

Implementasi Algoritma Hill Cipher untuk Proses Enkripsi dan Dekripsi Citra Berwarna dengan Modifikasi Padding

Dani Maulana Sholahudin¹, Asmunin²,

¹Jurusan Teknik Informatika/Fakultas Teknik, Universitas Negeri Surabaya

²Jurusan Teknik Informatika/Fakultas Teknik, Universitas Negeri Surabaya

danis3@mhs.unesa.ac.id

asmunin@unesa.ac.id

Abstrak— Teknologi digital yang berkembang menciptakan kemudahan untuk mengakses data digital misalnya foto yang telah disimpan dalam komputer. Namun di sisi lain perkembangan teknologi juga menimbulkan sebuah peluang kepada tindak kejahatan di dunia maya untuk mencuri data, mengubah data atau merusak data. Informasi yang penting akan menjadi sebuah masalah apabila jatuh di tangan orang yang salah dan tidak bertanggung jawab. Kriptografi sudah lama di pakai untuk keamanan data salah satunya adalah *hill cipher*. Pada penelitian ini penulis mencoba untuk membuat aplikasi keamanan data gambar dengan menggunakan algoritma *hill cipher* untuk enkripsi dan dekripsi gambar berwarna.

Pada penelitian ini algoritma *hill cipher* dengan modifikasi *padding* mampu mengenkripsi serta mendekripsi gambar dengan baik. Dengan adanya *padding* gambar tidak perlu di *resize* dan gambar murni dapat dienkripsi secara langsung. Kunci untuk enkripsi dan dekripsi gambar di masukan manual oleh pengguna agar memberikan keamanan yang kuat. Algoritma ini mampu mengenkripsi gambar dengan kecepatan kurang dari 1 detik namun kunci matriks harus matriks invertible. *hill cipher* dapat membaca beberapa ekstensi gambar misalnya jpg, png, tiff dan bmp.

Kata Kunci— Hill Cipher, Enkripsi, Dekripsi, Ekstensi, Kriptografi Simetris, Padding, Gambar

I. PENDAHULUAN

Informasi sangat penting maknanya dalam kehidupan dan menjadi komoditas yang sangat penting karena dengan adanya informasi dapat mengetahui data atau fakta dengan jelas dan mudah dimengerti, begitupun sebaliknya tanpa informasi maka kehidupan hampir semuanya tidak dapat dilakukan dengan baik. Seiring dengan berkembangnya informasi maka ancaman terhadap informasi itu sendiri semakin berkembang pula. Ancaman dalam hal keamanan data merupakan usaha seseorang yang ingin memperoleh akses-akses ilegal terhadap jaringan dan data tersebut. Pentingnya nilai dari data dan informasi mengakibatkan hanya boleh diakses oleh orang tertentu, apalagi jika data dan informasi tersebut merupakan aset bernilai yang harus dilindungi dengan perlindungan yang aman. Pada keamanan jaringan sangat diperlukan untuk menanggulangi ancaman tersebut sehingga membutuhkan sebuah penerapan mekanisme keamanan jaringan menggunakan teknik-teknik penyandian. Langkah-langkah untuk menjaga kerahasiaan data sangat dibutuhkan dengan

merancang sistem yang berfungsi untuk menjamin kerahasiaan data, mencegah informasi dari kasus penyadapan, serta menanggulangi informasi yang penting dan sensitif diambil oleh orang yang tidak berhak.

