ISSN: 2407 - 3911

IMPLEMENTASI STEGANOGRAFI PADA CITRA DIGITAL DAN KRIPTOGRAFI ALGORITMA HILL CHIPPER UNTUK PENGAMANAN INFORMASI BERUPA TEXT

Aldo[1], Lukman Hakim[2]
Technology and Design Department[1], Informatics Engineering[2]
Universitas Bunda Mulia
Jalan Lodan Raya No. 2, Ancol, Jakarta Utara
aldodoal19@gmail.com[1], lhakim@bundamulia.ac.id[2]

Abstrak

Pertukaran informasi sangatlah mudah dengan mengunakan internet sebagai penghubung dari pihak yang mengirim informasi ke pihak yang menerima informasi tersebut. Semakin mudah juga bagi pihak yang tidak berwenang untuk mendapatkan informasi yang akan dikirimkan dari pihak pengirim ke pihak penerima melalui internet. Maka itu informasi tersebut memerlukan fitur keamanan. Penyandian merupakan sebuah teknik keamanan untuk mengubah sebuah informasi berupa text, citra digital, suara, video menjadi sebuah informasi yang tidak memiliki arti tertentu atau teracak. Jika pihak yang memiliki informasi yang telah di sandikan ini tidak memiliki kunci untuk membuka enkripsi tersebut maka informasi tersebut tidak dapat dibaca dikarenakan tidak memiliki makna tertentu. Penyisipan merupakan sebuah fitur keamanan dimana sebuah informasi akan dimasukan kedalam sebuah media penampung atau informasi tersebut disembunyikan didalam media penampung. Pada penulisan ini akan difokuskan untuk membuat sebuah sistem yang dapat menyandikan , mendekripsi sandi , menyisipkan sebuah informasi ke dalam sebuah media penampung dan mengekstraksi informasi dari media tampung yang dapat berupa citra digital dengan format : jpeg, bitmap, dan png yang berguna untuk meningkatkan tingkat keamanan dari sebuah informasi.Algoritma penyandian merupakan algoritma yang mengubah sebuah informasi (*plain text*) menjadi sebuah informasi yang telah teracak (*ciphertext*) mengunakan kunci yang telah ditentukan dari pihak pengirim dan penerima. Algoritma penyandian yang digunakan adalah algoritma *Hill Cipher*. Yang akan dikombinasikan dengan metode *Least Significant Bit* sebagai metode pada proses penyisipan informasi. *LSB* akan mengubah setiap nilai bit terakhir dari setiap piksel pada citra tampung (*cover*) sesuai dengan nilai biner pesan secara berurutan, sehingga menyebabkan hasil akhir dari penyisipan (*stego image)* tidak akan mengalami perubahan secara signifikan jika dilihat oleh mata manusia.

Kata kunci:

Keamanan, Penyandian, Penyisipan, Hill Cipher, *Least Significant Bit*

Abstract

The exchange of information is very easy by using the internet as a liaison from the party who sends information to the party receiving the information. It is also easier for unauthorized parties to obtain information that will be sent from the sending party to the recipient via the internet. So that information requires security features. Encoding is a security technique to change information in the form of text, digital images, audio, video into information that has no meaning or is random. If the party who has the information that has been encoded does not have the key to open the encryption then the information cannot be read because it does not have a specific meaning. Insertion is a security feature wherein an information will be entered into a container media or the information is hidden in the container media.
At this writing will be focused on creating a system that can encode, decrypt passwords, insert an information into a container media and extract information from a media that can be a digital image with the format: jpeg, bitmap, and png which is useful for increasing the level of security from an information. Encryption algorithm is an algorithm that converts an information (plain text) into a randomized

information (ciphertext) uses the specified key from the sender and recipient. The encoding algorithm used is the Hill Cipher algorithm. Which will be combined with the Least Significant Bit method as a method in the information insertion process. LSB will change every last bit value of each pixel in the cover image according to the binary value of the message in sequence, so that the result of the stego image will not change significantly if seen by the human eye.

Keywords:

Security, Encryption, Insertion, Hill Cipher, Least Significant Bit

I. PENDAHULUAN

Pertukaran informasi sangatlah mudah dengan mengunakan internet sebagai penghubung dari pihak yang mengirim informasi ke pihak yang menerima informasi tersebut dalam hitungan detik. Informasi tersebut bisa berisikan media text, foto (citra digital), audio maupun video.kemudahan pengiriman informasi tersebut mengunakan internet dapat dimanfaatkan oleh pihak yang tidak berwenang seperti *hacker*, *cracker*, dan *carder* untuk mengambil informasi yang dikirimkan dari pengirim ke penerima. Setelah pihak yang tidak berwenang tersebut mendapatkan file tersebut, dengan mudah dapat dibuka,dibaca, diambil, dan dimanipulasi informasi yang berada didalam file tersebut. Oleh karena itu diperlukan pengamanan terhadap informasi yang akan dikirimkan dari pihak pengirim harus mengalami peningkatan untuk melindungi informasi yang akan dikirimkan melalui jaringan internet.

Peran keamanan informasi dalam proses pertukaran informasi sangat berperan penting agar informasi yang akan dikirimkan bersifat rahasia, hanya diketahui oleh pihak pengirim dan pihak penerima. Agar pihak lain yang tidak bertanggung jawab tidak mencuri dan merubah data atau informasi yang akan dikirimkan ke pihak penerima. Akibat adanya masalah tersebut diperlukanlah sebuah algoritma yang dapat memberikan keamanan lebih terhadap sebuah informasi tersebut, algoritma penyandian merupakan salah satu algoritma yang dapat memberikan keamanan lebih terhadap file tersebut. Algoritma penyandian berfungsi untuk membuat pesan yang akan dikirimkan menjadi pesan yang acak sehingga jika pesan yang dikirimkan jatuh pada tangan yang salah pun pesan tersebut tidak dapat dibaca atau tidak berguna. Salah satu algoritma penyandian merupakan algoritma *Hill Cipher*.

