KRIPTOGRAFI GAMBAR MENGGUNAKAN ALGORITMA *ONE-TIME PAD* DAN *VIGENERE CIPHER*

Miftaqul Huda[1], Aisyatul Karima[2]
Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jl. Nakula I No. 5-11, Semarang, Jawa Tengah 50131 - (024) 3517261
E-mail :miftaqulhuda24@gmail.com[1], aisyatul.karima@gmail.com[2]

Abstrak

Informasi khususnya yang berbentuk gambar sangat banyak digunakan saat ini, gambar ada yang bersifat rahasia dan ada yang tidak. Gambar yang bersifat rahasia perlu mendapatkan pengamanan agar kerahasian gambar tidak di ketahui oleh pihak yang tidak berwenang. Salah satu cara untuk melakukan pengamanan gambar adalah dengan teknik kriptorgrafi. Kriptografi gambar adalah teknik pengamanan gambar secara teknis dengan mengubah gambar kedalam bentuk lain menggunakan suatu kunci agar gambar tidak dapat dipahami secara visual. Dengan kunci yang sama, gambar yang telah diubah kedalam bentuk lain dapat dikembalikan menjadi bentuk gambar asli. Algoritma *one-time pad* dan *vigenere cipher* merupakan teknik enkripsi konvensional yang dapat digunakan untuk mengamankan informasi file gambar dengan teknik kriptografi. Penggabungan dua algoritma dalam kriptografi gambar akan menghasilkan gambar bentuk lain yang memiliki perubahan piksel yang lebih rumit dipecahkan dibandingkan dengan hanya menggunakan satu algoritma saja. Dari 100 kali percobaan yang dilakukan, enkripsi gambar dapat dilakukan dan persentase keberhasilannya 100%. Dalam percobaan deskripsi semua gambar dapat dikembalikan ke gambar asli dan persentase keberhasilan 100%. Dari penelitian ini dapat disimpulkan algoritma *one-time pad* dan *vigenere cipher* dapat digunakan melakukan kriptografi gambar dengan efektif.

Kata Kunci: Gambar, Kriptografi, Enkripsi Gambar, *One-Time Pad, Vigenere Cipher*.

Abstract

Images nformation is familiar in use today. Images are confidential and not confidential. Images are confidential need to get security so that the secrecy of images is not known by unauthorized parties. One of way to do security image is cryptography technique. Cryptography image is image technically security by changing the image into another form using a key for the image can not be understood visually. With the same key, the image that has been converted into other forms can be returned into the original image shape. Algorithms one-time pad and cipher vigenere a conventional encryption techniques that can be used to secure the information of the image file with cryptographic techniques. Merging two algorithms in cryptography image will result of other forms image that has more complex pixel changes compared solved than using only one algorithm.. Of the 100 experiments carried out, the image encryption can be done and the percentage of 100% success. In the experiment the description of all of the images can be restored to the original image and the percentage of 100% success. From this study it can be concluded algorithm and a one-time pad cipher vigenere perform cryptographic images can be used effectively.

Keywords: *Image, cryptography , image encryption , one-time pad , vigenere cipher.*

1. PENDAHULUAN

Seiring dengan sangat pesatnya kemajuan teknologi jaringan informasi khususnya di bidang computer, seseorang memungkinkan untuk bertukar informasi secara jarak dekat maupun jauh. Informasi ada yang bersifat umum dan ada yang bersifat rahasia. Bentuk inforasipun sangat banyak seperti teks, gambar, suara, video, dan lain sebagainya. Diera modern ini pertukaran informasi jarak jauh bukan merupakan suatu masalah lagi, dikarnakan adanya jaluk transmisi informasi jarak jauh. Jalur transmisi informasi jarak jauh sangat beragam bentuknya salah satunya dengan internet. Tetapi informasi yang melalui internet tidak terjamin kerahasiaannya. Dikarnakan internet adalah media transmisi informasi yang bisa di akses siapa saja, kapan saja, dan dimana saja. Dengan demikian semakin banyak pengguna maka semakin banyak serangan yang mungkin terjadi dalam proses pertukaran informasi di internet.

