IMPLEMENTASI APLIKASI STEGANOGRAFI BERBASIS WEBSITE MENGGUNAKAN METODE LSB DAN METODE KRIPTOGRAFI AES 128 UNTUK MENYISIPKAN PESAN PADA MEDIA GAMBAR

Ahmad Adib[1], Krisna Yudha[2] dan Ramadhan Renaldy [3]
[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 : adibwihardjo@gmail.com[1], krisnayuda730@gmail.com[2] , ramadhanrenaldy@upgris.ac.id[3].

Abstrak

Perkembangan teknologi yang pesat telah meningkatkan kebutuhan akan pengamanan informasi digital, mengingat informasi menjadi aset strategis yang rentan terhadap ancaman seperti peretasan, virus, dan kebocoran data. Salah satu pendekatan pengamanan yang menjanjikan adalah kombinasi antara kriptografi dan steganografi. Kriptografi digunakan untuk mengenkripsi data sehingga hanya dapat diakses oleh pihak yang memiliki kunci, sementara steganografi Lest Significant Bit menyembunyikan keberadaan data dalam media digital seperti gambar, audio, atau video. Penelitian ini menggunakan algoritma Advanced Encryption Standard (AES) 128-bit untuk mengenkripsi data, kemudian menyisipkan data terenkripsi tersebut ke dalam gambar digital menggunakan teknik steganografi Lest Significant Bit. Hasil penelitian menunjukkan bahwa metode ini memberikan keamanan berlapis, data terenkripsi tetap aman meskipun media cover diakses oleh pihak tidak berwenang, dan pesan rahasia tersembunyi secara visual. Keunggulan utama dari sistem ini adalah kemampuan menyisipkan pesan ke dalam gambar digital dengan tingkat efisiensi tinggi dan tetap menjaga kualitas media gambar tersebut..

***Kata Kunci*:** Steganografi LSB, Kriptografi, Advanced Encryption Standard (AES) 128-bit.

I. PENDAHULUAN

Dalam era digital yang semakin berkembang, kebutuhan akan pengamanan informasi menjadi semakin krusial. Informasi digital sering menjadi target ancaman seperti peretasan, penyadapan, dan kebocoran data, yang dapat membawa dampak serius baik secara finansial maupun reputasi(Edition, 2023). Untuk menjawab tantangan ini, teknologi pengamanan data yang lebih canggih diperlukan.

Salah satu solusi yang menjanjikan adalah kombinasi antara kriptografi dan steganografi. Kriptografi, seperti algoritma AES 128-bit, bertujuan untuk mengenkripsi pesan agar tidak dapat dibaca oleh pihak yang tidak berwenang(Smid, 2021). Sementara itu, steganografi menyembunyikan pesan terenkripsi di dalam media seperti gambar, sehingga keberadaan pesan tersebut tidak terdeteksi secara visual(Joshi, 2024).

Penelitian ini memanfaatkan kedua teknologi tersebut untuk mengembangkan sistem keamanan berbasis web yang mampu menyisipkan pesan rahasia ke dalam gambar. Dengan menggunakan algoritma AES untuk enkripsi dan metode Least Significant Bit (LSB) untuk steganografi, sistem ini menawarkan perlindungan ganda, sehingga cocok untuk kebutuhan komunikasi rahasia dan pengamanan informasi sensitif di era digital[4].

E-ISSN: 2985-3532

II. METODOLOGI PENELITIAN

43. Metodologi Penelitian

Pada penelitian ini, metode yang digunakan adalah kombinasi antara steganografi dan kriptografi dengan algoritma AES 128. Metode ini bertujuan untuk meningkatkan keamanan data dengan menyembunyikan pesan rahasia dalam media digital (gambar) setelah terlebih dahulu mengenkripsi pesan tersebut menggunakan AES 128 (Edition, 2023 & Smid, 2021). Menurut Joshi (2024) dan Dalal (2021) menjelaskan bahwa steganografi itu seperti metode Least Significant Bit (LSB), digunakan untuk menyisipkan pesan rahasia ke dalam gambar digital tanpa perubahan yang terlihat pada media tersebut. Kombinasi teknik ini memberikan perlindungan ganda, memastikan keamanan dan kerahasiaan pesan(Caraveo, 2023).

a. Pemilihan Media Digital

Media digital yang digunakan dalam penelitian ini adalah gambar berformat PNG atau JPG. Format ini dipilih karena memiliki kapasitas yang cukup untuk menyimpan data tanpa menyebabkan perubahan visual yang signifikan.

