EULER: Jurnal Ilmiah Matematika, Sains dan Teknologi
Journal Homepage: http://ejurnal.ung.ac.id/index.php/Euler
DOI: https://doi.org/10.34312/euler.v10i2.16646
Desember 2022, Vol. 10, No. 2, Hal. 181-192

Keamanan Pesan Menggunakan Kriptografi dan Steganografi *Least Significant Bit* pada File Citra Digital

Dian Eka Wijayanti[1*], Wulansari Romadlon[2]

[1,2] Jurusan Matematika, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
**Penulis Korespondensi. Email: dian@math.uad.ac.id*

Abstrak

Pada era saat ini sering terjadi gangguan keamanan data seperti pencurian data oleh orang yang tidak diinginkan. Untuk mengatasi permasalahan keamanan dapat ditangani menggunakan metode kriptografi dan steganografi. Proses kriptografi menghasilkan tulisan acak yang dapat mengaburkan pesan sehingga sulit dibaca oleh orang lain. Akan tetapi, kriptografi sendiri masih terlalu lemah untuk mengamankan pesan sehingga diperlukan steganografi untuk menyamarkan keberadaan pesan tersebut agar tidak terlihat oleh mata manusia. Selain menyembunyikan pesan, tujuan lainnya adalah mengetahui dampak dari penyisipan pesan. Dalam penelitian ini, dilakukan tahapan enkripsi dilanjutkan penyisipan dan dekripsi dilanjutkan ekstraksi. Pada proses enkripsi pesan rahasia menggunakan dua algoritma yaitu *Vigenere Cipher* dan *Playfair Cipher*. Pada proses penyisipan pesan rahasia menggunakan steganografi *Least Significant Bit* (LSB). Hasil kombinasi kriptografi dan steganografi mampu mengamankan pesan rahasia tanpa menimbulkan perubahan yang signifikan meskipun citra digital yang digunakan sebelum dan sesudah proses steganografi mengalami kenaikan ukuran, nilai *Mean Square Error* (MSE) yang diperoleh 0,000136 dan nilai *Peak Signal to Noise Ratio* (PSNR) 86,8062 dB, serta hasil enkripsi pesan cukup mengaburkan pola relasi pada pesan rahasia yang telah diubah dengan nilai *avalanche effect* sebesar 53,06%.

Kata Kunci: Kriptografi; *Vigenere Cipher; Playfair Cipher;* Steganografi; *Least Significant Bit;* Citra digital

Abstract

In the current era, data security disturbances often occur, such as data theft by unwanted people. To overcome security problems can be handled using cryptography and steganography methods. The cryptography process generates random writing that can obscure the message making it difficult for others to read. However, cryptography itself is still too weak to secure messages, so steganography is needed to disguise the existence of the message so that it is not visible to the human eye. Apart from hiding messages, another goal is to know the impact of message insertion. In this study, the encryption steps were followed by insertion and decryption followed by extraction. In the secret message encryption process using two algorithms, namely Vigenere Cipher and Playfair Cipher. In the process of inserting a secret message using Least Significant Bit (LSB) steganography. The results of the combination of cryptography and steganography are able to secure secret messages without causing significant changes even though the digital image used before and after the steganography process has increased in size, the Mean Square Error (MSE) value obtained is 0.000136 and the Peak Signal to Noise Ratio (PSNR) value is obtained. 86.8062 dB, and the result of message encryption is enough to obscure the relationship pattern in the modified secret message with an avalanche effect value of 53.06%.

Keywords: *Cryptography; Vigenere Cipher; Playfair Cipher; Steganography; Least Significant Bit; Digital Image*

1. Pendahuluan

Era industri 4.0 saat ini, kebutuhan manusia akan informasi semakin meningkat setiap harinya. Pencurian informasi salah satu peristiwa yang sering terjadi di era saat ini. Oleh sebab itu, dalam

Submit: 26 September 2022, Disetujui: 24 Oktober 2022, Online: 27 Oktober 2022

pertukaran informasi rahasia perlu dilakukan dengan hati - hati. Selain itu, informasi pada media digital saat ini dapat menyebar dengan cepat melalui jaringan internet. Dengan berkembangnya teknologi pada saat ini, kejahatan sistem informasi juga semakin meningkat. Oleh karena itu, sudah seharusnya dibarengi dengan perkembangan keamanan sistem informasi.

Alternatif keamanan yang dapat digunakan untuk menangani suatu permasalahan tentang kerahasiaan informasi ini, dikenal dengan istilah kriptografi. Kriptografi sendiri adalah ilmu yang merancang enkripsi yang kuat dengan menerapkan matematika yang kompleks. Enkripsi yang kuat tersebut dapat diartikan sebagai kita menyembunyikan suatu data rahasia yang tidak dapat diakses oleh pihak lain tanpa memiliki kunci dekripsinya. Jadi, seni kriptografi juga dianggap sebagai seni menulis di mana pertukaran data rahasia dapat dilakukan dengan aman sampai ke penerima [1]. Akan tetapi meskipun pesan telah terenkripsi dengan baik, nantinya akan muncul suatu permasalahan yaitu pesan yang telah terenkripsi dapat dilihat dengan mudah sehingga menimbulkan kecurigaan [2]. Oleh karena itu, untuk menghindari kecurigaan ini, kriptografi dapat dikombinasikan dengan salah satu teknik steganografi yaitu teknik *Least Significant Bit* (LSB).

