PENYANDIAN CITRA DIGITAL MENGGUNAKAN GABUNGAN ALGORITMA *PLAYFAIR*, ALGORITMA *VIGENERE* DAN *SHIFTROW*

SKRIPSI

Oleh

Nazar Amir
NIM 151810101015

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS JEMBER
2019

PENYANDIAN CITRA DIGITAL MENGGUNAKAN GABUNGAN ALGORITMA *PLAYFAIR*, ALGORITMA *VIGENERE* DAN *SHIFTROW*

SKRIPSI

diajukan guna memenuhi tugas akhir dan memenuhi salah satu syarat
untuk menyelesaikan Program Studi Matematika (S1)
dan mencapai gelar Sarjana Sains

Oleh

Nazar Amir
NIM 151810101015

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS JEMBER
2019

PERSEMBAHAN

Dengan nama Allah SWT Yang Maha Pengasih dan Maha Penyayang, skripsi ini saya persembahkan kepada:

1. Orang tua saya Bapak H. Mahmud bin Entan dan Ibu Hj. Aminah yang selalu mendoakan serta memberikan dukungan, semangat, dan materi.
2. Keluarga Besar di Jakarta yang selalu mengirimkan doa, semangat maupun nasihat.
3. Seluruh jajaran guru SDN 02 Pondok Kelapa, MTsN 42 Jakarta, dan MAN 9 Jakarta yang telah memberikan banyak ilmu dan pengetahuan.
4. Sahabat 'Songong' Bayu, Dwi, Ega, Hadi, Mahrita, Rencek, Salsa, dan Yanti yang selalu menemani dalam proses pengerjaan skripsi.
5. Teman-teman seperjuangan SIGMA'15 yang selalu memberikan semangat selama perkuliahan.
6. UKMS TITIK yang telah memberikan pengalaman organisasi yang luar biasa serta menjadi keluarga kedua selama berada di Jember.
7. Keluarga Besar MAN 9 Jakarta (GAMASETA) yang telah banyak membantu selama di Jember.
8. Semua pihak yang membantu penulis dalam menyelesaikan tugas akhir.

MOTTO

"*Allah tidak membebani seseorang, melainkan sesuai kemampuannya*".[1]

"Punya 1 ide fokus untuk dikerjakan lebih baik dari 100 ide hebat yang hanya jadi wacana".[2]

[1] Qs Al-baqarah 2:286

[2] Atta Halilintar

PERNYATAAN

Saya yang bertanda tangan dibawah ini:

nama : Nazar Amir

NIM : 151810101015

menyatakan dengan sesungguhnya bahwa karya ilmiah yang berjudul "Penyandian Citra Digital Menggunakan Gabungan Algoritma Playfair, Algoritma Vigenere dan Shiftrow" adalah benar-benar hasil karya sendiri, kecuali kutipan yang sudah saya sebutkan sumbernya, belum pernah diajukan pada institusi mana pun, dan bukan karya jiplakan. Saya bertanggung jawab atas keabsahan dan kebenaran isinya sesuai dengan sikap ilmiah yang harus dijunjung tinggi.

Demikian pernyataan ini saya buat dengan sebenarnya, tanpa ada tekanan dan paksaan dari pihak mana pun serta bersedia mendapat sanksi akademik jika ternyata di kemudian hari pernyataan ini tidak benar.

Jember, April 2019

Yang menyatakan,

Nazar Amir

NIM 151810101015

SKRIPSI

PENYANDIAN CITRA DIGITAL MENGGUNAKAN GABUNGAN ALGORITMA PLAYFAIR, ALGORITMA VIGENERE DAN SHIFTROW

Oleh

Nazar Amir
NIM 151810101015

Pembimbing

Dosen Pembimbing Utama : Abduh Riski, S.Si, M.Si.

Dosen Pembimbing Anggota : Ahmad Kamsyakawuni, S.Si, M.Kom.

PENGESAHAN

Skripsi berjudul "Penyandian Citra Digital Menggunakan Gabungan Algoritma Playfair, Algoritma Vigenere, dan Shiftrow" telah diuji dan disahkan pada:

hari, tanggal :

tempat :Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember.

Tim Penguji

Ketua,	Anggota I,
Abduh Riski, S.Si, M.Si.	Ahmad Kamsyakawuni, S.Si, M.Kom.
NIP. 199004062015041001	NIP. 197211291998021001
Anggota II,	Anggota III,
Kiswara Agung Santoso, S.Si., M.Kom.	Kusbudiono, S.Si., M.Si.
NIP. 197209071998031003	NIP. 197704302005011001

Mengesahkan

Dekan,

Drs. Sujito, Ph.D.

NIP. 196102041987111001

RINGKASAN

Penyandian Citra Digital Menggunakan Gabungan Metode Algoritma Playfair, Algoritma Vigenere, dan Shiftrow; Nazar Amir, 151810101015; 2019: 41 halaman; Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember.

Semakin berkembangnya kemajuan teknologi dan komunikasi membuat manusia dapat mengirimkan sebuah pesan ataupun informasi dengan sangat cepat dan mudah. Namun terdapat banyak kasus-kasus kejahatan pencurian data serta informasi yang bersifat rahasia sehingga dibutuhkan teknik pengamanan data teks maupun citra. Penggunaan teknik tersebut sangat penting untuk menjaga kerahasiaan suatu pesan.

Kriptografi merupakan sebuah cabang ilmu yang bertujuan untuk menjaga kerahasiaan sebuah informasi yang terdapat dalam sebuah pesan sehingga tidak mudah untuk diketahui oleh pihak yang tidak bertanggungjawab. Setyaningsih (2009), telah melakukan enkripsi pada data berupa citra digital menggunakan playfair cipher. Namun hasil yang didapat tidak terlalu baik karna *cipherimage* yang dihasilkan masih dapat dengan mudah dikenali bentuknya. Menurutnya tingkat keamanan akan lebih kuat apabila menggabungkan beberapa teknik dibandingkan menggunakan teknik cipher tunggal.. Setyaningsih (2011), mengembangkan teknik super enkripsi dimana dia melakukan penyandian citra menggunakan metode vigenere cipher yang dilanjutkan dengan playfair cipher. Hasil yang didapatkan memiliki tingkat keamanan yang lebih baik dibandingkan penelitian sebelumnya.

Data yang digunakan dalam penelitian ini adalah citra RGB dan citra *grayscale* yang akan digunakan sebagai *plain image* dan dua buah kunci matriks 16 x 16. Citra tersebut akan dienkripsi menggunakan algoritma *playfair* kemudian dilakukan pergeseran baris *(shift Rows),* dan dilanjutkan dengan enkripsi menggunakan algoritma *vigenere.* Hasil enkripsi yang didapatkan adalah sebuah *cipher image* yang berbeda dengan *plain image.*

Analisis keamanan dari algoritma yang dihasilkan menggunakan metode yang diajukan memiliki nilai analisis yang cukup baik dibandingkan dengan penelitian sebelumnya sehingga algoritma tersebut aman dari serangan statistik. Cipherimage yang dihasilkan memiliki nilai berkisar antara 99,5611% sampai 99,6281% untuk analisis NPCR dan 29,549% sampai 49,6577% untuk nilai analisis UACI. Untuk uji korelasi *cipherimage* yang dihasilkan menggunakan metode yang diajukan memiliki nilai sebesar -0,00585 sampai 0,0047655. Seluruh cipherimage memiliki penyebaran histogram yang cukup merata dibandingkan dengan metode lainnya. Hasil proses dekripsi berhasil mengembalikan *cipherimage* kembali seperti *plainimage* tanpa ada perubahan sedikitpun. Setelah dilakukan uji analisis korelasi antara *plainimage* dan *cipherimage* memiliki nilai sebesar 1, dan nilai 0 untuk uji analisis diferensial.

PRAKATA

Puji syukur kepada Allah SWT atas segala rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan tugas akhir yang berjudul "Penyandian Citra Digital Menggunakan Gabungan Algoritma Playfair, Algoritma Vigenere, dan Shiftrow". Tugas akhir ini disusun untuk memenuhi salah satu syarat pada program pendidikan strata satu (S1) Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember.

Pada kesempatan ini penulis mengucapkan terima kasih atas bantuan dan bimbingan dalam penyusunan tugas akhir ini, terutama kepada yang terhormat:

1. Drs. Sujito, Ph.D., selaku Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember;
2. Kusbudiono, S.Si., M.Si., selaku Ketua Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember;
3. Abduh Riski, S.Si., M.Si., selaku Dosen Pembimbing Utama dan Ahmad Kamsyakawuni, S.Si., M.Kom., selaku Dosen Pembimbing Anggota;
4. Kiswara Agung Santoso, S.Si., M.Kom. selaku Dosen Penguji I dan Kusbudiono, S.Si., M.Si., selaku Dosen Penguji II;
5. Kedua orang tua, Bapak H. Mahmud bin Entan dan HJ. Aminah, serta abang-abang, mpok-mpok dan adik yang selalu memberi dukungan dan doa;
6. Dosen dan Karyawan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember;
7. Teman-teman SIGMA yang telah memberikan banyak kenangan, dukungan, dan doa.

Penulis juga menerima segala kritik dan saran dari semua pihak demi kesempurnaan penyusunan tugas akhir ini. Akhirnya penulis berharap, semoga tugas akhir ini dapat bermanfaat.

Jember, April 2019

Penulis

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR LAMPIRAN

Halaman

BAB 1. PENDAHULUAN

1.1 Latar Belakang

Semakin berkembangnya kemajuan teknologi dan komunikasi telah merubah gaya hidup manusia secara signifikan salah satunya dalam mengirimkan sebuah pesan atau informasi. Manusia dapat mengirimkan sebuah pesan ataupun informasi dengan sangat cepat dan mudah. Namun terdapat banyak kasus-kasus kejahatan pencurian data serta informasi yang bersifat rahasia. Hal ini sangat berbahaya apabila orang-orang tersebut sengaja merubah isi data ataupun informasi tersebut sehingga dapat menimbulkan suatu kesalahpahaman.

Kriptografi merupakan sebuah cabang ilmu yang bertujuan untuk menjaga kerahasiaan sebuah informasi yang terdapat dalam sebuah pesan sehingga tidak mudah untuk diketahui oleh pihak yang tidak bertanggungjawab. Kriptografi merupakan sebuah metode yang cukup kuat dimana pesan tersebut disamarkan dengan menggunakan algoritma sandi sehingga menyerupai suatu bentuk. Sehingga data tersebut akan tetap terjaga rahasianya dan hanya dapat dipahami oleh pihak yang bersangkutan (Schneier, 1996).

Playfair cipher merupakan metode penyandian dalam kriptografi klasik dimana proses enkripsinya menggunakan pemrosesan dalam bentuk blok-blok yang sangat besar. Metode *playfair cipher* merupakan salah satu diantara metode kriptografi lainnya yang mudah tertebak sehingga diperlukan teknik gabungan dengan metode lain (Setyaningsih, 2009).

Setyaningsih (2009) telah melakukan proses penyandian citra menggunakan *playfair cipher*. Dalam melakukan proses enkripsi tersebut citra yang digunakan berukuran 256 x 256 piksel dengan menggunakan kunci random matriks ukuran 256. Namun hasil yang didapat tidak terlalu baik karna *cipherimage* yang dihasilkan masih dapat dengan mudah dikenali bentuknya. Menurutnya tingkat keamanan akan lebih kuat apabila menggabungkan beberapa teknik dibandingkan menggunakan teknik cipher tunggal.

Setyaningsih dkk (2011) kemudian mengembangkan konsep super enkripsi untuk meningkatkan keamanan data citra. Setyaningsih dkk menggunakan teknik

playfair cipher dan *vigenere cipher* untuk menyandikan sebuah citra. Hasil dari penyandian yang dilakukan oleh Setyaningsih dkk terbukti memiliki tingkat keamanan yang lebih kuat dibandingkan penelitian sebelumnya.

