STEGANOGRAFI LSB DENGAN MODIFIKASI KRIPTOGRAFI: CAESAR, VIGENERE, HILL CIPHER DAN PLAYFAIR PADA IMAGE

Arvin C Frobenius[1], Eko Rachmat Hidayat S. H. S[2]

Magister Teknik Informatika
Fakultas Teknik Informtika
Universitas Amikom Yogyakarta

arvinclaudyf@gmail.com[1], 007erachmat@gmail.com[2]

Abstrak

Pada era modern ini, teknologi informasi berkembang sangat pesat dan menjadi salah satu media popular didunia yang bertujuan dalam membentuk sistem dengan cara pengelolahan, pengumpulan, penyimpanan, sampai pengiriman. Dengan berkembangnya teknologi keamanan data harus diperhatikan, ini disebabkan oleh banyak pihak yang ingin mengakses informasi yang bukan haknya dan dapat juga menyalagunakan informasi tersebut, istilah ini sering disebut dengan cyber-crime. Terdapat teknik yang digunakan dalam pengaman data yaitu teknik kriptografi dan steganografi *Pada penelitian ini menggabungkan dua teknik, pertama teknik kriptografi menggunakan empat modifikasi yaitu Caesar cipher, vigenere, hill cipher, dan playfair. Kedua, menggunakan teknik steganografi LSB (least Significant Bit. Metode pengujian yang dilakukan pada penelitian ini menggunakan kapasitas penyisipan, histogram, pemotongan gambar, pengubahan ekstensi. Hasilnya menunjukan bahwa penyisipan data yang terdapat pada gambar mengalami penambahan ukuran file yaitu 192 KB dan 170 KB dengan karakter 17 dan 13 huruf dapat disimpulkan bahwa semakin banyak karakter huruf disisipkan pada gambar, semakin besar ukuran file gambar. Selain itu pada hasil histogram juga mengalami perbedaan yaitu pada nilai mean pada file gambar enkripsi mengalami peningkatan 220.87. Standard deviation mengalami penurunan pada file gambar enkripsi yaitu dengan nilai 72.35 dari 72.45.*

Kata Kunci: Kriptografi, Steganografi, Caesar Cipher, Vigenere, Hill Cipher, Playfair, SLB (Least Significant Bit).

1. Pendahuluan

Pada era modern ini, teknologi informasi berkembang sangat pesat dan menjadi salah satu media populer didunia yang bertujuan dalam membentuk sistem dengan cara pengelolahan, penyimpanan, pengiriman dan pengumpulan. Pada masa lalu pertukaran informasi masih menggunakan media kovensional yaitu surat-menyurat via pos. Saat ini dengan kemajuan teknologi pengiriman dapat lebih mudah dan cepat dengan menggunakan media digital yaitu internet. Metode digital saat ini untuk pertukaran data dapat menggunakan teks, audio, dan video dikirim dengan waktu sangat singkat. Disisi lain kemudahan yang diberikan juga memiliki dampak negatif yaitu kemungkinan terjadi penyalagunaan data dapat digunakan secara public. Pada ilmu keamanan data terdapat teknik kriptografi dan

steganografi untuk mengamankan data pribadi dengan cara mengenkrip data pribadi, sehingga tidak akan ada penyalagunaan data pribadi kita.

Pada penelitian Wimiliana, dkk (Syawal, 2016) menggunakan metode Hill Cipher dan Least Significant Bit (LSB) untuk mengenkripsi pesan yang dimasukan dalam gambar dan mengembalikan kembali pada pesan original. Penelitian ini menghasilkan website. Penelitian oleh muhamad (Wamiliana, 2017), menggunakan metode vigenere cipher dan metode LSB yang digunakan untuk menyisipkan pesan yang sudah terenkripsi dengan vigenere kemudian disisipkan kedalam gambar, tetapi kata yang disediakan untuk kata tidak terlalu banyak dan tidak dapat menggunakan spasi.

Pada penelitian yang dilakukan peneliti menggunakan metode teknik subtitusi yaitu mengombinasikan empat teknik yaitu caesar, vigenere, hill cipher, dan playfair. Selain itu, dikombinasikan dengan menggunakan teknik steganografi dengan metode LSB (*least significant bit*) untuk memberikan proteksi ganda pada pesan rahasia.

