Jurnal Elektronik Ilmu Komputer Udayana
Volume 13, No 2. November 2024

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Optimalisasi Keamanan Data Digital melalui Kombinasi Metode *AES* dan *Bit-Plane Complexity Segmentation*

Luh Gede Tresna Dewi[a1], Ngurah Agus Sanjaya ER[a2], I Komang Ari Mogi [a3], I Gede Surya Rahayuda [a4]

[a]Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Udayana
Badung, Bali, Indonesia

[1]trsdewi37@gmail.com@email.com
[2]agus_sanjaya@unud.ac.id
[3]arimogi@unud.ac.id
[4]igedesuryarahayuda@unud.ac.id

Abstrak

Di era digital informasi yang dipertukarkan melalui media digital sering kali bersifat sensitif dan dapat menimbulkan dampak serius jika jatuh ke tangan yang salah. Oleh karena itu, memastikan keamanan informasi adalah hal yang sangat penting. Salah satu metode yang banyak digunakan untuk melindungi informasi adalah kriptografi. Meskipun kriptografi memberikan tingkat keamanan yang tinggi, ada kelemahan dimana pesan terenkripsi masih dapat terlihat dan memicu kecurigaan pihak yang tidak berwenang. Untuk mengatasi kelemahan ini, steganografi digunakan sebagai solusi alternatif. Penelitian ini mengamankan data digital dengan mengkombinasikan metode kriptografi Advanced Encryption Standard (AES) dan steganografi Bit-Plane Complexity Segmentation (BPCS). Pesan teks dienkripsi menggunakan algoritma AES-128 bit, kemudian disisipkan ke dalam gambar melalui algoritma steganografi BPCS. Pengujian menunjukkan bahwa gambar hasil steganografi (stego image) memiliki kualitas visual tinggi dengan rata-rata nilai Peak Signal-to-Noise Ratio (PSNR) sebesar 76,768 dB dan Mean Square Error (MSE) rendah antara 0,00001 hingga 0,00271, yang mengindikasikan perubahan minimal pada gambar asli. Tingkat Avalanche effect (AE) dari algoritma AES-128 bit bervariasi antara 46,48% hingga 55,08%, dengan rata-rata keseluruhan 50,31%, menunjukkan respons yang baik terhadap perubahan kunci. Hasil penelitian ini menunjukkan bahwa kombinasi metode AES dan BPCS efektif dalam mengamankan data dan menjaga kualitas visual media digital.
.

Kata kunci: *Keamanan Data, Kriptografi, Steganografi, Advanced Encryption Standard, Bit-Plane Complexity Segmentation*

1. Pendahuluan

Di era digital yang terus berkembang, pertukaran informasi telah menjadi bagian tak terpisahkan dari aktivitas sehari-hari. Media digital memungkinkan pertukaran informasi menjadi lebih cepat, lebih mudah, dan lebih luas dalam cakupannya. Namun, kemudahan ini juga menimbulkan tantangan baru terkait keamanan informasi. Informasi yang dipertukarkan melalui media digital sering kali bersifat sensitif dan dapat memiliki dampak signifikan jika jatuh ke tangan yang salah. Oleh karena itu, penting untuk memastikan bahwa informasi tersebut diamankan dengan baik selama proses pertukaran. Permasalahan utama yang dihadapi dalam pertukaran informasi digital adalah bagaimana memastikan informasi tetap aman dan tidak dapat diakses oleh pihak yang tidak berwenang. Salah satu pendekatan yang umum digunakan untuk menjaga keamanan informasi adalah melalui penggunaan metode kriptografi. Kriptografi merupakan ilmu yang mempelajari teknik teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi [1]. Namun, meskipun pesan telah dienkripsi dengan kriptografi, keberadaannya masih terlihat dan dapat menimbulkan kecurigaan dari pihak

yang tidak berwenang. Untuk mengatasi masalah ini, steganografi digunakan sebagai metode tambahan. Steganografi merupakan teknik penyembunyian pesan yang memanfaatkan kekurangan sistem indera manusia seperti mata (*human visual system*) dan telinga *(human auditory system*) [2]. Pada steganografi informasi disembunyikan dalam media lain sehingga keberadaan informasi tersebut tidak terlihat. Dengan menggunakan kriptografi dan steganografi bersama-sama, diharapkan tingkat keamanan informasi dapat ditingkatkan secara signifikan.

Pada penelitian terdahulu telah digunakan metode RSA bersama dengan teknik *Bit-Plane Complexity Segmentation* (BPCS) untuk menyisipkan informasi rahasia ke dalam gambar. Metode ini memanfaatkan kemampuan RSA dalam mengenkripsi data dan kapasitas penyisipan BPCS yang tinggi. Hasil penelitian tersebut menunjukkan bahwa kombinasi kedua metode ini berhasil meningkatkan keamanan informasi. Namun, kelemahan yang ditemukan adalah kompleksitas perhitungan dan kebutuhan sumber daya yang tinggi saat menggunakan RSA. Untuk mengatasi kelemahan tersebut, penelitian ini memilih untuk menggunakan algoritma *Advanced Encryption Standard* (AES) sebagai pengganti RSA. AES merupakan algoritma kriptografi simetris yang artinya kunci enkripsi sama dengan kunci dekripsi sehingga dalam prosesnya tidak membutuhkan sumber daya yang besar. Berdasarkan hasil pada penelitian terdahulu waktu yang dibutuhkan untuk proses enkripsi menggunakan algoritma AES dibuktikan lebih cepat dibandingkan RSA [3]. Metode *Bit-Plane Complexity Segmentation* (BPCS) tetap digunakan dalam penelitian ini karena kemampuan penyisipan data yang tinggi dan kehandalannya dalam menyembunyikan data dalam gambar. Kombinasi antara AES dan BPCS diharapkan dapat menciptakan sistem yang lebih efisien dalam melindungi informasi sensitif selama pertukaran digital. Penelitian ini bertujuan untuk mengevaluasi dan mengoptimalkan kombinasi AES dan BPCS sehingga dapat menghasilkan sistem perlindungan informasi yang lebih baik.