Teknik steganografi *Least Significant Bit* (LSB) adalah salah satu cara paling umum yang digunakan untuk menyembunyikan pesan. LSB merupakan bagian dari urutan data yang berupa biner dengan nilai paling tidak signifikan atau minimum dan terletak di paling kanan dari string bit. Kebalikan dari LSB ini adalah *Most Significant Bit* (MSB), dalam hal ini angka yang paling berarti atau maksimal dan berada di paling kiri string [3].

Penelitian tentang kriptografi sebelumnya pernah dilakukan oleh Frobenius dan Hidayat [4] yang memberikan hasil bahwa penelitian tersebut berhasil mengkombinasikan empat metode kriptografi sekaligus dan *Least Significant Bit* (LSB) berbasis aplikasi *mobile* Android. Pada penelitian Handoko [5] yang melakukan kombinasi algoritma *Vigenere Cipher* dengan *Hill Cipher* yang digunakan untuk menyembunyikan pesan rahasia berupa teks. Dari penelitian ini didapatkan hasil nilai rata - rata *Avalanche Effect* 52,46% yang menunjukkan bahwa proses enkripsi dan dekripsi yang dilakukan telah berhasil mengamankan pesan rahasia. Selain itu, pada penelitian yang dilakukan oleh Pandey dan Badal [6] yang dalam penelitiannya memberikan hasil bahwa modifikasi *Playfair Cipher* lebih baik dalam mengamankan pesan dibandingkan *Playfair Cipher* asli.

Penelitian tentang steganografi sebelumnya pernah dilakukan oleh Modupe dkk [7] yang dilakukan dengan tujuan untuk mengetahui perbandingan LSB, MSB, dan PVD berdasarkan stenganografi citra. Penelitian yang dilakukan memberikan hasil bahwa metode LSB memberikan nilai PSNR dan SSIM yang lebih tinggi dibandingkan dengan metode MSB dan PVD dengan nilai MSE yang lebih rendah dibandingkan kedua teknik lainnya. Selain itu, pada penelitian yang dilakukan oleh Indrayani dan Subektiningsih [8] dengan memberikan hasil bahwa metode LSB dan MSB lebih baik dari aspek keamanan dibandingkan metode EoF dengan menggunakan format citra *Joint Picture Experts Group* (JPEG).

Pesan rahasia nantinya akan disisipkan ke dalam setiap bit pada citra digital, seperti penelitian yang dilakukan oleh Hafiz [3] yang memberikan hasil bahwa penyisipan pesan rahasia dilakukan pada wadah citra digital dalam format JPEG dan data tersembunyi dapat diekstraksi kembali dan waktu yang dibutuhkan dalam proses enkripsi dan dekripsi dipengaruhi oleh kecepatan komputer dan ukuran dari citra. Selain itu, pada penelitian yang dilakukan oleh Yakti dan Prayitno [9] yang bertujuan membandingkan dan menganalisa hasil pengolahan steganografi pada berbagai format gambar digital yang meliputi *Bitmapped Image* (BMP), *Portable Network Graphics* (PNG), Joint *Picture Experts Group* (JPEG), dan *Grafiphical Interchange Format* (GIF). Output steganografi yang dianalisis adalah *Mean Square Error* (MSE) dan *Peak Signal to Noise Ratio* (PSNR) menggunakan sampul citra yang diubah menjadi *grayscale*. Jumlah karakter yang digunakan pada pesan rahasia sebanyak 58, memberikan hasil bahwa format GIF merupakan format terbaik dengan MSE = 8, 697×10−4 dan PSNR = 78, 7369.

Untuk metode yang digunakan dalam pengenkripsian pesan di mana sebelumnya masih menggunakan *Playfair Cipher* klasik sehingga pada penelitian ini, data yang akan disisipkan ke adalah pesan teks dengan karakter berupa *printable characters* (karakter pada tabel ASCII 8-bit) menggunakan bahasa pemrograman python dengan karakter kuncinya dienkripsi terlebih dahulu menggunakan *Vigenere Cipher*. Hal ini dilakukan agar kunci yang dimiliki oleh pengirim dan penerima berbeda, berbeda dengan penelitian – penelitan sebelumnya yaitu kunci antara pengirim dan penerima sama sehingga keamanannya tidak terlalu kuat.

