NASKAH PUBLIKASI

PENERAPAN KOMBINASI ALGORITMA KRIPTOGRAFI (CAESAR, VIGENERE, ZIG-ZAG) DAN METODE STEGANOGRAFI LSB UNTUK MENGAMANKAN PESAN KE DALAM CITRA DIGITAL

Program Studi Informatika

Disusun Oleh :
MARCELINUS OKY IRWANTO RUING
5130411160

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI DAN ELEKTRO
UNIVERSITAS TEKNOLOGI YOGYAKARTA
2020

NASKAH PUBLIKASI

PENERAPAN KOMBINASI ALGORITMA KRIPTOGRAFI (CAESAR, VIGENERE, ZIG-ZAG) DAN METODE STEGANOGRAFI LSB UNTUK MENGAMANKAN PESAN KE DALAM CITRA DIGITAL

Disusun Oleh :

MARCELINUS OKY IRWANTO RUING
5130411160

Pembimbing,

Dr. Erik Iman Heri Ujianto, S.T., M.Kom. tgl._____

PENERAPAN KOMBINASI ALGORITMA KRIPTOGRAFI (CAESAR, VIGENERE, ZIG-ZAG) DAN METODE STEGANOGRAFI LSB UNTUK MENGAMANKAN PESAN KE DALAM CITRA DIGITAL

Marcelinus Oky Irwanto Ruing, Erik Iman Heri Ujianto
Program Studi Informatika, Fakultas Teknologi Informasi dan Elektro
Universitas Teknologi Yogykarta
Jl. Ringroad Utara Jombor Sleman Yogyakarta
E-mail : [1] marcelinusoky@gmail.com, [2] erik.iman@uty.ac.id

ABSTRAK

Ancaman terhadap keamanan data bisa menjadi masalah yang sering terjadi. Data rahasia yang akan dikirim memerlukan keamanan agar tidak dapat dipersalahgunakan oleh pihak-pihak yang tidak bertanggungjawab. Data yang akan disampaikan memerlukan keamanan agar hanya dapat digunakan oleh penerima yang sah. Pengamanan data atau pesan ini perlu diterapkan dalam sebuah sistem komputer. Penerapan Kriptografi dan Steganografi digunakan untuk membangun sistem pengamanan data yang mampu melakukan proses enkripsi, dekripsi dan penyisipan pesan ke dalam citra digital. Algoritma yang digunakan adalah algoritma kriptografi klasik dan teknik steganografi menggunakan metode LSB. Data berupa pesan teks akan dienkripsi dengan menggunakan 3 metode kriptografi dan pesan tersebut akan disisipkan ke dalam citra digital dengan metode steganografi LSB *(least Significant Bit).*

Kata Kunci: Enkripsi, Dekripsi, Citra, Steganografi

1. PENDAHULUAN

Kemajuan ilmu pengetahuan dan teknologi saat ini mendorong setiap orang/individu, instansi atau perusahaan baik pemerintah maupun swasta untuk senantiasa menemukan dan menggunakan teknologi sebagai alat bantu dalam menjalankan tugas – tugas dari setiap individu yang ada di dalamnya, serta membantu dalam pemecahan masalah – masalah yang dihadapi. Penerapan sistem informasi berbasis komputer dirasakan lebih efektif dan efisien dibandingkan dengan sistem konvensional atau manual. Sistem informasi berbasis komputer juga merupakan salah satu strategi keunggulan kompetitif dan merupakan pilihan yang tepat dalam peningkatan pelayanan. Ancaman terhadap keamanan pesan bisa kapan saja terjadi. Data rahasia yang akan dikirim memerlukan keamanan agar tidak dapat dipersalahgunakan oleh pihak-pihak yang lain. Data yang akan disampaikan memerlukan keamanan agar hanya dapat digunakan oleh penerima yang sah.

Perancangan sebuah sistem keamanan pesan pada media citra digital dilakukan dengan mengenkripsi terlebih dahulu, kemudian dilakukan penyembunyian pesan. Algoritma yang digunakan untuk melakukan proses enkripsi dan dekripsi adalah kombinasi dari tiga algoritma kriptografi klasik dan teknik penyisipan pesan teks ke dalam citra digital dilakukan dengan metode steganografi LSB. Data akan dienkripsi dahulu menggunakan algoritma yang sudah ada seperti algoritma Caesar Cipher, Vigenere Cipher dan Zig-Zag Cipher. Algoritma-algoritma ini memiliki kelebihan dan kekurangan masing-masing, oleh karena itu perlunya dilakukan kombinasi terhadap beberapa algoritma tersebut agar dihasilkan *ciphertext* yang sulit dikriptanalisis, kemudian dilakukan penyembunyian pesan ke dalam citra digital dengan metode LSB *(Least Significant Bit).*

Pada penelitian ini dilakukan penggabungan tiga algoritma yaitu Caesar Cipher, Vigenere Cipher, dan Zig-Zag Cipher untuk melakukan proses enkripsi *plaintext* menjadi *ciphertext* dan proses dekripsi *ciphertext* menjadi *plaintext* yang berupa pesan teks. Selain itu, proses pengamanan pesan yang sudah dienkripsi menjadi sebuah *ciphertext* dilakukan dengan menyisipkan pesan tersebut ke dalam citra digital dengan teknik steganografi berbasis metode LSB.

