Implementasi Hill Cipher Pada Kode Telepon dan Five Modulus Method dalam Mengamankan Pesan

Implementation of Hill Cipher in Telephone Code and Five Modulus Method for Securing Messages

Patmawati Hasan*[1], Selviana Yunita[2], Dony Ariyus[3]
[1] STIMIK Sepuluh Nopember Jayapura, [2,3]Universitas Amikom Yogyakarta
[1]Jl. Ardipura II No. 22 B Polimak – Jayapura, Tlp (0967) 533400, [2]Jl. Ring Road Utara, Yogyakarta, Tlp (0274) 884201
e-mail: [1]patmawatihasan@gmail.com, [2]selviana.yunita.ax@gmail.com, [3]dony.a@amikom.ac.id

Abstrak

Perkembangan teknologi yang canggih di era ini semakin pesat, pesan-pesan yang disembunyikan atau dirahasiakan dari orang-orang yang ingin mengakses pesan rahasia tersebut perlu dijaga keamanan dengan cara mengubah pesan tersebut menjadi sandi rahasia dan menyisipkan menggunakan teknik kriptografi dan steganografi. Sistem keamanan yang dibangun menggunakan kombinasi algoritma Hill cipher dan Five Modulus Method dengan tujuan membuat keamanan yang kuat dan berlapis tanpa mengurangi atau merusak pesan teks pada gambar. Sistem yang dibangun menggunakan bahasa pemograman Matlab. Algoritma yang digunakan memiliki kelebihan dalam mengekripsi data berdasarkan penelitian-penelitian terdahulu yang berhasil menggunakan teknik kriptografi dan steganografi. Hill Cipher menggunakan matriks berukuran (m x m) sebagai kunci dalam mengenkripsi dan dekrpsi data pada kode telepon yang telah dimodifikasi dengan tujuan meningkatkan kemananan. Sedangkan untuk steganografi menggunakan Five Modulus Method dengan memeriksa seluruh piksel dalam blok (k x k) dan mengubah setiap piksel menjadi sebuah angka yang habis dibagi 5. Hasil dari penelitian ini berupa sistem keamanan yang menggunakan Kombinasi Hill Cipher dan Five Modulus Method dalam Mengamankan Pesan Teks. Berdasarkan hasil tingkat akurasi yang dilakukan pengujian sebanyak lima (5) kali terhadap plaintext yang berbeda didapatkan tingkat akurasi sebesar 100% yaitu tidak ditemukan perbedaan. Selanjutnya dilakukan pengembangan agar tidak hanya dapat enkripsi text saja, tetapi dapat enkripsi file atau media lainnya.

Kata kunci*— Hill cipher, Five Modulus Method, Kode Telepon*

Abstract

The development of sophisticated technology in this era is increasingly rapid, messages that are hidden or kept secret from people who want to access these secret messages need to be kept safe by changing the message into a secret password and inserting it using cryptographic and steganographic techniques. The security system is built using a combination of the Hill cipher algorithm and the Five Modulus Method with the aim of creating a strong and layered security without reducing or damaging text messages in the image. The system was built using the Matlab programming language. The algorithm used has the advantage of encrypting data based on previous studies that have successfully used cryptographic and steganographic techniques. Hill Cipher uses a matrix of size (m x m) as a key in encrypting and decrypting data in a modified telephone code with the aim of increasing security. Whereas for steganography

using the Five Modulus Method by examining all pixels in a block (k x k) and converting each pixel into a number that has been divided 5. The results of this research are a security system that uses a combination of Hill Cipher and Five Modulus Method in Securing Text Messages. Based on the results of the accuracy level which was tested five times (5) times for different plaintext obtained an accuracy level of 100% that is not found differences. Further development is carried out so that it can not only encrypt text, but can encrypt files or other media.

Keywords— *Cryptography, Steganography, Hill cipher, Five Modulus Method*

1. PENDAHULUAN

Dalam kecanggihan teknnologi saat ini, proses berkirim pesan menjadi jauh lebih cepat dan mudah. Namun, perkembangan ini juga berdampak pada masalah keamanan, dimana informasi yang dikirimkan rentan mengalami pencurian, pembajakan, serta diketahui oleh pihak yang tidak bertanggung jawab. Menghadapi masalah tersrbut, diperlukan suatu metode agar informasi yang dikirimkan hanya dapat diterima oleh pihak yang memiliki kepentingan. Salah satu metode pengamanan pesan adalah melalui kriptografi dan steganografi.

Kriptografi adalah suatu cabang ilmu yang mempelajari bagaimana informasi yang dikirimkan tetap aman dan terjaga kerahasiaannya. Dua konsep utama kriptografi adalah enkripsi dan dekripsi [1]. Sedangkan steganografi adalah sebuah tindakan menyembunyikan pesan rahasia didalam suatu media, dengan sebagian besar sistem memanfaatkan kelemahan perseptual manusia. Steganografi seringkali disalah artikan dengan kriptografi dikarenakan keduanya sama-sama digunakan untuk melindungi informasi rahasia. Namun, jika keduanya digunakan secara bersamaan akan menggandakan perlindungan terhadap informasi [2]. Perbedaan utama dari kriptografi dan steganografi adalah kriptografi berfokus dalam menjaga isi pesan tetap rahasia, sedangkan steganografi berfokus dalam menjaga keberadaan pesan rahasia [3]. Berdasarkan pendapat diatas, maka penting untuk menggunakan kombinasi kriptografi dan steganografi demi memperoleh perlindungan terhadap informasi yang lebih optimal.