Kriptografi erat kaitannya dengan ilmu yang berdasarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data, dan *otentikasi* entitas [4]. Ilmu kriptografi sebenarnya telah lama digunakan yaitu sejak jaman sebelum mengenal metode pengiriman data menggunakan komputer bahkan sejak zaman romawi kuno sudah ada. Seiring dengan perkembangan teknologi telekomunikasi, maka semakin berkembang pula ilmu kriptografi baik jenis maupun fungsinya sebagai metode untuk enkripsi file teks maupun file citra. Di sini file citra digital atau gambar terkadang merupakan suatu aset yang berharga. Pada komputer, kebanyakan orang mempunyai file dengan tipe file dokumen dan gambar. Dengan ekstensi untuk dokumen yaitu doc, pdf, xlsx dan lain sebagainya, sementara untuk gambar yang memiliki ekstensi jpg, bmp, png, gif, dan tiff yang mana file-file tersebut masih dienkripsi dengan kunci simetris yaitu kunci yang digunakan untuk proses enkripsi dan proses dekripsi adalah kunci yang sama. Misalkan dalam kehidupan sehari-hari, terdapat suatu hasil pesanan desain yang masih tahap pengembangan yang perlu ditunjukkan kepada calon pembeli, gambar atau foto dokumentasi yang bersifat pribadi dan rahasia maka hal tersebut menjadi hal yang penting untuk diperhatikan keamanannya. Dengan uraian permasalahan tersebut maka salah satu upaya untuk mengamankan data yang berupa gambar warna adalah dengan melakukan penerapan suatu modifikasi algoritma kriptografi *hill cipher* terhadap enkripsi dan dekripsi gambar.

Dalam melakukan enkripsi dan dekripsi, berbagai cara pernah dilakukan sebelumnya. Penelitian yang dilakukan oleh Goutham, dkk yang berjudul “*Modified Hill Cipher Based Image Encryption Technique*”. Penelitian ini dilakukan untuk mengetahui tingkat keamanan dari Algoritma *Modified Hill Cipher* pada proses enkripsi dan dekripsi gambar. Proses enkripsi dimulai dengan proses mengonversikan gambar asli pada bentuk yang sesuai yaitu menjadi ukuran 256x256 piksel. Gambar hasil konversi ini kemudian dibagi menjadi 2x2 sub

matriks. Selanjutnya, men-generate matriks kunci berukuran 2x2 matriks. Proses selanjutnya dilakukan operasi aritmatika menggunakan matriks kunci, sehingga didapatkan gambar enkripsi. Untuk proses dekripsi gambar dilakukan dengan menggunakan matriks kunci yang sama dengan proses enkripsi. Pengujian pada Algoritma *Modified Hill Cipher* menghasilkan kesimpulan bahwa dari segi keamanan akan lebih baik, karena menggunakan kunci 128 bit, dimana didapatkan 2^{128} kombinasi, sehingga akan sulit dilakukan *brute force* [2].

Selain cara yang dijabarkan di atas terdapat cara yang pernah dilakukan sebelumnya dalam melakukan proses enkripsi dan dekripsi gambar. Penelitian yang dilakukan oleh Supiyanto, yang berjudul “Implementasi *Hill Cipher* Pada Citra Menggunakan *Koefisien Binominal* Sebagai Matriks Kunci”. Penelitian ini menggunakan koefisien koefisien binominal newton sebagai entri entri matriks kunci yang bertujuan untuk menentukan matriks kunci yang dijamin mempunyai invers. Koefisien binominal ini mempunyai aturan yang dikenal segitiga *pascal* yang berarti kunci yang digunakan selalu sama untuk satu matriksnya. Kesimpulan dari penelitian ini Koefisien koefisien binomial dapat dijadikan sebagai entri-entri dari matriks kunci. Matriks kunci yang dientri dibentuk dari koefisien binominal selalu mempunyai matriks invers karena determinan dari matriks kunci selalu sama dengan satu, penyandian citra *hill cipher* menunjukkan keteracakan warna yang signifikan yang berarti proses enkripsi berjalan dengan baik, proses dekripsi mengembalikan citra seperti semula [7].

