HASIL_CEK8_60010383

by Cek8_60010383 60010383

Submission date: 17-Dec-2020 09:56AM (UTC+0700)
Submission ID: 1477311585
File name: CEK8_60010383.pdf (415.55K)
Word count: 5245
Character count: 29876

Terakreditasi SINTA Peringkat 2
Surat Keputusan Dirjen Penguatan Riset dan Pengembangan Ristek Dikti No. 10/E/KPT/2019
masa berlaku mulai Vol. 1 No. 1 tahun 2017 s.d Vol. 5 No. 3 tahun 2021

Terbit online pada laman web jurnal: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 4 No. 3 (2020) 454 - 461 ISSN Media Elektronik: 2580-0760

Implementasi Algoritma *Playfair Cipher* dan *Least Significant Bit pada Citra Digital*

Hermansa[1], Rusydi Umar[2], Anton Yudhana[3]
[1]Magister Teknik Informatika, Fakultas Teknik Industri, Universitas Ahmad Dahlan
[2]Teknik Informatika, Fakultas Teknik Industri, Universitas Ahmad Dahlan
[3]Teknik Elektro, Fakultas Teknik Industri, Universitas Ahmad Dahlan
[1]himmaherman@gmail.com,[2]rusydi_umar@rocketmail.com, [3]eyudhana@mti.uad.ac.id

Abstract

Message security is very important now. Because security is part of the privacy of someone who wants to protect messages from those who do not have the right to read or receive them. The method used for securing information messages with message encryption and decryption techniques is the Playfair Cipher algorithm combined with the Least Significant Bit (LSB) method. In this study it was found that the Playfair Cipher algorithm is quite safe in implementing cryptographic encryption or ciphertext because the playfair cipher has a level of appearance of letters that is so difficult to predict so that the ciphertext becomes a randomized collection of data. For the Least Significant Bit (LSB) steganography method in the insertion of a secret or embedded message it is difficult to guess in plain view the changes that occur between before and after the image is inserted are not too significant. Also see the value of the Peak-Signal-to-Noise ratio or PSNR can still be considered good quality due to> 30 decibels (dB). So the final result of the combination of the Playfair Cipher algorithm with the Least Significant Bit (LSB) method is quite good in securing messages.

Keywords: implementation, playfair cipher, least significant bit, digital image

Abstrak

Keamanan pesan merupakan sesuatu hal yang sangat penting sekarang ini. Dikarenakan keamanan merupakan bagian privasi dari seseorang yang ingin menjaga pesan dari mereka yang tidak memiliki hak dalam membacanya atau menerimanya. Metode yang digunakan untuk pengamanan pesan informasi dengan teknik enkripsi dan dekripsi pesan adalah algoritma *Playfair Cipher* dengan dikombinasikan menggunakan metode *Least Significant Bit* (LSB). Dalam penelitian ini diperoleh bahwa algoritma *playfair cipher* cukup aman dalan implementasi enkripsi pesan rahasia atau *ciphertext* dikarenakan *playfair cipher* memiliki tingkat kemunculan huruf-huruf yang begitu sulit untuk diprediksi sehimgga *ciphertext* menjadi kumpulan data yang sudah teracak. Untuk metode steganografi *Least Significant Bit* (LSB) dalam penyisipan pesan rahasia atau *embedded* sulit ditebak secara kasat mata melihat perubahan yang terjadi antara sebelum dan sesudah gambar disisipkan tidak terlalu signifikan. Juga melihat nilai hasil *Peak-Signal-to-Noise ratio* atau PSNR masih dapat dianggap berkuaitas bagus dikarenakan >30 desibel (dB). Sehingga hasil akhir dari kombinasi algoritma *Playfair Cipher* dengan metode *Least Significant Bit* (LSB) cukup baik dalam pengamanan pesan.

Kata kunci: implementasi, playfair cipher, least significant bit, citra digital

1. Pendahuluan

Keamanan pesan merupakan sesuatu hal yang sangat penting sekarang ini[1]. Media sosial yang sering digunakan saat ini memang memiliki *security* tersendiri dalam menjaga keamanannya, namun sebaik-baik keamanan pada suatu sosial media pasti memiliki kelemahan atau celah dalam peretasan baik menggunakan *sofware* tertentu ataupun melalui jaringan. Kerentanan dalam *system* layanan *online* berpotensi diserang peretas, serangan pada layanan *online* dapat terjadi kapan saja dan butuh solusi untuk memperbaikinya[2]. Layanan-layanan mesin pencari selalu berkembang yang berdampak pada privasi pengguna termasuk opsi fitur untuk menjelajahi Internet secara pribadi[3][4].

Diterima Redaksi : 08-04-2020 | Selesai Revisi : 20-05-2020 | Diterbitkan Online : 20-06-2020

Sehingga keamanan dalam pengiriman pesan maupun komunikasi data harus menjadi perhatian yang lebih[5]. Aktifitas manusia saat ini sebagian besar berhubungan dengan data, informasi, dan komunikasi, serta dalam kegiatannya secara langsung maupun tidak langsung akan berhubungan dengan perangkat teknologi *computer*[6][7]. Teknologi yang semakin canggih menjadi bagian yang tidak bisa lepas dari kehidupan masyarakat, tidak hanya melakukan kegiatan-kegiatan positif namun kegiatan-kegiatan negatif juga[8][9]. Dampak dari banyaknya kejahatan menggunakan teknologi informasi khususnya menggunakan Internet, dapat kita lihat dari beberapa kejahatan sering dilakukan dalam bentuk serangan yang terjadi dalam lembaga atau instansi tertentu[10].