Dalam penelitiannya, Qazi menawarkan modifikasi algoritma *hill cipher* dengan melakukan penambahan transposisi, substitusi, serta pemindahan fungsi kiri dan kanan. Transposisi dan Substitusi plaintext dilakukan pada masing-masing matrik n x n. Setelah itu dilakukan pemindahan fungsi kiri dan kanan pada proses enkripsi. Penelitian dilakukan dengan menggunakan Matlab. Hasil penelitian menunjukkan jika algoritma yang ditawarkan memiliki hasil output yang lebih baik dalam hal ukuran file ketika dibandingkan dengan algoritma tradisional *hill cipher* [4].

Penelitian yang dilakukan oleh Prasad melakukan modifikasi pada matrik hill cipher dan affine hill cipher dengan menggunakan modulasi bilangan prima. Persamaan linear yang homogen dan bilangan prima digunakan menghasilkan matrik self-invertible yang dapat mengurangi kompleksitas komputasi pada saat dekripsi. Penelitian menunjukkan hasil bahwa algoritma ini cocok untuk gambar hitam putih dan berwarna [5].

Penelitian menggunakan Five Modulus Method dalam menyembunyikan pesan rahasia pada sebuah gambar. Keuntungan utama dari dari algoitma ini adalah menjaga ukuran gambar tetap konstan ketika pesan rahasia meningkatkan ukuran gambar. Pengujian dilakukan dengan cara menangkap sinyal *noise* puncak dalam suatu gambar. Diketahui berdasarkan nilai PSNR, gambar yang memiliki pesan rahasia memiliki nilai PSNR lebih tinggi. Algoritma ini sangat efisien untuk menyembunyikan data didalam gambar [6].

Alkadi melakukan penelitian untuk keamanan hybrid steganografi pada private cloud platform, dengan memanfaatkan algoritma Five Modulus Method. Pada algoritma yang ditawarkan, dilakukan proses *embedded* steganografi dan *cloud computing*, sehingga dapat

menghasilkan standar keamanan yang lebih baik. Dilakukan proses inverted pada piksel dengan menggunakn *Five Modulus Method*. Menggunakan Software as a Service (SaaS) Document Management, gambar disimpan dan dibagian kepada penerima yang akan mengurangi proses seperti *upload* dan *download.* Dengan adanya SaaS dapat lebih menghemat biaya, keamanan jaminan, serta lebih mudah terukur dalam proses berbagi pada *cloud computing* [7].

Ariyus melakukan penelitian dengan mengembangkan dari peneltian terdahulu berupa kombinasi dari 4 teknik subtitusi, salah satunya dengan menggunakan algoritma *hill cipher*. Cipher text kemudian disembunyikan dalam suatu gambar dengan algoritma *Least Significant Bit* (LSB). Penelitian ini memberikan penambahan sebelum proses substitusi standar sehingga meningkatkan tingkat keamanan meskupun enkripsi dilakukan dengan teknik yang sederhana. Hasil penelitian ini menujukkan jika penelitian ini hanya dapat diterapkan pada media sosial seperti Google+, Telegram, dan Google Drive karena terjadinya perubahan terhadap ukuran gambar. Metode yang diusulkan tidak dapat digunakan pada media sosial seperti intasgram, facebook, whatsapp, dan pinterest karena media sosial tersebut otomatis merubah ukuran gambar menjadi lebih kecil dari ukuran sebenarnya [8].

Penelitian lain mengenai modifikasi *Hill Cipher* dilakukan oleh Qasem. *Hill Cipher* sendiri merupakan kriptpgrafi klasik yang berdasarkan pada aljabar linear dengan transformasi liinear sederhana menggunakan matrik. Proses enkripsi dan dekripsi pada *hill cipher* menggunakan perkalian matrik yang berpotensi menghabiskan waktu, dan membuat hal ini menjadi salah satu masalah yang banyak dipelajari. Dalam penelitian ini, Qasem mengimplemntasikan *Message Passing Interface* (MPI) dan metode *MapReduce* untuk mendemonstrasikan efektivitasnya dalam mempercepat algoritma hill cipher dengan algoritma paralel pada sistem *multicore.* Hasil simulasi menemukan jika angka efisiensi MPI dan *MapReduce* adalah 93.71% dan 53.43%, mengindikasikan hasil yang lebih baik dibandingkan dengan metode sekunesial [9].

Joshi dalam penelitiannya mengusulkan suatu pendekatan baru dalam dunia steganografi dengan memanfaatkan kombinasi antara nilai pada karakter ASCII dengan nilai RGB pada suatu pixel, sehingga suatu karakter tunggal dapat tersimpan dalam sebuah pxel. Tujuan utama dai penelitian ini adalah menyediakan kapasitas maksimum pixel yang dapat dimiliki oleh suatu gambar. Pendekatan yang diusulkan adalah dengan cara mengambil karakter pertama dari suatu pesan dan membagi nilai karakter ASCII karakter tersebut menjadi tiga segmen. Kemudian tiga angka dari nilai karakter yang kemudian ditempatkan pada 3 pixel yang ada, yaitu RGB (Red, Green, and Blue). Sehingga akhirnya kombinasi dari ketiga angka ini dengan nilai RGB ini tidak akan memberikan perubahan kepada gambar yang awal [10].