Halini menyebabkan perlunya pengamanan yang bisa menjamin kerahasiaan informasi yang melalui internet. Kriptografi adalah ilmu yang dikembangkan untuk mempelajari cara-cara pengamanan kerahasiaan informasi secara matematis [1] [3]. Contoh Ilmu kriptografi juga digunakan pada perang dunia II, pemerintah NAZI Jerman membuat mesin enkripsi yang dinamakan Engima untuk melakukan komunikasi agar sekutu tidak mengetahui rencana yang akan NAZI lakukan, halini menjadikan sekutu sulit menangani serangan NAZI. Kemudian tak lama berselang Engima berhasil dipecahkan oleh sekutu, keberhasilan memecahkan Engima disinyalir sebagai faktor yang memperpendek perang dunia II.

Secara lebih jelas kriptografi adalah ilmu mengenai teknik enkripsi dimana data diubah menggunakan suatu kunci dan hasil data enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi adalah proses mendapatkan kembali data asli. Proses kriptografi dilakukan menggunakan suatu algoritma dengan beberapa parameter [5].

Kriptografi gambar merupakan teknik yang umum digunakan untuk melindungi citra dari pengaksesan ilegal. Enkripsi citra adalah mengubah citra ke dalam bentuk lain dengan suatu kunci sehingga tidak dapat dibaca secara visual. Dengan kunci yang sama, citra terenkripsi dapat dikembalikan menjadi bentuk citra semula [1].

One-time pad adalah salah satu stream cipher klasik yang secara matematis terbukti aman. *One-time pad* cocok digunakan untuk mengenkripsi citra karena dapat memproses data yang mengandung volume besar dengan proses lebih cepat dibanding dengan algoritma tradisonal seperti DES, AES, Blowfish, RSA dan lain-lain. Halini dikarenakan dikarenakan *one-time pad* tidak menggunakan skema perulangan (*round*) dan operasi XOR yang sederhana [1].

Vigenere cipher merupakan cipher yang setiap plainteks-nya mempunyai beberapa kemungkinan cipherteks, ini terjadi karena panjang kuncinya lebih dari satu [7].

Sehubungan dengan latar belakang, diperlukan pengamanan kerahasiaan gambar untuk disimpan sendiri atau untuk dikirimkan ke pihak lain yang tidak sekedar proteksi disk atau pengamanan secara hardware saja namun diperlukan salah satu teknik lain untuk pengamanan file. Sehingga penulis bermaksud membahas pengamanan kerahasiaan gambar yang mampu mengubah citra ke bentuk lain dengan menggabungkan dua algoritma *one-time pad* dan *vigenere cipher* agar hasil enkripsi lebih sulit dipacahkan.

2. LANDASAN TEORI

2.1 Tinjauan Studi

Berbagai penelitian yang dilakukan oleh peneliti terdahulu, hasil yang dikemukakan menunjuk berbagai pandangan tentang penerapan algoritma *one-time pad* dan *vigenere cipher* pada media citra digital. Peneleti terdahulu yang relevan dengan penelitian ini adalah sebagai berikut:

Enkripsi citra digital dengan alagoritma *one-time pad* dapat mengenkripsi data lebih cepat dikarenakan *one-time pad* tidak menggunakan skema perulangan (*round*) dan operasi XOR yang sederhana. Dengan sistem *chaos* sebagai pembangkit kunci bilangan acak agar *pseudo one-time pad* dapat di implementasikan mengenkripsi citra. Selain itu sistem *chaos* mempunyai karakteristik sensivitasnya terhadapat perubahan kecil parameter nilai awal. Sensitivasi ini berati perbedaan kecil pada nilai awal fungsi setelah fungsi diinterasi. [1].

