Kriptografi Teks dan Citra dengan Menggunakan Algoritma *Hill Cipher* pada Perangkat Android

Josua Freddy Orlando Siahaan, Aris Puji Widodo

Jurusan Ilmu Komputer/ Informatika, Fakultas Sains dan Matematika, Universitas Diponegoro
[1]siahaanjosua@gmail.com, [2]arispw@gmail.com

Abstract

Text files and images is one form of information is often exchanged. This exchange process does not guarantee that the file that is sent is not free from the threat of modification and duplication. Therefore the safety data from text files and images must be maintained in order to guarantee confidentiality and authenticity so that no misuse of the information would adversely affect certain parties. This thesis explores cryptography text and images using algorithms Hill Cipher on android devices. Hill Cipher algorithm selected for their turnaround times are not long enough and suitable for text or image file. The system runs on mobile devices that use the Android operating system. The results of this system is the ciphertext and cipherimage that can't be understood simply. The level of randomness ciphertext and cipherimage depending on the key is inserted. The more complex the key is inserted, the more randomly generated file so that the level of security of the files are also getting better.

Keywords **:** *Text, Image, Algorithm Hill Cipher, Cryptography, Android*

Abstrak

File teks dan citra merupakan salah satu bentuk informasi yang sering dipertukarkan. Proses pertukaran ini tidak menjamin bahwa *file* yang dikirimkan tidak lepas dari ancaman modifikasi dan duplikasi. Oleh karena itu keamanan data dari *file* teks dan citra harus terjaga agar dapat terjamin kerahasiaannya dan keasliannya sehingga tidak terjadi penyalahgunaan informasi yang akan merugikan pihak tertentu. Tugas akhir ini membahas tentang kriptografi teks dan citra menggunakan algoritma *Hill Cipher* pada perangkat android. Algoritma *Hill Cipher* dipilih karena waktu pemrosesannya yang tidak cukup lama dan cocok digunakan untuk *file* teks atau citra. Sistem ini berjalan pada perangkat *handphone* yang menggunakan sistem operasi android. Hasil dari sistem ini adalah *ciphertext* dan *cipherimage* yang tidak dapat dimengerti dengan kasat mata. Tingkat keacakan *ciphertext* dan *cipherimage* tergantung pada *key* yang dimasukkan. Semakin kompleks *key* yang dimasukkan maka semakin acak *file* yang dihasilkan sehingga tingkat keamanan dari *file* tersebut juga semakin bagus.

Kata kunci **:** Teks, Citra, Algoritma *Hill Cipher*, Kriptografi, Android

1. Pendahuluan

Perkembangan teknologi komunikasi dan informasi yang sangat pesat memberikan pengaruh besar bagi kehidupan manusia. Seiring dengan berkembangnya teknologi, maka proses pengiriman data dapat dilakukan dengan mudah dan melalui berbagai macam media yang ada, antara lain melalui media internet dengan menggunakan fasilitas *e-mail*, melalui transfer data antar perangkat *mobile* (*handphone*, PDA, dan *flashdisk*) maupun dengan teknologi radio *frequency* (*bluetooth*, IrDA, GPRS) hingga menggunakan jaringan computer [6].

Perkembangan yang pesat dalam proses pengiriman data membawa dampak yang sangat besar, yaitu masalah keamanan data yang dikirim. Kerahasiaan dan keamanan saat melakukan pertukaran data adalah hal yang sangat penting dalam komunikasi, baik untuk tujuan keamanan bersama, maupun untuk privasi individu. Keamanan jaringan menjadi faktor penting seiring dengan jumlah pertukaran data pada internet yang terus bertambah setiap harinya [5].

Agar data-data yang dikomunikasikan tidak diketahui oleh pihak-pihak yang tidak berkepentingan maka dicari cara untuk mengamankan data tersebut. Salah satu metode untuk menjaga keamanan data tersebut adalah dengan menyandikan isi dari data tersebut. Kriptografi memegang peranan yang sangat penting dalam menyandikan data, baik data yang bersifat teks maupun digital. Dalam kriptografi, terdapat dua proses penting, yaitu enkripsi dan dekripsi. Enkripsi adalah suatu metode yang digunakan untuk mengkodekan data sedemikan rupa sehingga keamanan informasinya terjaga dan tidak dapat dibaca tanpa didekripsi terlebih dahulu. Sedangkan dekripsi adalah kebalikan dari enkripsi [4].

