Pengenkripsian dan Dekripsi Gambar Menggunakan Algoritma AES dengan MAC untuk Peningkatan Keamanan

Ni Wayan Amanda Putri Astawa[a1], I Made Widiartha[a2]

[a]Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam,
Universitas Udayana
Jalan Raya Kampus Udayana, Bukit Jimbaran, Kuta Selatan, Badung, Bali Indonesia
[1]putrimanda985@gmail.com
[2]madewidiartha@unud.ac.id

Abstract

With the increasing importance of data security in digital image transmission and storage, this research presents an implementation of an image encryption and decryption program using the Advanced Encryption Standard (AES) algorithm combined with Message Authentication Code (MAC) for enhanced security. The program utilizes AES in Cipher Block Chaining (CBC) mode to ensure confidentiality and integrity of the image data. The unique key and initialization vector (IV) enhance the security of the encryption process. Additionally, the inclusion of MAC ensures data integrity and prevents unauthorized modifications during transmission or storage. The program offers a user-friendly web-based interface for easy usability. The implemented solution provides a high level of security for image data and can be applied in various applications requiring secure image transmission and storage. The effectiveness and reliability of the program are demonstrated through experimental results and evaluation.

Keywords: *Advanced Encryption Standard, Message Authentication Code, Hash, Encryption, Decryption*

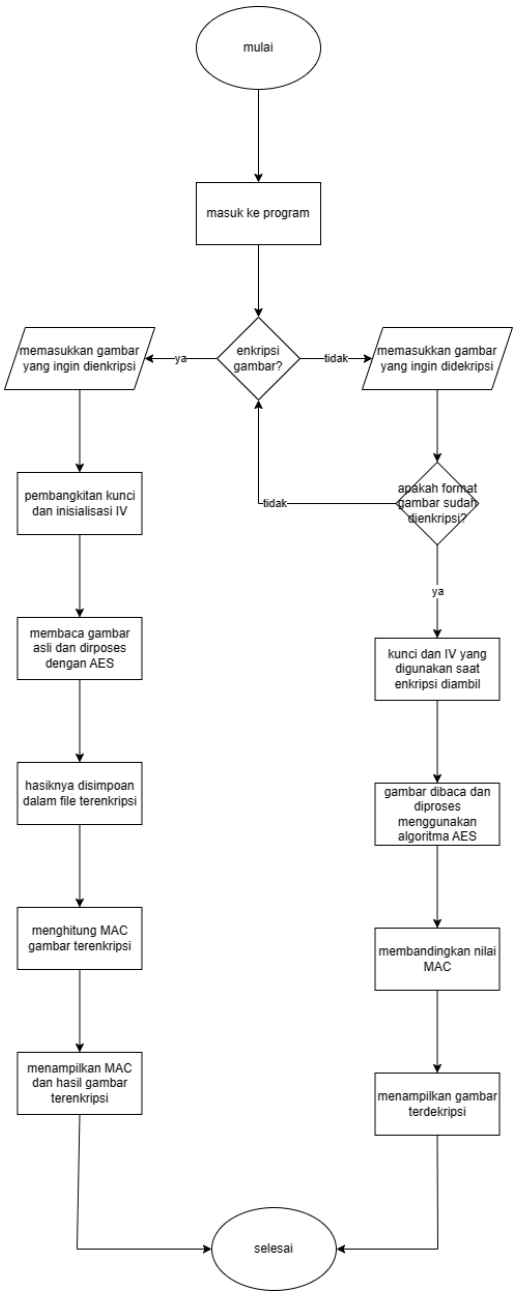
1. Pendahuluan

Dalam era digital yang terus berkembang, pertukaran informasi secara konvensional sudah mulai ditinggalkan dan digantikan dengan dunia maya atau digital. Yang dimana segala informasi dapat diakses melalui internet secara bebas. Salah satu contoh nyatanya adalah penggunaan gambar sebagai media komunikasi dan pertukaran informasi telah menjadi sangat umum untuk dilakukan [1]. Namun, dengan adanya perkembangan teknologi, kebutuhan untuk melindungi keamanan dan integritas gambar juga turut meningkat. Ancaman keamanan seperti peretasan, pencurian data, dan modifikasi yang tidak sah dapat mengancam kerahasiaan dan integritas gambar yang sensitif. Untuk dapat mengantisipasi terjadinya ancaman keamanan tersebut, diperlukan metode keamanan yang efektif dan juga kuat dalam menjaga kerahasiaan dan juga integritas gambar.