Oleh karena itu dibutuhkan suatu sistem yang dapat melindungin pesan informasi dengan aman. Diantara teknik keamanan pesan yang bisa digunakan yaitu, Kriptografi dengan algoritma *playfair Cipher*. Kriptografi merupakan teknik keamanan pesan dengan cara pesan dienkripsi atau diacak sedemikian rupa agar pesan tidak dapat dengan mudah dibaca oleh orang lain, kecuali yang diberikan kunci dekripsi sehingga dapat mengetahui pesan informasi yang diberikan. Namun dizaman digital sekarang kriptografi tidak hanya sekedar keamanan komunikasi akan tetapi juga bisa digunakan untuk pengamanan data integritas, keaslian dan pemalsuan atau manipulasi[11].

Teknik keamanan yang juga bisa dimanfaatkan adalah Metode Steganografi *Least Significant Bit* (LSB). Metode keamanan pesan informasi LSB merupakan teknik *embedded* atau penyisipan pesan kedalam sebuah wadah atau media penampung, dapat berupa *text, image, audio* dan *video*. Pada penelitian ini media yang digunakan untuk penerapan Metode LSB yaitu, *Citra Image* atau *Cover Image*.

Adapun penelitian yang berhubungan dengan teknik kriptografi *Playfair Cipher* maupun metode Steganografi *Least Significant Bit* (LSB) yaitu, peneliti [12],dalam penelitian dilakukan eksperimen penyisipan pesan teks kedalam wadah citra RGB 24 bit menggunakan metode LSB 2 bit dengan kombinasi algoritma LCG yang secara kasat mata kualitas *stego image* tidak jauh berbeda dengan *cover image* dengan pesan teks asli, penyisipan pesan menggunakan metode LSB 2 bit memberikan kualitas *stego image* yang termasuk tinggi, yaitu diatas 40 dB. Kemudian penelitian dari Ajar Rohman[13], dari hasil penelitian dengan menggunakan algoritma DES dengan steganografi menggunakan metode *End of File* (EOF) dalam perancangan dan pembuatan program aplikasi telah membuktikan bahwa aplikasi dapat mengacak dan menyembunyikan file dengan aman dan tidak menimbulkan kecurigaan pada pihak lain. Hasil yang diperoleh dari menggabung 2 buah *file* yang berbeda ekstensi menghasilkan ukuran yang lebih besar. Selanjutnya penelitian yang dilakukan oleh Bonifacius Vicky Indriyono[14], pada penelitian dilakukan kombinasi teknik keamanan pesan antara metode *Least Significant Bit* (LSB) dalam media gambar *bitmap 24 bit* dengan algoritma Rijndael dengan tujuan sistem keamanan yang lebih terjamin dari pihak-pihak yang tidak bertanggung jawab. Penelitian dilakukan oleh Muhammad Fitra Syawal[15], dalam hal ini peneliti menggunakan algoritma kriptografi Moderen dan klasik. Untuk proses penyisipan pesan kedalam gambar menggunakan metode steganografi *Least Significant Bit*. Pada *cover-image* tidak tidak terjadi perubahan yang begitu mencolok antara perbedaan sebelum dan sesudah pesan disisipkan. Penelitian terakhir yang dilakukan oleh Taronisokhi Zebua[16], pada penelitian ini mengkolaborasikan antara algoritma CBC dengan metode LSB mendapatkan perubahan nilai dari elemen warna setiap *pixel* pada pertukaran *bit-bit* data teks yang disembunyikan dengan metode LSB. Sehingga menyebabkan bertambahnya nilai-nilai *segment* warna menjadi 2 bit jika *bit citra* ditukar dari 0 menjadi 1 dan akan mengurangi 2 *bit* apabila *bit citra* yang ditukar dari 1 menjadi 0.

Adapun yang membedakan penelitian ini dengan penelitian sebelumnya yaitu, algoritma yang digunakan adalah kriptografi klasik *playfair cipher* yang masih menggunakan perhitungan manual dalam enkripsi dan dekripsinya, namun memiliki tingkat keamanan yang cukup baik dengan dikombinasikan metode *Least Significant Bit* (LSB) dalam *embedded* pada *Stego-object citra bitmap*. Kemudian dalam implementasi sistemnya menggunakan aplikasi dengan bantuan *tools Matlab*. Tujuan dari penelitian adalah membuat sistem keamanan sederhana yang mudah di implementasikan namun tingkat keamanannya dapat terjamin dengan baik.

2. Metode Penelitian

Metode yang digunakan untuk pengamanan pesan informasi dengan teknik enkripsi dan dekripsi pesan adalah algoritma *Playfair Cipher* dengan dikombinasikan menggunakan metode *Least Significant Bit* (LSB). Sehingga keamanan pesan yang hendak dikirimkan pada yang berhak menerima akan lebih aman dan terjamin serta tidak mudah untuk dibaca dan dibobol oleh pihak-pihak yang tidak bertanggung jawa.

2.1. Algoritma *Playfair Cipher*

Dalam penelitian Ananda Hariati[17], disebutkan bahwa *Playfair cipher* merupakan suatu diagram *cipher* substitusi yang ditemukan pada tahun 1854 oleh Charles Wheatstone dan telah digunakan oleh bangsa Inggris. Kunci yang digunakan ialah 25 buah huruf yang disusun dalam bentuk bujursangkar 5x5 dengan menghilangkan huruf J dalam suatu kalimat dan bukan menjadi kunci. *Cipher* ini mengenkripsi pasangan huruf (*bigram* atau *digraph*) menjadi pasangan huruf pula, jadi bukan huruf tunggal seperti pada *cipher* klasik lainnya[18].