Penggunaan *vigenere cipher* dalam gabungan metode penyandian selain karena mudah dan sederhana, *vigenere cipher* cukup berhasil dalam meningkatkan tingkat keamanan dari citra tersebut. Terdapat banyak penelitian yang menggunakan *vigenere cipher* sebagai metode gabungan seperti Amirudin (2016) menggabungkan algoritma RC4 dengan *vigenere cipher* implementasi algoritma pada citra *bitmap*. Kemudian Hardjo (2016) yang menggabungkan algoritma *Simplified-Data Encryption Standard* (S-DES) dengan *vigenere cipher* dalam penyandian citra. Kedua penelitian tersebut memiliki tingkat keamanan yang cukup kuat dalam menyandikan sebuah citra.

Shift Rows merupakan sebuah transposisi sederhana pergeseran elemen baris pada tabel ke kiri sejumlah karakter. *Shift rows* terdapat dalam beberapa algoritma kriptografi modern seperti S-DES, DES dan AES. Penggunaan *shift rows* bertujuan untuk merubah posisi baris pada tabel sehingga susunan tabel tersebut berbeda dengan tabel awal.

Berdasarkan penelitian Setyaningsih (2011) maka penulis ingin melakukan penelitian yang bertujuan untuk memperkuat tingkat keamanan pada penyandian citra digital. Penulis mengajukan algoritma *Playfair Cipher* untuk menyandikan sebuah citra dengan menggunakan kunci random matriks dan dilanjutkan dengan menambahkan proses *Shift Rows,* dan *Vigenere Cipher*. Pengamanan citra menggunakan metode ini memiliki harapan untuk memperkuat keamanan dari penelitian sebelumnya.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah tertera, maka rumusan masalah akan ditekankan pada :

a. Bagaimana proses enkripsi dan dekripsi citra secara sistematis dengan menggunakan *Playfair, Shift Rows Vigenere* dan metode gabungan *Playfair - Shift Rows, Playfair -Vigenere,* dan *Playfair-Shift Rows-Vigenere*?

b. Bagaimana perbandingan tingkat keamanan citra hasil penyandian dengan menggunakan *Playfair Cipher, Shift Rows, Vigenere Cipher* dan citra hasil penyandian dengan menggunakan metode gabungan *Playfair Cipher, Playfair Cipher-Shift Rows, Playfair Cipher-Vigenere Cipher,* dan *Playfair-Shift Rows-Vigenere Cipher*?

1.3 Tujuan Penelitian

Tujuan yang ingin didapat dari penelitian ini adalah sebagai berikut:

a. Melakukan proses enkripsi dan dekripsi citra secara sistematis menggunakan *Playfair, Shift Rows, Vigenere* dan metode gabungan *Playfair -Shift Rows, Playfair -Vigenere,* dan *Playfair-Shift Rows-Vigenere*.
b. Melakukan perbandingan tingkat keamanan citra hasil penyandian dengan menggunakan algoritma *Playfair, Shift Rows, Vigenere* dan citra hasil penyandian dengan menggunakan gabungan algoritma *Playfair, Playfair -Shift Rows, Playfair -Vigenere,* dan *Playfair-Shift Rows-Vigenere*.
c. Melakukan penambahan *Shift Rows* terhadap algoritma *Playfair* dan algoritma *Vigenere*.

1.4 Manfaat Penelitian

Manfaat yang ingin didapat dari penelitian ini adalah sebagai berikut:

a. Mengetahui proses enkripsi dan dekripsi citra secara sistematis menggunakan *Playfair Cipher, Shift Rows Vigenere* dan metode gabungan *Playfair -Shift Rows, Playfair -Vigenere,* dan *Playfair-Shift Rows-Vigenere*.
b. Mengetahui perbandingan tingkat keamanan citra hasil penyandian dengan menggunakan *Playfair, Shift Rows, Vigenere* dan citra hasil penyandian dengan menggunakan gabungan algoritma *Playfair, Playfair -Shift Rows, Playfair -Vigenere,* dan *Playfair-Shift Rows-Vigenere*.
c. Menambah pengetahuan dalam mengkaji permasalahan yang berkaitan dengan penyandian pesan berupa citra menggunakan *Playfair Cipher, Shift Rows, dan Vigenere Cipher* dengan bantuan *software* MATLAB**.**

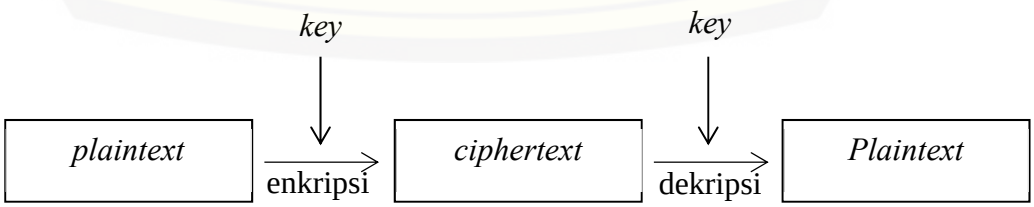
BAB 2. TINJAUAN PUSTAKA

2.1 Kriptografi

Kriptografi merupakan sebuah kata yang berasal dari Yunani yaitu *cryptós* artinya (rahasia), dan *gráphein* artinya (tulisan). Kriptografi berarti tulisan rahasia atau lebih umumnya yaitu sebuah ilmu untuk menjaga sebuah kerahasiaan suatu pesan tertentu dengan cara merubahnya kedalam bentuk yang sulit dimengerti (Munir, 2004).

Awalnya kriptografi hanya digunakan untuk menyamarkan sebuah sandi/pesan pada zaman dahulu. Namun semakin majunya teknologi seperti zaman sekarang peran kriptografi tidak hanya berfungsi untuk menyamarkan sebuah pesan tetapi juga dapat digunakan untuk mengatasi tindak kejahatan seperti penyadapan dan pembobolan data.

Dalam kriptografi terdapat dua buah metode yang sangat cukup penting dalam proses penyandian yaitu enkripsi dan dekripsi. Enkripsi adalah sebuah proses penyandian sebuah data atau informasi yang akan dikirim menjadi bentuk yang berbeda dengan data awal dengan menggunakan sebuah algoritma pada kriptografi. Sedangkan dekripsi adalah lawan dari enkripsi yaitu sebuah proses pegubahan data yang telah disamarkan menjadi bentuk semula data tersebut. Data atau informasi yang akan diubah biasa dikenal dengan *plaintext* dan hasil setelah dirubah bentuknya dikenal dengan *ciphertext.* Alur proses penyandian pada kriptografi dapat dilihat seperti Gambar 2.1.



Gambar 2.1 Proses Enkripsi dan Dekripsi

2.2 Citra

Citra merupakan sebuah media yang berperan penting sebagai pembentuk informasi visual. Citra dapat dibentuk dengan dua dan tiga dimensi untuk membentuk suatu objek.

Suatu citra didefinisikan sebagai fungsi $f(x,y)$ dimana pada Gambar 2.2 x dan y merupakan suatu koordinat dan f menyatakan intensitas atau nilai keabuan dari citra pada sebuah titik. Nilai derajat keabuan memiliki batas dari l_{min} sampai l_{max} atau bisa ditulis $l_{min} \leq f \leq l_{max}$.

Gambar 2.2 Koordinat Titik pada Suatu Citra

(Sumber: Gonzales,1977)

Suatu citra dapat diproses pada komputer jika sudah melalui proses digitalisasi yang mengubah sebuah citra menjadi nilai derajat keabuan atau yang biasa disebut dengan *pixel.* Hasil dari sebuah proses digitalisasi bisa disebut dengan citra digital.

Citra *grayscale* merupakan citra yang memiliki nilai derajat keabuan yang sama pada setiap kanalnya. Nilai derajat keabuan tersebut menggambarkan intensitas warna pada gambar. Berbeda dengan citra hitam putih, citra *grayscale* masih memiliki nilai sehingga terdapat warna abu-abu pada citra tersebut. Nilai derajat keabuan pada *grayscale* menunjukkan warna gelap apabila intensitasnya lemah dan warna terang apabila intensitasnya cukup kuat.

Citra RGB merupakan citra yang memiliki nilai *pixel* sehingga membentuk sebuah warna tertentu. Citra RGB memiliki tiga kanal yang merupakan komponen penyusun sebuah warna yaitu kanal *red, green,* dan *blue.*

2.3 *Playfair Cipher*

Playfair Cipher diciptakan oleh Sir Charles Wheatstone pada tahun 1854 yang kemudian dipopulerkan oleh Baron Lyon Playfair yang akhirnya namanya digunakan sebagai algoritma ini. Algoritma *playfair* banyak digunakan dan cukup ampuh pada saat perang terutama pada perang dunia I yang digunakan oleh pasukan tentara Inggris.

Playfair cipher merupakan algoritma yang menggunakan tabel 5x5 dalam proses penyandian. Pada awal ditemukannya *playfair* hanya dapat untuk menyandikan teks dimana 26 abjad pada alfabet kecuali huruf J dibentuk menjadi sebuah tabel ukuran 5 x 5. *Playfair cipher* merupakan algoritma klasik yang menggunakan metode substitusi dalam proses penyandiannya. *Playfair cipher* membutuhkan dua huruf yang berpasangan (bigram) untuk melakukan proses enkripsi maupun dekripsi. Tabel 2.1 merupakan tabel yang berisi tentang kunci awal dalam proses enkripsi pada playfair cipher.

Tabel 2.1 Rangkaian kunci pada *playfair cipher*

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

Beberapa aturan dalam melakukan proses penyandian *playfair cipher*, yaitu:

a. Jika dua huruf *plaintext* berada pada satu kolom yang sama maka setiap huruf diganti dengan huruf yang berada dibawahnya.
b. Jika dua huruf *plaintext* berada pada satu baris yang sama maka setiap huruf diganti dengan huruf yang berada disebelah kanannya.

c. Jika terdapat huruf yang ganda pada *plaintext* maka disisipkan huruf X dan jika *plaintext* memiliki huruf dengan jumlah ganjil maka ditambahkan huruf X pada akhir *plaintext*.

d. Jika dua huruf tidak berada pada baris dan kolom yang sama, maka huruf pertama diganti dengan huruf yang berpotongan pada baris huruf pertama dan kolom huruf kedua. Huruf kedua diganti dengan huruf pada titik sudut dari persegi yang dibentuk dari ketiga huruf tersebut.

(Nurkifli, 2014).

Contoh sederhana dari penyandian *playfair cipher* sebagai berikut:

Misal gunakan kunci dari kata ‘RUBAH’ yang akan digunakan untuk menyandikan *plaintext* ‘NAZARAMIR’. Tabel 2.2 merupakan tabel rangkaian kunci pada contoh enkripsi playfair cipher.

