COMBINATION OF CRYPTOGRAPHIC ALGORITHM AND STEGANOGRAPHY TO HIDDEN MESSAGE IN IMAGE

Yuliana[1], I Wayan Pandu Swardiana[2], Dony Ariyus[3]
1,2,3)Magister Telnik Informatika Universitas Amikom Yogyakarta
Jl. Ring Road Utara, Condong Catur, Sleman, Yogyakarta
Telp: (0274) 884201 - 207
Fax: (0274) 884208 Kodepos: 55283
yuliana.1020@students.amikom.ac.id, wayan.swardiana@students.amikom.ac.id,
dony.a@amikom.ac.id

Abstract

Along with the increasing use of the internet in Indonesia, the threat to messages in image media has increased. The confidential data that will be sent requires security so that it can be read by the recipient of the message. For this reason, it is necessary to design a security system for this picture's media message by encrypting and decrypting it then hiding the message. The algorithm used by combining various cryptographic algorithms and steganography techniques using the Least Significant Bit (LSB) method. The test results show the security of the message on the image media, especially in protecting the copyright rights of the image. The original image measuring 242 kb in the .jpg format will increase in value after adding secret data with a size of 536 kb using the .png format. This system successfully displays secret messages in the image and does not change the cover of the image.

Keyword: Kriptografi, Steganografi, Image

Abstrak

Seiring dengan meningkatnya penggunaan internet di Indonesia, ancaman terhadap pesan dalam media gambar menjadi ikut meningkat. Data rahasia yang akan dikirim memerlukan keamanan agar dapat dibaca oleh penerima pesan. Untuk itu Perlu dirancang sebuah sistem *security* terhadap pesan media gambar ini dengan mengenkripsi dan dekripsi terlebih dahulu kemudiaan dilakukan menyembunyikan pesan. Algoritma yang digunakan dengan mengkombinasi dari berbagai algoritma *kriptografi* dan teknik *steganografi* menggunakan metode *Least Significant Bit (LSB)*. Hasil pengujian menunjukkan keamanan pesan pada media gambar terutama dalam melindungi hak akses (*copyright*) gambar. Gambar original semula berukuran 242 kb dengan format .jpg akan mengalami kenaikan nilai setelah ditambahkan data rahasia dengan ukuran gambar 536 kb menggunakan format .png. Sistem ini berhasil menampilkan pesan rahasia yang ada didalam gambar dan tidak mengubah cover citra gambar.

Kata Kunci: *Kriptografi*, *Steganografi*, Gambar

1. Pengantar

Teknologi informasi tentunya sangat berkaitan dengan data informasi. Lalu lintas data ini sangatlah padat terutama di kota-kota besar di Indonesia. Namun demikian perlu menjadi perhatian untuk aspek keamanan data pada saat pengiriman terutama data rahasia. Dengan berbagai teknik banyak yang mencoba untuk mengakses informasi yang bukan haknya. Informasi yang aman tentunya memiliki pengamanan data yang sulit di dekripsi. Data informasi ini sebelumnya akan di enkripsi dulu menggunakan algoritma yang sudah ada seperti algoritma *caesar cipher, vigenere cipher, zig zag cipher,* dan lain lain. Algoritma ini tentunya memiliki kelebihan dan kekurangan masing-masing, oleh karena itu perlunya dilakukan kombinasi terhadap beberapa algoritma tersebut agar dihasilkan cipher teks yang

sulit di dekripsi kemudian dilakukan penyembunyian pesan kedalam gambar. Teknik ini ada sejak sebelum masehi dan kini seiring dengan kemajuan teknologi jaringan serta perkembangan dari teknologi digital, steganografi banyak dimanfaatkan untuk mengirim pesan melalui jaringan internet tanpa diketahui orang lain dengan menggunakan media digital berupa file citra [1].

Pada penelitian ini dilakukan penggabungan tiga algoritma yaitu algoritma *caesar cipher, algoritma vigenere cipher, dan algoritma zig zag cipher*. Hal ini dilakukan untuk menutupi kekurangan dari caesar cipher dan vigenere cipher dimana terdapat perulangan huruf pada *cipher* teks, dengan menambahkan algoritma *zig zag cipher* diharapkan dapat memperkuat keamanan pada pesan teks. Dengan hasil penggabungan ketiga metode ini diharapkan dapat memperkuat pesan digital agar tidak mudah di dekripsi. Selain melakukan penggabungan *kriptografi*, terdapat cara lain untuk menggamanakn pesan yaitu dengan teknik *steganografi*. Teknik ini untuk menyembunyikan pesan kedalam media gambar sehingga orang lain tidak menyadari ada pesan yang tersembunyi dala media gambar [2].

