PENGEMBANGAN APLIKASI STEGANOGRAFI MENGGUNAKAN KRIPTOGRAFI ADVANCE ENCRYPTION STANDARD DAN LEAST SIGNIFICANT BIT

[1]Evan Averill Andika, [2]Ramadhan Renaldy dan [3]M. Vendi Nur Rohim

[1,2,3]*Jurusan Informatika, Fakultas Teknik dan Informatika, Universitas PGRI Semarang*

Gedung B Lantai 3, Kampus 1 Jl. Sidodadi Timur 24, Semarang

E-mail : evanandika874@gmail.com [1], ramadhanrenaldy@upgris.ac.id [2], yaituvendi9890@gmail.com [3]

Abstrak - *Perlindungan data digital menjadi semakin penting seiring dengan meningkatnya ancaman pencurian informasi dan pelanggaran hak cipta. Penelitian ini mengembangkan aplikasi steganografi yang memanfaatkan teknik enkripsi Advanced Encryption Standard (AES) dan metode Least Significant Bit (LSB) untuk menyembunyikan pesan dalam gambar. Metode ini bertujuan untuk melindungi keaslian konten digital dengan cara menyisipkan informasi yang terenkripsi ke dalam bit paling tidak signifikan dari piksel gambar, sehingga keberadaan pesan tidak mudah terdeteksi. Proses dimulai dengan enkripsi pesan menggunakan AES-128, yang menghasilkan ciphertext yang aman. Selanjutnya, ciphertext tersebut disisipkan ke dalam gambar melalui teknik LSB, menjaga kualitas visual gambar tetap utuh. Hasil penelitian menunjukkan bahwa sistem ini efektif dalam menyimpan pesan yang dapat bertahan terhadap kompresi ringan dan manipulasi sederhana, sekaligus memastikan bahwa hanya pihak yang memiliki kunci dekripsi yang dapat mengakses informasi tersebut. Integrasi antara steganografi dan kriptografi ini menawarkan solusi yang handal untuk menjaga keamanan dan integritas data digital di era informasi saat ini.*

Kata kunci: *Steganografi, Kriptografi, AES, LSB, perlindungan data digital.*

I. PENDAHULUAN

Seiring perkembangan teknologi informasi dan komunikasi, konten digital seperti gambar, video, dan audio semakin mudah diakses, disalin, dan disebarluaskan. Namun, kemudahan ini juga menimbulkan permasalahan terkait perlindungan hak cipta dan keaslian data digital. Maraknya kasus plagiarisme dan penyalahgunaan konten digital memunculkan kebutuhan mendesak akan mekanisme yang efektif untuk melindungi karya digital dan mengidentifikasi pemilik sah dari konten tersebut. [1]

Salah satu solusi untuk melindungi hak cipta digital adalah teknik steganografi, yaitu teknik menyembunyikan informasi atau pesan dalam objek fisik atau pesan lain agar tidak terdeteksi. Untuk meningkatkan keamanan dalam proses steganografi, digunakan kriptografi Advanced Encryption Standard (AES) [2]. Dengan menggabungkan teknik steganografi dan enkripsi AES-128, pesan dapat disembunyikan secara aman dan hanya dapat diekstraksi serta dibaca oleh pihak yang memiliki kunci enkripsi yang tepat. Mengembangkan aplikasi steganografi yang menggabungkan metode Least Significant Bit (LSB) [3] untuk menyembunyikan pesan dan kriptografi Advanced Encryption Standard (AES) untuk mengamankan pesan.

Tujuan dari pengembangan aplikasi steganografi menggunakan kriptografi AES [4] dan metode Least Significant Bit (LSB) adalah untuk menciptakan sistem yang dapat menyembunyikan pesan secara aman dalam file digital. Aplikasi ini menggabungkan teknik steganografi untuk menyembunyikan pesan dan kriptografi AES untuk mengamankan pesan tersebut, sehingga hanya pihak yang berwenang yang dapat membacanya. Dengan cara ini, diharapkan dapat meningkatkan keamanan dan kerahasiaan informasi yang dikirimkan melalui media digital. [5]

E-ISSN: 2985-3532

Berikut adalah beberapa penelitian yang berhubungan dengan penerapan enkripsi AES dalam sistem informasi:

II. METODE PENELITIAN

1. Metode Penelitian

Enkripsi menggunakan Advanced Encryption Standard (AES) [6]merupakan salah satu metode enkripsi simetris yang paling banyak digunakan saat ini. Metode ini memiliki karakteristik penting seperti kecepatan, keamanan, dan efisiensi. AES [7]menggunakan algoritma blok simetris. Artinya, kunci yang sama digunakan untuk proses enkripsi dan dekripsi. Metode utama yang digunakan untuk enkripsi AES adalah:

1.1 SubBytes (pengganti byte)

Fase ini merupakan proses substitusi non-linear dimana setiap byte pada blok input diganti dengan byte lain berdasarkan tabel substitusi yang disebut S-Box (Substitution Box). S-Box dirancang agar tahan terhadap serangan kriptografi seperti serangan diferensial dan linier. Operasi ini dilakukan pada seluruh blok masukan 128-bit.

1.2 Pergeseran baris

Pada fase ini, baris-baris matriks blok (berukuran 4x4) diputar melingkar ke kiri. Baris pertama tidak berubah, baris kedua diputar 1 byte, baris ketiga diputar 2 byte, dan baris keempat diputar 3 byte. Fitur ini membantu menyebarkan data dan mempersulit penyerang untuk menebaknya.

1.3 MixColumns (mengacak kolom)

Operasi ini dilakukan untuk setiap kolom blok 4x4. Setiap kolom dianggap polinomial dan dikalikan dengan polinomial tetap di bidang Galois. Operasi ini mengacak kolom dan mengacak data byte di dalam kolom, sehingga mengubah satu byte dalam satu blok setelah operasi ini dapat memengaruhi seluruh kolom. Level ini tidak digunakan pada putaran terakhir enkripsi.

1.4 AddRoundKey (Tambahkan kunci bulat)

Selama setiap putaran enkripsi, blok data di-XOR dengan kunci putaran yang berbeda. Kunci bulat ini dihasilkan dari kunci master menggunakan proses perluasan kunci. Proses ini memastikan kunci yang berbeda digunakan pada setiap putaran, sehingga hasil enkripsi menjadi lebih aman.

1.5 Ekspansi kunci (ekspansi kunci)

AES menggunakan kunci dengan panjang tetap: 128, 192, atau 256 bit. Proses perluasan kunci menciptakan sekumpulan subkunci yang digunakan dalam setiap putaran enkripsi. Untuk kunci 128-bit, AES menggunakan 10 putaran, untuk kunci 192-bit menggunakan 12 putaran, dan untuk kunci 256-bit menggunakan 14 putaran.

1.6 Lingkaran enkripsi

Tergantung pada panjang kunci yang digunakan, jumlah putaran enkripsi untuk AES adalah:
AES-128: 10 putaran
Setiap putaran melakukan operasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey.
Namun, MixColumns tidak digunakan di babak terakhir.
Metode yang digunakan dalam penelitian ini melibatkan langkah-langkah berikut:
1.6.1 Enkripsi pesan ke gambar menggunakan AES-128, di mana pesan dikonversi ke format terenkripsi (ciphertext).

E-ISSN: 2985-3532

1.6.2 Penyisipan ciphertext ke dalam file gambar menggunakan teknik Least Significant Bit (LSB), yang memodifikasi bit-bit paling tidak signifikan dari piksel gambar.
1.6.3 Sistem diuji untuk memastikan pesan dalam gambar tetap tersembunyi dan terlindungi dari manipulasi, tanpa merusak kualitas gambar asli.
Proses enkripsi AES secara keseluruhan:

Teks biasa dibagi menjadi blok 128-bit. Blok ini diproses melalui tahap AddRoundKey. Blok tersebut kemudian melakukan serangkaian putaran menggunakan SubBytes, ShiftRows, MixColumns, dan AddRoundKey. Di babak final, hanya tiga operasi yang dilakukan: SubBytes, ShiftRows, dan AddRoundKey. Hasilnya adalah ciphertext terenkripsi dengan panjang yang sama dengan panjang input. keamanan AES [8]. AES dirancang agar sangat aman. Sampai saat ini, tidak ada serangan praktis yang dapat menembus AES dalam waktu yang wajar. Hal ini disebabkan oleh kombinasi operasi nonlinier (SubBytes), penyebaran (ShiftRows dan MixColumns), dan kombinasi tombol yang kompleks (AddRoundKey). AES efisien dalam perangkat keras dan perangkat lunak dan direkomendasikan untuk banyak aplikasi keamanan seperti VPN, enkripsi disk penuh, dan komunikasi terenkripsi.

