Volume 21 Nomor 1, Maret 2021

P-ISSN 1411-6669
E-ISSN 2722-9866

MIMS

MAJALAH ILMIAH

Matematika dan Statistika

DITERBITKAN OLEH:
JURUSAN MATEMATIKA
FMIPA - UNIVERSITAS JEMBER

MAJALAH ILMIAH
Matematika dan Statistika

Alamat Redaksi:
Jurusan Matematika FMIPA – Universitas Jember
Jalan Kalimantan No 37 Kampus Tegalboto Jember 68121
Telp. : (0331) 334293
E-mail: mims.fmipa@unej.ac.id
Website: https://jurnal.unej.ac.id/index.php/MIMS/index

Diterbitkan oleh : Jurusan Matematika – FMIPA Universitas Jember.
Tahun pertama terbit : Oktober 2000
Jumlah terbit : Dua kali setahun pada bulan Maret dan September
Gambar cover depan : rancang bangun geometri, iterasi dan regresi

Majalah Ilmiah Matematika dan Statistika	Volume 21 Nomor 1	Halaman: 1 – 62	Maret 2021	ISSN : 1411-6669 E-ISSN : 2722-9866

MAJALAH ILMIAH
Matematika dan Statistika

Volume 21 Nomor 1, Maret 2021

ISSN : 1411-6669
E-ISSN : 2722-9866

Daftar Isi

Penerapan Teknik Deformasi Benda Geometri Pada Lampu Dinding
(*The Application Deformation Technique of Geometry Objects in Wall Light*)
Christine Fatmasari, Bagus Juliyanto, Firdaus Ubaidillah ..... 1 – 14

Perbandingan Playfair Cipher Dengan 3D Playfair Cipher Pada Pengamanan Citra
(*Comparison of Playfair Cipher with 3D Playfair Cipher on Image Security*)
Rika Ayu Sukmawati , Abduh Riski , Ahmad Kamsyakawuni..... 15 – 24

Pemanfaatan Iterated Function System (IFS) Untuk Membangkitkan Motif Anyaman Ukuran $n \times n$
(*Utilization of Iterated Function System (IFS) to Generate Woven Pattern Size* $n \times n$)
Ingka Maris, Kosala Dwidja Purnomo, Bagus Juliyanto..... 25– 38

Pemodelan Ujung Batang dan Kait Gorden Dengan Kurva Bezier
(*Modeling of Curtains' End-Rods and Hook using Bézier Curves*)
Rokhmatul Istiqomah, Bagus Juliyanto, Firdaus Ubaidillah..... 39 – 52

Penentuan Jenis Fungsi Basis Radial Dalam Dual Reciprocity Boundary Element Method
(*On The Choice of Radial Basis Function in Dual Reciprocity Bondary Element Method*)
Millatuz Zahroh..... 53 – 62

Majalah Ilmiah Matematika dan Statistika Volume 21 Nomor 1 2021, 15 – 24
https://jurnal.unej.ac.id/index.php/MIMS/index ISSN 1441-6669

PERBANDINGAN *PLAYFAIR CIPHER* DENGAN *3D PLAYFAIR CIPHER* PADA PENGAMANAN CITRA

(*Comparison of Playfair Cipher with 3D Playfair Cipher on Image Security*)

Rika Ayu Sukmawati , Abduh Riski , Ahmad Kamsyakawuni

Jurusan Matematika, Fakultas MIPA, Universitas Jember
Jl. Kalimantan 37 Jember 68121, Indonesia
Email: rikaayusukmawati@gmail.com, {riski, kamsyakawuni}.fmipa@unej.ac.id

Abstract. The development of sending messages that are increasingly easy and sophisticated makes it easier for third parties to access or sabotage the contents of the message, so we need a science called cryptography to secure the message. This research is to secure the message on image encoding using Playfair Cipher and 3D Playfair Cipher. The process of encryption and decryption on Playfair Cipher uses two-letter pairs (bigram), while in 3D Playfair Cipher uses three-letter pairs (trigrams). The encryption process uses Playfair Cipher and 3D Playfair Cipher to produce a different image cipher with plain image visually. In the decryption process, the cipher image returns into the plain image using Playfair Cipher and 3D Playfair Cipher. Histogram analysis, NPCR, and UACI are used to see the difference between ordinary images and password images using Playfair Cipher and 3D Playfair Cipher. The average results of histogram analysis that shows safe based on research data are 14061,483 using 3D Playfair Cipher, the average NPCR results that show safe based on research data are 99.2% using Playfair Cipher, and the average UACI results showing safe based on research data is 29.1% using 3D Playfair Cipher. The results of the study indicate that the proposed method can be used to secure the message.