Selviana juga dalam penelitian melakukan modifikasi algoritma hill cipher dan twofish, pada proses enkripsi dan dekripsi file. Implementasi dari modifikasi algoritma algoritma hill cipher dengan kode wilayah yang kemudian di enkripsi dengan menggunakan metode Twofish sehinggan kriptanilisis tidak bebas mengakses keamanan data. Enkripsi berupa penyandian data dan informasi menjadi sesuatu yang tidak terbaca oleh pihak yang tidak berhak dan juga bermanfaat dalam memberikan tambahan informasi terkait proses enkripsi dan dekripsi yang terjadi pada algoritma twofish. Hasil dari enkripsi dengan algoritma ini adalah file yang dapat diakses melalui aplikasi notepad yang berisi simbol acak Namun pada penelitian modifikasi algoritma hill cipher dan twofish ini hanya menggunakan Teknik kriptografi untuk menyembunyikan file [11].

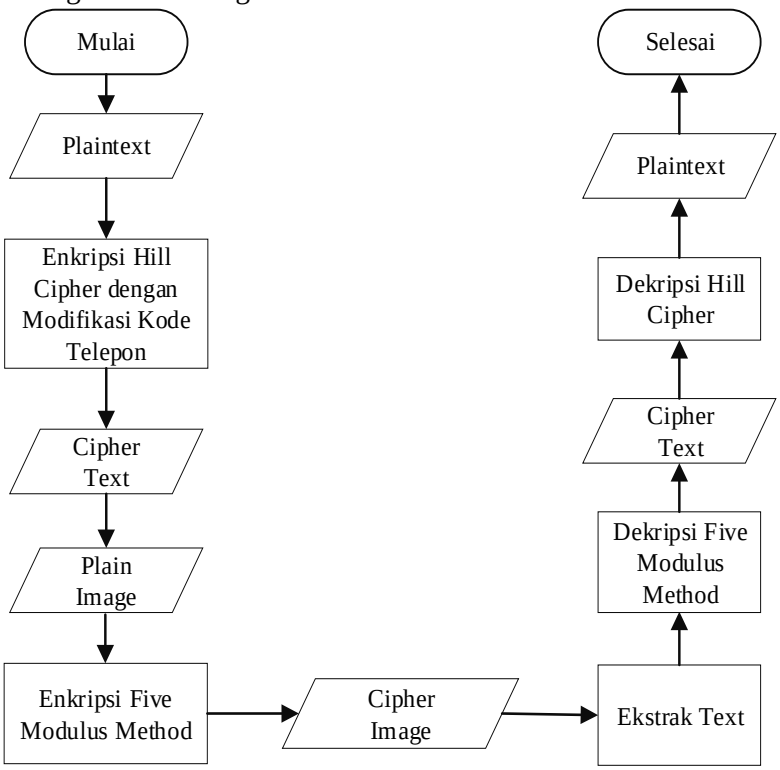
Berdasarkan penelitian yang telah dilakukan sebelumnya, penelitian ini menawarkan modifikasi algoritma dengan menggunakan algoritma *hill cipher* dan *Five Modulus Method* sebagai kombinasi algoritma dalam pengamanan pesan yang menggunakan teknik kriptografi dan steganografi. Tahap awal adalah melakukan enkripsi informasi dengan menggunakan algoritma *hill cipher* yang dikombinasikan dengan kode telepon. Setelah itu, *cipher text* akan disisipkan pada sebuah gambar dengan menggunakan algoritma *Five Modulus Method.*

Pengujian dilakukan dengan melakukan percobaan enkripsi pesan teks pada sistem sebanyak lima kali dan membandingkan dengan perhitungan manual.

2. METODE PENELITIAN

2.1. Alur Penelitian

Alur penelitian untuk menyembunyikan pesan rahasia menggunakan kombinasi algoritma *Hill cipher* dan *Five Modulus Method* dalam meningkatkan keamanan berlapis pada pesan teks dapat dilihat gambar 1 sebagai beriktu:



Gambar 1 Alur Penelitian

Pada gambar 1 Alur penelitian dibuat gambaran alur data secara detil sesuai dengan penggunaan algoritma sebagia berikut:

1. Hal pertama yang dilakukan adalah memasukkan *plaintext* yang akan di enkripsi.
2. *Plaintext* yang di enkripsi menggunakan algoritma *Hill cipher* dengan kunci kode telepon yang telah dimodifikasi.
3. Kemudian didapatkan *cipher text* yang nantinya akan disisipkan kedalam gambar.
4. Menyiapkan *plain image* yang akan disisipkan *cipher text*.
5. Setelah *plain image* dimasukkan kedalam system kemudian di enkripsi menggunakan algoritma *Five Modulus Method.*
6. Kemudian didapatkan *cipher image* yang didalamnya sudah di eksrak Text
7. Mendekripsikan *cipher image* untuk mendapatkan *chipper text*.
8. Langkah selanjutnya mendekripsikan *chipper text* menggunakan algoritma *Hill cipher*.
9. Akhir dari alur data tersebut adalah sebuah *plain text*.

