IMPLEMENTASI ALGORITMA *VIGENERE CHIPER* DAN *LEAST SIGNIFICANT BIT* (LSB) UNTUK MENYEMBUNYIKAN PESAN TEKS

Fajar Haditio [1*], M. Irham [2]

[1,2] Program Studi Sistem Informasi, Fakultas Teknik, Universitas Pamulang
Jl. Puspitek No. 23, Buaran, Serpong, Kota Tangerang selatan 15310

E-mail: haditiofajar@unpam.ac.id

ABSTRAK

IMPLEMENTASI ALGORITMA VIGENERE CHIPER DAN LEAST SIGNIFICANT BIT (LSB) UNTUK MENYEMBUNYIKAN PESAN TEKS. Keamanan sebuah data atau pesan menjadi hal yang penting dalam pertukaran informasi, terlebih jika data atau pesan tersebut merupakan data atau pesan yang bersifat penting dan rahasia agar terhindar dari pencurian data. Ada beberapa teknik yang dapat digunakan untuk menjaga keamanan sebuah data atau pesan, seperti teknik kriptografi dan steganografi. Salah satu algoritma yang digunakan pada kriptografi adalah *Vigenere Chiper* yakni mengubah isi pesan dengan menyandikannya. Algoritma vigenere sendiri terdiri dari algoritma enkripsi dan dekripsi. Sedangkan steganografi adalah menyisipkan data atau pesan pesan kedalam data atau pesan lain sehingga data atau pesan aslinya tidak diketahui keberadaannya. Salah satu algoritma yang mudah diterapkan adalah Least Significant Bit (LSB). Hasil penerapan algoritma Vigenere Chiper dan LSB yaitu pesan dapat disembunyikan pada gambar tanpa mengubah struktur gambar dan memiliki nilai MSE mendekati 0 dengan nilai PNSR lebih dari 40db, selain itu pesan yang dienkripsi pun dapat diacak sesuai perintah dan dapat didekripsi ke bentuk pesan semula.

Kata kunci: Keamanan data, Kriptografi, Steganografi, *Vigenere Chiper, Least Significant Bit*(LSB)

ABSTRACT

IMPLEMENTATION OF VIGENERE CHIPER ALGORITHMAND LEAST SIGNIFICANT BIT (LSB) TO HIDE TEXT MESSAGES. *The security of a data or message becomes important in the exchange of information, especially if the data or messages are data or messages that are important and confidential to avoid data theft. There are several techniques that can be used to maintain the security of a data or message, such as cryptography and steganography techniques. One of the algorithms used in cryptography is Vigenere Chiper ie change the contents of the message by encoding it. The vigenere algorithm itself consists of encryption and decryption algorithms. While steganografi is insert data or message message into data or other message so that data or message original not known existence. One of the easy-to-apply algorithms is the Least Significant Bit (LSB). With the two techniques used are expected to provide security to data or messages that we have. The results of the application of the Vigenere Chiper and LSB algorithms are messages can be hidden in the image without changing the image structure and the MSE value close to 0 db with PNSR value more dan 40 db, and the encrypted message can be scrambled according to the command and can be decrypted to the original message form.*

Keywords: Data security, Cryptography, Steganography, Vigenere Chiper, Least Significant Bit (LSB)

1. PENDAHULUAN

Diera pertukaran informasi sekarang ini, adalah menjadi hal yang biasa dilakukan oleh setiap orang seperti mengirim dan menerima data atau pesan, baik data berupa e-mail, dokumen, maupun berkas pribadi [1]. Namun dalam pertukaran informasi, terdapat aspek keamanan yang memegang peranan penting agar menghindari dari pencurian informasi oleh pihak-pihak yang tidak diinginkan, terutama jika informasi yang dikirim bersifat rahasia [2]. Untuk menangani hal tersebut, dapat dilakukan dengan teknik kriptografi.

Kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data serta otentikasi [3]. Namun disisi lain kriptografi dapat menimbulkan kecurigaan pada orang yang membaca data terenkripsi. Kecurigaan ini dapat memicu orang untuk memecahkan enkripsi tersebut walau membutuhkan waktu yang cukup lama [4]. Teknik lain sebagai upaya pengamanan data atau pesan kita, yaitu dengan menyembunyikan data atau pesan ke dalam data atau pesan lain atau yang biasa disebut teknik steganografi. Steganografi adalah ilmu dan seni menyembunyikan data atau pesan rahasia di dalam data atau pesan lain sehingga keberadaan data atau pesan rahasia tersebut tidak dapat [5]. Metode steganografi yang sederhana dan mudah diimplementasikan adalah metode *Least Significant Bit* (LSB).

Metode penyisipan LSB adalah menyisipkan data atau pesan dengan cara mengganti bit LSB pada representasi biner file gambar dengan representasi biner dari data atau pesan rahasia yang akan disembunyikan. Media yang digunakan untuk teknik steganografi adalah file gambar atau citra digital. Definisi citra menurut Kamus Webster adalah suatu representasi, kemiripan, atau imitasi dari suatu obyek atau benda [6]. Kelemahan dari metode LSB adalah data atau pesan rahasia yang disi sipkan dapat dengan mudah diambil dengan menggunakan metode LSB. Namun dengan metode ini memiliki kelebihan yang dapat menutupi kelemahan kriptografi yaitu menyembunyikan data.