Algoritma *Hill Cipher* merupakan algoritma kriptografi simetris yang bersifat *polyalphabetic* yang sering dikategorikan dengan *block cipher*, dikarenakan teks yang akan disandi akan dibagi menjadi beberapa blok dengan ukuran tertentu. Setiap karakter dalam suatu blok dapat pengaharui karakter lainnya dalam proses enkripsi dan dekripsi, sehingga karakter yang sama ketika di enkripsi akan menghasilkan karakter yang pasti berbeda dari karakter awalnya. *Hill Cipher* menggunakan teknik perkalian matriks dan teknik invers terhadap matriks. Kunci pada *Hill Cipher* adalah matriks n x n dengan n merupakan ukuran blok (Hasungian, 2013). Algoritma ini juga memiliki kelemahan yang dapat dipecahkan oleh kriptanalis, jika kriptanalis memiliki bagian dari plain text dan potongan cipher text yang berkorespondensi. Teknik kriptanalis ini sering disebut dengan *known-plain attack*. Untuk melengkapi kekurangan dari algoritma *Hill Cipher* diperlukanlah sebuah metode yang berfungsi untuk dapat menyisipkan sebuah informasi kedalam sebuah media penampung. Metode tersebut merupakan metode Steganografi yang bernama *Least Significant Bit.*

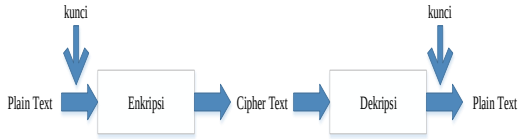
Steganografi merupakan seni untuk menyembunyikan pesan di dalam media digital sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu pesan didalam media tersebut (Sari, Sulindawaty, & Sihotang , 2017). Steganografi telah diterapkan dari zaman Yunani kuno dengan membuat tato yang berisi pesan rahasia yang disembunyikan dikepala pengirim pesan yang dibotaki dan menunggu rambut dari pengirim pesan tersebut tumbuh baru pengirim pesan tersebut berjalan ke tujuannya. Tujuan dari mengunakan Steganografi adalah untuk membantu melengkapi sistem keamaanan untuk mengirimkan sebuah infromasi dengan cara menyembunyikan pesan tersebut kedalam sebuah foto. Metode *Most Significant Bit* dan Metode *Least Significant Bit* merupakan 2 contoh metode steganografi. Pada jurnal ini penulis akan melakukan pengambungan antara algoritma *Hill Cipher* dan metode Steganografi *Least Significant Bit* untuk membuat sebuah applikasi yang dapat meningkatkan tingkat keamanan pada file berupa text.

II. LANDASAN TEORI

II.1 Kriptografi

Kriptografi (*cryptography*) berasal dari Bahasa Yunani: ”*cryptos*” artinya ”*secret*” (rahasia), sedangkan ”*graphein*” artinya ”*writing*” (tulisan),

Jadi, kriptografi berarti ”*secret writing*” (tulisan rahasia). Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. (Hasungian, 2013)



Gambar 1. Proses Enkripsi Dan Dekripsi

Algoritma Kriptografi memiliki tiga fungsi dasar yaitu: (Ariyus, 2008)

a. Enkripsi merupakan hal yang sangat penting dalam kriptografi, merupakan pengamanan data yang dikirimkan agar terjaga kerahasiaannya. Pesan asli disebut plaintext, yang diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan dengan cipher atau kode. Sama halnya dengan kita tidak mengerti akan sebuah kata maka kita akan melihatnya didalam kamus atau daftar istilah. Beda halnya dengan enkripsi, untuk mengubah teks-asli kebentuk teks-kode kita mengunakan algoritma yang dapat mengkodekan data yang kita ingini.
b. Dekripsi merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asal (teks-asli), disebut dengan dekripsi pesan. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan algoritma yang digunakan untuk enkripsi.
c. Kunci yang dimaksud di sini adalah kunci yang dipakai untuk melakukan enkripsidan dekripsi. Kunci terbagi menjadi dua bagian, kunci rahasia (*private key*) dank unci umum (*public key*)

II.2 Algoritma *Hill Cipher*

Algoritma Hill Cipher diciptakan pada tahun 1929 oleh Lester S. Hill digolongkan sebagai kriptografi *polyalphabetic*, yang berarti setiap karakter alfabet bisa dipetakan ke lebih dari satu macam karakter (Ariyus, 2008). Algoritma ini juga dikategorikan sebagain block cipher, karena setiap karakter pada satu blok akan mempengaharui hasil karakter lainnya dalam proses enkripsi dan proses dekripsi

Proses enkripsi pada *Hill Cipher* dilakukan per blok *plaintext*. Ukuran blok tersebut sama dengan ukuran matriks kunci. Sebelum membagi teks menjadi deretan blok-blok, *plaintext* terlebih dahulu dikonversi menjadi angka, masing-masing sehingga A=0, B=1, hingga Z=25 seperti pada Gambar 2. Secara matematis, proses enkripsi pada *Hill Cipher* adalah: (Hasungian, 2013)

$$C = (P\,.K) mod\ 26 \qquad \ldots[1]$$

C = Cipher text
P = Plain text
K = Kunci (Key)

Proses dekripsi pada *Hill Cipher* pada dasarnya sama dengan proses enkripsinya. Namun matriks kunci harus dibalik (*invers*) terlebih dahulu. Secara matematis, proses dekripsi pada *Hill Cipher* dapat diturunkan dari persamaan . seperti pada Gambar 3.

Rumus matematika dari dekripsi algoritma *Hill Cipher* adalah:

$$P = (K^{-1}\,.\,C)\ mod\ 26 \qquad \ldots[2]$$

Dimana untuk menentukan K^{-1} dengan mengunakan rumus modular invers :

$$\frac{1}{K}\ mod\ 26 = X\ atau\ (\det K * X\ mod\ 26) = 1 \quad \ldots[3]$$

II.3 Citra Digital

Secara harafiah, citra (image) adalah gambar pada bidang dua dimensi (dwimatra). Ditinjau dari sudut pandang matematis, citra merupakan fungsi menerus (continue) dari intensitas cahaya pada bidang dwimatra. Sumber cahaya menerangi objek, objek memantulkan kembali sebagian dari berkas cahaya tersebut.Pantulan cahaya ini ditangkap oleh alat-alat optik, misalnya mata pada manusia, kamer. Pemindai (scanner), dan sebagainya, sehingga bayangan objek yang disebut citra tersebut terekam.