2.2. Algoritma Hill Cipher

Pada tahun 1929 algoritma *Hill Cipher* diciptakan oleh Lester S. Hill. Teknik

kriptografi ini bermaksud untuk menciptakan *cipher* (kode) yang tidak dapat dipecahkan menggunakan teknik analisis frekuensi. *Hill Cipher* merupakan salah satu algoritma kriptografi kunci simetris yang memiliki beberapa kelebihan dalam enkripsi data. Algoritma *Hill Cipher* menggunakan matriks berukuran m x m sebagai kunci untuk melakukan enkripsi dan dekripsi [12]. Hill cipher dapat digolongkan sebagai kriptografi *polyalphabetic* yang dapat dikategorikan sebagai blok cipher, karena teks yang akan diproses dibagi menjadi blok-blok dengan ukuran tertentu. Menggunakan matriks berukuran m x n sebagai kunci untuk melakukan enkripsi dan dekripsi. Dasar teori matriks yang digunakan dalam Hill Cipher antara lain adalah perkalian antar matriks dan melakukan invers pada matriks [13]. Matriks K yang menjadi kunci ini harus merupakan matriks yang invertible, yaitu memiliki inverse K-1. Kunci harus memiliki invers karena matriks K-1 tersebut adalah kunci yang digunakan untuk melakukan dekripsi.

Dalam melakukan enkripsi pada algoritma Hill Cipher dilakukan blok per blok plainteks. Ukuran blok tersebut sama dengan ukuran matriks kunci. Sebelum membagi teks menjadi deretan blok-blok, plainteks mula-mula dikonversi menjadi angka, misalnya A=0, B=1, sampai Z=25. Secara matematis, proses enkripsi pada Hill Cipher adalah [14]:

C = K . P
C = Ciphertext
K = Kunci
P = Plaintext

2.3. Algoritma Five Modulus Method

Ide utama dari Five modulus method adalah berdasarkan pada satu konsep yaitu karakteristik umum pada sebagian besar gambar adalah pixel-pixel yang berdekatan saling berhubungan. Karena itu, untuk bi-level images, pixel yang saling berdekatan memilki kecenderungan menjadi sama dengan piksel yang asli. Five Modhulus Method membagi gambar menjadi setiap blok k x k pixel. Diketahui setiap pixel pada bi-level gery images memiliki memiliki nilai antara 0 sampai 255. Meskipun jika dapat diubah setiap nilai yang ada pada rentang teserbut menjadi nilai yang dapat dibagi 5, hal tersebut tidak akan mempengaruhi sistem penglihatan manusia. Konsep dasar dari FMM adalah dengan memeriksa seluruh pixel diblok k x k dan mengubah setiap pixel menjadi angka yang dapat dibagi menjadi 5 berdasarkan algoritma dibawah ini [6]:

If Pixel mod 5 = 4
Pixel=Pixel+1
Else if Pixel mod 5 = 3
Pixel=Pixel+2
Else if Pixel mod 5 = 2
Pixel=Pixel-2
Else if Pixel mod 5 = 1
Pixel=Pixel-1

2.4. Kode Telepon

Pada kunci dalam algortima *Hill Cipher* yang digunakan untuk menenkripsi *plaintext* yaitu kode telepon yang telah dimodifikasi dengan tujuan meningkatkan kemananan *plaintext* agar tidak diketahui orang-orang yang tidak bertanggung jawab. Berikut kunci kode telepon yang telah dimodifikasi pada table 1:

Tabel 1. Kunci Kode Telepon

Kode Telepon	Modifikasi Kunci	Keterangan
03-25	$\begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix}$	Sangkapura (Bawean)

04-31	$\begin{bmatrix}3 & 1\\1 & 4\end{bmatrix}$	Tomohon
04-35	$\begin{bmatrix}3 & 1\\5 & 4\end{bmatrix}$	Limboto
04-23	$\begin{bmatrix}2 & 1\\3 & 4\end{bmatrix}$	Makale
04-19	$\begin{bmatrix}1 & 1\\9 & 4\end{bmatrix}$	Jeneponto
04-17	$\begin{bmatrix}1 & 1\\7 & 4\end{bmatrix}$	Malino

3. HASIL DAN PEMBAHASAN

3.1 *Algoritma Hill Cipher*

a. Enkripsi Menggunakan Algoritma Hill Cipher

Pesan rahasia yang dijadikan *plaintext* (P A S C A S A R J A N A) dengan modifikasi kunci perblok dengan matrix (2 x 2) sebagai berikut :

