e-JOURNAL UNEJ ISSN: 2339-0069

Publikasi Ilmiah Elektronik Universitas Jember

http://jurnal.unej.ac.id/

BERKALA SAINSTEK

9 772339 006008

BERKALA SAINSTEK (BST) is published by University of Jember.

Mailing Address

Universitas Jember
Jl. Kalimantan 37 Kampus Tegalboto 68121
Email: berkala.sainstek@unej.ac.id
URL: https://jurnal.unej.ac.id/index.php/BST/index

Focus and Scope

BERKALA SAINSTEK (BST) is a national peer-reviewed and open access journal that publishes research papers encompasses all aspects of natural sciences, engineering, technology and computer science. All accepted manuscripts will be published worldwide BST has been indexed in OCLC WorldCat, Crossref, Google Scholar, and Base.

Editorial Board

Reviewer

Vol 6 No 2 (2018)

Published: 2018-12-31

Articles

Implementasi Algoritma *Reversed Vigenere Encryption* pada Pengamanan Citra

(Implementation of Reversed Vigenere Encryption Algorithm on Image Security)

Ahmad Rico Santoso, Abduh Riski, Ahmad Kamsyakawuni
Jurusan Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Jember (UNEJ)
Jln. Kalimantan 37, Jember 68121
E-mail: risky.fmipa@unej.ac.id

Abstrak

Pengamanan data atau informasi penting dilakukan untuk mencegah bocornya suatu pesan atau informasi kepada orang yang tidak berhak menerima. Pengamanan suatu data dapat dilakukan dengan menggunakan suatu teknik penyandian yang dinamakan dengan kriptografi. Pada penelitian ini, data yang digunakan adalah pesan/informasi berupa citra RGB sebanyak 10 buah citra. Pesan atau informasi pada penelitian disandikan menggunakan algoritma *Reversed Vigenere Encryption*. Tujuan dari penyandian citra RGB ini adalah untuk mengetahui bagaimana langkah-langkah enkripsi dan dekripsi serta hasil keamanan dari penyandian citra terhadap serangan-serangan kriptoanalisis. Adapun metode yang digunakan untuk menganalisis hasil enkripsi adalah anilisis histogram dan analisis diferensial. Hasil dari proses enkripsi dan dekripsi citra dapat dilakukan dengan baik namun masih menghasilkan *cipherimage* yang membentuk sebagian pola dari citra asli sehingga mudah ditebak oleh seseorang. Pada analisis histogram nilai-nilai *pixels* dari *cipherimage* belum menyebar secara merata sehingga hasil dari enkripsi citra masih memiliki ketahanan yang lemah terhadap serangan-serangan kriptoanalisis tipe statistik. Pada analisis diferensial, nilai NPCR menghasilkan nilai 100% yang berarti setiap *pixels* pada citra asli berubah bentuk secara total.

Kata Kunci: Kriptografi, Citra RGB, *Reversed Vigenere Encryption*.

Abstract

Security of data or information is important to prevent leaking of a message or information to people who are not eligible to receive. Security of a data can be done by using an encryption technique called cryptography. In this research, the data used is the message/information in the form of RGB image as much as 10 pieces of image. The message or information on the research is encrypted using Reversed Vigenere Encryption algorithm. The purpose of RGB image encoding is to find out how the encryption and decryption steps and the security results of image encoding against cryptanalysis attacks. The method used to analyze the results of the encryption is histogram analysis and differential analysis. The results of the encryption process and image decryption can be done well but still produce cipherimage that forms part of the pattern from the original image so easily guessed by someone. In the histogram analysis the pixels values of cipherimage have not spread evenly so that the results of the image encryption still have weak resistance against statistical type cryptanalysis attacks. In differential analysis, the value of NPCR yields a value of 100% which means that each pixels in the original image is totally transformed.

