JISKa, Vol. 1, No. 2, September, 2016, Pp. 67 – 74
ISSN 2527 - 5836

PENGAMANAN DATA FOTO PADA PERANGKAT OS ANDROID MENGGUNAKAN TEKNIK KRIPTOGRAFI *HILL CIPHER*

Aris Puji Widodo [(1)], Eko Adi Sarwoko [(2)], Edy Suharto [(3)]), Josua Freddy Orlando Siahaan [(4)]
Departemen Ilmu Komputer/Informatika, Fakultas Sain dan Matematika, Universitas Diponegoro
Jl.Prof. Soedarto No. 1 Temablang Semarang
e-mail : arispw@gmail.com

Abstract

The development of information technology needs to be accompanied by a more rapid security system in use was. One of them is the security of the file photo (image) that is stored on the mobile device OS android. The mobile device is a potential loss due to theft or misused by others who are not responsible, so that the information stored on them are very risky to be known by others. Therefore, to reduce the risk of opening the photo data of personal information stored on mobile devices, we need a mechanism for data security efforts of the photo. Security mechanism that is done is by storing the photo into encryption format and if you want to reopen the original information needs to be done to restore from encryption format to original format (encryption and decryption). The encryption format photo files stored on android OS devices used in this research is to use hill cipher algorithm. Hill cipher algorithm is a mathematical function that is used to perform encryption and decryption. Hill cipher is a poly alphabetic cipher can be categorized as a block cipher, because image files are processed will be divided into a number of blocks of a certain size. Each block will affect each other blocks in the encryption and decryption process, so that each block of the same is not mapped into the same block as well. In this study, also conducted measurement accuracy, performance encryption and decryption process by using a file size of photos and android OS devices vary.

The results of encryption and decryption process photo files generated in this study, will produce the photo file size larger than the original photo file. While the level of randomness information to each photo file encryption is done depends on the key index used. The larger the key index is used, the higher the degree of randomness of the encrypted photo file is generated.

Keywords : Cryptography, Hill Chiper, photo, Android, Mobile

Abstrak

Perkembangan teknologi informasi yang semakin cepat perlu dibarengi dengan sistem pengamanan dalam pemanfaatanya. Salah satu diantaranya adalah keamanan data-data file foto (citra) yang di simpan pada perangkat mobile OS android. Perangkat mobile sangat berpotensi terjadi kehilangan akibat pencurian atau disalahgunakan oleh pihak lain yang tidak bertanggung jawab, sehingga informasi yang tersimpan didalamnya sangat beresiko untuk diketahui oleh pihak lain. Oleh karena itu, untuk mengurangi resiko terbukanya informasi data foto pribadi yang tersimpan di perangkat mobile, diperlukan sebuah upaya mekanisme pengamanan data foto tersebut. Mekanisme pengamanan yang dilakukan adalah dengan cara menyimpan data foto tersebut ke dalam format sandi dan jika ingin membuka kembali informasi aslinya perlu dilakukan dengan mengembalikan dari format sandi ke format semula (enkripsi dan dekripsi). Adapun format sandi file foto yang disimpan di perangkat OS android yang digunakan pada penelitian ini adalah menggunakan algoritma hill chiper. Algoritma hill chiper adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan dekripsi. Hill cipher yang merupakan poly alphabetic cipher dapat dikategorikan sebagai block cipher, karena file foto yang diproses akan dibagi menjadi sejumlah blok dengan ukuran tertentu. Hasil proses enkripsi dan dekripsi file foto yang dihasilkan pada penelitian ini, akan menghasilkan ukuran file foto yang lebih besar dibandingkan dengan file foto aslinya. Sedangkan tingkat keacakan informasi pada file foto yang dilakukan enkripsi sangat tergantung pada indek kunci yang digunakan. Semakin besar indeks kunci yang digunakan, maka akan semakin tinggi tingkat keacakan file foto hasil enkripsi yang dihasilkan.