Tabel 2.2 Rangkaian kunci pada contoh *playfair*

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

a. Enkripsi

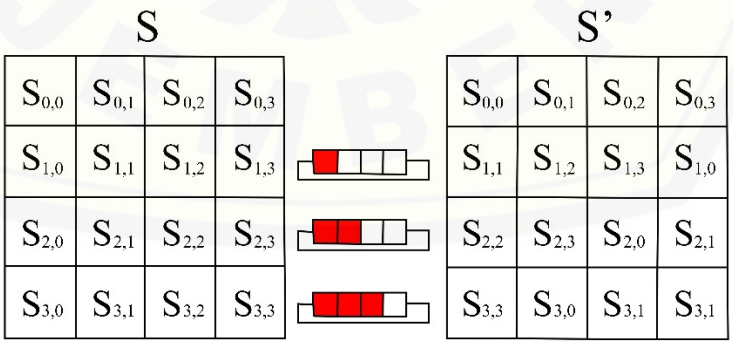
Kunci : RUBAH
Plaintext : NAZARAMIR
Digraf : {NA}, {ZA}, {RA}, {MI} dan {RX}
Enkripsi NA : MH
Enkripsi ZA : YH
Enkripsi RA : UH
Enkripsi MI : NK
Enkripsi RX : BV
Ciphertext : MHYHUHNKBV

b. Dekripsi

Kunci	: RUBAH
Ciphertext	: MHYHUHNKBV
Digraf	: {MH}, {YH}, {UH}, {NK}, dan {BV}
Enkripsi MH	: NA
Enkripsi YH	: ZA
Enkripsi UH	: RA
Enkripsi NK	: MI
Enkripsi BV	: RX
Plaintext	: NAZARAMIR

2.4 *Shift Rows*

Transformasi *shift rows* pada dasarnya merupakan proses pergeseran baris pada sebuah tabel. Arah pergeseran *shift rows* yaitu ke kiri dimana baris yang terletak dibagian paling kiri akan dipindahkan menjadi bit paling kanan. Pergeseran baris ke-*i* pada *state* ke arah kanan sejauh *i*. Proses pergeseran *shift rows* ditunjukkan dalam Gambar 2.3 dimana pada tabel S berisikan susunan asli *pixel* dan pada tabel S' menggambarkan hasil dari proses pergeseran baris. Pada kolom pertama tidak terjadi pergeseran baris tetapi pada kolom kedua terjadi pergeseran garis kekiri sebanyak 1 kali, kolom ketiga terjadi pergeseran sebanyak 2 kali dan kolom keempat terjadi pergeseran sebanyak 3 kali.



Gambar 2.3 Proses *Shift rows*

(Sibarani, 2017).

2.5 *Vigenere Cipher*

Vigenere cipher merupakan sebuah algoritma kriptografi cipher abjad-majemuk. Algoritma vigenere menggunakan tabel untuk melakukan suatu proses enkripsi. Setiap baris didalam tabel *vigenere* menandakan huruf-huruf *ciphertext*. Huruf yang sama pada *ciphertext* belum tentu berasal dari sebuah *plaintext* yang sama sehingga kenapa algoritma ini termasuk golongan cipher abjad-majemuk. Seperti algoritma lainnya, *vigenere cipher* juga memerlukan sebuah kunci (*key*) dalam proses enkripsi. Kunci pada *vigenere* akan berulang apabila kunci tersebut memiliki panjang yang lebih sedikit dibanding *plaintext*, sehingga kunci tersebut memiliki panjang yang sama dengan *plaintext*. Tabel 2.3 merupakan contoh tabel yang berisikan kunci pada proses enkripsi dengan algoritma vigenere cipher.

Tabel 2.3 Tabel *Vigenere Cipher*

	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
KUNCI	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

Algoritma *vigenere cipher* memiliki karakteristik dalam proses enkripsi dan dekripsi, yaitu:

a. Hanya mampu memuat 26 karakter huruf alfabet, sehingga tanda baca lain tidak dapat terbaca oleh *vigenere*.

b. Panjang kunci harus sama dengan panjang sebuh *plaintext*. Jika panjang kunci lebih pendek maka akan tejadi perulangan pada kunci sehingga memiliki panjang yang sama dengan *plaintext*.

2.5.1 Enkripsi *Vigenere Cipher*

Enkripsi pada *vigenere cipher* dapat dituliskan secara matematis dengan menggunakan operasi penjumlahan dan operasi *modulo*, yaitu:

$$C_i = (p_i + k_i)\ mod\ 26$$

Keterangan :

C_i = huruf ke-*i* pada *ciphertext*

p_i = huruf ke-*i* pada *plaintext*

k_i = huruf ke-*i* pada kunci

contoh enkripsi menggunakan algoritma *vigenere cipher* :

Plaintext = NAZARAMIR

Kunci = horehoreh

Ciphertext = UOQEYODMY

Vigenere cipher pada dasarnya memiliki nilai *ciphertext* dengan kunci yang berbeda-beda.

$$(N + h)\ mod\ 26 = U$$
$$(A + o)\ mod\ 26 = O$$

Proses enkripsi pada *vigenere* tidak selalu memiliki *cipherteks* yang sama walaupun huruf pada *plainteks* tersebut sama. Contoh: huruf *plainteks* A yang dienkripsi menjadi huruf A dan E sehingga setiap huruf *cipherteks* memiliki kemungkinan yang cukup banyak dari huruf *plainteks*.

2.5.2 Dekripsi *Vigenere Cipher*

Dekripsi pada *vigenere cipher* dapat dituliskan secara matematis dengan menggunakan operasi penjumlahan dan operasi *modulo*, yaitu:

$$p_i = (C_i - k_i)\ mod\ 26$$

Keterangan :

C_i = huruf ke-*i* pada *ciphertext*

p_i = huruf ke-*i* pada *plaintext*

k_i = huruf ke-*i* pada kunci

contoh dekripsi menggunakan algoritma *vigenere cipher* :

Ciphertext = UOQEYODMY

Kunci = horehoreh

Plaintext = NAZARAMIR

Vigenere cipher pada dasarnya memiliki nilai *ciphertext* dengan kunci yang berbeda-beda.

$$(U - h)\ mod\ 26 = N$$
$$(O - o)\ mod\ 26 = A$$

Pengembangan dari metode *vigenere cipher* untuk penyandian citra dilakukan dengan menggunakan *vigenere cipher* yang menggunakan nilai *modulo* 256 sesuai derajat keabuan warna pada citra (Setyaningsih. dkk., 2011).

Rumus enkripsi untuk menghitung nilai *cipherimage* tiap *pixel* adalah sebagai berikut:

$$E_{ki}(a) = (a + ki) mod\ 256$$

dimana:

a = intensitas ke- *i,j plainimage*

ki = kunci ke-*i*

sedangkan rumus untuk mendapatkan kembali *plainimage* yang berupa citra menggunakan rumus :

$$D_{ki}(a) = (a - ki)\ mod\ 256$$

dimana:

a = intensitas ke- *i,j cipherimage*

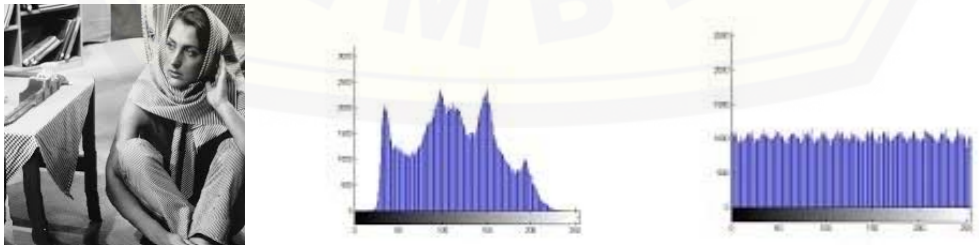
ki = kunci ke-*i*

vigenere cipher masih dapat dipecahkan dengan metode *exhaustive search* apabila panjang dari kunci diketahui sebab kunci berikutnya merupakan perulangan dari kunci sebelumnya (Setyaningsih. dkk., 2011).

2.6 Analisis Histogram

Analisis histogram adalah salah satu analisis keamanan pada pengolahan sebuah citra yang menunjukkan tampilan informasi tentang distribusi nilai pixel dalam sebuah citra. Sebuah *cipherimage* yang baik memiliki tingkat distribusi nilai *pixel* yang cukup merata pada histogramnya. *Cipherimage* yang memiliki nilai distribusi *pixel* yang tidak merata menandakan *cipherimage* tersebut tidak aman dan akan lebih mudah untuk diserang oleh *attacker*.

Histogram sering kali digunakan oleh *attacker* untuk melakukan kriptanalisis dengan membaca frekuensi kemunculan dari nilai *pixel* pada *cipherimage*. *Cipherimage* haruslah memiliki nilai histogram ynag cukup berbeda dengan *plainimage* agar tidak dapat diserang oleh *attacker* dengan cukup mudah. Suatu algoritma yang baik apabila menghasilkan nilai distribusi *pixel* yang cukup merata pada garis mendatar (absis) dan garis tegak (ordinat) seperti contoh pada gambar 2.4.



(a) Citra barbara (b) Histogram Citra Barbara (c) Histogram Hasil Enkripsi

Gambar 2.4 Analisis dengan Histogram Derajat Keabuan

(Behnia S. Dkk., 2007).

2.7 Analisis Diferensial

Analisis diferensial merupakan sebuah analisis yang berfungsi untuk mengevaluasi kekuatan suatu algoritma dalam mengenkripsi citra dari serangan diferensial. Terdapat beberapa indikator dalam analisis diferensial, namun dua indikator yang sering digunakan yaitu *Number of Pixels Change Rate (NPCR)* dan *Unifer Average Changing Intensity (UACI). UACI* bertugas untuk memfokuskan perbedaan antara dua buah gambar *cipherimage*, sementara *NPCR* berfokus pada jumlah absolut dari nilai *pixel* yang berubah akibat serangan diferensial. Perhitungan *NPCR* didefinisikan seperti persamaan (2.1).

$$\text{NPCR} = \frac{\sum_{i,j,k} D(i,j,k)}{L \times W \times H} \times 100\% \tag{2.1}$$

. Nilai $d_{i,j,k}$ dapat ditentukan sebagai berikut :

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

dimana :

D : variabel untuk menghitung banyaknya perbedaan *pixel*
i : baris citra
j : kolom citra
k : kanal citra
C_1 : *pixel plainimage*
C_2 : *pixel cipherimage*
L : panjang citra
W : lebar citra
H : tinggi citra

Perhitungan *UACI* didefinisikan seperti pada persamaan (2.2).

$$\text{UACI} = \frac{1}{L \times W \times H} \sum_{i,j,k} \left[\frac{|c_{1(i,j,k)} - c_{2(i,j,k)}|}{255} \right] \times 100\% \tag{2.2}$$

Keterangan :

L : panjang citra
W : lebar citra
H : tinggi citra

i : baris citra

j : kolom citra

k : kanal citra

C : *cipherimage*

P : *plainimage*

C_1 : *cipherimage* 1

C_2 : *cipherimage* 2

2.8 Analisis Koefisien Korelasi

Analisis koefisien korelasi merupakan salah satu faktor dari analisis statistik yang berfungsi untuk mengukur kemiripan antara *plainimage* dan *cipherimage.* Analisis ini menunjukkan tingkat keamanan dari sebuah algoritma enkripsi yang diajukan dari serangan statistik. Sehingga *cipherimage* yang dihasilkan harus lah memiliki perbedaan yang cukup signifikan dengan *plainimage.* Koefisien korelasi dapat dihitung dengan persamaan (2.3).

$$CorrCoef(x,y) = \frac{\sum_{i=1}^{n}(x_i-\mu(x))(y_i-\mu(y))}{\sigma(x)\sigma(y)} \quad (2.3)$$

dimana $\mu(x)$ dan $\mu(y)$ merupakan rata-rata dari x dan y :

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

x dan *y* adalah variabel dari *plainimage* dan *cipherimage.*

Simbol σ merupakan standar deviasi yang berfungsi untuk melihat seberapa dekat perbedaan nilai sebaran data dengan nilai rata-rata. Untuk mencari nilai standar penyimpangan pada koefisien korelasi adalah:

$$\sigma(x) = \sqrt{\sum_{i=1}^{n}(x_i-\mu(x))^2} \quad \text{dan} \quad \sigma(y) = \sqrt{\sum_{i=1}^{n}(y_i-\mu(y))^2} \quad (2.4)$$

Jika nilai koefisien korelasi sama dengan *satu*, maka *plainimage* dan *cipherimage* tidak memiliki perbedaan atau identik. Jika nilai koefisien korelasi sama dengan *nol*, maka *cipherimage* tersebut sangat berbeda dengan *plainimage*. Jika nilai koefisien korelasi sama dengan *minus satu* maka *cipherimage* tersebut merupakan negatif dari *plainimage* (Behnia S. Dkk., 2007).