2. LANDASAN TEORI

2.1. Kriptografi

Kata kriptografi berasal dari bahasa Yunani yang terdiri dari dua buah kata yaitu *cryptos* dan *graphia*. Kata *cryptos* berarti rahasia sedangkan *graphia* berarti tulisan yang secara umum memiliki makna tulisan rahasia. Menurut Dony Ariyus (2008), kriptografi adalah ilmu yang mempelajari tentang bagaimana menjaga kerahasiaan suatu pesan, agar isi pesan yang ditampilkan tersebut aman sampai ke penerima pesan.

Kriptografi adalah ilmu mengenai teknik enkripsi dimana "naskah asli" (*plaintext*) diacak menggunakan suatu kunci enkripsi menjadi naskah acak yang sulit dibaca (*ciphertext*) oleh seseorang

yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi bisa mendapatkan kembali data asli. Teknik enkripsi yang digunakan dalam kriptografi klasik adalah enkripsi simetris dimana kunci dekripsi sama dengan kunci enkripsi. Enkripsi, dekripsi dan pembuatan kunci untuk teknik enkripsi asimetris memerlukan komputasi yang lebih intensif dibandingkan enkripsi simetris, karena enkripsi asimetris menggunakan bilangan – bilangan yang sangat besar (Kromodimoeljo, 2010).

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 :

a) Menentukan kata yang akan menjadi kunci
b) Menentukan besarnya jumlah pergeseran huruf yang akan diganti berdasarkan kunci yang digunakan
c) Mengganti setiap huruf yang ada pada pesan sesuai dengan jumlah pergeseran huruf yang ditentukan dengan menggunakan kunci.
d) Merangkai kembali jumlah huruf sesuai dengan susunan pesan awal.

Setiap karakter pada informasi atau pesan teks yang akan diubah dengan menggeser karakter atau huruf kekanan dari karakter asli. Pergeseran huruf atau karakter diawali dengan karakter yang ada pada kata kunci. Sehingga dengan metode ini, karakter akan berubah menjadi karakter lain. Metode Caesar Cipher hanya menggunakan karakter huruf A, B, C, ..., Z dan dapat disamakan dengan angka 0, 1, 2, ..., 25.

2.1.2 Vigenere Cipher

Vigenere Cipher dikemukakan pertama kali oleh kriptologis dari Perancis bernama Blaise de Vigènere pada tahun 1586. Proses Vigenere Cipher dapat dilakukan dengan cara menggunakan tabel yang berisi alfabet yang disebut dengan bujur sangkar Vigenere Cipher untuk melakukan prosses dekripsi dan enkripsi.

	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 1 : Bujur Sangkar Vigenere

Pada gambar bujur sangkar vigenere, kolom paling kiri menyatakan huruf-huruf pada kata kunci sedangkan baris paling atas menyatakan huruf-huruf pada *plaintext. Ciphertext* dapat diperoleh dengan memasangkan huruf-huruf pada *plaintext* dengan huruf-huruf pada kata kunci. Jika panjang kunci (jumlah huruf) lebih pendek dari *plaintext*, maka kunci akan diulang hingga sama panjangnya dengan *plaintext.* Pengulangan ini biasa disebut sistem periodik.

Proses enkripsi dapat ditulis dalam bentuk operasi : Ci = (Pi + Ki) mod 26 sedangkan proses dekripsi dapat ditulis dengan bentuk operasi : Pi = (Ci – Ki) mod 26.

2.1.3 Zig-Zag Cipher

Zig-Zag Cipher adalah algoritma penyandian yang 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. Teknik yang diterapkan pada metode Zig-Zag Cipher adalah teknik Transposisi Cipher enkripsi dan dekripsi pesan dengan cara mengubah urutan huruf-huruf yang ada di dalam *plaintext* (pesan yang belum dienkripsi) menjadi *ciphertext* dengan cara tertentu agar isi pesan tersebut tidak dimengerti kecuali oleh orang-orang tertentu.

2.2. Steganografi *Least Significant Bit* (LSB)

Steganografi berasal dari Bahasa Yunani yaitu *Stegano* yang berarti "tersembunyi atau menyembunyikan" dan *graphy* yang berarti "Tulisan, jadi Steganografi adalah tulisan atau pesan yang disembunyikan.

Steganografi adalah teknik menyembunyikan tulisan pada suatu media tertentu seperti gambar, suara, dan lain-lain. LSB (*least Significant Bit)* adalah bagian dari barisan data biner yang mempunyai nilai paling kecil atau tidak berarti. LSB merupakan salahsatu teknik atau metode yang digunakan dalam sistem steganografi. Pada susunan bit di dalam sebuah *byte* (1 *byte* = 8 bit) memiliki bit yang paling berarti disebut MSB (*Most Significant Bit*) dan bit yang kurang berarti LSB (*Least Significant Bit*). Di dalam susunan *byte*, bit atau angka yang terletak paling akhir atau angka kedelapan merupakan LSB.