Kata Kunci : Kriptografi, *Hill Chiper*, Foto, Android, *Mobile*

1. PENDAHULUAN

Perkembangan teknologi informasi, terutama pada penyimpanan data yang disimpan pada sebuah device memungkinkan untuk dilakukan proses pemberian keamanan terhadap data itu sendiri. Mekanisme keamanan ini bertujuan untuk melindungi data terhadap pihak-pihak atau oleh orang yang tidak berkepentingan. Salah satu teknik yang digunakan untuk memberikan jaminan keamanan pada sebuah data yang tersimpan pada sebuah device adalah dapat dilakukan dengan menggunakan teknik kriptografi, dengan cara melakukan transformasi data asli ke dalam bentuk tertentu (bentuk sandi), sehingga data tersebut tidak mudah dimengerti oleh pihak lain (Acharya, 2010). Kriptografi memiliki 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 (Rahmani, 2014).

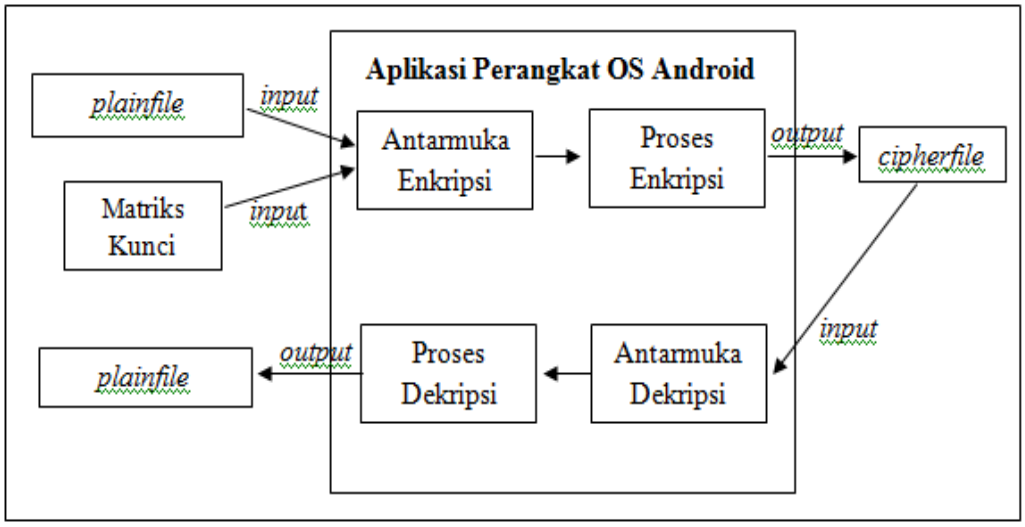
Dengan menggunakan kriptografi dapat memberikan jaminan keamanan dari data yang di simpan pada sebuah *device*. Maksudnya adalah pada saat melakukan penyimpanan data pada sebuah *device* sebaiknya dilakukan proses enkripsi terlebih dahulu, hal ini dapat mencegah terjadinya penyerangan ataupun pencurian terhadap data tersebut (Putra, 2010). Kemudian jika ingin melihat isi data yang asli perlu dilakukan proses dekripsi untuk mentransformasikan kembali dari data dalam bentuk sandi ke dalam data bentuk aslinya (Sutoyo, 2010; Utami, 2007).

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 (Rahman, 2013). 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 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* (Munir, 2006).

Penelitian ini akan menggunakan *file* berupa *file* foto (dapat juga disebut dengan citra) yang tersimpan pada perangkat OS Android yang akan disandikan dengan menggunakan algoritma *hill cipher*. Adapun untuk hasil akhirnya berupa *cipher-file* atau *file* foto yang sudah disandikan. Kemudian *cipher-file* yang telah dihasilkan dapat diubah kembali ke dalam bentuk foto aslinya dengan melalui proses dekripsi. Demikian juga pada penelitian ini akan dilakukan pengukuran akurasi kebenaran proses deskripsi dan kinerjanya dengan menggunakan data f*ile* foto dan *device* OS android yang bervariasi, sehingga dapat digunakan untuk menyajikan spesifikasi standart perangkat yang digunakan untuk melakukan penyandian terhadap ukuran *file* foto yang digunakan.