Keywords: Histogram Analysis, Image, NPCR, Playfair Cipher, 3D Playfair Cipher, UACI.
MSC2020: 94A60

1. Pendahuluan

Perkembangan teknologi yang semakin canggih membuat semakin mudahnya seseorang mengirimkan suatu pesan kepada orang lain tetapi hal ini juga dapat membuat semakin mudahnya pihak ketiga mengakses atau menyabotase isi pesan tersebut maka dibutuhkan suatu ilmu yang dinamakan kriptografi untuk mengamankan isi pesan. Kriptografi merupakan suatu ilmu untuk melindungi atau menyembunyikan pesan agar tidak diketahui oleh pihak ketiga dengan cara mengubah isi pesan asli menjadi kode – kode yang sulit dimengerti maknanya. Terdapat beberapa metode yang digunakan pada kriptografi, diantaranya adalah *Playfair Cipher* dan *3D Playfair Cipher*. *Playfair Cipher* merupakan salah satu metode kriptografi yang proses enkripsi dan dekripsinya menggunakan tabel berukuran 5×5, dimana setiap bagian dalam tabel kunci mewakili huruf-huruf kapital dalam alfabet dengan menghilangkan huruf J tanpa perulangan yang akan digunakan sebagai acuan proses enkripsi dan dekripsi. *Playfair Cipher* mengenkripsi pasangan huruf (digram) melalui kunci yang telah dituliskan pada tabel [1]. *Playfair Cipher* dikembangkan

menjadi *3D Playfair Cipher* untuk meningkatkan keamanan pesan teks. *3D Playfair Cipher* menggunakan kunci untuk melakukan proses enkripsi dan dekripsi, dimana kunci tersebut dituliskan pada empat tabel berukuran 4×4 yang mendukung 10 digit angka (0-9), 26 huruf (A-Z), dan 28 karakter khusus yang kemudian akan dijadikan acuan untuk proses enkripsi dan dekripsi. *3D Playfair Cipher* bekerja dalam bentuk trigram sebagai proses enkripsi dan dekripsi [2].

Pada penelitian kali ini membahas tentang peningkatan keamanan pada penyandian citra menggunakan algoritma *Playfair Cipher* dan *3D Playfair Cipher* yang dianalisis hasil enkripsinya menggunakan analisis histogram, NPCR, dan UACI.

Kriptografi

Kriptografi merupakan salah satu ilmu di bidang komputasi matematika yang mempelajari tentang bagaimana suatu pesan atau informasi agar tetap aman dan tidak dapat diketahui oleh pihak yang tidak berkepentingan. Terdapat beberapa aspek yang harus terpenuhi dalam keamanan informasi yaitu aspek kerahasiaan (*confidentiality*), integritas data (*data integrity*), otentifikasi (*authentication*), dan penyangkalan (*non repudiation*). Kriptografi (*cryptography*) merupakan ilmu dan seni untuk menjaga pesan agar aman. *Crypto* berarti *secret* yang artinya rahasia dan *graphy* berarti *writing* yang artinya tulisan. Kriptografi (*cryptography*) dapat diartikan sebagai tulisan atau pesan rahasia. Pesan yang dirahasiakan dinamakan *plaintext*, sedangkan pesan hasil penyandian disebut *ciphertext*. Proses penyandian *plaintext* menjadi *ciphertext* disebut enkripsi dan proses membalikkan *ciphertext* menjadi *plaintext* disebut dekripsi [3].

Playfair Cipher

Playfair menggunakan kunci dalam tabel berukuran 5×5 yang berisi 25 huruf alfabet dan mengganti huruf J menjadi huruf I yang ada didalam alphabet. Pada algoritma ini dibutuhkan dua huruf yang berpasangan (digram) dalam mengenkripsi dan mendekripsi pesan.

Tabel 1. Kunci pada *Playfair Cipher*

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

Beberapa aturan pada *Playfair Cipher* [1], yaitu:

a. *Playfair Cipher* mengenkripsi *plaintext* berupa huruf besar selain huruf J. Spasi, karakter yang bukan huruf besar, dan huruf J harus dihilangkan dari *plaintext.*
b. Apabila terdapat huruf J pada *plaintext*, maka digantikan dengan huruf I.
c. *Plaintext* yang akan dienkripsi dituliskan dalam pasangan huruf (bigram).

d. Apabila ada huruf yang sama dalam pasangan huruf, maka disisipkan huruf X atau Z di tengahnya. Huruf yang disisipkan sebaiknya huruf X, karena kemungkinan terdapat huruf X yang sama dalam bigram sangat kecil.
e. Apabila jumlah huruf pada *plaintext* adalah ganjil, maka dipilih sebuah huruf sembarang untuk ditambahan di akhir *plaintext*.