Citra digital merupakan citra yang dapat diolah oleh komputer yang terdiri atas kumpulan dari pixel. Didalam setiap pixel yang ada dicitra digital terdapat kumpulan ‘0’ dan ‘1’. Berikut merupakan beberapa format citra digital, antara lain : jpeg,gif,png,bmp.

Pada penulisan ini format citra digital yang dipakai sebagai cover image dan stego image adalah : jpeg,bmp,dan png.

PNG (*Portable Network Graphics*) adalah salah satu format penyimpanan citra yang menggunakan metode pemadatan yang tidak menghilangkan bagian

dari citra tersebut (Inggris *lossless compression*). Untuk keperluan pengolahan citra, meskipun format PNG bisa dijadikan alternatif selama proses pengolahan citra, karena format ini selain tidak menghilangkan bagian dari citra yang sedang diolah (sehingga penyimpanan berulang ulang dari citra tidak akan menurunkan kualitas citra) PNG (Format berkas grafik yang didukung oleh beberapa web browser. PNG mendukung transparansi gambar seperti GIF, berkas PNG bebas paten dan merupakan gambar bitmap yang terkompresi.

Gambaran dari citra digital dapat dimisalkan seperti melukis, dimana kita harus meliliki palet warna dan kanvas sebagai media penampung untuk warna yang akan di taruh. Dimana palet merupakan kumpulan dari warna yang akan menghasilkan sebuah citra dan setiap palet warna tersebut diberi nomor. Lalu warna dari palet tersebut akan dilukiskan ke sebuah kanvas. Kanvas dimisalkan berupa matriks yang setiap elemen dari matriks tersebut dapat diisi dengan setiap warna yang ada pada palet warna. Kumpulan angka (mewakili warna) dalam bentuk matriks inilah yang disebut dengan citra (Anwar, 2017). Sementara kumpulan informasi mengenai setiap warna yang berada dipalet warna disimpan didalam komputer melalui aplikasi untuk membuka citra seperti photosop dan paint.

II.4 Steganografi

Steganografi berasal dari bahasa yunani yang terbentuk dari kata *steganos* dan *graphia*. Steganos memiliki arti tersembunyi dan graphia memiliki arti tulisan, maka dapat disimpulkan bahwa steganografi merupakan ilmu atau seni untuk menyembunyikan pesan (Anwar, 2017). Tujuan mengapa sebuah pesan dimasukan ke dalam sebuah media penampung adalah agar pesan tersebut tidak dapat dibaca atau diketahui oleh pihak lain selain pihak yang menulis pesan tersebut dan pihak yang menerima pesan tersebut. Metode steganografi akan membahas bagaimana cara menyembunyikan sebuah pesan kedalam sebuah media penampung.

Perkembangan metode steganografi pada saat ini dapat digunakan dalam berbagai hal. Contohnya adalah pengunaan watermarking pada dokumen-dokumen penting.

Beberapa faktor yang harus diperhatikan dalam steganigrafi (Anwar, 2017), yaitu:

1. *Imperceptibility*. Keberadaan pesan rahasia tidak dapat dipersepsi oleh inderawi. Misalnya, jika covertext berupa citra digital , maka penyisipan pesan membuat citra stegotext sukar dibedakan oleh mata dengan citra digital covertext-nya. Jika covertext berupa audio, maka indera telinga tidak dapat mendeteksi perubahan pada audio stegotext-nya.
2. *Fidelity*. Mutu tidak berubah banyak akibat penyisipan. Perubahan tersebut tidak dapat dipersepsi oleh inderawi. Misalnya, jika covertext berupa citra, maka penyisipan pesan membuat citra stegotext sukar dibedakan oleh mata dengan citra covertext-nya. Jika covertext berupa audio, maka audio stegotext tidak rusak dan indera telinga tidak dapat mendeteksi perubahan tersebut.
3. *Recovery*. Pesan yang disembunyikan harus dapat diungkapkan kembali. Karena tujuan steganografi adalah data hiding, maka sewaktu-waktu pesan rahasia di dalam stegotext harus dapat diambil kembali untuk digunakan lebih lanjut.

II.5 Least Significant Bit

Metode yang digunakan untuk menyembunyikan pesan pada media digital tersebut berbeda-beda. Contohnya, pada berkas Image pesan dapat disembunyikan dengan menggunakan cara menyisipkannya pada bit rendah atau bit yang paling kanan (LSB) pada data pixel yang menyusun file tersebut. Pada berkas bitmap 24 bit, setiap pixel (titik) pada gambar tersebut terdiri dari susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (byte) dari 0 sampai 255. (Ricky, Setyaningsih, & Muhammad , 2018).

Jika dalam format binernya 00000000 sampai 11111111. Metode *Least Significant Bit* akan memasukan sebuah pesan yang telah diubah menjadi nilai biner ke dalam 1 bagian untuk warna biru dari citra digital karena bagian untuk warna biru merupakan bagian terakhir dalam sebuah pixel yang berukuran 8 bit dan tidak akan menghasilkan perubahan warna yang sangat signifikan jika dilihat dengan mata telanjang. Metode LSB hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Sehingga perubahan yang terjadi

tidak terlalu signifikan dan mata manusia pun tidak dapat membedakan perubahan yang kecil yang terjadi.

Keuntungan yang paling besar dari algoritma LSB ini adalah cepat dan mudah. Dan juga algoritma tersebut memiliki software steganografi yang mendukung dengan bekerja di antara unsur pokok warna LSB melalui manipulasi *pallete* yang menyebabkan ukuran gambar tidak akan jauh berubah. Sedangkan kekurangannya adalah pesan/data yang akan disisipkan terbatas, sesuai dengan ukuran citra.