2. METODE PENELITIAN

Tahapan yang digunakan pada penelitian ini, secara garis besar terdiri dari proses enkripsi, dan dekripsi citra. Adapun tahapan yang digunakan pada penelitian ini diberikan pada Gambar 1. sebagai berikut:



Gambar 1. Rancangan Penelitian

a. Menentukan *Plainfile* dan Matriks Kunci Simetris

Plainfile yang digunakan adalah *file* foto yang tersimpan pada perangkat OS android, dimana *file* foto inilah yang akan dienkripsikan. Pada penelitian ini *file* foto yang digunakan adalah sebuah *file* dalam format *file* RGB dengan ekstensi JPG dan BMP. Matriks kunci adalah *key* yang digunakan untuk mengenkripsi *plainfile.* Matriks kunci yang digunakan adalah matriks berordo 3 x 3 dan merupakan matriks yang *invertible* atau matriks yang memiliki *invers.* Hal ini diharuskan karena apabila matriks kunci yang digunakan tidak memiliki *invers,* maka *cipherfile* yang dihasilkan tidak dapat didekripsi.

b. Tahapan Algoritma Enkripsi

Berikut ini adalah algoritma untuk enkripsi sepertiyang diberikan pada Gambar 2:

1. *Input* file foto yang tersimpan pada perangkat OS android.
2. *Input* matriks kunci yang akan digunakan sebagai *key*.
3. Proses Enkripsi *Hill Cipher*.
4. *Output Cipherfile* yang sudah terenkripsi

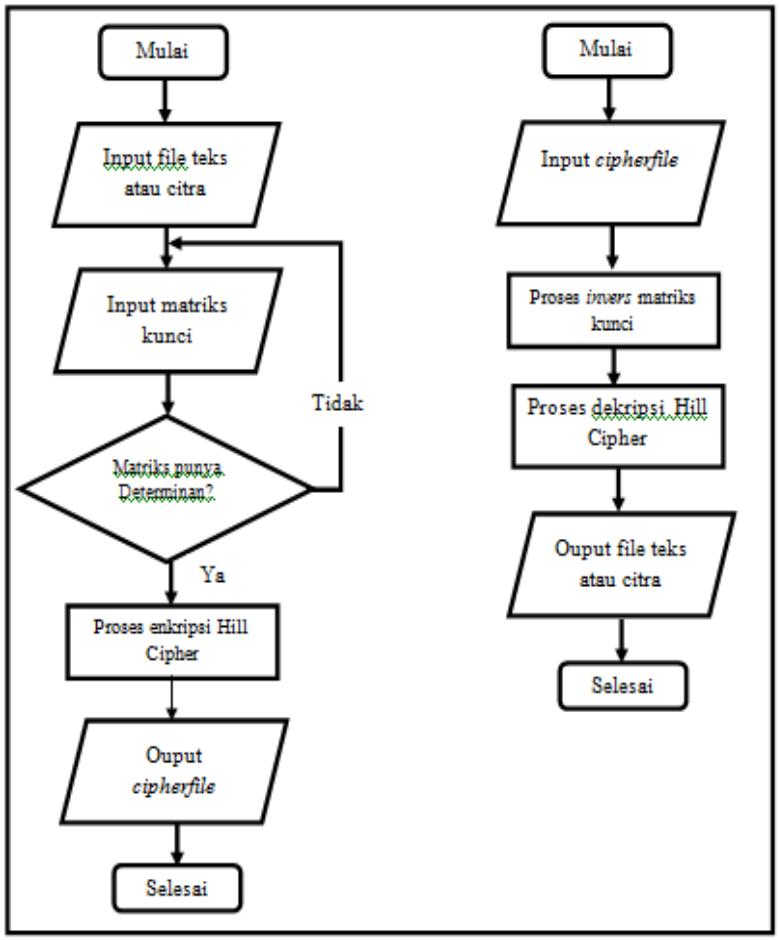
c. Tahapan Algoritma Dekripsi

Berikut ini adalah algoritma untuk dekripsi seperti yang diberikan pada Gambar 2:

1. *Input Cipherfile*.
2. *Input* matriks kunci yang digunakan.
3. Proses mencari *invers* dari matriks kunci.
4. Proses Dekripsi *Hill Cipher*.
5. *Output* file foto yang tersimpan pada perangkat OS android.

d. Pengukuran Akurasi dan Kinerja

Pengukuran akurasi kebenaran proses deskripsi dilakukan dengan membandingkan matrik *file* foto asli dengan *file* foto hasil dekripsi, sedangkan proses pengukuran kinerja enkripsi dan dekripsi dengan menggunakan algoritma *hill chipper* dilakukan dengan mengukur lamanya waktu eksekusi yang terjadi. Pada bagian ini dilakukan dengan menggunakan perangkat android dan ukuran *file* foto yang bervariasi dengan tujuan untuk memberikan justifikasi kelayakan.



Gambar 2. Proses Enkripsi (Kiri) dan Dekripsi (Kanan)

3. HASIL DAN PEMBAHASAN

3.1. PROSES ENKRIPSI FOTO

Proses enkripsi citra menggunakan algoritma *hill cipher* dilakukan dengan tahapan 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.
2. **Mengubah citra dan kunci menjadi matriks** Setelah memeriksa besar ukuran (untuk citra), aplikasi kemudian membaca *file* yang diinputkan dan mengubah 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. Selainitu determinan kunci yang diinputkan tidak boleh sama dengan nol. Apabila determinan kunci samadengan 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 samadengan nol maka akan muncul peringatan untuk mengganti kunci yang diinputkan.

4. **Melakukan proses enkripsi algoritma *hillcipher***
   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*, untuk citra dilakukan dengan menggunakan *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 sebuah *array*.
6. **Mengubah matriks menjadi citra dan *inverse* kunci untuk proses dekripsi**
   Matriks dari *cipherfile dari sebuah citra* kemudian dirubah menjadi bentuk *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 tahapan enkripsi ini adalah sebuah *cipherfile* dan *invers* kunci yang digunakan untuk proses dekripsi

3.2. PROSES DEKRIPSI FOTO

Proses dekripsi citra menggunakan algoritma *hill cipher* dilakukan dengan tahapan sebagai berikut:

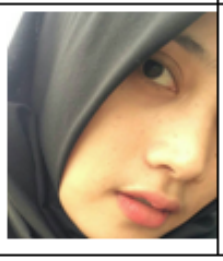
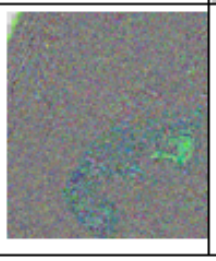
1. **Mengubah *cipherfile* dan kunci menjadi matriks**
   File teks atau citra dan kunci (*invers* kunci enkripsi) yang diinputkan diubah ke dalam bentuk sebuah matriks..
2. **Melakukan proses dekripsi *cipherfile***
   Setelah diubah kedalam bentuk matriks, proses selanjutnya adalah mendekripsi *cipherfile* 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* dari sebuah citra dilanjutkan dengan proses *modulo* 256.
4. **Mengubah matriks menjadi citra**
   Matriks hasil perkalian diubah ke dalam *array* 2 dimensi. Kemudian *array* angka *file* citra diubah menjadi derajat keabuan citra.
5. **Hasil proses dekripsi adalah *file* citra**
   Hasil dari proses dekripsi adalah *sebuah* citra asli.