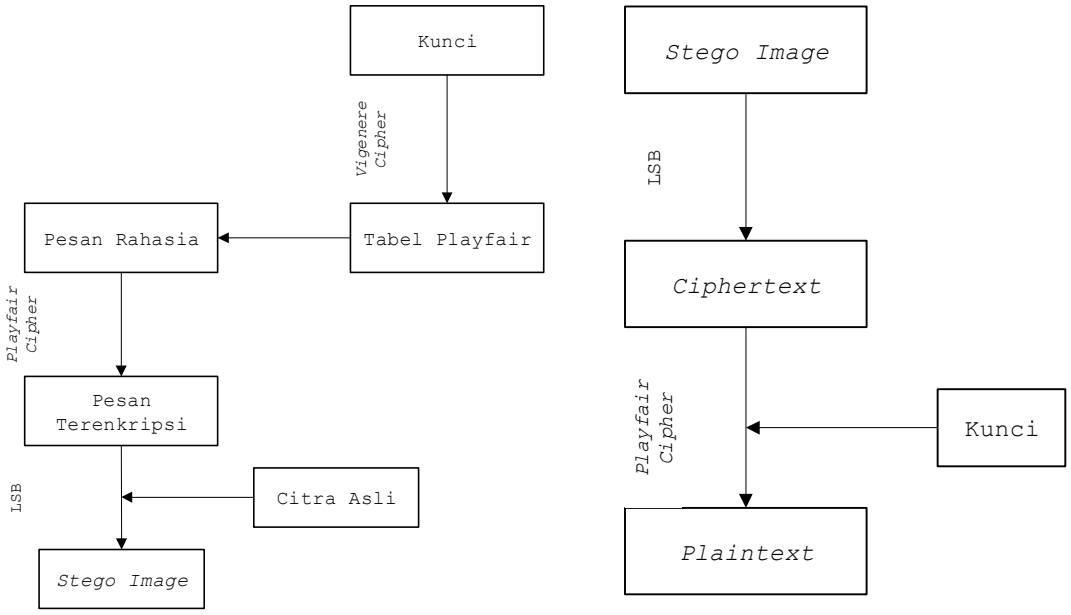
Dengan berkembangnya kemajuan saat ini, terdapat perkembangan resolusi gambar dari RGB ke RGBA sehingga pada penelitian ini file citra digital yang digunakan adalah file citra RGBA berformat PNG di mana format RGBA memiliki tambahan saluran warna yaitu Alpha yang berfungsi mengatur transparasi dalam citra. Dengan penggunakan file citra jenis RGBA berformat PNG ini diharapkan hasil dari steganografi yang dilakukan dapat memberikan hasil yang lebih baik di mana pada metode sebelumnya didapatkan perubahan ukuran pada *stego image* yang cukup besar.

Dengan demikian, penelitian ini dilakukan dengan tujuan untuk membuat keamanan pesan yang lebih kuat dibandingkan penelitian sebelumnya dan meminimalisir perubahan ukuran pada *stego image* menggunakan metode *Vigenere Cipher* dan *Playfair Cipher* dan dilanjutkan pesan yang telah terenkripsi nantinya akan disembunyikan ke dalam file citra digital dengan menggunakan metode LSB.

2. Metode Penelitian

2.1 Tahapan Penelitian

Penelitian ini menggunakan gabungan algoritma kriptografi *Vigenere Cipher* dan *Playfair Cipher* serta steganografi LSB. Pada penelitian ini *Vigenere Cipher* digunakan untuk mengenkripsi kunci agar diperoleh kunci yang berbeda antara pengirim dan penerima, sedangkan *Playfair Cipher* digunakan untuk mengenkripsi pesan sehingga didapatkan pesan acak. Kemudian LSB digunakan untuk menyembunyikan pesan ke dalam file citra digital sehingga keberadaannya tidak terlihat oleh mata manusia. Gambaran dari proses pada penelitian ini dapat dilihat pada Gambar 1.



Skema enkripsi dan penyisipan

Skema dekripsi dan ekstraksi

Gambar 1. Tahapan penelitian

2.2 Tinjauan Pustaka

Berikut merupakan teori – teori yang digunakan dalam penelitian ini.

2.2.1 Vigenere Cipher

Vigenere Cipher adalah bentuk sederhana dari *polyalphabetic substitution cipher*. Secara matematis, pengertian *Vigenere Cipher* dapat dijelaskan sebagai berikut.

Misalkan m sebagai bilangan bulat positif. Tentukan $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^m$. Untuk suatu kunci $K = (k_1, k_2, \dots, k_m)$, didefinisikan sebagai:

$$e_K = (x_1, x_2, \dots, x_m) = (x_1 + k_1, x_2 + k_2, \dots, x_m + k_m)$$

dan

$$d_K = (y_1, y_2, \dots, y_m) = (y_1 - k_1, y_2 - k_2, \dots, y_m - k_m),$$

di mana semua operasi dilakukan di $\mathbb{Z}_{26}$ [10].