Salah satu teknik penyandian dalam kriptografi adalah teknik kriptografi klasik. Dalam kriptografi klasik terdapat dua teknik dasar yang biasanya digunakan yaitu teknik substitusi dan teknik transposisi. Teknik substitusi dilakukan dengan penggantian setiap karakter teks asli dengan karakter lain. Sedangkan teknik transposisi dilakukan dengan menggunakan permutasi karakter. Teknik substitusi juga dibagi menjadi empat bagian yaitu *monoalphabetic cipher, homophonic cipher, polyalphabetic cipher* dan *polygram cipher.* Beberapa contoh teknik substitusi adalah Caesar *cipher* dan vigenere *cipher*. Selain teknik tersebut masih ada teknik kriptografi lainnya, yaitu *hill cipher*. *Hill cipher* termasuk kepada algoritma kriptografi klasik yang sangat sulit dipecahkan apabila hanya mengetahui berkas *ciphertext* saja. Karena *hill cipher* tidak mengganti setiap abjad yang sama pada *plaintext* dengan abjad lainnya yang sama pada *ciphertext* [3].

Penelitian ini akan menggunakan file berupa teks dan citra yang akan disandikan dengan menggunakan salah satu algoritma dari kriptografi yakni algoritma *hill cipher* dan dilakukan di salah satu sistem operasi yang digunakan oleh perangkat seluler yakni Android. Adapun untuk hasil akhirnya berupa *cipher-file* atau file teks maupun file citra yang sudah disandikan. Kemudian *cipher-file* yang telah dihasilkan dapat diubah kembali ke dalam bentuk teks dan citra asal dengan melalui proses dekripsi terlebih dahulu.

2. Dasar Teori

Sistem ini dikembangkan dengan metode-metode pendukung untuk melakukan proses penyadian teks dan citra.

2.1. Kriptografi

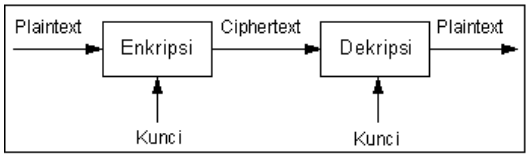
Kriptografi berasal dari bahasa yunani yaitu *kryptos* (tersembunyi atau rahasia) dan *graphien* (menulis) secara harafiah berarti salah satu metode untuk menjamin kerahasiaan dan integritas dari suatu informasi [4]. Kriptografi adalah seni atau sains yang meliputi prinsip-prinsip dan metode mengubah pesan dimengerti (*plaintext*) menjadi satu pesan yang tidak dapat dimengerti (*ciphertext*) dan kemudian mengubah pesan kembali ke bentuk aslinya [1].

Pada prinsipnya, kriptografi memiliki 4 komponen utama yaitu :

1. *Plaintext*, yaitu pesan asli yang dapat dibaca.
2. *Ciphertext*, yaitu pesan acak yang tidak dapat dibaca.
3. *Key*, yaitu kunci untuk melakukan teknik kriptografi.
4. *Algorithm*, yaitu metode untuk melakukan enkripsi dan dekripsi.

Sedangkan di dalam kriptografi terdapat dua proses dasar yang digunakan yaitu :

1. Enkripsi, yaitu sebuah proses menjadikan pesan yang dapat dibaca (*plaintext*) menjadi pesan acak yang tidak dapat dibaca (*ciphertext*).
2. Dekripsi, yaitu proses kebalikan dari enkripsi dimana proses ini akan mengubah pesan acak yang tidak dapat dibaca (*ciphertext*) menjadi pesan yang dapat dibaca (*plaintext*) dengan menggunakan algoritma ‘pembalik’ dan *key* yang sama. Alur proses enkripsi dan dekripsi dapat dilihat di gambar 2.1.



Gambar 2.1 Ilustrasi Sistem Kriptografi

2.2. Citra Digital

Agar dapat diolah dengan komputer digital, maka suatu citra harus direpresentasikan secara numerik dengan nilai-nilai diskrit. Representasi citra dari fungsi kontinu menjadi nilai-nilai diskri disebut digitalisasi. Citra yang dihasilkan inilah yang disebut citra digital [2]. Pada umumnya citra digital berbentuk persegipanjang, dan dimensi ukurannya dinyatakan sebagai tinggi x lebar atau lebar x panjang.

