Penyisipan Teks ke dalam Citra Digital menggunakan Kombinasi *Beaufort Cipher* dan Steganografi *Least Significant Bit*

Muhammad Aswiandi[1], I Kadek Dwi Nuryana[2]

[1,3] Jurusan Teknik Informatika, Fakultas Teknik, Universitas Negeri Surabaya
[1]muhammad.20115@mhs.unesa.ac.id
[2]dwinuryana@unesa.ac

***Abstrak*— Penelitian ini menerapkan teknik pengamanan pesan teks berlapis dengan mengkombinasikan algoritma kriptografi Beaufort Cipher dan steganografi Least Significant Bit (LSB) pada citra digital. Pesan teks terlebih dahulu dienkripsi menggunakan Beaufort Cipher menghasilkan ciphertext, kemudian ciphertext disisipkan ke dalam citra cover berformat JPG (RGB Color Model) menggunakan metode LSB. Implementasi dilakukan pada aplikasi desktop berbasis Java yang mendukung proses enkripsi, steganografi, ekstraksi, serta fitur chat rahasia real-time. Pengujian dilakukan terhadap variasi panjang pesan 1000, 3000, dan 5000 karakter serta lima citra uji berbeda. Hasil pengujian menunjukkan nilai MSE sangat rendah dengan nilai antara 0.0012 - 0.2047 dan nilai rata-rata PSNR berkisar 55–77 dB (kategori Excellent), serta analisis histogram citra stego tetap seragam. Hal ini membuktikan bahwa citra hasil stego tidak mengalami perubahan visual signifikan dan sulit terdeteksi keberadaan pesan tersembunyi. Metode kombinasi Beaufort Cipher dan LSB efektif memberikan perlindungan berlapis terhadap pesan rahasia pada komunikasi digital.**

***Kata Kunci*—** Steganografi, Least Significant Bit, Beaufort Cipher, Citra Digital, Keamanan Informasi, PSNR, MSE

I. PENDAHULUAN

Komunikasi internet antara dua entitas atau lebih memiliki tujuan untuk menyampaikan informasi. Informasi yang disampaikan dapat berupa teks, gambar, file, pesan publik serta bentuk bentuk percakapan. Bentuk informasi yang disampaikan juga dapat berupa informasi rahasia. Penggunaan internet saat ini telah menjadi selayaknya kebutuhan publik yang luas dan sangat terbuka. Kebocoran informasi rahasia dalam internet mungkin akan dapat terjadi, sehingga diperlukan sebuah mekanisme pengamanan yang cukup tangguh untuk menjaganya [1].

Pengamanan yang baik sangat dibutuhkan terhadap informasi ketika didistribusikan atau disimpan. Salah satu cara untuk melindungi file/data adalah dengan proses pemindahan data yang akan dikirim. Proses transmisi data dilakukan dengan menggunakan kriptografi. Kriptografi mencakup dua proses konversi informasi, termasuk dua proses *encryption* dan *decryption*, untuk menjaga kerahasiaan dan integritas informasi selama proses pengiriman [2].

Kriptografi merupakan suatu teknik yang digunakan untuk mengolah informasi asli menjadi informasi baru yang tidak dapat dibaca secara langsung oleh pihak yang tidak berwenang. Dalam kriptografi terdapat dua proses utama yang saling berkaitan, yaitu enkripsi dan dekripsi. Enkripsi merupakan proses pengubahan pesan asli menjadi pesan tersandi sehingga sulit dipahami, sedangkan dekripsi adalah proses kebalikan dari enkripsi, yaitu mengembalikan pesan tersandi menjadi pesan asli agar dapat dibaca kembali oleh penerima yang berhak [3]. Berbagai algoritma kriptografi dapat digunakan untuk menerapkan teknik tersebut, salah satunya adalah algoritma *Beaufort Cipher*.

Algoritma *Beaufort Cipher* merupakan turunan dari *Vigenere Cipher* dan bekerja dengan prinsip substitusi simetris dalam proses enkripsi dan dekripsi [4]. Algoritma ini termasuk ke dalam kriptografi klasik, karena mekanisme keamanannya sangat bergantung pada penggunaan kunci. Semakin panjang dan bervariasi karakter kunci yang digunakan, maka hasil enkripsi yang dihasilkan akan semakin acak sehingga pesan menjadi lebih sulit untuk dipahami oleh pihak yang tidak berwenang [5].