One-time pad digunakan untuk melindungi data pada *web* dengan mengkodekan atau menyembunyikan data dengan cara melakukan enkripsi nama dokumen, isi dokumen dan tanggal saat dokumen itu disimpan. Proses ini ditujukan agar admin yang mengelola dalam penyimpanan data itu tidak dapat mengetahui isi dokumen tersebut. Proses pengaman ini dengan mengenkripsi data terlebih dahulu lalu di simpan dalam database. Algoritma *one-time pad* menggunakan kunci yang sama dalam proses enkripsi maupun deskripsi. Algoritma ini akan mengharuskan pengirim dan penerima harus menyetujui suatu kunci tertentu sebelum terjadi komunikasi diantara kedua belah pihak [6].

Program enkripsi data dengan menggunakan algoritma *vigenere chiper* yang digunakan untuk pengamanan data pelanggan dan data harga. Teks di enkripsi terlebih dahulu lalu disimpan kedalam database. Implementasi program enkripsi data ini dapat meningkatkan keamanan pendataan penjualan khususnya pada data harga dan dapat meningkatkan keakuratan informasi, khususnya perhitungan harga jual [5].

Penggabungan dua algoritma yaitu stream chiper dan vigenere chiper untuk mengenkripsi data **.txt (Text Document)* dan **.rtf (Rich Text Format).* Proses enkripsi dengan menggunakan rumus gabungan dari algoritma *stream chiper* dan *vigenere chiper* ini menghasilkan algoritma yang cukup handal karena menggunakan 2 kunci berbeda, satu kunci dibangkitkan dengan karakter *plaintext* dan satu kunci di inputkan secara manual [7].

2.2 Kriptograafi

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti keabsahan (memperoleh tingkat kepercayaan yang berkaitan dengan seberapa jauh kebenarannya), integritas data (berhubungan dengan penjagaan dari perubahan data secara tidak sah) serta autentikasi data (berhubungan dengan identifikasi/ pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri) tersebut, dengan kata lain kriptografi digunakan untuk menjamin keleluasaan pribadi dan pembuktian keaslian pesan dalam berkomunikasi [6].

Pada dasarnya, kriptografi memiliki dua algoritma yaitu enkripsi dan dekripsi. Pesan yang dapat dibaca disebut sebagai plainteks, sedangkan teknik untuk membuat pesan tidak dapat terbaca disebut enkripsi. Pesan yang sudah melewati tahap enkripsi disebut

ciphertekst dan dekripsi adalah teknik untuk merubah ciphertekst menjadi plainteks, dan kunci adalah kode yang digunakan untuk melakukan peng-enkripsi-an atau pen-deskripsi-an suatu teks. Untuk selanjutnya piksel disebut sebagai objek plainteks [6].

2.3 *One-time pad (OTP)*

One-time pad (OTP) adalah stream cipher yang melakukan enkripsi dan ekripsi satu karakter setiap kali. Algoritma ini ditemukan pada tahun 1917 oleh Major Joseph Mauborgne sebagai perbaikan dari *vernam cipher* untuk menghasilkan keamanan yang sempurna. Mauborgne mengusulkan penggunaan *one-time pad* (*pad* = kertas bloknot) yang berisi deretan karakter-karakter kunci yang dibangkitkan secara acak. Satu *pad* hanya digunakan sekali (*one-time*) saja untuk mengenkripsi pesan, setelah itu *pad* yang telah digunakan dihancurkan supaya tidak dipakai kembali untuk mengenkripsi pesan yang lain. Enkripsi dapat dinyatakan sebagai penjumlahan modulo 26 dari satu karakter plainteks dengan satu karakter kunci *one-time pad*. Berikut ini persamaan enkripsi *one-time pad* 26 karakter ditunjukkan pada persamaan 2.1 dibawah ini :

$$c_i = (p_i + k_i) \bmod 26 \qquad (2.1)$$

Jika karakter yang digunakan adalah anggota himpunan 256 karakter (seperti karakter dengan pengkodean ASCII), maka persamaan enkripsinya ditunjukkan pada persamaan 2.2 dibawah ini.

