Volume 4, No. 1 - Mei 2019 ISSN : 2541-4313 (print) | 2548-5113 (online)

Fountain of Informatics

Journal

Penerbit:
Universitas Darussalam Gontor
Jl. Raya Siman Km.6 Siman Ponorogo 63471 - Telepon : (0352) 357 4562
www.unida.gontor.ac.id || informatika@unida.gontor.ac.id

FOUNTAIN OF INFORMATICS JOURNAL

ISSN (Print): 2541-4313

VOLUME 4, NOMOR 1, MEI 2019

Terbit dua kali setahun pada bulan Mei dan November.
Berisi tulisan yang diangkat dari hasil penelitian dalam bidang Informatika
Berisi tulisan yang diangkat dari hasil penelitian dalam bidang Informatika/Ilmu Komputer
(Sistem Informasi, Rekayasa Perangkat Lunak, Jaringan Komputer dan Game Technology)

Penerbit
Universitas Darussalam Gontor
Alamat: Jl. Raya Siman Km.6 Siman Ponorogo
Kode Pos: 63471 Telpon/Faximile: (+62 352) 357 4562 / (+62 352) 488182
Email: informatika@unida.gontor.ac.id, Website: http://ejournal.unida.gontor.ac.id/index.php/FIJ

DAFTAR ISI

DOI: http://dx.doi.org/10.21111/fij.v4i1.2906
Diterima: 14 Februari 2019 Revisi: 5 Mei 2019 Terbit: 10 Mei 2019

Pengamanan Citra Dengan Operator Algoritma Genetika

Abduh Riski [1)*], Ahmad Saiful Rizal [2)], Ahmad Kamsyakawuni [3)]

Jurusan Matematika FMIPA Universitas Jember [1), 2), 3)]
riski.fmipa@unej.ac.id [1)], ahmadsaifulrizal13@gmail.com [2)], kamsyakawuni.fmipa@unej.ac.id [3)]*

Abstrak

Perkembangan teknologi komputer yang semakin pesat tentu diperlukan teknik pengamanan data baik data teks maupun data citra. Pengamanan data menjadi hal yang sangat penting agar data yang dikirimkan tetap terjaga kerahasiaannya. Pada penelitian ini akan dibahas tentang Operator Algoritma Genetika dalam mengamankan data citra. Operator tersebut adalah crossover dan mutasi. Kunci yang digunakan berupa citra yang akan mengalami pergeseran bit. Proses enkripsi dengan Operator Algoritma Genetika menghasilkan citra yang terlihat acak dan susah untuk ditebak gambar aslinya. Proses dekripsi dengan Operator Algoritma Genetika dapat mengembalikan cipher image menjadi citra yang sebenarnya. Analisis keamanan dari metode yang digunakan menunjukkan bahwa algoritma aman dari serangan analisis frekuensi dibuktikan dengan analisis histogram, analisis diferensial dengan rata-rata NPCR 99,65% dan UACI 32,41%, dan analisis korelasi dengan rata-rata sebesar -0,01.

Kata kunci: *crossover, mutasi, enkripsi, dekripsi, histogram, diferensial, korelasi.*

Abstract

[Image Security with Operator of Genetic Algorithm] *The rapid development of computer technology needed a technique to secure data both text and image. Data security is vital that the data is sent still safe its confidentiality. In this article will be proposed about security image by Operator of Genetic Algorithm. These operators are crossover and mutation. The key is an image that will get bitshift. Encryption process with operator Genetic Algorithm producing the image which looks random and confusing to predict the original image. Decryption process with Operator Genetic Algorithm can change cipher image to the real image. Security analysis of the method which used indicates that algorithm is secured from analysis frequency attack, proven by analysis histogram, averages analysis differential NPCR 99,65% and UACI 32,41%, and averages correlation value -0,01.*

Keywords: *crossover, mutation, encryption, decryption, histogram, differential, correlation.*

1. PENDAHULUAN

Dalam dunia internet sering terjadi pencurian data seperti data keuangan, data privasi dan data citra. Salah satu cara untuk menjaga kerahasiaan data tersebut yaitu dengan teknik enkripsi dan dekripsi, yang terdapat dalam kriptografi. Teknik ini digunakan untuk menjamin komunikasi yang aman antara kedua pelaku sistem informasi. Kriptografi adalah salah satu ilmu untuk menjaga kerahasiaan dan keaslian data dengan mengubah data menjadi bentuk sandi sehingga data tersebut sulit dipahami oleh orang lain dan hanya dapat dipahami oleh penerima yang berwenang. Dengan kriptografi, data dikodekan dengan algoritma tertentu sehingga data yang dikirimkan sampai kepada penerima dengan aman. Dalam perkembangannya, proses kriptografi tidak hanya dilakukan dengan menggunakan algoritma kriptografi, tetapi juga algoritma lain seperti Algoritma Genetika.