Citra digital yang tingginya N, lebarnya M, dan memiliki L derajat keabuan dapat dianggap sebagai fungsi *f(x,y)*, dengan $0 \le x \le N$, $0 \le y \le M$ dan $0 \le f \le L$ [2].

Citra digital yang berukuran N x M lazim dinyatakan dengan matriks yang berukuran N baris dan M kolom sebagai berikut :

$$f(x,y)=\begin{bmatrix} f(0,0) & f(0,1) & \dots & f(0,M-1) \\ f(1,0) & f(1,1) & \dots & f(1,M-1) \\ \vdots & \vdots & \vdots & \vdots \\ f(N-1,0) & f(N-1,1) & \dots & f(N-1,M-1) \end{bmatrix} \quad \dots\dots\dots\dots\dots(1)$$

Indeks baris (i) dan indeks kolom (j) menyatakan suatu koordinat titik pada citra, sedangkan f(i, j) merupakan intensitas (derajat keabuan) pada titik (i, j). Masing-masing elemen pada citra digital (berarti elemen matriks) disebut *image element*, *picture element* atau *pixel* atau *pel.* Jadi, citra yang berukuran N x M mepunyai NxM buah *pixel.*

Proses digitalisasi citra ada dua macam :

1. Digitalisasi spasial (x, y), sering disebut sebagai penerokan.
2. Digitalisasi intensitas f(x, y), sering disebut sebagai kuantisasi.

2.3. Algoritma Hill Cipher

Kriptografi memiliki banyak metode yang bisa digunakan untuk memanipulasi warna pada citra maupun memanipulasi teks. Salah satunya adalah dengan menggunakan metode kriptografi klasik yaitu algoritma *Hill Cipher*. Algoritma *Hill Cipher*, yaitu sebuah teknik penyandian dengan menggunakan ide perkalian matriks yang ditemukan oleh Leister S. Hill pada tahun 1929. *Hill Cipher* disini akan bekerja untuk perkalian matrik baris dengan matrik kolom.

Dalam algoritma Hill Cipher, setiap karakter yang ada dalam *plaintext* terlebih dahulu dikonversi menjadi angka, seperti A=0, B=1, hingga Z=25. Sedangkan kunci pada algoritma ini adalah matriks n x n dengan n merupakan ukuran blok. Jika matriks kunci disebut sebagai M, maka matriks M adalah sebagai berikut:

$$K = \begin{bmatrix} k11 & k12 & ... & k1n \\ k21 & k22 & ... & k2n \\ ... & ... & ... & ... \\ kn1 & kn2 & ... & knn \end{bmatrix} \text{…….....……(2.2)}$$

Matriks K yang digunakan sebagai kunci harus merupakan matriks yang *invertible*, yaitu memiliki *multiplicative inverse* K^{-1} sehingga $K*K^{-1} = I$ [1].

Dalam proses enkripsi, *plaintext* yang ada dirubah ke dalam bentuk blok-blok secara berurutan sesuai dengan ukuran matriks kunci [1]. Misalkan matriks kunci K merupakan matriks berordo 3 x 3, maka persamaan yang dihasilkan :

$C_1 = (K_{11}P_1 + K_{12}P_2 + K_{13}P_3) \bmod 26$
$C_2 = (K_{21}P_1 + K_{22}P_2 + K_{23}P_3) \bmod 26$ ……(2.3)
$C_3 = (K_{31}P_1 + K_{32}P_2 + K_{33}P_3) \bmod 26$

Bentuk diatas juga dapat dinyatakan dalam bentuk vektor kolom dan matriks, yaitu:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \text{…….(2.4)}$$

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

Sehingga dapat disimpulkan bentuk umum dari proses enkripsi dan dekripsi adalah sebagai berikut:

1. Enkripsi

$C = K(P)$ ……(2.5)

2. Dekripsi

$P = K^{-1}(C)$ ……..(2.6)

2.4. Android

Android adalah sistem operasi berbasis Linux yang dirancang untuk perangkat seluler layar sentuh seperti telepon pintar dan computer tablet. Android awalnya dikembangkan oleh Android, Inc., dengan dukungan finansial dari Google. Sistem operasi ini dirilis secara resmi pada tahun 2007.