Enkripsi (penyandian) mengunakan *Vigenere Cipher*, dengan menerapkan penjumlahan pada operasi modulus, dapat dituliskan secara matematis sebagai berikut:

$$C_i \equiv (P_i + K_i) \bmod 26$$

atau $C_i = (P_i + K_i) - 26$ kalau hasil jumlah P_i dan K_i lebih dari 26

dan dekripsi,

$$P_i \equiv (C_i - K_i) \bmod 26$$

atau $P_i = (C_i - K_i) + 26$ kalau hasil pengurangan C_i dan K_i minus [10].

Modulo 26 digunakan ketika hanya 26 karakter yang diproses, dan jika jumlah total karakter yang diproses adalah 256 karakter ASCII, maka operasi yang digunakan adalah modulo 256. Ini tergantung pada jumlah karakter yang digunakan. Di bawah ini adalah daftar karakter yang digunakan.

Tabel 1. Konversi karakter ke urutan integer dari 0 – 25

Alfabet	A	B	C	D	E	F	G	H	I	J	K	L	M
Konversi	0	1	2	3	4	5	6	7	8	9	10	11	12
Alfabet	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Konversi	13	14	15	16	17	18	19	20	21	22	23	24	25

2.2.2 Playfair Cipher

Playfair Cipher atau Playfair Square ditemukan pada tahun 1854 oleh ahli fisika bernama Sir Charles yang kemudian dipromosikan oleh Baron Lyon Playfair. Tabel dari *Playfair Cipher* sendiri berbentuk matriks berukuran 5 × 5 yang terdiri atas huruf berjumlah 25 dan menggunakan masukkan dengan menghilangkan alfabet J [11]. *Playfair Cipher* merupakan bagian dari algoritma kriptografi klasik. Prosedur *Playfair Cipher* ini juga termasuk dalam kriptografi *polygram substitution cipher* yang mana dalam penerapannya melakukan pergantian karakter asli dengan karakter kunci dan dalam penentuan *ciphertext* menggunakan permutasi [12].

Berikut beberapa definisi yang berkaitan dengan *Playfair Cipher*:

Definisi 1 [13]**.** Permutasi merupakan salah satu cabang dari matematika diskrit, yaitu penataan kembali anggota-anggotanya menjadi suatu barisan atau himpunan terurut. Atau juga dapat disebut sebagai "urutan linier" atau "pengaturan anggota".

Definisi 2 [14]. Misalkan π adalah suatu permutasi. Didefinisikan matriks permutasi sebagai $P(\pi) = [\delta_{i,\pi(j)}]$, di mana $\delta_{i,\pi(j)} = \begin{cases} 1, & jika\ i = \pi(j) \\ 0, & jika\ i \neq \pi(j) \end{cases}$, sedemikian sehingga $ent_{ij}(P(\pi)) = \delta_{i,\pi(j)}$.

Dari definisi di atas dapat disimpulkan bahwa matriks permutasi terkait dengan *Playfair Cipher*. Matriks permutasi berkaitan dengan matriks identitas, yaitu matriks yang diperoleh dengan menukar elemen-elemen di dalam matriks identitas.

Berikut adalah tabel modifikasi yang akan digunakan pada *Playfair Cipher.*

Tabel 2. Tabel *Playfair Cipher*

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z	0	1
2	3	4	5	6	7	8
9	!	“	#	$	%	&
'	(	)	*	+	,	-

=

65	66	67	68	69	70	71
72	73	74	75	76	77	78
79	80	81	82	83	84	85
86	87	88	89	90	48	49
50	51	52	53	54	55	56
57	33	34	35	36	37	38
39	40	41	42	43	44	45

2.3 Pengujian Metode

2.3.1 Metode Kriptografi

Untuk mengetahui kekuatan enkripsi yang dihasilkan saat proses penyandian menggunakan metode kriptografi *Vigenere Cipher* dan *Playfair Cipher*. Pada pengujian ini dilakukan dengan parameter uji avalanche effect. Suatu *avalanche effect* dapat dikatakan baik apabila nilai perubahan setiap yang dihasilkan lebih dari 50% atau separuh dari keseluruhan bit [11]. Rumus perhitungan *avalanche effect* adalah sebagai berikut:

$$\text{Avalanche Effect} = \frac{\text{Jumlah Perubahan Bit}}{\text{Jumlah Seluruh Bit}} \times 100\%$$

2.3.2 Metode Steganografi

Pengujian metode dilakukan dengan tujuan untuk mengetahui apakah hasil yang diperoleh dalam penelitian ini. *Mean Squared Error* (MSE) dan *Peak Signal to Noise Ratio* (PSNR) merupakan salah satu parameter untuk mengukur seberapa bagus kualitas citra yang diperoleh [12].