K1 = PA = $\begin{bmatrix}2 & 1\\5 & 3\end{bmatrix}$

K2 = SC = $\begin{bmatrix}3 & 1\\1 & 4\end{bmatrix}$

K3 = AS = $\begin{bmatrix}3 & 1\\5 & 4\end{bmatrix}$

K4 = AR = $\begin{bmatrix}2 & 1\\3 & 4\end{bmatrix}$

K5 = JA = $\begin{bmatrix}1 & 1\\9 & 4\end{bmatrix}$

K6 = NA = $\begin{bmatrix}1 & 1\\7 & 4\end{bmatrix}$

Dalam proses penyandian harus menetapkan kunci matriks (2 x 2) terlebih dahulu untuk melakukan proses penyandian. Pesan yang disandikan maksimal 66 karakter tiap karakter harus berada diantara A-Z yang berjumlah 25 huruf dalam proses penyandian ini huruf besar dan kecil tidak dibedakan. Tahap-tahap enkripsi *plaintext* (PASCASARJANA) diantaranya:

Hal pertama yang dilakukan adalah mengkonversi deretan huruf *plaintext* menjadi deretan angka seperti Tabel 2 berikut:

Tabel 2. Konversi Deretan Huruf *Plaintext* menjadi Deretan Angka

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

Maka *plaintext* (PASCASARJANA) berbentuk seperti Tabel 3 berikut:

Tabel 3. Perubahan *plaintext*

Plaintext	P	A	S	C	A	S	A	R	J	A	N	A
Angka	15	0	18	2	0	18	0	17	9	0	13	0

Kemudian membagi deretan angka menjadi sebuah blok matrix (1 x 2) seperti berikut:

Blok 1 = $\begin{bmatrix} P \\ A \end{bmatrix} = \begin{bmatrix} 15 \\ 0 \end{bmatrix}$

Blok 2 = $\begin{bmatrix} S \\ C \end{bmatrix} = \begin{bmatrix} 18 \\ 2 \end{bmatrix}$

Blok 3 = $\begin{bmatrix} A \\ S \end{bmatrix} = \begin{bmatrix} 0 \\ 18 \end{bmatrix}$

Blok 4 = $\begin{bmatrix} A \\ R \end{bmatrix} = \begin{bmatrix} 0 \\ 17 \end{bmatrix}$

Blok 5 = $\begin{bmatrix} J \\ A \end{bmatrix} = \begin{bmatrix} 9 \\ 0 \end{bmatrix}$

Blok 6 = $\begin{bmatrix} N \\ A \end{bmatrix} = \begin{bmatrix} 13 \\ 0 \end{bmatrix}$

Selanjutnya mengenkripsikan modifikasi kunci perblok dengan matrix (2 x 2) yang di jumlahkan dengan *plaintext* blok matrix (1 x 2) menggunakan algoritma *Hill Cipher* untuh mendapatkan *chipertext* seperti berikut:

Blok 1 = $\begin{bmatrix} P \\ A \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix} x \begin{bmatrix} 15 \\ 0 \end{bmatrix} = \begin{bmatrix} 30 \\ 75 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 4 \\ 23 \end{bmatrix} = \begin{bmatrix} E \\ X \end{bmatrix}$

Blok 2 = $\begin{bmatrix} S \\ C \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 1 & 4 \end{bmatrix} x \begin{bmatrix} 18 \\ 2 \end{bmatrix} = \begin{bmatrix} 56 \\ 26 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 4 \\ 0 \end{bmatrix} = \begin{bmatrix} E \\ A \end{bmatrix}$

Blok 3 = $\begin{bmatrix} A \\ S \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 5 & 4 \end{bmatrix} x \begin{bmatrix} 0 \\ 18 \end{bmatrix} = \begin{bmatrix} 18 \\ 72 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 18 \\ 20 \end{bmatrix} = \begin{bmatrix} S \\ U \end{bmatrix}$

Blok 4 = $\begin{bmatrix} A \\ R \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} x \begin{bmatrix} 0 \\ 17 \end{bmatrix} = \begin{bmatrix} 17 \\ 68 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 17 \\ 16 \end{bmatrix} = \begin{bmatrix} R \\ Q \end{bmatrix}$

Blok 5 = $\begin{bmatrix} J \\ A \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 9 & 4 \end{bmatrix} x \begin{bmatrix} 9 \\ 0 \end{bmatrix} = \begin{bmatrix} 9 \\ 81 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 9 \\ 3 \end{bmatrix} = \begin{bmatrix} J \\ D \end{bmatrix}$

Blok 6 = $\begin{bmatrix} N \\ A \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 7 & 4 \end{bmatrix} x \begin{bmatrix} 13 \\ 0 \end{bmatrix} = \begin{bmatrix} 13 \\ 91 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 13 \\ 13 \end{bmatrix} = \begin{bmatrix} N \\ N \end{bmatrix}$

Maka hasil *chipertextnya* adalah (E X E A S U R Q J D N N).

b. Dekripsi Menggunakan Algoritma Hill Cipher

Pesan teks yang disandikan sebelumnya akan disisipkan kedalam gambar menggunakan Teknik steganografi. Kemudian chipertext (E X E A S U R Q J D N N) tersebut dikembalikan seperti semula atau didekripsiskan menggunakan algoritma hill cipher sebagai berikut:

Diketahui:

Blok 1 = $\begin{bmatrix} E \\ X \end{bmatrix}$ dengan K1 = $\begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix}$, maka

1. Det K = (2 x 3) – (1 x 5) = 1
2. Nilai invers Modulo 1^{-1} mod 26

   K = 1 = $\frac{26(1)+1}{1}$ = 27
3. Invers Kunci

   $K^{-1} = \begin{bmatrix} 3 & -1 \\ -5 & 2 \end{bmatrix}$
4. Mariks kunci *hill cipher*