2. Metode Penelitian

2.1 Tahapan Penelitian

Dalam tahapan penelitian pengembangan kriptografi yang melibatkan empat algoritma (Caesar, vigenere, hill dan playfair) yang dikombinasi LSB. Pada proses enkripsi plaintext akan dieksekusi dengan pertama yaitu Caesar, vigenere, hill, dan playfair dengan kata kunci yang diinputkan. Kata kunci ini akan digunakan sebagai kunci di setiap enkripsi. Selanjutnya terdapat proses memasukan chipper teks kedalam citra menggunakan metode LSB. Dapat dilihatt pada Gambar 1.

2.2 Kriptografi

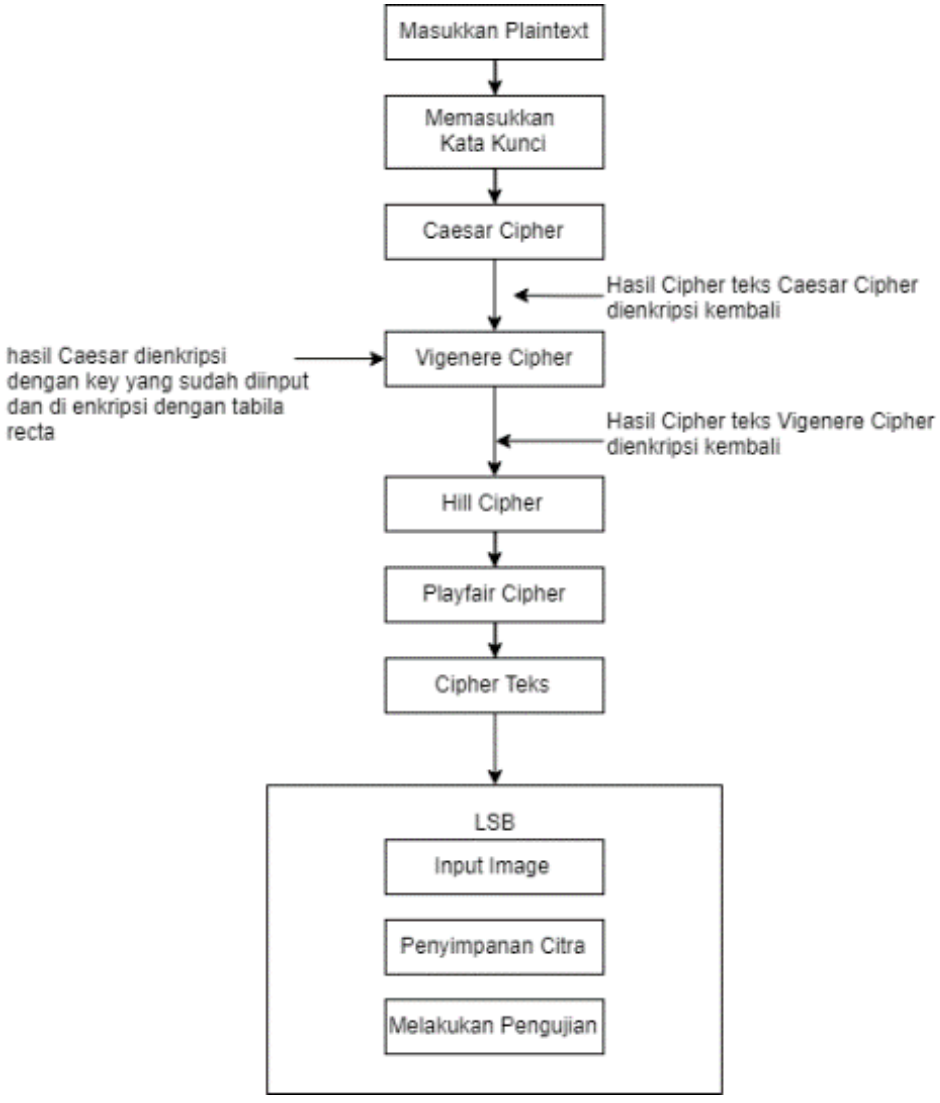
Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari satu tempat ke tempat lain. Dalam bahasa Yunani, kriptografi berasal dari kata *crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (menulis). Algoritma kriptografi terdiri dari tiga fungsi dasar yaitu (Ariyus, 2008):

- Enkripsi: merupakan pengaman data yang akan dikirim tetap terjaga kerahasiaannya. Istilah *plaintext* adalah pesan asli, sedangkan enkripsi dapat disebut dengan cipher atau kode.
- Deskripsi: merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk awalnya. Algoritma enksripsi berbeda dengan algoritma yang digunakan untuk deskripsi.