Tabel 1. Bujursangkar *Playfair Cipher*[18]

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

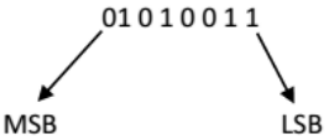
Tabel Bujur sangkar *Playfair Cipher* merupakan tabel yang dibentuk dari hasil kata kunci atau kalimat kunci yang disusun berdasarkan aturan dalam algoritma pengacakan metode *Playfair Cipher* dalam standar internasional.

Huruf-huruf didalam bujursangkar biasanya hasil permutasi huruf-huruf alfabet. Jumlah kemungkinan bujursangkar yang dapat dibuat adalah sebanyak permutasi dari 25 huruf alfabet, yaitu:
25! = 25!=15.511.210.043.330.985.984.000.000.

2.2. Metode *Least Significant Bit* (LSB)

Pada metode LSB, terdapat dua proses utama yakni proses penyisipan atau *embedding* dan proses pelepasan atau *extraction*. [14]. Tahapan dalam proses *embedding message* dimulai dari, memilih citra *image*, menyiapkan pesan informasi atau *ciphertext,* membuat *key file password* dalam tahapan *extract,* menyisipkan *file* kedalam *cover image* dan memetakkan menjadi *citra* baru. Untuk tahapan *extraction message* media peanampung dimulai dari, memilih *file image*, memasukkan *key file* dan menampilkan hasil perolehan pesan.

Didalam sebuah *byte* terdapat susunan bit, ada bit yang paling penting atau biasa disebut dengan *most significant bit* atau MSB dan bit yang kurang penting atau biasa disebut *least significant bit* atau LSB. Sebagaimana penjelasan dalam Gambar.1.



Gambar 1. Pembagian Bit dalam Byte[19]

3. Hasil dan Pembahasan

Pada penelitian ini menerapkan kombinasi keamanan pesan antara teknik kriptografi algoritma *Playfair Cipher* dengan teknik steganografi metode L*east Significant Bit* (LSB). Berikut ini adalah Enkripsi pesan rahasia menggunakan algoritma *playfair cipher,* kemudian hasil dari enkripsi tersebut akan disisipkan kedalam sebuah *citra image* berformat bitmap berukuran 512 x 512 dengan menggunakan metode steganografi *Least Significant Bit* (LSB).

3.2. Enkripsi dan *Encoding* Citra Pesan

Pada penerapan Algoritma *Playfair Cipher* membutuhkan kalimat atau pesan kunci sebagai kunci rahasia dalam mengacak pesan informasi yang hendak dikirimkan atau dienkripsi menggunakan tabel bujur sangkar, agar pesan informasi rahasia tersebut sulit untuk dibaca dan ditebak.

Tahapan pertama yang harus dilakukan dalam enkripsi pesan rahasia menggunakan algoritma *playfair cipher* yaitu, membuat kalimat kunci.

Kalimat Kunci: RAHASIA ORGANISASI

Apabila didalam kalimat kunci yang kita tulis terdapat huruf yang sama atau berulang maka huruf yang berulang atau sama tersebut dihilangkan, secara khusus jika terdapat huruf (J) maka huruf (J) tersebut juga harus dhilangkan karena sudah menjadi standar umum dalam pembentukan tabel bujur sangkar nantinya.

Hasil menghilangkan huruf berulang pada kalimat kunci:

RAHSIOGN

Pada tahapan kedua setelah menghilangkan huruf berulang atau khususnya huruf (J) yaitu, menambahkan huruf-huruf alfabet lainnya yang belum terdapat dalam kalimat kunci kecuali huruf (J), sehingga jumlah keseluruhan huruf yang terdapat dalam kalimat kunci berjumlah 25 huruf alfabet.

Hasil menambahkan huruf alphabet pada kalimat kunci:

RAHSIOGNBCDEFKLMPQTUVWXYZ

Pada tahapan ketiga setelah menambahkan huruf-huruf alfabet yang belum ada pada kalimat kunci kemudian dimasukkan huruf-huruf tersebut kedalam tabel bujur sangkar dengan susunan dari atas kebawah dan dari kiri kekanan, sehingga membentuk bujur sangkar *playfair*.

Tabel 2. Kunci Bujur Sangkar[18]

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

Tabel 2. Kunci Bujur Sangkar merupakan tabel yang didapatkan dari hasil enkirpsi dari kalimat kunci RAHASIA ORGANISASI. Tabel kunci bujur sangkar kemudian digunakan untuk dilakukan subtitusi terhadap pesan rahasia atau *Plaintext sehingga* menghasilkan pesan acak atau *Ciphertext*.

Pada tahapan keempat setelah kalimat kunci sudah disusun kedalam tabel bujur sangkar maka kemudian yang berikutnya, mempersiapkan pesan asli atau *plaintext* untuk kemudian akan diacak menggunakan tabel bujur sangkar yang telah dibuat.

Plaintext atau pesan rahasia:

Kita akan bertemu ditempat biasa untuk transaksi narkoba kita

Sebelum melakukan pengacakan terhadap pesan rahasia menggunakan tabel bujur sangkar maka pesan rahasia tersebut harus disusun dengan teknik yang telah ditetapkan dalam algoritma *playfair cipher* sebagaimana sebelumnya yang telah dilakukan pada kalimat kunci dalam membentuk tabel bujur sangkar:

(1) Ubah huruf *J* (jika ada) dengan huruf I.
(2) Tulis *message* atau *plaintext* dengan pasangan huruf (bigram).
(3) Tidak boleh sampai ada pasangan huruf yang sama, jika ada sisipkan diantaranya atau tengahnya dengan huruf lain.
(4) Jika jumlah huruf ganjil, bisa ditambahkan huruf *X* pada bigram terakhir.