Terdapat beberapa penelitian yang sudah dilakukan dan menjadi referensi penulis yaitu penelitian dengan judul Penerapan Kombinasi Sandi *Caesar* dan *Vigenere* untuk Pengaman Data Pesan, penelitian ini menerapkan algoritma *caesar cipher* dan *vigenere cipher* dalam mengenkripsi pesan digital sehingga pesan yang terkirim maupun diterima pengguna dapat aman tanpa disadap ataupun dimodifikasi [3]. Penelitian yang kedua dengan judul Penerapan *Kriptografi* Pada Teks Pesan dengan Menggunakan Metode *Vigenere Cipher* Berbasis *Android*, penelitian ini menerapkan algoritma *vigenere cipher* pada pengiriman pesan digital berupa sms, whatsapp, line, dan aplikasi sejenisnya melalui *platform* android [4]. Penelitian yang ketiga dengan judul Kombinasi Algoritma *Kriptografi Vigenere Cipher* dan *Hill Cipher* Untuk Penyandian Pesan Rahasia Pada Metode *Steganografi*, penelitian ini menerapkan algoritma *vigenere cipher* dan *hill cipher* dalam mengenkripsi dan dekripsi pesan digital kemudian di stegano menggunakan metode *Least Significant Bit* (LSB). Hasil penelitian ini berupa aplikasi yang diberi nama *steganocipher* berjalan pada aplikasi mobile dan dapat menyimpan teks pada gambar berformat JPG dan PNG [5].

Pada penelitian ini yang membedakan adalah algoritma yang digunakan yaitu tiga algoritma *(caesar cipher, vigenere cipher,* dan *zig zag cipher),* hasil dari enkripsi ke tiga algoritma tersebut akan dikombinasikan ke dalam algoritma *steganografi* dengan metode *Least Significant Bit* (LSB) untuk diterapkan pada citra gambar.

2. Tinjauan Pustaka

2.1 *Kriptografi*

Kata *kriptografi* berasal dari bahasa Yunani yang terdiri dari dua buah kata yaitu *cryptos* dan *graphia*. Kata *crypto* berarti rahasia sedangkan *graphia* berarti tulisan yang secara umum memiliki makna tulisan rahasia. Menurut Dony Ariyus pada bukunya yang berjudul Pengantar Ilmu *Kriptografi*: teori, analisis, dan implementasi tahun 2008 menjelaskan bahwa *kriptografi* adalah ilmu yang mempelajari tentang bagaimana menjaga kerahasiaan suatu pesan, agar isi pesan yang ditampilkan tersebut aman sampai ke penerima pesan [6].

Kriptografi adalah ilmu yang mempelajari bagaimana melakukan enkripsi dan dekripsi, dengan memanfaatkan model matematika tertentu. *Kriptografi* diilhami dengan teknik enkripsi atau teknik penyandian yang mengubah sebuah pesan yang dapat dibaca (*plaintext*) menjadi sebuah pesan yang acak dan sulit diartikan. Untuk dapat membaca pesan yang terenkripsi diperlukan proses terbalik dari enkripsi yang disebut dekripsi [7].

2.1.1 *Caesar Cipher*

Sandi Caesar diambil dari nama kaisar romawi Julius Caesar, dalam mengirimkan pesan Julius Caesar mengamankannya dengan cara isi pesan yang ada disandikan dengan mengganti posisi setiap huruf yang ada pada pesan dengan huruf lain yang memiliki posisi selisih huruf yang lain dari urutan *alfabet*. Adapun langkah-langkah yang dilakukan adalah sebagai berikut [8][9] :

a. Menentukan besarnya jumlah pergeseran huruf yang akan diganti.
b. Mengganti setiap huruf yang ada pada pesan sesuai dengan jumlah pergeseran huruf yang ditentukan.
c. Merangkai kembali jumlah huruf sesuai dengan susunan pesan awal.

2.1.2 *Vigenere Cipher*

Vigenere Cipher dikemukakan pertama kali oleh kriptologis dari Perancis bernama *Blaise de Vigènere* pada tahun 1586. Pada *kriptografi caesar* pergeseran akan sama pada seluruh pesan, jika kunci yang digunakan adalah huruf F, maka setiap huruf pada pesan akan bergeser 5 huruf. Begitu juga bila digunakan kunci-kunci lainnya. Pada *kriptografi caesar* tetapi setiap huruf di dalam *plaintext* akan mengalami pergeseran yang berbeda [10].

2.1.3 *Zig Zag Cipher*

Zig zag cipher adalah algoritma penyandian menggunakan model transposisi. Metode Transposisi adalah metode yang enkripsi dengan menyusun *plaintext* pada matriks secara baris, lalu dari hasil susunan tersebut menghasilkan sebuah *ciphertext* dengan mengambil rangkaian karakter secara kolom. Metode Transposisi juga disebut metode permutasi [11].

2.1.4 *Steganografi* Metode LSB

Steganografi adalah teknik menyembunyikan tulisan pada suatu media tertentu seperti gambar, suara, dan lain lain. Penggunaan *steganografi* bisanya untuk *watermarking* pada penanda hak cipta, tanda pengenalan pemilikan, *autentikasi* keaslian, *fingerprinting*, *copy control*, dan *covert communication* [12].