2. Metode Penelitian

2.1 Data dan Metode Pengumpulan Data

a. Data gambar yang digunakan dalam penelitian ini diperoleh dari dataset publik yang tersedia di platform Kaggle. Dataset tersebut berisi gambar-gambar yang diambil dalam berbagai kondisi dan situasi pencahayaan. Gambar yang digunakan dalam penelitian ini adalah gambar dengan format .png. Setiap gambar dalam dataset ini telah dipilih untuk memastikan keberagaman dan representativitas dari berbagai kondisi.

b. Data *plaintext* terdiri dari teks dalam format .txt yang dibuat secara acak. Masing-masing data *plaintext* akan disisipkan kedalam gambar.

c. Data kunci enkripsi terdiri dari kunci yang juga dibuat secara acak. Setiap kunci enkripsi memiliki panjang tetap yaitu 128-bit dan digunakan untuk mengenkripsi masing-masing teks *plaintext*.

2.2 Analisis Kebutuhan

Analisis kebutuhan merupakan proses penentuan kebutuhan atau kondisi yang harus dipenuhi dalam merancang dan membangun aplikasi penyisipan pesan pada gambar menggunakan algoritma *Advanced Encryption Standard* dan *Bit-Plane Complexity Segmentation*.

a. Analisis Kebutuhan Masukan

Kebutuhan masukan dibagi menjadi masukan untuk proses embedding dan masukan untuk proses ekstraksi. Masing masing proses memiliki kebutuhan berbeda sebagai berikut :

1. Proses Penyisipan

Sebelum proses penyisipan dilakukan, metode enkripsi AES (*Advanced Encryption Standard*) akan digunakan untuk mengamankan pesan rahasia sebelum disisipkan ke dalam data gambar. Setelah itu, data terenkripsi akan disisipkan ke dalam gambar yang diambil dari dataset Kaggle. Gambar yang digunakan berasal dari berbagai kondisi dan situasi pencahayaan, dengan gambar dalam format .png.

p-ISSN: 2301-5373
e-ISSN: 2654-5101

2. Proses Ekstraksi

   Algoritma steganografi yang dikembangkan dalam penelitian ini akan digunakan untuk mengekstrak pesan rahasia yang tersembunyi di dalam gambar. Setelah proses penyisipan selesai, gambar stego yang dihasilkan akan diproses dengan algoritma ekstraksi untuk mendapatkan kembali pesan rahasia yang telah disisipkan. Setelah berhasil diekstrak, pesan rahasia tersebut akan didekripsi menggunakan metode AES untuk mendapatkan pesan asli yang telah dienkripsi sebelumnya.

b. Analisis Kebutuhan Keluaran

Keluaran yang didapatkan dari masing masing proses diatas adalah sebagai berikut:

1. Gambar Steggo

   Gambar stego adalah file gambar yang diperoleh setelah proses penyisipan. Gambar ini menampung teks rahasia yang ingin disembunyikan oleh pengguna.

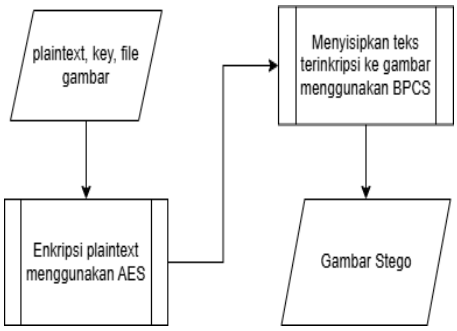
2. Teks Rahasia

   Teks rahasia adalah hasil keluaran dari proses extracting pada gambar stego. Teks rahasia merupakan file teks yang disembunyikan pada gambar dan dikembalikan ke bentuk aslinya setelah proses dekripsi.

2.3 Perancangan Sistem

a. Alur Penyisipan Teks

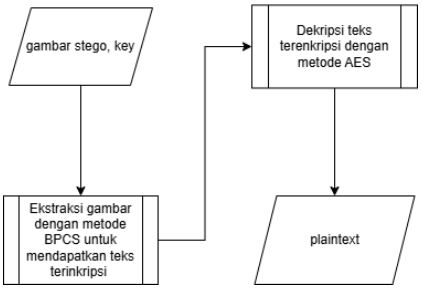
Langkah-langkah penyisipan pesan ke dalam gambar dapat dilihat pada sketsa diagram pada gambar 1.



Gambar 1. Ilustrasi Proses Penyisipan Teks

Proses penyisipan diawali dengan memasukan file *plaintext*, file gambar, dan kunci enkripsi. Berikutnya sistem akan melakukan enkripsi pada *plaintext* menggunakan algoritma AES-128. Selanjutnya, pesan yang dienkripsi (chipertext) disisipkan ke dalam gambar.