Pada tahap kelima *plaintext* apabila tidak terdapat huruf *J* maka *plaintext* langsung disusun dalam pasangan huruf (bigram):

Plaintext dalam susunan bigram:

Ki ta ak an be rt em ud it em pa tb ia sa un tu kt ra ns ak si na rk ob ak it ax

Dalam menghasilkan pesan rahasia (*ciphertext*) maka hendaknya penyusunan *plaintext* didalam tabel bujur sangkar harus sesuai dengan aturan enkripsi didalam *Playfair Cipher* adalah sebagai berikut:

(1) Jika ada dua huruf terdapat pada baris bujursangkar yang sama maka tiap huruf diganti dengan huruf dikanannya. Substitusi bersifat siklik, jadi jika ada huruf berada paling ujung kanan, maka huruf substitusinya adalah huruf diujung kiri pada baris yang sama.

ia,sa,tu,ra,si,ob

Enam bigram atau pasangan huruf tersebut terdapat pada baris bujur sangkar yang sama maka tiap huruf diganti dengan huruf dikanannya. Sehingga, (ia) menjadi (rh), (sa) menjadi (ih), (tu) menjadi (um), (ra) menjadi (ah), (si) menjadi (ir), (ob) menjadi (gc).

(2) Jika dua huruf terdapat pada kolom bujursangkar yang sama maka tiap huruf diganti dengan huruf dibawahnya. Substitusi bersifat siklik, jadi jika huruf berada paling bawah, maka huruf substitusinya adalah huruf paling atas pada kolom yang sama.

pa,tb,kt

Tiga bigram atau pasangan huruf tersebut terdapat pada kolom bujur sangkar yang sama maka tiap huruf diganti dengan huruf dibawahnya. Sehingga, (pa) menjadi (wg), (tb) menjadi (yk), (kt) menjadi (ty).

(3) Jika dua huruf tidak pada baris yang sama atau kolom yang sama, maka huruf pertama diganti dengan kolom huruf kedua. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari tiga huruf yang digunakan sejauh ini.

Ki,ta,ak,an,be,rt,em,ud,it,em,un,ns,ak,na,rk,ak,it,ax

Delapan belas bigram atau pasangan huruf tersebut tidak pada baris yang sama atau kolom yang sama, maka huruf pertama diganti dengan kolom huruf kedua, huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari tiga huruf yang digunakan sejauh ini. Sehingga, (Ki) menjadi (ls), (ta) menjadi (ps), (ak) menjadi (es), (an) menjadi (gh), (be) menjadi (gk), (rt) menjadi (ms), (em) menjadi (dp), (ud) menjadi (ml), (it) menjadi (su), (em) menjadi (dp), (un) menjadi (qc), (ns) menjadi (bh), (ak) menjadi (es), (na) menjadi (gh), (rk) menjadi (ds), (ak) menjadi (es), (it) menjadi (su), (ax) menjadi (wh).

Ciphertext yang didapatkan dari hasil substitusi dari pasangan huruf (bigram) dengan tabel *key* bujur sangkar adalah:

ls ps es gh gk ms dp ml su dp wg yk rh ih qc um ty ah bh es ir gh ds gc eh su wh

Setelah *ciphertext* yang didapatkan dari hasil permutasi didalam tabel bujur sangkar, selanjutnya *ciphertext* yang dihasilkan disisipkan kedalam citra *bitmap* dengan metode *Least Significant Bit* (LSB) menggunakan bantuan *software* Matlab.

Encoding atau penyisipan *file* pada media penyimpanan (*Stego Cover*) menggunakan metode *Least Significant Bit* (LSB). Metode LSB merupakan metode yang cukup sederhana dalam penerapannya namun sulit dibedakan hasil dari implementasinya, dikarenakan metode LSB hanya merubah bit akhir dari suatu *pixel citra* sehingga perubahan yang terjadi pada *citra image* hanya mengubah nilai bit satu lebih tinggi atau satu lebih rendah dari sebelumnya.

Adapun hasil pesan yang telah dienkripsi menggunakan Algoritma *Playfair Cipher* yang akan disisipkan kedalam media penyisipan atau *Stego Cover* adalah:

lspsesghgkmsdpmlsudpwgykrhihqcumtyahbhesirghdsgcehsuwh

Selanjutnya dikonversikan dalam bentuk bilangan biner dengan menggunakan bantuan tabel kode ASCII. Lihat table 3.

