DINAMIKA REKAYASA
http://dinarek.unsoed.ac.id

Vol. 16 No. 2 (2020) Hal. 139 - 146
p-ISSN1858-3075 **| e-ISSN 2527-6131**

LSB STEGANO PADA KOMBINASI KRITPOGRAFI SIMETRIS CAESAR-VIGENERE

LSB STEGANO IN COMBINATION OF SYMETRIC CRYPTOGRAPHY CAESAR-VIGENERE

Ibnu Utomo Wahyu Mulyono[1*], Ajib Susanto[2], Yupie Kusumawati[3]

*Email: ibnu.utomo.wm@dsn.dinus.ac.id

[1,2]Prodi Teknik Informatika, Universitas Dian Nuswantoro
[3]Prodi Sistem Informasi, Universitas Dian Nuswantoro

Abstrak—Dalam perkembangan teknologi komunikasi data, dan banyaknya problem mengenai manipulasi data maka perlu tindak lanjut mengenai teknik untuk mengamankan data. Steganografi adalah sebuah teknik untuk menyembunyikan pesan dengan menggunakan sebuah media atau juga disebut *cover*. Sedangkan LSB (*Least Significant Bit*) adalah sebagai algoritma atau metode menyembunyikan pesan yang akan disisipkan. Seperti pada perangkat keamanan lainnya, steganografi dapat digunakan sebagai pengamanan seperti citra dengan *watermarking* dengan alasan untuk perlindungan *copyright*. Metode LSB yang digunakan pada teknik *steganography* tergolong mudah pada penerapannya. Dasar dari metode ini adalah bilangan berbasis biner atau dengan kata lain angka 1 dan angka 0. Metode LSB berhubungan dengan ukuran 1 bit dan ukuran 1 *byte*. 1 *byte* yang terdiri dari 8 bit data. Dalam penelitian ini dilakukan penggabungan metode LSB dengan teknik super enkripsi kriptografi metode *Caesar Cipher* dan *Vigenere Cipher*. Kontribusi yang diberikan adalah melakukan proses LSB pada bit ke 7 dan ke 8 sehingga *imperceptibility* meningkat. Dari hasil penggabungan metode antara LSB dan kriptografi akan sulit dipecahkan, karena memiliki dua tingkat keamanan. Dapat disimpulkan bahwa sistem pengamanan pesan menggunakan kriptografi dan steganografi terbagi menjadi empat, yaitu *encode, decode*, enkripsi dan dekripsi. Tujuan utama untuk mengamankan subtansi data rahasia dengan cara menyamarkan dengan sebuah media agar sulit untuk teridentifikasi.

Kata kunci— LSB, kriptografi, stegano, *cipher*

Abstract—*In the development of data communication technology, and the many problems regarding data manipulation, it is necessary to follow up on techniques to secure data. Steganography is a technique for hiding messages by using a media or also called a cover. While LSB (Least Significant Bit) is an algorithm or method of hiding messages to be inserted. As with other security devices, steganography can be used as security such as imagery with watermarking on the grounds for copyright protection. The LSB method used in steganography techniques is relatively easy to apply. The basis of this method is binary based numbers or in other words number 1 and number 0. The LSB method is related to the size of 1 bit and size of 1 byte. 1 byte consisting of 8 data bits. In this study the authors combined the LSB method with the Cryptography Super Cryptography and Vigenere Cipher method. The contribution given to this research is to carry out the LSB process on the 7th and 8th bits so that impercepibility increases. From the results of the merging of methods between LSB and cryptography will be difficult to solve, because it has two levels of security. It can be concluded that the message security system using cryptography and steganography is divided into four, namely encode, decode, encryption and decryption. The main objective is to secure the substance of confidential data by disguising it with a media so that it is difficult to identify.*

Keywords— *LSB, cryptography, stegano, cipher*

I. PENDAHULUAN

Keamanan menjadi hal penting dalam jaringan komputer ataupun transmisi data. Pada suatu informasi akan memiliki nilai lebih tinggi apabila menyangkut aspek keputusan bisnis, keamanan maupun kepentingan privat atau publik. Dimana informasi tersebut akan lebih banyak diminati oleh berbagai pihak yang memiliki kepentingan di dalamnya. Ada banyak cara yang dapat digunakan untuk mengamankan data misalnya dengan

memberikan *password*, namun cara ini dapat dibobol oleh *cracker*, karena user dapat membuat kemungkinan-kemungkinan kata yang digunakan sebagai *password* oleh pihak yang menguncinya. Cara lain yang digunakan adalah menerapkan algoritma data *hiding*, seperti steganografi dengan kombinasi kriptografi dengan metode *Caesar Cipher* dan *Vigenere Cipher*.