Nilai MSE ini nantinya akan digunakan untuk menentukan nilai *Mean Squared Error* dengan cara membandingkan nilai pada setiap *pixel cover image* dengan nilai *stego image* untuk posisi *pixel* yang sama. Untuk menghitung MSE digunakan persamaan sebagai berikut:

$$MSE = \frac{1}{mn}\sum_{i}^{m}\sum_{j}^{n}\left(I_{i,j} - K_{i,j}\right)^2$$

Sedangkan nilai dari $PSNR$ digunakan untuk mengetahui bagus tidaknya kualitas citra dengan satuan decibel (dB). Kualitas citra itu sendiri dapat dihitung menggunakan rumus berikut:

$$PSNR = 10\log_{10}\left(\frac{{Max_i}^2}{MSE}\right)$$

Jika nilai PSNR kurang dari 30 dB, ini menunjukkan kualitas citra yang dihasilkan relatif rendah dengan distorsi yang terlihat jelas akibat adanya penyisipan pesan pada citra tersebut dan untuk nilai PSNR lebih dari 40 dB menunjukkan bahwa kualitas *stego image* yang tinggi [13].

Selain mencari nilai MSE dan PSNR pada penelitian ini dilakukan juga uji perbandingan ukuran untuk mengetahui perbedaan ukuran antara *cover image* dan *stego image* untuk mengetahui perubahan ukuran yang terjadi setelah adanya penyisipan pesan.

3. Hasil dan Pembahasan

3.1 Enkripsi Kunci

Proses enkripsi kunci diperlukan agar kunci yang digunakan dalam mengenkripsi pesan tidak sama antara pengirim dan penerima sehingga keamanan pesan menjadi lebih kuat. Proses ini dilakukan dengan menggunakan metode *Vigenere Cipher* sebagai berikut, dengan pesan "SERENDIPITY" dan kunci "JK" yang mana melalui proses di bawah ini,

Plaintext : SERENDIPITY
Kunci : JK

Mengkonversi pesan dan kunci ke dalam bentuk integer. Berikut hasil konversi berdasarkan pada Tabel 1.

Plaintext : 18 4 17 4 13 3 8 15 8 19 24
Kunci : 9 10 9 10 9 10 9 10 9 10 9

Setelah dikonversi, proses selanjutnya yaitu menghitung menggunakan persamaan pada *Vigenere Cipher* seperti berikut:

$$C\ 1\ = (\ 18 + 9\ )\ mod 26 = 1$$
$$C\ 2\ = (\ 4 + 10\ )\ mod 26 = 14$$
$$C\ 3\ = (\ 17 + 9\ )\ mod 26 = 0$$
$$C\ 4\ = (\ 4 + 10\ )\ mod 26 = 14$$
$$C\ 5\ = (\ 13 + 9\ )\ mod 26 = 22$$
$$C\ 6\ = (\ 3 + 10\ )\ mod 26 = 13$$
$$C\ 7\ = (\ 8 + 9\ )\ mod 26 = 17$$
$$C\ 8\ = (\ 15 + 10\ )\ mod 26 = 25$$
$$C\ 9\ = (\ 8 + 9\ )\ mod 26 = 17$$
$$C\ 10\ = (\ 19 + 10\ )\ mod 26 = 3$$
$$C\ 11\ = (\ 24 + 9\ )\ mod 26 = 7$$

Hasil mod 26 : 1 14 0 14 22 13 17 25 17 3 7

Dari hasil mod 26 kemudian konversikan kembali menjadi bentuk alfabet yang diperoleh, sehingga didapatkan.

Kunci : BOAOWNRZRDH

Kunci yang diperoleh pada metode ini akan digunakan untuk membuat tabel *Playfair Cipher* dan kunci hasil enkripsi ini nantinya akan diberikan kepada ke penerima sebagai kunci untuk membuka pesan yang dienkripsi.

3.2 Enkripsi dan Penyisipan

Proses selanjutnya yaitu enkripsi pesan untuk mengaburkan pesan rahasia menggunakan metode *Playfair Cipher* dengan kunci yang telah diproses pada proses enkripsi kunci dan secara sederhana dapat dijelaskan sebagai berikut.

Langkah pertama, yaitu membuat tabel *Playfair Cipher* 9 × 9 dengan memasukkan hasil enkripsi kunci pada proses sebelumnya ke dalam Tabel 2 yang merupakan tabel asli *Playfair Cipher*. Hasil modifikasi tersaji pada Tabel 3.

Tabel 3. Modifikasi *Playfair Cipher*

B	**O**	**A**	**W**	**N**	**R**	**Z**
D	**H**	C	E	F	G	I
J	K	L	M	P	Q	S
T	U	V	X	Y	0	1
2	3	4	5	6	7	8
9	!	“	#	$	%	&
'	(	)	*	+	,	-

=

66	79	65	87	78	82	90
68	72	67	69	70	71	73
74	75	76	77	80	81	83
84	85	86	88	89	48	49
50	51	52	53	54	55	56
57	33	34	35	36	37	38
39	40	41	42	43	44	45

Perancangan implementasi menggunakan python diperlukan untuk mempermudah dalam perhitungan karena semakin banyak jumlah *plaintext* maka akan semakin rumit perhitungannya. Berikut adalah implementasi semua proses enkripsi dari pesan rahasia menggunakan python.

```
Plaintext : SERENDIPITY
Masukkan kunci: JK
Ciphertext: MIWGBFFSD10Y
```

Gambar 2. Implementasi enkripsi pesan menggunakan python

Setelah keseluruhan proses enkripsi dilakukan, diperoleh hasil akhir *ciphertext* berupa **MIWGBFFSD10Y** yang mana *ciphertext* ini akan disembunyikan ke dalam citra digital agar keberadaannya tidak terlihat oleh mata manusia. Berikut adalah file citra yang digunakan sebagai *cover image* atau wadah penampung.