Penggunaan kriptografi mampu menjaga kerahasiaan dan keamanan informasi melalui proses penyandian data. Namun, hasil dari proses kriptografi berupa ciphertext cenderung terlihat mencurigakan sehingga berpotensi memicu upaya pihak ketiga untuk melakukan analisis atau pemecahan sandi. Oleh karena itu, diperlukan suatu teknik pendukung untuk menyamarkan keberadaan pesan tersebut dengan cara menyembunyikannya ke dalam media lain. Teknik pendukung ini dikenal sebagai steganografi, yang berfungsi untuk menyisipkan informasi rahasia ke dalam suatu media digital sehingga keberadaan pesan tidak mudah terdeteksi [6].

Steganografi merupakan teknik yang digunakan untuk menyembunyikan informasi rahasia ke dalam suatu media digital, seperti gambar, audio, maupun video, sehingga keberadaan pesan tersebut tidak dapat diketahui secara langsung. Secara teknis, steganografi mengacu pada proses penyisipan pesan rahasia ke dalam media lain (*cover media*) dengan tujuan agar pesan dapat dikirimkan tanpa menimbulkan kecurigaan dari pihak yang tidak berwenang [7].

Penggunaan media gambar atau citra digital dalam steganografi merupakan salah satu bentuk penerapan steganografi modern yang banyak digunakan saat ini. Dalam proses penyembunyian pesan ke dalam citra digital, informasi rahasia yang disisipkan tidak dapat terlihat secara kasat mata, sehingga pihak lain tidak menyadari bahwa citra tersebut mengandung pesan tersembunyi. Salah satu metode steganografi yang umum dan aman digunakan adalah *Least Significant Bit* (LSB). Metode LSB memiliki keunggulan dari sisi kecepatan dalam proses *embedding* dan *ekstraksi* pesan.

Selain itu, metode ini hanya memodifikasi bit paling rendah pada nilai piksel citra digital, sehingga perubahan yang terjadi tidak memengaruhi persepsi visual secara signifikan [8].

Penelitian ini bertujuan untuk menerapkan menyisipkan teks ke dalam citra digital dan mengukur hasil kombinasi dari algoritma kriptografi *Beaufort Cipher* dan metode *Least Significant Bit* (LSB).

II. METODE PENELITIAN

Metodologi penelitian yang digunakan pada penelitian ini disusun secara sistematis untuk menjelaskan tahapan-tahapan dalam menyelesaikan permasalahan penelitian. Alur penelitian dirancang secara logis, terstruktur, dan berurutan agar proses perancangan sistem pengamanan data dapat berjalan dengan baik. Model metode yang digunakan dalam penelitian ini adalah pembangunan sistem keamanan informasi berbasis kriptografi dan steganografi, dengan mengombinasikan algoritma Beaufort Cipher sebagai metode enkripsi dan metode Least Significant Bit (LSB) sebagai teknik penyisipan pesan ke dalam citra digital.

Pelaksanaan penelitian diawali dengan tahap riset awal, yaitu melakukan kajian literatur terhadap konsep kriptografi, steganografi, algoritma Beaufort Cipher, dan metode LSB, serta menentukan metode dan algoritma yang sesuai dengan tujuan penelitian. Tahap selanjutnya adalah pengumpulan data, yang dilakukan menggunakan teknik studi dokumentasi. Data yang dikumpulkan terdiri dari data teks (*plain text*) yang diperoleh dari situs https://loremipsum360.com sebanyak tiga data dengan variasi jumlah karakter, serta data citra digital yang diperoleh dari situs https://unsplash.com sebanyak lima citra sebagai media penampung (*cover image*).

Tahap berikutnya adalah implementasi program, yaitu pembuatan sistem yang mengintegrasikan algoritma Beaufort Cipher dan metode Least Significant Bit. Pada tahap ini dilakukan proses enkripsi pesan teks menggunakan algoritma Beaufort Cipher untuk menghasilkan *cipher text*. Cipher text tersebut kemudian disisipkan ke dalam citra digital menggunakan metode LSB untuk menghasilkan citra stego. Proses ini dirancang agar pesan rahasia tidak hanya terenkripsi dengan baik, tetapi juga tersembunyi secara visual sehingga tidak menimbulkan kecurigaan.

Dalam tahap perancangan data, data yang digunakan diklasifikasikan menjadi dua jenis, yaitu data citra dan data teks. Data citra berupa file berekstensi *.jpg*, sedangkan data teks dibagi ke dalam tiga kategori berdasarkan jumlah karakter, yaitu 1000, 3000, dan 5000 karakter. Data teks yang telah disiapkan kemudian disimpan dalam format *.txt* untuk selanjutnya diproses oleh sistem.