Dari pemaparan di atas, penulis bermaksud menerapkan gabungan teknik Kriptografi metode Vigenere dan teknik Steganografi metode *Least Significant Bit* (LSB) kedalam sebuah aplikasi untuk menjaga keamanan data atau pesan kita. Algoritma vigenere dipilih karena algoritma ini dibandingkan dengan algoritma monoalfabetik lainnya adalah sandi ini tidak begitu rentan terhadap metode pemecahan sandi yang disebut analisis frekuensi. Sedangkan metode LSB dipilih untuk mengkamuflasekan data atau pesan teks. Selain itu, hal ini juga untuk menutupi kelemahan Algoritma Vigenere Data atau pesan akan diubah dengan menyandikannya (Enkripsi) terlebih dahulu menggunakan algoritma Vigenere, dan setelah itu kita sisipkan ke dalam gambar menggunakan metode LSB.

2. TINJAUAN PUSTAKA

Terdapat beberapa penelitian tentang kriptografi dan steganografi yang sudah dilakukan diantaranya :

Penelitian yang dilakukan oleh Toni [7] meneliti tentang perbandingan metode LSB dan EOF untuk steganografi citra *digital*, hasil dari penelitian tersebut menunjukan kelebihan metode LSB lebih banyak dibandingkan dengan metode EOF. Hal tersebut dikrekan pesan yang tela disisipkan ke daam citra digital menggunaan metode LSP mengalami sedikit penurunan kualitas citra yang tidak terlalu berpengaruh terhadap mata manusia dibanding dengan menggunakan metode EOF.

Selain itu penelitian yang dilakukan oleh Priyono [2] yang mengamankan pesan teks menggunakan metode *caesar chiper* untuk enkripsi isi pesan. Namun enkripsi pada *Caesar Chipper* hanya dengan menggeser masing-masing karakter pesan dengan kunci yang sama, sehingga jika kunci yang digunakan untuk enkripsi diketahui maka akan dengan mudah memecahkan pesan yang telah dienkripsi sebelumnya. Oleh karena itu penambahan algoritma *vigenere chipper* digunakan untuk menambah keamanan pesan karena enkripsi pada vigenere chipper menggnakan kunci yang tidak sama ditiap karakternya.

Penelitian yang dilakukan oleh Taufik dan Aditama [4] yang menggabungkan algoritma enkripsi RSA dan steganografi LSB untuk mengamankan pesan digital. Kesimpulan yang diperoleh yaitu data hasil image setelah dilakukan proses *encoding* pesan menggunakan LSB menunjukan angka MSE dan PNSR yang baik, yaitu menunjukan nilai MSE hamper mendekati angka 0 db dan nilai PNSR lebih dari 40 db.

Penelitian lain yang dilakukan oleh Abduh Riski [8] menunjukan bahwa algoritma

vigenere chipper tidak hanya dapat digunakan untuk mengamankan pesan teks, tetapi juga dapat mengamnkan informasi pribadi yang bersifat rahasia seperti data rekam medis pasien. Hal ini menunjukan bahwa algoritma ini dapat diandalkan untuk melakukan penyamaran dan pengamanan suatuu informasi dengan baik

3. METODOLOGI

Penelitian terkait pengamanan pesan teks ini dilakukan melalui beberapa tahapan penelitian agar lebih sistematis dan terarah. Tahapan ini juga mempermudah dalam penulisan artikel. Tahapan ini bisa dilihat pada gambar 1.

Gambar 1. Tahapan Penelitian

Berdasarkan gambar 1, tahapan penelitian ini dimulai dengan melakukan kajian atau tinjauan pustaka. Tinjauan pustaka dilakukan untuk mengumpulkan untuk mempelajari dan mengumpulkan informasi dari berbagai penelitiartikel maupun jurnal ilmiah yang memiliki keterkaitan dan relevan dengan penelitian yang dilakukan. Informasi tersebut berkaitan dengan algortima *vigenere chiper*, *LSB* dan penelitian-penelitian sebelumnya. Hasil dari penelitian-penelitian sebelumnya dapat dilihat pada bagian tinjauan pustaka.

Tahapan selanjutnya setelah melakukan tinjauan pustaka adalah merancang konsep pengamanan pesan teks. Konsep pengamanan pesan teks akan mengkombinasikan algortima *vigenere chiper* dan algortima *LSB*. Konsep pengamanan tersebut dapat dilihat pada gambar.

Setelah konsep pengamanan pesan teks dibuat, tahapan selanjutnya adalah dengan menerapkan konsep pengamanan pesan teks pada bebrapa contoh kasus. Tahapan penelitian selanjutnya membahas terhadap hasil dari penerpan konsep pengamanan tersebut. Tahapan terakhir dari penelitian ini adalah membuat atau menarik kesimpulan dari penerapan konsep yang telah dilakukan.

3.1 Daftar Karakter

Karakter-karakter yang digunakan pada penelitian ini akan menggunakan karakter tertentu atau sudah ditentukan. Daftar karakter tersebut dapat dilihat pada tabel 1.