b. Alur Ekstraksi Gambar Stego

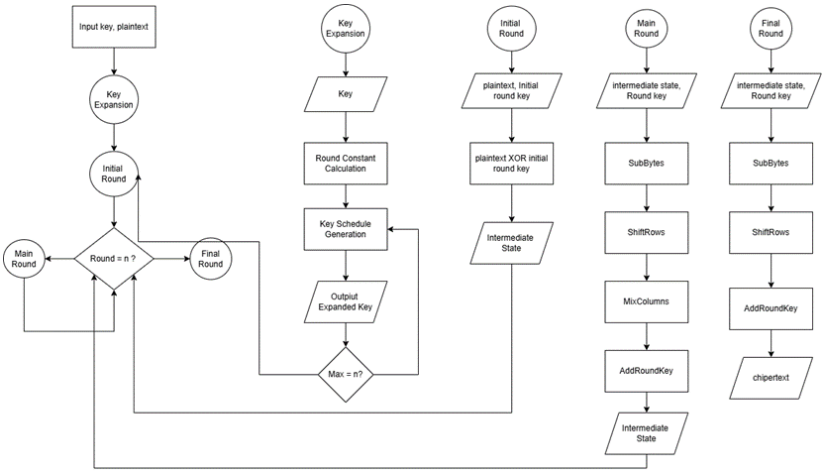


Gambar 2. Ilustrasi Proses Ekstraksi Gambar Stego

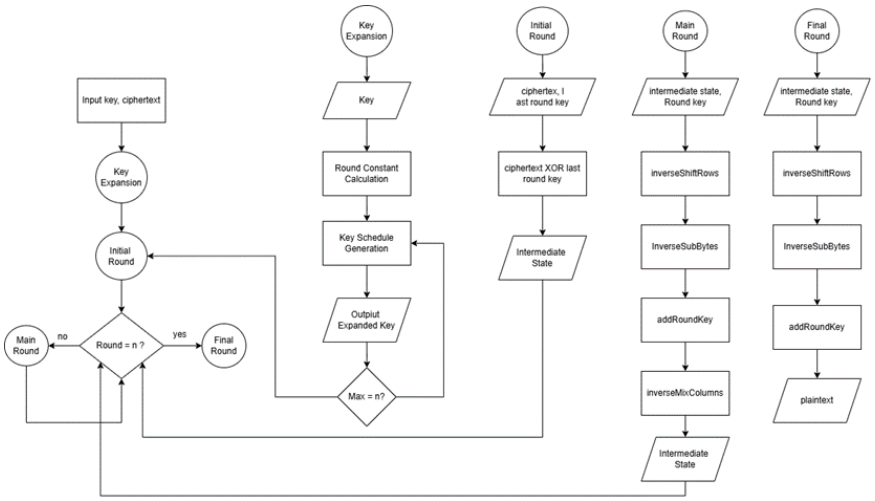
Proses ekstraksi diawali dengan memasukan gambar stego dan kunci dekripsi yang sama dengan kunci enkripsi. Berikutnya sistem akan melakukan ekstraksi chipertext pada file gambar. Setelahnya akan dilakukan dekripsi chipertext menggunakan algoritma AES-128, maka akan dihasilkan *plaintext*. Langkah-langkah penyisipan pesan ke dalam gambar dapat dilihat pada sketsa diagram pada gambar 2.

c. Alur Algoritma *Advanced Encryption Standard*

Algoritma *Advanced Encryption Standard* (AES) adalah algoritma enkripsi simetris. Panjang kunci yang digunakan dalam penelitian ini yaitu 128-bit. Kunci tersebut digunakan untuk proses enkripsi dan dekripsi. Alur Enkripsi algoritma AES-128bit dapat dilihat pada gambar 3 dan Alur dekripsi dapat dilihat pada gambar 4.



Gambar 3. Alur Enkripsi Algoritma AES



Gambar 1 Alur Dekripsi Algoritma AES

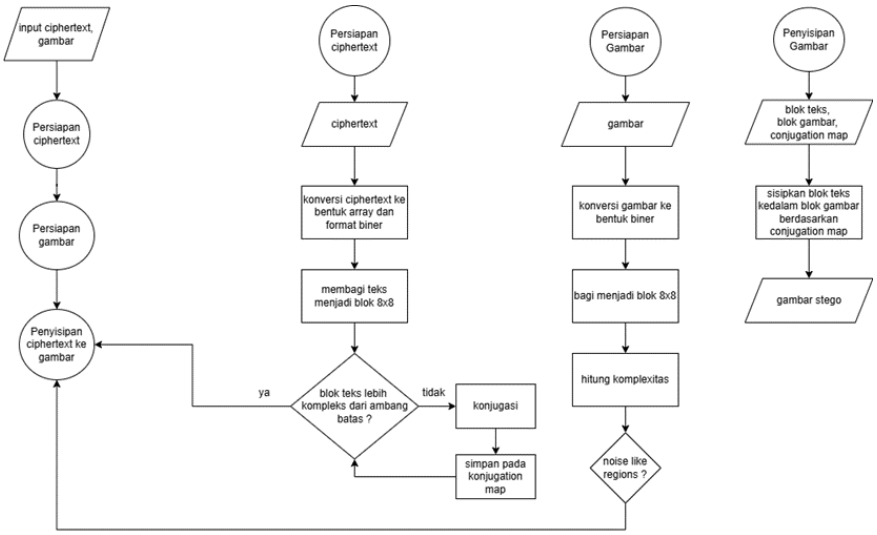
Kunci algoritma AES didapatkan melalui proses inisialisasi dan pengelompokan kunci, yang melibatkan penggunaan kunci awal yang diberikan dan langkah-langkah tambahan untuk menghasilkan kunci tambahan yang akan digunakan dalam setiap putaran algoritma AES. Proses enkripsi algoritma AES terdiri dari 4 jenis transformasi bytes, yaitu *SubBytes, ShiftRows, MixColumns, dan AddRoundKey*. Pada awal proses enkripsi, input yang telah disalin ke dalam state akan mengalami transformasi byte *AddRoundKey.* Setelah itu, state akan mengalami transformasi *SubBytes, ShiftRows, MixColumns,* dan *AddRoundKey* secara berulang-ulang sebanyak Nr. Proses ini dalam algoritma AES disebut sebagai round function. Round yang terakhir agak berbeda dengan round-round sebelumnya dimana pada round terakhir, state tidak mengalami transformasi

p-ISSN: 2301-5373
e-ISSN: 2654-5101

MixColumns. Sedangkan untuk proses dekripsi untuk mendapatkan kembali teks yang telah dienkripsi maka proses dilakukan secara terbalik dari proses enkripsi.

d. Alur Algoritma *Bit-Plane Complexity Segmentation*

Algoritma BPCS (*Bit-Plane Complexity Segmentation*) adalah salah satu metode dalam steganografi, yaitu teknik menyembunyikan informasi dalam media digital. Algoritma ini bekerja dengan menyisipkan pesan rahasia ke dalam gambar digital dengan memanfaatkan kompleksitas bit-plane dari gambar tersebut. Bit-plane dalam gambar digital mengacu pada lapisan data biner yang mewakili setiap bit dari nilai piksel gambar. Alur proses penyisipan dari algoritma *Bit-Plane Complexity Segmentation* dapat dilihat pada gambar 5.