Perangkat android yang merupakan *open source* (sumber terbuka) dan lisensi perizinan yang terbuka memungkinkan perangkat lunak untuk dimodifikasi secara bebas dan didistribusikan oleh para pembuat perangkat, dan pengembang aplikasi. Faktor tersebut yang telah memberikan kontribusi terhadap perkembangan Android, menjadikannya sebagai sistem operasi telepon yang paling banyak digunakan di dunia.

Aplikasi Android dikembangkan dalam bahasa pemrograman Java dengan menggunakan kit pengembangan perangkat lunak Android (SDK). SDK ini terdiri dari seperangkat perkakas pengembangan, termasuk *debugger*, perpustakaan perangkat lunak, *emulator* headset, dokumentasi, kode sampel, dan tutorial. Android juga didukung secara resmi oleh lingkungan pengembangan terpadu yaitu Android Studio.

3. Analisis dan Perancangan Aplikasi

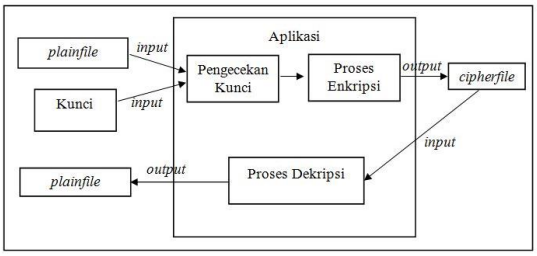
Aplikasi Kriptografi Teks dan Citra dengan Menggunakan Algoritma *Hill Cipher* pada Perangkat Android merupakan aplikasi yang digunakan untuk menyembunyikan pesan berupa teks dan citra. Aplikasi ini dapat membantu pengguna untuk mengamankan teks dan citra sehingga orang lain yang tidak berwenang tidak dapat mengetahui dan memahami informasi dalam citra tersebut. Aplikasi ini dikembangkan pada Android.

3.1. Arsitektur Aplikasi

Aplikasi Kriptografi *file* teks dan citra dengan menggunakan Algoritma *Hill Cipher* dikembangkan berbasis *mobile*. Aplikasi ini dapat membantu pengguna untuk mengamankan *file* sebelum melakukan pengiriman *file* tersebut sehingga orang lain yang tidak berkepentingan tidak dapat mengetahui dan memahami informasi yang terdapat di dalam *file* tersebut.

Aplikasi ini terdiri atas empat fitur utama yaitu enkripsi teks, enkripsi citra, dekripsi teks dan dekripsi citra. Dalam pengenkripsiannya proses enkripsi teks dan enkripsi citra tidak jauh berbeda. Perbedaan yang utama terletak di *file* inputan, enkripsi teks menginputkan *file* teks sedangkan enkripsi citra menginputkan *file* citra. Secara sederhana pengertian enkripsi teks dan enkripsi citra adalah sebagai berikut. Proses enkripsi teks mengubah *file* teks yang diinputkan menjadi *file* yang tidak dapat dibaca (*ciphertext*) dan proses enkripsi citra mengubah *file* citra yang diinputkan menjadi *file* yang tidak dapat dibaca (*cipherfile*).

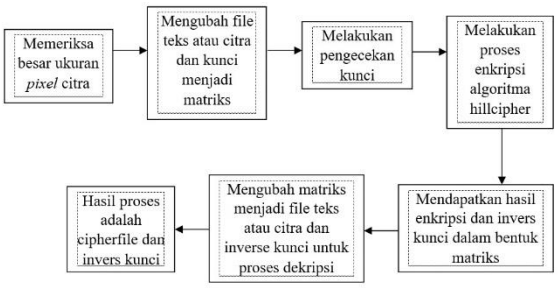
Pada proses dekripsi teks dan dekripsi citra, *ciphertext* atau *cipherfile* diinputkan kemudian dilakukan proses dekripsi, *output* dari proses dekripsi teks adalah *plaintext* dan *output* dari dekripsi citra adalah *plainfile.* Secara garis besar, alur enkripsi dan dekripsi *file* dengan menggunakan algoritma *Hill Cipher* ditunjukkan pada gambar 3.1 :



Gambar 3.1. Deskripsi Umum Aplikasi Kriptografi *File* Teks dan Citra dengan menggunakan Algoritma *Hill Cipher*

3.2. Alur Proses Enkripsi

Alur kerja proses enkripsi teks dan citra menggunakan algoritma *hillcipher* digambarkan pada Gambar 3.2