Tabel 1. Daftar Karakter Yang Digunakan

Desimal	Simbol	Desimal	Simbol
0	A	48	(
1	n	49	)
2	B	50	_
3	o	51	+
4	C	52	-
5	p	53	=
6	D	54	tab
7	q	55	a
8	E	56	N
9	r	57	b
10	F	58	O
11	s	59	c
12	G	60	P
13	t	61	d
14	H	62	Q
15	u	63	e
16	I	64	R
17	v	65	f
18	J	66	S
19	w	67	g
20	K	68	T
21	x	69	h
22	L	70	U
23	y	71	i
24	M	72	V

25	z	73	j
26	\n atau Enter	74	W
27	0	75	k
28	1	76	X
29	2	77	l
30	3	78	Y
31	4	79	m
32	5	80	Z
33	6	81	<
34	7	82	>
35	8	83	,
36	9	84	.
37	spasi	85	?
38	!	86	/
39	@	87	:
40	#	88	;
41	$	89	{
42	%	90	}
43	^	91	[
44	&	92	]
45	*	93	`
46	"	94	~
47	‘	95	\

Pada tabel 1 berisi karakter-karakter yang akan digunakan untukproses enkripsi dan dekripsi menggunkan algoritma *vigenere chiper*. Karakter-karakter tersebut terdiri dari huruf kecil maupun kapital dan beberapa simbol yang terdapat pada keyboard.

3.2 Proses Enkripsi dan *Encode*

Enkripsi merupakan proses pengubahan data asli menjadi data acak berdarakan kunci yang telah ditentukan. Sedangkan Encode merupakan proses penyisipan data ke dalam sebuah media gambar atau video.

Secara keseluruhan proses enkripsi dan *encode* teks pesan pada penelitian ini dapat dilihat pada Gambar 2.

Gambar 2. Proses Enkripsi dan *Encode* Teks Pesan

Terlihat pada gambar 2 terdapat 6 tahapan untuk melakukan pengamanan teks pesan dalam proses enkripsi menggunakan algoritma *vigenere chiper* dan *encode* hasil enkripsi menggunakan algoritma LSB.

Tahapan pertama adalah menentukan plain teks atau teks yang masih bisa dipahami yang akan diacak melalui proses enkripsi. Pada tahap ini pula penentuan kunci untuk proses enkripsi ditentukan [9], kunci ini pula yang akan digunakan untuk proses dekripsi.

Selanjutnya palin teks yang sudah dienkripsi menjadi *chiper* teks akan disisipkan kedalam sebuah gambar melalui proses *encode*. Pada tahap ini tidak memerlukan kunci karena *chiper* teks akan langsung disisipkan ke dalam sebuah gambar.

Rumus yang digunakan untuk melakukan proses enkripsi dapat dilihat pada persamaan 1, sedangkan untuk dekripsi menggunakan persamaan 2.

$$Ci = Ek(Mi) = (Mi + Ki) \bmod 96 \quad (1)$$

Dimana jika Ci > 96 maka Ci - 96

$$Mi = Dk(Ci) = (Ci - Ki) \bmod 96 \quad (2)$$

Dimana Jika Mi < 0 maka Mi + 96

Persamaan 1 merupakan rumus enkripsi algortima *vigenere chiper.* Dengan

ketentuan “Ci” merupakan *chipertext* yang akan terbentuk, “Mi” merupakan pesan teks berupa *palin* teks dan “Ki” merupakan kunci untuk proses enkripsi.

Contoh sederhana pada penerapan persamaan 1 seperti tabel 2 di bawah ini.

Tabel 2. Contoh Enkripsi Vigenere

Plainteks	T	A
Key	S	S
Hasil Enkripsi		
*Cipher*teks	!	S

Contoh huruf T yang memiliki nilai desimal 84 dan huruf S yang memiliki nilai desimal 67, jika dimasukan ke dalam persamaan 1 adalah.

Huruf T

(Huruf T) Ci = (68+66) mod 96

(Huruf T) Ci = 38 (Karakter !)

Dan Huruf A

(Huruf A) Ci = (0+66) mod 96

(Huruf A) Ci = 66 (Huruf S)

Selanjutnya chiper teks akan di encode menggunakan algoritma LSB. Algoritma LSB merupakan metode steganografi yang paling sederhana dan mudah diimplementasikan [10]. Metode ini menggunakan citra digital sebagai covertext. Pada susunan bit di dalam sebuah byte (1 *byte* = 8 bit), ada bit yang paling berpengaruh (most significant bit atau MSB) dan bit yang paling kurang berpengaruh (least significant bit atau LSB). Sebagai contoh byte 11010010, angka bit 1 (pertama, digaris-bawahi) adalah bit MSB, dan angka bit 0 (terakhir, digaris-bawahi) adalah bit LSB [11]. Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan byte tersebut menyatakan warna merah, maka perubahan satu bit LSB tidak mengubah warna merah tersebut secara berarti. Mata manusia tidak dapat membedakan perubahan kecil tersebut. Seperti contoh di bawah ini, sebelum segmen pixel-pixel sebuah citra ditambahkan.