Gambar 2. Alur Penyisipan Algoritma BPCS

1. Gambar yang akan disisipi data dibaca dan dikonversi menjadi array numpy dan teks rahasia yang akan disisipkan juga dibaca dan dikonversi menjadi array numpy dengan menambahkan padding agar ukuran sesuai.
2. Setiap piksel dalam gambar dikonversi ke representasi biner (*bit-plane*). Dalam bit-plane, setiap bit dari nilai piksel diubah menjadi satu bidang terpisah.
3. Bit-plane yang telah dibuat kemudian diubah dari mode *Plain Binary Code* (PBC) menjadi *Canonical Gray Code* (CGC). Hal ini dilakukan untuk meningkatkan daya tahan terhadap perubahan pada gambar.
4. Bit-plane dibagi menjadi blok-blok kecil sesuai dengan ukuran yang telah ditentukan. Yaitu, blok-blok berukuran 8x8 piksel.
5. Kompleksitas setiap blok dalam bit-plane dihitung. Kompleksitas ini diukur berdasarkan jumlah transisi bit 0 ke 1 dan 1 ke 0 di dalam blok.
6. Ambang batas kompleksitas ditentukan yaitu 4,5. Blok dengan kompleksitas di bawah ambang batas ini dianggap sebagai area "*noise-like*" dan cocok untuk penyisipan data.
7. Blok-blok dengan kompleksitas di bawah ambang batas diubah (dikonjugasi) untuk meningkatkan kompleksitasnya. Ini dilakukan untuk memastikan bahwa blok-blok yang akan disisipi data terlihat seperti "*noise*".
8. Pesan rahasia dibagi menjadi blok-blok yang sesuai ukuran. Blok-blok pesan ini kemudian disisipkan ke dalam blok-blok gambar yang telah dipilih berdasarkan kompleksitasnya. Jika blok yang akan disisipi memiliki kompleksitas di bawah ambang batas, blok ini dikonjugasi sebelum disisipi data.

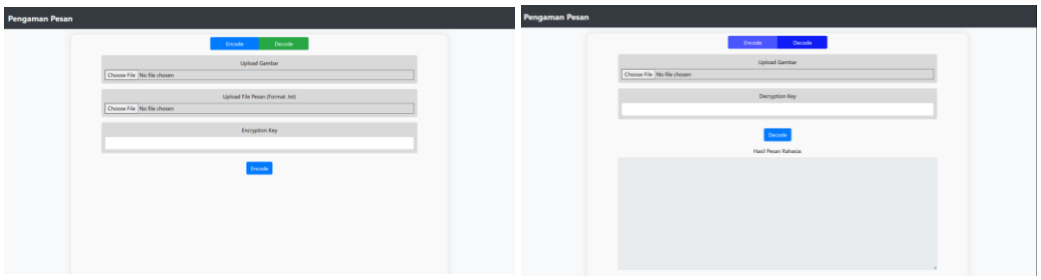
9. Setelah data disisipkan, bit-plane diubah kembali dari CGC ke PBC. Bit-plane yang telah dimodifikasi digabungkan kembali menjadi array gambar asli.

Untuk mendapatkan kembali data yang telah disisipkan maka perlu dilakukan ekstraksi Alur proses ekstraksi dari algoritma *Bit-Plane Complexity Segmentation* yaitu:

1. Gambar yang telah disisipi data dibaca dan dikonversi menjadi array numpy.
2. Gambar yang telah disisipi data dikonversi kembali menjadi *bit-plane*.
3. Bit-plane diubah dari mode CGC kembali ke mode PBC.
4. Bit-plane dibagi menjadi blok-blok kecil sesuai dengan ukuran yang telah ditentukan.
5. Blok-blok yang telah disisipi data diidentifikasi berdasarkan kompleksitasnya. Jika blok tersebut dikonjugasi selama penyisipan, maka blok tersebut harus didekonjugasi.
6. Data rahasia diekstraksi dari blok-blok yang sesuai. Data yang diekstraksi kemudian digabungkan untuk membentuk pesan rahasia asli.
7. Padding yang ditambahkan selama penyisipan data dihapus untuk mendapatkan pesan asli tanpa tambahan data.

e. Perancangan Desain Antarmuka Sistem

Perancangan desain antarmuka adalah suatu proses untuk mendesain tampilan antarmuka untuk pengguna. Proses ini bertujuan untuk membuat interaksi pengguna dan sistem sesederhana dan seefisien mungkin untuk mencapai tujuan pengguna. Dalam penelitian ini, perancangan desain antarmuka menggunakan 1 halaman dengan 2 menu yaitu menu *encode* dan menu *decode*.



Gambar 3. Rancangan Halaman Website

Pada menu *encode* terdapat sebuah kolom untuk input file gambar yang akan dijadikan sebagai cover image, lalu terdapat pula kolom untuk input file teks berupa teks yang akan disisipkan kedalam gambar cover, lalu terdapat kolom untuk memasukan kunci enkripsi, kunci enkripsi akan digunakan kembali pada proses dekripsi untuk mendapatkan kembali teks yang telah dienkripsi. Selain halaman *encode*, terdapat juga halaman *decode* yang berfungsi untuk mendapatkan kembali teks yang telah disisipkan pada gambar. Pada halaman *decode* terdapat kolom untuk memasukan gambar stego yang didapatkan dari proses *encode*, lalu terdapat kolom untuk memasukan kunci dekripsi, lalu terdapat kolom untuk menampilkan teks yang sudah didapatkan kembali dari gambar stego. Rancangan halaman website dapat dilihat pada gambar 6.

