Jurnal Ilmu Komputer Revolusioner

Vol.8 No.12, Desember 2024
ISSN: 24430355

IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) UNTUK PENGAMANAN CITRA DIGITAL

Maulana Akbar
Universitas Islam Sumatera Utara
E-mail: maulanaa.akbar7@gmail.com

Abstrak

Pada era digital saat ini, keamanan data menjadi hal yang sangat penting, terutama dalam melindungi informasi sensitif yang disimpan dalam bentuk citra digital. Algoritma Advanced Encryption Standard (AES) adalah salah satu metode enkripsi yang diakui memiliki tingkat keamanan tinggi dan banyak digunakan untuk pengamanan data digital. Penelitian ini bertujuan untuk mengimplementasikan algoritma AES dalam pengamanan citra digital dengan memfokuskan pada proses enkripsi dan dekripsi. Penelitian ini menggunakan citra digital sebagai objek data yang dienkripsi menggunakan kunci AES 192-bit, yang diharapkan mampu melindungi data dari akses tidak sah. Metodologi penelitian ini melibatkan beberapa tahapan, Dimulai dari pengumpulan beberapa data citra digital, pemrosesan algoritma AES untuk enkripsi dan dekripsi, hingga evaluasi hasil dalam bentuk analisis performa dan kualitas citra. Evaluasi dilakukan dengan mengukur perubahan yang terjadi pada citra hasil enkripsi dan dekripsi. Hasil penelitian menunjukkan bahwa implementasi algoritma AES berhasil mengamankan citra digital dengan tingkat keandalan yang tinggi, sekaligus menjaga kualitas citra yang didekripsi mendekati bentuk aslinya. Implementasi ini diharapkan dapat memberikan kontribusi dalam pengembangan teknologi keamanan data citra digital yang lebih aman dan andal.

Kata Kunci — Advanced Encryption Standard (AES), Enkripsi, Dekripsi, Citra Digital, Keamanan Data.

1. PENDAHULUAN

Perkembangan teknologi digital saat ini telah membawa kemajuan signifikan dalam berbagai sektor, termasuk komunikasi, bisnis, dan hiburan. Salah satu media digital yang paling banyak digunakan adalah gambar yang banyak digunakan dalam berbagai aplikasi seperti fotografi, media sosial, kesehatan, serta keamanan dan pengawasan. Namun, dengan meningkatnya penggunaan gambar digital, muncul pula ancaman serius terhadap privasi dan keamanan data, terutama dalam hal pencurian, manipulasi, atau penyebaran gambar tanpa izin.

Pengamanan citra digital menjadi hal yang sangat penting untuk melindungi informasi sensitif yang terkandung dalam gambar. Salah satu teknik umum yang digunakan untuk menjaga kerahasiaan data adalah dengan kriptografi. Kriptografi merupakan ilmu ataupun seni mengamankan data dengan cara mengenkripsinya sehingga tidak bisa diakses oleh pihak yang tidak berwenang (Budiman et al., 2023).

Di antara berbagai algoritma kriptografi yang ada, Advanced Encryption Standar atau yang disingkat dengan AES merupakan salah satu algoritma yang diakui secara luas karena tingkat keamanannya yang tinggi, efisiensi, dan kecepatan dalam memproses data. AES telah menjadi standar enkripsi yang disetujui oleh NIST (National Institute of Standards and Technology) dan digunakan dalam berbagai aplikasi, termasuk komunikasi data, pengamanan jaringan, dan pengolahan citra digital.

AES bekerja dengan mengenkripsi blok data berukuran 128-bit dan menggunakan

kunci sepanjang 128, 192, atau 256-bit, yang memberikan fleksibilitas dalam tingkat keamanan. Penggunaan AES dalam pengamanan citra digital menawarkan berbagai keuntungan, termasuk kemampuannya untuk menjaga kualitas gambar serta melindungi informasi di dalam gambar dari akses yang tidak sah.

Namun, meskipun algoritma AES telah terbukti andal untuk enkripsi data umum, implementasinya pada citra digital memerlukan penelitian lebih lanjut untuk memastikan bahwa proses enkripsi tidak merusak kualitas citra dan tetap efisien secara komputasi. Oleh karena itu, penelitian ini bertujuan untuk mengimplementasikan algoritma AES pada citra digital dan menganalisis performanya dalam menjaga keamanan serta mempertahankan kualitas gambar.