- Kunci: merupakan yang dipakai untuk melakukan enkripsi dan deskripsi. Kunci dibagi menjadi dua yaitu kunci rahasia dan kunci umum.

Kriptografi dibedakan menjadi dua yaitu kriptografi klasik dan kriptografi modern. Berikut penjelasannya (Ariyus, 2008):

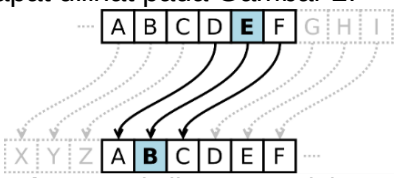
- Kriptografi klasik merupakan suatu algoritma yang menggunakan satu kunci untuk mengamankan data. Terdapat dua teknik dasar algoritma ini yaitu teknik subtitusi dan teknik transposisi.
- Kriptografi Modern merupakan suatu algoritma yang mempunyai kerumitan yang komplek karena dioperasikan menggunakan komputer.



Gambar 1. Tahapan Penelitian

2.3 Caesar Cipher

Caesar cipher merupakan enkripsi yang sering digunakan karena sederhana untuk digunakan. Teknik caesar ini termasuk algoritma kriptografi klasik dengan teknik subtitusi. Teknik ini dapat dilakukan dengan cara melakukan aturan pergeseran kunci kekanan atau kekiri sesuai yang ditentukan. Teknik pada enkripsi caesar cipher dapat dilihat pada Gambar 2.



Gambar 2. Teknik Caesar Cipher

Berikut contoh dalam melakukan enkripsi menggunakan Caesar cipher, sebagai contoh dengan jumlah pergeseran 2.

Plaintext: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Ciphertext: CDEFGHIJKLMNOPQRSTUVWXYZAB

Caesar cipher dapat dapat dinyatakan dalam matematis dalam proses enkripsi dan deskripsinya, berikut rumus matematis Caesar cipher. Rumus enkripsi Caesar Cipher dapat dilihat pada persamaan (1) dan rumus enkripsi Caesar Cipher dapat dilihat pada persamaan (2). Kelemahan Caesar cipher adalah *brute foce attact* ataupun dapat dipecahkan dengan menggunakan *exhaustive key search*.

$$E_n(x) = (x + n)\ mod\ 26 \quad (1)$$

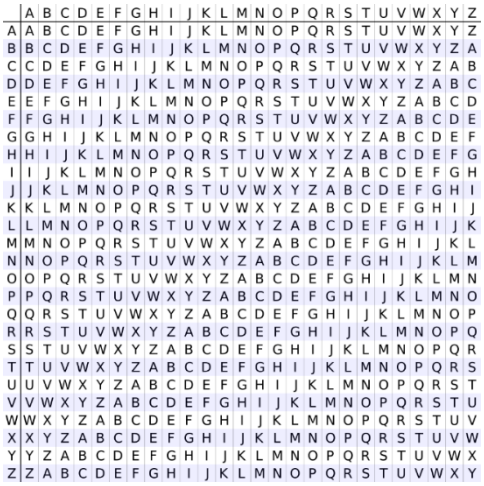
$$D_n(x) = (x - n)\ mod\ 26 \quad (2)$$

2.4 Vigenere

Vigenere merupakan bentuk sederhana dari sandi polialfabetik. Kelebihan dari sandi ini disbanding sandi Caesar adalah sandi ini tidak begitu rentan terhadap pemecahan sandi yang disebut analisis frekuensi (Cahyadi, 2012). Pada vigenere terbagi menjadi dua teknik subtitusi yaitu angka dan huruf.

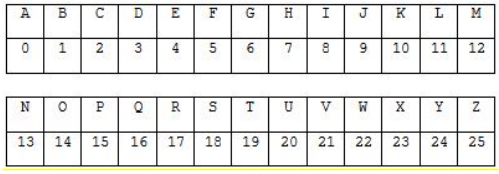
- Angka yaitu teknik subtitusi dilakukan dengan menggantikan huruf alphabet dengan angka, proses ini seperti pada metode Caesar.
- Huruf merupakan pengembangan dari Caesar cipher, tetapi jumlah pergeseran hurufnya berbeda-bedauntuk setiap periode. Untuk mengenkripsi pesan dengan kode vigenere menggunakan *tabila recta*. Tabila recta digunakan untuk memperoleh teks-kode dengan

menggunakan kunci tertentu. Berikut contoh gambar pada teknik huruf dan angka dilihat pada Gambar 3 dan Gambar 4.