1.6.4 Flowchart system

Penjelasan flowchart:

-Upload gambar: Pengguna memasukkan gambar yang ingin disisipkan pesan ke gambar

-Input pesan: Pengguna memasukkan pesan yang akan di berikan ke gambar.

-Input kunci 16 bit: Pengguna memasukkan kunci sepanjang 16 bit.

-Enkripsi pesan menggunakan AES-128: Mengenkripsi pesan dengan algoritma AES-128.

-Konversi Hasil Enkripsi ke Format Biner: mengubah hasil enkripsi kedalam format biner.

-Sisipkan ke Piksel: hasil enkripsi(dalam biner) disisipkan kedalam pixel gambar menggunakan algoritma LSB.

-Simpan gambar: Gambar yang sudah disisipi pesan ke gambar terenkripsi akan otomatis tersimpan.

E-ISSN: 2985-3532

Gambar 25: Flowchart Menyisipkan Pesan Ke Gambar

Penjelasan flowchart:
-Upload gambar berpesan: Pengguna memasukkan gambar yang sudah disisipkan pesan.

-Input kunci 16 bit: Pengguna memasukkan kunci sepanjang 16 bit.

-Validasi Kunci: memeriksa apakah kunci yang dimasukkan sama dengan kunci yang digunakan saat memberi penyisipkan pesan ke gambar

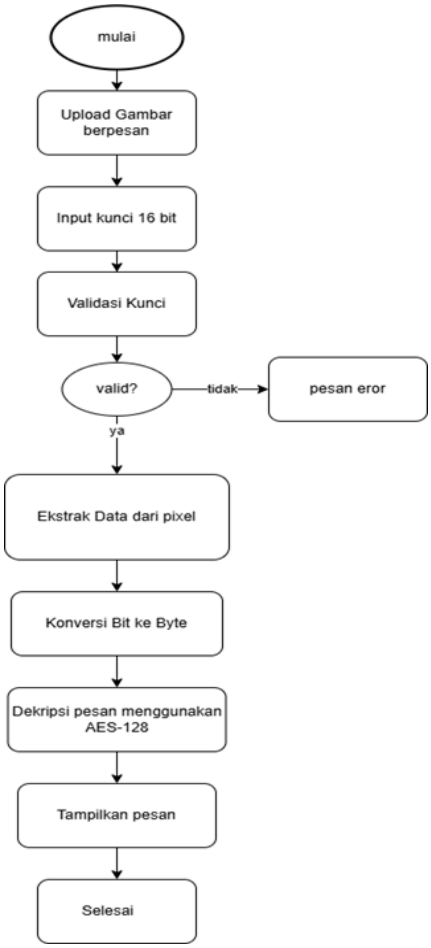
--Ekstrak Data dari pixel: mengambil data dari gambar.

-Konversi Bit ke Byte: data yang di dapat dari gambar masih berupa bit dirubah menjadi Byte.

-Dekripsi pesan dari gambar menggunakan AES-128: mendekripsi pesan dari gambar menggunakan AES-128.

-Tampilkan pesan: menampilkan pesan yang berhasil diekstrak dari gambar.

E-ISSN: 2985-3532



Gambar 26: Flowchart Ekstraksi Pesan Ke Gambar

III. HASIL DAN PEMBAHASAN

Gambar 27: Gambar Sebelum Di Enkripsi

E-ISSN: 2985-3532

Gambar 28: Gambar Sesudah Di Enkripsi

Extracted pesan: pasti bisa

Gambar 29: Gambar Extracted Pesan

Analisis Proses Penyisipan Pesan

Proses penyisipan pesan dalam aplikasi ini dilakukan dengan teknik Least Significant Bit (LSB), dikombinasikan dengan enkripsi AES-**128** untuk memastikan keamanan pesan.