Dengan semakin tingginya resiko terhadap privasi dan keamanan dalam dunia digital, solusi enkripsi yang efektif seperti AES sangat diperlukan, terutama untuk melindungi citra digital yang seringkali mengandung informasi pribadi atau rahasia.

2. METODE

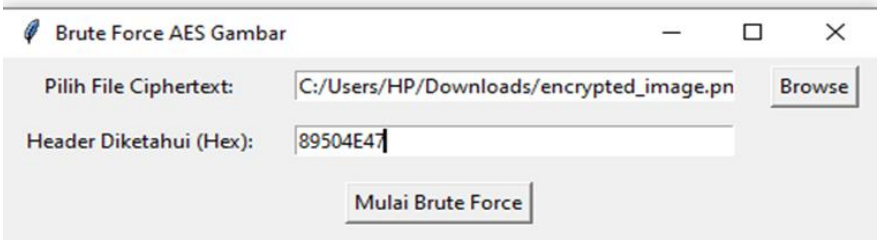
Dalam penelitian ini sumber data menjadi elemen krusial yang mendukung keberhasilan dan kevalidan penelitian ini. Sumber data utama dalam penelitian ini adalah citra digital dalam format PNG, JPEG atau JPG. Citra digital dipilih sebagai objek penelitian karena peran pentingnya dalam berbagai aspek kehidupan modern, termasuk komunikasi, media sosial, dan aplikasi internet lainnya. Data citra ini digunakan sebagai objek yang akan dienkripsi menggunakan algoritma kriptografi Advance Encryption Standart(AES) yang telah ditingkatkan keamanannya.

3. HASIL DAN PEMBAHASAN

Implementasi Pengamanan Pesan Gambar dengan menggunakan algoritma AES terbukti aman untuk mengamankan citra digital. Enkripsi berhasil mengubah citra yang dapat dibaca menjadi bentuk yang tidak dapat dikenali, dan hanya dapat dikembalikan ke bentuk asli menggunakan kunci yang tepat. Hal ini menunjukkan bahwa AES merupakan algoritma yang dapat digunakan untuk aplikasi yang memerlukan pengamanan citra, seperti pengamanan citra medis, citra pribadi, dan lain-lain.

Hasil dekripsi menunjukkan bahwa citra yang didekripsi sangat mirip dengan citra asli. Namun, sedikit perbedaan dalam kualitas gambar dapat terjadi karena proses pengolahan digital dan kompresi. Meskipun demikian, perbedaan tersebut sangat kecil dan dapat diterima dalam banyak aplikasi, khususnya dalam konteks pengamanan citra.

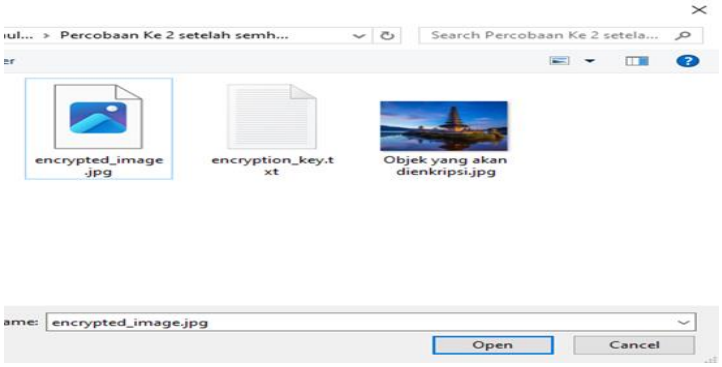
AES merupakan algoritma enkripsi simetris yang dirancang untuk melindungi data dengan Tingkat keamanan data yang cukup tinggi, AES bekerja dengan membagi data menjadi blok 128-bit dan menggunakan metode kriptografi untuk mengenkripsi dan mendekripsi data. Pemilihan Panjang kunci 128, 192, dan 256 tidak mempengaruhi ukuran file dalam enkripsi dan dekripsi, akan tetapi mempengaruhi iterasi Tingkat keamanan dan kinerja serangan dalam proses pengujian kemanan dengan menggunakan brute force. Ini terjadi pada saat pengujian brute force. Setiap kunci membutuhkan waktu eksekusi yang berbeda dalam menyelesaikan proses kriptanalisis.