	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	V
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	W
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	X
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 3. teknik Vigenere Pada Huruf.



A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Gambar 4. Teknik Vigenere Pada Angka

2.5 Hill Cipher

Hill cipher merupakan algoritma menggunakan matriks berukuran ordo m x m sebagai kunci dan deskripsi. Dasar teori menggunakan perkalian matrik dalam membuat enkripsi dan melakukan invers pada matrik untuk melakukan proses deskripsi. berikut matematis perkalian matrik untuk enkripsi dan invers untuk deskripsi. Rumus erkalian matrik 2x2 ditunjukan pada persamaan (3), rumus Perkalian matrik 2x2 ditunjukan pada persamaan (4), dan rumus Invers Matrik untuk Deskripsi ditunjukkan pada persamaan (5).

$$\begin{bmatrix} a & b \\ d & c \end{bmatrix} x \begin{bmatrix} p & q \\ s & r \end{bmatrix} = \begin{bmatrix} ap + br & aq + bs \\ cp + dr & cq + ds \end{bmatrix} \quad (3)$$

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} x \begin{bmatrix} p & q & r \\ s & t & u \\ v & w & x \end{bmatrix} =$$

$$\begin{bmatrix} ap + bs + cv & aq + bt + cw & ar + bu + cx \\ dp + es + fv & dq + et + fw & dr + eu + fx \\ gp + hs + iv & gq + ht + iw & gr + hu + ix \end{bmatrix} \quad (4)$$

$$\begin{bmatrix} a & b \\ d & c \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \quad (5)$$

Hill cipher merupakan polyalphabetic cipher dapat dikategorikan sebagai block cipher karena teks yang akan diproses akan dibagi menjadi block-block dengan ukuran tertentu. Setiap karakterdalam satu blok akan saling mempengaruhi karakter lainnya dalam proses enkripsi dan deskripsinya, sehingga karakter sama tidak dipetakan menjadi karakter yang sama pula (Sari dan Sihotang, 2017).

2.6 Kode Playfair

Kode playfair ditemukan oleh Sir Charles dan Baron lyon Playfair pada tahun 1854. Kunci dari cipher playfair menggunakan matriks 5 x 5 (dengan masukan terdiri dari 25 karakter dan membuang J yang ada di dalam alphabet) (Ariyus, 2008).

Playfair cipher merupakan suatu algoritma kriptografi klasik yang termasuk ke dalam polygram chipher, dimana plainteks diubah menjadi bentuk poligram dan proses enkripsi juga deksripsi dilakukan untuk poligram (Solihin, dkk., 2017).

2.7 LSB Based Image Steganography.

Semua file yang terdapat dalam komputer dapat digunakan sebagai media, seperti file gambar berformat jpeg, gif, bmp, atau music dalam format mp3, bahakan video dengan format wav atau avi. Semua media ini dapat dijadikan tempat untuk menyembunyikan sebuah pesan tanpa menghilangi fungsi dan kualitas tidak jauh beda dengan yang aslinya [6].

Sebuah teknik yang popular pada teknik steganografi, LSB (The least Significant Bits) perlindungan data media digital digunakan untuk menyembunyikan sebuah pesan. Paling sederhana teknik LSB adalah LSB replacement. Steganografi LSB replacement membalik bit terakhir pada setiap nilai data untuk mencerminkan pesan yang membutuhkan untuk disembunyikan (Cahyadi, 2012). Untuk menyembunyikan suatu gambar dalam LSB pada setiap byte dari gamabr 24-bit, dapat disimpan 3 byte dalam setiap pixel.