III. ANALISIS DAN PERANCANGAN

III.1 Perancangan Sistem

Pada pembangunan sistem akan digunakan model pengembangan *waterfall*, dikarenakan model pengembangan waterfall melaksanakan proses pembangunan sistemnya secara bertahap dan tidak ada proses dikerjakan secara bersamaan.Berikut adalah tahapan-tahapan yang dilakukan pada perancangan sistem dengan model *waterfall*:

a) Analisis Kebutuhan
   i. Analisis Kebutuhan Fungsional
      a. Dapat melakukan proses enkripsi plain text .
      b. Dapat melakukan proses dekripsi cipher text.
      c. Dapat menyisipkan cipher text kedalam cover image.
      d. Dapat mengekstraksi ciphertext dari stego image
   ii. Analisis Kebutuhan Non Fungsional

      Kebutuhan perangkat keras (Hardware) yang diperlukan untuk mengimplementasikan sistem minimal memiliki spesifikasi sebagai berikut:

      a. Prosesor : intel dual core
      b. Operating System : windows
      c. Ram : 1gb
      d. Penyimpaan : 150 gb

b) Desain Sistem (*System Design*)

Setelah Analisis Kebutuhan, tahapan selanjutnya adalah merancang desain sistem yang memenuhi sesuai dengan ketentuan yang telah dibuat pada analisa kebutuhan, agar perancangan sistem untuk tahap selanjutnya lebih mudah.

c) Penulisan Kode Program

Bahasa pemrograman yang digunakan dalam membangun sistemini adalah bahasa pemrograman Visual Basic, sedangkan aplikasi yang digunakan untuk menulis kode program adalah Microsoft Visual Stuido 2012.

d) Pengujian (*System Testing*)

Pengujian dilakukan dengan metode black box untuk menguji fungsional dari sistem yang dibuat.

e) Pengoperasian dan Pemeliharaan (*Operation and Maintenance*)

Setelah sistem telah selesai dibangun secara keseluruhan, jika terdapat masalah atau ada kekurangan, maka akan dilakukan penelitan terhadap permasalahan serta pengembangan untuk menanggulangi masalah yang ada pada sistem tersebut.

Flowchart diagram pada gambar 2.a menjelaskan alur kerja proses enkripsi dan penyisipan dari sistem secara keseluruhan. Berikut merupakan penjelasan detailnya:

a. Pengguna memulai applikasi. Kegiatan ini ditandai dengan tanda “Mulai”.
b. Pengguna memasukan *plain text*, matriks kunci, dan *cover image*.
c. Pengguna menjalankan proses enkripsi *plain text* yang akan menghasilkan *cipher text*.
d. Pengguna menjalankan proses penyisipan *cipher text* yang akan menghasilkan *stego image*.
e. Pengguna menyimpan hasil dari *stego image* setelah selesai maka proses enkripsi dan penyisipan telah selesai.

Flowchart diagram pada gambar 2.b menjelaskan alur kerja proses dekripsi dan ekstraksi dari sistem secara keseluruhan. Berikut merupakan penjelasan detailnya:

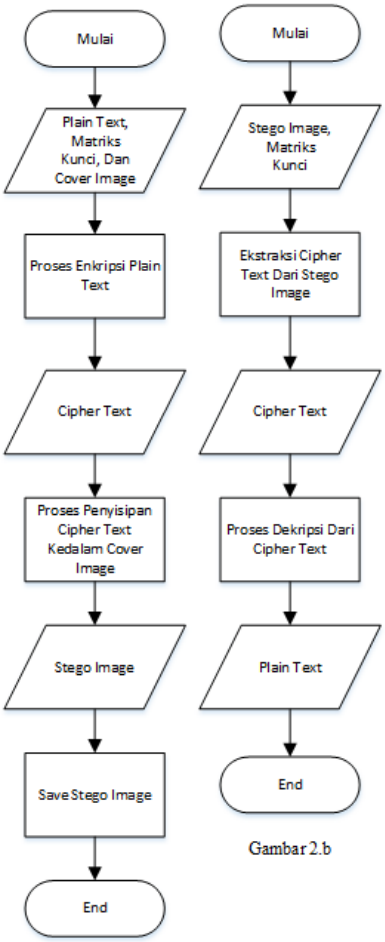
a. Pengguna memulai applikasi. Kegiatan ini ditandai dengan tanda “Mulai”.
b. Pengguna memasukan matriks kunci, dan *stego image*.
c. Pengguna menjalankan proses ekstraksi *cipher text* yang dari *stego image.*
d. Pengguna menjalankan proses dekripsi *cipher text* yang akan menghasilkan *plain image.*
e. Setelah selesai maka proses dekripsi dan ekstraksi telah selesai.

Flowchart diagram pada gambar 3.a menjelaskan cara kerja proses enkripsi algoritma *Hill Cipher*. Berikut merupakan penjelasan detailnya:

a. Pengguna memulai applikasi. Kegiatan ini ditandai dengan tanda "Mulai".
b. Pengguna memasukan matriks kunci, dan *plain text*.
c. Pengguna menjalankan proses cek *invers* matriks, jika matriks kuncinya memiliki *invers* maka matriks tersebut bisa dipakai. Jika tidak ada maka matriks tersebut tidak bisa di pakai.
d. Sistem akan mengubah setiap karakter dari *plain text* menjadi sebuah nilai integer.
e. Sistem akan menyusun karakter berdasarkan ordo matriks.
f. Sistem akan melakukan perkalian kunci matriks dengan nilai integer dari *plain text* lalu hasilnya akan dimoduluskan.
g. Sistem akan mengubah nilai integer hasil dari perkalian kunci matriks dengan nilai integer dari *plain text*. Hasil dari proses ini merupakan *cipher text.*
h. Setelah *cipher text* telah dihasilkan maka proses enkripsi algoritma *Hill Cipher* telah selesai.

Flowchart diagram pada gambar 3.b menjelaskan cara kerja proses dekripsi algoritma *Hill Cipher*. Berikut merupakan penjelasan detailnya:

a. Pengguna memulai applikasi. Kegiatan ini ditandai dengan tanda "Mulai".
b. Pengguna memasukan *invers* matriks kunci, dan *cipher text*.
c. Sistem akan mengubah setiap karakter dari *cipher text* menjadi sebuah nilai integer .
d. Sistem akan menyusun karakter berdasarkan ordo matriks.
e. Sistem akan melakukan perkalian *invers* kunci matriks dengan nilai integer dari *cipher text* lalu hasilnya akan dimoduluskan.
f. Sistem akan mengubah nilai integer hasil dari perkalian *invers* kunci matriks dengan nilai integer dari *plain text*. Hasil dari proses ini merupakan *plain text.*
g. Setelah *plain text* telah dihasilkan maka proses dekripsi algoritma *Hill Cipher* telah selesai.