   $27\ x \begin{bmatrix} 3 & -1 \\ -5 & 2 \end{bmatrix} = \begin{bmatrix} 81 & -27 \\ -135 & 54 \end{bmatrix}$ Mod 26 = $\begin{bmatrix} 3 & 25 \\ 21 & 2 \end{bmatrix}$
5. Dekripsi *hill cipher*

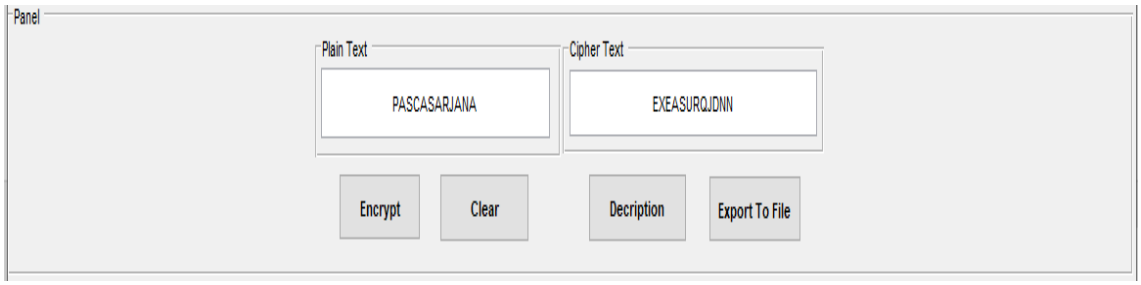
   $\begin{bmatrix} 3 & 25 \\ 21 & 2 \end{bmatrix} x \begin{bmatrix} 4 \\ 23 \end{bmatrix} = \begin{bmatrix} 587 \\ 130 \end{bmatrix}$ Mod 26 = $\begin{bmatrix} 15 \\ 0 \end{bmatrix}$

   $\begin{bmatrix} 15 \\ 0 \end{bmatrix} = \begin{bmatrix} P \\ A \end{bmatrix}$

Selanjutnya dengan proses yang sama dari blok 1 untuk mendapatkan hasil blok 2 sampai dengan blok 6 menggunakan algoritma *hill cipher*.

c. Implementasi Enkripsi Menggunakan Algoritma Hill Cipher

Dengang menggunakan Bahasa Pemograman MATLAB hasil algoritma *Hill Cipher* dapat dilihat pada Gambar 1 :

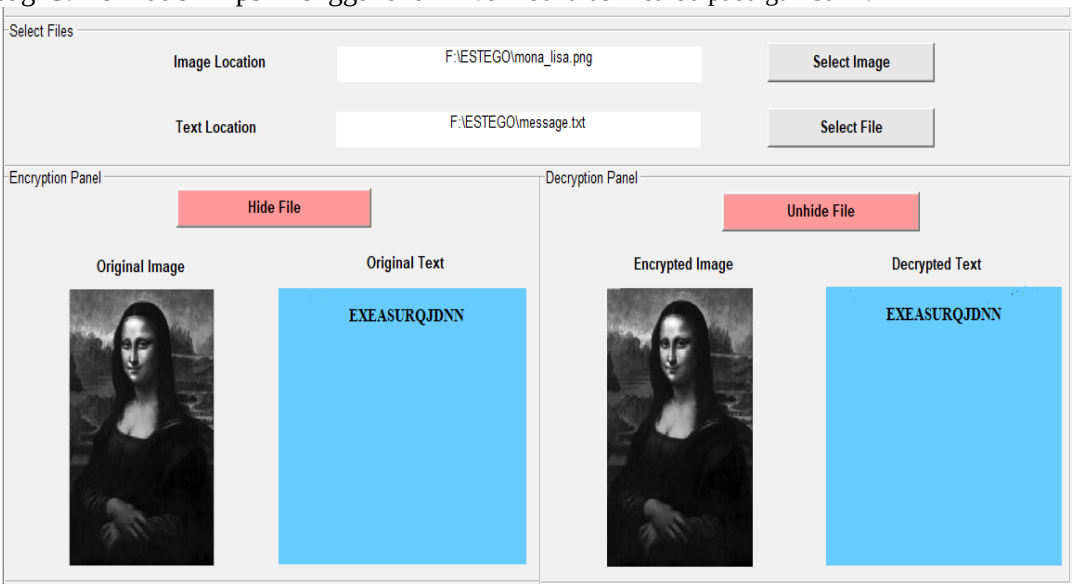


Gambar 1 Hasil Enkripsi Hill Cipher

Pada gambar 1 terdapat buttom encrypt, clear, description dan Export to File, fungsi enport to file adalah dengan menyimpan chipertext ke dalam sebuah notepad yang akan disisipkan kedalam gambar menggunakan algoritma Five Modhulus Method.