2.8 Testing Method

Pada tahap ini peneliti akan melakukan uji pada gambar untuk ketahanan, keamanan, dan kapasitas. Selain itu, menggunakan testing method untuk mengetahui perbandingan data original dengan data yang sudah mengalami enkripsi. Berikut metode yang akan digunakan oleh peneliti:

1. Histogram

   Grafik yang menunjukan frekuensi kemunculan setiap nilai gradasi warna. Histogram digunakan untuk menguji kehandalan sebuah gambar. Hasil dari test histogram dapat mengetahui seberapa besar perbandingan histogram pada file gambar asli dengan file gambar yang telah terenkripsi.
2. Kapasitas penyisipan

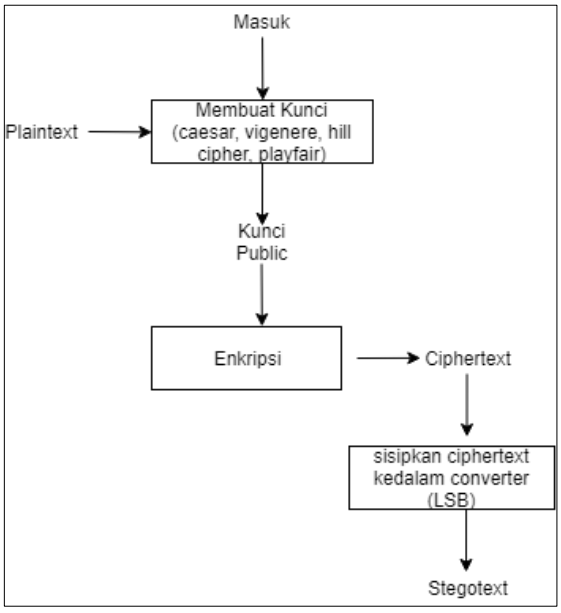
   Pada metode ini akan menguji seberapa besar perubahan besar ukuran file pada file gambar antara file gambar original dan file gambar terenkripsi.
3. Pengubahan ekstensi file

   Ekstensi file adalah jenis sebuah file yang meliputi nama dan dan nama ekstensi “Namafile.ekstensi”. pada metode ini bertujuan untuk mengetahui ketahanan dan keamanan pada file rahasia dengan merubah-merubah ekstensi file.
4. Pemotongan gambar

3. Hasil Analisis

3.1 Schema System Encryption

Pada penelitian ini para peneliti mengembangkan sistem menggunakan aplikasi berbasis mobile. Proses utama pada sistem ini adalah menggabungkan steganografi LSB pada citra digital gambar dengan empat metode kriptografi klasik yaitu Caesar, vigenere, hill cipher dan playfair. Skema proses enskripsi ditunjukkan pada Gambar 5.

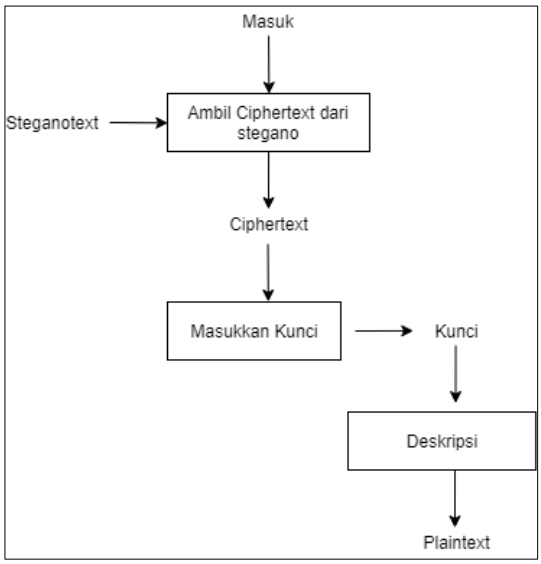


Gambar 5. Skema proses Enkripsi

Pada Gambar 5 merupakan proses enkripsi pesan, proses ini dilakukan oleh orang yang akan mengirim pesan rahasia. Pada proses enkripsi akan dibuat terlebih dahulu beberapa kunci untuk yang meliputi Caesar, Vigerene, Hill Cipher, dan playfair. Setelah membuat kunci akan melakukan proses menjadi enkripsi dan menghasilkan ciphertext. Ciphertext yang sudah didapatkan disisipkan dalam media berupa file gambar png dengan metode LSB. Hasil dari proses sisip pesan ini adalah file gambar yang sudah berisi pesan rahasia.