$$c_i = (p_i + k_i) \bmod 256 \qquad (2.2)$$

Setelah pengirim mengenkripsi pesan dengan kunci, dia menghancurkan kunci tersebut. Penerima pesan menggunakan *pad* yang sama untuk mendekripsikan karakter-karakter cipherteks menjadi karakter-karakter plainteks dengan persamaan 2.3 berikut.

$$p_i = (c_i - k_i) \bmod 26 \qquad (2.3)$$

untuk alfabet 26-huruf, atau untuk alfabet 256-karakter dengan persamaan 2.4 dibawh ini.

$$p_i = (c_i - k_i) \bmod 256 \qquad (2.4)$$

Perhatikan bahwa panjang kunci harus sama dengan panjang plainteks, sehingga tidak ada kebutuhan mengulang penggunaan kunci selama proses enkripsi (seperti halnya pada v*ernam cipher*) [1].

2.4 Vigenere cipher

Vigenere cipher termasuk dalam cipher abjad majemuk (polyalphabetic substitution cipher) yang dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigenere pada abad 16 (tahun 1586). Vigenere Cipher adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi Caesar berdasarkan huruf-huruf pada kata kunci. Vigenere Cipher menggunakan tabel seperti pada tabel 2.2, Vigenere Cipher dengan angka dalam melakukan enkripsi.

Teknik dari substitusi vigenere cipher bisa dilakukan dengan dua cara [10]:

a. *Vigenere Cipher* dengan Angka

Tabel 1 Vigenere cipher dengan angka

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

Jika ditukar dengan angka, maka kunci dengan huruf “HUDA”

K = (7, 20, 3, 0)

Dan plainteks nya “ SONA “ akan menjadi

P = (11,20,10,0).

Dari contoh tabel, maka dapat disimpulkan bahwa rumus dari enkripsi dan dekripsi data vigenere cipher adalah [10]:

Enkripsi :

ci = (pi+ ki) mod 26

Deskripsi :

pi = (ci – ki) mod 26 ; untuk ci > = ki

pi = (ci + 26 – ki) mod 26 ; untuk ci < = ki

Keterangan :

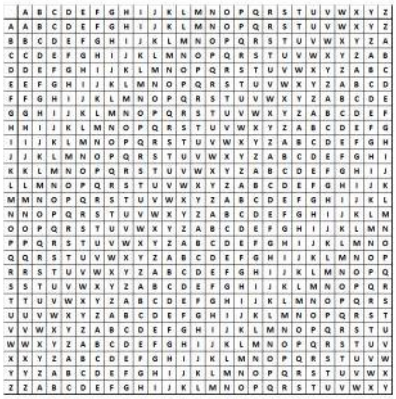
c = Ciphertext p = Plaintext

k = Kunci

b. Vigenere Cipher dengan Huruf

Vigenere Cipher dengan huruf berisi alfabet yang dituliskan dalam 26 baris, masing masing baris digeser ke kiri dari baris sebelumnya membentuk ke-26 kemungkinan sandi Caesar setiap huruf disediakan dengan menggunakan baris yang berbeda-beda sesuai kunci yang diulang [10].

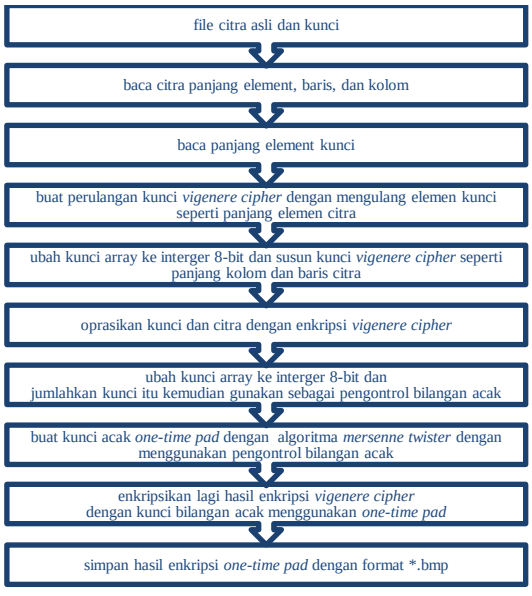
Tabel 2 Vigenere Cipher dengan Huruf



3. METODE

Metode yang di usulkan dalam penelitian ini adalah sebagai berikut:

A. Proses Enkripsi



Gambar 3.1 Gambar Proses Enkripsi

B. Proses Deskripsi

Gambar 3.2 Gambar Proses Deskripsi

4. ANALISIS DAN PEMBAHASAN

4.1 Analisis Plainteks

Plainteks yang digunakan adalah berupa citra digital bertipe *grayscale* berformat *.bmp yang memiliki ukuran minimal 1 x 1 piksel dan maxsimal tak terhinga.

4.2 Analisis Kunci

Kunci yang digunakan adalah bilangan array mininimal 1 karakter dan maksimal seperti panjang element plainteks.

4.3 Enkripsi

Proses enkripsi dilakukan dua kali menggunakan algoritma algoritma *vigenere cipher* dan *one-time pad*.

Sebuah contoh menggunakan kunci “huda”dan plainteks sebagai berikut

Gambar 4.1 Plainteks secara intensitas piksel

Prosen enkripsi sebagai berikut :

A. Enkripsi *Vigenere Cipher*

Dalam proses enkripsi yang pertama ini menggunakan algoritma *vigenere cipher* dengan persamaan 4.5 dibawah ini.

$$c_i = (p_i + k_i) \bmod 256 \quad (4.5)$$

Berikut adalah proses enkripsi *vigenere cipher*:

1. Citra yang dijadikan *p* di baca panjang *m*, *n*, dan elementnya (*m* x *n*).
2. Kemudian *k* dibaca panjang elemntnya dan di looping sesuai panjang element *p*.
3. Setelah panjang element *k* sama dengan *p*, maka *k* di ubah ke bilangan *interger* 8-bit lalu di susun menjadi *m* dan *n* seperti *p*.
4. Lalu *p* dan *k* di oprasikan dengan persamaan enkripsi *vigenere cipher*. Pada tabel 4.5 dibawah ini adalah *p* dan *k vigenere cipher* pada *f* (1,1) sampai *f* (1,5).

Tabel 4.5 Nilai *p* dan *k* pada *f* (1,1) sampai *f* (1,5)

	f (1,1)	*f* (1,2)	*f* (1,3)	*f* (1,4)	*f* (1,5)
p	213	217	220	220	221
k	104	117	100	97	104

Dari *p dan k* diatas maka *c* dapat diketahui dengan pengoprasian sebagai berikut :

$c_{(1,1)} = (213 + 140) \bmod 256 = 61$
$c_{(1,2)} = (217 + 117) \bmod 256 = 78$
$c_{(1,3)} = (220 + 100) \bmod 256 = 64$
$c_{(1,4)} = (220 + 97) \bmod 256 = 61$
$c_{(1,5)} = (221 + 104) \bmod 256 = 69$

5. Proses enkripsi diatas akan diteruskan hingga elemen *m* dan *n* habis dan hasil *c* akan menjadi *p* dalam enkripsi menggunakan algoritma *one-time pad.*

B. Enkripsi *One-Time Pad*

Dalam proses enkripsi yang kedua ini menggunakan algoritma *one-time pad* dengan persamaan 4.6 dibawah ini.

$$c_i = (p_i + k_i) \bmod 256 \quad (4.6)$$

Berikut adalah proses enkripsi *one-time pad* :

1. Kunci "huda" akan di uba kebilangan *interger* 8-bit kemudian bilangan itu di jumlahkan dan digunakan sebagai pengontrol kunci bilangan acak *mersenne twister.*
2. Setelah pengontrol kunci bilangan acak di tentukan maka kunci dibuat dengan fungsi jadi algoritma *mersenne twister* pada *matlab* sesuai panjang elemen *m* dan *n*.
3. Setelah *k* jadi, lalu *p* dan *k* di oprasikan dengan persamaan enkripsi *one-time pad.* Pada tabel 4.6 dibawah ini adalah nilai *p* dan *k one-time pad* pada *f* (1,1) sampai *f* (1,5).