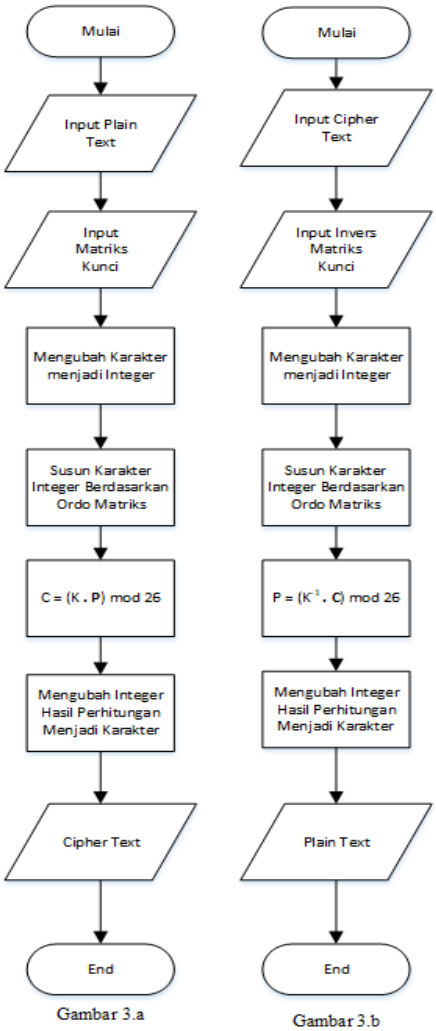
Gambar 2.a. Flowchart Alur Sistem Enkripsi Dan Penyisipan ; Gambar 2.b. Flowchart Alur Sistem Dekripsi Dan Ekstraksi

Flowchart diagram pada gambar 4.a menjelaskan cara kerja proses penyisipan mengunakan metode *Least Significant Bit.* Berikut merupakan penjelasan detailnya:

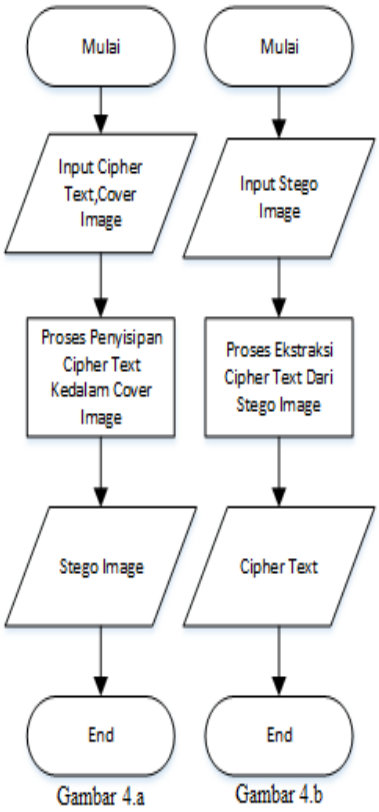
a. Pengguna memulai applikasi. Kegiatan ini ditandai dengan tanda "Mulai".
b. Pengguna memasukan *cipher text dan cover image*.
c. Pengguna menjalankan proses penyisipan *cipher text* kedalam *cover image*.
d. Setelah proses penyisipan selesai maka hasil dari proses tersebut adalah *stego image*.
e. Setelah *stego image* dihasilkan maka proses penyisipan mengunakan metode *Least Significant Bit* telah selesai.

Flowchart diagram pada gambar 4.b menjelaskan cara kerja proses ekstraksi mengunakan metode *Least Significant Bit.* Berikut merupakan penjelasan detailnya:

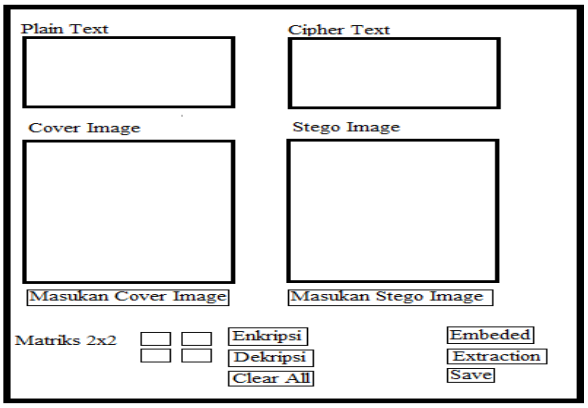
a. Pengguna memulai applikasi. Kegiatan ini ditandai dengan tanda "Mulai".
b. Pengguna memasukan *stego image*.
c. Pengguna menjalankan proses ekstraksi *cipher text* dari *stego image*.
d. Setelah proses ekstraksi selesai maka hasil dari proses tersebut adalah *cipher text*.
e. Setelah *cipher text* dihasilkan maka proses ekstraksi mengunakan metode *Least Significant Bit* telah selesai



Gambar 3.a. Flowchart Enkripsi Algoritma *Hill Cipher* & Gambar 3.b. Flowchart Dekripsi Algoritma *Hill Cipher*



Gambar 4.a. Flowchart Penyisipan Mengunakan Metode *Least Significant Bit*; Gambar 4.b. Flowchart Ekstraksi Mengunakan Metode *Least Significant Bit*



Gambar 5. Desain Antarmuka Sistem

Gambar 5 merupakan tampilan desain antarmuka dari sistem. Pengguna akan memasukan *plaintext*. Setelah memasukan *plaintext* pengguna harus memasukan nilai dari matriks 2x2. Setelah itu pengguna dapat melakukan proses enkripsi dan hasilnya akan ditamplikan pada *textbox cipher text* . Lalu pengguna dapat memilih dan memasukan file citra digital yang akan dimasukan. Setelah itu pengguna dapat

melakukan proses *Embeded* (proses penyisipan). Setelah hasil dari penyisipan telah selesai, maka pengguna dapat menyimpan *stego image*. Pengguna juga dapat memasukan *cover image* dan melakukan proses *ekstraction* (proses extraksi) lalu memasukan nilai matriks 2x2 yang digunakan untuk mendekripsi cipher text menjadi plain text. Hasil tampilan antarmuka ada pada Gambar 6.