Dalam penelitian terdahulu, telah dilakukan pengamanan data teks menggunakan operator algoritma genetika. Operator tersebut adalah *crossover* dan *mutation*. *Crossover* yang digunakan adalah *crossover* dua titik, sedangkan mutasi yang digunakan adalah *flipping of bits*. Teks yang akan disandikan terlebih dahulu dikonversi menjadi biner [1].

Algoritma Genetika juga telah digunakan untuk menyandikan citra. Kunci yang digunakan diperoleh dari *random* rangkaian DNA. Dalam proses penyandian citra, citra yang digunakan hanya terbatas di ukuran 256×256 piksel dan citra yang dihasilkan masih terlihat polanya [2]. Penelitian ini dilakukan dengan harapan agar pesan citra yang disandikan memiliki tingkat keamanan yang tinggi. Sehingga penulis mengajukan Operator Algoritma Genetika untuk menyandikan citra dan kunci yang digunakan juga berupa citra yang akan mengalami pergeseran ke kiri 1-bit.

2. BAHAN DAN METODE

Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu *crypto* berarti rahasia dan *graphia* berarti tulisan. Kriptografi adalah ilmu yang mempelajari bagaimana pesan yang dikirim dapat disampaikan kepada

penerima dengan aman. Kriptografi bertujuan untuk menjaga kerahasiaan informasi yang terkandung dalam data sehingga data tersebut tidak dapat diketahui oleh pihak yang tidak sah [3].

Dalam kriptografi terdapat proses enkripsi dam dekripsi. Enkripsi adalah proses penyandian pesan asli (*plain image*) menjadi pesan rahasia (*cipher image*) dengan menggunakan kunci. Sedangkan dekripsi adalah pengembalian pesan yang telah dienkripsi [4].

Proses enkripsi dan dekripsi ditunjukkan pada Gambar 1.

Gambar 1. Proses Enkripsi dan Dekripsi Pesan

Citra

Citra adalah gambar yang didalamnya terdapat kumpulan-kumpulan piksel yang disusun dalam larik dua dimensi. Setiap piksel diwakili oleh dua bilangan bulat untuk menunjukkan lokasinya dalam bidang citra, sedangkan untuk menunjukkan terang gelap piksel tersebut seringkali menggunakan nilai dengan besar 8 bit yang berarti terdapat 2^8 atau 256 derajat keabuan dengan selang nilai 0 sampai 255, dimana 0 menyatakan warna hitam, 255 menyatakan warna putih dan tingkat abu-abu berada di antara nilai 0 dan 255 [5]. Citra digital adalah citra yang dapat diolah langsung oleh komputer secara numerik, disimpan pada komputer sebagai angka untuk menunjukkan besar intensitas pada setiap piksel. Citra digital berukuran $N \times M$ dinyatakan dengan matriks berukuran N baris dan M kolom, serta memiliki NM buah piksel [6].

Basis Bilangan

Bilangan berdasarkan basisnya terdiri dari beberapa macam diantaranya bilangan desimal dan bilangan biner. Bilangan desimal merupakan bilangan yang mempunyai basis sebanyak 10, yaitu 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Sedangkan bilangan biner merupakan bilangan yang memiliki basis sebanyak 2 yaitu 0 dan 1. Suatu basis bilangan dapat dikonversi ke basis bilangan yang lain, yaitu dari bilangan desimal ke bilangan biner, begitu juga sebaliknya [7]. Bilangan biner memiliki beberapa operasi bilangan salah satunya adalah XOR. p dan q adalah sebuah proposisi. Pernyataan yang salah dinyatakan dalam bit 0 dan pernyataan yang benar dinyatakan dalam bit 1 seperti pada Tabel 1.