Tabel 3. Konversi Pesan Enkripsi Ke Kode ASCII[20]

Indeks ke-i	Ciphertext (C)	Kode ASCII
C1	l	108
C2	s	115
C3	p	112
C4	s	115

Indeks ke-i	Ciphertext (C)	Kode ASCII
C5	e	101
C6	s	115
C7	g	103
C8	h	104
C9	g	103
C10	k	107
C11	m	109
C12	s	115
C13	d	100
C14	p	112
C15	m	109
C16	l	108
C17	s	115
C18	u	117
C19	d	100
C20	p	112
C21	w	119
C22	g	103
C23	y	121
C24	k	107
C25	r	114
C26	h	104
C27	i	105
C28	h	104
C29	q	113
C30	c	99
C31	u	117
C32	m	109
C33	t	116
C34	y	121
C35	a	97
C36	h	104
C37	b	98
C38	h	104
C39	e	101
C40	s	115
C41	i	105
C42	r	114
C43	g	103
C44	h	104
C45	d	100
C46	s	115
C47	g	103
C48	c	99
C49	e	101
C50	h	104
C51	s	115
C52	u	117
C53	w	119
C54	h	104

Tabel 3. Konversi Pesan Enkripsi Ke Kode ASCII merupakan tabel yang digunakan untuk melakukan perubahan atau konversi dari hasil pesan rahasia algoritma P*layfair Cipher* dalam bentuk *Cipherext* atau pesan yang sudah melalui pengacakan kedalam bentuk kode ASCII yang kemudian membantu dalam penyisipan pesan rahasia kedalam *Cover Image* atau media penampung menggunakan metode *Least Significant Bit* (LSB). Setelah konversi karakter pesan rahasia telah didapatkan maka selanjutnya merubah bilangan kode ASCII ke kode Hexa Biner.

Tabel 4. Konversi Kode ASCII Ke Kode Biner[20]

Karakter	Kode ASCII	Kode Biner
l	108	01101100
s	115	01110011

Karakter	Kode ASCII	Kode Biner
p	112	01110000
s	115	01110011
e	101	01100101
s	115	01110011
g	103	01100111
h	104	01101000
g	103	01100111
k	107	01101011
m	109	01101101
s	115	01110011
d	100	01100100
p	112	01110000
m	109	01101101
l	108	01101100
s	115	01110011
u	117	01110101
d	100	01100100
p	112	01110000
w	119	01110111
g	103	01100111
y	121	01111001
k	107	01101011
r	114	01110010
h	104	01101000
i	105	01101001
h	104	01101000
q	113	01110001
c	99	01100011
u	117	01110101
m	109	01101101
t	116	01110100
y	121	01111001
a	97	01100001
h	104	01101000
b	98	01100010
h	104	01101000
e	101	01100101
s	115	01110011
i	105	01101001
r	114	01110010
g	103	01100111
h	104	01101000
d	100	01100100
s	115	01110011
g	103	01100111
c	99	01100011
e	101	01100101
h	104	01101000
s	115	01110011
u	117	01110101
w	119	01110111

Tabel 4. Konversi Kode ASCII Ke Kode Biner, merupakan tabel yang digunakan untuk melakukan perubahan atau konversi dari hasil kode ASCII,dalam bentuk karakter atau angka ke bentuk kode biner yang kemudian dilakukan perubahan bit LSB *Cover Image* atau media penampung menjadi *stego image* atau media penampung yang sudah disisipkan pesan rahasia (*Embedded Image*) menggunakan metode *Least Significant Bit* (LSB).

Bilangan biner yang didapatkan dari hasil konversi dari karakter pesan enkripsi atau *ciphertext* kemudian dimasukkan kedalam citra bitmap 512x 512 sehingga perubahan yang terjadi pada citra bitmap tidak terlalu signifikan karena dalam metode LSB yang dirubah

hanya bit akhir dari gambar sehingga sulit dibedakan antara sebelum dan seseudah penyisipan pesan rahasisa.

Misalkan disisipkan kata "ls" sudah dienkripsi menggunakan algoritma *Playfair Cipher*, maka langkah selanjutnya yang harus dilakukan adalah sebagai berikut.

Tiap karakter diambil kode ASCII:

l = 108

s = 115

Mengkonversi kode ASCII kedalam biner:

l = 108 = 01101100

s= 115 = 01110011

Selanjutnya pengambilan nilai untuk penyisipan pesan dari *pixel* 512 x 512 yang diwakili oleh *pixel* 6 x 6.

Pxl1	Pxl2	Pxl3	Pxl4	Pxl5	Pxl6
Pxl7	Pxl8	Pxl9	Pxl10	Pxl11	Pxl12
Pxl13	Pxl14	Pxl15	Pxl16	Pxl17	Pxl18
Pxl19	Pxl20	Pxl21	Pxl22	Pxl23	Pxl24
Pxl25	Pxl26	Pxl27	Pxl28	Pxl29	Pxl30
Pxl31	Pxl32	Pxl33	Pxl34	Pxl35	Pxl36

Gambar 2. *Pixel* image *Bitmap*[11]

Nilai yang didapatkan dari masing-masing *pixel* adalah:

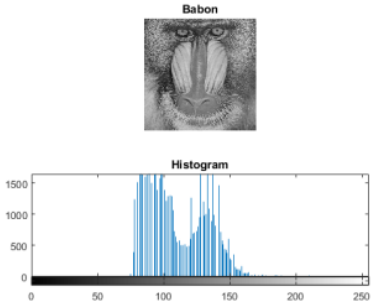
P1 : 160 = 10100000
P2 : 185 = 10111001
P3 : 130 = 10000010
P4 : 125 = 11111101
P5 : 250 = 11111010
P6 : 205 = 11001101
P7 : 108 = 11011100
P8 : 215 = 11010111
P9 : 220 = 11011100
P10 : 135 = 10000111
P11 : 168 = 10101000
P12 : 145 = 10010001
P13 : 230 = 11100110
P14 : 255 = 11111111
P15 : 203 = 11001011
P16 : 142 = 10001110

Setelah pesan rahasia dikonversi ke biner maka selanjutnya pesan rahasia tersebut disisipkan kedalam biner *pixel* pada bit akhir atau *least siginificant bit citra bitmap*.