Steganografi adalah suatu teknik penyembunyian pesan dengan suatu cara sehingga selain pengirim dan penerima, tidak ada seorangpun yang mengetahui bahwa ada suatu pesan rahasia [1]. Metode ini melakukan penyembunyian pesan atau informasi kedalam media lain seperti citra digital, teks video atau suara. Steganografi membutuhkan dua properti, yaitu informasi dan media penampung atau yang biasa disebut dengan *cover*. Penyisipan informasi digital dilakukan pada *bit-bit pixel* yang terdapat pada citra. Penggunaan citra sebagai media penyisipan pesan tidak akan menimbulkan kecurigaan pada pengelihatan manusia [2].

Teknik lain pada *data hiding* yaitu kriptografi. Kriptografi dapat berjalan menggunakan kunci simteris dan asimetris. Pada kunci simetris, lebih mudah operasinya, seperti halnya pada algoritma *Vigenere Cipher*. Kekuatan dari *vigenere cipher* adalah bahwa algoritma ini tidak rentan terhadap analisis frekuensi [3] dan merupakan bentuk yang paling sederhana dari sandi alfabetik. Menurut Soofi [4] dalam penelitiannya yang mengimplementasikan *Vigenere cipher* dengan media teks alphabet dari A sampai Z. Pendekatan yang diusulkan membuat *Vigenere cipher* lebih kuat melawan serangan kasiski dan *friedman* untuk menemukan panjang kunci. Seperti yang dapat kita lihat dalam contoh bahwa teknik yang diusulkan juga mengubah ruang antara kata-kata menjadi teks sandi yang akan membantu penerima untuk membaca pesan teks biasa dengan mudah setelah proses dekripsi. Sedangkan menurut Sari [5], dalam penelitiannya menggunakan *Caesar Cipher-One Time Pad* pada media gambar dan menyatakan bahwa algoritma gabungan dan algoritma *One Time Pad-Caesar Cipher* cepat dan sulit untuk dipecahkan. Penelitian lain telah dilakukan untuk mendapatkan hasil optimal dengan menggabungkan *Vigenre-Caesar* pada data teks seperti yang telah dilakukan oleh [6], dengan hasil *cipher* teks memiliki pola kunci enkripsi yang berbeda dan *crypto system Vigenere* akan lebih sulit untuk diuraikan menggunakan serangan frekuensi.

Artikel ini akan membahas mengenai keamanan data dengan menggunakan steganografi, LSB (*Least Significant Bit*) dan menggunakan kriptografi dengan menggunakan tiga kombinasi teknik pengamanan data. Steganografi merupakan suatu teknik untuk menyembunyikan informasi yang bersifat peribadi yang hasilnya akan tampak seperti informasi normal dan tidak akan terlihat mencuri perhatian. Dalam pembahasan ini akan menggunakan LSB (*Least Significant Bit*) yaitu salah satu metode steganografi yang paling sederhana, dan memiliki kapasitas penyimpanan cukup besar. Agar data yang tersimpan semakin aman dan tidak dapat teridentifikasi isi pesan tersebut, digunakan kriptografi dengan metode *caesar cipher*. Dari ketiga kombinasi tersebut dapat menjadi solusi dalam pengiriman pesan. Artikel ini bertujuan untuk mengimplementasikan teknik steganografi dengan metode LSB (*Least Significant Bit*) dan enkripsi kriptografi pada proses penyisipan pesan kedalam citra menggunakan *software* MATLAB R2015a.