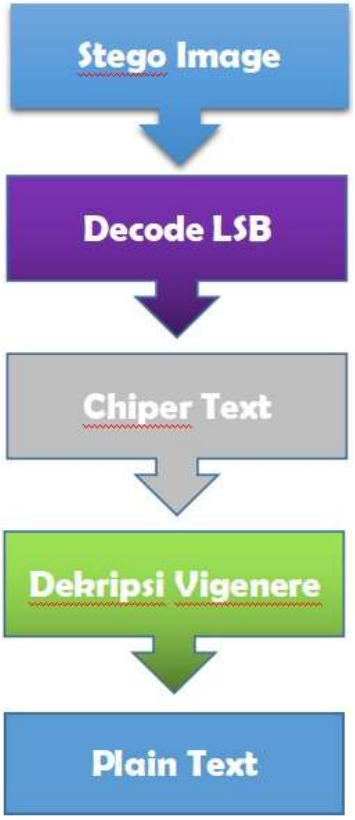
00110011 10100010 11100010 10101011
00100110 10010110 11001001 10001000
10100011

Kemudian pesan rahasia yang sudah dikonversi menjadi bilangan biner, contoh di atas karakter ! (angka desimal 38) menjadi bilangan biner yaitu 00100001. Maka setiap bit dari pesan tersebut menggantikan posisi LSB dari segmen *pixel-pixel* citra di atas menjadi.

00110010 10100010 11100011 10101010
00100110 10010110 11001000 10001000
10100011

3.3 Proses Dekripsi dan *Decode*

Proses dekripsi dan *decode* pesan teks yang sudah dienkripsi dan disembunyikan melalui proses *decode*, secara keseluruhan dapat dilihat pada gambar 3 di bawah ini.



Gambar 3. Proses *Decode* dan Dekripsi Pesan Teks

Pada proses di atas terlihat bahwa, proses *decoding* dan dekripsi pesan teks ini merupakan proses kebalikan dari proses enkripsi dan *decode* pesan teks sebelumnya.

Langkah pertama diawali dengan memilih gambar *stegoimage* yang berisi pesan teks yang sudah dienkripsi. Selanjutnya gambar tersebut akan diproses melalui proses *decoding* untuk mengambil bit terlemah dari gambar untuk diekstraksi menjadi pesan teks yang dienkripsi.

Pesan teks enkripsi yang sudah diekstaraksi selanjutnya akan dideksripsi menjadi palin teks, pada proses ini memerlukan kunci yang sama seperti pada

proses enkripsi untuk mendapatkan pesan aslinya.

Seperti pada proses *encoding* sebelumnya, dimana segmen *pixel-pixel* citra yang sudah diproses menjadi bentuk seperti di bawah ini.

00110010 10100010 11100011 10101010
00100110 10010110 11001000 10001000
10100011

Kemudian bit-bit terlemah diambil untuk dikonversi menjadi bilangan biner menjadi 00100001. Selanjutnya bilangan biner ini akan di konversi kembali menjadi karakter !

Proses selanjutnya adalah mendekripsikan pesan yang sudah didapat dari proses *decoding* untuk di dekripsi menjadi pesan aslinya.

Rumus yang digunakan untuk proses dekripsi ini dapat dilihat pada persamaan 2. dimana "Ci" merupakan chiper teks yang akan didekripsi, "Ki" yang merupakan kunci dan "Pi" yang merupakan palin teks atau hasil dari proses dekripsi.

Sebagai contoh penerapan persamaan 2 di atas dapat dilihat pada tabel 3.

Tabel 3 Contoh Dekripsi Vigener

*Cipher*teks	!	S
Key	S	S
Hasil Enkripsi		
Plainteks	T	A

Contoh karakter ! yang memiliki nilai desimal 38 dan huruf S yang memiliki nilai desimal 66, jika dimasukan ke dalam persamaan 1 adalah.

Huruf T

(Huruf T) Ci = (66-38) mod 96

(Huruf T) Ci = 68 (Huruf T)

Dan Huruf A

(Huruf A) Ci = (66-66) mod 96

(Huruf A) Ci = 0 (Huruf A)

3.4 Parameter Pembanding

Parameter pembanding image sebelum dan sesudah penyisipan pesan yang digunakan yaitu *Mean Square Error (MSE)* dan *Peak Signal to Noise Ratio (PSNR)*. Parameter ini digunakan untuk membandingkan antara kedua metode pada hasil penyisipannya.

3.4.1 *Means Square Error (MSE)*

Mean Squared Error (MSE) digunakan untuk mengukur kinerja algoritma steganografi pada sebuah citra. Citra cover dibandingkan dengan citra sisipan dengan memeriksa selisih nilainya. Perhitungan nilai MSE dari citra berukuran M x N pixel, dilakukan sesuai dengan rumus pada persamaan dibawah ini :

$$MSE = \frac{1}{M * N} \sum_{x=1}^{M} \sum_{y=1}^{N} (f(x,y) - f'(x,y))^2$$

Keterangan :
M dan N : ukuran panjang dan lebar citra.
f(x,y) : intensitas citra di titik (x,y) dari citra yang asli.
f'(x,y) : intensitas citra di titik (x,y) dari citra hasil penyisipan.

Semakin kecil nilai MSE mendekati nilai 0, semakin baik prosedur yang dilakukan dalam proses penyisipan. Artinya kualitas citra setelah dilakukan penyisipan pesan hampir sama dengan kualitas citra asalnya karena memiliki tingkat kesalahan yang kecil [7].