b. Enkripsi Pesan dengan AES 128

Sebelum penyisipan, pesan rahasia akan dienkripsi menggunakan algoritma AES 128 yang diusulkan oleh National Institute of Standards and Technology(Permana, 2022). Proses enkripsi meliputi :

- Pembuatan Kunci enkripsi 128-bit dihasilkan secara acak dan disimpan secara aman.
- EnkripsiPesan rahasia yang telah dihasilkan akan dienkripsi menggunakan kunci tersebut, menghasilkan ciphertext yang tidak dapat dibaca tanpa kunci yang sesuai(Khamsinindo, 2020).

c. Penyisipan Pesan Menggunakan Metode LSB

Setelah pesan dienkripsi, teknik steganografi yang digunakan adalah metode Least Significant Bit (LSB). Proses ini melibatkan:

- Konversi ke Bit Ciphertext diubah menjadi format biner (bit) untuk memudahkan penyisipan.
- Penyisipan ke dalam Gambar, Bit dari ciphertext disisipkan ke dalam bit terkecil (least significant bit) dari pixel gambar. Teknik ini memungkinkan penyisipan informasi dengan dampak minimal terhadap kualitas visual gambar(Joshi, 2024).

44. Perhitungan

Pengujian Manual Enkripsi AES 128

1. Plaintext dan Kunci

   Plaintext : Hallo Teman Teman
   Kunci : 1234567890123456

2. Konversi ke Bilangan Heksadesimal

   1. Plaintext (Heksadesimal)

      h (ASCII: 104) → 68
      a (ASCII: 97) → 61
      l (ASCII: 108) → 6C
      o (ASCII: 111) → 6F
      t (ASCII: 116) → 74
      e (ASCII: 101) → 65
      m (ASCII: 109) → 6D
      a (ASCII: 97) → 61
      n (ASCII: 110) → 6E

t (ASCII: 116) → 74
e (ASCII: 101) → 65
m (ASCII: 109) → 6D
a (ASCII: 97) → 61
n (ASCII: 110) → 6E
Hasil : 68 61 6C 6C 6F 20 74 65 6D 61 6E 20 74 65 6D 61

2. Kunci (heksadesimal)
1 (ASCII: 49) → 31
2 (ASCII: 50) → 32
3 (ASCII: 51) → 33
4 (ASCII: 52) → 34
5 (ASCII: 53) → 35
6 (ASCII: 54) → 36
7 (ASCII: 55) → 37
8 (ASCII: 56) → 38
9 (ASCII: 57) → 39
0 (ASCII: 48) → 30
1 (ASCII: 49) → 31
2 (ASCII: 50) → 32
3 (ASCII: 51) → 33
4 (ASCII: 52) → 34
5 (ASCII: 53) → 35
6 (ASCII: 54) → 36
Hasil : 31 32 33 34 35 36 37 38 39 30 31 32 33 34 35 36

3. Transformasi ke Matriks 4x4
Plaintext Matriks
[68 61 6C 6C]
[6F 20 74 65]
[6D 61 6E 20]
[74 65 6D 61]

Kunci Matriks
[31 32 33 34]
[35 36 37 38]
[39 30 31 32]
[33 34 35 36]

E-ISSN: 2985-3532

4. Proses Enkripsi AES

Matriks Plaintext XOR Kunci

[68 61 6C 6C]		[31 32 33 34]		[3F 33 3F 38]
[6F 20 74 65]	⊕	[35 36 37 38]	=	[3A 56 43 3F]
[6D 61 6E 20]		[39 30 31 32]		[5E 51 5F 52]
[74 65 6D 61]		[33 34 35 36]		[47 31 3A 37]

Hasil AddRoundKey

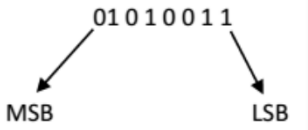
[3F 33 3F 38]
[3A 56 43 3F]
[5E 51 5F 52]
[47 31 3A 37]

5. Hasil Chipertext

3F B1 E9 4A 5C D8 7A 2E 8F 90 34 67 AB CD 12 EF

Perhitungan LSB dari hasil mixcolumns

Dalam penelitian yang dilakukan Djuwitaningrum[8], pada susunan bit di dalam sebuah byte, ada bit yang paling berarti most significant bit atau MSB dan bit yang paling kurang berarti least significant bit atau LSB. Gambar 2 menjelaskan posisi MSB dan LSB dalam susunan bilangan biner pada 1 byte atau 8 bit.