Least Significant Bit (LSB) merupakan salah satu teknik dalam *Steganografi*. LSB menambahkan bit data yang akan disembunyikan (pesan) di bit terakhir yang paling cocok atau kurang berarti. Misalkan bit pada image dengan ukuran 3 *pixel* sebagai berikut :

(0011111 11101001 11001000)
(0011111 11001000 11101001)
(1100000 00100111 11101001)

Pesan yang akan disisipkan adalah karakter ‘A’ yang memiliki biner 10000001, stego image yang akan dihasilkan adalah :

(0011111**1** 1110100**0** 1100100**0**)
(0011111**0** 1100100**0** 1110100**0**)
(1100000**0** 0010011**1** 11101001)

Ada dua teknik yang dapat digunakan pada LSB, yaitu penyisipan secara sekuensial dan secara acak. Penyisipan sekuensial dilakukan berurutan sedangkan acak dilakukan dengan acak pada *image* dengan memasukan kata kunci [13].

3. Metodelogi Penelitian

3.1 Prinsip Kerja Sistem

Kombinasi beberapa Algoritma *Kriptografi* yaitu *Caesar chiper, Vigenere chiper* dan *Zig zag Chiper* dilakukan penggabungan dalam mengenkripsi dan mendekripsi data berupa

teks pesan. Kemudian hasil dari ke tiga algoritma tersebut disisipkan kedalam gambar. Untuk mempermudah dalam proses menyisipan pesan kedalam gambar, maka dibuat suatu sistem *steganografi* dengan metode *Least Significant Bit* (LSB) dengan 3 proses yaitu:(1) mengambil gambar, (2) menambah gambar, (3) menampilkan pesan dan jumlah biner. Fungsi dari kombinasi Algoritma *Kriptografi* dan *Steganografi* dalam proses penyandian data tidak hanya dilakukan jika memungkinkan. Adapun kelebihan yang didapatkan dengan menerapkan kombinasi dari beberapa penggabungan algoritma ini, proses enkripsi teks menjadi berlipat ganda sehingga dihasilkan *chiper* yang acak dan tersembunyi.

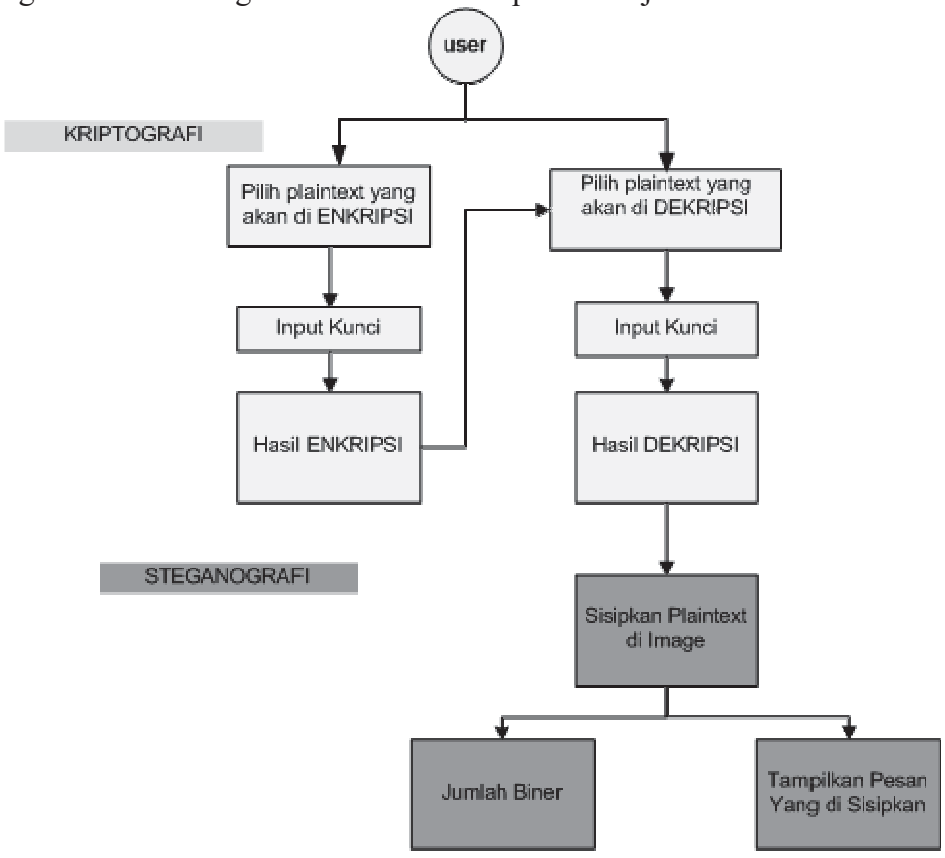
3.2. Tahap Penelitian

Pada perancangan sistem yang akan diterapkan pada penelitian ini akan dijelaskan melalui alur kerja sistem. Dari alur tersebut permodelan interaksi dari keseluruhan alur kerja sistem dapat digambarkan dengan baik.