3.3. HASIL ENKRIPSI DAN DEKRIPSI FOTO

Proses enkripsi citra merupakan proses untuk menyembunyikan citra sehingga menghasilkan citra yang acak dan tidak menampilkan informasi apapun. Berdasarkan Tabel 1 dapat dilihat bahwa hasil enkripsi citra menghasilkan citra yang acak dan tidak memberikan informasi secara lebih lengkap. Hasil enkripsi yang diberikan pada tabel 1 tampak sebuah perbedaan hasil enkripsinya berdasarkan 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**". 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***). Proses dekripsi citra merupakan proses untuk mengembalikan citra acak menjadi citra asli yang mengandung informasi secara lengkap. Hasil dekripsi citra dapat diberikan pada Tabel 1.

Kemudian untuk melakukan pengukuran akurasi dan kinerja dari proses enkripsi dan dekripsi dari aplikasi yang telah dihasilkan pada penelitian ini, maka dilakukan eksperimen dengan ukuran file yang bervariasi. Berdasarkan file-file yang bervariasi tersebut diatas pada saat dilakukan proses enkripsi dan dekripsi dilakukan pengukuran terhadap perubahan ukuran file dan lamanya waktu proses enkripsi dan dekripsinya. Ukuran file hasil enkripsi akan menjadi lebih besar, karena pada file asli akan ditambahi informasi yang digunakan untuk melakukan pengacakan dari *file* aslinya. Demikian pula *file* hasil proses dekripsinya juga memiliki ukuran *file* yang lebih besar dari *file* aslinya yang digunakan sebagai sumber, dan minimal ukuran *file*-nya sama dengan *file* hasil proses enkripsi. Hasil eksperimen untuk pengukuran lamanya waktu eksekusi juga dilakukan dengan menggunakan variasi dimensi dan ukuran file foto. Masimum file foto yang digunakan pada penelitian ini adalah file dengan dimensi 800x800 dengan ukuran 1.7 MB. Adapun dengan ukuran file maksimum tersebut lamanya waktu eksekusi sebesar 3. 988-an *second*. Adapun hasil eksperimen proses enkripsi dan dekripsi diberikan pada Tabel 2.

Tabel 1. Hasil Enkripsi Dan Dekripsi Foto

No	Nama File / Ukuran *Pixel*	Kunci	Citra Asli	Citra Enkripsi	Citra Hasil Dekripsi
1	Baboon24.bmp 512 x 512	sanfoundr			
2	Bird.bmp 256 x 256	sanfoundr			
3	Peppers512 warna.bmp 512 x 512	sanfoundr			
4	Wanita.jpg 747 x 747	sanfoundr			