2.3. Citra Digital

Citra digital merupakan representatif dari citra yang diambil oleh mesin dengan bentuk pendekatan berdasarkan sampling dan kuantisasi. Sampling pada citra menyatakan besarnya kotak-kotak yang disusun dalam baris dan kolom serta menyatakan besar kecilnya ukuran *pixel* (titik) pada citra. Kuantisasi menyatakan besarnya nilai tingkat kecerahan yang dinyatakan dalam nilai tingkat keabuan (*grayscale*) sesuai dengan jumlah bit biner yang digunakan oleh

mesin, dengan kata lain kuantisas pada citra menyatakan jumlah warna yang terdapat pada citra. Citra digital adalah representasi dari intesitas cahaya dalam bentuk diskrit pada bidang 2 dimensi. Citra tersusun dari sekumpulan piksel (*picture element*) yang memiliki koordinat (x,y) yang menujukan letak atau posisi piksel dan amplitudo f (x,y) menujukan nilai intensitas warna citra. Ada beberapa jenis citra digital yang sering digunakan, yaitu sebagai berikut:

1. Citra Biner (Monokrom)

   Citra biner (Monokrom) merupakan citra yang hanya terdri dari 2 warna yaitu hitam dan putih. Citra biner hanya membutuhkan 1 bit di memori untuk menyimpan kedua warna tersebut.

2. Citra *Grayscale* (Skala Keabuan)

   Citra *grayscale* merupakan suatu citra yang hanya memiliki warna tingkat keabuan dan hanya membutuhkan intensitas tunggal. Intensitas dari citra *grayscale* disimpan dalam 8 bit integer yang memberikan 256 kemungkinan dimulai dari level 0 sampai 256 dimana 0 untuk warna hitam dan 256 untuk warna putih dan nilai diantaranya merupakan derajat keabuan. Banyaknya warna tergantung tergantung jumlah bit yang disediakan di dalam memori. Citra 2 bit mewakili 4 warna, citra 3 bit mewakili 8 warna, citra 3 bit mewakili 12 warna dan seterusnya.

3. Citra Warna (RGB)

   Citra warna (RGB) merupakan citra yang tersusun dari 3 warna yaitu merah, hijau dan biru (*Red, Green and Blue*). Setiap warna dasar mengggunakan penyimpanan 8 bit (1 byte), yang artinya setia warna memiliki gradasi sebanyak 255 warna. Pada citra RGB 24-bit, masing-masing kanal warna memiliki nilai intensitas piksel dengan kedalaman bit sebesar 8-bit yang artinya memiliki varisi warna sebanyak $2^8 = 256$ derajat warna (0-255). Setiap piksel pada citra RGB memiliki nilai intensitas yang merupakan kombinasi nilai dari R (*Red*), G (*Green*) dan B (*Blue*). Variasi warna pada setiap piksel adalah sebanyak 255 x 255 x 255 = 16.777.216.

2.4. *Peak Signal to Noise Ratio* (PSNR)

Peak Signal to Noise Ratio merupakan perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut yang diukur dalam satuan desibel. Standar nilai PSNR pada citra 8 bit adalah 30dB - 40dB atau lebih. Mengukur PSNR dapat dilakukan dengan mengetahui nilai MSE atau *Mean Square Error* yang merupakan nilai *error* kuadrat rata-rata antara citra *cover* dan citra Steganografi. Semakin besar nilai PSNR maka semakin baik kualitas citra Steganografi, semakin rendah nilai MSE maka akan semakin baik kualitas citra Steganografi tersebut. Nilai MSE dan PSNR dapat dihitung dengan persamaan di bawah ini :

$$MSE = \frac{1}{MN} \sum_{y=1}^{M} \sum_{x=1}^{N} [I(x,y) - I'(x,y)]^2$$

Gambar 2 Rumus MSE

$$PSNR = 10.log \left(\frac{MAXi^2}{MSE} \right)$$

Gambar 3 Rumus PSNR

Dimana :
MSE = nilai *Mean Square Error*
PSNR = nilai *Peak Signal to Noise Ratio*
MAXi = nilai maksimum pixel suatu citra yaitu 2^8-1 = 255 (citra 8 bit)
M = panjang citra stego (dalam *pixel*)
N = lebar citra stego (dalam *pixel*)
I(x,y) = nilai piksel dari citra cover
I'(x,y) = nilai piksel dari citra stego

3. METODOLOGI PENELITIAN

3.1. Pengumpulan Data

Pengumpulan data adalah suatu metode dan prosedur yang digunakan untuk mendapatkan suatu informasi tentang apa saja yang harus dikerjakan pada saat pengembangan sistem yang akan dibangun. Pada tahap ini untuk membangun sistem, maka akan dilakukan dengan cara :

3.1.1 Observasi

Peneliti melakukan pengamatan, mencari dan menemukan informasi-informasi, fakta dan data secara objektif, sistematis, nyata dan dapat dipertanggungjawabkan berdasarkan pengetahuan dan gagasan terkait yang telah diketahui sebelumnya dan dibutuhkan guna melanjutkan suatu penelitian.