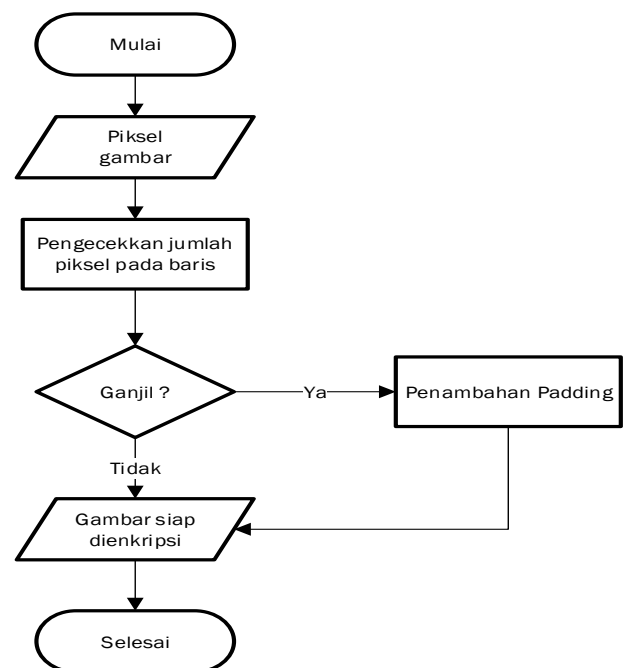
Selanjutnya penelitian juga pernah dilakukan oleh Deliana Br Tarigan yang berjudul “Implementasi Algoritma Kriptografi *Hill Cipher* Dalam Penyandian Data Gambar”. Pada penelitian ini penulis mencoba menjelaskan proses penyandian gambar dan merancang aplikasi untuk penyandian data gambar menggunakan metode *hill cipher*. Pada proses enkripsi kunci menggunakan matriks 2x2, kemudian *plaintext* dibagi menjadi beberapa blok untuk dilakukan pengoperasian menggunakan algoritma *hill cipher*. Untuk proses dekripsi hampir sama dengan proses enkripsi namun matriks kunci harus dibalik (*invers*). Kesimpulan dari penelitian ini adalah *hill cipher* dapat digunakan untuk penyandian gambar selain itu penerapan metode *hill cipher* dalam penyandian gambar adalah dengan mengubah nilai RGB menjadi bilangan desimal kemudian dienkripsi. Di dalam penelitian ini penulis menyertakan saran file gambar yang digunakan tidak hanya berekstensi jpg, karena dalam penelitian ini aplikasi penyandian data gambar hanya dapat digunakan pada file berekstensi .jpg [8].

II. METODOLOGI PENELITIAN

Dengan menggunakan algoritma *hill cipher* untuk proses enkripsi dan dekripsi citra menggunakan *padding*, maka enkripsi akan dilakukan pengujian yang meliputi pengaruh matriks kunci terhadap hasil enkripsi, pengaruh terhadap gambar *black white*, *grayscale*, RGB serta pegujian terhadap waktu dan ukuran gambar. Adapun proses tahapan yang dilakukan seperti pada Gbr 1.

A. Penambahan *Padding*

Berikut merupakan alur penambahan *padding* sebelum citra dienkripsi:



Gbr. 1 Alur Penambahan *Padding*

Penambahan *padding* dilakukan apabila jumlah piksel pada baris berjumlah ganjil, jika genap maka tidak perlu ditambahkan *padding*

Contoh

Jumlah piksel pada baris = 3, maka ditambahkan *padding*. Nilai *padding* sama dengan nilai piksel pada baris terakhir. Seperti Gbr 2.

Sebelum di padding			Sesudah di padding		
3,7,5	4,4,1	1,2,1	3,7,5	4,4,1	1,21
1,1,2	2,3,7	0,5,8	1,1,2	2,3,7	058
2,8,1	7,1,1	8,2,3	2,8,1	7,1,1	8,2,3
2,8,1	7,1,1	8,2,3	2,8,1	7,1,1	8,2,3

Gbr. 2 *Padding*

B. Proses Enkripsi

Pada Gbr 2 menunjukkan alur proses enkripsi dari sistem yang diajukan.



Gbr. 3 Alur Proses Enkripsi

Contoh pemecahan chanel citra sesuai RGB dapat dilihat pada Gbr 4.