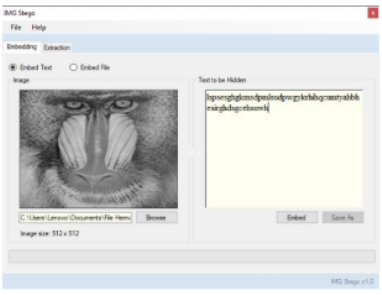
P1 : 1010000**0** diganti 0 = 1010000**0** = 160
P2 : 1011100**1** diganti 1 = 1011100**1** = 185
P3 : 1000001**0** diganti 1 = 1000001**1** = 131
P4 : 1111110**1** diganti 0 = 1111110**0** = 124
P5 : 1111101**0** diganti 1 = 1111101**1** = 251
P6 : 1100110**1** diganti 1 = 1100110**1** = 205
P7 : 1101110**0** diganti 0 = 1101110**0** = 108
P8 : 1101011**1** diganti 0 = 1101011**0** = 214
P9 : 1101110**0** diganti 0 = 1101110**0** = 220
P10 : 1000011**1** diganti 1 = 1000011**1** = 135
P11 : 1010100**0** diganti 1 = 1010100**1** = 169
P12 : 1001000**1** diganti 1 = 1001000**1** = 145
P13 : 1110011**0** diganti 0 = 1110011**0** = 230
P14 : 1111111**1** diganti 0 = 1111111**0** = 254
P15 : 1100101**1** diganti 1 = 1100101**1** = 203
P16 : 1000111**0** diganti 1 = 1000111**1** = 143

3.3. Hasil Penyisipan Pesan (*Stego Image*) dan Uji Kualitas Citra

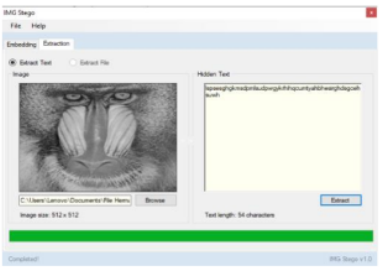
Pada hasil *embedded* atau penyisipan pesan rahasia (*Ciphertext*) dilakukan dengan bantuan *software Matlab* dalam uji cobanya, sebagaimana yang terlihat pada Gambar 3.



Gambar 3. Hasil Penyisipan *Ciphertext* pada *Citra*[21]



Gambar 4. Proses Penyisipan Pesan Rahasia (*Ciphertext)*



Gambar 5. Proses Ekstraksi Pesan Rahasia (*Ciphertext)*

Kemudian untuk mengetahui kualitas *citra image* hasil dari *encoding* menggunakan metode LSB dilakukan perhitungan nilai *Mean Square Error* (MSE) dan *Peak Signal to Noise Ratio* (PSNR). MSE merupakan hasil kesalahan rata-rata kuadrat dari citra asli dengan citra

hasil. MSE dikatakan baik jika mempunyai nilai yang rendah.

Rumus untuk menghitung MSE adalah:

$$MSE = \frac{1}{MN}\sum_{x}^{M} = 1 \sum_{y}^{N} = 1|f(x,y) - g\ (x,y))^2| \quad (1)$$

Dimana:

MSE = Nilai Mean Square Error dari citra
(x,y) = Kordinat masing-masing pixel
N = Lebar citra dalam *pixel*
M = Panjang citra dalam *pixel*

Rumus persamaan MSE digunakan untuk menghitung atau mengetahui nilai sebuah kesalahan yang dapat terjadi dengan perbandingan selisih nilai *pixel* pada *citra* sebelum dan sesudah disisipkan pesan rahasia, dengan standar posisi *pixel* yang sama. Oleh karena itu dengan menggunakan persamaan MSE dapat diketahui presentase kesalahan kualitas *pixel* pada citra, yang disebabkan proses penyisipan pesan kedalam *cover image*. Sehingga dapat disimpulkan sebuah *stego image* tersebut berkualitas dengan baik atau tidak.

PSNR diukur dalam satuan decibel (dB). Untuk melakukan perhitungan nilai PSNR, terlebih dahulu harus dicari nilai MSEnya. Kualitas citra dikatakan baik jika nilai PSNR semakin besar.

Rumus untuk menghitung PSNR adalah:

$$PSNR = 2_{Log\frac{MAX}{\sqrt{MSE}}} \quad (2)$$

Dimana:

PSNR = Nilai PSNR citra (dalam dB)
MSE = Nilai MSE
MAX = Nilai Maximum *pixel*

Rumus persamaan PSNR digunakan untuk menghitung atau mengetahui perbandingan nilai *Pixel* pada *Citra Image* sebelum dan sesudah pesan rahasia atau *Ciphertext* disisipkan dengan menggunakan satuan decibel (dB). Sehingga hasil dari penggunaan persamaan PSNR dapat digunakan dalam membedakan kualitas *citra* untuk menilai tingkat keberhasilan penyisipan pesan rahasia kedalam wadah media digital atau *Stego Image*.