Gambar 3. *Cover image*

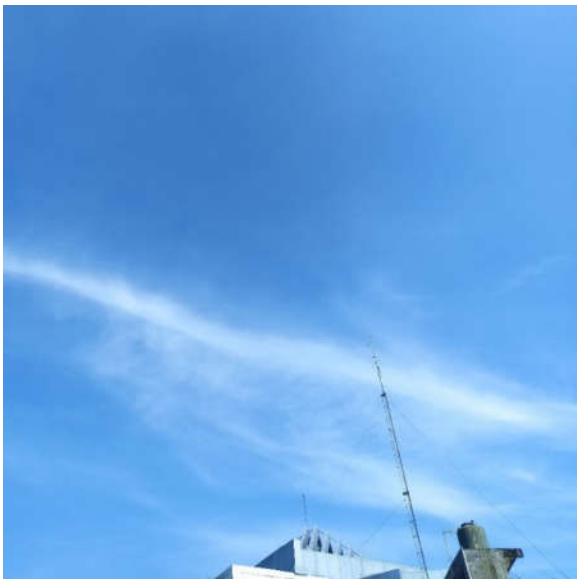
Sehingga penyisipan metode LSB diimplementasikan menggunakan python dan memberikan hasil yang ditampilkan pada Gambar 4.

```
Proses Steganografi LSB
1: Encode
2: Decode
1
Masukkan source image path
/content/Gambar 5.png
Masukkan pesan rahasia
MIWGBFFSD10Y
Masukkan destination image path
Gambar 5_Encode.png
Encoding...
Gambar Berhasil Dikodekan
```

Gambar 4. Implementasi *encode*

3.3 Ekstraksi dan Dekripsi

Setelah langkah-langkah alam proses penyisipan pesan ke dalam citra dengan tujuan agar pesan yang telah enkripsi dapat disembunyikan di dalam gambar sehingga tidak terlihat oleh mata telanjang manusia, maka dihasilkan *stego image* pada Gambar 5.



Gambar 5. *Stego image*

Gambar 5, merupakan file citra yang telah mengalami penyisipan pesan ke dalam bit terakhir pada file tersebut. File citra hasil penyisipan disebut *stego image* dan dari file ini nantinya akan dilakukan ekstraksi untuk mengambil pesan yang disembunyikan didalamnya.

Proses ekstraksi metode LSB diimplementasikan menggunakan python dan memberikan hasil yang ditampilkan pada Gambar 6.

```
Proses Steganografi LSB
1: Encode
2: Decode
2
Masukkan Source Image Path
/content/Gambar 5_Encode.png
Decoding...
Hidden Message: MIWGBFFSD10Y
```

Gambar 6. Implementasi *decode*

Untuk memperoleh pesan rahasia yang asli maka diperlukan proses dekripsi agar pesan yang tersembunyi hasil ekstraksi dari *stego image* dapat dibaca. Berikut adalah implementasi semua proses dekripsi dari pesan rahasia menggunakan python.

```
Ciphertext : MIWGBFFSD10Y
Masukkan kunci: BOAOWNRZRDH
Plaintext: SERENDIPITYX
```

Gambar 7. Implementasi dekripsi pesan menggunakan python

3.4 Pengujian Metode

3.4.1 Metode Kriptografi

Untuk memperoleh pesan rahasia yang asli maka diperlukan proses dekripsi agar pesan yang tersembunyi hasil ekstraksi dari *stego image* dapat dibaca. Berikut adalah implementasi semua proses dekripsi dari pesan rahasia menggunakan python.

Pengujian pada metode kriptografi ini dilakukan untuk mengetahui pengaruh kunci yang digunakan terhadap kekuatan enkripsi dengan parameter *avalanche effect*. Hasil *avalanche effect* sebagai berikut:

$$\text{Avalanche Effect} = \frac{26}{49} \times 100\%$$

$$\text{Avalanche Effect} = 53{,}06\%$$

Pertama untuk mencari nilai *avalanche effect*, diperlukan nilai jumlah perubahan bit. Perubahan jumlah bit ini diperoleh dari perubahan jumlah bit yang terdapat pada tabel *Playfair Cipher* dengan kunci yang telah terenkripsi "BOAOWNRZRDH". Adapun, perubahan jumlah bit seperti pada Tabel 4.