	Red				Green				Blue		
R1	3	4	1	G1	7	4	2	B1	5	1	1
	1	2	0		1	3	5		2	7	8
R2	2	7	8	G2	8	1	2	B2	1	1	3
	2	7	8		8	1	2		1	1	3

Gbr. 4 Channel Citra

Proses enkripsi dilakukan dengan mengalikan nilai piksel tiap dua baris blok dengan matriks kunci, lalu *dimodulus 256*.

Misalnya :

Kunci	Piksel
-------	--------

$$R1 = \begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix} \times \begin{bmatrix} 3 & 4 & 1 \\ 1 & 2 & 0 \end{bmatrix} \% 256$$

Maka hasil dari R1 adalah

$$R1 = \begin{bmatrix} 15 & 22 & 4 \\ 12 & 18 & 3 \end{bmatrix}$$

Langkah perhitungan dilakukan juga pada 2 blok selanjutnya, G1, G2, B1, hingga B2, sehingga didapatkan hasil seperti Gbr 5.

Red			Green			Blue		
15	22	4	31	25	23	26	25	28
12	18	3	24	21	21	21	24	27
14	49	56	56	7	14	7	7	21
12	42	48	48	6	12	6	6	18

Gbr. 5 Hasil perhitungan

Kemudian channel digabungkan kembali dan mendapatkan gambar hasil enkripsi seperti pada Gbr 6.

RGB								
15,31,26	22,25,25	4,23,28						
12,24,21	18,21,24	3,21,27						
14,56,7	49,7,7	56,14,21						
14,56,7	49,7,7	56,14,21						

Gbr. 6 Hasil Enkripsi

C. Proses Dekripsi

Proses dekripsi merupakan proses dimana pengembalian *cipherimage* menjadi *plainimage* atau data seperti semula. Pada proses ini membutuhkan kunci *privat* yang mana hanya boleh di ketahui oleh orang yang dikehendaki saja, alur proses dekripsi dapat dilihat pada Gbr 7.



Gbr. 7 Alur Proses Dekripsi

Proses dekripsi sama seperti proses enkripsi namun tiap 2 blok channel RGB dilakukan pengalihan invers matriks kunci
Misalnya

$$\text{Matriks Kunci} = \begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix} \quad \text{Invers Matriks Kunci} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$$R1 = \begin{bmatrix} \text{Kunci} \\ 3 & -3 \\ -3 & 4 \end{bmatrix} \times \begin{bmatrix} \text{Piksel} \\ 15 & 22 & 4 \\ 12 & 18 & 3 \end{bmatrix} \% 256$$

maka hasilnya

$$R1 = \begin{bmatrix} 3 & 4 & 1 \\ 1 & 2 & 0 \end{bmatrix}$$

Proses perhitungan dilanjutkan sesuai chanel maka akan dihasilkan seperti pada Gbr. 8.

Red			Green			Blue		
3	4	1	7	4	2	5	1	1
1	2	0	1	3	5	2	7	8
2	7	8	8	1	2	1	1	3
2	7	8	8	1	2	1	1	3

Gbr. 8 Hasil Perhitungan

kemudian channel digabungkan kembali seperti Gbr. 9.

RGB		
3,7,5	4,4,1	1,2,1
1,1,2	2,3,7	0,5,8
2,8,1	7,1,1	8,2,3
2,8,1	7,1,1	8,2,3

Gbr. 9 Hasil Perhitungan

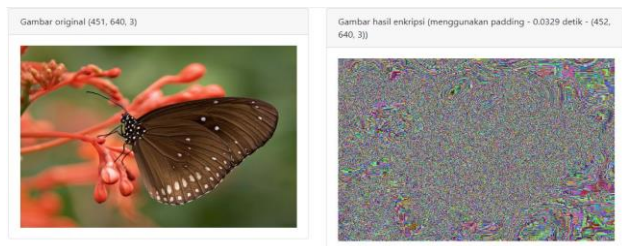
III. HASIL DAN PEMBAHASAN

Aplikasi ini dibuat menggunakan *python*, pada Gbr. 10 merupakan tampilan aplikasi enkripsi dan dekripsi gambar berwarna dengan modifikasi *padding*