2.4 Pengujian Sistem

a. Pengujian *Avalanche effect*

Untuk mengetahui ketahanan hasil enkripsi terhadap serangan kriptanalisis perlu dilakukan pengujian terhadap *ciphertext* hasil enkripsi. Pengujian yang dilakukan yaitu menilai *Avalanche effect* dari hasil enkripsi. Perhitungan nilai *Avalanche effect* dilakukan dengan menghitung jumlah bit yang berubah pada *ciphertext* ketika satu bit kunci diubah. Langkah - langkah pengujian yang dilakukan yaitu :

1. Melakukan enkripsi terhadap *plaintext* dengan menggunakan kunci enkripsi pertama hingga menghasilkan *ciphertext* pertama.

p-ISSN: 2301-5373
e-ISSN: 2654-5101

2. Melakukan enkripsi terhadap *plaintext* yang sama dengan sebelumnya namun kunci enkripsi yang digunakan diubah 1 bitnya hingga menghasilkan *ciphertext* kedua.
3. Melakukan perhitungan jumlah bit yang berubah dengan mebandingkan *ciphertext* pertama dan *ciphertext* kedua.
4. Melakukan perhitungan *Avalanche effect* dengan rumus :

$$Avalanche\ effect\ = \frac{\text{Jumlah bit } ciphertext \text{ yang berubah}}{\text{total bit pada } ciphertext} \times 100\% \quad (1)$$

Dengan rumus tersebut, semakin tinggi persentase perubahan bit *ciphertext*. Pengujian *Avalanche effect* dianggap baik apabila terjadi perubahan bit yang menunjukkan antara 45-60% (50% adalah hasil yang dianggap baik dalam pengujian) [4].

b. Pengujian MSE dan PSNR

Untuk mengetahui kualitas dari penyisipan yang dilakukan, dilakukan uji Peak Signal to Noise Ratio (PSNR) dan *Mean Square Error* (MSE) untuk mengetahui seberapa besar error dan penurunan kualitas media penampung. MSE adalah nilai error kuadrat rata-rata antara citra asli dengan citra asli dan dekripsi. Sedangkan PSNR adalah perbandingan antara nilai maksimum dari kualitas citra asli dan citra yang sudah mengalami proses dekripsi. Adapun langkah-langkah pengujian nilai PSNR dan MSE adalah sebagai berikut.

1. Input foto asli dan foto-stego.
2. Proses penghitungan nilai *Mean Square Error* (MSE). Secara teori, nilai MSE dapat dihitung dengan rumus :

$$\mathrm{MSE} = \frac{1}{\mathrm{NxM}} \sum_{\mathrm{i}=0}^{\mathrm{N}-1} \sum_{\mathrm{j}=0}^{\mathrm{M}-1} \left(\mathrm{I}_{(\mathrm{ij})} - \mathrm{K}_{(\mathrm{ij})}\right)^2 \quad (2)$$

3. Proses penghitungan nilai Peak Signal to Noise Ratio (PSNR). Secara teori, nilai PSNR dapat dihitung dengan rumus :

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{\mathrm{MAX}^2}{\mathrm{MSE}}\right) \quad (3)$$

4. Output berupa nilai MSE dan nilai PSNR.

Algoritma steganografi yang baik berdasarkan kualitas citra adalah yang memiliki nilai PSNR lebih dari 40db dan nilai MSE yang semakin mendekati angka 0 [5].

c. Pengujian Kinerja Sistem

Pengujian ini bertujuan untuk mengevaluasi performa sistem dalam hal kecepatan dan efektivitas dalam menyisipkan data dan mengekstraksi data. Evaluasi yang dilakukan yaitu mengukur kecepatan *Encode* dan *Decode* untuk mengetahui lama waktu yang dibutuhkan untuk menyisipkan *plaintext* ke dalam gambar (*Encode*) dan mengekstraksi teks rahasia dari gambar stego (*Decode*), selain itu dilakukan juga evaluasi integritas data dimana setelah proses *Encode* dan *Decode*, hasil *Decode* harus sama persis dengan *plaintext* yang disisipkan. Tidak boleh ada perubahan atau kehilangan informasi. Untuk mengetahui kinerja sistem dalam melakukan *Encode* dan *Decode* maka perlu untuk dilakukan pengujian terhadap sistem yang telah dibuat. Adapun langkah - langkah yang dilakukan dalam pengujian ini yaitu :

1. Memasukan File gambar yang akan digunakan sebagai media penyisipan.
2. Memasukan File *Plaintext* yang akan disisipkan.
3. Memasukan kunci yang akan digunakan untuk enkripsi lalu lakukan *Encode*.
4. Hitung waktu yang dibutuhkan sistem dalam melakukan *Encode*, lalu unduh gambar stego yang dihasilkan.
5. Lakukan *Decode* dengan memasukan file gambar stego yang telah diunduh dan kunci yang sama seperti kunci enkripsi yang telah digunakan untuk proses *Encode*.
6. Hitung waktu yang dibutuhkan sistem untuk melakukan proses *Decode*, lalu bandingkan apakah teks hasil *Decode* sesuai dengan *plaintext* awal yang disisipkan.

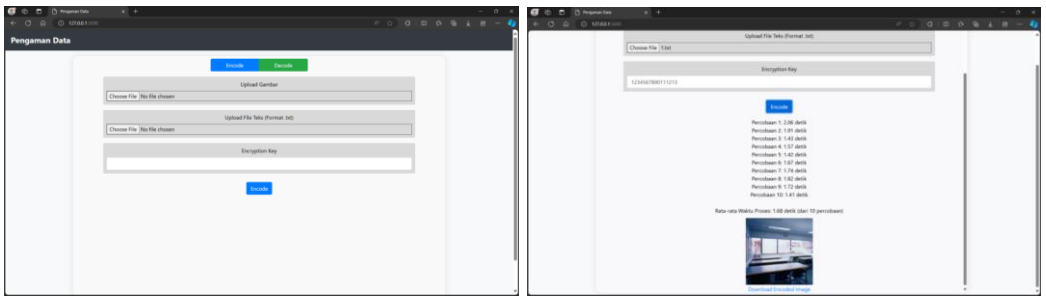
3. Hasil dan Pembahasan

3.1 Hasil Implementasi Antarmuka

Setelah melalui proses perancangan terhadap sistem, adapun hasil perancangan website adalah sebagai berikut;