Gambar 1 Tampilan Pengujian Kriptanalisis Bruteforce

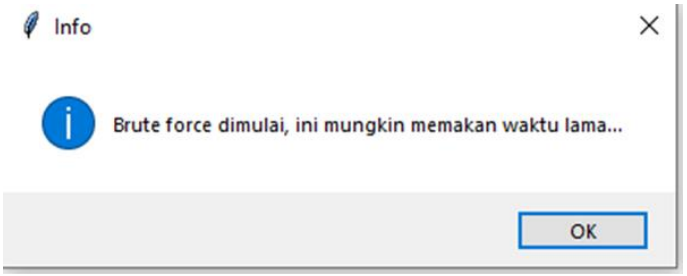
Gambar 1 menunjukkan tampilan pengujian Kriptanalisis menggunakan Bruteforce.

Pada gambar tersebut dapat dilihat tombol untuk mencari file yang akan di kriptanalisis dan kode header (He) yang merupakan kode extensi jenis file, misalkan ketika kita ingin menkripstanalisis jenis png, maka kode header yang kita masukkan adalah 89504E47.
Misalkan kita ingin mengkriptanalisis sebuah gambar yang menggunakan kunci 192 bit



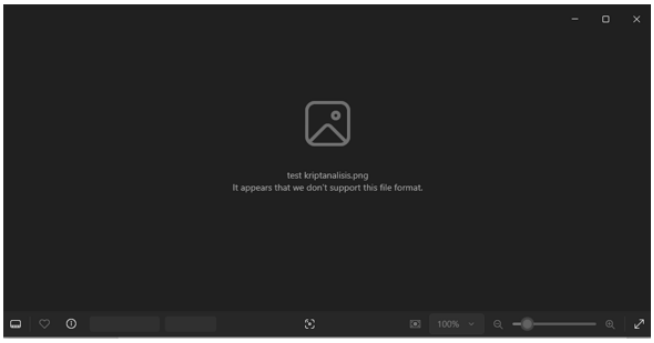
Gambar 2 Pemilihan Gambar Yang Akan Dikriptanalisis

Gambar 2 menunjukkan proses pemilihan gambar yang akan dikriptanalisis dengan menggunakan bruteforce. Kemudian pada saat kita memilih gambar yang akan kita akan kriptanalisis, dan kita masukkan nilai header hexanya, maka program akan menampilkan notifikasi sebagai berikut :



Gambar 3 Notifikasi Bruteforce Siap Akan Dijalankan

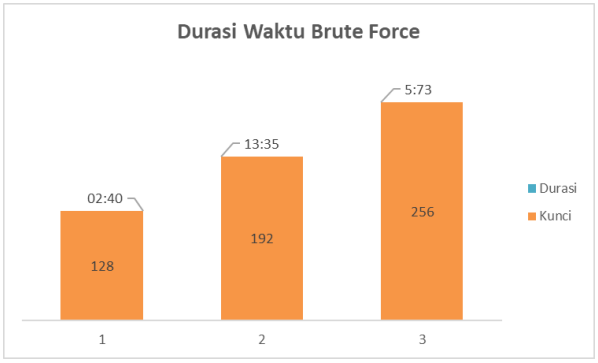
Gambar 3 merupakan notifikasi bruteforce siap akan dijalankan dan akan memerlukan waktu yang lama untuk proses kriptanalisis. Jika proses Kriptanalisis telah selesai dilakukan, maka program akan memberikan notifikasi jika program sudah menemukan kunci, akan tetapi pada saat dibukak gambar yang telah dikriptanalisis, gambar eror dan tidak bisa dibuka.



Gambar 4 Hasil Kriptanalisis Dengan Menggunakan Kunci 192 Bit

Gambar 4.15 menunjukkan gambar hasil kriptanalisis menggunakan Bruteforce.

Dengan menggunakan algoritma AES sebagai metode pengaman gambar berhasil mengecoh bruteforce dalam mendekripsi file gambar yang telah dienkripsi. Untuk ukuran file kriptanalisis sama persis dengan ukuran enkripsi.



Gambar 5 Grafik Durasi Waktu Kriptanalisis Brute Force

Gambar 5 menunjukkan Grafik durasi waktu yang yang dibutuhkan dalam mengkriptanalisis Brute Force. Dalam grafik tersebut menunjukkan durasi waktu kriptanalisis dengan panjang kunci 128 bit membutuhkan waktu 2,40 detik, kemudian untuk kriptanalisis dengan Panjang kunci 192 bit membutuhkan waktu durasi 13,35 detik, dan untuk kriptanalisis dengan Panjang kunci 256 bit membutuhkan waktu 5,75 detik.