3.4.1 *Peak Signal to Noise Ratio (PSNR)*

Peak Signal to Noise Ratio (PSNR) merupakan nilai yang menunjukkan tingkat toleransi noise tertentu pada banyaknya noise suatu sinyal citra. *Noise* merupakan kerusakan sinyal pada bagian tertentu dalam sebuah citra sehingga mengurangi kualitas sinyal tersebut. Persamaan untuk menghitung PSNR.

$$PSNR = 20^* \log\left(\frac{255}{\sqrt{MSE}}\right)$$

Keterangan :
MSE adalah nilai *Mean Squared Error*

Berbanding terbalik dengan nilai MSE, semakin besar nilai PSNR maka aka semakin baik kulitas citra steganografi. Citra yang memiliki nilai PNSR di bawah 30 db dikategorikan buruk, sedangkan nilai PNSR lebih besar atau sama dengan 40 db dikategorikan baik [7].

4. HASIL DAN PEMBAHASAN

Pada bagian ini akan menerapkan algoritma vigenere dan LSB menjadi sebuah aplikasi bernama *vigetegano.* Implementasi kasus berdasarkan proses yang ditunjukan pada gambar 2 dan 3. Pesan teks yang akan digunakan sebagai contoh kasus pada penelitian ini adalah "Wabah Covid 19" dengan kunci pesan "Bahaya".

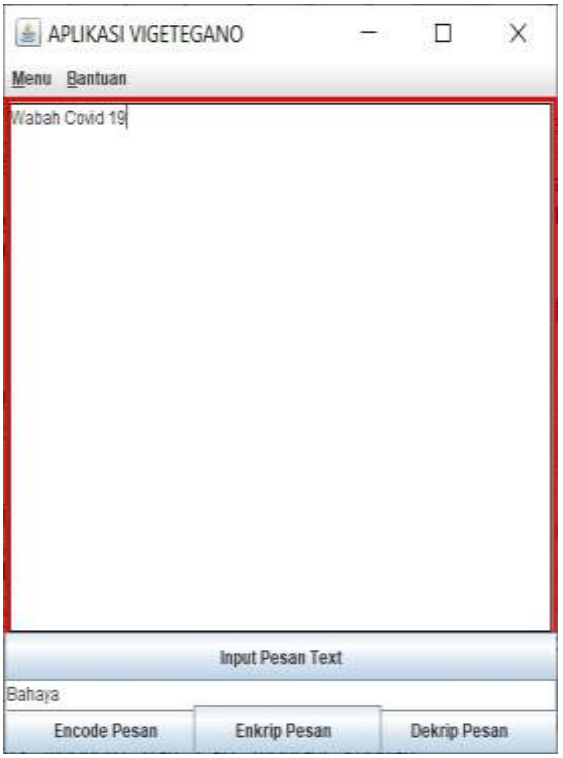
4.1 Proses Enkripsi Pesan

Pada bagian ini pesan yang masih berbentuk palinteks akan dienkripsi menjadi chiper seperti pada tabel 4 secara manual dan membandingkan hasil enkripsi menggunakan aplikasi vigetegano seperti gambar 4 dan 5.

Tabel 4 Enkripsi Pesan Secara Manual

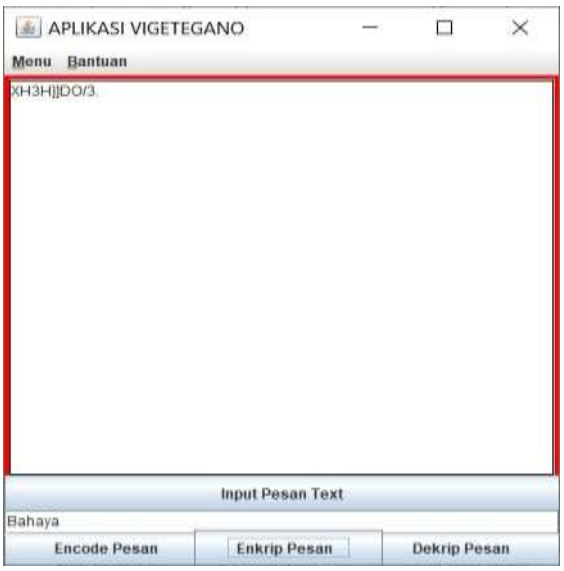
Plain (Mi)		Kunci (Ki)		(Mi+Ki) mod 96	Hasil	Chiper (Ci)
W	74	B	2	(74+2)mod96	76	X
a	55	a	55	(55+55) mod96	14	H
b	57	h	69	(57+69) mod96	30	3
a	55	a	55	(55+55) mod96	14	H
h	69	y	23	(69+23) mod96	92	]
spasi	37	a	55	(37+55) mod96	92	]
C	4	B	2	(4+2)mod96	6	D
o	3	a	55	(3+55)mod96	58	O
v	17	h	69	(17+69) mod96	86	/
i	71	a	55	(71+55) mod96	30	3
d	61	y	23	(61+23) mod96	84	.
spasi	37	a	55	(37+55) mod96	92	]
1	28	B	2	(28+2)mod96	30	3
9	36	a	55	(36+55) mod96	91	[

Tabel di atas merupakan hasil enkipsi menggunakan algoritma *vigenere chiper*, dimana teks hasil enkripsi ini memiliki perbedaan bentuk dan isi antara pesan asli dengan pesan hasil enkripsi. Sedangkan jika menggunakan aplikasi vigetegano seperti ditunjukan gambar 4 dan 5 di bawah ini.



Gambar 4 Proses pada Aplikasi *Vigetegano*

Hasil enkripsi pada aplikasi vigetegano ditunjukan seperti gambar di bawah ini.