3.2 *Algoritma Five Modhulus Method*

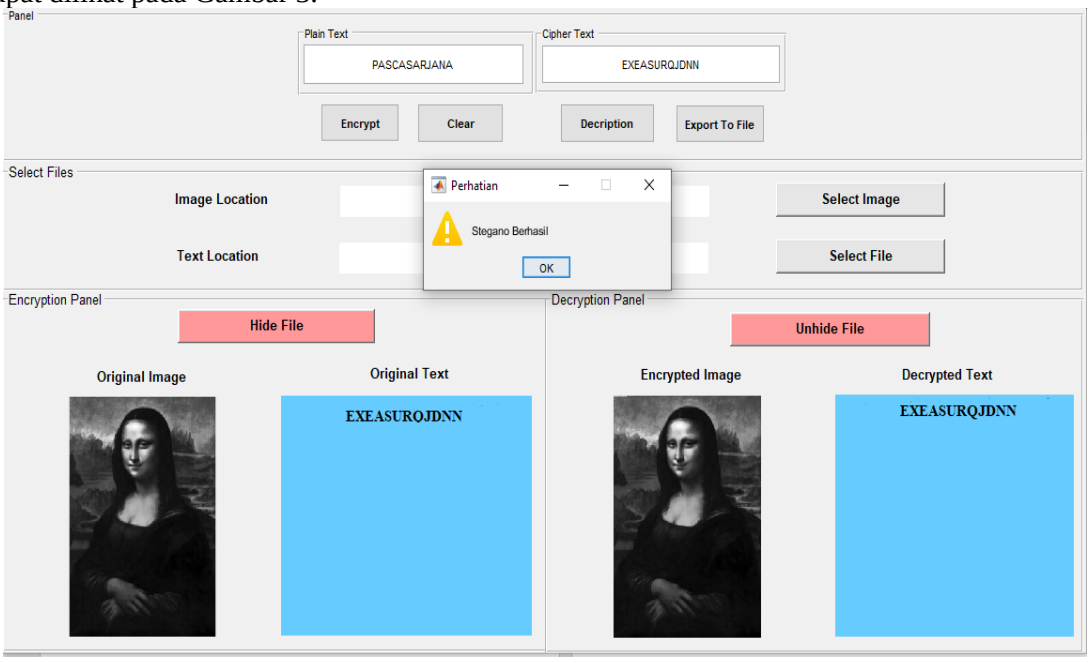
Algoritma Five Modhulus Method membagi gambar menjadi setiap blok k x k pixel. Diketahui setiap pixel pada bi-level gery images memiliki memiliki nilai antara 0 sampai 255. Meskipun jika dapat diubah setiap nilai yang ada pada rentang teserbut menjadi nilai yang dapat dibagi 5. Berikut enkripsi menggunakan Five Modhulus Method pada gambar 2.



Gambar 2. Hasil enkripsi dan deskripsi Algoritma Five Modhulus Method

Pada gambar 2 *ciphertext* yang disimpan kedalam notepad telah disisipkan kedalam gambar monalisa.png dengan dimensions 250 x 360 pixel. Besaran gambar sebelum disisipkan *chipertext* adalah 38,9 Kb namun setelah disisipkan *chipertext* berubah menjadi 55,8 Kb namun tetap memiliki dimensions yang sama.

Selanjutnya tampilan keseluruhan dari kombinasi *Hill Cipher* dan *Five Modulus Method* dapat dilihat pada Gambar 3.



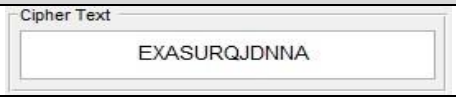
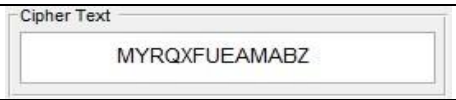
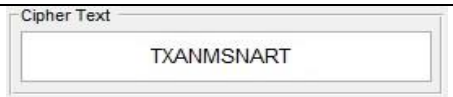
Gambar 3 Kombinasi Hill Cipher dan Five Modulus Method

Pada Gambar 3 menampilkan keseluruhan fungsi dari masing-masing algoritma yang dibuat dalam satu form menu.

3.3 *Pengujian*

Pengujian akurasi dengan mencocokkan hasil enkripsi *hill cipher* pada sistem dengan data perhitungan manual. Pengujian dilakukan sebanyak lima (5) kali yaitu dengan memasukkan *plaintext* yang berbeda pada tiap-tiap pengujian dapat dilihat pada tabel 4.

Tabel 4. Pengujian Tingkat Akurasi

No	Plaintext	Hasil enkripsi Manual	Hasil enkripsi Sistem	Hasil Uji (%)
1	PASCASARJANA1	EXEASURQJDNNA		100
2	MODIFIKASI 12.	MYRQXFUEAMABZ		100
3	AAAAAAAAAA	TXANMSNART		100
4	ATURAN	TFZKNA		100
5	AMIKOM, KAMPUS WUNGU.	MKIWCOPKSIWAPSIQASDKW		100
Rata-rata hasil uji akurasi				100%

Berdasarkan pengujian pada Tabel 4 dengan kunci kode telepon tersebut tidak ditemukan perbedaan hasil enkripsi maupun dekripsi sehingga didapatkan tingkat akurasi untuk algoritma ini sebesar 100 %.

Kemudian peneliti melakukan pengujian gambar pada Five Modulus Method dengan mencoba 4 gambar dengan ukuran dan tipe gambar yang berbeda didapatkan perubahan kapasitas gambar yang tidak terlalu besar pada tabel 5.