KESIMPULAN

1. Berdasarkan hasil implementasi yang telah dilakukan, dapat disimpulkan bahwa algoritma AES dengan kunci 192 bit efektif dalam mengamankan citra digital. Kualitas citra yang didekripsi tetap baik dan hampir tidak terlihat perbedaannya dari citra asli.
2. Tingkat kemanan enkripsi dan dekripsi terjamin dengan ukuran kunci 192 bit, dimana proses durasi kriptanalisis dengan menggunakan brute force lebih lama dibandingkan dengan ukuran kunci 128 dan 256 bit.
3. Proses kriptanalisis dilakukan dengan menggunakan bruteforce, dimana proses dekripsi dilakukan dengan cara 2besar kunci atau misalkan kita menggunakan kunci 128bit, maka bruteforce akan menghitung 2128bit dalam proses iterasi mencari kunci

Saran

1. Saran untuk penelitian selanjutnya adalah mengoptimalkan algoritma ini agar lebih efisien dalam menangani citra dengan ukuran yang lebih besar dan menggunakan mode enkripsi yang lebih kompleks dalam meningkatkan kecepatan dan keamanan file citra.

REFERENCES

Agita, Y., Tarigan, P., Aulia, R., & Marwan, A. (2024). Algoritma AES 128 dalam Mengenkripsikan Berkas Bansos Kecamatan Tigabinanga Berbasis Web. 17(2), 2580–2582.

Budiman, M. A., Rachmawati, D., & Syahnan, I. P. (2023). A tutorial on using ElGamal cryptosystem and RC4-P1 cipher in a hybrid scheme. Journal of Physics: Conference Series, 2421(1), 012033. https://doi.org/10.1088/1742-6596/2421/1/012033

Gonzalez, R. C., & Woods, R. E. (2018). 4TH EDITION Digital image processing.

Gunawan, I. (2021). Peningkatan Pengamanan Data File Menggunakan Algoritma Kriptografi AES Dari Serangan Brute Force. TECHSI - Jurnal Teknik Informatika, 13(1), 14. https://doi.org/10.29103/techsi.v13i1.2395

Katz, J., & Lindell, Y. (2021). Introduction to Modern Cryptography (Thrid Edit). Chapman & Hall. https://www.ptonline.com/articles/how-to-get-better-mfi-results

Mahesa, K., Sugiantoro, B., & Prayudi, Y. (2019). Pemanfaatan Metode DNA Kriptografi dalam Meningkatkan Keamanan Citra Digital. Jurnal Ilmiah Informatika (JIF), 2615–1049.

Pan, H., Zhang, Q., Caragea, C., Dragut, E., & Jan, L. (n.d.). FlowLearn : Evaluating Large Vision-Language Models on Flowchart Understanding.

Papilaya, R. M., & Pradana, R. (2024). PENGAMANAN FILE MARKETING PADA YAYASAN PENDIDIKAN DESAIN INDONESIA MENGGUNAKAN ALGORITMA AES-256 BERBASIS WEB MARKETING FILES SECURITY AT THE INDONESIAN DESIGN

EDUCATION FOUNDATION USING WEB-BASED AES-256. 3(September), 109–117.
Paul, G., & Maitra, S. (2011). RC 4 Stream Cipher variants And It's Variants. In Teaching Mathematics and its Applications (Vol. 29, Issue 3). https://doi.org/10.1093/teamat/hrq007
Ratna, S. (2020). Pengolahan Citra Digital Dan Histogram Dengan Phyton Dan Text Editor Phycharm. Technologia: Jurnal Ilmiah, 11(3), 181. https://doi.org/10.31602/tji.v11i3.3294
Rilo Pambudi, A., Garno, & Purwantoro. (2020). DETEKSI KEASLIAN UANG KERTAS BERDASARKAN WATERMARK DENGAN PENGOLAHAN CITRA DIGITAL. Jurnal Informatika Polinema, 6(4), 69–74.
Romzi, M., & Kurniawan, B. (2020). Pembelajaran Pemrograman Python Dengan Pendekatan Logika Algoritma. JTIM: Jurnal Teknik Informatika Mahakarya, 03(2), 37–44.
Sinaga, M. C. (2017). Kriptografi dan Python. Academia, 157. https://www.academia.edu/34788898/Kriptografi_dan_Python_pdf