Perancangan proses sistem dijelaskan menggunakan flowchart untuk menggambarkan alur kerja sistem secara menyeluruh. Proses sistem dibagi menjadi tiga bagian utama, yaitu proses enkripsi, proses dekripsi, dan proses hasil. Pada proses enkripsi, pengguna memasukkan citra asli, file teks, dan *secret key*. Sistem kemudian melakukan enkripsi teks menggunakan algoritma Beaufort Cipher dan menyisipkan hasil enkripsi ke dalam citra menggunakan metode LSB hingga menghasilkan citra stego. Pada proses dekripsi, pengguna memasukkan citra stego dan *secret key*, kemudian sistem mengekstraksi cipher text dari citra dan mendekripsinya kembali menjadi plain text. Proses hasil digunakan untuk membandingkan citra asli dan citra stego melalui perhitungan nilai MSE, PSNR, serta analisis histogram.

Selain itu, dilakukan perancangan tampilan antarmuka untuk mempermudah pengguna dalam mengoperasikan sistem. Antarmuka yang dirancang meliputi halaman enkripsi, halaman dekripsi, halaman hasil pengujian, dan halaman chat. Halaman chat berfungsi sebagai fitur utama yang mengintegrasikan seluruh proses sistem, yaitu enkripsi pesan, penyisipan pesan ke dalam citra, serta pengiriman citra stego sebagai media komunikasi rahasia.

Tahap akhir penelitian adalah perancangan pengujian, yang bertujuan untuk mengevaluasi kualitas citra steganografi. Pengujian dilakukan dengan menghitung nilai Mean Square Error (MSE) dan Peak Signal-to-Noise Ratio (PSNR) serta melakukan analisis histogram untuk mengetahui perubahan distribusi nilai piksel antara citra asli dan citra stego. Hasil pengujian ini digunakan untuk menentukan tingkat kualitas citra, tingkat imperceptibility, serta efektivitas kombinasi algoritma Beaufort Cipher dan metode Least Significant Bit dalam menjaga kerahasiaan dan kualitas citra digital.

III. HASIL DAN PEMBAHASAN

Sistem enkripsi penyisipan teks ke dalam citra digital menggunakan kombinasi kritografi dan steganografi pada algoritma *Beaufort Cipher* dan metode *Least Significant Bit* menggunakan data citra dan *plain text* sebagai data yang akan dipakai dalam pengujian. Penjelasan data yang digunakan sebagai berikut.

1. Citra

   Citra digunakan sebagai *media cover* pada metode steganografi. Citra yang digunakan memiliki kriteria yaitu citra *model* RGB dan berekstensi .jpg. Dataset citra diperoleh dari alamat *website* https://unsplash.com/

Gambar 1. Citra Media Cover

2. Plain Text
   Plain text digunakan untuk data penyisipan ke dalam citra menggunakan metode steganografi serta digunakan untuk proses kritografi untuk menghasilkan *cipher text*. Data *plain text* dihasilkan dari alamat *website* https://loremipsum360.com. Penerapan data bisa dilihat pada Tabel 1.

Tabel 1. Data Plain Text

No	Data	Data Karakter
1	Plain text1	*Doing business like this takes much more effort than doing your own business*
2	Plain text2	*It showed a lady fitted out with a fur hat and fur boa who sat upright … He'd fall right off his desk!*
3	Plain text3	*Doing business like this takes much more effort than doing your own business … these gentlemen are always still sitting there eating their breakfasts… let him know just what I feel*

Penerapan proses merupakan tahapan yang menjelaskan bagaimana alur dari algoritma *Beaufort Cipher* dan *Least Significant Bit* dapat berjalan sesuai yang telah dijelaskan pada BAB II. Pada tahapan ini akan menjelaskan langkah-langkah penerapan yang dimulai dari proses enkripsi *plain text* ke dalam *cipher text* dan proses *embedding* hasil *cipher text* ke dalam citra.