Proses pertama adalah proses enkripsi yang dimulai dengan memilih *plaintext* yang akan di enkripsi, setelah itu dilanjutkan dengan memasukkan kunci enkripsi untuk kemudian dilakukan proses enkripsi yang akan menghasilkan *plaintext* hasil.

Proses kedua adalah dekripsi, pada proses ini *file* yang sebelumnya sudah melalui proses enkripsi dimasukkan lagi sebagai *plaintext input*-an yang kemudian ditambahkan dengan kunci yang sama, hal ini diperlukan karena peran kunci adalah validasi untuk dapat melanjutkan proses dekripsi. *Output* dari proses ini adalah *file* dokumen yang telah terdekripsi.

Proses ketiga adalah proses steganografi dengan input gambar dan menyisip file teks pada gambar, maka outputnya adalah jumlah biner dan menampil pesan yang disisipkan didalam gambar. Berikut gambar 1 adalah alur proses kerja dari keseluruhan sistem.



Gambar 1. Alur Kerja Sistem

4. Hasil dan Pembahasan

4.1 Penerapan Kombinasi Metode

4.1.1 Proses Penerapan Metode *Caesar Cipher*

Caesar cipher digunakan sebagai pembentuk kunci awal untuk digunakan pada proses enkripsi pesan. Berikut pesan yang akan digunakan **"KESULITANYANGMEMBENTUK SAYA"** dan kunci **" RUMIT".**

KEYWORD RULE

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

PLAINTEXT LETTER

K	**E**	**S**	**U**	**L**	**I**	**T**	**A**	**N**	**Y**	**A**	**N**	**G**	**M**	**E**	**M**	**B**	**E**	**N**	**T**	**U**	**K**	**S**	**A**	**Y**	**A**
F	T	P	S	G	D	Q	R	J	Y	R	J	B	H	T	H	U	T	J	Q	S	F	P	R	Y	R

Menghasilkan enkripsi

F	**T**	**P**	**S**	**G**	**D**	**Q**	**R**	**J**	**Y**	**R**	**J**	**B**	**H**	**T**	**H**	**U**	**T**	**J**	**Q**	**S**	**F**	**P**	**R**	**Y**	**R**

3.1.2 Proses Penerapan Metode *Vigenere Cipher*

Vigenere cipher merupakan *polyalphabetic substitution cipher* dan dikembangkan dari modifikasi *caesar cipher*. *Vigenere cipher* dianggap sebagai sistem enkripsi yang paling aman. Pada *vigenere cipher*, kunci yang digunakan berupa karakter yang dimasukkan oleh pengguna. Tabel *Vigenere Chiper* yang sudah di modifikasi dan digunakan sebagai berikut:

Tabel 1. Tabel *Vigenere Chiper*

	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

Kata kunci = RUMIT

F	T	P	S	G	D	Q	R	J	Y	R	J	B	H	T	H	U	T	J	Q	S	F	P	R	Y	R
R	U	M	I	T	R	U	M	I	T	R	U	M	I	T	R	U	M	I	T	R	U	M	I	T	R

Dengan menghasilkan enkripsi baru tujuannya adalah untuk menyandikan data text.

W	N	B	A	Z	U	K	D	R	R	I	D	N	P	M	Y	O	F	R	J	J	Z	B	Z	R	I

3.1.3 Proses Penerapan Metode *Zig Zag Cipher*

Dengan menggunakan enkripsi: 3 dan *Offset*:0 (artinya dalam 3 baris dimulai dari baris ke-0 atau awal atau paling atas).

Proses Enkripsi

W				Z				R				N				O				J				R	
	N		A		U		D		R		D		P		Y		F		J		Z		Z		I
		B				K				I				M				R				B			

Hasil enkripsi

W	Z	R	N	D	J	R	N	A	U	D	R	D	P	Y	F	J	Z	Z	I	B	K	I	M	R	B

Dan menghasilkan Enkripsi Akhir

W	Z	R	N	D	J	R	N	A	U	D	R	D	P	Y	F	J	Z	Z	I	B	K	I	M	R	B

3.2. Teknik Penyembunyian Data (*Steganografi*) Metode LSB

Teknik penyembunyian data didalam citra gambar dilakukan akan mengubah kualitas citra tersebut. Adapun kriteria yang harus diperhatikan dalam penyembunyian data adalah:

a. Kualitas citra penampung tidak jauh berubah. Setelah dilakukan penambahan data rahasia, hasil citra steganografi masih terlihat dengan baik. Pengamat tidak mengetahui jika didalam citra tersebut terdapat data rahasia.
b. Data yang disembunyikan harus mampu bertahan terhadap manipulasi yang dilakukan pada citra penampung. Apabila pada citra dilakukan pengelohan, maka data yang disembunyikan tidak rusak.
c. Data yang disembunyikan harus dapat diungkapkan kembali (*recovery*) dengan menentukan jumlah biner pada data yang diinput kedalam citra.
d. Data yang dijadikan cover harus lebih besar dari data rahasia agar data rahasia tidak terlihat. Dan data tersebut sebaiknya digunakan satu kali. Karena apabila digunakan lebih dari satu kali, dapat menimbulkan kecurigaan pihak lain.