Tabel 5. Hasil Perhitungan Kualitas Citra (PSNR)[22]

Citra (Pixel)	Cover Image	Stego Image	Pesan Encoding	Pesan Decoding	PSNR (dB)
512 x 512	233 KB	352 KB	53Byte	53Byte	83.54

Tabel 5 Hasil Perhitungan Kualitas citra menunjukkan bahwa perbandingan nilai kualitas citra pada sebelum pesan rahasia disisipkan dan ketika kualitas citra telah disisipkan tidak mengalami perubahan yang siginifikan dilihat dari nilai PSNR dengan presentase sebesar 83.54 dB, yang masuk dalam kategori baik yaitu diatas 40 dB. Sehingga citra image yang terlihat setelah penyisipan rahasia tidak mengalami distorsi atau sulit dibedakan antara sesudah dan sebelum penyisipan pesan rahasia

3.4. Analisis Hasil Ekstraksi (Decoding) dan Dekripsi Pesan (Stego Image)

Adapun dalam proses Dekripsi algoritma Playfair cipher adalah dengan membalikkan proses dari Enkripsi Langkah-langkahnya adalah sebagai berikut:

(1) Jika ada dua huruf pada baris bujursangkar yang sama maka tiap huruf diganti dengan huruf kirinya.
(2) Jika dua huruf terdapat pada kolom bujur sangkar yang sama maka tiap huruf diganti dengan huruf diatasnya.
(3) Jika ada dua huruf tidak pada baris yang sama atau kolom yang sama, maka huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari tiga huruf yang digunakan sampai sejauh ini.
(4) Membuang huruf X yang tidak mengandung makna.

Adapun ekstraksi pada LSB dilakukan dengan cara bit-bit terakhir yang ada pada stego image atau media penampung yang sudah disisipi dengan pesan rahasia dikonversi kebiner dan mengambil bit paling terakhir.

P1 : 10100000 = 0
P2 : 10111001 = 1
P3 : 10000011 = 1
P4 : 11111110 = 0
P5 : 11111011 = 1
P6 : 11001101 = 1
P7 : 11011100 = 0
P8 : 11010110 = 0
P9 : 11011100 = 0
P10 : 10000111 = 1
P11 : 10101001 = 1
P12 : 10010001 = 1
P13 : 11100110 = 0
P14 : 11111110 = 0
P15 : 11001011 = 1
P16 : 10001111 = 1

Dari perhitungan diatas maka didapatkan bit terakhir yaitu, “01101101 01010111”. Setelah bit akhir pada pixel sudah didapatkan maka kemudian dikonversi kedalam nilai ASCII dan dilanjutkan dengan diubah dalam bentuk karakter.

01101100 = 108 = l 01110011 = 115 = s

4. Kesimpulan

Algoritma *Playfair Cipher* memiliki kelebihan dalam pengamanan pesan rahasia walaupun tergolong teknik kriptografi klasik yang sederhana namun sulit untuk ditebak, proses alurnya dengan cara pesan dienkripsi melalui *table key* bujur sangkar yang kemudian dilakukan substitusi secara berpola, sehingga orang akan sulit dalam mengetahui pesan asli yang sudah dienkripsi dengan teknik bigram atau pasangan huruf pada *table* kunci rahasia. Begitupun dengan Metode *Least*

Siginificant Bit (LSB) dalam penyisipan pesan rahasia mempunyai kelebiihan tersendiri dalam hal perubahan bit akhir atau LSB yang tidak terjadi perubahan yang siginifikan dikarenakan perubahan bit yang diubah pada *pixel* gambar adalah bit yang tidak memilliki nilai ketergantungan kualitas *pixel* pada gambar.Sehingga dengan menggunakan metode LSB sangat memungkinkan pesan yang disisipkan kedalam *citra image* sulit dibedakan antara kualitas gambar sebelum dan sesudah disisipkan pesan rahasia.

Dalam penelitian ini diperoleh bahwa algoritma *playfair cipher* cukup aman dalan implementasi enkripsi pesan rahasia atau *ciphertext* dikarenakan *playfair cipher* membuat analisis frekuensi menjadi sangat sulit, sebab frekuensi kemunculan huruf-huruf didalam *ciphertext* menjadi data (*flat*). Untuk metode steganografi *Least Significant Bit* (LSB) dalam penyisipan pesan rahasia atau *embedded* sulit ditebak secara kasat mata melihat perubahan yang terjadi antara sebelum dan sesudah gambar disisipkan tidak terlalu signifikan. Juga melihat nilai hasil *Peak-Signal-to-Noise ratio* atau PSNR masih dapat dianggap berkualitas bagus dikarenakan >30 desibel (dB). Sehingga hasil akhir dari kombinasi algoritma *Playfair Cipher* dengan metode *Least Significant Bit* (LSB) cukup baik dalam pengamanan pesan. Namun meskipun *Playfair Cipher* sulit dipecahkan dengan analisis frekuensi relatif huruf-huruf, namun ia masih dapat dipecahkan dengan analisis frekuensi pasangan huruf, sehingga dalam pengembangan kedepannya dapat menggunakan algoritma kriptografi moderen seperti, AES. DES, TripleDES, RSA dan yang semisalnya. Begitupun dengan metode steganografi LSB yang memiliki kelemahan jika *citra-stego* atau media penampung dimanipulasi misalnya *resize,* kompresi, mengubah kontras gambar, dan sebagainya, maka bit-bit LSB dari *Citra-stego* akan rusak sehingga pesan tidak dapat diekstraksi seperti semula. Oleh karena itu pengembangan sistem kedepannya dapat mencoba metode steganografi lainnya seperti, BPCS atau *End of File* (EoF). Kemudian media penampung tidak harus *citra* dapat juga menggunakan, *text, audio* ataupun *Video*.

Daftar Rujukan

[1] Yudhana, A., Hermansa, Umar, R., 2020. Pangamanan Pesan Menggunakan Kriptografi Caesar Cipher dan Steganografi EOF pada Citra. *J. Sains Komput. Inform.*, vol. 4, pp. 157–169.

[2] Yudhana, A., Riadi, I and Ridho, F., 2018. DDoS classification using neural network and naïve bayes methods for network forensics. *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 11, pp. 177–183.