Proses enkripsi *plain text* ke dalam *cipher text* menggunakan algoritma *Beaufort Cipher*. Tahapan yang dilakukan yaitu menentukan *plain text* dan *key*. Kemudian setiap karakter pada *plain text* dan *key* akan dipasangkan, setiap pasangan karakter harus memiliki *index* yang sama. Setiap karakter akan direprentasikan menjadi nilai desimal sesuai dengan ASCII. Perhitungan nilai *cipher text* diperoleh dari pengurangan nilai karakter *key* dan nilai karakter *plain text*, kemudian mencari nilai sisa hasil pembagian menggunakan nilai 256. Contoh perhitungan menggunakan *plain text* yaitu "GAMBAR" dan *key* yaitu "SECRET". Proses perhitungan nilai *cipher text* dalam dilihat pada Tabel 2.

$$Cc = (k - Pc) \bmod 256$$

Tabel 2. Hasil Perhitungan Nilai *Cipher Text*

***Index* ke-i**	***Key* (ASCII)**	***Plain Text* (ASCII)**	**Proses Perhitungan**	**Cipher Text (ASCII)**
1	S (83)	G (71)	(83 – 71) *mod* 256	FF (12)
2	E (69)	A (65)	(69 – 65) *mod* 256	EOT (4)
3	C (67)	M (77)	(67 – 77) *mod* 256	ö (246)
4	R (82)	B (66)	(82 – 66) *mod* 256	DLE (16)
5	E (69)	A (65)	(69 – 65) *mod* 256	EOT (4)
6	T (84)	R (82)	(84 – 82) *mod* 256	STX (2)

4.2.1 Proses Embedding Cipher Text ke dalam Citra

Proses *embedding* ke dalam citra menggunakan metode *Least Significant Bit*. Langkah pertama yaitu menentukan citra sebagai media penampung dan menentukan teks yang akan disisipkan. Teks yang akan disisipkan ke dalam citra adalah hasil enkripsi yaitu *cipher text*. Nilai di dalam citra dan setiap karakter pada teks akan direprentasikan menjadi nilai *biner* sesuai dengan ASCII. Nilai teks yang disisipkan akan berada di nilai *pixel* citra pada layer *Red*, *Green* dan *Blue*.

Pengambilan nilai citra menggunakan *pixel* 3x3 sebagai perwakilan. Nilai *pixel* masing-masing akan dikonversikan ke dalam bilangan *biner*, dapat dilihat pada Tabel 3.

Tabel 3. Konversi Nilai *Pixel* ke Nilai *Biner*

No	***Pixel***	***Biner***
1	120	01111000
2	230	11100110
3	225	11100001
4	90	01011010
5	100	01100100
6	150	10010110
7	100	01100100
8	132	10000100
9	234	11101010

Selanjutnya teks akan disisipkan ke dalam biner pixel yang dilakukan pada bit terakhir citra, adapun teks yang akan disisipkan yaitu huruf "A" yang mempunyai nilai desimal 65, kemudian dikonversikan menjadi bilangan biner dengan nilai "01000001". Penyisipan dapat dilihat pada Tabel 4.

Tabel 4. Penyisipan Nilai Biner Teks ke dalam Biner Pixel

No	***Biner* sebelum penyisipan**	***Biner* sesudah penyisipan**
1	01111000	01111000
2	11100110	11100111
3	11100001	11100000
4	01011010	01011010
5	01100100	01100100
6	10010110	10010110

Langkah terakhir setelah penyisipan biner yaitu mengkonversikan hasil *biner* menjadi nilai desimal yang dimana nilai desimal tersebut akan digunakan pada nilai *pixel* untuk citra yang baru atau yang disebut citra stego. Konversi hasil *pixel* dapat dilihat pada Tabel 5.

Tabel 5. Hasil Konversi Nilai *Biner* ke Nilai Desimal/*Pixel*

No	***Biner* sesudah penyisipan**	**Desimal/ *Pixel***
1	01111000	120
2	11100111	231
3	11100000	224
4	01011010	90

5	01100100	100
6	10010110	150
7	01100100	100
8	10000100	132
9	11101011	235

Berdasarkan hasil implementasi proses embedding menggunakan metode Least Significant Bit (LSB), diperoleh fakta bahwa ukuran file citra stego mengalami peningkatan dibandingkan dengan ukuran file citra asli. Peningkatan ukuran file ini bukan disebabkan oleh perubahan dimensi citra (resolusi), melainkan dipengaruhi oleh penambahan informasi data tersembunyi (ciphertext) yang disisipkan ke dalam struktur bit piksel citra. Pada proses penyisipan, setiap karakter ciphertext yang telah dienkripsi menggunakan algoritma Beaufort Cipher dikonversikan ke dalam bentuk biner dan dimasukkan ke dalam bit LSB pada kanal warna Red, Green, dan Blue. Semakin banyak jumlah karakter yang disisipkan, maka semakin banyak bit piksel yang mengalami modifikasi.