Tabel 1. Operasi XOR biner (Latif *et al*., 2011)

p	q	$p \oplus q$
1	1	0
1	0	1
0	1	1
0	0	0

Pergeseran Bit

Pergeseran bit (bitshift) yang digunakan yaitu pergeseran 1-bit ke kiri. Dalam pergeserannya terdapat aturan yang ditetapkan yaitu jika angka paling kiri sebelum digeser adalah 1 maka akan di-XOR dengan 0001 1011 sedangkan jika angka paling kiri adalah 0 sebelum terjadi pergeseran maka tidak perlu di-XOR dengan 0001 1011 [8].

Algoritma Genetika

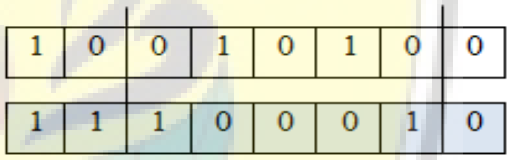
Algoritma Genetika merupakan proses pencarian yang *metaheuristic* sehingga penekanan pemilihan operator yang digunakan sangat menentukan keberhasilan Algoritma Genetika dalam menemukan solusi optimum suatu masalah. Operator-operator tersebut adalah sebagai berikut [9]:

a. Seleksi

Seleksi adalah proses penentuan individu mana yang akan menjadi *parent.*

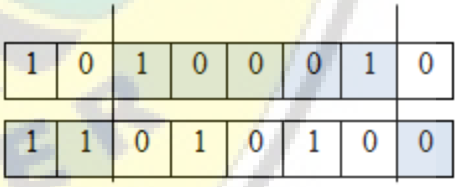
b. *Crossover*

Crossover merupakan pertukaran gen-gen dalam kromosom yang bertujuan untuk menambah keanekaragaman kromosom. Kromosom merepresentasikan piksel dengan kedalaman 8 bit, sedangkan gen adalah nilai 0 dan 1. Pemilihan titik *crossover* ditunjukkan pada Gambar 2.



Gambar 2. Pemilihan titik *Croosover*

Titik yang dipilih yaitu 3 dan 7, kemudian diantara titik tersebut terjadi pertukaran gen sehingga terlihat seperti Gambar 3.



Gambar 3. Hasil *Crossover*

Pada penelitian ini akan digunakan crossover dengan memilih dua titik *nonrandom* dari dua kromosom, kemudian dilakukan pertukaran bitstring di antara kedua kromosom tersebut.

c. Mutasi

Mutasi merupakan proses perubahan nilai gen dalam suatu kromosom. Pada proses mutasi, jika gen bernilai 0 maka berubah menjadi 1 dan jika bernilai 1 maka akan menjadi 0. Mutasi yang digunakan pada penelitian ini yaitu mutasi kebalikan (*flipping of bits*), semua bit 0 dirubah menjadi bit 1 dan begitu juga sebaliknya. Sehingga mutasi yang digunakan memiliki probalitas mutasi 1.

Analisis Histogram

Analisis histogram merupakan analisis keamanan yang memperlihatkan gambaran informasi tentang distribusi nilai piksel pada sebuah citra. Distribusi nilai piksel pada suatu citra yang terenkripsi (*cipher image*) harus merata pada histogramnya. *Cipher image* yang tidak merata penyebaran pikselnya maka akan rentan untuk diserang oleh *attacker* sehingga *cipher image* tersebut tidak cukup aman. *Attacker* seringkali memanfaatkan frekuensi kemunculan piksel dengan tujuan untuk melakukan kriptanalisis. Agar *attacker* sulit untuk melakukan analisis frekuensi maka histogram *cipher image* seharusnya berbeda signifikan atau tidak memiliki kesamaan dengan histogram *plain image* [10].

Analisis Diferensial

Analisis diferensial digunakan untuk menguji perubahan elemen warna pada *cipher image*. Analisis diferensial dapat ditentukan dengan dua indikator pengukuran yang biasa digunakan, yaitu *Number of Pixels Change Rate* (*NPCR*) dan *Unifer Average Changing Intensity* (UACI). NPCR digunakan untuk mengetahui perubahan piksel antara *plain image* dan *cipher image*, sedangkan UACI berfokus pada interval perbedaan nilai piksel antara *plain image* dan *cipher image*. Perhitungan *NPCR* didefinisikan seperti pada persamaan (1).