II. TINJAUAN PUSTAKA

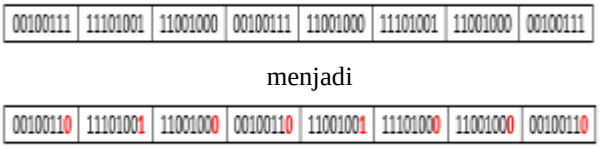
A. Steganografi LSB (*Least Significant Bit*)

Steganografi berasal dari bahasa Yunani yang terdiri dari dua kata, yaitu *steganos* dan *graphia*. *Steganos* berarti tersembunyi dan *graphia* artinya tulisan. Dengan demikian, steganografi adalah ilmu atau seni untuk menyembunyikan pesan [7]. Media penampung yang banyak digunakan untuk menyembunyikan yaitu citra digital. Penyisipan informasi pada media citra digital dilakukan pada bit-bit *pixel* yang terdapat pada citra. Penggunaan citra digital sebagai media penampung mempunyai kelebihan karena indra pengelihatan manusia memiliki keterbatasan terhadap warna, sehingga dengan keterbatasan tersebut manusia sulit membedakan citra digital yang asli dengan citra digital yang telah disisipi pesan rahasia.

Metode LSB digunakan dalam teknik *steganografi* dikarenakan tergolong mudah dalam penerapannya. Untuk menjelaskan metode ini, misalkan *cover-object* yang digunakan berupa citra digital (media gambar). Dasar dari metode ini adalah bilangan berbasis biner atau dengan kata lain angka 0 dan 1. Karena data digital merupakan susunan antara angka 0 dan angka 1 maka proses penerapannya lebih mudah. Metode ini berhubungan erat dengan ukuran 1 bit dan ukuran 1 *byte* 1 bit data dapat dikatakan terdiri dari 8 bit data [8]. Dimana bit pada posisi paling kanan yang disebut dengan bit pada posisi LSB.

Gambar-1. Gambar asli dan gambar hasil proses stegano

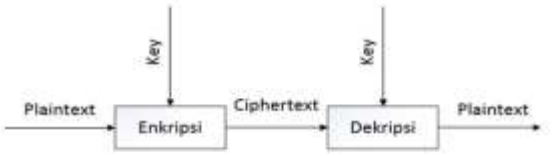
Metode *Least Significant Bit* bahkan mampu menyembunyikan gambar dalam 24-bit, 8-bit, ataupun yang berformat *grayscale*. Konsepnya sederhana membuat LSB menjadi mudah dalam implementasinya untuk digunakan, khususnya untuk kebutuhan dalam dunia steganografi [9]. Teknik steganografi dengan menggunakan metode LSB adalah teknik dimana kita mengganti bit pada posisi LSB pada data dengan bit yang dimiliki oleh data yang akan disembunyikan. Karena bit yang diganti hanyalah bit yang paling akhir, maka meskipun data telah berubah, kita tetap tidak akan bisa mengenalinya, karena *stego* yang dihasilkan hampir sama persis dengan media sebelum disisipi oleh data yang ingin disembunyikan, seperti ilustrasi pada Gambar-2 dengan pesan berupa data biner dengan nilai bit **01001000**.



Gambar-2. Proses penyisipan pesan pada LSB

B. Kriptografi *Caesar Cipher*

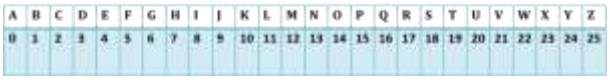
Kriptografi (*cryptography*) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu *kripto* dan *graphia*. *Kripto* artinya menyembunyikan, sedangkan *graphia* artinya tulisan. Kriptografi merupakan ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti maknanya [3]. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, integritas data, serta autentika data. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi. Kriptografi dapat pula diartikan sebagai ilmu atau seni yang menjaga keamanan pesan. Pada prinsipnya, kriptografi memiliki 4 komponen utama [4] yaitu: *plaintext* yaitu pesan yang dapat dibaca, *ciphertext* yaitu pesan acak yang tidak dapat dibaca, *key* yaitu kunci untuk melakukan kriptografi, *algorithm* yaitu metode untuk melakukan enkripsi dan dekripsi sesuai Gambar-3.



Gambar-3. Proses kriptografi

Caesar cipher merupakan sebuah metode sederhana, metode ini juga disebut sebagai subtitusi kode yang pertama dalam dunia penyandian, karena penyandian ini terjadi pada saat pemerintahan Yulius Caesar [10]. Dengan mengganti posisi huruf awal dengan alphabet atau disebut dengan algoritma ROT3 (penambahan 3).