Selain itu, peningkatan ukuran file citra juga dipengaruhi oleh format penyimpanan citra digital yang digunakan. Pada format citra tertentu seperti PNG atau BMP, proses penyimpanan ulang (*re-saving*) citra stego setelah embedding dapat menyebabkan metadata file bertambah atau mekanisme kompresi menjadi kurang optimal dibandingkan citra asli. Hal ini mengakibatkan ukuran file citra stego menjadi lebih besar meskipun secara visual tidak mengalami perubahan yang signifikan. Dengan kata lain, perubahan ukuran file bersifat struktural pada data biner citra, bukan perubahan visual.

Peningkatan ukuran file ini sejalan dengan hasil pengujian kualitas citra menggunakan nilai MSE, PSNR, dan analisis histogram, yang menunjukkan bahwa meskipun ukuran file bertambah, kualitas visual citra stego tetap terjaga dengan sangat baik dan berada pada kategori excellent. Oleh karena itu, dapat disimpulkan bahwa pembesaran ukuran file citra merupakan konsekuensi logis dari proses penyisipan data rahasia dan tidak mengurangi efektivitas metode kombinasi algoritma Beaufort Cipher dan steganografi LSB dalam menjaga kerahasiaan serta keutuhan informasi.

Citra yang digunakan sebagai media *cover* menampung variasi jumlah karakter yaitu 1000, 3000 dan 5000 karakter. Hasil citra dari penerapan proses kombinasi algoritma *Beaufort Cipher* dan *Least Significant Bit* yang telah dilakukan ditunjukkan pada Gambar 2-4.

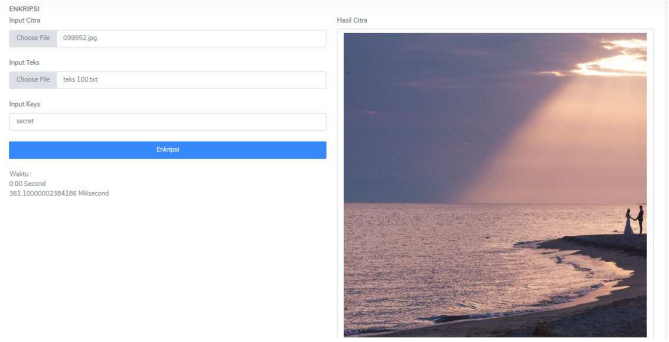
Gambar 2. Citra stego 1000 karakter

Gambar 3. Citra stego 3000 karakter

Gambar 4. Citra stego 5000 karakter

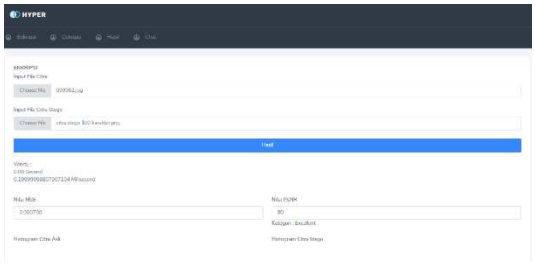
Penerapan tampilan/implementasi *user interface* adalah tahapan membangun aplikasi berdasarkan perancangan sebelumnya pada BAB III. Pada sistem yang dibangun memiliki 3 halaman yaitu halaman enkripsi, halaman dekripsi dan halaman hasil.

Halaman enkripsi merupakan tampilan utama dari sistem dan adalah tampilan awal yang disajikan oleh sistem pada saat pertama kali dijalankan. Halaman ini berfungsi untuk menghasilkan citra stego. Pada halaman ini user memasukkan data seperti data citra digital, data *file* teks dan data *key*. Setelah mengisi data kemudian klik tombol enkripsi sehingga akan munculkan citra stego. Tampilan halaman enkripsi bisa dilihat pada Gambar 14.



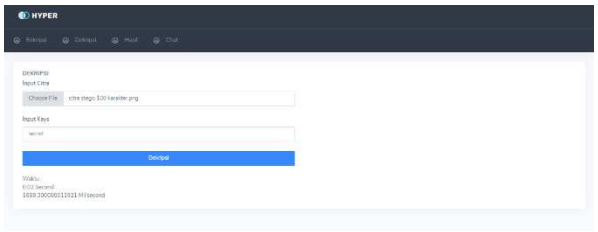
Gambar 5. Halaman Enkripsi

Halaman dekripsi merupakan halaman untuk mendapatkan teks dari citra stego yang disisipkan sebelumnya. Pada halaman ini user memasukkan data seperti data citra stego dan data key. Setelah mengisi data kemudian klik tombol dekripsi sehingga akan munculkan file teks dekripsi dari citra stego. Tampilan halaman dekripsi bisa dilihat pada Gambar 15.