BAB 3. METODE PENELITIAN

3.1 Data Penelitian

Data yang akan digunakan pada penelitian ini adalah citra *grayscale* dan citra RGB yang berfungsi sebagai *plainimage*. Data yang digunakan berjumlah 5 citra yang akan diuji pada penelitian kali ini. Berikut adalah data-data yang akan diuji saat penelitian seperti pada Gambar 3.1.

(a) Citra Monas

(b) Citra Harimau

(c) Citra Kopi

(d) Citra Ayunan

(e) Citra Mobil

(f) Citra Anak

(g) Citra Wanita

(h) Citra Sayur

(i) Citra Babon

(j) Citra Huruf

Gambar 3.1 Data Citra Penelitian

(sumber : **https://www.desktop-background.com/wallpaper**)

3.2 Langkah-langkah Penelitian

Langkah - langkah pada penelitian ini adalah sebagai berikut:

a. Studi Literatur

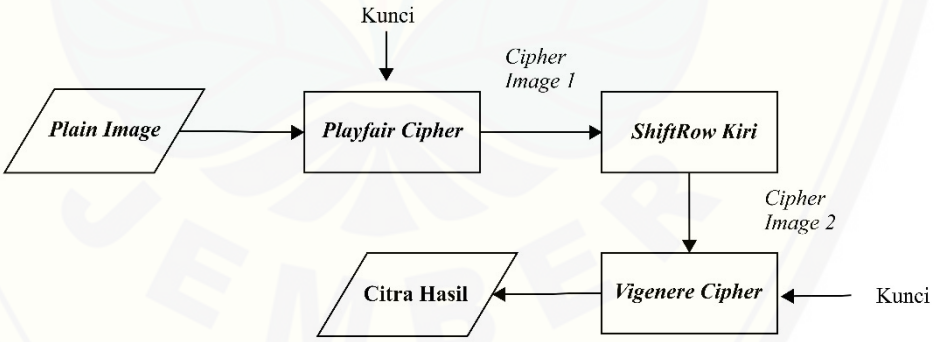
Pada tahap ini, penulis melakukan pemahaman mengenai teori-teori yang terkait pada penelitian seperti *Playfair Cipher, Shift Rows* dan *Vigenere Cipher*.

b. Percobaan Enkripsi dan Dekripsi

Percobaan dilakukan dengan menggunakan citra sebagai *plainimage* yang akan dienkripsi menggunakan kunci matriks acak sebesar 16 x 16 yang sudah dipersiapkan terlebih dahulu.

Adapun langkah-langkah enkripsi dengan metode gabungan *Playfair Cipher*, *Shift rows*, dan *Vigenere Cipher*:

1. Menyiapkan kunci random matriks ukuran 16 x 16 yang kemudian disimpan untuk proses enkripsi dan dekripsi.
2. Memasukkan *plainimage* yang akan diuji.
3. Melakukan proses *playfair cipher* dengan menggunakan *plainimage* dan kunci yang telah dibuat pada awal penelitian.
4. Hasil dari langkah ketiga kemudian akan dilakukan proses pergeseran baris (*shift rows*). Setiap *pixel* pada baris akan bergeser ke kiri sebanyak 1 kali.
5. Hasil dari langkah keempat kemudian akan dilakukan proses *vigenere cipher* dengan menggunakan kunci yang sama saat proses *playfair cipher*. Kunci pada *vigenere* akan dibuat berulang sesuai dengan jumlah *pixel* pada gambar yang akan diuji.
6. Hasil dari langkah kelima yaitu output berupa gambar yang sudah dienkripsi menggunakan metode tersebut. Gambar 3.2 menjelaskan alur proses enkripsi plainimage sehingga menghasilkan sebuah cipherimage.

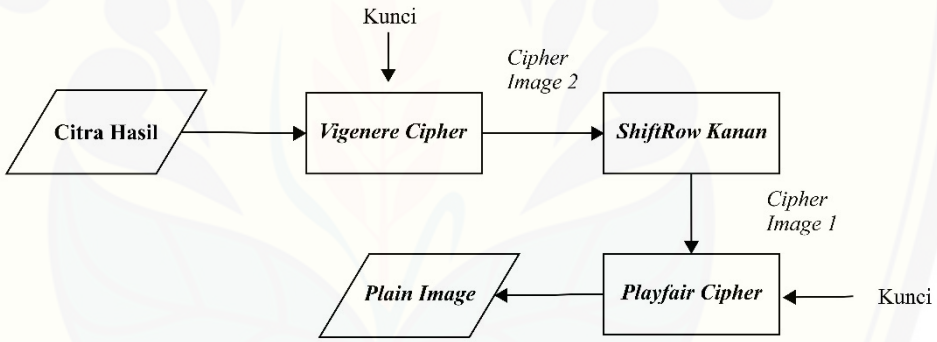


Gambar 3.2 Proses Enkripsi pada metode gabungan *Playfair Cipher*, *Shift rows*, dan *Vigenere Cipher*.

Langkah – langkah proses dekripsi pada tahap percobaan ini adalah sebagai berikut:

1. Menyiapkan *cipherimage* yang telah diciptakan pada proses enkripsi.

2. Lakukan proses *vigenere cipher* menggunakan kunci yang sama saat proses enkripsi yaitu kunci random matriks 16 x 16 yang diulang sesuai dengan jumlah *pixel* pada gambar.
3. Hasil dari langkah kedua kemudian akan dilakukan proses pergeseran baris (*shift rows*). Sama seperti saat proses enkripsi, tetapi arah pergeseran *pixel* pada baris sebanyak 1 kali ke kanan.
4. Hasil dari langkah ketiga kemudian akan dilakukan proses *playfair cipher* dengan menggunakan kunci *random* matriks 16 x 16 yang sudah ditetapkan sejak awal.
5. Hasil dari langkah kelima merupakan sebuah gambar yang menjadi *plainimage* pada penelitian ini. Gambar 3.3 menjelaskan alur proses dekripsi cipherimage sampai kembali menjadi sebuah plainimage.



Gambar 3.3 Proses Dekripsi pada metode gabungan *Playfair Cipher*, *Shift rows*, dan *Vigenere Cipher*.

c. Pembuatan Program Aplikasi Enkripsi dan Dekripsi.

   Tahap ini dilakukan pembuatan program enkripsi dan dekripsi citra dengan menggunakan program MATLAB R2015b.

d. Simulasi Program Aplikasi Enkripsi dan Dekripsi.

   Proses simulasi program aplikasi enkripsi dan dekripsi dengan cara menguji program tersebut untuk melakukan penyandian pada data gambar yang akan diteliti sehingga didapatkan analisis hasil enkripsi dan dekripsi.

e. Analisis Citra Hasil Enkripsi dan Dekripsi.

Analisis hasil dilakukan setelah mendapat hasil akhir yang disimulasi menggunakan program MATLAB R2015b untuk menganalisis histogram dan menganalisis koefisien korelasi.

f. Kesimpulan

Membuat kesimpulan dari penelitian yang telah dilakukan, yaitu dengan menganalisis proses enkripsi *plainimage* menjadi *cipherimage* maupun proses dekripsi, serta menganalisis tingkat keamanan dari metode yang digunakan.

Langkah-langkah penelitian dengan *flowchart* seperti pada Gambar 3.4

Gambar 3.4 Skema langkah-langkah penelitian

BAB 5 KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian, didapatkan beberapa kesimpulan sebagai berikut:

a. Seluruh *plainimage* berhasil dienkripsi dan c*ipherimage* yang dihasilkan pada penelitian ini berhasil pula untuk didekripsikan. Hasil dekripsi tersebut memiliki nilai uji korelasi sebesar 1 serta nilai *UACI* dan *NPCR* sebesar 0. Hal ini berarti bahwa *cipherimage* tersebut identik dengan *plainimage*.
b. Berdasarkan data yang diperoleh dalam perhitungan nilai *UACI*, *NPCR*, dan uji korelasi. Cipherimage yang diajukan peneliti memiliki nilai yang lebih baik. Sehingga metode ini cukup kuat dalam mengamankan sebuah citra.
c. Penambahan metode *Shift rows* sebanyak 1 *pixel* tidak memiliki pengaruh yang cukup signifikan pada hasil enkripsi.

5.2 Saran

Saran yang perlu diperhatikan untuk penelitian selanjutnya adalah:

a. Menerapkan algoritma *Playfair Cipher-Shift Rows-Vigenere Cipher* untuk melakukan proses penyandian sebuah audio ataupun video.
b. Menggabungkan metode ini dengan algoritma kriptografi modern yang lain
c. Melakukan pergeseran baris yang lebih berpola dan variatif sehingga *cipherimage* yang dihasilkan memiliki keamanan yang lebih kuat.
d. Dalam menyimpan *cipherimage* hasil enkripsi atau dekripsi lebih baik menggunakan format *bmp agar citra tersebut tidak mengalami perubahan nilai *pixel*.

DAFTAR PUSTAKA

Amirudin, R. 2016. *Implementasi Algoritma Kriptografi RC4 dan Vigenere Cipher pada Citra Bitmap*. Semarang: Program Studi Teknik Informatika, Universitas Dian Nuswantoro.

Behnia, S., A. Akhsani, S.Abadpour, H. Mahmoudi, dan A. Akhavan. 2007. *A fast chaotic Encryption Scheme Based on Piecewise Nonlinear Chaotic Maps*. Physics Letters A 366: 391-396.

Gonzales, R.C. 1997. *Digital Image Processing*. USA : Addison-Wesley Publishing.

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.

Nurkifli, E. H. 2014. *Modifikasi Algoritma Playfair dan Menggabungkan dengan Linear Feedback Shift Register (LFSR). Sentika*. Yogyakarta: Seminar Nasional Teknologi Informasi dan Komunikasi 2014 (sentika 2014) ISSN: 2089-9813.

Munir, R. 2004. *Steganografi dan Watermarking*. *Bahan Kuliah ke-7* IF5054 Kriptografi. Departemen Teknik Informatika Institut Teknologi Bandung 2004.

Schneier, B. 1996. *Applied Cryptography 2nd.* John Wiley & Sons. New York.

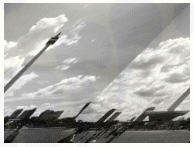
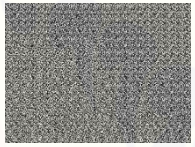
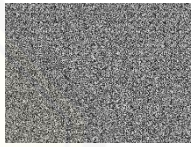
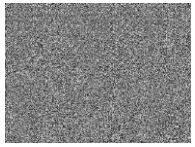
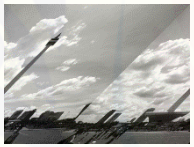
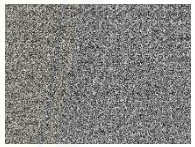
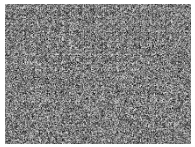
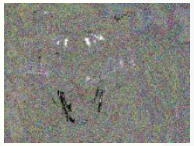
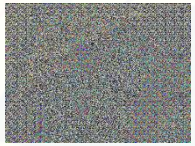
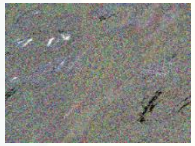
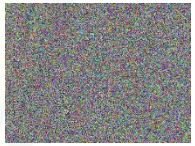
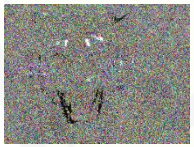
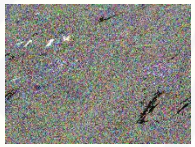
Setyaningsih, E. 2009. *Penyandian Citra Menggunakan Metode Playfair Cipher*. Yogyakarta : Institut Sains & Teknologi AKPRIND.