[3] Umar, R., Yudhana, A., and Faiz, M.N., 2018. Experimental analysis of web browser sessions using live forensics method. *Int. J. Electr. Comput. Eng.*, vol. 8, no. 5, pp. 2951–2958.

[4] Umar, R., Yudhana, A., Bintang, R.A.K.N., 2018. Perancangan perbandingan live forensics pada keamanan media sosial Instagram, Facebook dan Twitter di Windows 10. *Pros. SNST ke-9 Tahun 2018 Fak. Tek. Univ. Wahid Hasyim*, pp. 125–128.

[5] Wahyu, Y., Yudhana, A., Riadi, I., 2018. Analisis Deteksi Vulnerability Pada Webserver Open Jurnal System Menggunakan OWASP Scanner. p. 8.

[6] Riadi, I., Umar, R., and Nasrulloh, I.M., 2018. Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (Nij). vol. 3, no. 1, pp. 70–82.

[7] Umar, R., Yudhana, A., and Nur Faiz, M., 2016. Analisis Kinerja Metode Live Forensics Untuk Investigasi Random Access Memory Pada Sistem Proprietary. *Pros. Konf. Nas. Ke-4 Asos. Progr. Pascasarj. Perguru. Tinggi Muhammadiyah*, pp. 207–211.

[8] Syahib, M.I., Riadi, I and Umar, R., 2018. Analisis Forensik Digital Aplikasi Beetalk Untuk Penanganan. *Semin. Nas. Inform. 2018 (semnasIF 2018) UPN "Veteran" Yogyakarta, 24 Novemb. 2018*, vol. 2018, no. November, p. 134.

[9] Zuhriyanto, I., *et al*., 2018. Perancangan Digital Forensik Pada Aplikasi. vol. 2018, no. November, pp. 86–91.

[10] Yudhana, A., Riadi, I., and Anshori, I., 2018. Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist. *It J. Res. Dev.*, vol. 3, no. 1, p. 13.

[11] Arif, M.H., and Fanani, A.Z., 2016. Kriptografi Hill Cipher Dan Least Significant Bit Untuk Keamanan Pesan Pada Citra. *CSRID (Computer Sci. Res. Its Dev. Journal)*, vol. 8, no. 1, p. 60.

[12] Djuwitaningrum, E. R., and Apriyani, M., 2016. Teknik Steganografi Pesan Teks Menggunakan Metode Least Significant Bit Dan Algoritma Linear Congruential Generator. *Ta*, vol. IV, no. 2, pp. 79–85.

[13] Rohmanu, A., 2017. Implementasi Kriptografi dan Steganografi Dengan Metode Algoritma Des dan Metode End Of File Ajar Rohmanu. *J. Inform. SIMANTIK*, vol. 1, no. 2, pp. 1–11.

[14] Indriyono, B.V., 2016. Penerapan Keamanan Penyampaian Informasi Melalui Citra dengan Kriptografi Rijndael dan Steganografi LSB. *Creat. Inf. Technol. J.*, vol. 3, no. 3, p. 228.

[15] Syawal, M.F., Fikriansyah, D.C., and Agani, N., 2016. Implementasi Teknik Steganografi Menggunakan Algoritma Vigenere Cipher Dan Metode LSB. *J. TICOM*, vol. 4, no. 3, pp. 91–99.

[16] Zebua, T., 2015. Pengamanan Data Teks Dengan Kombinasi Cipher Block Chaining dan LSB-1. in *Seminar Nasional Inovasi dan Teknologi (SNITI)*.Tuktuk Siadong, Indonesia5-6 September 2015.

[17] Hariati, A., Hardiyanti, K., and Putri, W.E., 2018.Kombinasi Algoritma Playfair Cipher Dengan Metode Zig-zag Dalam Penyandian Teks. *Sinkron*, vol. 2, no. 2, pp. 13–17.

[18] Azmi, F., and Anugrahwaty, R., 2017. Analisis Matriks 5x7 Pada Kriptografi Playfair Cipher. *J. Penelit. Tek. Inform.*, vol. 1, no. 2, pp. 27–30.

[19] Gunawan, I., 2018. Penggunaan Algoritma Kriptografi Steganografi Least Significant Bit Untuk Pengamanan Pesan Teks dan Data Video. *J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 2, no. 1, p. 57.

[20] Insanudin, E., 2016. Aplikasi Enkripsi dan Dekripsi Menggunakan Algoritma Vigenere Cipher ASCII Berbasis Java.Universitas Islam Ngeri Sunan Gunung Djati Bandung.

[21] Setiadi, D.R.I.M., Handoyo, A. E., Rachmawanto, E. H., Sari, C. A., and Susanto, A., 2018. Teknik Penyembunyian dan Enkripsi Pesan pada Citra Digital dengan Kombinasi Metode LSB dan RSA. *J. Teknol. dan Sist. Komput.*, vol. 6, no. 1, p. 37.

[22] Djuwitaningrum, E. R., and Apriyani, M., 2016.Teknik Steganografi Pesan Teks Menggunakan Metode Least Significant Bit dan Algoritma Linear Congruential Generator (Text Message Steganography Using Least Significant Bit Method and Linear Congruential Generator Algorithm). vol. IV, no. November, pp. 79–85.

HASIL_CEK8_60010383

ORIGINALITY REPORT

5%	5%	2%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	alihamidi.wordpress.com Internet Source	3%
2	doku.pub Internet Source	2%

Exclude quotes	On	Exclude matches	< 2%
Exclude bibliography	On		