Keywords: *Kriptografi, Citra RGB, Reversed Vigenere Encryption.*

PENDAHULUAN

Perkembangan teknologi dan informasi pada saat ini berkembang sangat pesat dengan berbagai fitur-fitur terbaru. Perkembangan teknologi dan informasi ini masih perlu diperhatikan terutama masalah keamanan data dan informasi. Pengamanan data dan informasi penting dilakukan untuk mencegah bocornya suatu pesan atau informasi kepada orang yang tidak berhak menerima. Oleh karena itu, pengamanan suatu data perlu diperhatikan dan dilakukan dengan menggunakan suatu teknik yang dinamakan dengan kriptografi. Kriptografi merupakan suatu ilmu dan seni untuk melindungi atau menyembunyikan pesan/informasi agar tidak mudah diketahui oleh orang yang tidak berhak menerima pesan/informasi. Pada penelitian ini, penyandikan pesan/informasi dalam bentuk citra RGB. Pesan atau informasi yang disandikan menggunakan algoritma kriptografi klasik yaitu algoritma *Reversed Vigenere Encryption*. Sebelumnya Sengupta [7] telah menggunakan algoritma *Reversed Vigenere Encryption* untuk mendesain suatu sistem keamanan pada sistem *cloud computing*. Pada penelitian tersebut, algoritma *Reversed Vigenere Encryption* pada dasarnya sama dengan algoritma *Vigenere Cipher*, hanya saja kunci pada algoritma ini dibalik atau dilakukan transposisi kebalikan (*permutation reversed*). Pada penelitian ini, algoritma *Reversed Vigenere Encryption* akan diterapkan pada pengamanan citra. Tujuan dilakukan penelitian ini adalah untuk mengetahui bagaimana hasil penyandian citra serta hasil keamanannya terhadap serangan-serangan kriptoanalisis.

Dasar Teori

Kriptografi

Kriptografi merupakan suatu ilmu atau teknik yang digunakan untuk menyembunyikan suatu pesan/informasi agar tidak dapat diketahui oleh pihak yang tidak berhak mendapatkan informasi tersebut. Secara bahasa kriptografi

berasal dari bahasa yunani yaitu "crypto" dan "graphia". Kata "crypto" berarti rahasia dan "graphia" berarti tulisan. Sehingga menurut terminologi, kriptografi merupakan suatu ilmu dan seni untuk menjaga keamanan atau kerahasiaan pesan ketika pesan dikirim dari suatu tempat ketempat yang lain [1].

Teknik Transposisi

Teknik transposisi merupakan teknik memindahkan posisi karakter teks asli ke posisi teks lain tanpa mengubah nilai aslinya. Salah satu contoh sederhana dari teknik transposisi adalah teknik transposisi columnar. Teknik transposisi columnar mengubah karakter teks asli dengan cara menulis karakter teks asli dengan orientasi baris dengan panjang karakter yang sama kemudian teks sandi didapatkan dengan menulis ulang teks sesuai kolom yang disepakati sebelumnya.

Sebagai contoh, teks asli adalah "JURUSAN MATEMATIKA", maka dengan menulis tabel yang terdiri dari 6 kolom dengan orientasi baris didapatkan:

Kunci	:	4 2 1 6 3 5
Teks asli	:	J U R U S A
		N M A T E M
		A T I K A X

String X digunakan untuk mengisi sel kosong pada tabel. Selanjutnya tulis teks sandi sesuai dengan urutan berdasarkan kunci dengan orientasi kolom sehingga didapatkan teks sandi:

RAIUMTSEAJNAAMXUTK [6].

Vigenere Cipher

Vigenere cipher merupakan teknik enkripsi pada kriptografi klasik yang diperkenalkan oleh diplomat Perancis, yaitu Blaise de Vigenere pada Abad 16 pada tahun 1586. Sebelumnya Giovon Batista telah memperkenalkan untuk pertama kali pada tahun 1553 seperti yang terdapat dalam buku *La Cifra del Sig.* Algoritma ini baru dikenal luas setelah 200 tahun kemudian dan dinamakan kode *Vigenere* untuk digunakan oleh tentara Konfederasi (*Confederate Army*) pada Perang Sipil Amerika. Kode *Vigenere* berhasil dipecahkan oleh Babbage dan Kasiski pada pertengahan Abad 19. Pada teknik substitusi *vigenere* setiap teks kode bisa memiliki banyak kemungkinan teks asli. Teknik dari substitusi vigenere cipher bisa dilakukan dengan dua cara yaitu dengan menggnakan angka dan menggunakan huruf [2].