Gambar 5 Hasil Enkripsi *Vigetegano*

Pada gambar di atas terlihat bahwa proses enkripsi pada pesan teks telah merubah bentuk pesan aslinya menjadi pesan yang sulit dipahami makna aslinya.

Jika dibandingkan antara pesan asli yaitu “Wabah Covid 19” yang kita bisa pahami maknanya sebagai sebuah peringatan menjadi “XH3H]]DO/3.]3[” yang sulit dipahami maknanya. Hasil inilah yang menjadi tujuan sebenarnya dari proses enkripsi yaitu mengamankan pesan teks dari makna aslinya menjadi makna yang sulit dipahami.

4.2 Proses Encoding Pesan

Proses selanjutnya adalah mengencoding chiper teks yang sudah terbentuk untuk disisipkan ke dalam sebuah gambar pada aplikasi vigetego. Proses ini seperti ditunjukan pada gambar 6.

Gambar 6 Proses *Encoding* pada Aplikasi Vigetegano

Hasil dari proses encoding ditunjukan pada tabel 5, dimana akan membandingan dua gambar sebelum dan sesudah proses *encoding*. Proses *encoding* pesan dilakukan sebanyak tiga kali dengan jumlah karakter yang berbeda-beda pada masing-masing percobaan.

Table 5. Perbandingan Sebelum dan sesudah encoding

Gambar asli (Size: 362 Kb)

Gambar Setelah Encoding 1 (Size: 362 Kb)

Jumlah Karakter Sisipan: 14 Karakter MSE: 0.0000986 db dan PNSR: 88.19 db
Gambar Setelah Encoding 2 (Size: 363 Kb)

Jumlah Karakter Sisipan: 289 Karakter MSE: 0.0016 db dan PNSR: 75.98 db
Gambar Setelah Encoding 3 (Size: 364 Kb)

Jumlah Karakter Sisipan: 867 Karakter MSE: 0.0049 db dan PNSR: 71.22 db

Berdasarkan tabel 5 di atas, bahwa perbandingan antara gambar asli dan gambar setelah dilakukan proses *encoding* tidak memiliki perbedaan secara kasat mata secara visual. Sedangkan dari segi ukuran pun tidak terlalu jauh berbeda, dimana gambar setelah proses *encoding* memiliki ukuran yang lebih besar, hal ini dikarenakan

gambar tersebut sudah disisipi teks hasil enkripsi.

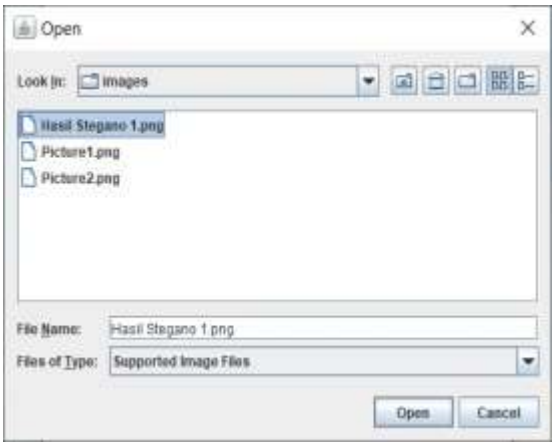
Dari ketiga gambar hasil dari proses encoding LSB menunjukan bahwa semakin banyak karakter yang disisipkan kedalam gambar akan menghasilkan ukuran gambar stego yang semakin besar pula. Selain itu nilai MSE dan PNSR dari masing-masing gambar mengalami penurunan kualitas gambar, dimana nilai MSE yang semakin membesar dan nilai PNSR yang semakin kecil. Hal ini dikarenakan semakin banyak karakter yang disisipkan ke dalam gambar, akan menjadikan nilai dari setiap bit-bit yang terdapat pada gambar akan terganti oleh bit-bit dari karakter pesan.

Meskipun peningkatan nilai MSE dan penurunan nilai PNSR yang didapat mengalami perubahan, namun hal tersebut masih menunjukan nilai dengan kategori baik. Nilai MSE yang diperoleh mendekati angka 0 yang artinya memiliki kesalahan yang hampir tidak ada, sedangkan nilai PNSR yang didapat lebih dari 40 yang termasuk kategori baik.

4.3 Proses *Decoding* Pesan

Pada tahap selanjutnya, akan dilakukan pengujian untuk mengekstrasi gambar yang berisi teks enkripsi. Proses ini ditunjukan oleh gambar 7, 8 dan 9.

Langkah pertama adalah dengan memilih gambar yang berisi pesan yang sudah berbentuk chiper.



Gambar 7. Pilih Gambar Yang Berisi Chiper Teks

Kemudian pilih dan klik tombol “Decode Gambar ke Pesan” untuk melakukan proses decoding yang akan diproses oleh aplikasi seperti gambar 8.

Gambar 8. Proses Decoding Oleh Aplikasi

Kemudian aplikasi akan melakakukan proses decoding gambar untuk mengekstrasi gambar menjadi pesan perbentuk teks chiper seperti gambar 9.