3.1.2 Literasi

Teknik literasi dilakukan dengan mencari informasi dan materi yang dapat membantu dalam pengembangan sistem yang akan dibangun. Penulis mencari dan mengumpulkan berbagai jenis literasi seperti buku, jurnal, paper dan bentuk penulisan lain yang sudah dilakukan sebelumnya dan berkaitan dengan penelitian yang akan dilakukan oleh peneliti.

3.1.3 Pengumpulan Data Citra Digital

Pada penelitian ini, peneliti akan melakukan pemilihan dan percobaan terhadap berbagai citra digital dengan ukuran, tipe dan dimensi piksel yang berbeda untuk memperoleh hasil yang beragam

3.2. Analisis Perancangan Sistem

Setelah data–data yang diperlukan sudah terkumpul, analisis sistem dilakukan dengan menggunakan instrumen-instrumen yang sudah terkumpul tersebut dan meliputi kegiatan penggambaran sistem yang sedang berjalan, analisis

kelemahan-kelemahan sistem yang sudah ada, serta solusi perancangan sistem informasi pengolahan data yang lebih baik.

3.2.1 Prinsip Kerja Sistem

Pada penelitian ini algoritma kriptografi yaitu Caesar Cipher, Vigenere Cipher dan Zig-Zag Cipher dikombinasikan dalam mengenkripsi *plaintext* dengan menggunakan kunci. Hasil dari enkripsi tersebut yang berupa *ciphertext* kemudian disisipkan ke dalam citra digital dengan sistem steganografi metode *Least Significant Bit* (LSB). *Ciphertext* yang dihasilkan bisa kembali didekripsi dengan kombinasi algoritma kriptografi dan kunci yang sama.

3.2.2 Desain Sistem

Tahap berikutnya yaitu tahap perancangan sistem, dalam penelitian ini peneliti menggambarkan proses alur sistem laporan yang dihasilkan sistem bagi pengguna, menggunakan alur kerja sistem yang memudahkan peneliti untuk mengetahui asal data, arah tujuannya, hingga di mana data akan disimpan.

3.3. Implementasi

Berdasarkan rancangan alur sistem yang dibangun dan desain data yang dibuat, maka peneliti akan membangun sistem yang dapat melakukan enkripsi dan dekripsi pesan teks dalam proses kriptografi klasik dan mampu menyisipkan pesan teks ke dalam citra digital dengan metode Steganografi LSB, dengan menggunakan bahasa pemrograman PHP. Implementasi sistem dilakukan dengan proses kriptografi dengan mengkombinasikan tiga metode yaitu, Caesar Cipher, Vigenere Cipher dan Zig-Zag Cipher dan juga proses steganografi LSB dengan menyisipkan pesan teks ke dalam citra digital.

3.4. Pengujian

Metode pengujian sistem yang akan diakukan terhadap aplikasi yang dibuat adalah menguji nilai PSNR (*Peak Signal to Noise Ratio*) yaitu mengukur dan menentukan kemampuan aplikasi dalam menyisipkan pesan teks ke dalam citra digital steganografi dalam satuan desibel.

4. HASIL DAN PEMBAHASAN

Pada penelitian ini, peneliti akan membahas dan menjelaskan tentang proses Kriptografi dan Steganografi serta proses pengujian sistem yang dibuat. Berdasarkan beberapa data citra digital, *ciphertext* dan kunci yang digunakan pada penelitian ini, peneliti akan mengambil satu sampel untuk menjelaskan bagaimana proses yang terjadi. Sebagai contoh, peneliti akan mengambil sampel pada pada sebuah citra digital dan sebuah contoh *ciphertext* “SEMANGATREVISI” serta “WISUDA” sebagai kunci