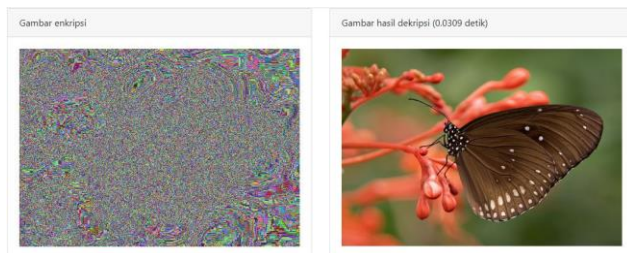
Gbr. 10 Tampilan awal

Di dalam tampilan awal enkripsi pengguna dapat memilih untuk menjadikan gambar sebagai enkripsi atau untuk melakukan dekripsi. Untuk melakukan enkripsi pengguna memasukan kunci matriks 2x2 sedangkan untuk melakukan dekripsi pengguna memasukan kunci matriks 2x2 yang telah ditentukan oleh pengguna ketika melakukan enkripsi pada gambar tersebut.

Tampilan gambar saat enkripsi yang ditunjukkan pada Gbr.11, sedangkan untuk proses dekripsi ditunjukkan pada Gbr. 12.



Gbr.11 Enkripsi



Gbr. 12 Dekripsi

A. Data

Tahap awal dalam penelitian ini adalah melakukan persiapan data, masing masing gambar mempunyai kode sebagai identitas. Pada Tabel 1 ditunjukkan data gambar yang akan dijadikan sebagai penelitian.

TABEL I
DATA GAMBAR

Kode	Gambar	Tipe
G01		.bmp
G02		.jpg
G03		.png
G04		.tiff
G05		.jpg

B. Hasil Pengujian

1. Pengujian Berdasarkan Kunci

Pada tahap pertama pengujian enkripsi dilakukan untuk menguji kunci matriks yang digunakan sebagai enkripsi gambar. Pengujian ini bertujuan untuk mengetahui perbedaan kunci yang dimasukan. Hasil dari

pengujian kunci matriks algoritma *hill cipher* dapat dilihat berdasarkan Tabel 2 :

TABEL 2
PENGUJIAN KUNCI

No	Plain Image	Kunci Matriks (Chiper Image)				
		1 1 1 2	4 3 3 3	49 78 54 65	73 39 46 35	588 485 323 276
1						
2						
3						
4						
5						

Berdasarkan hasil pengujian kunci pada tabel 8 dapat disimpulkan bahwa kunci yang dimasukan akan mempengaruhi hasil dari enkripsi

2. Pengujian Berdasarkan Dimensi

Pada tahap ini dilakukan pengujian terhadap dimensi. Pada pengujian ini bertujuan untuk mengetahui peran dari *padding*. Berikut adalah pengujian dimensi yang dapat dilihat pada Tabel 3

TABEL 3
PENGUJIAN DIMENSI

No	Image Kode	Plain Image	Chiper Image
1	G01	1280 x 720	1280 x 720
2	G02	640 x 451	640 x 452 Menggunakan padding
3	G03	512 x 512	512 x 512
4	G04	256 x 256	256 x 256
5	G05	400 x 333	400 x 334 Menggunakan padding

Berdasarkan hasil dari pengujian yang ditunjukkan pada tabel 3 dapat disimpulkan bahwa pada gambar yang memiliki baris piksel ganjil maka pada proses enkripsi akan ditambahkan *padding* piksel sedangkan pada gambar dengan jumlah baris piksel genap tidak ditambahkan *padding* piksel.