$$npcr = \left(\frac{1}{m \times n \times p}\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{p} d_{i,j,k}\right) \times 100\% \quad (1)$$

dimana m, n dan p merupakan lebar, tinggi dan dimensi dari citra sedangkan $d_{i,j,k}$ ditentukan sebagai berikut:

$$d_{i,j,k} = \begin{cases} 0, \text{jika } c_{i,j,k}^{(1)} = c_{i,j,k}^{(2)} \\ 1, \text{jika } c_{i,j,k}^{(1)} \neq c_{i,j,k}^{(2)} \end{cases} \quad (2)$$

dimana $c_{i,j,k}^{(1)}$ dan $c_{i,j,k}^{(2)}$ merupakan nilai derajat keabuan dari baris i, kolom j, dan kanal k dari citra $c^{(1)}$ (*plain image*) dan $c^{(2)}$(*cipher image*).

Sedangkan perhitungan UACI dirumuskan seperti pada persamaan (2).

$$U = \left(\frac{1}{m \cdot n \cdot p}\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{p}\frac{\left|c_{i,j,k}^{(1)} - c_{i,j,k}^{(2)}\right|}{255}\right) \times 100\% \quad (3)$$

Cipher image dikatakan baik apabila nilai NPCR atau UACI antara *cipher image* dan *plain image* memenuhi batas minimum NPCR sebesar 98.87% dan UACI sebesar 32.17% [11].

Analisis Korelasi

Analisis korelasi digunakan untuk menunjukkan korelasi antara *plain image* dan *cipher image* berdasarkan pada nilai-nilai pikselnya. Algoritma enkripsi yang diajukan akan sangat aman jika *cipher image* yang dihasilkan sungguh berbeda dengan *plain image*. Koefisien korelasi dirumuskan seperti persamaan (3).

$$r_{xy} = \frac{\sum_{i=1}^{n}(x_i - \mu(x))(y_i - (\mu(y))}{\sigma(x)\sigma(y)} \quad (4)$$

di mana r_{xy} menyatakan nilai korelasi, $\mu(x)$ dan $\mu(y)$ adalah rata-rata dari *x* dan *y* dengan perhitungan seperti persamaan (4).

$$\mu(x) = \frac{1}{n}\sum_{i=1}^{n} x_i \quad \text{dan} \quad \mu(y) = \frac{1}{n}\sum_{i=1}^{n} y_i \quad (5)$$

x dan *y* adalah derajat keabuan dari *plain image* dan *cipher image*. Sedangkan perhitungan dari standar deviasi (σ) dirumuskan seperti persamaan (5).

$$\sigma(x) = \sqrt{\sum_{i=1}^{n}(x_i - \mu(x))^2} \quad (6)$$
$$\sigma(y) = \sqrt{\sum_{i=1}^{n}(y_i - \mu(y))^2}$$

Jika koefisien korelasi sama dengan *nol* maka *cipher image* sepenuhnya berbeda dengan *plain image*. Jika koefisien korelasi sama dengan *satu*, itu berarti *cipher image* identik dengan *plain image* [12].

Data Penelitian

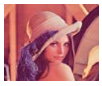
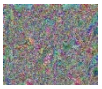
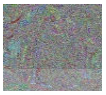
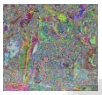
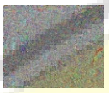
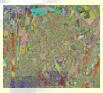
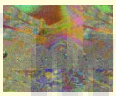
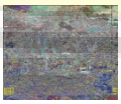
Data yang digunakan dalam penelitian ini adalah data primer dan data sekunder dari http://informatika.stei.itb.ac.id/~rinaldi.munir/Koleksi/ , berupa citra RGB dan citra *grayscale*. Metode dalam penelitian ini terdiri beberapa langkah, diantaranya:

1. Bangkitkan kunci citra, lalu konversi kedalam biner dengan kedalaman 8-bit
2. Geser 1 bit ke kiri sebanyak 6 kali pada setiap 8-bit kunci. jika angka paling kiri sebelum digeser adalah 1 maka akan di-XOR dengan 0001 1011 sedangkan jika angka paling kiri adalah 0 sebelum terjadi pergeseran maka tidak perlu di-XOR dengan 0001 1011. Kemudian ubah kembali kebentuk desimal.
3. Masukkan *plain image* kemudian diperoleh derajat keabuannya dalam bentuk desimal.
4. Lakukan operasi penjumlahan modulo 256 antara kunci yang telah mengalami pergeseran dengan *plain image*.
5. Lakukan proses *crossover* dengan memilih dua titik dari dua kromosom kemudian terjadi pertukaran bitstring diantara dua titik tersebut.
6. Lakukan proses mutasi dengan mengubah nilai gen, jika bernilai 1 maka berubah menjadi 0 dan jika bernilai 0 maka menjadi 1.