Gambar 9. Hasil Proses Decoding pada Gambar Stego

Dapat terlihat bahwa hasil ekstraksi gambar pada proses *decoding* di atas menghasilkan pesan teks chiper yang sama persis seperti pada proses enkripsi pada gambar 6. Proses ini menunjukan jika proses encoding tidak merubah pesan teks chiper pada proses enkripsi ketika disisipkan ke dalam gambar, sehingga pesan yang diekstraksi sama persis. Proses selanjutnya adalah mendekripsi pesan teks chiper menjadi pesan atau teks aslinya sebelum

dilakukan proses enkripsi pada gambar 10 dan 11.

4.4 Dekripsi Pesan

Tahapan selanjutnya adalah mendekripsikan pesan teks chiper menjadi pesan aslinya menjadi plainteks sebelum dilakukan proses enkripsi. Proses ini akan mengembalikan pesan teks chiper yang akan ditranslasikan menggunakan kunci yang sama seperti pada proses enkripsi.

Proses ini akan ditunjukan oleh tabel 5 proses enkripsi secara manual dan gambar 10 dan 11 dengan menggunakan aplikasi *Vigetegano.*

Table 5. Proses Dekripsi Secara Manual

Plain (Mi)		Kunci (Ki)		(Mi+Ki)mod 96	Hasil	Chiper (Ci)
X	76	B	2	(76-2)mod96	74	W
H	14	a	55	(14-55)mod96	55	a
3	30	h	69	(30-69)mod96	57	b
H	14	a	55	(14-5)mod96	55	a
]	92	y	23	(92-23)mod96	69	h
]	92	a	55	(92-55)mod96	37	
D	6	B	2	(6-2)mod96	4	C
O	58	a	55	(58-55)mod96	3	o
/	86	h	69	(86-69)mod96	17	v
3	30	a	55	(30-55)mod96	71	i
.	84	y	23	(84-23)mod96	61	d
]	92	a	55	(92-55)mod96	37	
3	30	B	2	(30-2)mod96	28	1
[	91	a	55	(91-55)mod96	36	9

Pada proses dekripsi secara manual pada tabel di atas terlihat bahwa pesan yang berbentuk teks chiper dapat dikembalikan ke bentuk semula dengan menggunakan kunci yang sama dengan kunci yang digunakan ketika proses enkrisi sebelumnya. Proses dekripsi tidak akan berhasil mengembalikan pesan ke bentuk semula ketika proses sebelum enkripsi jika menggunakan kunci yang berbeda. Perbedaan hasil dekripsi jika menggunakan kunci yang berbeda ditunjukan pada tabel 6, dimana kunci sebenarnya adalah “bahaya” diganti dengan “Danger”.

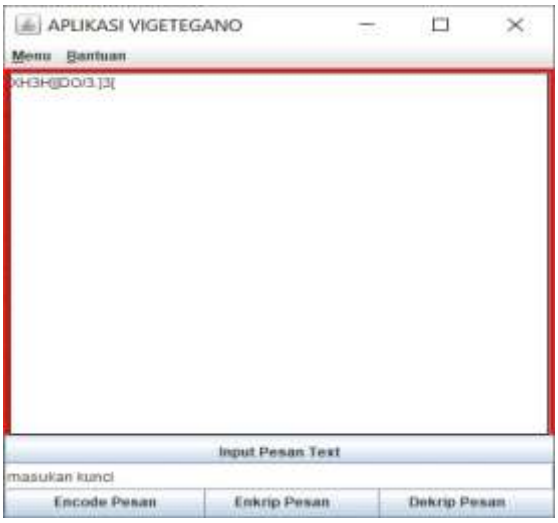
Table 6. Proses Dekripsi Menggunakan Kunci Yang Berbeda

Plain (Mi)		Kunci (Ki)		(Mi+Ki)mod 96	Hasil	Chiper (Ci)
X	76	D	6	(76-6)mod96	70	U
H	14	a	55	(14-55)mod96	55	a
3	30	n	1	(30-1)mod96	29	2
H	14	g	67	(14-67)mod96	43	^
]	92	e	63	(92-63)mod96	29	2
]	92	r	9	(92-9)mod96	83	,
D	6	D	6	(6-6)mod96	0	A
O	58	a	55	(58-55)mod96	3	o
/	86	n	1	(86-1)mod96	85	?
3	30	g	67	(30-	59	c

				67)mod96		
.	84	e	63	(84-63)mod96	21	x
]	92	r	9	(92-9)mod96	83	,
3	30	D	6	(30-6)mod96	24	M
[	91	a	55	(91-55)mod96	36	9

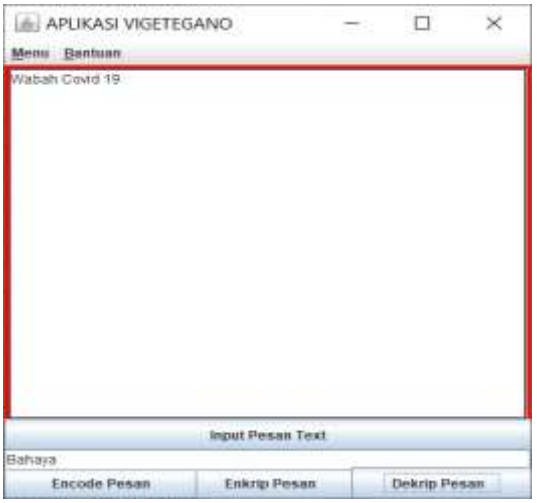
Dapat terlihat pada tabel dekripsi di atas, jika menggunakan kunci yang berbeda dari kunci aslinya akan menghasilkan palinteks yang berbeda dimana pesan teks aslinya. Proses dekripsi dengan menggunakan kunci "Bahaya" akan menghasilkan palinteks "Wabah Covid 19", sedangkan jika menggunakan kunci "Danger" akan menghasilkan palinteks "Ua2^2,Ao?cx,M9" yang berbeda jauh dengan pesan aslinya.