Vigenere Cipher Menggunakan Angka

Kunci yang digunakan pada *vigenere cipher* dibuat berulang sepanjang plainteks sehingga jumlah huruf pada kunci akan sama dengan jumlah huruf pada plainteks. Pergeseran setiap huruf pada plainteks akan ditentukan oleh huruf pada kunci yang mempunyai posisi yang sama dengan huruf pada plainteks. Adapun fungsi enkripsi dan dekripsi pada vigenere cipher adalah seperti pada Persamaan (1) dan Persamaan (2) berikut:

$$Ci = E(Pi) = (Pi + Ki) \bmod 26 \quad (1)$$

$$Pi = D(Ci) = (Ci - Ki) \bmod 26 \quad (2)$$

dengan Ci = Cipherteks, Pi = Plainteks dan Ki = Kunci [4].

Vigenere Cipher Menggunakan Huruf

Teknik substitusi *vigenere cipher* menggunakan huruf bisa digunakan tabel sebagai berikut:

Tabel 3.1 Substitusi *Vigenere Cipher* Menggunakan Huruf

Kunci \ Plainteks	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Plainteks :SAYA BELAJAR KRIPTOGRAFI CITRA
Kunci :SAYA BELAJAR KRIPTOGRAFI CITRA
Cipherteks:KAWA CIWASAI UIQEMCMIAKQ EQMIA

Cara menentukan cipherteks pada system ini, pada tabel bisa dilihat pada posisi horizontal merupakan plainteks dan pada posisi vertical kunci, jika plainteks huruf K maka lihat posisi letak huruf K pada plainteks tabel dan posisi huruf K pada posisi kunci, jika sudah menemukan tarik garis lurus kebawah dari plainteks dan garis lurus kesamping dari posisi kunci sehingga menemukan huruf U, maka huruf U yang akan menjadi cipherteks dan begitu seterusnya [1].

Reversed Vigenere Encryption

Reversed Vigenere Encryption merupakan algoritma kriptografi klasik seperti *Vigenere cipher* pada umumnya tetapi kunci yang digunakan pada algoritma dilakukan transposisi kebalikan (*permutation reversed*) terlebih dahulu. Sebagai contoh yaitu jika terdapat kunci yang akan digunakan adalah "KEAMANAN" maka kunci tersebut dilakukan transposisi kebalikan (*permutation reversed*) terlebih dahulu sehingga kunci akhir yang akan digunakan adalah "NANAMAEK" [7].

Analisis Histogram

Analisis histogram merupakan analisis yang digunakan untuk memperkirakan keamanan dan ketahanan hasil enkripsi dari serangan-serangan kriptanalisis tipe statistik. Pada analisis histogram suatu citra yang terenkripsi harus memiliki penyebaran enkripsi pada nilai-nilai *pixel* di setiap saluran warna secara merata agar penyerang tidak dapat mengekstrak informasi statistik dari frekuensi nilai-nilai *pixel* di setiap saluran warna [3].

Analisis Diferensial

Analisis diferensial digunakan untuk menguji pengaruh perubahan setiap *pixel* pada citra yang terenkripsi. Terdapat dua Indikator pengukuran yang umum digunakan pada analisis ini yaitu *Number of Pixels Change Rate* (NPCR) dan *Unified Average Changing Intensity* (UACI). *Number of Pixels Change Rate* (NPCR) merupakan persentase

banyaknya *pixels* yang berubah pada citra asli ketika dienkripsi sedangkan *Unified Average Changing Intensity* (UACI) merupakan persentase perubahan warna terpadu pada citra asli ketika dienkripsi melalui selisih antara nilai-nilai *pixels* pada citra asli dengan citra hasil enkripsi. Adapun perhitungan NPCR didefinisikan sebagai berikut:

$$NPCR = \left(\frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} d_{i,j} \right) \times 100 \quad (3)$$