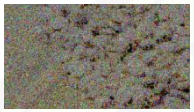
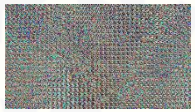
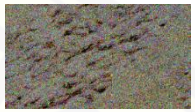
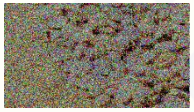
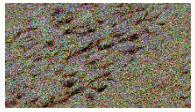
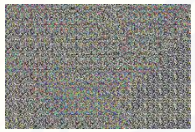
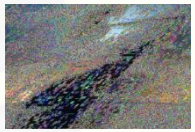
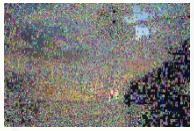
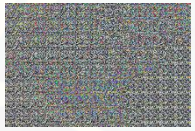
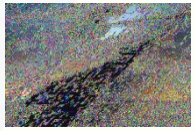
Setyaningsih, E., Iswahyudi, C., Widyastuti, N. 2011. *Konsep Super Enkripsi untuk Meningkatkan Keamanan Data Citra*. Jurnal *TICOM*, 4(3):1-9.

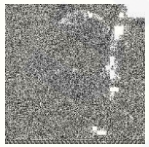
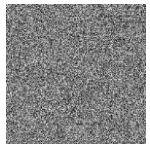
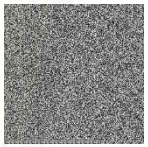
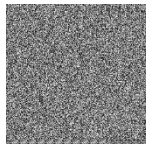
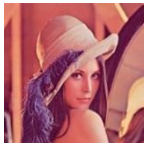
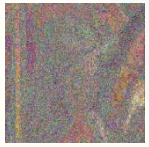
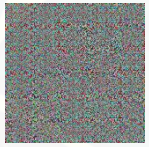
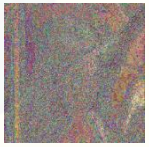
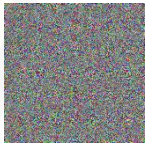
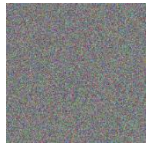
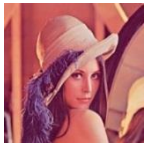
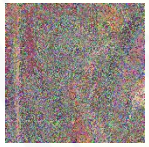
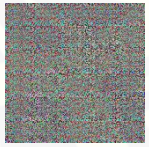
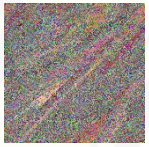
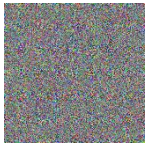
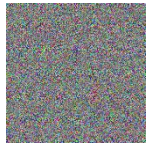
Sibarani, E.B.H. 2017. Zarlis, M. Sembiring, R.W., *Analisis Kripto Sistem Algoritma AES dan Elliptic Curve Crypthography (ECC) untuk Keamanan Data*. ISSN: 2540-7600

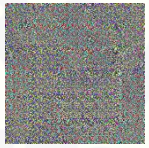
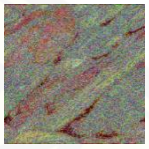
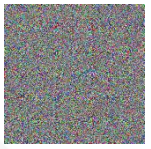
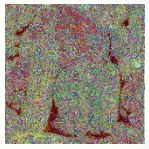
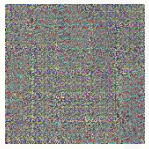
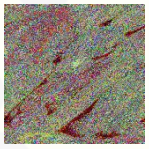
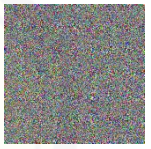
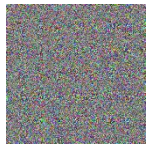
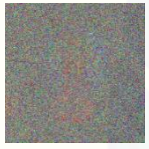
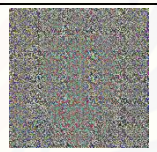
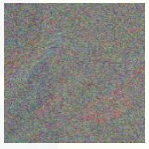
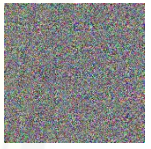
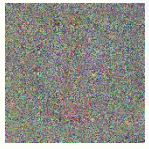
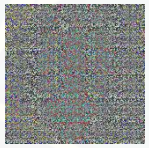
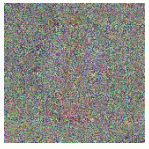
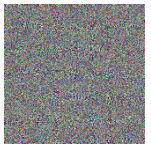
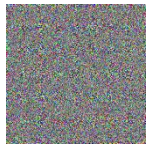
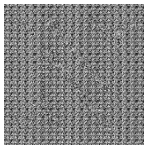
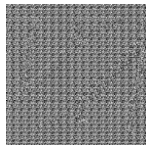
LAMPIRAN

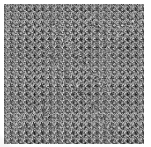
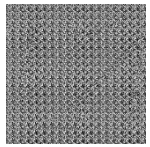
Lampiran A. Hasil Proses Enkripsi

No	*Plainimage*	Kunci	*Playfair*	*Shift Rows*	*Vigenere*	*Playfair - Shift Rows*	*Playfair - Vigenere*	*Playfair – Shift Rows- Vigenere*
1		Kunci 1						
2		Kunci 2						
3		Kunci 1						
4		Kunci 2						

No	*Plainimage*	Kunci	*Playfair*	*Shift Rows*	*Vigenere*	*Playfair - Shift Rows*	*Playfair - Vigenere*	*Playfair – Shift Rows- Vigenere*
5		Kunci 1						
6		Kunci 2						
7		Kunci 1						
8		Kunci 2						
9		Kunci 1						

No	*Plainimage*	Kunci	*Playfair*	*Shift Rows*	*Vigenere*	*Playfair - Shift Rows*	*Playfair - Vigenere*	*Playfair – Shift Rows- Vigenere*
10		Kunci 2						
11		Kunci 1						
12		Kunci 2						
13		Kunci 1						
14		Kunci 2						

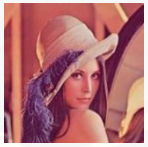
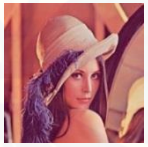
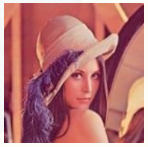
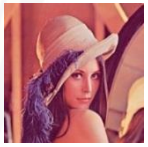
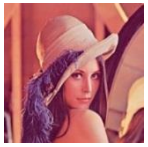
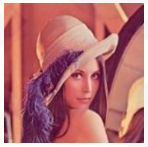
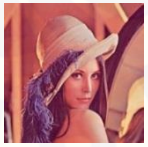
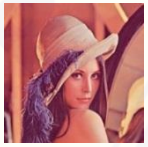
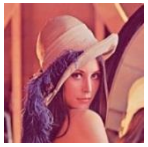
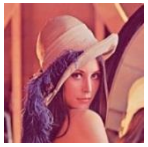
No	*Plainimage*	Kunci	*Playfair*	*Shift Rows*	*Vigenere*	*Playfair - Shift Rows*	*Playfair - Vigenere*	*Playfair – Shift Rows- Vigenere*
15		Kunci 1						
16		Kunci 2						
17		Kunci 1						
18		Kunci 2						
19		Kunci 1						

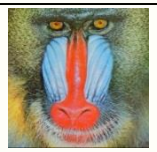
No	*Plainimage*	Kunci	*Playfair*	*Shift Rows*	*Vigenere*	*Playfair - Shift Rows*	*Playfair - Vigenere*	*Playfair – Shift Rows- Vigenere*
20		Kunci 2						

Lampiran B. Hasil Proses Dekripsi

No	*Plainimage*	Kunci	*Playfair*	*Shift Rows*	*Vigenere*	*Playfair - Shift Rows*	*Playfair - Vigenere*	*Playfair – Shift Rows- Vigenere*
1	Citra Monas	Kunci 1						
2	Citra Monas	Kunci 2						
3	Citra Harimau	Kunci 1						
4	Citra Harimau	Kunci 2						

No	*Plainimage*	Kunci	*Playfair*	*Shift Rows*	*Vigenere*	*Playfair - Shift Rows*	*Playfair - Vigenere*	*Playfair – Shift Rows- Vigenere*
5	Citra Kopi	Kunci 1						
6	Citra Kopi	Kunci 2						
7	Citra Ayunan	Kunci 1						
8	Citra ayunan	Kunci 2						
9	Citra Mobil	Kunci 1						

No	*Plainimage*	Kunci	*Playfair*	*Shift Rows*	*Vigenere*	*Playfair - Shift Rows*	*Playfair - Vigenere*	*Playfair – Shift Rows- Vigenere*
10	Citra Mobil	Kunci 2						
11	Citra Anak	Kunci 1						
12	Citra Anak	Kunci 2						
13	Citra Wanita	Kunci 1						
14	Citra Wanita	Kunci 2						

No	*Plainimage*	Kunci	*Playfair*	*Shift Rows*	*Vigenere*	*Playfair - Shift Rows*	*Playfair - Vigenere*	*Playfair – Shift Rows- Vigenere*
15	Citra Sayur	Kunci 1						
16	Citra Sayur	Kunci 2						
17	Citra Babon	Kunci 1						
18	Citra Babon	Kunci 2						
19	Citra Huruf	Kunci 1	N	N	N	N	N	N

No	*Plainimage*	Kunci	*Playfair*	*Shift Rows*	*Vigenere*	*Playfair - Shift Rows*	*Playfair - Vigenere*	*Playfair – Shift Rows- Vigenere*
20	Citra Huruf	Kunci 2						

Lampiran C. Hasil Nilai *NPCR* Setelah Dienkripsi

No	*Plainimage*	Kunci	*NPCR*					
			Playfair	*Shift Rows*	*Vigenere*	*Playfair - Shift Rows*	*Playfair - Vigenere*	*Playfair – Shift Rows - Vigenere*
1	Citra Monas	Kunci 1	72,8888%	98,0309%	99,6094%	98,8188%	99,6014%	99,6067%
2	Citra Monas	Kunci 2	72,8888%	98,0309%	99,6094%	98,8208%	99,5875%	99,6247%
3	Citra Harimau	Kunci 1	92,203%	99,0253%	99,6094%	99,514%	99,6024%	99,6056%
4	Citra Harimau	Kunci 2	92,203%	99,0253%	99,6094%	99,5174%	99,604%	99,61%
5	Citra Kopi	Kunci 1	86,7069%	97,2426%	99,6054%	98,5406%	99,6081%	99,6118%
6	Citra Kopi	Kunci 2	86.7069%	97,2426%	99,6054%	98,4924%	99,6007%	99,6033%
7	Citra Ayunan	Kunci 1	67,9429%	99,1388%	99,6155%	99,4106%	99,6099%	99,618%
8	Citra Ayunan	Kunci 2	67,9429%	99,1388%	99,6155%	99,4224%	99,6309%	99,6082%
9	Citra Mobil	Kunci 1	63,7816%	98,8243%	99,6108%	99,155%	99,6142%	99,6132%
10	Citra Mobil	Kunci 2	63,7816%	98,8243%	99,6108%	99,1543%	99,6095%	99,6281%

No	*Plainimage*	Kunci	*NPCR*					
			Playfair	*Shift Rows*	*Vigenere*	*Playfair - Shift Rows*	*Playfair - Vigenere*	*Playfair – Shift Rows - Vigenere*
11	Citra Anak	Kunci 1	91,861%	96,6705%	99,6094%	98,2315%	99,6124%	99,614%
12	Citra Anak	Kunci 2	91,861%	96,6705%	99,6094%	98,1216%	99,6063%	99,6277%
13	Citra Wanita	Kunci 1	85,8343%	98,566%	99,6087%	99,4173%	99,5986%	99,6202%
14	Citra Wanita	Kunci 2	85,8343%	98,566%	99,6217%	99,3908%	99,6064%	99,6103%
15	Citra Sayur	Kunci 1	82,7594%	98,2577%	99,6087%	98,9582%	99,5961%	99,6045%
16	Citra Sayur	Kunci 2	82,7594%	98,2577%	99,6217%	98,9494%	99,6037%	99,6196%
17	Citra Babon	Kunci 1	96,068%	99,0542%	99,6087%	99,5844%	99,5895%	99,612%
18	Citra Babon	Kunci 2	96,068%	46,781%	99,6217%	96,068%	99,612%	99,6105%
19	Citra Huruf	Kunci 1	8,5383%	46,781%	99,6094%	48,499%	99,6106%	99,5611%
20	Citra Huruf	Kunci 2	8,5383%	46,781%	99,6094%	48,4013	99,6009%	99,5877%