Tabel 2. Hasil Proses Enkripsi dan Dekripsi Foto

No	Citra	Kunci (Key)	Dimensi Citra	Ukuran Citra Asli (MB)	Ukuran Citra Hasil Enkripsi (MB)	Ukuran Citra Hasil Dekripsi (MB)	Type	Waktu Enkripsi (S)	Waktu Dekripsi (S)
1	Wanita.jpg	sanfoundr	747 x 747	0.04	1.64	1.64	RGB	3.022	3.338
2	Makanan.jpg	sanfoundr	777 x 780	0.12	1.77	1.77	RGB	3.302	3.293
3	Bayi.jpg	sanfoundr	772 x 786	0.08	1.77	1.77	RGB	3.498	3.490
4	Bird.bmp	bbabcbbdd	256 x 256	0.06	0.19	0.25	Grayscale	0.474	0.446
5	Boat.bmp	bbabcbbdd	512 x 512	0.25	0.77	0.77	Grayscale	1.525	1.512
6	Camera.bmp	bbabcbbdd	256 x 256	0.06	0.19	0.19	Grayscale	0.404	0.455
7	Circles.bmp	bbabcbbdd	256 x 256	0.06	0.19	0.19	Grayscale	0.454	0.426
8	Goldhill.bmp	bbabcbbdd	256 x 256	0.06	0.19	0.19	Grayscale	0.401	0.452
9	San.bmp	bbabcbbdd	256 x 256	0.06	0.19	0.19	Grayscale	0.467	0.414
10	Lena.bmp	bbabcbbdd	256 x 256	0,06	0.19	0.19	Grayscale	0.503	0.441
11	Baboon24.bmp	bbabcbbdd	512 x 512	0.75	0.77	0.77	RGB	1.520	1.480
12	Girl-warna-.bmp	bbabcbbdd	256 x 256	0.06	0.19	0.19	RGB	0.402	0.573
13	Lenawarna.bmp	bbabcbbdd	512 x 512	0.75	0.77	0.77	RGB	1.552	1.535
14	Pepperswarna.bmp	bbabcbbdd	512 x 512	0.75	0.77	0.77	RGB	1.482	1.516
15	Orang.png	bbabcbbdd	732 x 732	1.41	1.57	1.57	RGB	2.988	2.941
16	Wanita.jpg	bbabcbbdd	747 x 747	0.04	1,64	1,64	RGB	3.022	3.338
17	Makanan.jpg	bbabcbbdd	777 x 780	0.12	1.77	1.77	RGB	3.278	3.307
18	Bayi.jpg	bbabcbbdd	772 x 786	0.08	1.77	1.77	RGB	3.307	3.311

Berdasarkan eksperimen yang telah dilakukan, maka proses enkripsi selalu menghasilkan *file* citra yang selalu dalam bentuk acak, dan pada proses dekripsi selalu menghasilkan *file* asli sesuai dengan file sumber yang digunakan. Perbedaan kunci yang digunakan pada proses ini akan memberikan perbedaan pada tingkat keacakan informasi pada sebuah *file* hasil enkripsi sehingga tidak memungkinkan untuk melakukan enkripsi dan dekripsi sebuah *file* dengan menggunakan kunci yang berbeda. Proses enkripsi *file* citra yang dapat diproses menggunakan sistem ini hanya *file* foto yang memiliki ukuran maksimal 800 x 800 *pixel*, hal ini dikarenakan keterbatasan pada perangkat OS android yang digunakan pada penelitian ini, yaitu dengan spesifikasi *Quad-Core* 1,2 GHz, RAM 1,00 GB, *Memory Internal* 8 GB.

4. KESIMPULAN

Kesimpulan yang dapat diperoleh pada penelitian ini adalah sebagai berikut:

1. Proses dekripsi membutuhkan *invers* dari kunci yang digunakan, kunci yang tidak memliki *invers* tidak dapat digunakan. Hal ini dikarenakan bahwa kunci yang tidak memiliki *invers,* jika digunakan maka proses enkripsi dapat dilakukan, akan tetapi proses dekripsi tidak akan menghasilkan *file* aslinya.
2. Tingkat keacakan *file* foto hasil enkripsi bergantung pada indeks kunci yang digunakan, yaitu dimulai dari nilai **a=0**, **b=1**, sampai dengan **z=25**. Semakin besar nilai indeks kunci yang digunakan, maka akan semakin menghasilkan tingkat keacakan yang tinggi terhadap *file* foto hasil enkripsi.
3. Hasil proses enkripsi dan dekripsi *file* foto yang dihasilkan pada penelitian ini, akan menghasilkan ukuran *file* foto yang lebih besar dibandingkan dengan *file* foto aslinya.
4. Waktu proses enkripsi dan dekripsi dari *file* foto sangat tergantung pada besarnya *pixel file* foto yang digunakan. Semakin besar ukuran *pixel* dari *file* foto, maka semakin lama besarnya waktu yang dibutuhkan untuk melakukan proses enkripsi dan dekripsi *file* foto tersebut.

5. DAFTAR PUSTAKA

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.*

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

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

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.

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.

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

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

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