Algoritma Advanced Encryption Standard (AES) dapat menjadi salah satu solusi yang cukup efektif dalam mengantisispasi terjadinya ancaman dalam citra gambar. Metode AES akan digunakan untuk mengenkripsi gambar, sehingga hanya pihak yang memiliki munci enkripsi yang tepat dapat mendeksripsikannya. Selanjutnya, digunakan pula algoritma Message Authentication Code (MAC) yang akan memastikan integritas data dengan menandatangani gambar yang telah dienkripsi, sehingga perubahan yang tidak sah dapat terdeteksi. Dalam penelitian ini, penulis juga menggunakan fungsi Hash sebagai mekanisme verifikasi integritas dengan menyimpan nilai hash dari gambar yang telah dienkripsi dan ditandatangani.

2. Metode Penelitian

2.1 Desain Sistem



Gambar 1. Flowchart Sistem

Pertama, pengguna diminta untuk memilih gambar yang akan dienkripsi. Setelah gambar asli dipilih, program membuka gambar tersebut dan melakukan proses enkripsi. Gambar terenkripsi kemudian disimpan ke dalam file. Selain itu, program juga menghitung MAC (Message Authentication Code) dari gambar asli sebagai tanda verifikasi. MAC tersebut disimpan dalam file terpisah yang akan digunakan nanti.

Ketika pengguna ingin mendekripsi dan memverifikasi gambar terenkripsi, mereka memilih gambar terenkripsi yang akan diolah. Program membuka gambar terenkripsi dan memulai proses verifikasi MAC. Verifikasi ini penting untuk memastikan bahwa gambar terenkripsi tidak

mengalami perubahan atau kerusakan yang tidak sah. Jika verifikasi MAC berhasil, program melanjutkan dengan proses dekripsi. Gambar terenkripsi didekripsi dan hasilnya disimpan ke dalam file terpisah. Akhirnya, gambar terdekripsi ditampilkan kepada pengguna untuk dilihat.

2.2 Pemrosesan Awal

Pada tahap ini, gambar yang diunggah oleh pengguna diambil sebagai input. Langkah pertama yang dilakukan adalah memvalidasi format gambar untuk memastikan bahwa gambar yang diunggah memiliki format yang valid, seperti JPEG, PNG, atau format gambar lainnya. Validasi ini penting untuk memastikan bahwa gambar dapat diterima dan diproses dengan benar. Setelah validasi format, gambar yang valid kemudian akan dienkripsi menggunakan algoritma enkripsi yang dipilih, dalam kasus ini yaitu Advanced Encryption Standard (AES). Tujuan dari enkripsi ini adalah untuk melindungi kerahasiaan gambar dengan mengubah kontennya menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang.

Selanjutnya, dalam rangka memverifikasi integritas gambar, dilakukan pembangkitan Message Authentication Code (MAC) menggunakan algoritma hash seperti SHA-256. MAC ini berguna untuk memastikan bahwa gambar tidak mengalami perubahan atau kerusakan pada saat ditransmisikan atau disimpan. MAC akan menjadi referensi untuk memverifikasi apakah gambar telah mengalami perubahan yang tidak sah. Setelah gambar dienkripsi dan MAC dihasilkan, gambar terenkripsi beserta MAC-nya disimpan dalam penyimpanan yang relevan, seperti file atau database. Hal ini bertujuan untuk menjaga keamanan gambar yang terenkripsi dan memfasilitasi proses pemulihan saat diperlukan.

Dalam keseluruhan pemrosesan awal ini, langkah-langkah tersebut memiliki peran penting dalam menjaga keamanan dan integritas gambar pada aplikasi berbasis web. Validasi format gambar memastikan bahwa gambar yang diunggah sesuai dengan harapan, sementara enkripsi dan MAC membantu melindungi kerahasiaan dan memverifikasi integritas gambar.