Penyembunyian data dilakukan dengan mengganti bit-bit data didalam segmen citra melalui bit-bit data rahasia yaitu melalui teknik metode LSB.

1101001<u>0</u>

***Most Significant Bit* (MSB)** **_Least Significant Bit_ (LSB)**

Artinya: bit yang cocok untuk digantikn adalah bit LSB, karena perubahan yang terjadi hanya mengubah nilai *byte* satu lebih tinggi atau lebih rendah dari nilai sebelumnya. Contohnya: *byte* tersebut menyatakan warna keabuan tertentu, maka perubahan satu bit LSB tidak mengubah warna keabuan tersebut secara bearti. Namun mata manusia tidak dapat membedakan perubahan yang kecil [14].

00110011 10100010 11100010 01101111

Sekumpulan data citra setelah ‘ 0 1 1 1 ‘ disembunyikan:

0 0 1 1 0 0 10 1 0 1 0 0 0 11 1 1 1 0 0 0 11 0 1 1 0 1 1 11

Untuk memperkuat teknik penyembunyian data, bit-bit data rahasia tidak digunakan untuk mengganti *byte-byte* yang berurutan, namun dipilih pada susunan *byte* secara acak.

Misalkan jika terdapat 50 byte dan 6 bit data yang akan disembunyikan, maka byte yang diganti bit LSB-nya dipilih secara acak. Misalkan *byte* angka 36, 5, 21, 10, 18, 49.

Jika menggunakan bahasa pemprograman PHP, fungsi yang akan digunakan untuk encoding atau menyembunyikan pesan ke dalam gambar, berikut adalah *source codenya :*

```
// Fungsi encoding steganografi LSB
function EncodeStegoLSB($pesan, $img) {
	$img = imagecreatefromjpeg('files/'.$img);
	//list($width, $height, $type, $attr) = getimagesize('files/'.$img);
	$message = $pesan.chr(0);
	$x=imagesx($img);
	$y=imagesy($img);
	$px=0; $py=23; $h = 23;
	for( $i=0;$i<strlen($message);$i++ ) {
		$px += $h;
		if( $px > $x ) {
			$px = $px%$x;
$rgb = imagecolorat($img, $px, $py);
$R = ($rgb >> 16) & 0xFF; $G = ($rgb >> 8) & 0xFF;
$B = $rgb & 0xFF;
$m = ord($message{$i});
$R = ($R&0xf8)| ($m&0x07);
$G =($B&0xf8)|(($m>>3)&0x07);
	$B = ($B&0xf8)| (($m>>6)&0x03);
	$t = imagecolorallocate($img, $R , $G , $B );
	imagesetpixel( $img , $px,$py , $t );}
	echo "Banyak biner: <b>".(strlen($message)*8)."</b> biner<br><br>";
	if(imagepng($img,'files/sample.png')) {
```

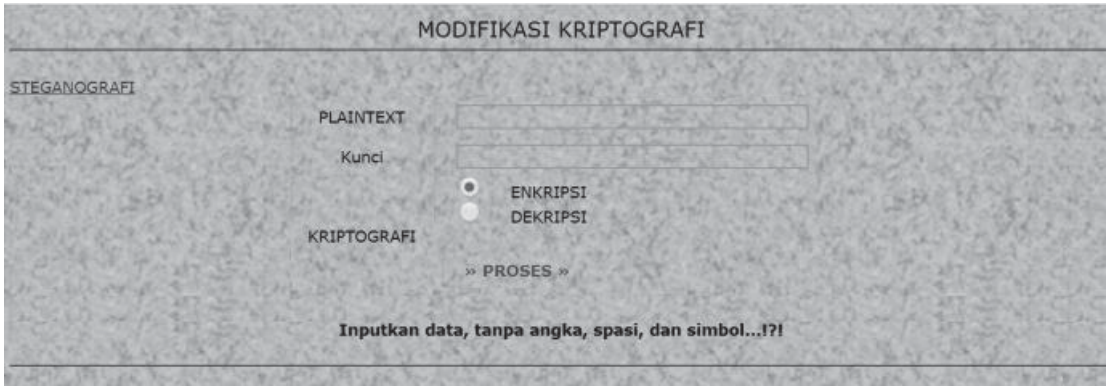
Kemudian berikut *source code* fungsi pesan untuk mendecoding gambar yang telah ditambah pesan rahasia sebagai berikut :

```
// Fungsi decoding steganografi LSB
function DecodeStegoLSB($img, $length) {
	$img = imagecreatefrompng("files/$img");
	//Stegano Dekripsi LSB
	$message='';
	$x=imagesx($img);
	$y=imagesy($img);
	$px=0;
	$py=23;
	$h = 23;
	while( TRUE ){
		$px += $h;
		if( $px > $x ) {
			$px = $px%$x;
			$py += $h; }
$rgb = imagecolorat($img, $px, $py);
		$R = ($rgb >> 16) & 0x7;
		$G = ($rgb >> 8) & 0x7;
```

```
            $B = $rgb & 0x3;
            $m = $R + ($G<<3) + ($B<<6);
            $g=dechex($G<<3);
            $b=dechex($B<<6);
        if( $m==0 ) break;
        $message .= chr($m);
        }
?>
```