1. **Teknik LSB** memungkinkan perubahan yang sangat kecil pada piksel gambar. Perubahan ini tidak mempengaruhi kualitas visual gambar secara signifikan karena hanya bit paling rendah dari tiap piksel yang diubah. Hal ini membuat pesan menjadi "invisible" atau tidak terlihat oleh mata manusia.

2. **Proses Enkripsi dengan AES-128** memastikan bahwa pesan yang disisipkan dalam gambar tidak dapat dibaca oleh pihak yang tidak memiliki kunci dekripsi. AES-128 adalah algoritma yang diakui secara luas karena memiliki tingkat keamanan yang tinggi dan efisiensi komputasi yang baik.

Alur Penyisipan Pesan

- **Enkripsi Pesan**: Sebelum disisipkan, teks pesan dienkripsi menggunakan AES-128 dengan kunci yang telah ditentukan. Proses ini mengonversi teks menjadi data terenkripsi dalam format biner.

- **Penyisipan ke dalam Piksel**: Data hasil enkripsi kemudian disisipkan ke dalam bit paling rendah dari komponen piksel hijau pada gambar. Pemilihan komponen hijau dilakukan karena mata manusia kurang sensitif terhadap perubahan intensitas hijau dibandingkan dengan merah atau biru.

Analisis Proses Ekstraksi dan Dekripsi Pesan

Proses ekstraksi pesan melibatkan pengambilan bit-bit dari komponen piksel yang telah dimodifikasi. Setelah bit-bit ini diambil, proses dilanjutkan dengan dekripsi menggunakan kunci AES-128 untuk mengembalikan teks pesan asli.

E-ISSN: 2985-3532

Keberhasilan Ekstraksi
Keberhasilan ekstraksi bergantung pada beberapa faktor:

1. **Konsistensi Data**: Bit-bit yang disisipkan harus diambil dengan urutan yang benar untuk memastikan akurasi data yang diekstrak.
2. **Kunci Dekripsi**: Tanpa kunci AES-128 yang benar, data hasil ekstraksi tidak dapat didekripsi menjadi teks yang dapat dibaca. Ini menambah lapisan keamanan tambahan terhadap upaya pihak yang tidak berwenang untuk membaca pesan.

Keamanan Pesan
Penggunaan enkripsi **AES-128** dalam proses ini memberikan beberapa keunggulan keamanan:

1. **Kerumitan Kriptografi**: AES-128 memiliki panjang kunci 128bit, yang berarti ada 2^128 kemungkinan kombinasi kunci. Hal ini membuat upaya untuk memecahkan kunci dengan serangan brute-force menjadi tidak praktis.
2. **Integritas Pesan**: Dengan enkripsi AES, hanya pihak yang memiliki kunci yang benar yang dapat mengekstrak dan membaca pesan. Ini melindungi pesan dari upaya manipulasi atau pemalsuan.

Kendala dalam Implementasi
Beberapa kendala yang ditemukan dalam implementasi ini meliputi:

1. **Kapasitas Penyisipan Terbatas**: Teknik LSB memiliki keterbatasan kapasitas penyisipan. Semakin besar ukuran pesan, semakin besar potensi degradasi kualitas gambar.
2. **Ketahanan Terhadap Serangan**: Teknik LSB kurang tahan terhadap serangan manipulasi gambar yang agresif, seperti rotasi, perubahan skala, atau pemotongan gambar secara ekstrem.
3. **Kebergantungan pada Kualitas Gambar**: Gambar dengan resolusi rendah atau kompresi tinggi memiliki lebih sedikit ruang untuk menyisipkan pesan tanpa mengurangi kualitas visual.