3. HASIL DAN PEMBAHASAN

Penelitian dilakukan dengan mengenkripsi 12 citra dengan kunci dan ukuran yang berbeda. Hasil proses enkripsi ditunjukkan pada Tabel 2.

Tabel 2. Hasil Enkripsi *Plain Image*

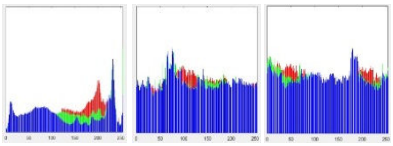
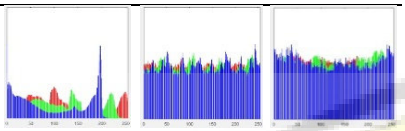
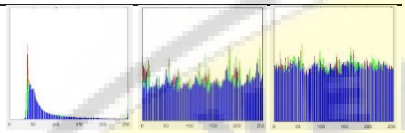
No	*Plain image*	Kunci	*Cipher Image* (*bitshift 6*)	*Cipher Image* (*bitshift 8*)
1	 (256× 256)	 (128×128)		
2	 (512×512)	 (512×512)		
3	 (512×512)	 (576 × 576)		
4	 (576×576)	 (512 × 512)		
5	 (512×512)	 (640 × 480)		
6	 (256×256)	 (678 × 508)		
7	 (640× 480)	 (442×786)		
8	 (640× 480)	 (752 × 564)		
9	 (800× 600)	 (582 × 437)		
10	 (678 ×508)	 (640 × 480)		
11	(752 ×564)	(678 × 508)		
12	(582 ×437)	(512 × 512)		

a. Analisis Histogram

Analisis histogram untuk menganalisis keamanan tentang penyebaran nilai piksel antara *plain image* dengan *cipher image*. Histogram ditunjukkan pada Tabel 3

Tabel 3 Histogram *plain image* dan *cipher image*

No	Data Penelitian	*Plain Image*	*Cipher image* (*bitshift 6*)	*Cipher image* (*bitshift 8*)
1	Citra Babon			
2	Citra Burung			
3	Citra Lada			
4	Citra Lena			
5	Citra Gadis			
6	Citra Teks			
7	Citra Mountain			
8	Citra Hotel Medan			
9	Citra Bekas Tsunami			

No	Data Penelitian	*Plain Image*	*Cipher image* (*bitshift 6*)	*Cipher image* (*bitshift 8*)
10	Citra Pulau Merah			
11	Citra Teluk Ijo			
12	Citra Malioboro			

b. Hasil Analisis Diferensial

Analisis diferensial digunakan untuk melihat besar perbedaan antara *plain image* dan *cipher image* dengan menghitung nilai NPCR dan UACI. NPCR menyatakan perubahan posisi piksel citra sebelum dan sesudah enkripsi. UACI merepresentasikan interval perubahan piksel antara *plain image* dan *cipher image*. Hasil dari analisis diferensial ditunjukkan seperti pada Tabel 4.

Tabel 4. Hasil Analisis Diferensial *plain image* dan *cipherimage* bitshift 6 dan bitshift 8

No	Citra	NPCR (%)		UACI (%)	
		Bitshif 6	Bitshif 8	Bitshif 6	Bitshif 8
1.	Babon	99,59	99,59	29,40	29,20
2.	Burung	99,63	99,62	28,35	28,31
3.	Lada	99,61	99,59	32,06	32,08
4.	Lena	99,64	99,60	28,50	29,18
5.	Gadis	99,57	99,61	30,88	31,05
6.	Teks	99,92	99,70	33,87	34,83
7.	Mountain	99,58	99,59	35,17	34,74
8.	Hotel	99,61	99,62	34,31	35,11
9.	Tsunami	99,60	99,56	34,59	34,97
10	P. Merah	99,68	99,51	34,49	33,70
11	Teluk Ijo	99,62	99,61	33,17	33,53
12	Maliobor o	99,66	99,62	34,09	33,05

c. Hasil Analisis Koefisien Korelasi.