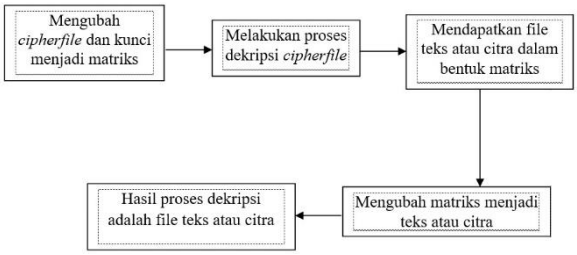
Gambar 3.2. Alur Kerja Proses Enkripsi *File* Teks atau Citra

Alur proses enkripsi *file* teks atau citra pada gambar 3.2 dijelaskan sebagai berikut:

1. Memeriksa besar ukuran *pixel* citra
   Proses pertama yang dilakukan dalam enkripsi adalah memeriksa besar ukuran citra yang diinputkan. Misalnya besar ukuran *pixel* citra yang akan diinputkan adalah 900x900, maka aplikasi akan memberikan peringatan untuk mengganti citra karena maksimal besar ukuran *pixel* yang diperbolehkan adalah 800x800. Pemeriksaan besar ukuran *pixel* ini hanya untuk citra saja, sedangkan untuk teks tidak ada pemeriksaan besar ukuran sehingga untuk teks langsung dilanjutkan ke proses selanjutnya.
2. Mengubah *file* teks atau citra dan kunci menjadi matriks
   Setelah memeriksa besar ukuran (untuk citra), aplikasi kemudian membaca *file* yang diinputkan dan mengubahnya ke dalam bentuk matriks angka yang nantinya siap digunakan untuk pemrosesan enkripsi dengan algoritma *hill cipher*.
3. Melakukan pengecekan kunci
   Kunci yang diinputkan juga memililki kriteria tertentu, karena kunci yang digunakan harus dibentuk ke dalam matriks 3x3, maka panjang karakter untuk kunci adalah harus 9 karakter. Selain itu determinan kunci yang diinputkan tidak boleh sama dengan nol. Apabila determinan kunci sama dengan nol, maka kunci tidak memiliki invers, dan enkripsi hanya bisa dilakukan searah tanpa dapat melakukan dekripsi kembali. Jika kunci yang diinputkan kurang atau lebih dari 9 karakter, serta determinan kunci sama dengan nol maka akan muncul peringatan untuk mengganti kunci yang diinputkan.
4. Melakukan proses enkripsi algoritma *hill cipher*
   File dan kunci yang telah diubah ke dalam bentuk matriks selanjutnya diproses enkripsi dengan algoritma *hill cipher*. Pemrosesan dilakukan dengan mengalikan matriks kunci dengan matriks dari *file* yang diinputkan. Setelah itu dilanjutkan dengan proses modulo, dimana untuk teks dilakukan modulo 26 dan untuk citra dilakukan modulo 256.
5. Mendapatkan hasil enkripsi dan *invers* kunci dalam bentuk matriks
   Hasil dari proses enkripsi adalah *cipherfile* dan *invers* kunci dalam bentuk matriks. Selanjutnya *cipherfile* dan *invers* kunci ini akan diubah ke dalam bentuk *array*.
6. Mengubah matriks menjadi teks atau citra dan *inverse* kunci untuk proses dekripsi
   Matriks dari *cipherfile* kemudian akan dirubah ke dalam bentuk *array*. Jika awalnya merupakan sebuah teks, maka array yang dibentuk adalah *array* 1 dimensi. Sedangkan untuk citra, array yang dibentuk merupakan *array* dua dimensi berdasarkan panjang dan lebarnya (x,y). *Inverse* kunci yang awalnya sebuah matriks diubah menjadi array dan array yang isinya angka diubah menjadi *array* huruf untuk mendapatkan kunci dekripsi.
7. Hasil proses adalah *cipherfile* dan *invers* kunci
   Hasil dari proses yang dilakukan pada alur enkripsi ini adalah sebuah *cipherfile* dan *invers* kunci untuk proses dekripsi nantinya

3.3. Alur Proses Dekripsi

Alur Kerja Proses Dekripsi teks dan citra dengan menggunakan algoritma *hill cipher* dijelaskan oleh Gambar 3.3