4.1. Enkripsi

4.1.1 Caesar Cipher

Plaintext : SEMANGATREVISI
Kunci : WISUDA

Tabel 1: Proses Enkripsi

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

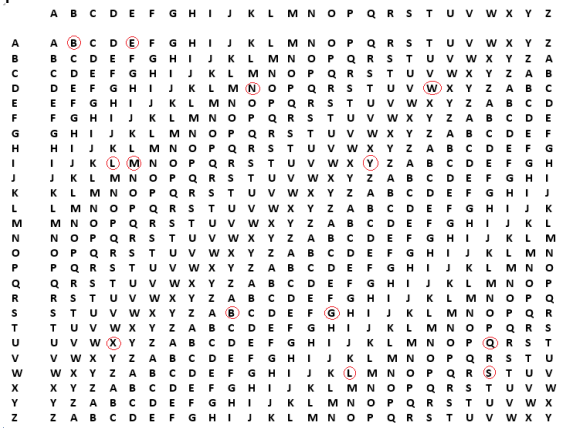
Ciphertext : PDJWKBWQODTEPE

4.1.2 Vigenere Cipher

Tabel 2: Pengulangan Kunci

P	D	J	W	K	B	W	Q	O	D	T	E	P	E
W	I	S	U	D	A	W	I	S	U	D	A	W	I

Pada tabel di atas, jika panjang kunci kurang dari panjang *plaintext* maka kunci dituliskan berulang hingga memiliki jumlah atau panjang karakter yang sama dengan *plaintext.* Proses enkripsi Vigenere Cipher dapat dilakukan dengan memasangkan *plaintext* dan kunci dengan menggunakan bujur sangkar vigenere seperti di bawah ini dimana *plaintext* pada posisi horizontal dan kunci pada posisi vertikal.



Gambar 4: Bujur Sangkar Vigenere Cipher

Berdasarkan proses enkripsi Vigenere di atas dengan menggunakan bujur sangkar Vigenere maka, diperoleh *ciphertext* : LLBQNBSYGXWELM yang akan menjadi *plaintext* untuk proses enkripsi Zig-Zag Cipher.

4.1.3 Zig-Zag Cipher

Berikut ini merupakan proses enkripsi dengan metode Zig-Zag Cipher dengan pola offset = 0 dengan pola kunci 3 baris. Panjang atau banyaknya kolom berdasarkan jumlah karakter pada *plaintext.*

Tabel 3: Proses Enkripsi Zig-Zag Cipher

L				N				G				L	
	L		Q		B		Y		X		E		M
		B				S				W			

Baris 1 : LNGL
Baris 2 : LQBYXEM
Baris 3 : BSW
Jadi *ciphertext* yang dihasilkan adalah LNGLLQBYXEMBSW

4.2. Steganografi LSB

Pada data citra1 yang memiliki dimensi 593 x 530 piksel akan disipkan suatu barisan pesan LNGLLQBYXEMBSW yang merupakan *ciphertext* dari hasil enkripsi sebelumnya. Misalkan kita mengambil dua huruf awal pada *ciphertext* di atas yaitu L dan N yang akan disisipkan pada 6 piksel pada citra1 yang memiliki matriks tingkat keabuan dengan biner sebagai berikut :

11000100 00001010 01100001 10110000 00111000 01001101

01000011 11001000 01100100 01100101 00100010 11111010

00011001 10010110 00101101 00101100 01000010 01100011

Matriks piksel di atas akan disipkan dua huruf L dan N yang berdasarkan kode ASCII huruf L = 76 = 01001100 dan N = 78 = 01001110. Proses pergantian bit dilakukan menurut kolom sehingga menghasilkan perubahan seperti di bawah ini :

11000100 00001010 01100000 10110001 00111001 01001100

01000011 11001001 01100100 01100100 00100011 11111010

00011000 10010111 00101100 00101100 01000011 01100011

4.3. Dekripsi

4.3.1 Zig-Zag Cipher

Ciphertext : LNGLLQBYXEMBSW

Proses dekripsi Zig-Zag Cipher dilakukan sama dengan proses enkripsinya yaitu dengan menggunakan pola *offset* = 0 dan pola kunci 3 baris. Terdapat 14 karakter pada *ciphertext* di atas, sehingga jumlah kolom pada tabel perhitungan sama dengan jumlah karakter tersebut. Deretan karakter pada *ciphertext* akan dibagi menjadi 3 bagian dan diisi ke dalam kolom dengan pola Zig-Zag sesuai urutan baris pada pada pembagian tersebut. Berikut ini proses dekripsi Zig-Zag Cipher :

Tabel 1: Proses Dekripsi Zig-Zag Cipher

L				N				G				L	
	L		Q		B		Y		X		E		M
		B				S				W			

Plaintext bisa diperoleh dengan membaca menyusun karakter-karakter tersebut dengan cara atau pola Zig-Zag sehinga diperoleh hasil LLBQNBSYGXWELM. Hasil tersebut akan didekripsikan lagi dengan metode Vigenere Cipher.

4.3.2 Vigenere Cipher

Ciphertext : LLBQNBSYGXWELM

Kunci : WISUDA

Tabel 2: Pengulangan Kunci Dekripsi Vigenere

L	L	B	Q	N	B	S	Y	G	X	W	E	L	M
W	I	S	U	D	A	W	I	S	U	D	A	W	I

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

Gambar 5: Penomoran Alfabet

Proses dekripsi akan dilakukan dengan perhitungan di bawah ini :

P*i* = (C*i* – K*i*) mod 26 ; untuk **C*i* >= K*i***

P*i* = (C*i* + 26 – K*i*) mod 26 ; untuk **C*i* <= K*i***

Semisal diambil contoh perhitungan pasangan karakter atau huruf kolom pertama pada Tabel 5.5 di atas yaitu "L" dan "W" dengan menggunakan persamaan di atas

Diketahui :

C*i* = L = 11 dan **K*i*** = W = 22 (untuk **C*i* <= K*i*)**

Maka :

P*i* = (C*i* + 26 – K*i*) mod 26 ; untuk **C*i* <= K*i***

= (11 + 26 – 22)

= 15

Berdasarkan aturan penomoran alfabet pada Gambar 5.49 di atas maka, didapat 15 = P. Semua pasangan karakter berikutnya dapat dihitung dengan persamaan seperti contoh di atas dengan memperhatikan perbandingan besar kecilnya nilai huruf pada *ciphertext* dan kunci sehingga diperoleh *ciphertext* PDJWKBWQODTEPE.