3.2 Schema *Decryption System*

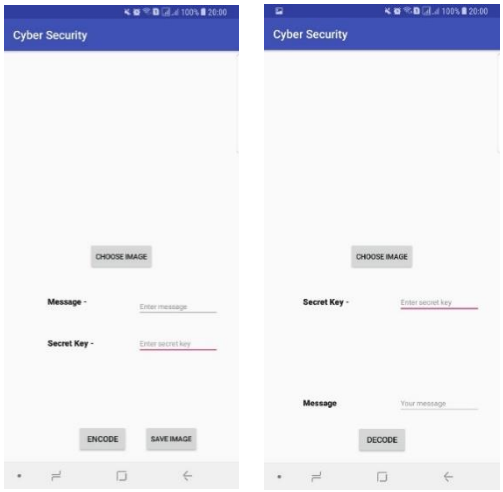
Pada schema system description adalah proses mengembalikan data pesan rahasia menjadi pesan asli. Proses ini dilakukan oleh orang yang menerima pesan rahasia. Langkah Proses description merupakan kebalikan proses encryption yaitu pertama Pesan yang masih berupa ciphertext diambil dari file gambar dengan menggunakan metode LSB, kedua ciphertext harus dideskripsi untuk mendapatkan pesan rahasia. Pada proses ini untuk mendeskripsi harus melakukan proses kebalikan dari proses enksripsi dengan menggunakan kunci. Dengan demikian pesan rahasia yang sebenarnya dapat dibaca. *Schema decryption system* ditunjukkan pada Gambar 6.



Gambar 6. *Schema decryption system*

3.3 *User* Interface *Application*

Pada implementasi penelitian ini peneliti menggunakan aplikasi berbasis mobile. Berikut *user interface* aplikasi dapat dilihat pada Gambar 7.



Gambar 7. User Interface Application

Terdapat dua interface, pertama *interface* untuk membuat pesan rahasia (*ciphertext*), dan interface lainnya digunakan untuk mengembalikan pesan rahasia menjadi pesan deskripsi (plaintext).

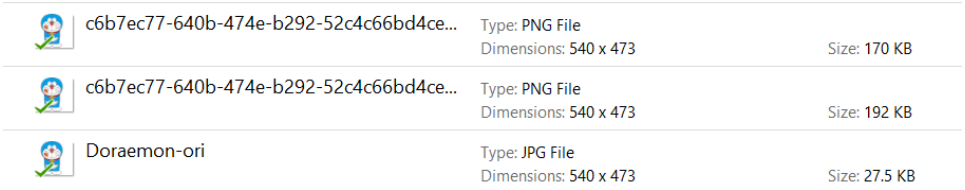
Pada tahap proses pengujian kapasitas penyisipan, dilakukan sebanyak tiga kali untuk mengetahui seberapa besar ukuran kapasitas file gambar. File gambar menggunakan gambar PNG dengan kapasitas file original adalah 27.5 KB dengan ukuran dimensi (pixel) 540 x 473. *File image original* ditunjukkan pada Gambar 8.

Gambar 8. File Image Original

Setelah dilakukan proses enkripsi dengan teknik kombinasi kriptografi: Caesar, vigenere, hill dan playfair dan disisipkan pada file gambar menggunakan metode LSB dengan file gambar PNG dihasilkan dengan tiga kali uji coba dengan jumlah karakter berbeda. Hasil ditunjukan pada Tabel 1 dan Gambar 9.

Tabel 1. Hasil pengujian kapasitas penyisipan

Nama	Kata	Karakter	Ukuran (KB)	Dimensi
Ori	0	null	27.5	540x473
Enkrip1	17	ujianakhirsemester	192	540x473
Enkrip2	13	Ujiansemester	170	540x473

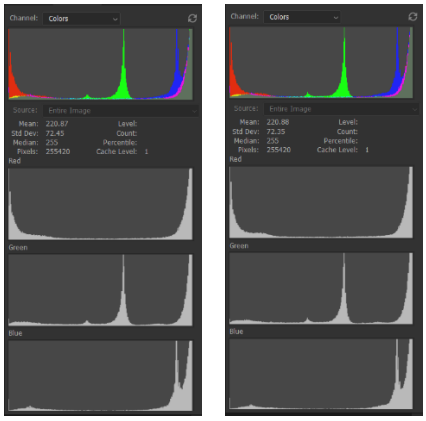


Gambar 9. Hasil pengujian kapasitas penyisipan

Dari hasil ini menunjukan bahwa kapasitas ukuran file mengalami perubahan dari tiga kali uji coba. Pada data pengujian dapat diperhatikan jika semakin besar karakter kata yang dimasukan semakin besar ukuran yang akan disimpan tetapi dengan ukuran dimensi sama seperti original. Seperti data "Enkrip1" dan "Enkrip2" dengan jumlah kata 17 huruf dan 13 huruf menghasilkan ukuran 192 KB dan 170 KB denngan dimensi tetap sama yaitu 540x473.