Langkah-langkah enkripsi *Playfair Cipher* [1] yaitu:
a. Apabila ada dua huruf terdapat pada baris kunci yang sama, maka setiap huruf diganti dengan huruf di kanannya.
b. Apabila ada dua huruf terdapat pada kolom kunci yang sama, maka setiap huruf diganti dengan huruf di bawahnya.
c. Apabila ada dua huruf tidak pada baris atau kolom yang sama, maka huruf pertama diganti dengan dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari huruf yang digunakan.

Langkah-langkah dekripsi *Playfair Cipher* [1] yaitu:
a. Apabila ada dua huruf terdapat pada baris kunci yang sama maka tiap huruf diganti dengan huruf di kirinya.
b. Apabila ada dua huruf terdapat pada kolom yang sama maka tiap huruf diganti dengan huruf diatasnya.
c. Jika dua huruf tidak pada baris yang sama atau kolom yang sama, maka huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari huruf yang digunakan.

3D Playfair Cipher

3D Playfair Cipher adalah pengembangan dari *Playfair Cipher* melalui tabel yang semula berukuran 5×5 menjadi empat tabel berukuran 4×4 untuk menuliskan kunci sebagai acuan untuk menyelesaikan proses enkripsi dan dekripsi.

Tabel 2. Kunci pada *3D Playfair Cipher*

TINGKAT 1			
0	1	2	3
4	5	6	7
8	9	A	B
C	D	E	F

TINGKAT 2			
G	H	I	J
K	L	M	N
O	P	Q	R
S	T	U	V

TINGKAT 3			
W	X	Y	Z
!	“	=	$
%	&	‘	(
)	*	+	,

TINGKAT 4			
-	.	/	:
;	<	=	>
?	@	[	\
]	^	_	|

Proses enkripsi pada *3D Playfair Cipher* adalah *plaintext* akan dipecah menjadi trigram (pasangan yang tediri dari tiga huruf). Huruf tambahan X dan Z digunakan untuk memenuhi trigraph, X ditambahkan jika terdapat tersisa satu tempat kosong pada pesan, X dan Z ditambahkan jika terdapat dua tempat kosong. Contohnya LOLLIPOP akan dirubah menjadi {LOL}, {LIP}, {OPX}, dan GOODGRACES menjadi {GOO}, {DGR}, {ACE), {SXZ). Proses enkripsi dan dekripsi menggunakan model *circular,* dimana penggantian huruf dalam trigram akan diganti oleh pesan yang sehubungan dengan posisi huruf dalam trigram di baris, kolom, dan tingkat dengan cara melingkar [2].

Tabel 3. Proses enkripsi pada *3D Playfair Cipher*

Trigram *Plaintext*	Trigram *Plaintext*			Trigram *Ciphertext*
	Kar-1	Kar-2	Kar-3	
Kar-1	Baris	Kolom	Tingkat	Kar-1
Kar-2	Tingkat	Baris	Kolom	Kar-2
Kar-3	Kolom	Tingkat	Baris	Kar-3

Proses dekripsi sama seperti proses enkripsi yaitu dengan model melingkar, akan tetapi hanya berbeda pada urutannya yaitu baris, tingkat, kolom dalam trigraf [2].

Tabel 4. Proses dekripsi pada *3D Playfair Cipher*

Trigram *Ciphertext*	Trigram *Ciphertext*			Trigram *Plaintext*
	Kar-1	Kar-2	Kar-3	
Kar-1	Baris	Tingkat	Kolom	Kar-1
Kar-2	Kolom	Baris	Tingkat	Kar-2
Kar-3	Tingkat	Kolom	Baris	Kar-3

Citra

Citra adalah gambar (*image*) pada bidang dua dimensi. Citra dapat dilakukan proses komputasi pada program komputer apabila citra didigitalkan terlebih dahulu. Citra memiliki dua jenis yaitu citra *grayscale* dan citra RGB (citra warna atau *truecolor*).

Citra *grayscale* merupakan citra digital yang hanya memiliki satu nilai kanal pada setiap *pixel*-nya, artinya nilai *Red = Green = Blue.* Nilai-nilai tersebut digunakan untuk menunjukkan intensitas warna. Citra yang ditampilkan terdiri atas warna abu-abu, bervariasi pada warna hitam sebagai bagian intensitas terlemah dan putih sebagai intensitas terkuat [4].