III.2 PROSES ENKRIPSI

Misalkan informasi (*Plain Text*) yang akan dikirim adalah "Hai Kamu !" ubah plain text ke nilai numerik seperti A=0 sampai Z=25 dan mengunakan kunci matriks 2x2.

$$Kunci = \begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix}$$

Tabel 1. Indeks Karakter

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

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

Tabel 2. Indeks Angka dan Tanda Baca

0	1	2	3	4	5	6	7	8	9	spasi	!	?
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

Mengubah nilai karakter menjadi nilai numerik berdasarkan Tabel 1 dan Tabel 2:

$$\begin{bmatrix} H \\ a \end{bmatrix} = \begin{bmatrix} 7 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} i \\ spasi \end{bmatrix} = \begin{bmatrix} 8 \\ 10 \end{bmatrix}$$

$$\begin{bmatrix} K \\ a \end{bmatrix} = \begin{bmatrix} 10 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} m \\ u \end{bmatrix} = \begin{bmatrix} 12 \\ 20 \end{bmatrix}$$

$$\begin{bmatrix} spasi \\ ! \end{bmatrix} = \begin{bmatrix} 10 \\ 11 \end{bmatrix}$$

Perhitungan nilai numerik cipher text mengunakan rumus : $C = (P \,.\, K) mod\ 26$

$$\begin{bmatrix} 7 \\ 0 \end{bmatrix}\begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix} = \begin{bmatrix} 7.2 + 0.3 \\ 7.5 + 0.7 \end{bmatrix} = \begin{bmatrix} 14 \\ 35 \end{bmatrix} mod\ 26 = \begin{bmatrix} 14 \\ 9 \end{bmatrix} = \begin{bmatrix} O \\ j \end{bmatrix}$$

$$\begin{bmatrix} 8 \\ 10 \end{bmatrix}\begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix} = \begin{bmatrix} 8.2 + 10.3 \\ 8.5 + 10.7 \end{bmatrix} = \begin{bmatrix} 46 \\ 110 \end{bmatrix} mod\ 26 = \begin{bmatrix} 20 \\ 6 \end{bmatrix} = \begin{bmatrix} u \\ 6 \end{bmatrix}$$

$$\begin{bmatrix} 10 \\ 0 \end{bmatrix}\begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix} = \begin{bmatrix} 10.2 + 0.3 \\ 10.5 + 0.7 \end{bmatrix} = \begin{bmatrix} 20 \\ 50 \end{bmatrix} mod\ 26 = \begin{bmatrix} 20 \\ 24 \end{bmatrix} = \begin{bmatrix} U \\ Y \end{bmatrix}$$

$$\begin{bmatrix} 12 \\ 20 \end{bmatrix}\begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix} = \begin{bmatrix} 12.2 + 20.3 \\ 12.5 + 20.7 \end{bmatrix} = \begin{bmatrix} 84 \\ 200 \end{bmatrix} mod\ 26 = \begin{bmatrix} 6 \\ 18 \end{bmatrix} = \begin{bmatrix} g \\ s \end{bmatrix}$$

$$\begin{bmatrix} 10 \\ 11 \end{bmatrix}\begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix} = \begin{bmatrix} 10.2 + 11.3 \\ 10.5 + 11.7 \end{bmatrix} = \begin{bmatrix} 53 \\ 127 \end{bmatrix} mod\ 26 = \begin{bmatrix} 1 \\ 23 \end{bmatrix} = \begin{bmatrix} 1 \\ * \end{bmatrix}$$

Maka hasil perhitungan menjadi **Oju6Uygs1***

III.3 PROSES DEKRIPSI

Proses dekripsi akan mengunakan rumus :

$$P = (K^{-1} \,.\, C)\ mod\ 26$$

Menghitung determinan matriks :

$$Adj = \begin{bmatrix} 7 & -3 \\ -5 & 2 \end{bmatrix}$$

$$determinan = \begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix} = ((2 * 7) - (3 * 5))$$

$$= (14 - 15)$$

$$= -1\ mod\ 26$$

$$= -1$$

$$\frac{1}{determinan} mod\ 26 = x$$

$$(determinan * X)mod\ 26 = 1$$

$$(-1 * X)mod\ 26 = 1$$

$$X = 25$$

$$K^{-1} = \left(\frac{1}{determinan} mod\ 26\right) * \begin{bmatrix} 7 & -3 \\ -5 & 2 \end{bmatrix}$$

$$= 25 * \begin{bmatrix} 7 & -3 \\ -5 & 2 \end{bmatrix}$$

$$= \begin{bmatrix} 175 & -75 \\ -125 & 50 \end{bmatrix}$$

$$= \begin{bmatrix} 19 & 3 \\ 5 & 24 \end{bmatrix}$$

Perhitungan dekripsi hill cipher :

$$\begin{bmatrix} 14 \\ 9 \end{bmatrix}\begin{bmatrix} 19 & 3 \\ 5 & 24 \end{bmatrix} = \begin{bmatrix} 14.19 + 9.3 \\ 14.5 + 9.24 \end{bmatrix} = \begin{bmatrix} 293 \\ 286 \end{bmatrix} mod\ 26 = \begin{bmatrix} 7 \\ 0 \end{bmatrix} = \begin{bmatrix} H \\ a \end{bmatrix}$$

$$\begin{bmatrix} 20 \\ 6 \end{bmatrix}\begin{bmatrix} 19 & 3 \\ 5 & 24 \end{bmatrix} = \begin{bmatrix} 20.19 + 6.3 \\ 20.5 + 6.24 \end{bmatrix} = \begin{bmatrix} 398 \\ 244 \end{bmatrix} mod\ 26 = \begin{bmatrix} 8 \\ 10 \end{bmatrix} = \begin{bmatrix} i \\ spasi \end{bmatrix}$$

$$\begin{bmatrix} 20 \\ 24 \end{bmatrix}\begin{bmatrix} 19 & 3 \\ 5 & 24 \end{bmatrix} = \begin{bmatrix} 20.19 + 24.3 \\ 20.5 + 24.24 \end{bmatrix} = \begin{bmatrix} 168 \\ 676 \end{bmatrix} mod\ 26 = \begin{bmatrix} 10 \\ 0 \end{bmatrix} = \begin{bmatrix} K \\ a \end{bmatrix}$$

$$\begin{bmatrix} 6 \\ 18 \end{bmatrix}\begin{bmatrix} 19 & 3 \\ 5 & 24 \end{bmatrix} = \begin{bmatrix} 6.19 + 18.3 \\ 6.5 + 18.24 \end{bmatrix} = \begin{bmatrix} 168 \\ 462 \end{bmatrix} mod\ 26 = \begin{bmatrix} 12 \\ 20 \end{bmatrix} = \begin{bmatrix} m \\ u \end{bmatrix}$$

$$\begin{bmatrix}1\\23\end{bmatrix}\begin{bmatrix}19 & 3\\5 & 24\end{bmatrix} = \begin{bmatrix}1.19 + 23.3\\1.5 + 23.24\end{bmatrix} = \begin{bmatrix}88\\557\end{bmatrix} mod\ 26 = \begin{bmatrix}10\\11\end{bmatrix} = \begin{bmatrix}spasi\\!\end{bmatrix}$$