4.3.3 Caesar Cipher

Ciphertext : PDJWKBWQODTEPE

Kunci : WISUDA

Tabel 3: Enkripsi Caesar Cipher

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

Plaintext dapat diperoleh dengan memasangkan deretan huruf pada *ciphertext* dengan baris pertama yang merupakan baris kunci. Berdasarkan proses dekripsi Caesar Cipher di atas maka, diperoleh *plaintext* SEMANGATREVISI.

4.4. Hasil Citra

Berikut ini merupakan sampel citra digital yang akan disisipkan pesan dan perubahan yang terjadi pada citra digital tersebut setelah disisipkan pesan teks.

Ciphertext : LNGLLQBYXEMBSW

Dimensi : 441 x 253
Ukuran : 23,6 KB
Tipe : JPEG

Gambar 5: Citra Cover

Dimensi : 441 x 253
Ukuran : 84,1 KB
Tipe : PNG

Gambar 6: Citra Stego

4.5. Pengujian PSNR

Berdasarkan dari hasil pengujian aplikasi dalam proses Kriptografi dan Steganografi dengan ukuran citra, pesan teks dan jenis citra yang berbeda maka, didapat hasil *Peak Signal to Noise Ratio* (PSNR) sebagai berikut :

Tabel 4: Nilai Peak Signal to Noise Ratio

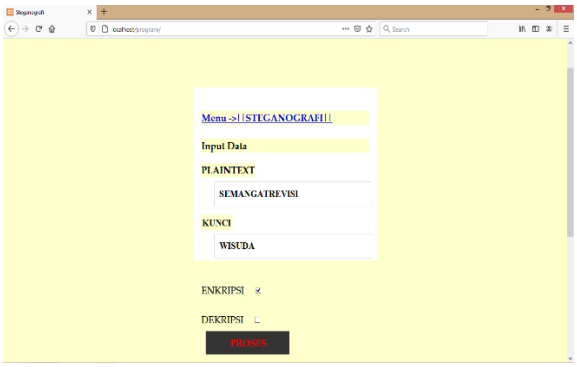
No	Nama File	Resolusi (*pixel*)		Ukuran File (KB)		PSNR (dB)			
		Sebelum	Sesudah	Sebelum	Sesudah	R	G	B	Rata-Rata
1	gambar1	256 x 192	256 x 192	24,0	103	42,446	47,862	45,65	45,319
2	gambar2	593 x 530	593 x 530	93,0	481	42,237	49,994	41,461	44,564
3	gambar3	750 x 500	750 x 500	54,0	122	40,464	44,895	35,449	40,269
4	gambar4	1170 x 550	1170 x 550	145	999	49,424	50,57	48,348	49,447
5	gambar5	1920 x 1221	1920 x 1221	234	2370	47,743	49,658	49,346	48,915
6	gambar6	2999 x 1910	2999 x 1910	323	1300	44,235	50,78	48,237	47,751
7	gambar7	750 x 500	750 x 500	59,5	254	47,567	43,497	37,464	42,842
8	gambar8	256 x 256	256 x 256	9,87	62,2	43,767	41,995	50,724	45,495
9	gambar9	441 x 253	441 x 253	23,6	84,1	50,497	47,106	46,243	46,654
10	gambar10	253 x 199	253 x 199	13,7	49,1	32,849	48,734	44,354	41,979
11	gambar11	512 x 512	512 x 512	50,8	92,2	33,66	40,349	48,567	47,862
12	gambar12	259 x 154	259 x 154	4,27	17,9	35,656	38,267	42,767	38,897
13	gambar13	151 x 194	151 x 194	6,34	12,0	44,647	46,224	35,849	47,858
14	gambar14	296 x 170	296 x 170	9,48	60,2	47,786	41,580	43,667	40,78
15	gambar15	640 x 426	640 x 426	91,9	546	49,76	47,862	45,656	43,897
16	gambar16	700 x 489	700 x 489	181	632	48,687	51,205	41,647	41,945
17	gambar17	200 x 252	200 x 252	10,8	66,0	46,89	43,533	47,86	49,106
18	gambar18	1000 x 625	1000 x 625	161	999	42,987	39,833	48,761	43,86
19	gambar19	1600 x 1000	1600 x 1000	434	2280	50,456	43,319	49,687	47,821
20	gambar20	1280 x 743	1280 x 743	148	1080	41,787	44,247	45,894	43,976

Mengukur PSNR dapat dilakukan dengan mengetahui nilai MSE atau *Mean Square Error* yang merupakan nilai *error* kuadrat rata-rata antara citra *cover* dan citra Steganografi. Semakin besar nilai PSNR maka semakin baik kualitas citra Steganografi, semakin rendah nilai MSE maka akan semakin baik kualitas citra Steganografi tersebut.