3. Pengujian Berdasarkan Waktu

Berdasarkan hasil percobaan waktu enkripsi terhadap gambar yang telah dipersiapkan sebelumnya dengan menggunakan kunci matriks yang sama dengan tujuan

untuk mengetahui kecepatan dalam enkripsi dan dekripsi gambar dengan menggunakan algoritma hill cipher menggunakan spesifikasi laptop asus a442ur intel core i5 dengan RAM 4 Gb ,maka dapat dapat diperoleh hasil yang dapat dilihat pada tabel 4 :

TABEL 4
PENGUJIAN WAKTU




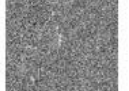






No	Plain Image	Penguian Ke- (detik)					Rata-rata (detik)
		1	2	3	4	5	
1	G01	0.0878 detik	0.0868 detik	0.0848 detik	0.0827 detik	0.0967 detik	0.08776 detik
2	G02	0.0359 detik	0.032 detik	0.0319 detik	0.0329 detik	0.0319 detik	0.03292 detik
3	G03	0.0369 detik	0.0319 detik	0.0429 detik	0.0369 detik	0.0319 detik	0.0361 detik
4	G04	0.0249 detik	0.012 detik	0.012 detik	0.014 detik	0.015 detik	0.01558 detik
5	G05	0.019 detik	0.024 detik	0.0329 detik	0.0229 detik	0.0199 detik	0.02374 detik

Berdasarkan hasil pengujian tabel 4 dapat disimpulkan bahwa hasil dari pengujian waktu menggunakan algoritma hill cipher, hasil pengujian memerlukan waktu kurang dari 1 detik untuk semua gambar yang telah dilakukan pengujian.

4. Pengujian Tipe Gambar

Gambar pada data yang telah dipersiapkan sebelumnya menggunakan tipe gambar yang berbeda dengan demikian pengujian dapat mengetahui hasil dari masing masing tipe gambar dan mengetahui perbedaan dari masing masing tipe gambar. Berikut merupakan hasil dari pengujian tipe gambar :

TABEL 5
PENGUJIAN TIPE IMAGE

No	Plain Image	Tipe Gambar	Jenis Gambar	Chiper Image
1		.jpg	RGB	
2		.tiff	Grayscale	
3		.jpg	Black and white	
4		.png	RGB	
5		.bmp	RGB	











Berdasarkan hasil pengujian pada tabel 5 dapat disimpulkan bahwa hasil yang diperoleh dari pengujian ini adalah untuk tipe gambar .jpg, .tiff, .png, .bmp dapat dienkripsi dengan menggunakan algoritma hill cipher,

namun untuk jenis gambar Black and white hasil enkripsi tidak dapat menghasilkan hasil yang baik.

5. Pengujian Dekripsi

Berdasarkan tabel 6 pengujian terhadap hasil enkripsi (chiper image) yang bertujuan untuk mengetahui hill cipher dapat mengembalikan cipher image kembali ke gambar semula (plain image). Berikut hasil pengembalian chiper image ke plain image :

TABEL 6
PENGUJIAN DEKRIPSI

No	Cipher Image	Plain Image
1		
2		
3		
4		
5		

Berdasarkan hasil pengujian pada Tabel 6 dapat disimpulkan bahwa chiper image dapat dikembalikan menjadi gambar awal dengan baik menggunakan algoritma hill cipher

6. Pengujian Perubahan Chiper Image

Berdasarkan hasil enkripsi perlu dilakukan pengujian terhadap perubahan gambar. Tujuan dari pengujian ini adalah untuk mengetahui hasil enkripsi jika dilakukan perubahan terhadap gambar. Perubahan tersebut meliputi brightness, watermark dan resize dari hasil enkripsi. Pada Tabel 7 merupakan hasil dari pengujian.