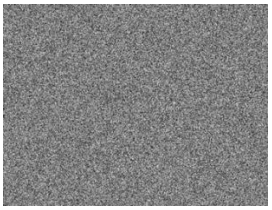
Tabel 4.6 *Nilai p* dan *k one-time*

	f (1,1)	*f* (1,2)	*f* (1,3)	*f* (1,4)	f (1,5)
p	144	133	4	47	65
k	83	55	196	242	254

Dari *p dan k* diatas maka *c* dapat diketahui dengan pengoprasian sebagai berikut :

$c_{(1,1)} = (61+83) \bmod 256 = 144$
$c_{(1,2)} = (78+55) \bmod 256 = 133$
$c_{(1,3)} = (64+196) \bmod 256 = 4$
$c_{(1,4)} = (61+ 242) \bmod 256 = 47$
$c_{(1,5)} = (69+ 254) \bmod 256 = 65$

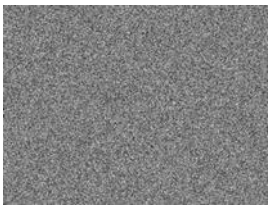
Proses enkripsi diatas akan diteruskan hingga elemen *m* dan *n* habis dan hasil *c* akan menjadi hasil enkripsi dalam penelitian ini.



Gambar 4.2 Gambar Enkripsi

4.4 Deskripsi

Proses deskripsi menggunakan dua algoritma dan kunci yang sama seperti enkripsi. Dibawah ini merupakan plain pada proses deskripsi.



Gambar 4.3 Gambar Plainteks Deskripsi

A. Deskripsi *One-Time Pad*

Dalam proses deskripsi yang kedua ini menggunakan algoritma *one-time pad* dengan persamaan 4.7 dibawah ini.

$$d_i = (p_i - k_i) \bmod 256$$

Berikut adalah proses deskripsi *one-*time *pad* :

1. Citra yang dijadikan *p* di baca panjang *m*, *n*, dan elementnya (*m* x *n*).
2. Kunci "huda" akan di ubah kebilangan *interger* 8-bit kemudian bilangan itu di jumlahkan dan digunakan sebagai pengontrol kunci bilangan acak *mersenne twister*.
3. Setelah pengontrol kunci bilangan acak di tentukan maka kunci dibuat dengan fungsi jadi algoritma *mersenne twister* pada *matlab* sesuai panjang elemen *m* dan *n*.
4. Setelah *k* jadi, lalu *p* dan *k* di oprasikan dengan persamaan deskripsi *one-time pad.* Pada tabel 4.7 berikut ini adalah nilai *p* dan *k* *one-time pad* pada *f* (1,1) sampai *f* (1,5).

Tabel 4.8 Nilai *p* dan *k* pada *f* (1,1) sampai *f* (1,5)

	f (1,1)	*f* (1,2)	*f* (1,3)	*f* (1,4)	f (1,5)
p	144	133	4	47	65
k	83	55	196	242	254

Dari *p* dan *k* diatas maka *c* dapat diketahui dengan pengoprasian sebagai berikut :

$c_{(1,1)} = (144\text{-}83) \bmod 256 = 61$
$c_{(1,2)} = (133\text{-}55) \bmod 256 = 78$
$c_{(1,3)} = (4\text{-}196) \bmod 256 = 64$
$c_{(1,4)} = (47\text{-}242) \bmod 256 = 61$
$c_{(1,5)} = (65\text{-}254) \bmod 256 = 69$

5. Proses deskripsi diatas akan diteruskan hingga elemen *m* dan *n* habis dan hasil *c* akan menjadi plainteks deskripsi *vigenere cipher*.