Teknik penyandian ini termasuk sandi tersubtitusi pada setiap huruf pada *plaintext* digantikan oleh huruf lain yang memiliki sebuah posisi tertentu dalam alphabet [11], dengan penomoran alphabet sesuai Gambar-4. Secara detail Tabel-1 menjelaskan penggeseran yang terjadi pada huruf alphabet.



Gambar-4. Penomoran alphabet

Contoh:
Kunci=3
Kata yang akan dienkripsi=SAYA
En (X) = (X + K) mod (Jumlah Huruf)

(18 + 3) mod (26) => 21 mod 26 = 21 || 21 = V
(0 + 3) mod (26) => 3 mod 26 = 3 || 3 = D
(24 + 3) mod (26) => 27 mod 26 = 1 || 1 = B
(0 + 3) mod (26) => 3 mod 26 = 3 || 3 = D

HASIL : SAYA = > VDBD

C. Kriptografi *Vigenere Cipher*

Vigenere cipher adalah metode *encrypting* abjad teks dengan menggunakan serangkaian berbeda *Caesar cipher* berdasarkan surat kata kunci [6]. Ini adalah bentuk sederhana *polyalphabetic subtitusion. Vigenere cipher* merupakan sistem sandi poli-alfabetik mengenkripsi sekaligus sebuah teks yang terdiri dari beberapa huruf. *Vigenere cipher* menggunakan subtitusi dengan fungsi *shift* seperti pada *Caesar cpher* [3] yang dihitung menggunakan Tabel *Tabula Recta* sesuai Gambar-5.

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	D
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	C
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	B
Z	Z	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

Gambar-5. Tabel *Vigenere Cipher*

Rumus enkripsi *vigenere cipher* sesuai persamaan (1) dan persamaan (2):

$$Pi=(Ci-Ki) \bmod 26 \quad (1)$$

atau

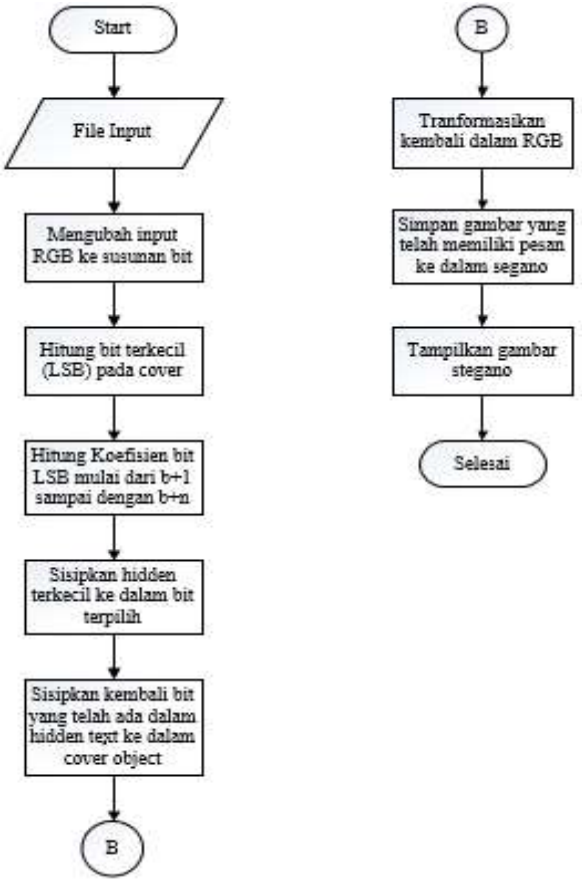
$$Ci=(Pi+Ki)-26 \quad (2)$$

kalau hasil penjumlahan Pi dan Ki lebih dari 26
dimana:
Ci=nilai desimal karakter *ciphertext* ke-i
Pi=nilai desimal kerakter *plaintext* ke-i
Ki=nilai desimal kunci ke-i