2.3 Proses Enkripsi

Proses enkripsi dalam program ini dilakukan menggunakan algoritma AES (Advanced Encryption Standard) dalam mode CBC (Cipher Block Chaining), yang memberikan tingkat keamanan yang tinggi. Pertama-tama, pengguna memilih gambar yang akan dienkripsi melalui antarmuka aplikasi berbasis web. Setelah gambar dipilih, program membuka gambar asli dan mempersiapkan kunci dan vektor inisialisasi (IV) yang diperlukan untuk proses enkripsi. Selanjutnya, gambar asli dienkripsi dengan menggunakan algoritma AES dalam mode CBC. Pada mode CBC, setiap blok gambar dienkripsi secara berurutan dengan blok sebelumnya sebagai vektor inisialisasi. Hal ini membantu dalam menciptakan perubahan yang signifikan pada setiap blok enkripsi, sehingga menjaga kerahasiaan dan keamanan data.

Selain enkripsi gambar, program juga menerapkan algoritma MAC (Message Authentication Code) untuk memastikan integritas dan otentikasi data. Algoritma MAC yang digunakan dalam program ini adalah HMAC-SHA256 (Hash-based Message Authentication Code dengan fungsi hash SHA256). MAC dihasilkan dari gambar terenkripsi dan kunci yang sama yang digunakan dalam proses enkripsi. Fungsi MAC memastikan bahwa gambar terenkripsi tidak mengalami perubahan atau manipulasi selama proses penyimpanan atau transfer. Dengan menggabungkan enkripsi AES dalam mode CBC dan algoritma MAC, program ini memberikan keamanan yang kuat terhadap gambar yang dienkripsi. Enkripsi melindungi kerahasiaan gambar asli, sementara MAC memastikan integritas dan otentikasi data pada tahap dekripsi. Kombinasi kedua teknik ini memberikan lapisan keamanan yang kokoh dan melindungi gambar terenkripsi dari serangan dan manipulasi yang tidak sah.

2.4 Proses Dekripsi

Proses dekripsi dalam program ini dilakukan setelah pengguna memilih gambar terenkripsi melalui antarmuka aplikasi berbasis web. Setelah gambar terenkripsi dipilih, program membuka file gambar terenkripsi dan memulai proses dekripsi. Pertama, program membaca isi file gambar

terenkripsi dan mempersiapkan kunci dan vektor inisialisasi (IV) yang sama yang digunakan dalam proses enkripsi. Kunci dan IV ini penting untuk mendekripsi gambar dengan benar. Selanjutnya, program menggunakan algoritma AES dalam mode CBC untuk mendekripsi gambar terenkripsi. Dengan menggunakan kunci dan IV yang tepat, setiap blok gambar terenkripsi didekripsi secara berurutan. Proses dekripsi ini mengembalikan gambar ke bentuk aslinya.

Selama proses dekripsi, program juga memverifikasi integritas dan otentikasi gambar dengan menggunakan algoritma MAC (Message Authentication Code). Program menghasilkan MAC baru dari gambar terdekripsi dan menggunakan kunci yang sama yang digunakan dalam proses enkripsi. MAC ini kemudian dibandingkan dengan MAC asli yang disimpan bersama gambar terenkripsi. Jika kedua MAC cocok, itu menunjukkan bahwa gambar tidak mengalami perubahan selama proses penyimpanan atau transfer. Setelah proses dekripsi selesai, gambar terdekripsi ditampilkan ke pengguna melalui antarmuka aplikasi. Pengguna dapat melihat gambar dalam bentuk aslinya, seperti sebelum dienkripsi. Proses dekripsi ini memberikan kemampuan untuk mengembalikan gambar ke bentuk aslinya setelah melalui proses enkripsi. Algoritma AES dalam mode CBC dan verifikasi MAC memastikan bahwa gambar terdekripsi akurat dan tidak mengalami modifikasi yang tidak sah.

3. Hasil dan Pembahasan

3.1 Uji Coba Sistem

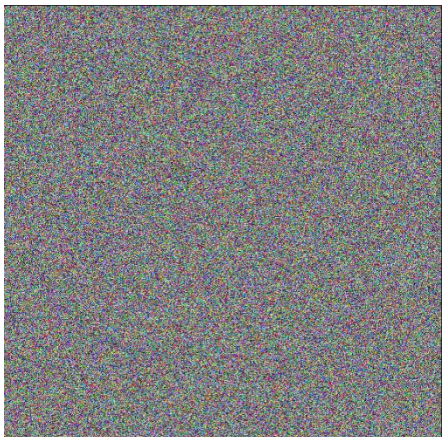
a. Proses Enkripsi

Pengujian ini dilakukan untuk melihat apakah alogritma AES dapat mengenkripsi gambar dengan langkah-langkah sebagai berikut:

1. Memilih gambar yang akan dienkripsi.
2. Menghasilkan kunci acak dan inisialisasi vektor (IV) untuk AES.
3. Membuka gambar asli.
4. Mengenkripsi gambar menggunakan AES dalam mode CBC dengan kunci dan IV yang dihasilkan.
5. Menghasilkan MAC (Message Authentication Code) dari gambar terenkripsi untuk integritas dan autentikasi.
6. Menyimpan gambar terenkripsi dan MAC ke dalam file.
7. Menghasilkan output berupa gambar terenkripsi dan MAC.

Tabel 1. Proses Enkripsi

Sebelum

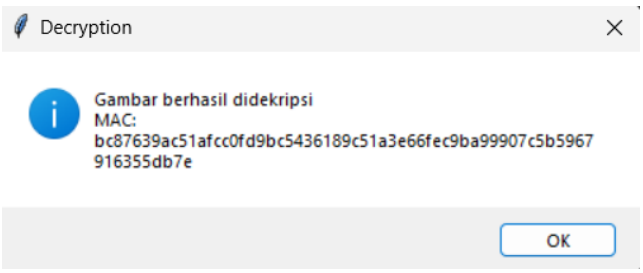

Sesudah

Nilai MAC


b. Proses Dekripsi

Pengujian ini dilakukan untuk melihat apakah algoritma AES dapat mengdekripsi gambar dengan langkah-langkah sebagai berikut:

1. Memilih gambar terenkripsi yang akan didekripsi.
2. Membuka gambar terenkripsi dan MAC dari file.
3. Memverifikasi integritas dan autentikasi gambar terenkripsi menggunakan MAC.
4. Mendapatkan kunci dan IV yang digunakan saat proses enkripsi.
5. Mendekripsi gambar menggunakan AES dalam mode CBC dengan kunci dan IV yang sesuai.
6. Menghilangkan padding yang ditambahkan saat enkripsi.
7. Menyimpan gambar terdekripsi ke dalam file.
8. Menghasilkan output berupa gambar terdekripsi.

Tabel 2. Proses Dekripsi

Nilai MAC


Dapat kita lihat bahwa nilai MAC dari enkripsi dan dekripsi sama. Hal itu menunjukkan bahwa gambar tidak mengalami perubahan selama proses penyimpanan atau transfer.

4. Kesimpulan

Penelitian ini berhasil mengimplementasikan program enkripsi dan dekripsi gambar dengan menggunakan algoritma AES dan MAC. Program ini memberikan tingkat keamanan yang tinggi terhadap data gambar dengan menggunakan kunci dan IV yang unik, serta mode CBC untuk melindungi kerahasiaan data. Adanya algoritma MAC juga menjaga integritas data. Implementasi ini dapat digunakan dalam berbagai aplikasi yang membutuhkan keamanan data gambar.

Daftar Pustaka

[1] B. S. A. Priandana and I. M. Widiartha, "Pengembangan Aplikasi Berbasis Mobile Untuk Pengamanan Teks Menggunakan Metode Advanced Encryption Standard dan Least Significant Bit," Jurnal Nasional Teknologi Informasi dan Aplikasinya

[2] G. D. M. Zulma, H. B. Seta and T. Yuniati, "Implementasi Algoritma AES Dan Bcrypt untuk Pengamanan File Dokumen," Jurnal Informatik, 2022.

[3] G. Y. Pangestu, A. I. Hadiana and P. N. Sabrina, "Kriptografi Untuk Enkripsi Ganda Pada Gambar Menggunakan Algoritma AES (Advanced Encryption Standard) Dan RC5 (Rivest Code 5)," Informatics And Digital Expert (Index), vol. IV, 2022.

[4] A. T. Hlaing and M. T. M. Win, "Secure Image Steganography using Canny Magic LSB Substitution Method and HMAC Algorithm," in Universal Academic Cluster International July Conference, Bangkok, 2019.

[5] R. N. Sihombin and Y. Hasan, "Implementasi Algoritma Advanced Encryption Standard (Aes) Dalam Mengamankan File Citra Dokumen," in Seminar Nasional Inovasi dan Teknologi Informasi SNITI, Medan, 2016.