Selain itu jika proses dekripsi dengan menggunakan aplikasi *Vigetegano* akan ditunjukan pada gambar 10 dan 11.



Gambar 10. Chiper Teks Yang Akan Didekripsi

Untuk melakukan dekripsi chiper teks pada aplikasi Vigetegano adalah cukup dengan memasukan kunci pada kolom "masukan kunci" yang akan digunakan oleh aplikasi mendekripsikan chiper teks. Selanjutanya pesan aka didekripsikan dengan menekan tombol "Dekripsi Pesan" dan hasil dekripsinya ditunjukan oleh gambar 11.



Gambar 11. Proses Dekripsi Pada Aplikasi Vigetegano

Dapat terlihat pada gambar di atas bahwa dekripsi pesan dapat dilakukan oleh aplikasi vigetegano dengan mengembalikan pesan teks chiper menjadi palinteks seperti bentuk semula.

5. KESIMPULAN

Berdasarkan penelitian dan pembahasan pada penelitian ini dapat disimpulkan yaitu penerapan algoritma vigenere chiper dapat menyembunyikan pesan dengan menyamarkan pesan aslinya ke dalam bentuk teks chiper. Selain itu teks chiper disembunyikan ke dalam gambar untuk menambah pengamanan dengan tidak terlalu mengubah bentuk gambar aslinya. Hasil ini ditunjukan dengan nilai MSE yang didapat menunjukan angka mendekati 0, dan nilai PNSR lebih dari 40 db.

Untuk saran pengembangan penelitian selanjutnya dapat menerapkan algoritma enkripsi asimetris agar menambah tingkat keamanan enkripsi pesan, selain itu dapat menerapkan penggunaan video untuk media penyisipan pesan atau informasi sehingga tidak hanya menggunakan gambar sebagai media penyembunyian pesan.

DAFTAR PUSTAKA

[1] A. A. Permana, "Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android," *J. Al-AZHAR Indones. SERI SAINS DAN*

Teknol., vol. 4, no. 3, p. 110, 2018, doi: 10.36722/sst.v4i3.280.

[2] P. Priyono, “Penerapan Algoritma Caesar Cipher Dan Algoritma Vigenere Cipher Dalam Pengamanan Pesan Teks,” *J. Ris. Komput.*, vol. 3, Nomor:, no. Algoritma Caesar Cipher, pp. 351–356, 2016.

[3] A. Menez, P. VanOorschot, and S. Vanstone, *Handbook of Applied Cryptography*. 1997.

[4] T. R. Kuncoro and R. Aditama, “Analisis Kombinasi Algoritma Kriptografi Rsa Dan Algoritma Steganografi Least Significant Bit (Lsb) Dalam Pengamanan Pesan Digital,” *Statmat J. Stat. Dan Mat.*, vol. 1, no. 2, pp. 60–82, 2019, doi: 10.32493/sm.v1i2.2947.

[5] R. Munir, *Kriptografi*. Bandung: Informatika, 2006.

[6] A. I. . Balza and M. Firdausy, *Teknik Pengolahan Citra Digital Menggunakan Delphi*. Yogyakarta: Andi, 2005.

[7] T. Sahata P, “Analisa Perbandingan Least Significant Bit (Lsb) Dan End of File (Eof) Untuk Steganografi Citra Digital Menggunakan Matlab,” *J. INFOTEK*, vol. 1, no. 3, pp. 187–194, 2016.

[8] M. Z. A. ABDUH RISKI, AHMAD KAMSYAKAWUNI, “IMPLEMENTASI VIGENERE CIPHER PADA Pendahuluan Citra Digital,” vol. 02, no. 01, pp. 23–30, 2018.

[9] G. Dwi, Rumani, and M. Nasrun, “Implementation of Cryptography and Steganography in Image Media Using the Blowfish Algorithm and the Least Significant Bit Method,” *e-Proceeding Eng.*, vol. 2, no. 2, pp. 3762–3769, 2015.

[10] Z. A. I. Niswati, “STEGANOGRAFI BERBASIS LEAST SIGNIFICANT BIT (LSB) Abstrak . Penelitian ini bertujuan untuk menerapkan metode LSB untuk menyisipkan pesan gambar ke gambar grayscale . Hal ini diperlukan karena sering terjadi bahwa pesan gambar dikirim adalah pesan rahasi,” vol. 5, no. 2, pp. 181–191, 1979, [Online]. Available: https://journal.lppmunindra.ac.id/index.php/Faktor_Exacta/article/download/194/185.

[11] P. H. Rantelinggi, E. Saputra, J. T. Informatika, U. Papua, and P. Korespondensi, “Algoritma Kriptografi Triple Des Dan Steganografi Lsb Sebagai Triple Des Cryptography Algorithm and Lsb Steganography As,” vol. 7, no. 4, 2020, doi: 10.25126/jtiik.202071838.