Tabel 4. Modifikasi *Playfair Cipher*

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z	0	1
2	3	4	5	6	7	8
9	!	"	#	$	%	&
'	(	)	*	+	,	-

Tabel *Playfair Cipher*

B	**O**	**A**	**W**	**N**	**R**	**Z**
D	**H**	C	E	F	G	I
J	K	L	M	P	Q	S
T	U	V	X	Y	0	1
2	3	4	5	6	7	8
9	!	"	#	$	%	&
'	(	)	*	+	,	-

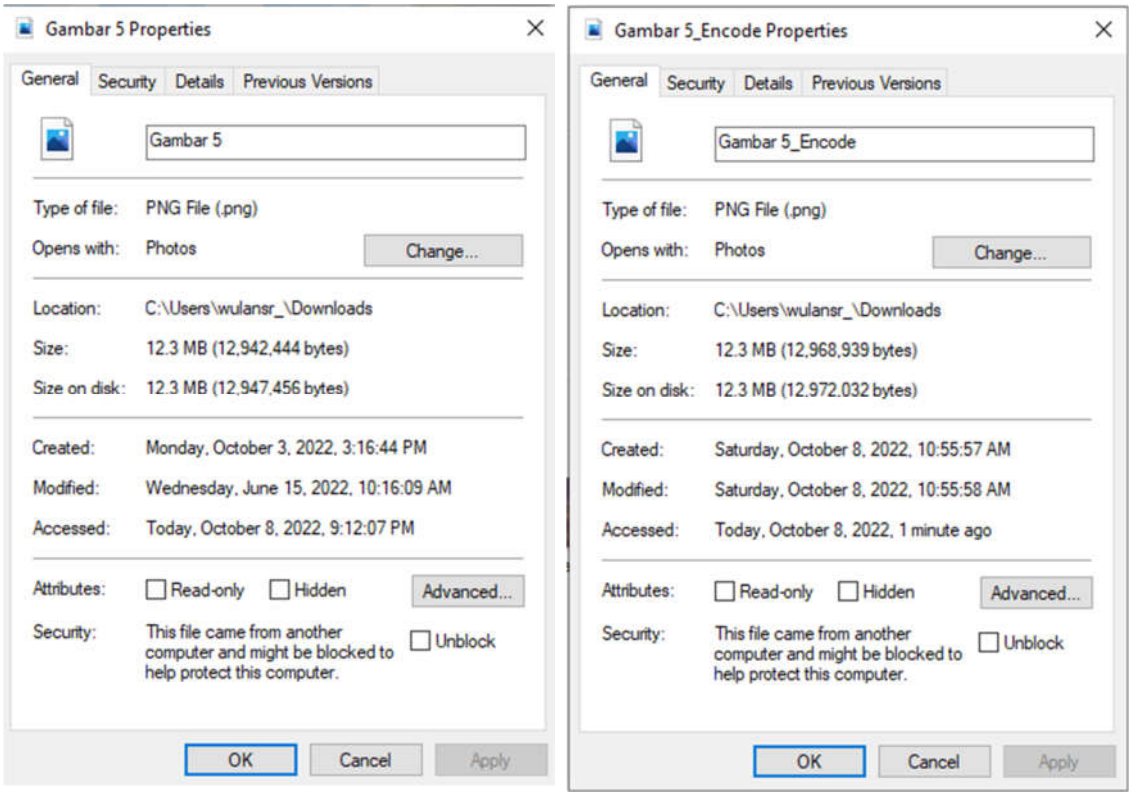
Tabel *Playfair Cipher* dengn kunci "**BOAOWNRZRDH**"

Dari Tabel 4, dapat dilihat bahwa dengan kunci yang telah terenkripsi dapat membuat perubahan susunan karakter pada tabel sebanyak 26 karakter dan untuk jumlah seluruh bitnya, diambil 49 bit mengikuti jumlah seluruh karater yang ada pada tabel *Playfair Cipher*. Hasil yang didapatkan adalag nilai *avalanche effect* sebesar 53,06% dan ini merupakan hasil dari uji coba kekuatan enkripsi menggunakan kriptografi *Vigenere Cipher* dan *Playfair Cipher*.

3.4.2 Metode Steganografi

1. Pengujian ukuran

Pengujian ukuran dilakukan untuk mengetahui adanya pengaruh perubahan ukuran setelah dilakukannya penyisipan pesan ke dalam citra. Hasil yang diperoleh ditampilkan pada Gambar 8.



Ukuran *cover image* Ukuran *stego image*

Gambar 8. Pengujian ukuran

Dari hasil yang diperoleh pada Gambar 8, diketahui bahwa file mengalami perubahan ukuran dari 12.947 Kb menjadi 12.972 Kb. Hal ini menunjukkan bahwa meskipun citra telah disisipi oleh pesan rahasia tidak selalu membuat citra yang dihasilkan tidak mengalami perubahan ukuran secara signifikan.