yang mana m dan n adalah lebar dan tinggi citra sedangkan $d_{i,j}$ ditentukan sebagai berikut:

$$d_{i,j} = \begin{pmatrix} 0, & jika\ c_{i,j}^{(1)} = c_{i,j}^{(2)} \\ 1 & jika\ c_{i,j}^{(1)} \neq c_{i,j}^{(2)} \end{pmatrix}$$

yang mana $c_{i,j}^{(1)}$ dan $c_{i,j}^{(2)}$ merupakan nilai derajat keabuan dari baris *i* dan kolom *j* dari citra $c^{(1)}$ dan citra $c^{(2)}$.

Sedangkan perhitungan UACI didefinisikan sebagai berikut:

$$UACI = \left(\frac{1}{m \times n} \sum_{i=0}^{m-1} \frac{\sum_{j=0}^{n-1} \left(c_{i,j}^{(1)} - c_{i,j}^{(2)} \right)}{255} \right) \times 100 \quad (4)$$

Secara teori, nilai minimum yang baik pada indikator NPCR adalah sebesar 99,6094% dan pada indikator UACI sebesar 33,4635% [5] sedangkan menurut Boriga, dkk. [3] nilai pada indikator NPCR dapat dikatakan tahan terhadap serangan diferensial pada nilai minimal 98,87% dan pada indikator UACI sebesar minimal 32,17%.

METODE PENELITIAN

Data Penelitian

Data yang digunakan pada penelitian kali ini adalah citra RGB berdimensi 128 x 128 *pixels* yang disebut sebagai *plainimage*. Data yang akan diuji sebanyak 10 citra. Berikut adalah data-data yang akan digunakan pada penelitian:

Gambar 1. Citra Paprika

Gambar 2. Citra Babon

Gambar 3. Citra Lena

Gambar 4. Citra Perempuan

Sumber: www.informatika.stei.itb.ac.id/~rinaldi.munir/.../CitraUji.htm
Sumber: pemrogramanmatlab.files.wordpress.com/2016/09/lena.jpg

Gambar 5. Citra Buah

Gambar 6. Citra Jodipan

Gambar 7. Citra Pelangi

Gambar 8. Citra Tulip

Gambar 9. Citra Pramuka

Gambar 10. Citra Kawah Ijen

Sumber: http://bobo.grid.id/Sains/Iptek/Fakta...Pelangi
Sumber: https://ilmubudidaya.com/cara-menanam...tulip
Sumber: http://www.sehatfresh.com/buah-yang...remaja/
Sumber: sekilaskendari.blogspot.co.id/2017/12/...html

Langkah Penelitian

Adapun langkah-langkah pada penelitian kali ini adalah sebagai berikut:

a. Studi literatur mengenai citra dan kriptografi khususnya tentang teori yang berkaitan dengan algoritma Reversed Vigenere Encryption

b. Percobaan enkripsi dan dekripsi citra RGB menggunakan gabungan Reversed Vigenere Encryption

c. Pembuatan program enkripsi dan dekripsi citra RGB

d. Uji coba program enkripsi dan dekripsi citra RGB menggunakan aplikasi yang telah dibuat

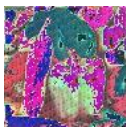
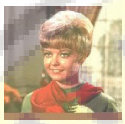
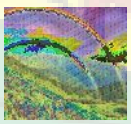
Analisis hasil program enkripsi dan dekripsi citra RGB menggunakan analisis histogram dan analisis diferensial.

HASIL PENELITIAN

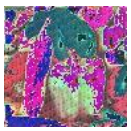
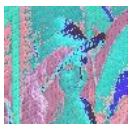
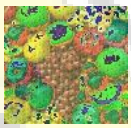
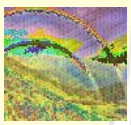
Pada penelitian ini, data yang digunakan adalah citra RGB berdimensi 128 x 128 *pixels* sebanyak 10 buah citra. Langkah-langkah proses enkripsi dan dekripsi dilakukan menggunakan Persamaan (1) dan Persamaan (2) dengan kunci berupa karakter yang dibalik.