Gambar 3.3. Alur Kerja Proses Enkripsi *File* Teks atau Citra

Alur kerja proses enkripsi *file* teks atau citra (Gambar 3.3) dijelaskan sebagai berikut:

1. Mengubah *cipherfile* dan kunci menjadi matriks
   File teks atau citra dan kunci (*invers* kunci enkripsi) yang diinputkan diubah ke dalam bentuk matriks terlebih dahulu.
2. Melakukan proses dekripsi *cipherfile*
   Setelah diubah ke dalam bentuk matriks, proses selanjutnya adalah mendekripsi *cipherfile* dengan cara mengalikan kembali matriks kunci dengan matriks *cipherfile*.
3. Mendapatkan *file* teks atau citra dalam bentuk matriks
   Hasil dari perkalian matriks kunci dengan matriks *cipherfile* dilanjutkan dengan proses modulo. Untuk teks dilakukan proses modulo 26 dan untuk citra dilakukan proses modulo 256.
4. Mengubah matriks menjadi teks atau citra
   Matriks hasil perkalian diubah ke dalam array. Untuk *file* teks diubah ke dalam array 1 dimensi sedangkan untuk citra diubah ke dalam array 2 dimensi. Kemudian array angka *file* teks diubah menjadi huruf dan array angka *file* citra diubah menjadi derajat keabuan citra.
5. Hasil proses dekripsi adalah *file* teks atau citra
   Hasil proses dekripsi adalah *file* teks atau citra awal.

4. Analisis Hasil Penelitian

Tahap analisis hasil merupakan bahasan dari tiap kejadian yang terjadi dalam kasus uji pada penelitian. Untuk data yang ditampilkan pada bahasan pada sub-bab ini hanya berupa sampel dari setiap kejadian yang terjadi dalam penelitian Kriptografi Teks dan Citra dengan Menggunakan Algoritma *Hill Cipher* pada Perangkat Android.

4.1. Hasil Proses Enkripsi Teks

Proses enkripsi teks merupakan proses untuk menyandikan teks sehingga menghasilkan teks yang acak dan tidak menampilkan informasi apapun. Hasil enkripsi teks dapat dilihat pada Tabel 4.3.

Tabel 4.3. Hasil Enkripsi Teks

No	*Plaintext*	Kunci	Waktu Enkripsi	*Ciphertext*
1	enkripsiteks	sanfoundr	0,030518 ms	umbhdgzkjuay
2	enkripsiteks	bbabcbbdd	0,030518 ms	rovzwiabvoqk
3	kriptografi	sanfoundr	0,030517 ms	ygfkxweizmhl
4	kriptografi	bbabcbbdd	0,030517 ms	bahipkxofnvd
5	penyandiantek	sanfoundr	0,030518 ms	xbmdqncxlaviyya
6	penyandiantek	bbabcbbdd	0,030518 ms	tkoyllltbgdekkk

Dari tabel 4.3. dapat dilihat bahwa hasil enkripsi teks menghasilkan teks yang acak dan tidak memberikan informasi apapun. Kata kunci yang dimasukkan juga memberikan perbedaan hasil di *ciphertext* nya tetapi tidak memberikan perbedaan waktu yang cukup signifikan. Apabila total huruf pada teks yang dimasukkan dimodulo dengan angka 3 dan menghasilkan nilai 0, maka teks tersebut akan langsung dienkripsi tanpa adanya penambahan ataupun perubahan pada teks aslinya. Sedangkan untuk teks yang apabila total hurufnya dimodulo dengan angka 3 dan menghasilkan nilai 1, maka akan dilakukan penambahan dua buah huruf ‘a’ di akhir dari teks tersebut. Begitu juga untuk teks yang apabila total hurufnya dimodulo dengan angka 3 dan menghasilkan nilai 2, maka akan dilakukan penambahan satu buah huruf ‘a’ diakhir dari teks tersebut. Penambahan huruf ini dilakukan agar proses enkripsi dari teks tersebut seimbang karena matriks kunci yang digunakan merupakan matriks yang berordo 3x3.

4.2. Hasil Proses Dekripsi Teks

Proses dekripsi teks merupakan proses untuk mengembalikan teks acak menjadi teks asli yang mengandung informasi. Hasil enkripsi teks dapat dilihat pada Tabel 4.4.