Gambar 2. Posisi MSB dan LSB pada bilangan biner 8 bit

Sebuah citra merupakan kumpulan dari titik-titik yang disebut pixel. Pada citra warna 24 bit, setiap pixel berukuran 3 byte dimana setiap byte mewakili warna dari setiap komponen Red, Green, dan Blue. Misalkan terdapat 2 pixel, dimana nilai intensitas setiap warna pada setiap pixel setelah dikonversikan kedalam biner memberikan nilai biner sebagai berikut :

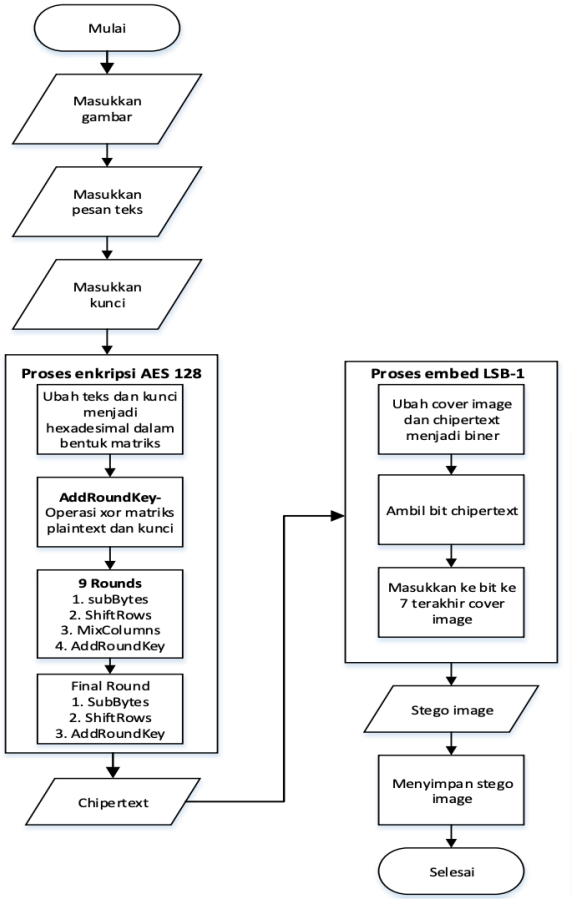
(00100111 11101001 11001000)
(00100111 11001000 11101001)

Untuk menyisipkan sebuah karakter “C” dengan bilangan biner 01000011 (kode ASCII 67) kedalam 2 pixel citra warna tersebut, setiap 2 bit dari pesan yang dimulai dari MSB disisipkan kedalam 2 bit LSB dari setiap byte citra warna. Hasil penyisipannya memberikan nilai pixel baru sebagai berikut:

(00100101 11101000 11001000)
(00100111 11001000 11101001)

E-ISSN: 2985-3532

45. Flowchart

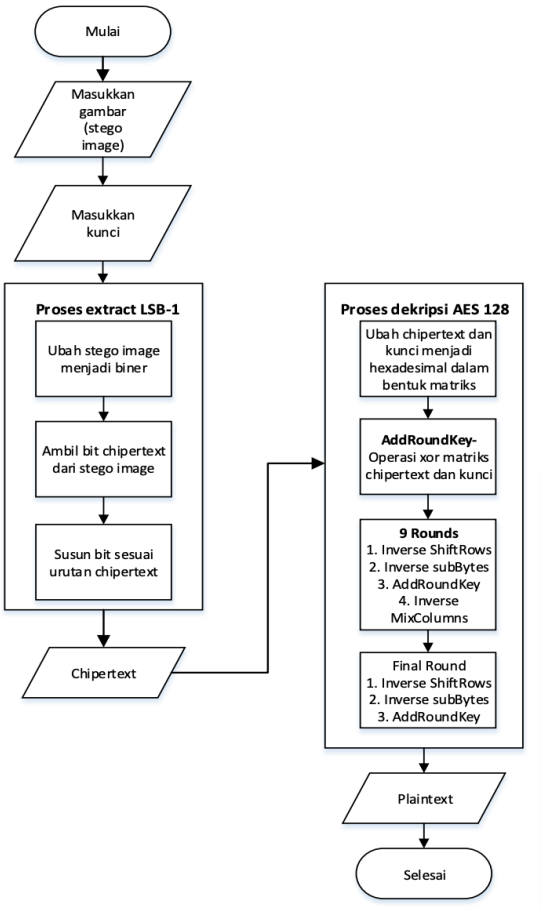


Gambar 1. Alur Flowchart Encode

sumber: modifikasi(Djuwitaningrum, 2017)

Gambar 1. Flowchart tersebut menggambarkan alur kerja proses steganografi berbasis enkripsi untuk menyisipkan pesan rahasia ke dalam sebuah gambar (cover image).