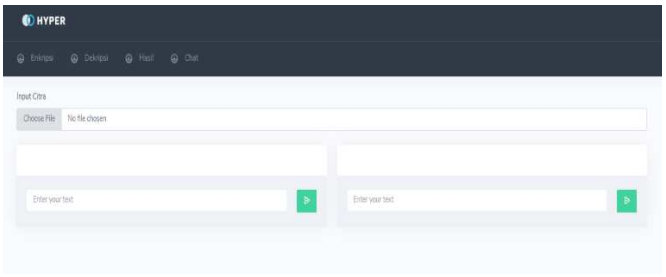
Gambar 6. Halaman Dekripsi

Halaman hasil merupakan halaman untuk mendapatkan hasil perhitungan pada citra asli dan citra stego. Pada halaman ini *user* memasukkan data seperti data citra asli dan data citra stego. Setelah mengisi data kemudian klik tombol hasil. Hasil perhitungan akan tampil seperti nilai MSE, nilai PSNR dan Histogram. Tampilan halaman hasil bisa dilihat pada Gambar 7.



Gambar 7. Halaman Hasil

Halaman Chat merupakan fitur dari aplikasi yang memungkinkan dua pengguna atau lebih melakukan komunikasi rahasia secara real-time dengan memanfaatkan citra digital sebagai media pengiriman pesan. Fitur ini mengintegrasikan seluruh proses yang telah dirancang sebelumnya, yaitu enkripsi pesan menggunakan *Beaufort Cipher*, penyisipan pesan terenkripsi ke dalam citra melalui teknik *Least Significant Bit* (LSB), serta pengiriman citra stego kepada penerima. Tampilan halaman *chat* bisa dilihat pada Gambar 8.



Gambar 8. Halaman *Chat*

Pengujian menggunakan pengukuran nilai MSE, nilai PSNR dan Analisis Histogram dengan tujuan untuk mengetahui pengukuran kualitas citra yang dihasilkan setelah enkripsi. Pengujian citra akan dilakukan pada 5 data citra uji dan 3 variasi jumlah karakter.

Hasil perhitungan nilai MSE adalah nilai *error* kuadrat rata-rata antara citra asli dengan citra stego. Nilai MSE dihasilkan dari perbandingan nilai *pixel* rata-rata citra asli dan citra stego. Hasil perhitungan yang sudah dilakukan dapat dilihat pada Tabel 6.

Tabel 6. Hasil Perhitungan Nilai MSE

No	Citra	Jumlah Karakter		
		1000	3000	5000
		MSE		
1	Citra1.png	0.001285	0.003820	0.179758
2	Citra2.png	0.001314	0.003846	0.196694
3	Citra3.png	0.001263	0.003774	0.153975
4	Citra4.png	0.001271	0.003840	0.130917
5	Citra5.png	0.001273	0.003833	0.204786

Nilai MSE yang digunakan untuk menghasilkan nilai PSNR diperoleh pada tabel. PSNR merupakan nilai hasil kualitas pada citra stego. Hasil perhitungan yang sudah dilakukan dapat dilihat pada Tabel 10.

Tabel 7. Hasil Perhitungan Nilai PSNR

No	Citra	Jumlah Karakter		
		1000	3000	5000
		PSNR		
1	Citra1.png	77.04 dB	72.30 dB	55.58 dB
2	Citra2.png	76.94 dB	72.27 dB	55.19 dB
3	Citra3.png	77.12 dB	72.36 dB	56.25 dB
4	Citra4.png	77.08 dB	72.29 dB	56.97 dB
5	Citra5.png	77.06 dB	72.31 dB	55.01 dB

Berdasarkan hasil perhitungan PSNR pada Tabel 10, diperoleh nilai PSNR tertinggi sebesar 77.12 dB pada penyisipan 1000 karakter dan nilai PSNR terendah sebesar 55.01 dB pada penyisipan 5000 karakter. Hasil tersebut menunjukkan bahwa kualitas citra stego sangat baik (Excellent) pada penyisipan 1000 dan 3000 karakter karena nilai PSNR berada di atas 60 dB. Namun, pada penyisipan 5000 karakter, nilai PSNR mengalami penurunan hingga berada pada rentang 55–57 dB, yang termasuk kategori *Good*

hingga *Very Good*, meskipun masih tergolong memiliki kualitas visual yang baik dan sulit dibedakan secara kasat mata dari citra asli.

Algoritma enkripsi yang digunakan adalah AES-256 dengan mode CTR (atau CBC). Kunci yang digunakan adalah 256-bit yang di-generate secara random.