3.3 Implementasi Program

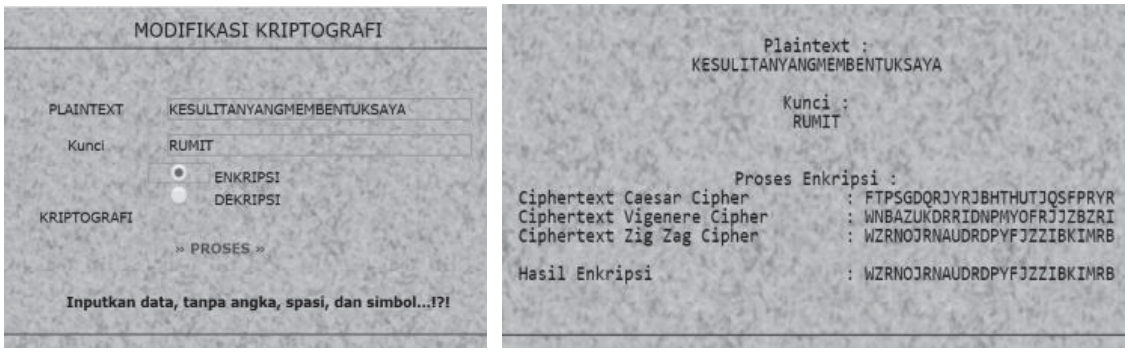
Halaman tampilan awal atau *Interface Program* untuk Proses Implementasi Program pada Gambar 2.



Gambar. 2 Halaman Utama

3.3.1 Proses Enkripsi

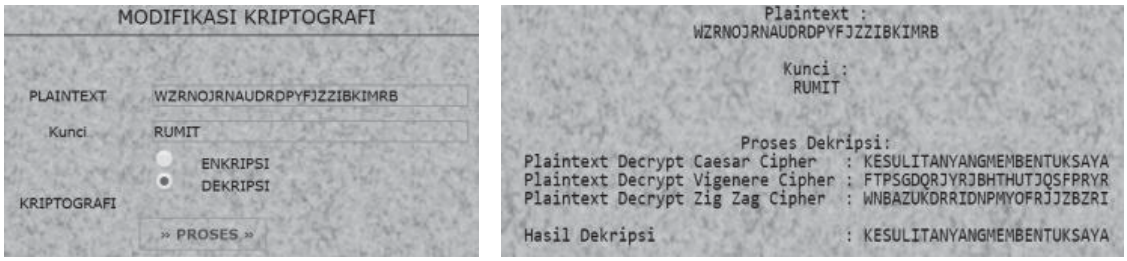
Berikutnya diberi plaintext dengan teks pesan yang akan digunakan “KESULITAN YANG MEMBENTUK SAYA” dan Kata Kunci “ RUMIT”. hasil dari proses enkripsi dari penerapan kombinasi 3 Algoritma *Caesar chiper, vigenere* dan *zigzag*. Menghasilkan output berupa teks enkripsi seperti Gambar 3.



Gambar 3. Proses Enkripsi dan Hasil

3.3.2 Proses Dekripsi

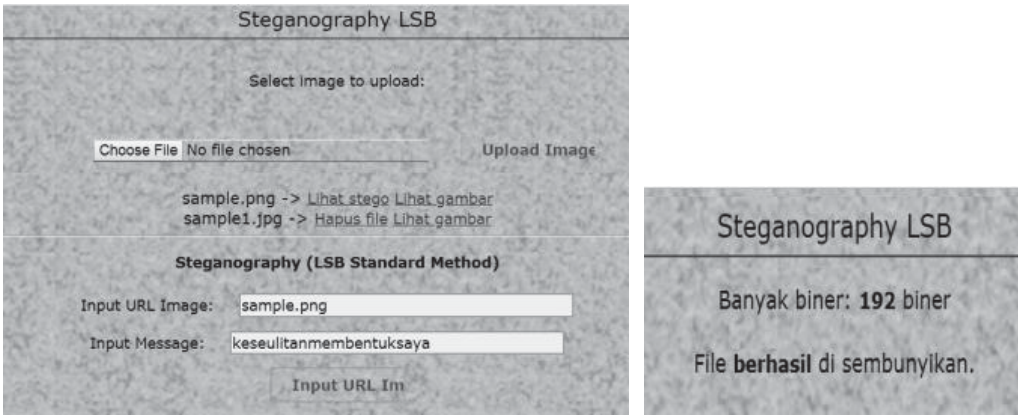
Proses dekripsi dapat dilihat pada Gambar 4 berikut.