Lampiran D. Hasil Nilai *UACI* Setelah Dienkripsi

No	*Plainimage*	Kunci	*UACI*					
			Playfair	*Shift Rows*	*Vigenere*	*Playfair - Shift Rows*	*Playfair - Vigenere*	*Playfair – Shift Rows - Vigenere*
1	Citra Monas	Kunci 1	24,0638%	13,8218%	32,4462%	26,2989%	32,3738%	32,4538%
2	Citra Monas	Kunci 2	24,1132%	13,8218%	32,4685%	26,5%	32,5215%	32,421%
3	Citra Harimau	Kunci 1	27,7836%	24,5892%	30,3795%	29,963%	30,3636%	30,3841%
4	Citra Harimau	Kunci 2	27,1642%	24,5892%	30,3865%	29,9953%	30,3859%	30,3912%
5	Citra Kopi	Kunci 1	32,6372%	18,7108%	38,7193%	35,1699%	38,7157%	38,8699%
6	Citra Kopi	Kunci 2	30,9523%	18,7108%	38,7532%	34,2088%	38,697%	38,7870%
7	Citra Ayunan	Kunci 1	21,7438%	29,2342%	32,9738%	32,173%	32,9074%	32,9156%
8	Citra Ayunan	Kunci 2	21,5569%	29,2342%	32,9169%	32,0913%	32,8883%	32,9689%
9	Citra Mobil	Kunci 1	19,3109%	21,8696%	30,766%	27,7079%	30,7535%	30,7676%
10	Citra Mobil	Kunci 2	19,23%	21,8696%	30,7704%	27,8344%	30,7489%	30,7873%

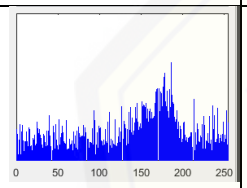
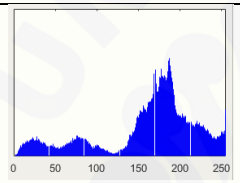
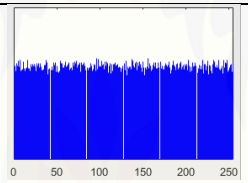
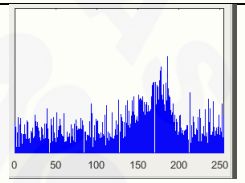
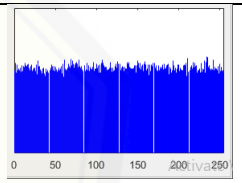
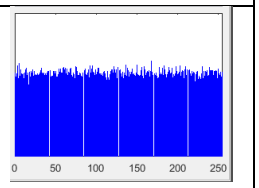
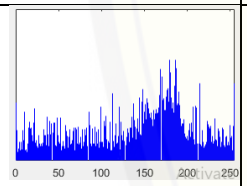
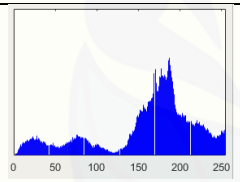
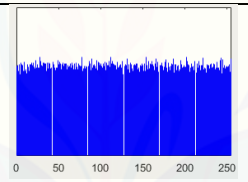
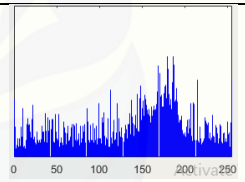
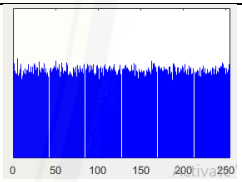
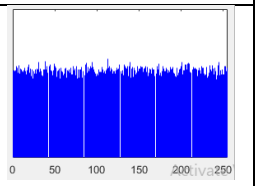
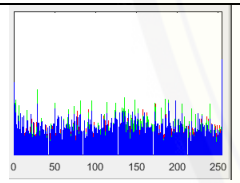
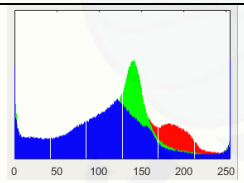
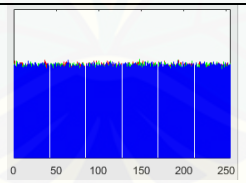
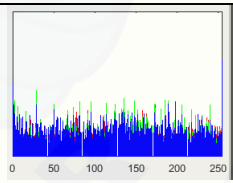
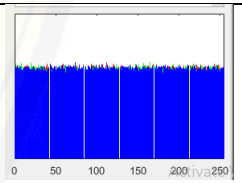
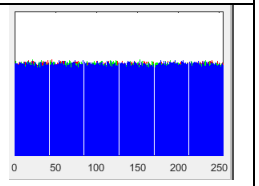
No	*Plainimage*	Kunci	*UACI*					
			Playfair	*Shift Rows*	*Vigenere*	*Playfair - Shift Rows*	*Playfair - Vigenere*	*Playfair – Shift Rows - Vigenere*
11	Citra Anak	Kunci 1	27,8115%	18,5962%	30,9913%	30,155%	30,9186%	30,9985%
12	Citra Anak	Kunci 2	27,4824%	18,5962%	30,978%	30,1326%	30,80%	30,8257%
13	Citra Wanita	Kunci 1	26,3659%	18,9441%	30,4415%	28,8%	30,4447%	30,4786%
14	Citra Wanita	Kunci 2	25,8384%	18,9441%	30,4785%	28,7763%	30,4515%	30,4609%
15	Citra Sayur	Kunci 1	26,623%	21,831%	32,2216%	30,3334%	32,1763%	32,23%
16	Citra Sayur	Kunci 2	25,7402%	21,831%	32,2671%	29,9487%	32,2117%	32,2358%
17	Citra Babon	Kunci 1	28,9459%	22,0464%	29,5468%	29,5415%	29,5318%	29,549%
18	Citra Babon	Kunci 2	27,8363%	22,0464%	29,6269%	28,8376%	29,578%	29,6117%
19	Citra Huruf	Kunci 1	4,0624%	41,541%	49,6954%	41,2016%	49,6721%	49,6577%
20	Citra Huruf	Kunci 2	2,8907%	41,541%	49,5179%	41,6728%	49,5589%	49,4829%

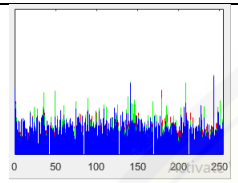
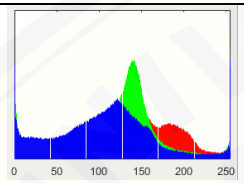
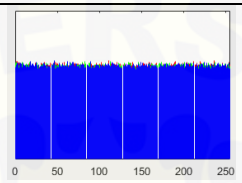
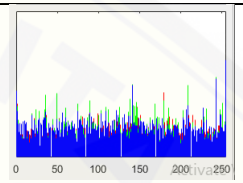
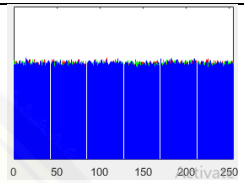
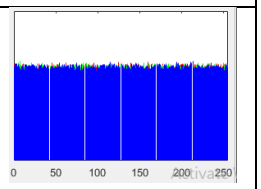
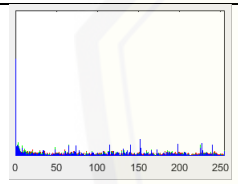
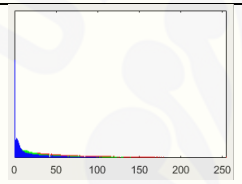
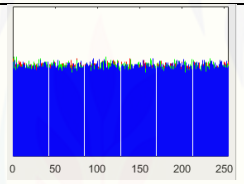
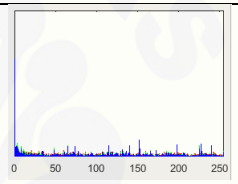
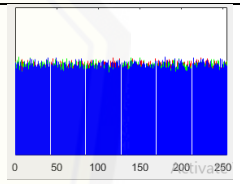
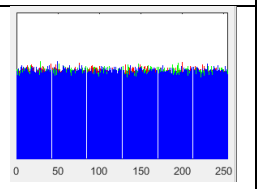
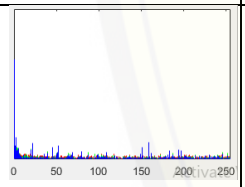
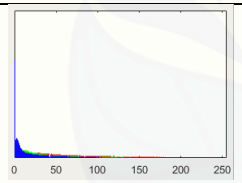
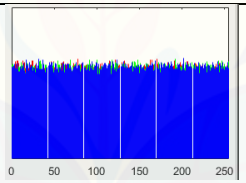
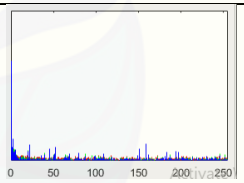
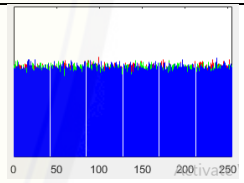
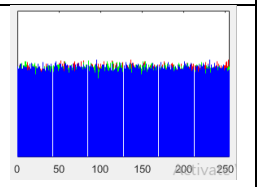
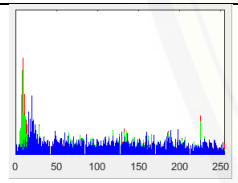
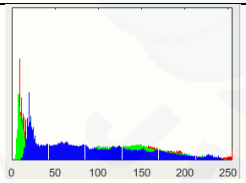
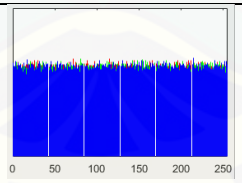
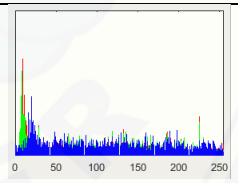
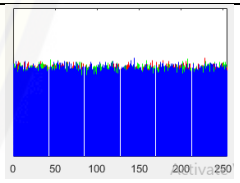
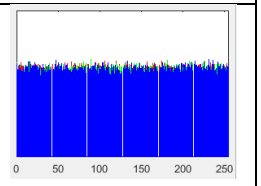
Lampiran E. Hasil Nilai Koefisien Korelasi Setelah Dienkripsi