TABEL 7
PERUBAHAN CIPHER

Kode	Brightness	Resize	Watermark
G01 CHIPER	GAGAL DIKEMBALIKAN	GAGAL DIKEMBALIKAN	GAGAL DIKEMBALIKAN
G02 CHIPER	GAGAL DIKEMBALIKAN	GAGAL DIKEMBALIKAN	GAGAL DIKEMBALIKAN
G03 CHIPER	GAGAL DIKEMBALIKAN	GAGAL DIKEMBALIKAN	GAGAL DIKEMBALIKAN
G04 CHIPER	GAGAL DIKEMBALIKAN	GAGAL DIKEMBALIKAN	GAGAL DIKEMBALIKAN
G05 CHIPER	GAGAL DIKEMBALIKAN	GAGAL DIKEMBALIKAN	GAGAL DIKEMBALIKAN

- [5] Supiyanto, S. (2015, December). Implementasi Hill Cipher Pada Citra Menggunakan Koefisien Binomial Sebagai Matriks Kunci. In *Seminar Nasional Informatika (SEMNASIF)* (Vol. 1, No. 1).
- [6] Tarigan, D. B. (2014). Implementasi Algoritma Kriptografi Hill Cipher dalam Penyandian Data Gambar. Teknik Informatika STMIK Budi Darma Medan. *Jurnal Informatika*, 7(2), 76-81.

Berdasarkan hasil pengujian pada Tabel 7 dapat disimpulkan bahwa hasil enkripsi gagal untuk dikembalikan atau gagal didekripsi karena cipher telah terjadi perubahan pada *cipher image*, perubahan ini mengakibatkan nilai piksel yang berubah pada gambar hasil enkripsi.

IV. KESIMPULAN

Berdasarkan hasil dan pembahasan, dapat disimpulkan bahwa algoritma *hill cipher* untuk setiap kunci yang dimasukan akan berpengaruh pada hasil enkripsi, semakin tinggi angka matriks yang dimasukan maka semakin kuat segi keamanannya atau hasil enkripsi semakin tidak beraturan pikselnya. *Padding* juga berperan baik untuk metode ini karena setiap gambar tidak perlu *resize*. Algoritma *hill cipher* mampu mengenkripsi gambar dengan cepat dengan kecepatan kurang dari 1 detik. Untuk tipe gambar algoritma ini dapat digunakan untuk beberapa tipe gambar tetapi untuk jenis gambar lebih maksimal untuk gambar yang bervariasi banyak dan tidak maksimal untuk gambar black and white. Algoritma *hill cipher* dapat mengembalikan hasil enkripsi dengan baik jika kunci yang dimasukan sesuai.

Algoritma *hill cipher* tidak dapat mengembalikan hasil enkripsi yang sudah mengalami perubahan karena merubah nilai piksel pada gambar hasil enkripsi.

UCAPAN TERIMA KASIH

Puji syukur penulis kepada Tuhan Yang Maha Esa yang telah memberikan kemudahan dan kelancaran sehingga penulis dapat menyelesaikan artikel ini. Terima kasih untuk orang tua yang selalu mendoakan agar artikel ini segera terselesaikan dan tidak lupa kepada teman teman yang telah membantu mensukseskan untuk penyelesaian artikel ini.

REFERENSI

- [1] Goutham L, Mahendra M S, Manasa AP, Mr Prajwalasimha SN. (2017). Modified Hill Cipher Based Image Encryption Technique, *ijasret Volume 5* (issue IV)
- [2] R. Sadikin, Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java, Yogyakarta: Penerbit Andi, 2012
- [3] Renaldi, Y., Zarkasi, A., & Prasetyo, A. P. P. (2019). *DETEKSI KEMATANGAN PADA BUAH TOMAT BERDASARKAN WARNA BUAH MENGGUNAKAN WEBCAM* (Doctoral dissertation, Sriwijaya University).
- [4] Reza, S., & Juliasari, N. (2018). PENERAPAN KRIPTOGRAFI PADA APLIKASI SECURE-MAIL BERBASIS WEB MENGGUNAKAN ALGORITMA CAESAR CIPHER DAN RC4. *SKANIKA*, 1(1), 229-236