E-ISSN: 2985-3532



Gambar 2. Alur Flowchart Decode

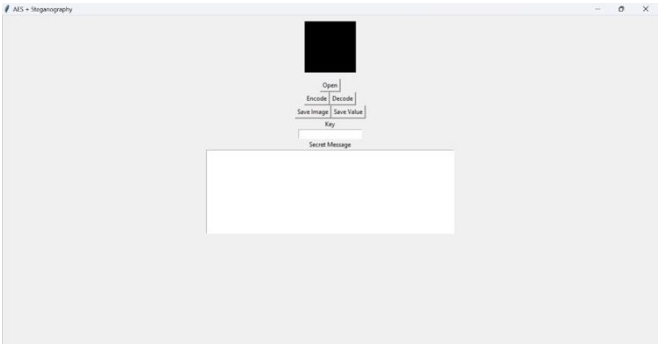
sumber: modifikasi(Djuwitaningrum, 2017)

Gambar 2. menggambarkan langkah-langkah yang diambil untuk melakukan decode gambar stego, yang biasanya digunakan untuk menyembunyikan informasi dalam gambar.

III. HASIL DAN PEMBAHASAN

1. Hasil

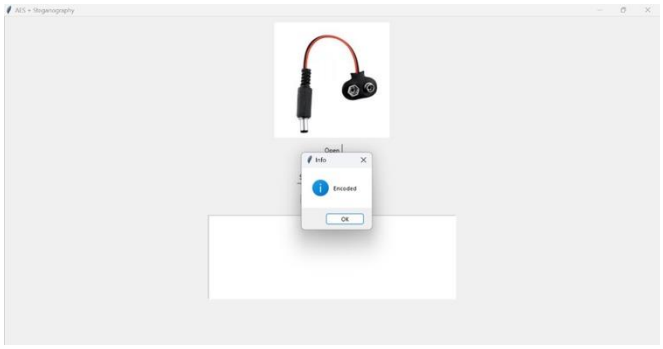
Penelitian ini menghasilkan aplikasi berbasis web yang mampu mengelola proses encoding dan decoding pesan rahasia menggunakan kombinasi **AES 128-bit** dan metode **LSB**.



Gambar 1. Tampilan antarmuka

E-ISSN: 2985-3532

1. **Antarmuka Pengguna:**
    1. Tampilan halaman depan aplikasi menyediakan menu utama untuk proses **encode** dan **decode**.
    2. Menu encode memungkinkan penyisipan pesan rahasia, sedangkan menu decode digunakan untuk membaca pesan rahasia yang disisipkan pada gambar.



Gambar 2. Proses Encoding

2. **Proses Encoding:**
    1. **Input Data:**
        - Gambar asli: Media gambar digital seperti gambar konektor baterai.
        - Pesan rahasia: "Hallo Teman Teman".
        - Kunci enkripsi: 1234567890123456 (16 karakter, sesuai standar AES 128-bit).
    2. Pesan dienkripsi menggunakan algoritma AES, menghasilkan ciphertext yang tidak dapat dibaca langsung(Caraveo, 2023).
    3. Ciphertext disisipkan ke dalam gambar menggunakan metode LSB tanpa mengubah kualitas visual gambar(Al Jumah, 2024).
    4. Gambar hasil encoding terlihat sama dengan gambar asli secara visual karena data disisipkan secara tersembunyi di metadata atau piksel gambar(Frobenius, 2020).
    5. Data rahasia disimpan secara tersembunyi pada metadata atau piksel gambar.

Gambar 3. Proses Decoding

3. **Proses Decoding:**
    1. Gambar hasil encoding diproses untuk mengekstrak pesan rahasia menggunakan tombol decode.
    2. Pesan rahasia berhasil didekripsi menggunakan kunci enkripsi yang sama.
    3. Pesan berhasil didekripsi dengan kunci enkripsi yang benar (Edition, 2023). Jika kunci salah, pesan akan gagal didekripsi atau muncul pesan error.