4.6. Implementasi

4.6.1 Halaman Proses Enkripsi

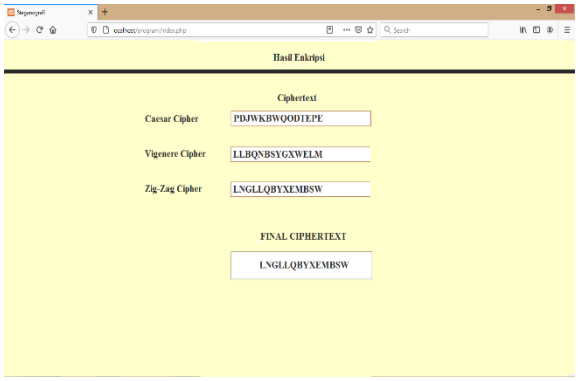
Halaman ini merupakan halaman yang menampilkan proses input kata kunci dan pesan teks yang akan dienkripsi dengan tiga metode yaitu, Caesar Cipher, Vigenere Cipher dan Zig-Zag Cipher.



Gambar 7: Halaman Kriptografi

4.6.2 Halaman Hasil Enkripsi

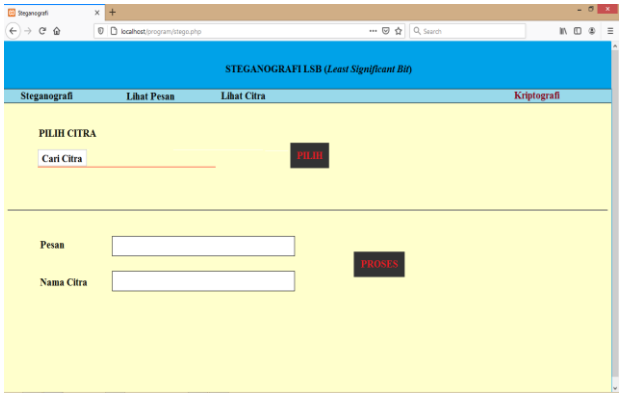
Pada halaman ini menampilkan hasil enkripsi *plaintext* dengan metode Caesar Cipher, Vigenere Cipher dan Zig-Zag Cipher serta menampikan final *Ciphertext* yang dihasilkan.



Gambar 8: Hasil Enkripsi

4.6.3 Halaman Steganografi

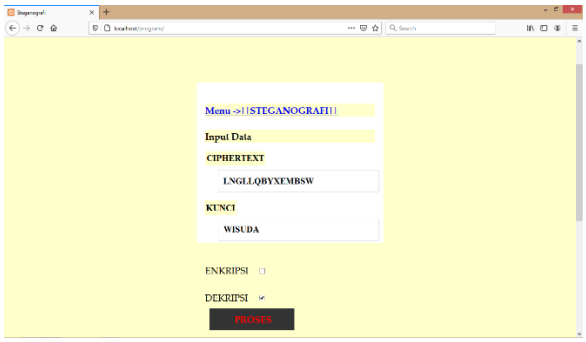
Halaman steganografi merupakan halaman yang menampilkan proses steganografi dengan metode *Least Significant Bit* (LSB). Pada halaman ini akan ditampilkan proses pemilihan citra digital yang akan digunakan dan memasukan pesan teks ke dalam citra digital tersebut.



Gambar 9: Halaman Steganografi

4.6.4 Halaman Proses Dekripsi

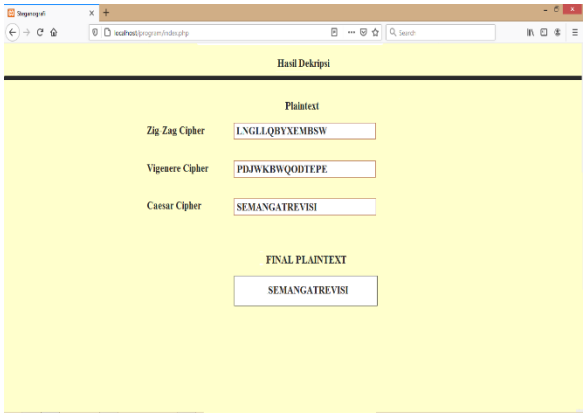
Pada halaman ini menampilkan proses dekripsi *Ciphertext* dengan metode Caesar Cipher, Vigenere Cipher dan Zig-Zag Cipher serta menampikan hasil akhir dari proses dekripsi.



Gambar 10: Proses Dekripsi

4.6.5 Halaman Hasil Dekripsi

Halaman ini merupakan halaman yang menampilkan dan memberitahukan hasil dari proses dekripsi *ciphertext* menjadi *plaintext* atau pesan asli.