Tabel 4.4. Hasil Dekripsi Teks

No	*Ciphertext*	Kunci	Waktu Dekripsi	*Plaintext*
1	umbhdgzkjuay	sanfoundr	0,030517 ms	enkripsiteks
2	rovzwiabvoqk	bbabcbbdd	0,030518 ms	enkripsiteks
3	ygfkxweizmhl	sanfoundr	0,030518 ms	kriptografia
4	bahipkxofnvd	bbabcbbdd	0,030517 ms	kriptografia
5	xbmdqncxlaviyya	sanfoundr	0,030517 ms	penyandiantekaa
6	tkoyllltbgdekkk	bbabcbbdd	0,030518 ms	penyandiantekaa

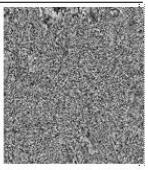
Dari tabel 4.4 dapat dilihat hasil dari dekripsi teks yang dilakukan. Teks ‘kriptografi’ yang dimasukkan memiliki total huruf 11 dan apabila dimodulo dengan angka 3 menghasilkan sisa 2, maka untuk melengkapi sisa tersebut ditambahkan satu buah huruf ‘a’ diakhir sebelum dilakukan proses enkripsi. Sehingga didapatkan hasil dekripsi dari *ciphertext* yaitu ‘kriptografia’. Begitu juga dengan teks ‘penyandiantek’ yang dimasukkan memiliki total huruf 13 dan apabila dimodulo dengan angka 3 menghasilkan sisa 1, maka untuk melengkapi sisa tersebut ditambahkan dua buah huruf ‘a’ diakhir teks. Sehingga didapatkan hasil dekripsi dari *ciphertext* yaitu ‘pennyandiantekaa’. Sedankan untuk teks

'enkripsiteks' yang dimasukkan memiliki total huruf 12 dan apabila dimodulo dengan 3 menghasilkan sisa 0, maka tidak perlu adanya penambahan huruf. Sehingga didapatkan hasil dekripsi dari *ciphertext* yaitu 'enkripsiteks'.

4.3. Hasil Proses Enkripsi Citra

Proses enkripsi citra merupakan proses untuk menyembunyikan citra sehingga menghasilkan citra yang acak dan tidak menampilkan informasi apapun. Hasil enkripsi citra dapat dilihat pada Tabel 4.5.

Tabel 4.5. Hasil Enkripsi Citra

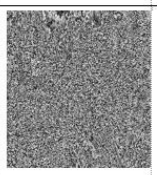
No	Nama File / Ukuran *Pixel*	Kunci	Waktu Enkripsi	Citra Asli	Citra Enkripsi
1	Lena512warna.bmp 512 x 512	sanfoundr	1,576 s		
2	Lena512warna.bmp 512 x 512	bbabcbbdd	1.461 s		
3	Lena.bmp 256 x 256	sanfoundr	0.555 s		
4	Lena.bmp 256 x 256	bbabcbbdd	0.503 s		

Dari tabel 4.5. dapat dilihat bahwa hasil enkripsi citra menghasilkan citra yang acak dan tidak memberikan informasi apapun. Hasil enkripsi pada tabel 4.5. terlihat perbedaan dari kunci yang dimasukkan. Citra yang menggunakan kunci 'sanfoundr' terlihat lebih acak daripada citra yang menggunakan kunci 'bbabcbbdd'. Hal ini dikarenakan kunci 'sanfoundr' memiliki nilai kompleksitas yang lebih banyak dibandingkan kunci 'bbabcbbdd'. Dari tabel 4.5. dapat kita lihat waktu enkripsi dari citra tersebut. Untuk citra yang berwarna memiliki waktu enkripsi yang lebih lama. Hal ini dikarenakan operasi perkalian matriks yang dilakukan untuk citra berwarna lebih banyak. Perkalian matriks untuk citra berwarna dilakukan pada tiap layernya, yaitu layer R(*red*), G(*green*), dan B(*blue*).

4.4. Hasil Proses Dekripsi Citra

Proses dekripsi citra merupakan proses untuk mengembalikan citra acak menjadi citra asli yang mengandung informasi. Hasil dekripsi citra dapat dilihat pada Tabel 4.6.