Gambar 4. Proses Dekripsi dan Hasil

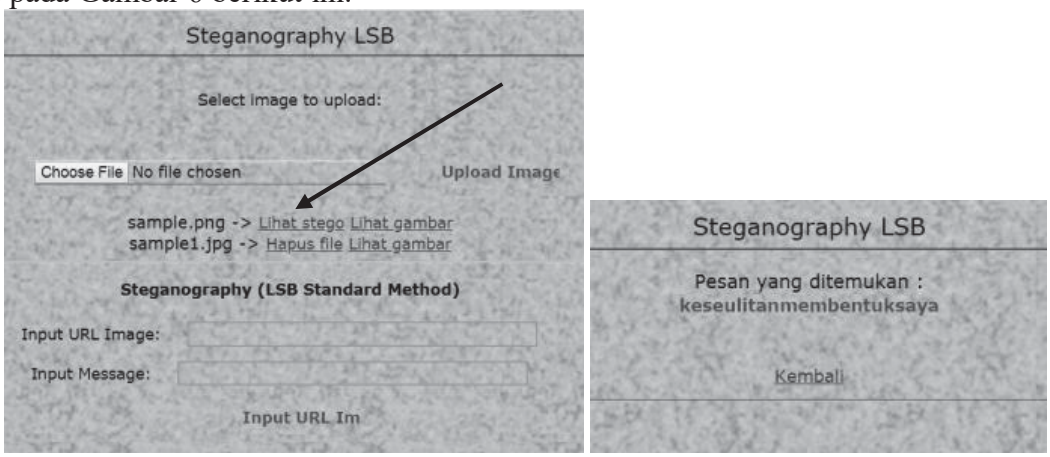
3.3.3 Pengujian Steganografi Menggunakan Metode LSB

Langkah pertama user harus memilih gambar yang akan disisipkan pesan rahasia kedalam menu *choose file* kemudian *upload image*, setelah itu user menginputkan url gambar yang telah di upload tadi, dan menginput pesan rahasia. Berikut tampilan proses *steganografi* dan tampilan gambar banyaknya jumlah biner pada file terlihat pada Gambar 5.



Gambar 5. Tampilan Proses Penyisipan Gambar dan jumlah biner

Kemudian proses jika ingin menampilkan gambar dan pesan rahasia, user mengklik menu lihat *stegano* Maka program akan menampilkan pesan rahasia yang telah diinput terlihat pada Gambar 6 berikut ini:

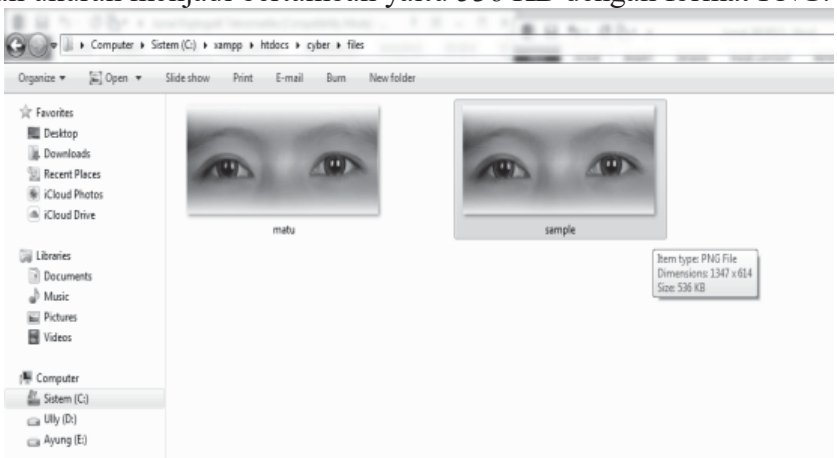


Gambar 6. Proses Menu *Steganografi* dan tampilan pesan

Untuk melihat perbandingan gambar yang telah di sisipkan pesan tidak akan mengalami perubahan kualitas gambar yang signifikan seperti kualitas warna (*brightness* atau *contrast*). Perbedaannya terletak pada jumlah ukuran gambar dan format gambar tersebut sebagai contoh berikut gambar pertama yang akan disisipkan pesan: Pada Gambar 7 menunjukkan jumlah ukuran 242 KB dengan format .JPG.

Gambar 7. Hasil Gambar Sebelum Disisipkan pesan

Kemudian berikut adalah gambar yang telah disisipkan pesan, pada Gambar 8 ini menunjukan jumlah ukuran menjadi bertambah yaitu 536 KB dengan format PNG.