Gambar 11: Hasil Dekripsi

4.6.6 Halaman Lihat Pesan Steganografi

Halaman ini merupakan halaman yang manampilkan pesan yang telah berhasil disisipkan ke dalam citra stego

Gambar 12: Lihat Pesan Steganografi

5. PENUTUP

5.1. Simpulan

Berdasarkan rancangan, pembuatan dan pembahasan penelitian dan aplikasi yang telah dibuat, maka peneliti menemukan beberapa kesimpulan tentang penelitian ini sebagai berikut :

1. Sistem atau aplikasi yang telah dibangun mampu melakuan proses enkripsi pesan teks dengan algoritma kriptografi melalui tiga metode klasik yaitu, Caesar Cipher, Vigenere Cipher dan Zig-Zag Cipher secara berurutan.
2. Sistem atau apliksi yang telah dibangun mampu melakukan proses dekripsi pesan teks yang telah dienkripsi sebelumnya ke dalam bentuk semula dengan algoritma kriptografi Zig-Zag Cipher, Vigenere Cipher dan Caesar Cipher secara berurutan.
3. Sistem atau aplikasi yang dibangun mampu melakukan proses penyisipan pesan teks ke dalam sebuah citra digital dengan algoritma metode steganografi *Least Significant Bit* (LSB).

5.2. Saran

Secara umum berdasarkan penelitian yang telah dilakukan, didapat beberapa saran yang ingin disampaikan oleh peneliti terkait penelitian ini adalah sebagai berikut :

1. Sistem atau aplikasi yang telah dibangun belum bisa melakukan proses enkripsi dan dekripsi pesan teks berupa simbol, angka dan menggunakan spasi sehingga disarankan untuk penelitian pengembangan selanjutnya bisa mengembangkan keterbatasan tersebut.
2. Sistem atau aplikasi yang dibangun hanya dapat melakukan proses enkoding pada steganografi LSB secara otomatis, sehingga disarankan untuk penelitian selanjutnya dapat dikembangkan proses dekoding secara terpisah dengan menggunakan kata kunci.

DAFTAR PUSTAKA

Amin, M.M. (2016). *Implementasi Kriptografi Klasik pada Komunikasi Berbasis Teks.* Jurnal Pseudocode, Vol.3, No.2, ISNN: 2355-5920.

Ariyus, Dony. (2008). *Keamanan Data dan Komunikasi*. Yogyakarta: Graha Ilmu.

Hallim, A., dkk. (2010). *Pembuatan Perangkat Lunak Media Pembelajaran Kriptografi Klasik.* Makalah Seminar Proyek Akhir. Politeknik Elektronika Negeri Surabaya – Institut Teknologi Sepuluh Nopember.

Hariati, A., dkk. (2018). *Kombinasi Algoritma Playfair Cipher denagn Metode Zig-Zag dalam Penyandian Teks.* Publikasi Jurnal dan Penelitian Teknik Informatika. Vol.2 No.2

Hondro, R.K. (2015). *Aplikasi Enkripsi dan Dekripsi SMS dengan Algoritma Zig-Zag Cipher pada Mobile Phone Berbeasis Android.* Pelita Informatika Budi Darma. Vol. 10, No. 3. Hal. 122-127. ISSN: 2301-9425.

Ganesha, D. A., dkk. (2015). *Implementasi Kriptografi dan Steganografi pada Media Gambar Menggunakan Algoritma Blowfish dan Metode Least Significant Bit.* e.Proceeding of Engineering. Vol.2 No.2 Hal 3762.

Kromodimoeljo S. (2010). *Teori dan Aplikasi Kriptografi*. SPK IT Consulting. http://www.buku-e.lipi.go.id/utama.cgi?lihatarsip&sent001&1254672494 diakses pada 2 November 2019

Putra, D. (2010). *Pengolahan Citra Digital*. Yogyakarta: Andi.

Putri, T.E., dkk. (2017). *Perbaikan Algoritma Steganografi Teknik Least Significant Bit untuk Aplikasi Keamanan Data.* JoP. Vol. 3 No. 1 Hal 27-32. ISSN : 2502-2016. Universitas Gajah Mada.

Susanto, I.A., Solichin, A. (2018). *Enkripsi Data Penggajian dengan Algoritma Caesar Cipher dan Vigenere Cipher pada PT. Kemasindo Cepat Nusantara.* Skanika, Vol.1, No.1., Universitas Budi Luhur.

Sutoyo,T.,dkk. (2009). *Teori Pengolahan Citra Digital*. Yogyakarta: Andi

Yank K. (2012). *PHP & MySQL: Novice to Ninja.* SitePoint. https://www.goodreads.com/book/show/13355763-php-mysql diakses pada 16 Oktober 2019

Zuli, F., Irawan, A. (2014). *Penerapan Kombinasi Sandi Caesar dan Vigenere untuk Pengamanan Data Pesan.* Jurnal Sistem Informasi. Vol. 7 No. 2 Hal. 1-11.