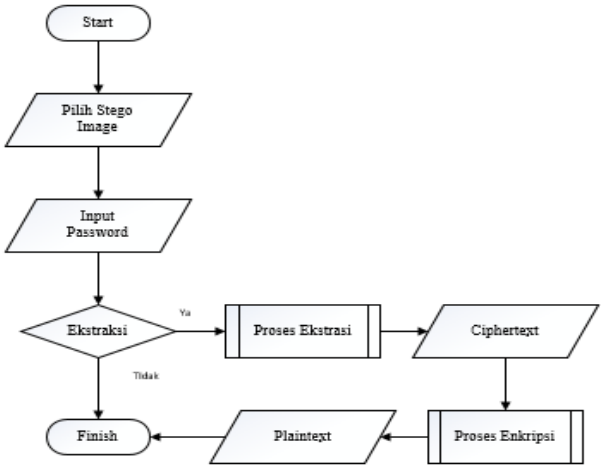
III. METODE

Dalam sebuah perancangan sistem tentunya sangat penting dalam pembuatan perangkat lunak. *Flowchart* dipakai untuk menggabungkan struktur menyeluruh dan aliran sistem ke pengguna akhir karena sistem ini dapat menawarkan tampilan fisik yang berperan penting pada keterkaitan *hardware* dan data media. Setelah tahap dan alur sudah didapatkan maka disini akan diperlihatkan tahapan dalam *flowchart*. Secara umum proses steganografi ada dua, yaitu penyisipan pesan (*embedding*) dan proses pembacaan pesan (ekstraksi). Gambar-6 adalah proses *embedding* pada metode LSB [1].

Diagram alir menjelaskan proses *embed* pada metode LSB. Pada langkah awal adalah memilih file yang akan diinput yang selanjutnya file yang diinput tersebut harus diubah dalam RGB dan dijadikan menjadi bit-bit. Kemudian menghitung bit terkecil pada cover, menghitung koefisien bit LSB mulai dari b+1 sampai dengan b+n. Langkah selanjutnya adalah sisipkan *hidden* terkecil dalam bit terpilih kemudian sisipkan kembali bit yang telah ada dalam *hidden text* dalam *cover object* sesuai ilustrasi pada Gambar-6.



Gambar-6. Proses Stegano LSB



Gambar-7. Proses Kriptografi Caesar-Vigenere

Diagram alir pada Gambar-7 menjelaskan proses enkripsi pada kriptografi. Langkah pertama yang dilakukan adalah pilih *image cover* yang akan dienkripsi, setelah diinput masukkan kunci untuk mengenkripsi. Kemudian akan diekstraksi dan menjadi *ciphertext*. Selanjutnya proses enkripsi dan

menjadi *plaintext*. Digunakan 2 buah alat pengujian yaitu PSNR dan *entropy*. *Peak Signal-to-Ratio (PSNR)* merupakan nilai perbandingan antara harga maksimum dari intensitas citra terhadap *error citra* yaitu MSE. Untuk menghilangkan nilai PSNR digunakan persamaan 3 dan 4 sebagai berikut:

$$PSNR = 10 \log 10 \frac{MAX^2}{MSE} \quad (3)$$

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} [f((i,j) - g(i,j))]^2 \quad (4)$$

Dimana:
MSE : nilai MSE
MAX : nilai maksimum dari *pixel* citra yang digunakan
m : panjang citra stego (dalam *pixel*)
f(i,j) : nilai piksel dari citra *cover*
n : lebar citra stego (dalam pixel)
g(i,j) : nilai piksel pada citra stego

Pada persamaan (5), *entropy* mengukur ketidakpastian suatu variabel acak, dimana P adalah jumlah partisi.

$$Entropy = -\sum_i \sum_j p(i,j) \log(p(i,j)) \quad (5)$$

IV. HASIL DAN PEMBAHASAN

Pada makalah ini digunakan 10 buah citra: 6 warna dan 4 *grayscale* berukuran 512x512 piksel untuk proses LSB-Vigenere. Hasil steganografi seperti pada Gambar-8 merupakan contoh 3 buah citra yang sudah di-stegano. Pada Gambar-8, tampak bahwa ukuran gambar tidak berubah sama sekali.