Gambar 8. Hasil Gambar Setelah Disisipkan pesan

Hasil dari Pengujian sistem penggunaan kombinasi Algoritma *Kriptografi* dan *steganografi* LSB yang dibuat ini terdiri dari beberapa proses yaitu:

a. *Kriptografi* : (1) Enkripsi, (2) Dekripsi Mengenkripsi pesan menggunakan 3 metode; *caesar chiper, vigenere chiper* dan *zigzag chiper*. Setelah ditemukan hasil enkripsi maka proses berikutnya pesan di dekripsi kembali.
b. *Steganografi*: (1) Mengambil gambar, (2) menambah pesan kedalam gambar, (3) menampilkan pesan rahasia kedalam gambar. Sebagai pelengkap dikombinasikan menggunakan *steganografi* metode LSB. Proses pertama meload gambar yang ingin ditambahkan pesan rahasia, kemudian menambah pesan rahasia kedalam gambar *(encoding image)* dan telah ditentukan juga jumlah *biner* yang terinput dalam gambar dengan menampilkan pesan rahasia dan gambar.Untuk ukuran (*size*) dari file gambar yang telah disisipkan pesan rahasia menjadi bertambah besar.
c. Ukuran semula file gambar original *size* 242 kb dengan format .jpg setelah ditambah pesan rahasia mengalami kenaikan angka berukuran 536 kb dan menjadi format .png.

3. Kesimpulan

Penerapan penggabungan tiga algoritma *(caesar cipher, vigenere cipher,* dan *zig zag cipher)* dapat meningkatkan keamanan pesan dalam media gambar dan mengurangi kelemahan masing-masing algoritma. Dengan mengkombinasikan algoritma *kriptografi* dan *Steganografi* untuk menyembunyikan pesan pada gambar, tingkat keamanan data bisa lebih

terjaga keaslian datanya. Terutama dalam melindungi hak cipta (*copyright*) pada sebuah gambar tersebut.

Daftar Pustaka

[1] Yakub. (2012). *Pengantar Sistem Informasi*. Graha 11mu. Yogyakarta.
[2] Zunaidi, M., Suharsil. (2018). *Pengamanan Citra Digital Menggunakan Kombinasi Antara Algoritma AES Dan Metode LSB*. J-SISKO TECH, 1(2), 36–50.
[3] Zuli, F., Irawan, A. (2014). *Penerapan Kombinasi Sandi Caesar dan Vigenere untuk Pengaman Data Pesan*. Jurnal Sistem Informasi, 7(2) 1-11.
[4] Permana, A.P. (2018). *Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android*. Jurnal Al-Azhar Indonesia Seri Sains dan Teknologi, Vol 4. No 3.
[5] Hidayat, M.H., dkk. (2018). *Kombinasi Algoritma Kriptografi Vigenere Cipherdan Hill Cipher Untuk Penyandian Pesan Rahasia Pada Metode Steganograf*. Jurnal Skripsi, Vol 1 No 1.
[6] Ariyus, Dony. (2008). *Keamanan Data dan Komunikasi*. Graha 11mu. Yogyakarta.
[7] Gusmayuda Rizki A. *Steganografi pada Media Video Digital dengan Menggunakan Metode FFT (Fast Fourier Transform) dan LSB (Least Significant Bit)*. Teknik Informatika, Fakultas Teknik dan Ilmu Komputer, Universitas Komputer Indonesia.
[8] Gunawan, I. (2018). *Kombinasi Algoritma Caesar Cipher dan Algoritma RSA untuk Pengaman File Dokumen dan Pesan Teks*. Jurnal Nasional Information dan Teknologi Jaringan, Vol 2 No 2.
[9] Zuli, F., Irawan, A. (2014). *Penerapan Kombinasi Sandi Caesar dan Vigenere untuk Pengaman Data Pesan*. Jurnal Sistem Informasi, 7(2) 1-11
[10] Ariyus, Dony. (2008). *Keamanan Data dan Komunikasi*. Graha 11mu. Yogyakarta.
[11] Hondro, Rivalri Kristianto. *Aplikasi Enkripsi dan Dekripsi SMS Dengan Algoritma Zig zag Cipher Pada Mobile Phone Berbasis Android*. Pelita Informatika Budi Darma, Volume X, No. 3.
[12] Ariyus, Dony. (2008). *Keamanan Data dan Komunikasi*. Graha 11mu. Yogyakarta
[13] Aditya, Y., Pratama, A., Nurlifa, A. (2010). *Studi Pustaka Untuk Steganografi Dengan Beberapa Metode*. Seminar Nasional Aplikasi Teknologi Informasi (SNATI).
[14] Gusmayuda Rizki A. *Steganografi pada Media Video Digital dengan Menggunakan Metode FFT (Fast Fourier Transform) dan LSB (Least Significant Bit)*. Teknik Informatika, Fakultas Teknik dan Ilmu Komputer, Universitas Komputer Indonesia.