Analisis korelasi digunakan untuk mengukur kekuatan hubungan antara *plain image* dengan *cipher image* berdasarkan nilai-nilai pikselnya seperti pada Tabel 5.

Tabel 5. Hasil analisis Koefisien Korelasi

No	Data Penelitian	Bitshift 6	Bitshift 8
1.	Citra Babon	-0,004	0,01
2.	Citra Burung	-0,01	-0,022
3.	Citra Lada	0,001	0,005
4.	Citra Lena	-0,02	0,012
5.	Citra Gadis	-0,002	-0,03
6.	Citra Teks	0,008	0,003
7.	Citra Mountain	0,0024	0,022
8.	Citra Hotel	0,0089	-0,03
9.	Citra Tsunami	-0,032	-0,078
10.	Citra P. Merah	-0,061	-0,001
11.	Citra Teluk Ijo	0,0022	-0,005
12.	Citra Malioboro	-0,023	0,079

d. Hasil Analisis ketika Dekripsi.

Analisis NPCR, UACI dan Korelasi antara *plain image* dan *decrypted image* pada bitshift 6 maupun bitshift 8 ketika proses dekripsi seperti yang ditunjukkan Tabel 6.

Tabel 6. Hasil Analisis ketika Dekripsi

No	Citra	NPCR (%)	UACI (%)	Korelasi
1.	Citra Babon	0	0	1
2.	Citra Burung	0	0	1
3.	Citra Lada	0	0	1
4.	Citra Lena	0	0	1
5.	Citra Gadis	0	0	1
6.	Citra Teks	0	0	1
7.	Mountain	0	0	1
8.	Citra Hotel	0	0	1
9.	Tsunami	0	0	1
10	P. Merah	0	0	1
11	Teluk Ijo	0	0	1
12	Malioboro	0	0	1

Hasil penelitian menunjukkan bahwa proses enkripsi berjalan dengan baik dengan adanya perubahan piksel antara *plain image* dengan *cipher image*, dan susah untuk ditebak gambar aslinya serta tidak mengandung cukup informasi dari *plain image*. Proses enkripsi citra menghasilkan citra yang terlihat acak dan tidak berpola. Secara visual, dari *cipher image* yang dihasilkan, bitshift 6 lebih baik daripada bitshift 8 karena bitshift 6 lebih terlihat acak dari kerapatan titik-titiknya.

Proses dekripsi berhasil mengembalikan *cipher image* menjadi citra sebenarnya (*plain image*) tanpa ada piksel yang berubah. Hal ini didasarkan pada nilai NPCR dan UACI antara *plain image* dengan citra hasil dekripsi sebesar 0% dan nilai korelasi sebesar 1, yang berarti bahwa semua piksel antara *plain image* dengan citra hasil dekripsi adalah sama.

Adapun hasil dari analisis histogram menghasilkan histogram yang tidak merata pada *plain* image karena ada beberapa piksel yang mendominasi sedangkan histogram *cipher image* penyebaran nilai pikselnya merata karena tidak ada piksel yang mendominasi sehingga *cipher image* yang dihasilkan tidak rentan dan tahan terhadap serangan kriptanalis dan metode yang diajukan cukup aman. Histogram bitshift 6 dan bitshift 8 hampir tidak dapat dibedakan dari 12 perlakuan dalam penelitian,

Terlihat pada uji diferensial menggunakan nilai NPCR, bitshift 6 lebih baik dari bitshift 8, karena sebagian besar nilai NPCR bitshift 6 lebih besar dari bitshift 8. Yaitu pada citra burung, citra lada, citra lena, citra teks, citra tsunami, citra pulau merah, citra teluk ijo dan citra malioboro seperti yang ditunjukkan pada Tabel 4. Sedangkan nilai UACI yang diperoleh adalah sebesar 28,35% hingga 35,17%. Pada Tabel 4 nilai NPCR telah memenuhi nilai batas minimumnya yaitu 98,87%. Untuk nilai UACI terdapat beberapa citra yang tidak memenuhi batas nilai minimumnya tetapi masih mendekati nilai minimum yang dianjurkan. Meskipun terdapat beberapa citra yang tidak memenuhi batas minimum nilai UACI, namun citra tersebut masih kuat terhadap serangan kriptanalis, dibuktikan secara visual bahwa *cipher image* yang dihasilkan terlihat acak dan tidak berpola

Dari Tabel 5 juga terlihat bahwa bitshift 6 lebih baik daripada bitshift 8 karena hasil nilai koefisien korelasi bitshift 6 lebih mendekati 0 yang menunjukkan bahwa *cipher image* yang dihasilkan benar-benar berbeda dengan *plain image*. Hasil analisis koefisien korelasi antara citra hasil dekripsi dengan *plain image* pada Tabel 6 menunjukkan nilai 1, itu artinya citra hasil dekripsi dengan *plain image* adalah identik karena terdapat korelasi yang kuat diantara piksel-piksel pada citra tersebut.

4. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, didapat beberapa kesimpulan sebagai berikut:

a. Pada proses enkripsi, citra akan melewati tahap *crossover* dua titik dan dilanjutkan dengan mutasi yaitu perubahan nilai bit dari 0 menjadi 1 dan sebaliknya, serta kunci yang digunakan akan mengalami pergeseran 1-bit ke kiri sehingga didapatkan hasil akhir *cipher image* yang terlihat acak dan tidak berpola. *Cipher image* yang dihasilkan sepenuhnya berbeda dengan *plain image*. Sedangkan pada proses dekripsi dapat mengembalikan *cipher image* menjadi citra yang sebenarnya tanpa menghilangkan informasi yang terkandung didalamnya.
b. Berdasarkan hasil analisis keamanan dilihat dari histogram, NPCR, UACI, dan koefisien korelasi. Penyandian citra dengan operator Algoritma Genetika memiliki tingkat keamanan yang tinggi sehingga sulit untuk diserang oleh kriptanalis.

5. DAFTAR PUSTAKA

[1] Sindhuja, K., dan P. Devi. 2014. A Symmetric Key Encryption Technique Using Genetic Algorithm. *International Journal of Computer Science and Information Technologies (IJCSIT)* 5 (1): 414-416

[2] Pujari, S. K., G. Bhattacharjee, dan S. Bhoi. 2017. A Hybridized Model for Image Encryption through Genetic Algorithm and DNA Sequence. *6th International Conference on Smart Computing and Communications (ICSCC)* 125 (2018): 165-171.

[3] Setyaningsih, E. 2015. *Kriptografi dan Implementasinya Menggunakan MATLAB.* Yogyakarta: ANDI.

[4] Ariyus, D. 2008. *Pengantar Ilmu Kriptografi.* Yogyakarta: ANDI.

[5] Ahmad, U. 2005. *Pengolahan Citra Digital dan Teknik Pemrogramannya.* Yogyakarta: GRAHA ILMU.

[6] Hardjo, A. B. 2016. Enkripsi Citra RGB dengan Algoritma Simplified-Data Encryption Standard (S-DES) dan DNA-Vigenere Cipher. *Skripsi*. Jember: Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember.

[7] Latif, S., J. Qayyum, M. Lal, dan F. Khan. 2011. Complete Description of Well-Known Number Systems using Single Table. *International Journal of Electrical and Computer Sciences IJECS* 11 (3):23-29.

[8] Stallings, W. 2006. *Cryptography and Network Security: Principles and Practices*. New Jersey: Pearson Education Inc Standard (S-DES) dan DNA-Vigenere Cipher. *Skripsi*. Jember: Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember.

[9] Dias, M., C. Suhery, dan T. Rismawan. 2016. Penerapan Kriptografi Menggunakan Algoritma Knapsack, Algoritma Genetika, dan Algoritma Arnold's Catmap pada Citra. *Jurnal Coding, Sistem Komputer Untan* 4 (2): 119-129.

[10] Behnia, S., A. Akhshani, S. Ahadpour, H. Mahmodi, dan A. Akhavan. 2007. A Fast Chaotic Encryption Scheme Based on Piecewise Nonlinear Chaotic Maps. *Physics Letters A* 366: 391-396

[11] Boriga, R. E., A. C. Dăscălescu, dan A. V. Diaconu. 2014. A New Fast Image Encryption Scheme Based on 2D Chaotic Maps. *IAENG International Journal of Computer Science* 41 (4).

[12] Mousa, A., O.S. Faragallah, S. El-Rabaie, dan E.M. Nigm. 2013. Security Analysis of Reverse Encryption Algorithm for Databases. *International Journal of Computer Applications (0975-8887)* 66 (14): 19-27.