III.4 PROSES PENYISIPAN

Misalkan huruf **"J"** merupakan kata yang sudah melalui proses enkripsi mengunakan algoritma *Hill Cipher*.

Misalkan telah diketahui nilai dari masing-masing pixel adalah:

P1 : 250 = 11111010

P2 : 156 = 10011100

P3 : 124 = 01111100

P4 : 122 = 01111010

P5 : 131 = 10000011

P6 : 222 = 11011110

P7 : 142 = 10001110

P8 : 108 = 01101100

Berikut merupakan langkah penyisipannya.

Ubah karakter menjadi sebuah nilai integer menggunakan kode ASCII : J = 74 . Langkah selanjutnya adalah mengkonversi nilai integer tersebut kebentuk biner : J = 01001010. Lalu lakukan proses penyisipan dengan cara mengganti bit terakhir pada biner pixel *cover image* dengan biner pesan .

P1 :1111101**0** diganti 0 = 1111101**0** =250

P2 :1001110**0** diganti 1 = 1001110**1** =157

P3 :0111110**0** diganti 0 = 0111110**0** =124

P4 :0111101**0** diganti 0 = 0111101**0** =122

P5 :1000001**1** diganti 1 = 1000001**1**=131

P6 :1101111**0** diganti 0 = 1101111**0** =222

P7 :1000111**0** diganti 1 = 1000111**1**=143

P8 :0110110**0** diganti 0 = 0110110**0** =108

III.5 PROSES EKSTRAKSI

Merupakan sebuah proses yang mengambil bit-bit terakhir pixel dari *stego image*. Kemudian kumpulan bit terakhir tersebut disusun dan dikonversikan menjadi nilai kode ASCII. Berikut merupakan langkahnya:

Mengambil bit terakhir pixel *stego image*

P1 : 250 = 1111101**0** =

P2 : 157 = 1001110**1** = 1

P3 : 124 = 0111110**0** = 0

P4 : 122 = 0111101**0** = 0

P5 : 131 = 1000001**1**= 1

P6 : 222 = 1101111**0** = 0

P7 : 143 = 1000111**1**= 1

P8 : 108 = 0110110**0** =0

Dari hasil ekstraksi diatas diperoleh dikumpulkan menjadi urutan **"01001010"** kemudian dikonversikan kedalam nilai kode ASCII dan dikonversikan kebentuk karakter huruf atau angka atau tanda baca.

0100101 = 74 = J

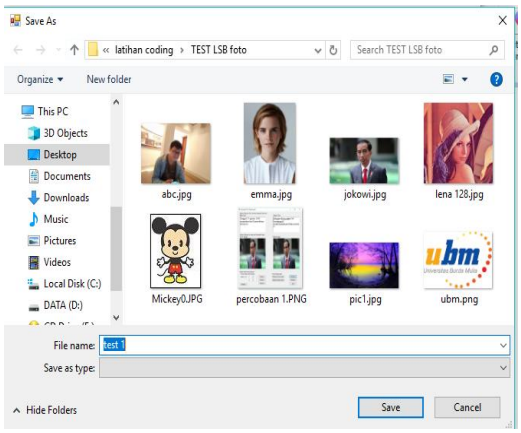
Setelah itu *cipher text* akan di dekripsi mengunakan algoritma *Hill Cipher*.

III.6 TAMPILAN ANTARMUKA

Pengguna harus memasukan *plain text* , *cipher tex t*,nilai matriks ,*cover image* ,*stego image* seperti pada gambar 6.

Gambar 6. Antarmuka Sistem

Pengguna dapat memilih citra digital yang akan dimasukan, seperti pada gambar 7.



Gambar 7. Cari *Cover Image* atau *Stego Image*

HASIL PENELITIAN

Tabel 3. Analisa Hasil Enkripsi Dan Dekripsi

Plain Text	Kunci	Cipher Text	Invers Kunci	Status
Universitas Bunda Mulia.	$\begin{bmatrix}3 & 7\\5 & 10\end{bmatrix}$	Vwpqbi gofru8 Nxirs-Ualfn0	$\begin{bmatrix}24 & 17\\1 & 25\end{bmatrix}$	Sukses
Apakah Jakarta Merupakan Ibukota Indonesia?	$\begin{bmatrix}19 & 0\\4 & 97\end{bmatrix}$	Azaiad8[aialxy8lył qbaian8K uiuxy8Kn gryuwg&4	$\begin{bmatrix}11 & 0\\10 & 11\end{bmatrix}$	Sukses
Kemerdekaan Indonesia Tanggal 17 Agustus 1945.	$\begin{bmatrix}7 & 4\\8 & 9\end{bmatrix}$	Imwcbhq: aab?Ezzu dkcio?Dw lcqwn-9)(Csuud ek-!1491	$\begin{bmatrix}7 & 14\\20 & 17\end{bmatrix}$	Sukses
Gerhana Bulan Total 28 Juli 2018 Disebut Sebagai yang Terlama!	$\begin{bmatrix}7 & 6\\4 & 11\end{bmatrix}$	Oqfpan i6Xqzs v6Jwdy h/ (&Jytm ?:83: Viwibu d-Eibkow k6sany 4Bqdhu co'	$\begin{bmatrix}11 & 20\\22 & 7\end{bmatrix}$	Sukses
Dunia militer Indonesia juga berhasil mempersembahkan prestasi yang membanggakan pada bulan November lalu. TNI AD berhasil menjadi juara umum dalam lomba tembak ASEAN Army Rifle Meet (AARM) ke-27 yang diselenggarakan di Singapura dengan perolehan 9 trofi, 31 medali emas, 10 medali perak, dan 10 medali perunggu.	$\begin{bmatrix}6 & 11\\9 & 14\end{bmatrix}$	Evkvg emydct e7Juqp sroog oxkc)a doqloo u5midg dowkfs zuimg*r jockpoo ?knaq? mifsnay igkna'o hqg sdovg* Ybolfsd o"kryd/ 9SKV8 MY!ynx rqsns ylkcdcj 3iqyyx &ggya: sbova: mjfsg ctfsgk8 MWKN A8Maju (lfvre& Mizq/4 AAAJ," aq/(- @oiot;c mmpilk yifegkn a;cc4O ootjcvc g kfotna' odoxux ena389 swlob// 3; yfaryc4 awqs//6 9 yfaryc4 ejyxc2; cna)06 misbyd' ododyyi d/	$\begin{bmatrix}6 & 25\\11 & 10\end{bmatrix}$	Sukses