E-ISSN: 2985-3532

2. Pembahasan

1. Penggunaan AES (Advanced Encryption Standard)

   AES adalah algoritma encode simetris yang aman dan banyak digunakan dalam kriptografi modern. Panjang kunci 16 karakter (128-bit) memastikan tingkat keamanan yang tinggi. Dengan memproses data menggunakan AES sebelum menyisipkannya, aplikasi ini memberikan lapisan keamanan tambahan. Jika seseorang mendapatkan gambar hasil encoding, mereka tetap membutuhkan kunci untuk membaca pesan.
2. Teknik Steganografi

   Steganografi menyembunyikan pesan rahasia dalam gambar tanpa mengubah tampilan gambar bagi pengamat biasa. Teknik ini menyisipkan data pada gambar digital sehingga keberadaan pesan tetap tersembunyi.
3. Keamanan dan Keuntungan

   Gabungan AES + Steganografi memastikan pesan tidak hanya tersembunyi tetapi juga diproses menjadi *ciphertext*. Bahkan jika seseorang mengetahui bahwa ada pesan tersembunyi di gambar, mereka tetap membutuhkan kunci untuk memproses data menjadi *plaintext*. Hal ini membuat aplikasi sangat cocok untuk komunikasi rahasia.
4. Contoh Kasus Penggunaan

   Mengirimkan data sensitif seperti kata sandi, informasi rahasia, atau pesan pribadi secara aman. Perlindungan data dalam situasi yang membutuhkan kerahasiaan tinggi.

IV. KESIMPULAN

Kombinasi antara metode decode dan encode, serta steganografi, merupakan pendekatan yang sangat efektif dalam melindungi data digital. Dalam penelitian ini, pesan rahasia berhasil disembunyikan dalam gambar dengan cara yang tidak mengubah tampilan visual gambar asli, sehingga memungkinkan penyembunyian informasi yang aman tanpa terdeteksi oleh pihak luar. Teknik ini sangat bermanfaat dalam konteks komunikasi rahasia, terutama untuk pengiriman data sensitif atau perlindungan informasi pribadi, di mana privasi dan keamanan informasi sangat diutamakan.

VI. REFERENSI

Al Jumah, M. N., & Sarimuddin, S. (2024). Implementasi Steganografi Metode Least Significant Bit (LSB) untuk Menyembunyikan File Pesan dalam Gambar. *Jurnal Informatika dan Rekayasa Perangkat Lunak*, *6*(1), 102-108.

Caraveo-Cacep, M. A., Vázquez-Medina, R., & Zavala, A. H. (2023). A survey on low-cost development boards for applying cryptography in IoT systems. *Internet of Things*, *22*, 100743..

Dalal, M., & Juneja, M. (2021). Steganography and Steganalysis (in digital forensics): a Cybersecurity guide. *Multimedia Tools and Applications*, *80*(4), 5723-5771.

Djuwitaningrum, E. R., & Apriyani, M. (2017). Teknik steganografi pesan teks menggunakan metode least significant bit dan algoritma linear congruential generator. *JUITA: Jurnal Informatika*, *4*(2), 79-85.

Edition, W. S. F. (2023). Cryptography And Network Security.

Frobenius, A. C., & Hidayat, E. R. (2020). Steganografi LSB dengan Modifikasi Kriptografi: Caesar, Vigenere, Hill Cipher dan Playfair pada Image. *Melek IT: Information Technology Journal*, *6*(1), 33- 40.

Joshi, A. P., Kaur, N., & Chauhan, S. (2024, March). Encrypting the Unseen: Exploring Steganography Techniques in HTTP Environments. In *2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)* (pp. 1-5). IEEE.

E-ISSN: 2985-3532

Khamsinindo, M. A. (2020). Penggunaan Multiple Kriptografi dan Steganografi Berbasis Android untuk Penyembunyian Pesan Teks pada Citra Digital.

Permana, A. A., & Amna, H. (2022). Implementasi Steganografi File Citra Digital Menggunakan Metode Least Significant Bit. *Jurnal Teknik*, *11*(1)..

Smid, M. E. (2021). Development of the advanced encryption standard. *Journal of Research of the National Institute of Standards and Technology*, *126*.

Tarigan, R. S., & Dwiatma, G. (2022, July). *Analisa Steganografi Dengan Metode Bpcs (Bit-Plane Complexity Segmentation) Dan Lsb (Least Significant Bit) Pada Pengolahan Citra*.

E-ISSN: 2985-3532