3.4 *Histogram*

Dalam pengujian Histogram penelitian ini menggunakan tools dari aplikasi photoshop CC 2018 versi 19.1.6. pengujian dilakukan untuk mengetahui perubahan dan perbedaan frequensi warna pada gambar sebelum disisipi pesan rahasia kecil ataupun besar. Perbandingan histogram dilakukan pada file gambar original dan file gambar yang telah di enkripsi. Hasil dari pengujian histogram pada file gambar PNG ditunjukkan pada Gambar 10.



Original Enkripsi1

Gambar 10 Hasil Pengujian Histogram

Pada tahap hasil pengujian histogram dihasilkan bahwa terdapat perbedaan pada hasil instogram file gambar original dengan file gambar yang terenkripsi. Hasil perbedaan histogram terletak pada bagian standard deviation dan mean. Hasil pengujian menggunakan histogram ditunjukkan pada Tabel 2.

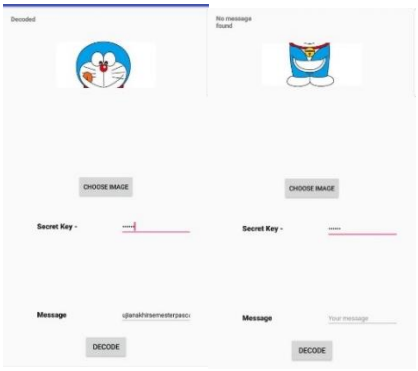
Tabel 2. Hasil Histogram

	Original	Enkripsi1
Mean	220.87	220.88
Std Dev	72.45	72.35
Median	255	255
Pixels	255420	255420
Dimensi	540x473	540x473

Data menunjukan nilai pada mean antara file gambar original dengan enkripsi1 mengalami perbedaan dengan nilai masih-masing adalah 220.87 dan 220.88, ini mununjukan mengalami peningkatan pada nilai mean. Pada nilai standard deviation file gamabr original memiliki nilai 72.45 dan pada file gambar enkripsi1 memiliki nilai 72.35, ini menunjukan mengalami penurunan pada bagian standard deviation.

3.5 *Pemotongan* File Gambar

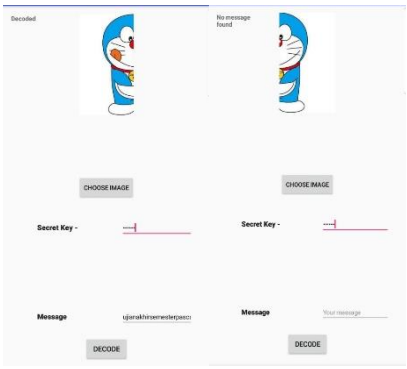
Dalam pengujian pemotongan file gamabr pada penelitian ini digunakan untuk mengetahui isi pesan rahasia yang disisipkan pada gambar mengalami kerusakan atau tidak. Dari hasil pemotongan selanjutnya ingin diketahui letak penyisipan pesan rahasia pada pixel gambar. Pada pengujian pemotongan file gambar dibagi menjadi empat bagian yaitu atas, bawah, kanan dan kiri. Dalam pengujian gambar ini file gambar berformat PNG. Hasil dari uji pemotongan ditunjukkan pada Gambar 10.



Gambar 11. Pemotongan Gambar Atas dan Bawah

Pada hasil pengujian pemotongan file gambar bagian atas didapatkan hasil bahwa pesan rahasia yang disisipkan pada gambar tidak memiliki kerusakan dan pesan rahasia masih dapat untuk diakses.

Selanjutnya, pada pengujian pemotongan file gambar bagian bawah yang sudah mengalami enkripsi. Pada hasil pemotongan gambar file bawah menghasilkan bahwa file mengalami kerusakan yaitu tidak adanya file rahasia yang ditemukan. Pada tahap ketiga dan keempat melakukan pemotongan file gambar bagian kanan dan kiri. Hasil dapat dilihat pada Gambar 12.