Cover Image	Stego Image
	
Image ID *Dimensions : 512x512* *Width : 512 pixels* *Height : 512 pixels* *Horizontal resolution :96 dpi* *Vertikal resolution: 96 dpi* *Bit depth : 24*	*Image ID* *Dimensions : 512x512* *Width : 512 pixels* *Height : 512 pixels* *Horizontal resolution : 96 dpi* *Vertikal resolution : 96 dpi* *Bit depth : 24*

	
Image ID *Dimensions : 256x256* *Width : 256 pixels* *Height : 256 pixels* *Horizontal resolution : 96 dpi* *Vertikal resolution : 96 dpi* *Bit depth : 24*	*Image ID* *Dimensions : 256x256* *Width : 256 pixels* *Height : 256 pixels* *Horizontal resolution : 96 dpi* *Vertikal resolution : 96 dpi* *Bit depth : 24*

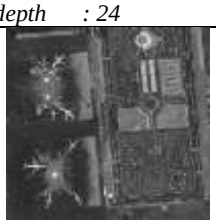
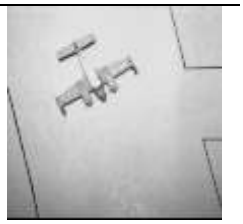
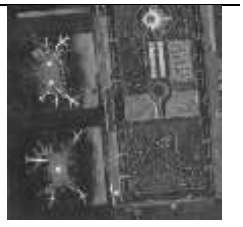
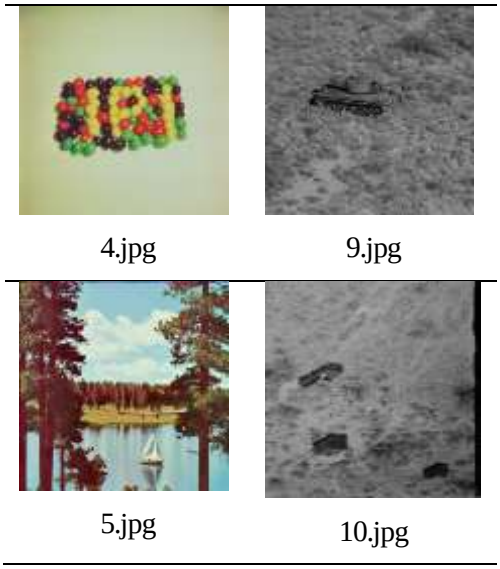



Image ID *Dimensions : 1024x1024* *Width : 1024 pixels* *Height : 1024 pixels* *Horizontal resolution : 96 dpi* *Vertikal resolution : 96 dpi* *Bit depth : 24*	*Image ID* *Dimensions : 1024x1024* *Width : 1024 pixels* *Height : 1024 pixels* *Horizontal resolution : 96 dpi* *Vertikal resolution : 96 dpi* *Bit depth : 24*

Gambar-8. Hasil pengujian *cover image* dan *tego image*

	
1.jpg	6.jpg
	
2.jpg	7.jpg
	
3.jpg	8.jpg



Gambar-9. Gambar yang akan diuji

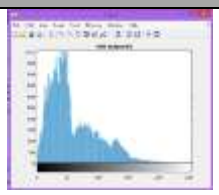
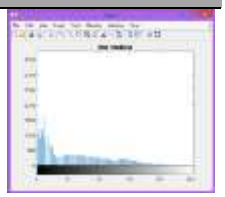
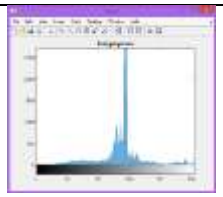
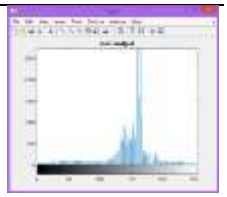
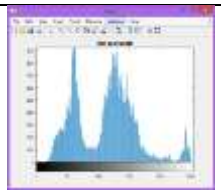
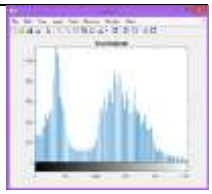
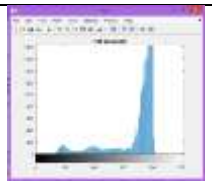
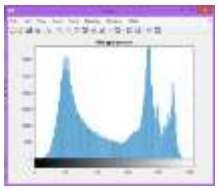
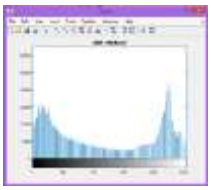
Melalui LSB-*Vigenere*, citra pada Gambar-9 telah dilakukan proses stegano-kripto dengan hasil pada Tabe-1. Dapat dilihat bahwa apda Tabel-1, dihasikan PSNR lebih dari 40 dB. Menurut Sari [12], nilai PSNR yang memenuhi *Human Visual System* dan secara kasat mata tidak terdapat perbedaan dengan gambar aslinya yaitu pada rentang nilai 35 dB atau lebih. Pengujian lain dilakukan menggunakan perhitungan entropi. Menurut [1], entropi adalah nilai keterlacakan distribusi derajat keabuan citra. sedangkan nilai entropi yang baik yaitu mendekati 7.