Tabel 8. Hasil Pengujian Avalanche Effect

Ukuran Pesan	Avalanche Effect (%)	Keterangan
1000 karakter	49.87	Sangat baik
3000 karakter	50.12	Sangat baik
5000 karakter	49.94	Sangat baik
Rata-rata	49.98	Excellent

Berdasarkan hasil pengujian pada Tabel 11, dapat diketahui bahwa algoritma enkripsi AES-256 yang digunakan dalam penelitian ini menunjukkan nilai Avalanche Effect yang sangat baik. Nilai Avalanche Effect berada pada rentang 49.87% hingga 50.12% untuk berbagai ukuran pesan, dengan nilai rata-rata sebesar 49.98%. Nilai tersebut mendekati kondisi ideal, yaitu 50%, yang menunjukkan bahwa perubahan satu bit pada plaintext atau kunci enkripsi menghasilkan perubahan sekitar setengah dari total bit pada ciphertext. Hal ini membuktikan bahwa algoritma AES-256 mampu menghasilkan difusi yang kuat, sehingga ciphertext menjadi sangat sensitif terhadap perubahan kecil pada input.

Hasil perhitungan *Correlation Coefficient & Entropy* sebagai berikut:

Tabel 9. Hasil Correlation Coefficient & Entropy

Metrik	Nilai Rata-rata	Ideal
Correlation Coefficient	0.0012	≈ 0
Entropy Ciphertext	7.998	8.000
Entropy Plaintext	4.21	-

Hasil pengujian Correlation Coefficient dan Entropy pada Tabel 9 menunjukkan bahwa algoritma enkripsi AES-256 mampu menghasilkan ciphertext dengan tingkat keacakan yang sangat tinggi. Nilai Correlation Coefficient rata-rata sebesar 0.0012, yang mendekati nilai ideal yaitu 0, menandakan bahwa tidak terdapat hubungan linier antara plaintext dan ciphertext. Hal ini menunjukkan bahwa pola asli data berhasil dihilangkan secara efektif oleh proses enkripsi. Selain itu, nilai Entropy ciphertext sebesar 7.998 sangat mendekati nilai maksimum ideal, yaitu 8.000 untuk data 8-bit. Nilai ini menunjukkan bahwa tingkat ketidakpastian dan keacakan data hasil enkripsi sangat tinggi, sehingga ciphertext sulit dianalisis atau diprediksi. Sebaliknya, nilai Entropy plaintext sebesar 4.21 menunjukkan bahwa data asli memiliki tingkat keacakan yang lebih rendah dibandingkan ciphertext.

Analisis Histogram dilakukan untuk mengetahui perubahan distribusi *pixel* citra pada citra asli dan citra stego dan menggunakan grafik histogram pada visualisasi terhadap perubahan *pixel*. Nilai perubahan *pixel* menggunakan citra pada variasi 5000 jumlah karakter sebagai perwakilan. Hasil perubahan dapat dilihat pada Tabel 10.

Tabel 10. Nilai Perubahan Pixel Citra dan Citra Stego

Index Pixel	***Pixel* Citra Asli**	***Pixel* Citra Stego**
0	75	74
1	88	88
2	123	122
4	72	72
5	85	84
6	120	120
8	73	72
9	86	86
10	121	120
12	78	78
13	91	90
14	126	126
…	…	…
4194301	50	50
4194302	61	61
4194303	255	255

Perbandingan nilai perubahan pixel dapat dilihat menggunakan visualisasi grafik histogram untuk menampilkan perubahan distribusi pixel yang jelas pada citra asli dan citra stego.

IV. KESIMPULAN

Berdasarkan hasil penerapan dan pengujian sistem penyisipan teks ke dalam citra digital menggunakan kombinasi algoritma kriptografi Beaufort Cipher dan metode steganografi Least Significant Bit (LSB), dapat disimpulkan bahwa sistem yang dibangun berhasil mengamankan sekaligus menyembunyikan pesan teks dengan baik. Algoritma Beaufort Cipher mampu mengenkripsi pesan sehingga isi informasi tidak dapat dibaca secara langsung tanpa kunci yang sesuai, sedangkan metode LSB mampu menyisipkan pesan terenkripsi ke dalam citra digital tanpa menimbulkan perubahan visual yang signifikan. Hasil pengujian menunjukkan bahwa peningkatan jumlah karakter pesan yang disisipkan berpengaruh terhadap peningkatan nilai MSE dan penurunan nilai PSNR, namun nilai MSE yang diperoleh masih berada pada rentang rendah, yaitu antara 0,001263 hingga 0,204786, serta nilai PSNR berada pada rentang 55 dB hingga 77 dB yang termasuk dalam kategori kualitas citra excellent. Selain itu, hasil analisis histogram memperlihatkan bahwa distribusi nilai piksel citra stego sangat mendekati distribusi citra asli, sehingga citra hasil penyisipan tidak menimbulkan kecurigaan secara visual. Dengan demikian, kombinasi algoritma Beaufort Cipher dan metode LSB terbukti efektif dalam menyisipkan teks ke dalam citra digital secara aman dan imperceptible.

