kecepatan dan OFB untuk keamanan yang lebih tinggi. Hasil ini dapat digunakan sebagai pedoman

bagi para praktisi dan peneliti dalam memilih mode enkripsi yang paling cocok berdasarkan kebutuhan mereka, menjamin bahwa data sensitif dan berharga tetap aman dalam berbagai kondisi operasional.

Kata Kunci: *Galois Counter Mode*, *Cipher Feedback, Output Feedback ,Advanced Encryption Standard*, Enkripsi Gambar, RGB Images, Kecepatan Enkripsi, Keamanan Enkripsi

ABSTRACT

This research investigates the comparison of Galois Counter Mode, Output Feedback, and Cipher Feedback modes in AES algorithm regarding encryption speed and security of RGB images. This research aims to find a mode that has a balance between speed and security level between Galois Counter Mode, Output Feedback (OFB) and Cipher Feedback (CFB), in the context of image encryption. The main objectives include evaluating the encryption speed and security level of AES. In addition, this research compares the performance of GCM, OFB, and CFB to determine the optimal approach for secure and efficient image encryption. The research methodology involves several steps: Data Collection, Pixel Division, Initialization, Encryption, and Testing. Images from the Unsplash website were used as input data. The images were divided into six equal parts to increase the encryption speed through parallel processing. The AES encryption key is generated, and a unique nonce is used for each encryption process. The AES-GCM, AES-OFB, and AES-CFB algorithms are implemented, with the encryption process executed in parallel for the divided image parts. The encryption results are evaluated using NPCR (Number of Pixel Changing Rate) and UACI (Unified Average Changing Intensity) metrics to measure sensitivity and distortion.

The test results show that the three modes have similar encryption speeds and produce very high Number of Pixel Change Rate (NPCR) values, reaching 99.61% on average. This value indicates that the three methods effectively disguise the original image through significant pixel changes. In addition, the Unified Average Changing Intensity (UACI) test revealed high consistency in the variation of pixel intensity changes, with UACI values ranging from 29.55% to 39.22%. The results also showed that all encryption modes were able to maintain pixel congruency between the original and decrypted images, indicating that the encryption-decryption process is lossless. Overall, the three encryption modes proved to be very effective and reliable in protecting the integrity and security of image data without loss of information.

This research confirms that GCM, OFB, and CFB are all effective and reliable choices for image encryption, with GCM being the best choice for speed requirements and OFB for higher security.

Keywords: Galois Counter Mode, Advanced Encryption Standard, Image Encryption, RGB Images, Encryption Speed, Encryption Security