Adapun hasil enkripsi dan dekripsi citra dari data penelitian menggunakan metode algoritma *Reversed Vigenere Encryption* adalah sebagai berikut:

Tabel 1. Hasil Enkripsi pada *Plainimage*

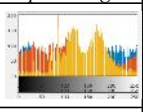
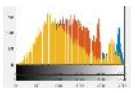
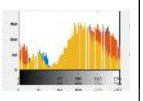
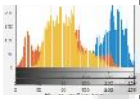
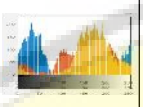
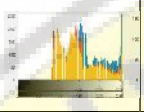
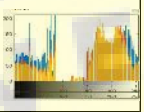
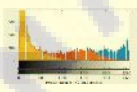
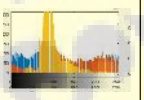
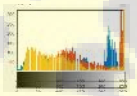
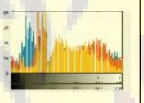
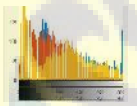
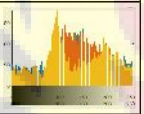
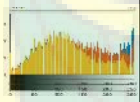
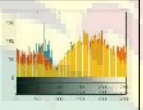
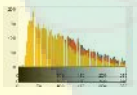
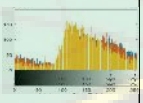
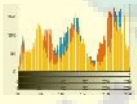
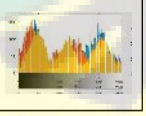
No	Data Penelitian	*Plainimage*	*Cipherimage*
1	Citra Paprika		
2	Citra Babon		
3	Citra Lena		
4	Citra Anak Perempuan		
5	Citra Buah		
6	Citra Kampung Jodipan		
7	Citra Pelangi		
8	Citra Bunga Tulip		
9	Citra Pramuka		
10	Citra Kawah Ijen		

Tabel 2. Hasil Dekripsi pada *Cipherimage*

No	Data Penelitian	*Cipherimage*	*Plainimage*
1	Citra Paprika		
2	Citra Babon		
3	Citra Lena		
4	Citra Anak Perempuan		
5	Citra Buah		
6	Citra Kampung Jodipan		
7	Citra Pelangi		
8	Citra Bunga Tulip		
9	Citra Pramuka		
10	Citra Kawah Ijen		

Adapun hasil analisis histogram dan analisis diferensial akan ditampilkan pada Tabel 3 dan Tabel 4.

Tabel 3. Hasil Histogram pada *Plainimage* dan *Cipherimage*

No	Data Penelitian	Histogram *Plainimage*	Histogram *Cipherimage*
1	Citra Paprika		
2	Citra Babon		
3	Citra Lena		
4	Citra Anak Perempuan		
5	Citra Buah		
6	Citra Kampung Jodipan		
7	Citra Pelangi		
8	Citra Bunga Tulip		
9	Citra Pramuka		
10	Citra Kawah Ijen		

Tabel 4. Hasil Nilai NPCR dan UACI

No	Data Penelitian	Nilai NPCR	Nilai UACI
1	Citra Paprika	100%	38,1455%
2	Citra Babon	100%	35,0934%
3	Citra Lena	100%	38,0692%
4	Citra Anak Perempuan	100%	42,9228%
5	Citra Buah	100%	35,7417%
6	Citra Kampung Jodipan	100%	42,8014%
7	Citra Pelangi	100%	34,4879%
8	Citra Bunga Tulip	100%	39,8137%
9	Citra Pramuka	100%	33,4116%
10	Citra Kawah Ijen	100%	42,5391%