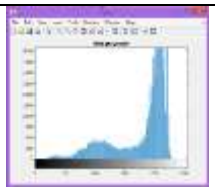
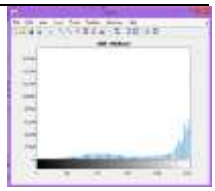
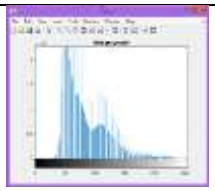
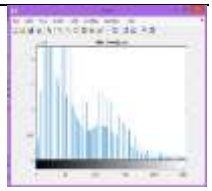
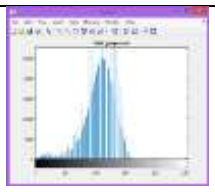
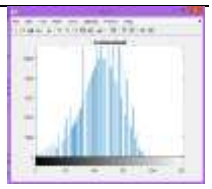
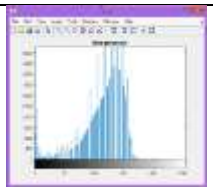
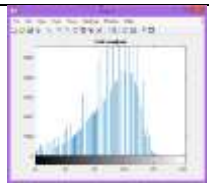
Tabel-1. Hasil Pengujian MSE dan PSNR

Nama File	PNSR (dB)		Entropy sebelum imadjust	
	Citra Stego-Kripto Asli	Citra Stego-Kripto setelah imadjust	Citra warna	Citra Grayscale
1.jpg	86,21	72,02	6,256	-
2.jpg	65,80	67,02	6,335	-
3.jpg	44,21	46,37	6,440	-
4.jpg	55,35	56,98	6,852	-
5.jpg	55,33	61,41	6,558	-
6.jpg	70,10	73,90	-	6,785
7.jpg	69,22	70,19	6,886	
8.jpg	67,11	67,27	-	6,746
9.jpg	69,99	70,12	-	6,885
10.jpg	52,71	69,88	-	6,865

Berdasarkan Tabel-1 di dapat hasil nilai entropi dari 10 gambar yang digunakan mendekati nilai 7. Tidak terdapat perbedaan antara gambar warna dan gambar *grayscale* bahwa kedua jenis gambar tersebut tetap mencapai nilai entropi yang baik. Dalam hal ini, nilai entropi juga tidak berpengaruhi perolehan nilai PSNR, dimana nilai entropi tinggi tidak selalu menghasilkan nilai entropi tinggi pula. Pada gambar 5.jpg nilai memiliki entropi 6,558 dan PSNR 61,41 dB, sedangkan gambar 4.jpg memiliki nilai entropi lebih tinggi dari entropi gambar 5.jpg, yaitu 6,852 memiliki PSNR yang lebih rendah dari gambar 5.jpg, yaitu 56,98 dB.

Tabel-2. Hasil perbandingan citra *grayscale* hasil proses kriptografi dan *imadjust* untuk memperbaiki aspek *impercept*

Nama file	*Grayscale*	*Imadjust*
1.jpg		
2.jpg		
3.jpg		
4.jpg		
5.jpg		
6.jpg		

7.jpg		
8.jpg		
9.jpg		
10.jpg		

Sesuai hasil pada Tabel-2, dapat dilihat bahwa histogram gambar asli dan histogram gambar hasil imadjust jauh berbeda, sehingga apabila gambar tersebut dilihat oleh mata awam maka tampak adanya perbedaan signifikan. Proses *imadjust* digunakan untuk memperbaiki nilai PSNR pada hasil akhir proses stego-kripto.