B. Deskripsi *Vigenere Cipher*

Dalam proses deskripsi yang kedua ini dengan algoritma *vigenere cipher* yang menggunakan persamaan 4.7 dibawah ini.

$$c_i = (p_i - k_i) \bmod 256$$

Berikut adalah proses deskripsi *vigenere cipher*:

1. Disini *k* = "huda" (4.6) dibaca panjang elemntnya dan di looping sesuai panjang element *p*.
2. Setelah panjang element *k* sama dengan *p*, maka *k* di ubah ke bilangan *interger* 8-bit lalu di susun menjadi *m* dan *n* seperti *p*.
3. Lalu *p* dan *k* di oprasikan dengan persamaan deskripsi *vigenere cipher*. Pada tabel 4.8 dibawah ini adalah *p* dan *k* *vigenere cipher* pada *f* (1,1) sampai *f* (1,5).

Tabel 4.8 Nilai *p* dan *k* pada *f* (1,1) sampai *f* (1,5)

	f (1,1)	*f* (1,2)	*f* (1,3)	*f* (1,4)	*f* (1,5)
p	213	217	220	220	221
k	104	117	100	97	104

Dari nilai *p dan k* diatas maka *c* dapat diketahui dengan pengoprasian deskripsi sebagai berikut :

$c_{(1,1)} = (144\text{-}83) \bmod 256 = 61$
$c_{(1,2)} = (133\text{-}55) \bmod 256 = 78$
$c_{(1,3)} = (4\text{-}196) \bmod 256 = 64$
$c_{(1,4)} = (47\text{-}242) \bmod 256 = 61$
$c_{(1,5)} = (65\text{-}254) \bmod 256 = 69$

4. *Proses* deskripsi diatas akan diteruskan hingga elemen m dan n habis dan hasil c akan menjadi hasil deskripsi dalam penelitian ini. Berikut ini adalah hasil deskripsi.

Gambar 4.4 Gambar Deskripsi

4.5 Hasil dan Pengujian

Hasil dan pengujian merupakan perhitungan nilai MSE dan PSNR pada citra ter enkripsi dan terdeskripsi agar mengetahui apakah bisa algoritma *one-time pad* dan *vigenere cipher* merubah gambar ke bentuk lain (enkripsi) dan mengembalikan gambar ke bentuk asli (deskripsi). Gambar yang telah terenkripsi akan dilakukan penghitungan MSE dan PSNR, semakain besar nilai MSE dan semakin kecil nilai PSNR berarti semakin bagus dalam merubah gambar ke bentuk lain. PAda gambar terdeskripsi dilakukan juga perhitungan MSE dan PSNR, semakin kecil nilai MSE dan semakin besar nilai PSNR maka semakin mirip citra deskripsi dengan citra asli.

No	MSE Enkripsi	PSNR Enkripsi	MSE Deskripsi	PSNR Deskripsi
1	10903.195	7.789	0	*inf*
2	10841.808	7.814	0	*inf*
3	10720.941	7.862	0	*inf*
4	10716.881	7.864	0	*inf*
5	5329	10.898	0	*inf*
6	13225	6.950	0	*inf*
7	13926.196	6.726	0	*inf*
-	-	-	-	-
100	14855.297	6.446		*inf*
Rata-rata			0	*Inf*

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan oleh peneliti, maka dapat disimpulkan beberapa hal sebagai berikut:

a. Dari 100 kali eksperimen kriptografi gambar dengan menggabungkan dua algoritma *vigenere cipher* dan *one-time pad* dapat melakukan pengamanan gambar secara visual (enkripsi) dan dapat mengembalikan gambar ke bentuk aslinya (deskripsi).
b. Dengan melakukan kriptografi gambar menggunakan dua algoritma *vigenere cipher* dan *one-time pad*, gambar mendapat kerahasiaan yang lebih karena melalui dua kali proses enkripsi.
c. Dari hasil pengujian kesalahan disimpulkan bahwa algoritma *vigenere cipher* dan *one-time pad* untuk kriptografi sangatlah bagus karna tidak ada kesalahan pada citra yang telah di deskripsi dan hal ini menujukkan keaslian gambar yang melalui proses kriptografi terjaga dengan baik.