Gambar 12. Pemotongan File Gambar Bagian Kanan dan Kiri

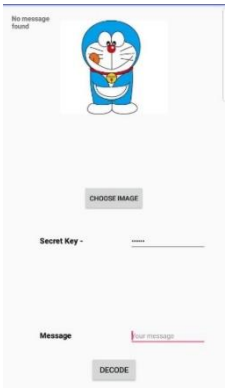
Pada hasil pemotongan file gambar kanan dan kiri dihasilkan bahwa pada pemotongan file gambar kiri bagian kiri menunjukan bahwa pesan rahasia tidak mengalami kerusakan dan pada file gambar bagian kanan mengalami kerusakan dan file rahasia tidak ditemukan.

Dari hasil uji coba pemotongan file gambar pada beberapa bagian dapat ditemukan letak Sehingga dapat disimpulkan bahwa pesan rahasia dapat ditemukan di posisi mana pesan rahasia disisipkan pada file gambar. Berikut Gambar 13 dimana posisi pesan rahasia disisipkan pada pixel gambar.

Gambar 13. Posisi Pesan Rahasia pada Pixel Gambar.

3.6 *Perubahan* Ekstensi File

Pada pengujian yang dilakukan pada tahap ini adalah perubahan file gambar dari PNG menjadi JPEG. Pada pengujian ini ingin mengetahui apakah terdapat kerusakan pada pesan rahasia pada gambar. Berikut hasil dari percobaan perubahan ekstensi file pada Gambar 14.



Gambar 14. Perubahan Ekstensi JPEG

Hasil menunjukan bahwa perubahan file ekstensi dari PNG ke JPEG mengalami kerusakan yaitu pesan rahasia tidak ditemukan dan diketahui ukuran kapasitas file dari file gambar yang sudah di enkripsi dan di ubah pada bentuk JPEG mengalami penyusutan dimana hasilnya ditunjukkan pada Tabel 3.

Tabel 3. Penyusutan File Enkripsi PNG ke JPEG

PNG Original	PNG Enkripsi	JPEG
27.5 KB	192 KB	42.3 KB

4. Kesimpulan

Kesimpulan pada penelitian berhasil mengkombinasikan empat metode teknik kriptografi yaitu Caesar, vigenere, hill, playfair dan least significant bit (LSB) berbasis aplikasi *mobile* Android. Aplikasi ini dapat digunakan untuk menyembunyikan pesan yang telah di enkripsi dan disimpan kedalam gambar berformat PNG. Berdasarkan uji coba yang dilakukan menghasilkan bahwa penyisipan data yang terdapat pada gambar mengalami penambahan ukuran file yaitu 192 KB dan 170 KB dengan karakter 17 dan 13 huruf dapat disimpulkan bahwa semakin banyak karakter huruf disisipkan pada gambar, semakin besar ukuran file gambar. Selain itu pada hasil histogram juga mengalami perbedaan yaitu pada nilai mean pada file gambar enkripsi mengalami peningkatan 220.87. Standard deviation mengalami penurunan pada file gambar enkripsi yaitu dengan nilai 72.35 dari 72.45.

Daftar Pustaka

Syawal Muhamad F. (2016). Implementasi Teknik Steganografi Menggunakan Algoritma Vigenere Cipher dan Metode LSB. Vol 4. Jurnal TICOM

Wamiliana, Adrian R, Jayanti E. F. (2017). Implementasi Kriptografi Dan Steganografi Pada Media Gambar Menggunakan Hill Cipher Dan Least Significant Bit (LSB). Vol 5. Jurnal Komputasi.

Ariyus, D. (2008). *Pengantar ilmu kriptografi: teori analisis & implementasi*. Penerbit Andi.

Cahyadi, T. (2012). Implementasi Steganografi LSB Dengan Enkripsi Vigenere Cipher Pada Citra JPEG. *Transient*, *1*(4), 281-288.

Rusman, E. S. (2016). "Steganalisis Dalam Pengujuan Citra DIgital Dengan Pengguna Crystalize Dan Histogram Pada Image BMP," Issuu, Tasikmalaya.

Sari, J. I., dan Sihotang, H. T. (2017). Implementasi Penyembunyian Pesan Pada Citra Digital Dengan Menggabungkan Algoritma HILL Cipher Dan Metode Least Significant BIT (LSB). *Jurnal Mantik Penusa*, *1*(2).

Solihin, I., Mesran, M., dan Siahaan, A. P. U. (2017). IMPLEMENTASI ALGORITMA SUPER PLAYFAIR CHIPHER DAN TWO SQUARE CIPHER DALAM PENGAMANAN PESAN TEKS. *KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer)*, *1*(1).