a. Halaman *Encode*

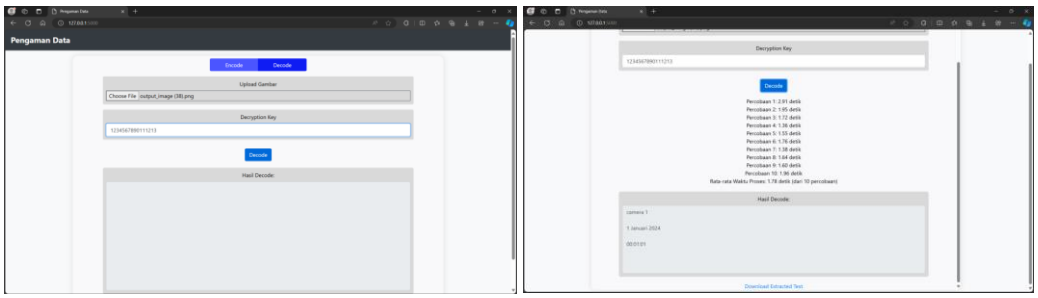
Pada Halaman *Encode* user dapat memasukan gambar, *plaintext*, dan kunci enkripsi. Kemudian ketika user menekan tombol *encode* maka hasil *encode* akan ditampilkan seperti pada gambar 7. User juga dapat mengunduh gambar hasil penyisipan agar pesan dapat dikirim dengan aman.



Gambar 7. Tampilan Menu *Encode*

b. Halaman *Decode*

Pada halaman *decode* user dapat memasukan gambar stego dan kunci dekripsi, kemudian ketika user menekan tombol *decode* sistem akan menampilkan hasil *decode* seperti pada gambar 8.



Gambar 8. Tampilan Menu *Decode*

3.2 Hasil Pengujian *Avalanche effect*

Dalam pengujian *Avalanche effect* ini dilakukan perhitungan jumlah bit yang berbeda antara dua *ciphertext*, kemudian dihitung persentasenya sebagai *Avalanche effect*. Hasil pengujian dapat dilihat pada tabel 1.

Tabel 1. Hasil Pengujian *Avalanche effect*

No	*Plaintext*	Key 1	Key 2	*Ciphertext* 1	*Ciphertext* 2	Avalanche Effect
1	camera 1 1 Januari 2024 00:01:01	1234567890111213	1234567890111214	000b8dd966b305cc83b97332d734e84019bf91ccbb001ecc39cfba732329a509a67f648d45b57e5dbb07044ef8436352	0759c1334975ca365e6bcf06fcdb0558e2bb23922f877600892e02424d2dd7a689234e97d4a69c6709cad981ee77ab0d	52.84%

p-ISSN: 2301-5373
e-ISSN: 2654-5101

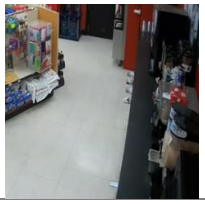
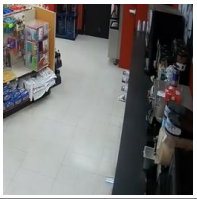
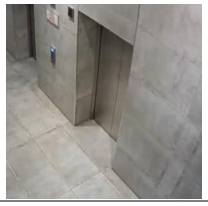
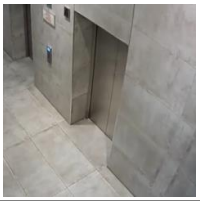
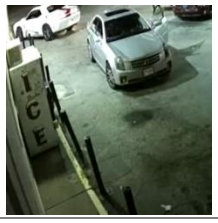
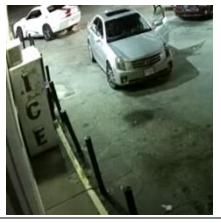
No	*Plaintext*	Key 1	Key 2	*Ciphertext* 1	*Ciphertext* 2	Avalanche Effect
2	Camera 2 2 Februari 2025 11:02:30	s9ai5BEo2 @pQ3h7i	s9ai5BEo2 @pQ3h7j	f30c97c0fe9701222 aef1c95a7a6b59c9 cf6d58506372f8bdb 2ac40e4e556dd4a6 39daf68fb8c9679d3 9405d16953f03	a8ac168fb4affd955 0f2f836c32a85bf17 910486ad7b807252 099396f71e7592f2c 76ee570f42684337 96165b9862040	49.74%
3	Camera 3 3 Maret 2026 22:03:27	o82AvbY20 kKm31dw	o82AvbY20 kKm31dy	83bee816f4b8800d 765205ed697f26ed c1fd73f8a1b4efbcd 97c1552e6025186	68e2a75b7309972d 373b5232feed8b95 9ad1735156492939 57c0aa472e1b24cb	52.34%
4	Camera 4 4 April 2027 12:14:29	k#19Js1aq4 67CBwi	l#19Js1aq4 67CBwi	06d1adefc84242cb 03d032b76ff58c44a b636a98faf9aab29 14373e22f01a849	9f0e1899bb44415d effc758d3b24cf4c2 887ab746fdff82341 83ca0b23854612	46.48%
5	Camera 5 5 Mei 2028 08:23:16	Y7za@K98 %aOw53m G	Z7za@K98 %aOw53m G	b99fc88ff108f70b33 80a0d306e9cd1623 1ddea146a6fb7f5fe 5bc1534210229	3618c0af29439ba7 6997b8a4088bda4f 5f49017b613f2637c 7707c1ecf8294e8	48.05%
6	Camera 6 6 Juni 2029 04:08:12	q7za@K98 %aOw53m G	o7za@K98 %aOw53m G	3dc263a584f1265c a6ced455dc72f518f 2d93ae978547124 2d5b2e5520bee03 a	fab7c7393fa61c3e4 a9c6b9ebe2516526 652a56612a10c028 eca63bd4779389c	55.08%
7	Camera 7 7 Juli 2030 11:18:30	k#19Js1aq4 67CBwi	k#19Js1ar4 67CBwi	9fd88d7013a172b1 1c8466340a185acc 521ab39736875d8 31e5e9869e9f9772 4	5588ae23ac20a7a7 6bcef623df91ea5c1 fae75ebbda7a649a 40613712c2c2198	48.05%
8	Camera 8 8 Agustus 2031 11:18:30	o82AvbY20 kKm31dw	o82AvbY30 kKm31dw	635f83b4ea7c7acd c194ccbb76996abf 2310bcfd46516375 0384b7708d29770 578aa7a94152952 8d1d8da18d6bd03 3c6	86ddbfd9c6cc0b1fb 2f92818d18e5dd78 7fa003afd5a20979c f5bc8bbbcd3f109f8 0541eac10b4091fe 257e58e38fcf6	51.30%
9	Camera 9 9 September 2032 11:18:30	123456789 0111213	123456799 0111213	e35676f6ab3a65e2 2c743a72974f3cf23 70f9bc0aeea44ea4 85def2b8bc365ac6 a8ed86c07cf24e8fd 3e258df4f4e7a1	c8af7b25eb1710ef2 051ad59e04cb7096 b8a3509efc1541ac b5b369e495cb6e76 2a98bcfcc3ffae6f2e ec7031be109a4	48.96%
10	Camera 10 10 Oktober 2033 11:18:30	s9ai5BEo2 @pQ3h7i	s9ai5BEo1 @pQ3h7i	387d503ae1b6d9c6 26da73ba67c4bca3 cf76e55b38c4b81d 861406abbf539703 098a4da66d62d9b 2cbd7a03478a1456 0	bc0e7137103f4c88 e36a595db1864118 7e6ad40e7fdb7bbd 3c3cf2f2d0aaf1593 a7528b1fd161bd6e 24ec2676112927d	50.26%
			Rata - rata			50.31%