V. PENUTUP

A. Kesimpulan

Berdasarkan dari hasil dan pembahasan yang telah dilakukan maka dapat ditarik kesimpulan bahwa teknik steganografi dengan metode LSB dan enkripsi kriptografi dua lapis yaitu *caesar cipher* dan *vigenere cipher* yang tepat untuk diimplementasikan dalam pengamanan pesan yang disisipkan pada file image. Hasil dari proses *embed* dan ekstrak dari metode LSB dari hasil embed dan ekstrak tersebut diambil 2 bit yang terakhir yang berupa angka 0 atau angka 1. Hasil percobaan membuktikan bahwa lsb-Vigenere dapat melakukan proses *embeding* dan ekstraksi dengan baik dibuktikan oleh nilai PSNR dan entropi, serta histogram citra. Nilai entropi terbaik yaitu 6,886 pada citra berwarna, dan nilai PSNR terbaik yaitu 72,02 dB. dengan demikian penggunaan LSB dapat memenuhi *imperceptibility*.

B. Saran

Untuk hasil lebih maksimal, dapat digunakan kombinasi antara teknik LSB dengan algoritma kriptografi modern yang lebih rumit.

DAFTAR PUSTAKA

[1] Bhaudhayana, G. W., Widiartha, I. M. 2015. Implementasi algoritma kriptografi aes 256 dan metode steganografi lsb pada gambar bitmap. *Jurnal ilmu komputer Universitas Udayana*, *8*(2): 15-25.

[2] Handoyo, A. E., Rachmawanto, E. H., Sari, C. A., Susanto, A. 2018. Teknik Penyembunyian dan Enkripsi Pesan pada Citra Digital dengan Kombinasi Metode LSB dan RSA. *Jurnal Teknologi dan Sistem Komputer*, *6*(1): 37-43.

[3] Mandal, S. K., Deepti, A. R. 2016. A Cryptosystem based on Vigenere cipher by using mulitlevel encryption scheme. *International Journal of Computer Science and Information Technologies*, *7*(4): 2096-2099.

[4] Soofi, A. A., Riaz, I., Rasheed, U. 2016. An enhanced Vigenere cipher for data security. *International Journal of Scientific & Technology Research*, *5*(3): 141-145.

[5] Sari, C. A., Erawan, L., Rachmawanto, E. H., Permana, T. S. 2017. An Enhancement of One Time Pad Based on Monoalphabeth Caesar Cipher to Secure Grayscale Image. *Journal of Applied Intelligent System*, *2*(2): 88-100.

[6] Kester, Q. A. 2012. A cryptosystem based on Vigenère cipher with varying key. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, *1*(10): 108-113.

[7] Ilaga, K. R., Sari, C. A., Rachmawanto, E. H. 2018. A High Result for Image Security Using Crypto-Stegano Based on ECB Mode and LSB Encryption. *Journal of Applied Intelligent System*, *3*(1): 28-38.

[8] Karim, S. M., Rahman, M. S., Hossain, M. I. 2011. A new approach for LSB based image steganography using secret key. *14th International Conference on Computer and Information Technology (ICCIT 2011)*. 286-291.

[9] Al-Husainy, M. A. F. 2011. Word-Based LSB Image Steganography. *International Journal of Advanced Research in Computer Science*, *2*(6): 15-19.

[10] Rachmawati, D., Hardi, S. M., & Pasaribu, R. P. 2019. Combination of columnar transposition cipher caesar cipher and lempel ziv welch algorithm in image security and compression. *Journal of Physics: Conference Series* 1339(1): 1-6.

[11] Purnama, B., & Rohayani, H. 2015. A New Modified Caesar Cipher Cryptography Method With Legible Ciphertext From A Message To Be Encrypted. *Procedia Computer Science*, *59*: 195-204.

[12] Sari, C. A., Rachmawanto, E. H., & Kusuma, E. J. 2019. Good Performance Images Encryption Using Selective Bit T-des On Inverted Lsb Steganography. *Jurnal Ilmu Komputer dan Informasi*, *12*(1): 41-49.