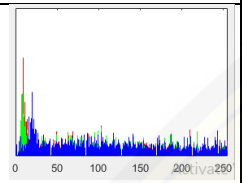
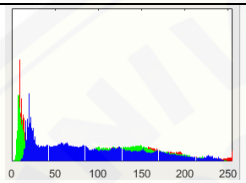
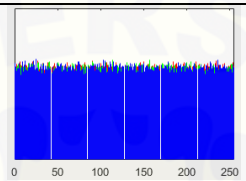
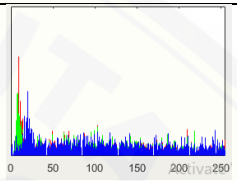
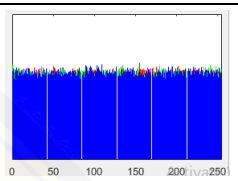
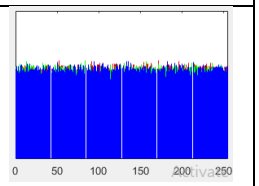
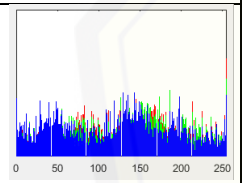
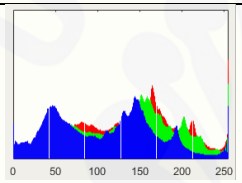
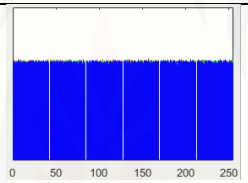
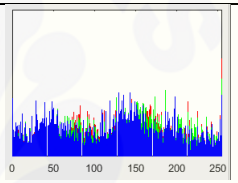
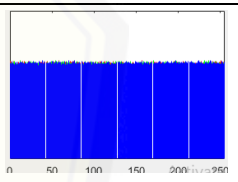
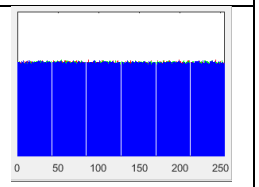
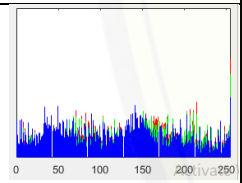
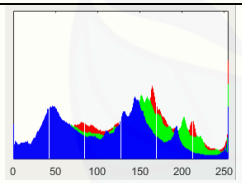
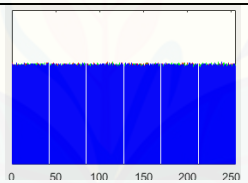
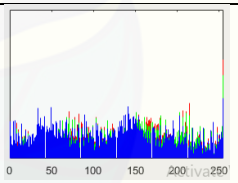
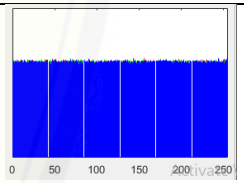
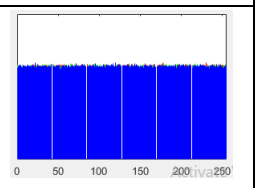
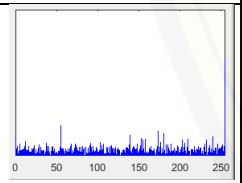
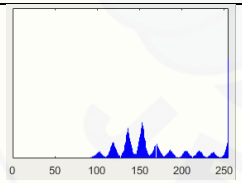
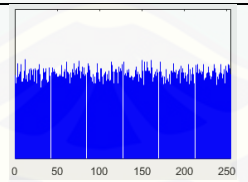
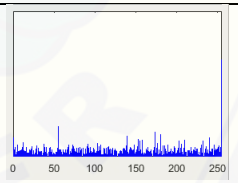
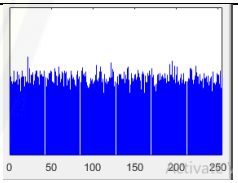
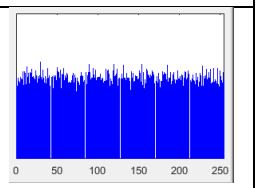
No	*Plainimage*	Kunci	Koefisien Korelasi					
			Playfair	*Shift Rows*	*Vigenere*	*Playfair - Shift Rows*	*Playfair - Vigenere*	*Playfair – Shift Rows - Vigenere*
1	Citra Monas	Kunci 1	0,13264	0,66075	0,0013863	0,10721	0,0023272	-0,00026419
2	Citra Monas	Kunci 2	0,11817	0,66075	-0,0003357	-0,002879	0,10032	0,001346
3	Citra Harimau	Kunci 1	0,10509	0,030198	0,0003450	0,00079681	0,001056	-0,00027484
4	Citra Harimau	Kunci 2	0,1257	0,030198	0,0003543	0,0025617	-0,00028733	-2,6246e-05
5	Citra Kopi	Kunci 1	0,15893	0,1688	-0,0006149	0,03784	-0,00076233	-0,0014973
6	Citra Kopi	Kunci 2	0,20135	0,1688	-0,0012514	0,049745	0,00075071	-0,00082878
7	Citra Ayunan	Kunci 1	0,33701	-0,083451	-0,0017433	-0,045327	-0,0022902	0,00095339
8	Citra Ayunan	Kunci 2	0,34439	-0,083451	0,0004894	-0,03958	9,9969e-05	0,0023293
9	Citra Mobil	Kunci 1	0,33859	0,23527	0,0004415	0,054817	0,00051886	0,000056001
10	Citra Mobil	Kunci 2	0,34444	0,23527	5,1192e-05	0,05603	-0,00066582	0,00055935

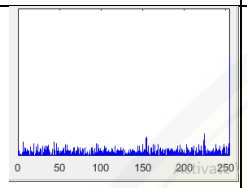
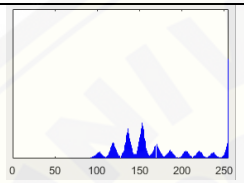
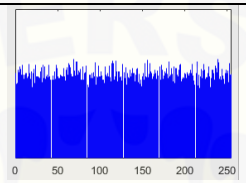
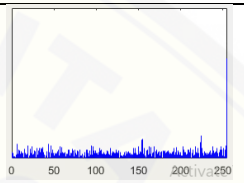
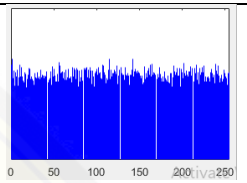
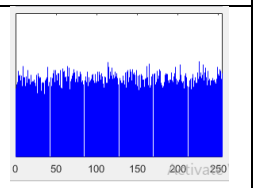
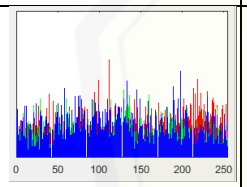
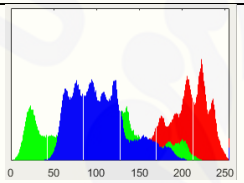
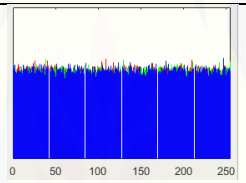
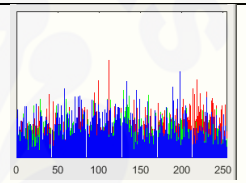
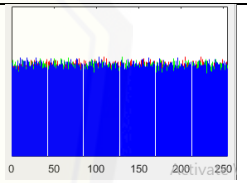
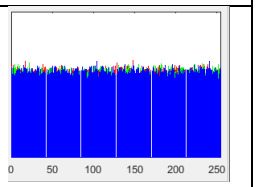
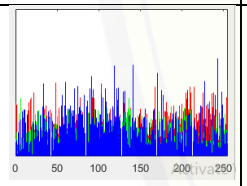
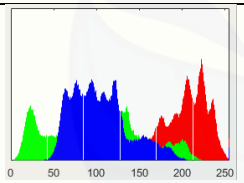
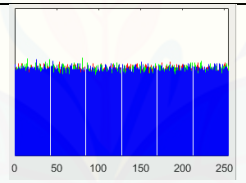
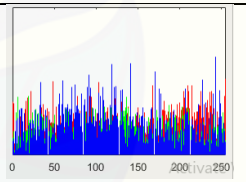
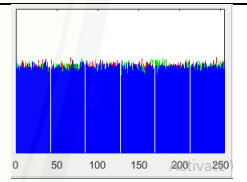
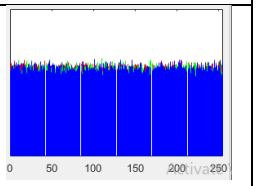
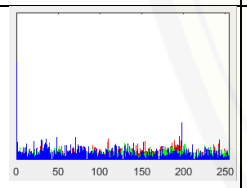
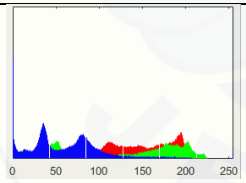
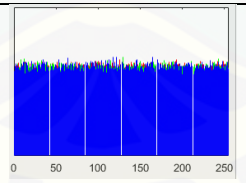
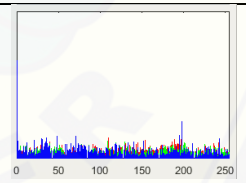
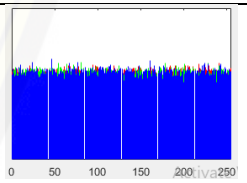
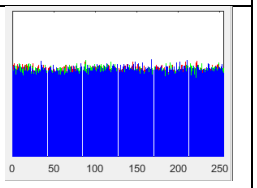
No	*Plainimage*	Kunci	Koefisien Korelasi					
			Playfair	*Shift Rows*	*Vigenere*	*Playfair - Shift Rows*	*Playfair - Vigenere*	*Playfair – Shift Rows - Vigenere*
11	Citra Anak	Kunci 1	0,1774	0,084453	-0,0064226	0,043733	0,00039322	-0,0058506
12	Citra Anak	Kunci 2	0,18555	0,084453	-0,0035042	0,040158	-0,0043763	0,0047655
13	Citra Wanita	Kunci 1	0,12282	0,42689	-0,0004098	0,05323	-0,0008246	-0,0021773
14	Citra Wanita	Kunci 2	0,13115	0,42689	-0,0015158	0,047932	0,0012143	-0,0018269
15	Citra Sayur	Kunci 1	0,19958	0,33488	-0,0001151	0,072415	0,00119995	-0,00062964
16	Citra Sayur	Kunci 2	0,22149	0,33488	-0,0026342	0,081436	0,0070634	-0,00081556
17	Citra Babon	Kunci 1	0,037862	0,10733	0,0030481	0,0046556	0,0015587	-0,00038419
18	Citra Babon	Kunci 2	0,058768	0,10733	-0,0006588	0,058766	-0,00035654	-0,00086581
19	Citra Huruf	Kunci 1	0,92827	-0,084451	-0,0025166	-0,085152	-0,0017001	-0,00074165
20	Citra Huruf	Kunci 2	0,95511	-0,084451	0,0037968	-0,090879	0,0013985	0,0041551

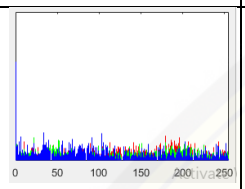
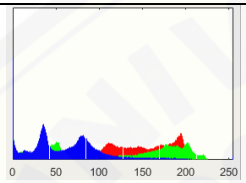
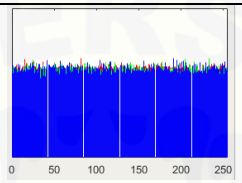
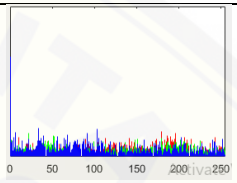
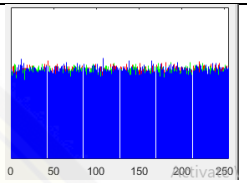
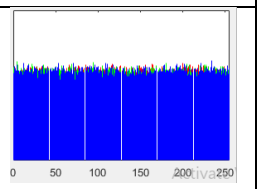
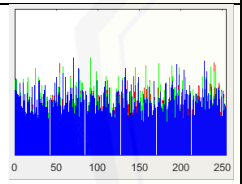
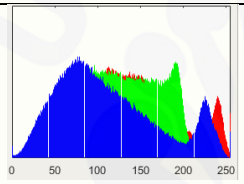
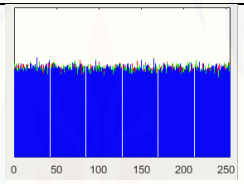
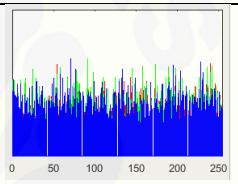
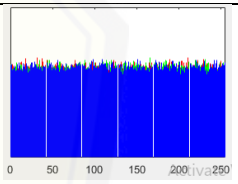
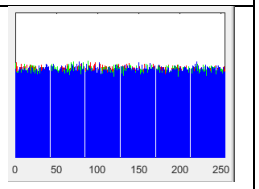
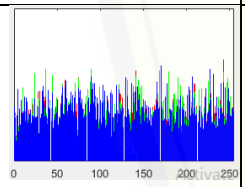
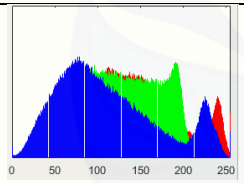
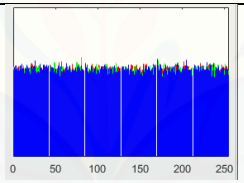
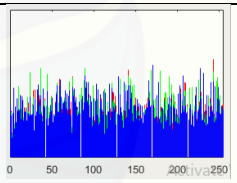
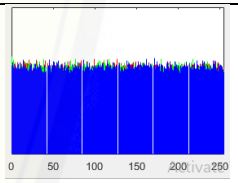
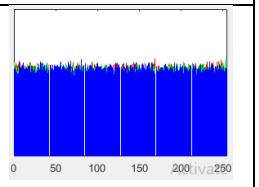
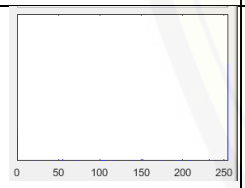
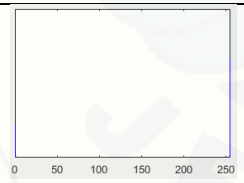
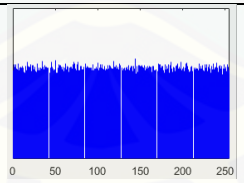
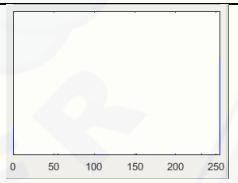
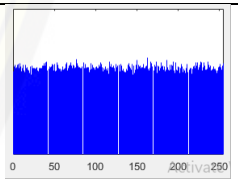
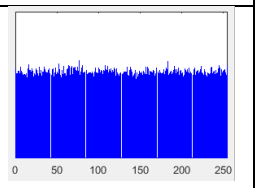
Lampiran F. Hasil Histogram Setelah Dienkripsi