Pengujian dilakukan pada sepuluh percobaan yang berbeda. Setiap percobaan menggunakan *plaintext* dan kunci enkripsi yang berbeda. Untuk setiap percobaan, *plaintext* dienkripsi dua kali dengan kunci yang berbeda yang memungkinkan perbandingan langsung antara *ciphertext* yang dihasilkan dari perubahan kunci yang dilakukan. Setelah *ciphertext* pertama dan *ciphertext* kedua dengan kunci yang diubah telah didapatkan, selanjutnya dilakukan perhitungan *Avalanche effect* dengan memasukan *ciphertext* ke program perhitungan.Hasil pengujian menunjukkan nilai *Avalanche effect* yang bervariasi antara 46.48% hingga 55.08%, dengan rata-rata keseluruhan sebesar 50.31%. Pada hasil pengujian tersebut, nilai *Avalanche effect* yang tinggi, seperti pada percobaan keenam dengan 55.08%, menunjukkan bahwa algoritma enkripsi memberikan respons yang kuat terhadap perubahan pada *plaintext* atau kunci. Artinya, setiap perubahan kecil pada *plaintext* atau kunci enkripsi akan menghasilkan perubahan yang signifikan pada *ciphertext*. Secara keseluruhan, pengujian ini menunjukkan bahwa algoritma enkripsi yang digunakan dalam semua percobaan mampu menjaga tingkat *Avalanche effect* dengan nilai rata-rata sebesar 50.31%.

3.3 Pengujian Hasil Penyisipan

Pengujian dilakukan dengan sepuluh percobaan, masing-masing dengan gambar asli yang berbeda, yang disisipkan data *ciphertext* menghasilkan gambar baru yang disebut stego image. Gambar asli dan stego image kemudian diinput ke program perhitungan untuk mendapatkan nilai MSE dan PSNR. Hasil pengujian dapat dilihat pada tabel 2.

Tabel 2. Hasil Pengujian MSE dan PSNR

No	Gambar Asli	*Ciphertext*	Stego Image	MSE	PSNR
1		000b8dd966b305cc83b97332d734e84019bf91ccbb001ecc39cfba732329a509a67f648d45b57e5dbb07044ef8436352		0.00278	73.679 db
2		f30c97c0fe9701222aef1c95a7a6b59c9cf6d58506372f8bdb2ac40e4e556dd4a639daf68fb8c9679d39405d16953f03		0.00263	73.923 db
3		83bee816f4b8800d765205ed697f26edc1fd73f8a1b4efbcd97c1552e6025186		0.00191	75.314 db
4		06d1adefc84242cb03d032b76ff58c44ab636a98faf9aab2914373e22f01a849		0.00179	75.601 db
5		b99fc88ff108f70b3380a0d306e9cd16231ddea146a6fb7f5fe5bc1534210229		0.00067	79.857 db
6		3dc263a584f1265ca6ced455dc72f518f2d93ae9785471242d5b2e5520bee03a		0.00030	83.244 db
7		9fd88d7013a172b11c8466340a185acc521ab39736875d831e5e9869e9f97724		0.0017	75.613 db

p-ISSN: 2301-5373
e-ISSN: 2654-5101

No	Gambar Asli	*Ciphertext*	Stego Image	MSE	PSNR
8		635f83b4ea7c7acdc194ccbb76996abf2310bcfd465163750384b7708d29770578aa7a941529528d1d8da18d6bd033c6		0.0027	73.726 db
9		e35676f6ab3a65e22c743a72974f3cf2370f9bc0aeea44ea485def2b8bc365ac6a8ed86c07cf24e8fd3e258df4f4e7a1		0.0018	75.549 db
10		387d503ae1b6d9c626da73ba67c4bca3cf76e55b38c4b81d861406abbf539703098a4da66d62d9b2cbd7a03478a14560		0.00051	81.014 db
		Rata -rata			76.758 db

Dalam pengujian ini, nilai MSE bervariasi dari 0.00030 hingga 0.00278, menunjukkan bahwa teknik penyisipan data yang digunakan efektif dalam mempertahankan kualitas gambar asli. Sedangkan PSNR pada pengujian ini berkisar antara 73.679 dB hingga 83.244 dB, dengan rata-rata 76.758 dB. Nilai ini menunjukkan bahwa kualitas visual yang baik dari gambar stego.