Proses enkripsi dan dekripsi pada data penelitian menggunakan kunci = JURUSAN MATEMATIKA. Berdasarkan hasil enkripsi pada data penelitian, proses enkripsi pada citra berjalan dengan baik namun hasil enkripsi masih membentuk pola trhadap citra asli sehingga masih mudah diduga bagaimana bentuk citra aslinya. Proses Enkripsi citra RGB menggunakan algoritma *Reversed Vigenere Encryption* dengan modifikasi algoritma *Skipjack* mengalami perubuhan *pixels* secara signifikan terhadap citra aslinya. Hal ini didasarkan pada nilai NPCR yang mencapai 100% yang menandakan bahwa *pixels* pada *plainimage* terenkripsi secara keseluruhan. Pada proses dekripsi, *cipherimage* berhasil dikembalikan sesuai dengan bentuk citra aslinya (*plainimage*) tanpa ada nilai-nilai *pixels* pada citra asli yang berubah. Berdasarkan hasil histogram, nilai-nilai *pixels* pada *ciphermage* masih belum menyebar secara merata sehingga berdasarkan teori [3] dapat dikatakan bahwa *cipherimage* yang dihasilkan dengan menggunakan metode *Reversed Vigenere* masih memiliki ketahanan yang lemah terhadap serangan-serangan kriptoanalisis tipe statistik. Pada hasil penelitian, nilai UACI yang diperoleh menggunakan metode *Reversed Vigenere Encryption* didapatkan hasil sebesar 33,4116% hingga 42,9228%. Berdasarkan teori analisis diferensial [3], *cipherimage* yang dihasilkan dapat dikatakan baik terhadap serangan diferensial. Hal ini didasarkan pada nilai NPCR dan UACI yang telah memenuhi nilai batas minimal.

KESIMPULAN

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

a. Proses Enkripsi *plainimage* menggunakan algoritma *Reversed Vigenere Encryption* menghasilkan *cipherimage* yang masih membentuk sebagian pola terhadap citra asli sehingga masih mudah diduga bagaimana bentuk *plainimage*.
b. Proses Dekripsi *cipherimage* menggunakan gabungan algoritma *Reversed Vigenere Encryption* dapat dilakukan dengan baik tanpa mengubah nilai-nilai *pixels* pada citra aslinya.
c. *Chiperimage* yang dihasilkan dari proses enkripsi menggunakan metode algoritma *Reversed Vigenere Encryption* masih memiliki ketahanan yang lemah terhadap serangan-serangan kriptoanalisis tipe statistik. Hal ini didasarkan pada hasil analisis histogram pada *cipherimage* yang memiliki penyebaran nilai-nilai *pixels* yang belum tersebar secara merata.

Berdasarkan analisis diferensial, *cipherimage* yang dihasilkan masih kuat dan tahan terhadap serangan diferensial. Hal ini didasarkan pada nilai NPCR dan UACI yang dihasilkan telah memenuhi batas minimal nilai NPCR dan UACI.

DAFTAR PUSTAKA

[1] Ariyus, D. 2006. *Kriptografi Keamanan Data dan Komunikasi*. Yogyakarta: Graha Ilmu.
[2] Ariyus, D. 2008. *Pengantar Ilmu Kriptografi*. C.V Andi Offset.

[3] Boriga, R.E., A.C. Dascalescu dan A.V. Diaconu. 2014. A New Fast Image Encryption Scheme Based on 2D Chaotic Maps. https://pdfs.semanticscholar.org/3c7e/a5908fe266ef743260fcd3bb98992238a6fc.pdf [Diakses pada 12 Maret 2018].

[4] Hallim, A., I.U. Nadhori dan Setiawardhana. 2010. Pembuatan Perangkat Lunak Media Pembelajaran Kriptografi Klasik. http://repo.pens.ac.id/444/1/873.pdf [Diakses pada 9 April 2018].

[5] Kwok, H.S. dan W.K.S. Tang. A Fast Image Encryption System Based on Chaotics Maps with Finite Precision Representation. https://pdfs.semanticscholar.org/1c97/58e931426b892d75cf640917d88aa87d05d4.pdf [Diakses pada 24 Maret 2018].

[6] Sadikin, R. 2012. *Kripografi Untuk Keamanan Jaringan*. Yogyakarta: C.V Andi Offset.

[7] Sengupta, N. dan J. Holmes. 2013. Designing of Cryptography Based Security System for Cloud Computing. *International Conference on Cloud & Ubiquitous Computing & Emerging Technologies*. 20: 53.