Tabel 5. Hasil Pengujian Gambar

No	Nama File	Ukuran File Asli (Byte)	Hasil Enkripsi Ukuran Gambar (Byte)	Selisih Ukuran Gambar (Byte)
1	Mona_lisa.png	39.881	57.211	17.330
2	Earth_(16530938850).jpg	1.051.749	1.241.899	190.150
3	giphy.gif	208.614	320.453	111.839
4	smiley.bmp	354.870	474.436	119.566

Hasil pengujian gambar pada tabel 5 menampilkan perbedaan ukuran ketika disisipkan teks yang sudah di enkripsi. Selisih pada setiap gambar ditampilkan untuk mengetahui ukuran file yang telah disisipkan teks.

4. KESIMPULAN

Pada penelitian ini, beberapa kesimpulan yang diperoleh adalah:

a. Pada awalnya plaintext di enkripsi dengan menggunakan algoritma hill cipher dengan kunci menggunkana kode telepon. Hasil ciphertext kemudian akan disisipkan pada gambar dengan menggunakan algoritma Five Modulus Method.
b. Berdasarkan hasil tingkat akurasi yang dilakukan pengujian sebanyak lima (5) kali terhadap *plaintext* yang berbeda didapatkan tingkat akurasi sebesar 100% yaitu tidak ditemukan perbedaan hasil enkripsi ataupun dekripsi.
c. Ukuran gambar pada Five Modulus METHOD yang telah disisipkan pesan rahasia tidak banyak mengalami perubahan dengan melakukan empat (4) kali pengujian untuk ukuran file gambar yang berbeda-beda. Namun selalu mendapatkan penambahan ukuran file bila disisipkan pesan yang sudah di enkripsi melalui hill cipher.

5. SARAN

Saran untuk penelitian selanjutnya adalah, dapat dilakukan pengembangan terhadap metode yang di usulkan, sehingga tidak hanya dapat enkripsi text saja, tetapi dapat enkripsi file, serta steganografi yang dilakukan tidak terbatas pada file image saja, namun dapat dilakukan dalam file yang berbentuk video dan media lainnya.

DAFTAR PUSTAKA

[1] Dony Ariyus, 2008, Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi, Andi Offset.

[2] Swain G. and Lanka S. K., 2012, A Quick review of Network Security and Steganography, *International Journal of Electronics and Computer Science Engineering*, vol. 1, no. 2, pp.426-435.

[3] Wang H and Wang S., 2004, Cyber warfare: Steganography vs. Steganalysis, Communications of the ACM, vol. 47, no. 10..

[4] Qazi, F., Khan, F.H., Agha, D.S., Khan, S.A., Rehman, S.U., 2019, Modification in Hill Cipher For Crtptogtraphic Application, *3C Tecnologia. Glosas de Innovacion aplicadas a la pyme*, ISSN: 2254-4143.

[5] Prasad, MG. V., Sundarayya, P., 2016, Generalized Self-Invertiblekey Generation Algorithm by using Reflection Matrix in Hill Cipher and Affine Hill Cipher, *International journal of pharmacy & Technology*. ISSN; 0975-766X.

[6] Jassim, F. A., 2013, A Novel Steganography Algorithm for Hiding Text in Image using Five Modulus Method, *International Journal of Computer Applications*, Volume 72 No. 17.

[7] Alkadi, I., Robert, S., 2017, Application and Implementation of Secure Hybrid Steganography Algorithm in Private Cloud Platform. *Journal of Computer Science Application and Information Technology*. DOI: http://dx.doi.org/10.15226/2474-9257/2/2/00105.

[8] Ariyus, D., Ardiansyah., 2019, Optimization Substitution Cipher and Hidden Plaintext in Image Data Using LSB Method, *Journal of Phisics: Conference Series*, Volume 1201.

[9] Qasem, M.H., Qatawneh, M., 2018, Parallel Hill Cipher Encryption Algoritm, *Inetrnational Journal of Computer Application*, Volume 179, No. 19.

[10] Joshi, K., 2018, A New Approach of Text Steganography Using ASCII Values, *International Journal of Engineering Research & Technology (IJERT)*, Vol. 7 Issue 5.
[11] S. Yunita, P. Hasan, and D. Ariyus, 2019, Modifikasi Algoritma Hill Cipher dan Twofish Menggunakan Kode Wilayah Telepon, *Sisfotenika*, vol. 9, no. 2, pp. 213–224.
[12] Jane Irma Sari, Sulindawaty, Hengki Tamando Sihotang, 2017, Implementasi Penyembunyian Pesan Pada Citra Digital dengan Menggabungkan Algoritma Hill Cipher dan Metode Least Significant BIT (LSB), *Jurnal Mantik Penusa*, Volume 1 No 2 Desember 2017
[13] Forouzan, Behrouz, 2006, Cryptography and Network Security, McGraw-Hill.
[14] Kaharuddin, E. Pawan, and D. Ariyus, 2019, Kombinasi Arnold Cat Map dan Modifikasi Hill Cipher Menggunakan Kode Bunyi Beep BIOS PHOENIX, *Sisfotenika*, vol. 9, no. 2, pp. 159–168.