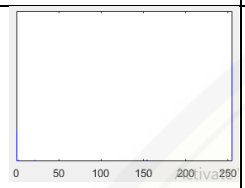
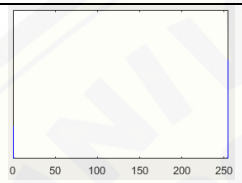
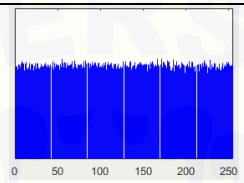
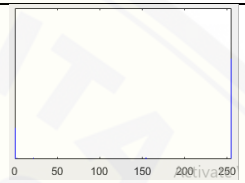
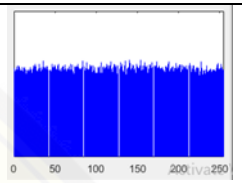
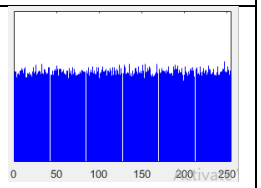
No	*Plainimage*	Kunci	*Playfair*	*Shift Rows*	*Vigenere*	*Playfair - Shift Rows*	*Playfair - Vigenere*	*Playfair – Shift Rows- Vigenere*
1	Citra Monas	Kunci 1						
2	Citra Monas	Kunci 2						
3	Citra Harimau	Kunci 1						

No	*Plainimage*	Kunci	*Playfair*	*Shift Rows*	*Vigenere*	*Playfair - Shift Rows*	*Playfair - Vigenere*	*Playfair – Shift Rows- Vigenere*
4	Citra Harimau	Kunci 2						
5	Citra Kopi	Kunci 1						
6	Citra Kopi	Kunci 2						
7	Citra Ayunan	Kunci 1						

No	*Plainimage*	Kunci	*Playfair*	*Shift Rows*	*Vigenere*	*Playfair - Shift Rows*	*Playfair - Vigenere*	*Playfair – Shift Rows- Vigenere*
8	Citra Ayunan	Kunci 2						
9	Citra Mobil	Kunci 1						
10	Citra Mobil	Kunci 2						
11	Citra Anak	Kunci 1						

No	*Plainimage*	Kunci	*Playfair*	*Shift Rows*	*Vigenere*	*Playfair - Shift Rows*	*Playfair - Vigenere*	*Playfair – Shift Rows- Vigenere*
12	Citra Anak	Kunci 2						
13	Citra Wanita	Kunci 1						
14	Citra Wanita	Kunci 2						
15	Citra Sayur	Kunci 1						

No	*Plainimage*	Kunci	*Playfair*	*Shift Rows*	*Vigenere*	*Playfair - Shift Rows*	*Playfair - Vigenere*	*Playfair – Shift Rows- Vigenere*
16	Citra Sayur	Kunci 2						
17	Citra Babon	Kunci 1						
18	Citra Babon	Kunci 2						
19	Citra Huruf	Kunci 1						

No	*Plainimage*	Kunci	*Playfair*	*Shift Rows*	*Vigenere*	*Playfair - Shift Rows*	*Playfair - Vigenere*	*Playfair – Shift Rows- Vigenere*
20	Citra Huruf	Kunci 2						

Lampiran G. Skrip Program Enkripsi dan Dekripsi pada MATLAB R2015b

```
%ENKRIPSI PLAYFAIR CIPHER - SHIFT ROWS - VIGENERE CIPHER
function Cipherimage=PlayfairCipherEn(Plainimage,Key)
[m2,n2,o1]=size(Plainimage);
Cipherimage=Plainimage;
for k=1:o1
    for i=1:m2
        for j=1:2:n2
            NK1=Cipherimage(i,j,k);
            NK2=Cipherimage(i,j+1,k);
            [a1,b1]=find(Key==NK1);
            [a2,b2]=find(Key==NK2);
            if NK1~=NK2
                if a1==a2 %jika sebaris
                    Cipherimage(i,j,k)=Key(a1,mod(b1,16)+1);
                    Cipherimage(i,j+1,k)=Key(a2,mod(b2,16)+1);
                elseif b1==b2 %jika sekolom
                    Cipherimage(i,j,k)=Key(mod(a1,16)+1,b1);
                    Cipherimage(i,j+1,k)=Key(mod(a2,16)+1,b2);
                else
                    Cipherimage(i,j,k)=Key(a1,b2);
                    Cipherimage(i,j+1,k)=Key(a2,b1);
                end
            end
        end
    end
end
% Shift Rows
function output=ShiftRowEn(input)
[m,n]=size(input);
output=input;
for i=1:m
    output(i,:)=input(i,mod((1:n)-2+i,n)+1);
end
%UJI ANALISIS
% Analisis Koefisien Korelasi
function corr=CoefCorr(plainimage,cipherimage)
[m,n,o]=size(plainimage);
mup=sum(sum(sum(plainimage)))/(m*n*o);
muc=sum(sum(sum(cipherimage)))/(m*n*o);
sigp=sqrt(sum(sum(sum((plainimage-mup).^2))));
sigc=sqrt(sum(sum(sum((cipherimage-muc).^2))));
corr=sum(sum(sum((plainimage-mup).*(cipherimage-
muc))))/(sigp*sigc);
% Analisis NPCR
function npcr=NPCRcal(plainimage,cipherimage)
[m,n,o]=size(plainimage);
dij=plainimage-cipherimage;
dij(dij~=0)=1;
npcr=sum(sum(sum(dij)))/(m*n*o)*100;
% Analisis UACI

function uaci=UACIcal(plainimage,cipherimage)
[m,n,o]=size(plainimage);
uaci=sum(sum(sum((abs(plainimage-cipherimage))/255)))/(m*n*o)*100;
```

```
% Analisis Histogram

function Histogram(cipherimage,vpop)
o=size(cipherimage,3);
color='rgb';
if vpop==1
    for i=1:o
        h=imhist(uint8(cipherimage(:,:,i)));
        if o==3
            bar(0:255,h,0,color(i),'EdgeColor',color(i));
        else
            bar(0:255,h,0,'k','EdgeColor','k');
            bar(h,'k','EdgeColor','k');
        end
        hold on
        maxv(i)=max(h);
    end
    hold off
    xlim([0 255]); ylim([0 1.5*max(maxv)]);
elseif vpop==2
    h=imhist(uint8(cipherimage(:,:,vpop-1)));
    bar(0:255,h,0,color(vpop-1),'EdgeColor',color(vpop-1));
    xlim([0 255]); ylim([0 1.5*max(h)]);
elseif vpop==3
    h=imhist(uint8(cipherimage(:,:,vpop-1)));
    bar(0:255,h,0,color(vpop-1),'EdgeColor',color(vpop-1));
    xlim([0 255]); ylim([0 1.5*max(h)]);
elseif vpop==4
    h=imhist(uint8(cipherimage(:,:,vpop-1)));
    bar(0:255,h,0,color(vpop-1),'EdgeColor',color(vpop-1));
    xlim([0 255]); ylim([0 1.5*max(h)]);
end
set(gca,'YTick',[]);


%DEKRIPSI PLAYFAIR CIPHER - SHIFT ROWS - VIGENERE CIPHER

function Plainimage=PlayfairCipherDe(Cipherimage,Key)
[m2,n2,o1]=size(Cipherimage);
Plainimage=Cipherimage;
for k=1:o1
    for i=1:m2
        for j=1:2:n2
            NK1=Plainimage(i,j,k);
            NK2=Plainimage(i,j+1,k);
            [a1,b1]=find(Key==NK1);
            [a2,b2]=find(Key==NK2);
            if NK1~=NK2
                if a1==a2 %jika sebaris
                    Plainimage(i,j,k)=Key(a1,mod(b1-2,16)+1);
                    Plainimage(i,j+1,k)=Key(a2,mod(b2-2,16)+1);
                elseif b1==b2 %jika sekolom
                    Plainimage(i,j,k)=Key(mod(a1-2,16)+1,b1);
                    Plainimage(i,j+1,k)=Key(mod(a2-2,16)+1,b2);
                else
                    Plainimage(i,j,k)=Key(a1,b2);
                    Plainimage(i,j+1,k)=Key(a2,b1);
```

```
                end
            end
        end
    end
end
% Shift Rows
function output=ShiftRowDe(input)
[m,n]=size(input);
output=input;
for i=1:m
    output(i,:)=input(i,mod((1:n)-i,n)+1);
end
%UJI ANALISIS
% Analisis Koefisien Korelasi
function corr=CoefCorr(plainimage,cipherimage)
[m,n,o]=size(plainimage);
mup=sum(sum(sum(plainimage)))/(m*n*o);
muc=sum(sum(sum(cipherimage)))/(m*n*o);
sigp=sqrt(sum(sum(sum((plainimage-mup).^2))));
sigc=sqrt(sum(sum(sum((cipherimage-muc).^2))));
corr=sum(sum(sum((plainimage-mup).*(cipherimage-
muc))))/(sigp*sigc);
% Analisis NPCR
function npcr=NPCRcal(plainimage,cipherimage)
[m,n,o]=size(plainimage);
dij=plainimage-cipherimage;
dij(dij~=0)=1;
npcr=sum(sum(sum(dij)))/(m*n*o)*100;
% Analisis UACI

function uaci=UACIcal(plainimage,cipherimage)
[m,n,o]=size(plainimage);
uaci=sum(sum(sum((abs(plainimage-cipherimage))/255)))/(m*n*o)*100;

% Analisis Histogram

function Histogram(cipherimage,vpop)
o=size(cipherimage,3);
color='rgb';
if vpop==1
    for i=1:o
        h=imhist(uint8(cipherimage(:,:,i)));
        if o==3
            bar(0:255,h,0,color(i),'EdgeColor',color(i));
        else
            bar(0:255,h,0,'k','EdgeColor','k');
            bar(h,'k','EdgeColor','k');
        end
        hold on
        maxv(i)=max(h);
    end
    hold off
    xlim([0 255]); ylim([0 1.5*max(maxv)]);
elseif vpop==2
    h=imhist(uint8(cipherimage(:,:,vpop-1)));
    bar(0:255,h,0,color(vpop-1),'EdgeColor',color(vpop-1));
    xlim([0 255]); ylim([0 1.5*max(h)]);
```

```
elseif vpop==3
    h=imhist(uint8(cipherimage(:,:,vpop-1)));
    bar(0:255,h,0,color(vpop-1),'EdgeColor',color(vpop-1));
    xlim([0 255]); ylim([0 1.5*max(h)]);
elseif vpop==4
    h=imhist(uint8(cipherimage(:,:,vpop-1)));
    bar(0:255,h,0,color(vpop-1),'EdgeColor',color(vpop-1));
    xlim([0 255]); ylim([0 1.5*max(h)]);
end
set(gca,'YTick',[]);
```