3.4 Pengujian Kinerja Sistem

Hasil pengujian yang dapat dilihat pada tabel 3 menunjukkan waktu yang dibutuhkan untuk proses *Encode* dan *Decode* relatif singkat, yaitu sekitar 1,3 hingga 1,9 detik. Hal ini menunjukkan bahwa sistem yang diimplementasikan cukup efisien dalam hal waktu, dimana waktu yang dibutuhkan untuk *Encode* dan *Decode* cenderung konsisten, meskipun ada sedikit variasi tergantung pada ukuran dan kompleksitas gambar asli. Hasil pengujian juga menunjukan bahwa untuk semua sepuluh percobaan, *plaintext* asli berhasil diekstraksi dari stego image dengan tepat. Ini menandakan bahwa tidak ada kehilangan data atau perubahan dalam pesan yang disisipkan selama proses penyisipan dan ekstraksi. Pengujian ini menunjukkan bahwa teknik yang digunakan efektif dalam menyisipkan dan melindungi pesan dalam gambar digital. Teknik ini memastikan bahwa pesan tersembunyi dapat diekstraksi dengan akurasi yang baik.

Tabel 2. Hasil Pengujian MSE dan PSNR

No	*Plaintext*	Gambar Asli	Waktu *Encode*	Hasil *Decode*	Waktu *Decode*
1	camera 1 1 Januari 2024 00:01:01	gambar 1.png	1,59 detik	camera 1 1 Januari 2024 00:01:01	1,69 detik
2	Camera 2 2 Februari 2025 11:02:30	gambae 2.png	1.75 detik	Camera 2 2 Februari 2025 11:02:30	1,84 detik
3	Camera 3 3 Maret 2026 22:03:27	gambar 3.png	1,52 detik	Camera 3 3 Maret 2026 22:03:27	1,60 detik
4	Camera 4 4 April 2027 12:14:29	gambar 4.png	1,45 detik	Camera 4 4 April 2027 12:14:29	1,28 detik
5	Camera 5 5 Mei 2028 08:23:16	gambar 5.png	1,86 detik	Camera 5 5 Mei 2028 08:23:16	1,56 detik
6	Camera 6 6 Juni 2029 04:08:12	gambar 6.png	1,62 detik	Camera 6 6 Juni 2029 04:08:12	1,29 detik

No	*Plaintext*	Gambar Asli	Waktu *Encode*	Hasil *Decode*	Waktu *Decode*
7	Camera 7 7 Juli 2030 11:18:30	gambar 7.png	1,37 detik	Camera 7 7 Juli 2030 11:18:30	1,34 detik
8	Camera 8 8 Agustus 2031 11:18:30	gambar 8.png	1,55 detik	Camera 8 8 Agustus 2031 11:18:30	1,66 detik
9	Camera 9 9 September 2032 11:18:30	gambar 9.png	1,63 detik	Camera 9 9 September 2032 11:18:30	1,94 detik
10	Camera 10 10 Oktober 2033 11:18:30	gambar 10.png	1,73 detik	Camera 10 10 Oktober 2033 11:18:30	1,76 detik

4. Kesimpulan

Kesimpulan yang didapatkan dari penelitian ini adalah sebagai berikut:

a. Berdasarkan pengujian terhadap implementasi Algoritma *Advanced Encryption Standard* yang telah dilakukan hasil pengujian dengan sepuluh kali percobaan menunjukkan nilai rata-rata *Avalanche effect* sebesar 50,31%, artinya algoritma dapat menghasilkan perubahan yang baik dalam *ciphertext* ketika dilakukan perubahan satu bit pada kunci enkripsi sehingga sulit bagi kriptanalis untuk melakukan serangan karena nilai ideal untuk AE dikategorikan baik jika perubahan dalam bit bernilai sebesar 45%-60% (50% adalah hasil yang sangat baik).

b. Berdasarkan pengujian terhadap implementasi algoritma steganografi BPCS (*Bit-Plane Complexity Segmentation*) yang telah dilakukan didapatkan nilai MSE yang bervariasi dari 0,00001 hingga 0,00271 dan rata-rata nilai PSNR 76.758 dB yang artinya kualitas visual dari stego images yang dihasilkan baik, karena nilai PSNR di atas 40 dB dianggap menunjukkan kualitas yang baik.

Referensi

[1] Permana, A. A., Nurnaningsih, D., "Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes)", *Jurnal Teknik Informatika*, vol. 11, no. 2, p. 177-186. 2018.

[2] Malvi, A., Painem, P., "Pengamanan File Gambar pada Media Video dengan Kriptografi Algoritma RSA dan Steganografi Algoritma End of File (EOF)", *Informatik: Jurnal Ilmu Komputer*, vol. 16, no. 2, p. 67-74. 2020.

[3] Nawawi, D. B., Huda, M. M., & Prabowo, T., "Perbandingan Enkripsi *Advanced Encryption Standard* dan Enkripsi Rivest Shamir Adleman", *G-Tech: Jurnal Teknologi Terapan*, vol. 8, no. 3, p. 1649–1655. 2024

[4] Muslih, M., Handoko, L. B., "PENGUJIAN *AVALANCHE EFFECT* PADA KRIPTOGRAFI TEKS MENGGUNAKAN AUTOKEY CIPHER", *Seminar Nasional Teknologi dan Multidisiplin Ilmu (SEMNASTEKMU)*, vol. 2, no. 1, p. 127-134. 2022.

[5] Pamungkas, N. B., Darwis, D., Nurjayanti, D., Prastowo, A. T., "Perbandingan Algoritma Pixel Value Differencing dan Modulus Function pada Steganografi untuk Mengukur Kualitas Citra dan Kapasitas Penyimpanan", *J. Inform*, vol. 20, no. 1, p. 67-77. 2020