Tabel 4.6. Hasil Dekripsi Citra

No	Nama File / Ukuran *Pixel*	Kunci	Waktu Dekripsi	Citra Enkripsi	Citra Hasil Dekripsi
1	Lena512warna.bmp 512 x 512	sanfoundr	1,546 s		
2	Lena512warna.bmp 512 x 512	bbabcbbdd	1,526 s		
3	Lena.bmp 256 x 256	sanfoundr	0,489 s		
4	Lena.bmp 256 x 256	bbabcbbdd	0,441 s		

Dari tabel 4.6. dapat dilihat bahwa dekripsi citra menghasilkan citra yang sama dengan citra aslinya.

4.5. Hasil Pengujian

Berdasarkan pengujian yang telah dilakukan, proses enkripsi selalu menghasilkan *file* yang acak baik itu *file* teks maupun citra dan proses dekripsi selalu menghasilkan *file* asli sesuai dengan yang dimasukkan. Perbedaan kunci yang dimasukkan memberikan perbedaan pada tingkat keacakan pada *file* hasil enkripsi sehingga tidak memungkinkan untuk mengenkripsi dan mendekripsi sebuah *file* dengan kunci yang berbeda. Dalam pengenkripsian *file* teks memiliki batas dalam pemakaiannya. Jenis masukan teks yang dapat diproses hanya berupa huruf kecil dari 'a-z' dengan total 26 karakter. Sedangkan *file* citra yang dapat diproses hanya citra yang memiliki ukuran maksimal 800 x 800 *pixel*.

5. Kesimpulan

Kesimpulan yang dapat diambil dari penelitian mengenai Kriptografi Teks dan Citra menggunakan Algoritma *Hill Cipher* pada Perangkat Android :

1. Proses enkripsi citra dengan algoritma *hill cipher* menunjukkan keteracakan warna yang cukup signifikan, hal ini menunjukkan bahwa algoritma *hill cipher* termasuk algoritma yang aman untuk proses penyandian data.
2. Proses dekripsi membutuhkan *invers* dari kunci yang dimasukkan. Kunci yang tidak memliki *invers* tidak dapat digunakan dalam aplikasi ini. Apabila kunci yang tidak memiliki *invers* dimasukkan maka proses enkripsi dapat dilakukan tetapi proses dekripsi tidak akan menghasilkan *file* asli.
3. Dalam proses enkripsi *file* citra, apabila total *pixel* citra dimodulo dengan angka 3 dan menghasilkan sisa, maka sisa *pixel* tersebut tidak dienkripsi atau dengan kata lain tidak dikalikan dengan matriks kunci.
4. Tingkat keacakan citra hasil enkripsi bergantung pada indeks kunci yang digunakan. Indeks kunci yang digunakan dimulai dari nilai a=0, b=1, sampai dengan z=25. Semakin besar indeks kunci yang digunakan, maka semakin acak juga citra hasil enkripsi yang dihasilkan.
5. Waktu enkripsi dan dekripsi dari citra bergantung pada besar dari *pixel* citra yang dimasukkan. Semakin besar ukuran *pixel* dari citra, maka semakin lama juga waktu yang dibutuhkan untuk proses enkripsi dan dekripsi.

6. Referensi

[1] Acharya, B., Kumar, S. P., & Panda, G. (2010). Image Encryption Using Advanced Hill Cipher Algorithm. *ACEEE International Journal on Signal and Image Processing Vol. 1, No 1, Jan 2010.*

[2] Munir, R. (2004). *Pengolahan Citra Digital dengan Pendekatan Algoritmik.* Bandung: Penerbit Informatik Bandung.

[3] Munir, R. (2006). *Kriptografi.* Bandung: Institut Teknologi Bandung.

[4] Rahman, M. N., Abidin, A. F., & Usop, S. M. (2013). Cryptography : A New Approach of Classical Hill Cipher. *International Journal of Security and its Apllication Vol. 7, No. 2*, 180-190.

[5] Rahmani, M. K., Arora, K., & Pal, N. (2014). A Crypto-Steganography: A survey. *(IJACSA) International Journal of Advanced Computer Science and Application Vol. 5, No. 7*, 149-155.

[6] Utami, & Sukrisno. (2007). *Implementasi Steganografi EoF dengan Gabungan Enkripsi Rijndael, Shift Chiper dan Fungsi Hash.* Yogyakarta.

[7] T. Sutoyo, E. M. (2009). *Teori Pengolahan* Citra *Digital.* Yogyakarta: Penerbit Andi.

[8] Putra, D. (2010). *Pengolahan* Citra *Digital.* Yogyakarta: Penerbit Andi.