5.2 Saran

Saran – saran yang berguna untuk pengembangan aplikasi ini adalah sebagai berikut :

a. Aplikasi dapat dikembangkan lagi menggunakan tampilan GUI agar lebih menarik digunakan.
b. Algoritma *Mersenne Twister* sebagai pembangkit kunci bilangan acak dapat di ganti dengan algoritma yang lebih mangkus untuk kriptografi.
c. Aplikasi dapat dikembangkan dengan bahasa pemrograman lain yang lebih powerfull dan cepat.

DAFTAR PUSTAKA

[1] M. Edisuryana, R. R. Isnanto dan M. Somantri, "Aplikasi Steganografi Citra Berformat Bitmap dengan menggunakan

metode *End Of File*", *Transient,* vol. 2, no. 3, 2013.

[2] B. Rakhmat dan M. Fairuzabadi, "Steganografi Menggunakan Metode Least Significant Bit dengan Kombinasi Algoritma Kriptografi Vigenere Dan RC4", *Jurnal Dinamika Informatika,* vol. 5, no. 2, 2010.

[3] A. Prabowo, A. Hidayanto dan Y. Christiyono, "Penyembunyian Data Rahasia pada Citra Digital Berbasis *Chaos* dan *Discrete Cosine Transform",Transmisi,* vol. 13, no. 2, 2011.

[4] Faradisa dan B. F. Budiono, "Implementasi Metode Huffman Sebagai Teknik Kompresi Citra", *Jurnal Elektro Eltek,* vol.2, no. 2, 2011.

[5] C-C. Chang, P-Y. Lin, J-C. Chuang, "A Grayscale Image Steganography Based upon Discrete Cosine Transformation", *Journal of Digital Information Management,* vol.8, no.2, 2010.

[6] M. Yunus dan A. Harjoko, "Penyembunyian Data pada File Video Menggunakan Metode LSB dan DCT", *IJCCS,* vol.8, no. 1, 2014.

[7] T. Suyono, S.Si., M.Kom., E. Mulyanto, S.Si., M.Kom., Dr. V. Suhartono, O. D. Nurhayati, M.T dan Wijanarto, M.Kom., "Teori Pengolahan Citra Digital", *Andi,* 2009.

[8] H. Patel dan P. Dave, "Steganography Technique Based on DCT Coefficients", *International Journal Of Engineering Research and Applications,* vol. 2, no. 1, 2012.

[9] P. V. Bodhak dan B. L Gunjal, "Improved Protection In Video Steganography Using DCT & LSB", *International Journal Of Engineering and Innovative Technology,* vol. 1, no. 4, 2012.

[10] C. Iswahyudi, "Prototype Aplikasi Untuk Mengukur Kematangan Buah Apel Berdasarkan Kemiripan Warna", *Journal Teknologi,* vol. 3, no. 2, pp. 107-112, 2010.

[11] M. Wahid, "Steganografi Citra Digital Dengan Discrete Wavelet Transform (DWT) dan Discrete Cosine Transform (DCT)", 2014.

[12] M. K. Mathur, S. Loonker dan Dr. D. Saxena, "Lossless Huffman Coding Technique For Image Compression And Reconstruction Using Binary Trees", *IJCTA,* vol. 3, no. 1, 2012.

[13] R. Wissarto, "Implementasi Slantet Transform (SLT) dan Huffman Coding Pada Steganografi Citra *Grayscale*", 2014.

[14] R. A. Saragih dan H. Gunawan, "Simulasi Penyembuhan Error pada Citra Menuggunakan Metode Multi Directional Interpolation (MDI)", *Electrial Engineering Journal,* vol. 2, no. 1, pp. 13-27, 2011.

[15] N. Jain, S. Meshram and S. Dubey, "Image Steganography Using LSB and Edge Detection Technique", *International Journal of Soft Computing and Engineering (IJSCE),* Vol.2, no. 3, 2012.

[16] D. Putra, "Pengolahan Citra Digital, *Andi,* 2010