Meskipun sistem yang dibangun telah menunjukkan hasil yang baik, penelitian ini masih memiliki beberapa keterbatasan yang dapat dikembangkan lebih lanjut. Penelitian selanjutnya disarankan untuk menambahkan variasi jenis format citra digital, seperti *.png*, *.tif*, dan *.gif*, serta

meningkatkan jumlah karakter pesan yang disisipkan hingga lebih dari 10.000 karakter guna menguji kapasitas dan ketahanan sistem secara lebih menyeluruh. Selain itu, pengujian kualitas citra dapat dikembangkan dengan menambahkan parameter evaluasi lain, seperti Structural Similarity Index Measure (SSIM), Quality Index, Average Quantization Error (AVQ), atau metode evaluasi lainnya agar analisis kualitas citra menjadi lebih komprehensif. Pengembangan pada aspek keamanan algoritma enkripsi juga dapat dilakukan dengan mengombinasikan Beaufort Cipher dengan algoritma kriptografi modern untuk meningkatkan tingkat keamanan sistem secara keseluruhan.

REFERENSI

[1] E. Ardhianto, W. T. Handoko, E. Supriyanto, and H. Murti, "Evolusi Cipher Vigenere dalam Peningkatan Pengamanan Informasi," *J. Inform. Upgris*, vol. 7, no. 2, pp. 23–27, 2021, doi: https://doi.org/10.26877/jiu.v7i2.9333.

[2] H. Putri, L. Virna, T. Febrianti, and T. Sutabri, "Pengamanan Data Transmisi Aplikasi Web Menggunakan Algoritma Kriptografi RSA: Studi Kasus dan Analisis," *Mifortekh J. Manaj. Inform. Teknol.*, vol. 5, no. 1, pp. 153–170, 2025, doi: https://doi.org/10.51903/rdbsne23.

[3] S. Simangunsong and M. Syahrizal, "Modifikasi Pembangkit Kunci Algoritma Berufort Cipher Berdasarkan Pembangkit Kunci CSPRING Berbasis RSA," *J. Ilmu Komputer, Teknol. dan Inf.*, vol. 2, no. 2, pp. 39–47, 2024, doi: https://doi.org/10.62866/jurikti.v2i2.157.

[4] E. Ndruru and T. Zebua, "Pembangkitan Kunci Beaufort Cipher Dengan Teknik Blum-blum Shub pada Pengamanan Citra Digital," *Bull. Inf. Technol.*, vol. 3, no. 2, pp. 149–154, 2022, doi: https://doi.org/10.47065/bit.v3i2.302.

[5] S. P. Kurnia, S. Ndruru, N. P. Tambunan, M. Hasbiallah, and A. T. Zy, "Analisis Performa Beaufort Cipher dan ROT13 dalam Proses Enkripsi dan Dekripsi pada Data Teks," *J. Media Inform.*, vol. 6, no. 2, pp. 1058–1065, 2025, doi: https://doi.org/10.55338/jumin.v6i2.5363.

[6] A. S. Fadel, R. D. Saputra, R. N. Putra, and Y. Fatma, "Analisis Keamanan Steganografi Teks dengan Metode LSB (Least Significant Bit) pada Citra Digital," *J. Comput. Sci. Inf. Technol.*, vol. 5, no. 1, pp. 36–41, 2024, doi: https://doi.org/10.37859/coscitech.v5i1.6759.

[7] M. A. Firdaus and A. Rahmatulloh, "Implementasi Steganografi Citra Digital LSB Menggunakan Enkripsi AES-256 dan Embedding Pseudorandom," *JITET J. Inform. dan Tek. Elektro Terap.*, vol. 13, no. 1, pp. 411–418, 2025, doi: https://doi.org/10.23960/jitet.v13i1.5620.

[8] A. M. Ramadhani and T. Hasanuddin, "Modifikasi Least Significant Bits pada Gambar sebagai Data Hiding Steganography," *Indones. J. Data Sci.*, vol. 2, no. 2, pp. 91–102, 2021, doi: https://doi.org/10.56705/ijodas.v2i3.48.