Tabel 4. Analisa Hasil Penyisipan Dan Ekstraksi

Cipher Text	Citra Asli	Citra Hasil	Ukuran Asli	Ukuran Hasil	Sukses
Vwpqbigofru8Nxirs-Ualfn0	Ubm.png 	Ubm.jpg 	5,44 kb	8,62kb	Sukses
Azaiad8Daialxy8lybqbaian8Ktuiuxy8Knfgryuwg&4	Jakarta.jpg 	Jakarta2.jpg 	12,3kb	134kb	Sukses
Imwcbhqsaab?Ezzudkcio?Dwlcqwn-9)(Csuudek-!1491	Jokowi.jpg 	Jokowi2.jpg 	6,02 kb	98,9 kb	Sukses
Oqfpani6Xqzsv6Jwdyh/ (&Jytm?:83: Viwibud-Eibkowk6sany4Bqdhuco'	Emma.png 	Emma2.jpg 	5,38 kb	92,0 kb	Sukses
Evkvg emydcte7Juqpsroog oxkc)adoqloou5midgdowkfszuimg*rjockpoo?knaq?mifsnayigkn a'ohqg sdovg*Ybolfsdo"kryd/9SKV8MY!ynxrqsns ylkcdcj3iqyyx&ggya:sbova:mjfsg ctfsgk8MWKNA8Maju(lfvre&Mizq/4AAAJ,"aq/(-@oiot;cmmpilkyifegkna;cc4Oootjcvcg kfotna'odoxuxena389swlob//3; yfaryc4awqs//69 yfaryc4ejyxc2;cna)06 misbyd'ododyyid/	TNI.bmp 	TNI2.jpg 	7,91 kb	124 kb	Sukses

IV. KESIMPULAN DAN SARAN

Berdasarkan analisa dan implementasi enkripsi , dekripsi , penyisipan , dan ekstraksi pada citra digital dengan menggunakan algoritma *Hill Cipher* dan metode *Least Significant Bit* maka penulis menyimpulkan bahwa :

1. Proses enkripsi dan dekripsi pada informasi berupa text menggunakan algoritma *hill cipher* berhasil dilakukan sesuai dengan tahapan – tahapan sehingga dapat menghasilkan sebuah *cipher text* yang berupa pengacakan karakter baik huruf besar , huruf kecil , angka , tanda baca sebagian.
2. Proses penyisipan *cipher text* kedalam sebuah citra digital berhasil dilakukan pada citra digital dengan format : jpeg,bitmap,png dan tidak mengalami perubahan secara signifikan yang dapat dilihat oleh mata manusia. Walaupun ukuran antara *cover image* dan *stego image* mengalami perubahan yang signifikan.

3. Proses ekstraksi *cipher text* dari citra digital berhasil dilakukan dan *cipher text* tidak mengalami perubahan. Dan dapat dilakukan proses dekripsi setelah ekstraksi

Pada penulisan ini masih terdapat beberapa kendala , kekurangan dan kelemahan yang dapat dikembangkan dalam penulisan selanjutnya. Saran bagi penulis selanjutnya yaitu sebagai berikut:

1. Masih terdapat beberapa simbol dan tanda baca yang tidak dapat digunakan pada penelitian ini. Diharapkan penulis selanjutnya dapat mengembangkan simbol dan tanda baca tersebut dapat digunakan pada proses enkripsi dan dekripsi mengunakan algoritma *hill cipher.*
2. Pada proses enkripsi dan dekripsi harus mengunakan matriks yang *reversible*.
3. Penulis selanjutnya dapat mengunakan matriks kunci selain matriks berordo 2x2. Seperti matriks berordo 3x3 atau berordo matriks 4x4.
4. Penulis selanjutnya dapat mengkompersi hasil *stego* yang telah disisipkan *cipher text* agar tidak mengalami perubahan ukuran yang signifikan terhadap *cover image.*

REFERENSI

Analisis Kompresi Steganography Pada Citra Digital Dengan Menggunakan Metode Least Significant Bit Berbasis Mobile Android 2018. Jurnal Coding. Rekayasa Sistem Komputer Volume 06, No. 03(2018), hal 75-86

Anwar, S. (2017). Implementasi Pengamanan Data Dan Informasi Dengan Metode Steganografi LSB Dan Algoritma Kriptografi AES. Jurnal Format Volume 6 Nomor 1 Tahun 2017, 65-74.

Implementasi Algoritma Hill Cipher Dalam Penyandian Data 2013. Pelita Informatika Budi Darma, Volume : IV, Nomor: 2, Agustus 2013115-122

Pengantar Ilmu KRIPTOGRAFI Teori, Analisis, dan Implementasi 2008.Yogyakarta.Andy Offset

Sulindawaty. (2017). Implementasi Penyembunyian Pesan Pada Citra Digital Dengan Menggabungkan Algoritma Hill Cipher Dan Metode Least Significant Bit (Lsb) *Jurnal* Manajemen dan Informatika Pelita Nusantara Volume 1 No 2 Desember 2017 1-8

Winarno. (2012) Implementasi Steganografi Menggunakan Metode Least Significant Bit dan Kriptografi Advanced Encryption Standard ULTIMATICS, Vol. IV, No. 1 | Juni 20122424-32