IV. KESIMPULAN

Dalam era digital, perlindungan data menjadi isu krusial akibat meningkatnya ancaman seperti pencurian informasi dan pelanggaran hak cipta. Salah satu pendekatan yang digunakan untuk mengatasi masalah ini adalah melalui teknik steganografi, yang disertai dengan enkripsi untuk meningkatkan keamanannya. Advanced Encryption Standard (AES) dipilih sebagai algoritma enkripsi karena tingkat keamanannya yang tinggi dan efisiensinya dalam berbagai implementasi. Hasil implementasi menunjukkan bahwa sistem mampu mengenkripsi dan menyisipkan pesan ke dalam file gambar secara efektif. Pesan yang telah disisipkan tetap dapat bertahan terhadap kompresi ringan dan manipulasi sederhana, sehingga meningkatkan perlindungan terhadap pelanggaran hak cipta. Selain itu, penggunaan AES-128 terbukti efisien untuk memproses file gambar dengan ukuran sedang tanpa memengaruhi kualitas file.

Penelitian ini membuktikan bahwa integrasi steganografi dengan enkripsi AES dan LSB memberikan solusi yang handal untuk menjaga keamanan dan integritas data digital.

E-ISSN: 2985-3532

V. SARAN

Saran untuk penelitian ini adalah bisa lebih baik lagi kedepannya dalam mengembangkan sistem, lebih baik lagi dalam pengujian kinerja aplikasi/sistem pada berbagai jenis media, peningkatan keamanan melalui penambahan layer kriptografi, pengujian pada berbagai variasi kunci kriptografi, meningkatkan dokumentasi dan panduan pengguna

VI. DAFTAR PUSAKA

[1] S. E. Ghrare, M. A. Abouras, and I. A. Akermi, "Development of Hybrid Data Security System using LSB Steganography and AES Cryptography," 2023.

[2] F. Baso, "Performance Analysis of The Last Significant Bit (LSB) Method in Steganography for Data Hiding in Image Data," *Computer, Information, Embedded, Network, and Intelligence System*, vol. 1, no. 1, p. 2023, [Online]. Available: https://journal.lontaradigitech.com/SCIENTIST

[3] M. Miftahul Amri, M. Waeno, and M. Zain Musa, "LSB Steganography to Embed Creator's Watermark in Batik Digital Arts," *Engineering Science Letter*, vol. 2, no. 01, pp. 27–32, Mar. 2023, doi: 10.56741/esl.v2i01.301.

[4] E. Phyu, S. Win, and A. History, "Data Hiding to Image Smart Phone Using AES and LSB Algorithms ARTICLE INFO ABSTRACT." [Online]. Available: www.jcsts.one

[5] R. S. Hameed, S. S. Mokri, M. S. Taha, and M. M. Taher, "High Capacity Image Steganography System based on Multi-layer Security and LSB Exchanging Method," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 8, pp. 108–115, 2022, doi: 10.14569/IJACSA.2022.0130814.

[6] Y. Moussa and W. Alexan, "Message Security through AES and LSB Embedding in Edge Detected Pixels of 3D Images," in *2nd Novel Intelligent and Leading Emerging Sciences Conference, NILES 2020*, Institute of Electrical and Electronics Engineers Inc., Oct. 2020, pp. 224–229. doi: 10.1109/NILES50944.2020.9257937.

[7] P. Gaur, "AES Image Encryption (Advanced Encryption Standard)," *Int J Res Appl Sci Eng Technol*, vol. 9, no. 12, pp. 1357–1363, Dec. 2021, doi: 10.22214/ijraset.2021.39542.

[8] A. Hamdy, "Image Processing and AES for Secure Communications Bachelor Thesis", doi: 10.13140/RG.2.2.36193.22884.

[9] A. Davy Wiranata and R. T. Aldisa, "Aplikasi Steganografi Menggunakan Least Significant Bit (LSB) dengan Enkripsi Caesar Chipper dan Rivest Code 4 (RC4) Menggunakan Bahasa Pemrograman JAVA," *Jurnal Teknologi Informasi dan Komunikasi)*, vol. 5, no. 3, p. 2021, 2021, doi: 10.35870/jti.

[10] N. Sofian, A. Wicaksana, and S. Hansun, "LSB steganography and AES encryption for multiple PDF documents," in *Proceedings of 2019 5th International Conference on New Media Studies, CONMEDIA 2019*, Institute of Electrical and Electronics Engineers Inc., Oct. 2019, pp. 100–105. doi: 10.1109/CONMEDIA46929.2019.8981842.

E-ISSN: 2985-3532