2. MSE dan PSNR

Pengujian MSE dan PSNR dilakukan dengan tujuan mengetahui rata-rata error dan kualitas dari citra yang dihasilkan dari proses penyisipan pesan menggunakan metode LSB. Berikut adalah hasil yang diperoleh dari pengujian yang telah dilakukan.

```
Pengujian Metode MSE dan PSNR
input Cover Image dan ekstensinya :Gambar 5.png
input Stego Image dan ekstensinya :Gambar 5_Encode.png
Nilai MSE : 0.00013566266164909986
Nilai PSNR : 86.80620027365082 dB
```

Gambar 9. Hasil pengujian MSE dan PSNR

Dilihat dari hasil yang diperoleh dapat dikatakan bahwa metode LSB ini baik digunakan, sebab *noise* yang dihasilkan tidak ada dan *stego image* yang dihasilkan tidak mengalami perubahan yang signifikan terhadap *cover image*.

4. Kesimpulan

Dari hasil penelitian yang diperoleh dapat disimpulkan bahwa hasil *Ciphertext* yang dihasilkan dari kombinasi teknik substitusi antara *Vigenere Cipher* dan *Playfair Cipher* cukup acak dan dapat mengaburkan pola relasi pada *plaintext*. Pesan rumit yang digunakan dalam proses penyisipan dapat dikembalikan menjadi pesan rahasia yang dapat dibaca dengan menggunakan program dan kunci yang sesuai.

Penyisipan pesan menggunakan metode LSB dapat dilakukan dengan file citra berformat PNG dengan jenis RGBA dan pesan yang telah disisipkan dapat diambil kembali menggunakan program dan kunci yang sesuai. Proses penyisipan pesan mengakibatkan citra mengalami kenaikan ukuran kapasitas, akan tetapi kualitas citra hasil steganografi tidak berubah secara signifikan dan tidak dapat dilihat langsung oleh mata manusia sehingga tidak membuat orang lain curiga.

Referensi

[1] R. K. Choubey and A. Hashmi, "Cryptographic Techniques in Information Security," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 1, no. 3, pp. 2456–3307, 2018, [Online]. Available: www.ijsrcseit.com

[2] A. E. Handoyo, D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, and A. Susanto, "Message Concealment and Encryption Technique in Digital Image with Combination of LSB and RSA Methods," *J. Teknol. dan Sist. Komput.*, vol. 6, no. 1, pp. 37–43, Feb. 2018, doi: 10.14710/jtsiskom.6.1.2018.37-43.

[3] A. Hafiz, "Steganografi Berbasis Citra Digital Untuk Menyembunyikan Data Menggunakan Metode Least Significant Bit (LSB)," *J. Cendikia*, vol. XVII, 2019.

[4] A. Claudy Frobenius and E. S. Rachmat Hidayat H S, "Steganografi LSB dengan Modifikasi Kriptografi: Caesar, Vigenere, Hill Cipher Dan Playfair Pada Image," *Melek IT Inf. Technol. Journal.*, vol. 6, no. 1, pp. 33–40, 2020.

[5] L. Budi Handoko, "Sekuriti Teks Menggunakan Vigenere Cipher Dan Hill Cipher," 2022.

[6] A. PANDEY and N. Badal, "A Modified Circular Version of Playfair Cipher," *SSRN Electron. J.*, 2019, doi: 10.2139/ssrn.3351022.

[7] A. O. Modupe, A. E. Adedoyin, and A. O. Titilayo, "A Comparative Analysis of LSB, MSB and PVD Based Image Steganography," *Int. J. Res. Rev.*, vol. 8, no. 9, pp. 373–377, Sep. 2021, doi: 10.52403/ijrr.20210948.

[8] R. Indrayani and Subektiningsih, "Perbandingam Metode LSB, MSB, dan EoF pada Implementasi Steganografi Citra dengan Format JPEG," vol. 12, 2022.

[9] B. K. Yakti and R. H. Prayitno, "Perbandingan Dan Analisa Gambar Pada Steganografi Berdasarkan MSE Dan PSNR," *ICIT J.*, vol. 6, no. 2, pp. 138–152, 2020, doi:

10.33050/icit.v6i2.1105.

[10] B. Deepa, V. Maheswari, and V. Balaji, “An Efficient Cryptosystem Using Playfair Cipher Together with Graph Labeling Techniques,” *J. Phys. Conf. Ser.*, vol. 1964, no. 2, 2021, doi: 10.1088/1742-6596/1964/2/022016.

[11] Aminudin, A. F. Helmi, and S. Arifianto, “Analisa Kombinasi Algoritma Merkle-Hellman Knapsack Dan Logaritma Diskrit Pada Aplikasi Chat,” *J Surg CI Res*, vol. 5, no. 1, pp. 47–55, 2014.

[12] R. Kumar, G. Sharma, and V. Sanduja, “A Real Time Approach to Compare PSNR and MSE Value of Different Original Images and Noise (Salt and Pepper, Speckle, Gaussian) Added Images,” 2018. [Online]. Available: www.ijltemas.in

[13] K. Hani, “Algoritma Kriptografi dan Steganografi Untuk Pengamanan Pesan Ke Dalam Citra,” Universitas Islam Negeri Maulana Malik Ibrahim Malang, 2020.