Citra berwarna yaitu citra yang nilai *pixel*-nya merepresentasikan warna tertentu. Banyaknya warna yang mungkin digunakan bergantung kepada kedalaman *pixel* citra yang bersangkutan. Citra RGB direpresentasikan dalam beberapa kanal yang menyatakan komponen-komponen warna penyusun. Banyak kanal yang digunakan bergantung pada model warna yang digunakan pada citra tersebut [5].

ASCII

ASCII (*American Standard Code for Information Intercange*) merupakan standar internasional dalam kode huruf dan simbol yang bersifat universal. ASCII digunakan oleh komputer dan alat komunikasi lainnya untuk menunjukkan teks [5].

ASCII merupakan kode yang digunakan untuk merepresentasikan huruf, angka dan simbol. Jumlah ASCII adalah 250 kode. ASCII 0-127 merupakan kode untuk manipulasi teks, sedangkan ASCII 128-255 merupakan kode untuk manipulasi grafik.

Analisis Histogram

Teknik analisis histogram digunakan untuk melihat kesesuaian distribusi warna antara *plainimage* dengan *cipherimage*. Jika histogram *cipherimage* memiliki keragaman distribusi dan memiliki perbedaan yang signifikan dengan *plainimage*, maka dapat dikatakan *cipherimage* tidak memberikan petunjuk untuk melakukan *statistical attack* pada *cipherimage* yang dihasilkan. Pengujian X^2 digunakan untuk menganalisis keseragaman histogram dari gambar yang terenkripsi.

$$X^2 = \sum_{i=0}^{2} \frac{(v_i - v_0)^2}{v_0} \tag{1}$$

dimana v_i merupakan frekuensi yang diamati dari nilai *pixel* $i(0 \leq i \leq 255)$ dan v_0 merupakan frekuensi yang diharapkan dari sebuah nilai *pixel* i, jadi $v_0 = \frac{m \times n}{2}$, dimana m merupakan panjang citra dan n merupakan lebar citra . Semakin kecil hasil dari X^2 maka tingkat keseragaman dalam histogram semakin merata dan hasil dari pengenkripsian semakin baik (aman), sedangkan semakin besar hasil dari X^2 maka tingkat keseragaman dalam histogram semakin tidak merata dan hasil dari pengenkripsian tentunya semakin tidak baik (tidak aman) [6].

NPCR

NPCR (*Number of Pixel Change Rate*) yaitu untuk menjamin bahwa pada setiap *pixel* terdapat perubahan elemen warna.

$$\text{NPCR} = \left(\sum_{i=1}^{m} \sum_{j=1}^{n} \sum_{k=1}^{o} \frac{d_{i,j,k}}{T} \right) \times 100\% \tag{2}$$

Nilai $d(i,j,k)$ adalah banyaknya perbedaan *pixel* yang dikalikan dengan nilai 100% setelah itu dibagi dengan lebar dan tinggi dari citra sampel. Kanal pada setiap jenis citra berbeda, diantaranya *Greyscale* yang memiliki 1 kanal, hitam putih memiliki 2 kanal, dan RGB memiliki 3 kanal. *Cipherimage* dapat dikatakan baik (aman) jika nilai pada indikator NPCR semakin besar [6].

UACI

UACI (*Unified Averaged Changed Intensity*) merupakan salah satu parameter yang digunakan untuk menganalisa perubahan satu *pixel* dalam *plainimage* yang menyebabkan perubahan besar pada *cipherimage*.

$$\text{UACI} = \left(\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{o}\frac{|C_1(i,j,k)-C_2(i,j,k)|}{F.T}\right)\times 100\% \qquad (3)$$

Cipherimage dapat dikatakan baik (aman) jika nilai pada indikator UACI semakin besar [6].

2. Metodologi

Data yang digunakan pada penilitian ini adalah citra yang disebut sebagai *plainimage*. Data yang digunakan untuk pengujian pada penelitian ini sebanyak 5 kunci dan 10 citra.

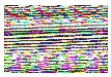
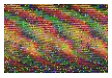
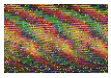
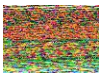
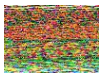
Langkah-langkah penelitian yang dilakukan adalah pertama mengumpulkan literatur yang berkaitan dengan Playfair Cipher dan 3D *Playfair Cipher*. Kedua melakukan percobaan enkripsi dan dekripsi menggunakan *Playfair Cipher* dan 3D *Playfair Cipher*. Kemudian pembuatan program enkripsi dan dekripsi pada citra menggunakan *software* MATLAB R2015b dan disimulasikan program enkripsi dan dekripsi yang telah dibuat pada *software* MATLAB R2015b. Selanjutnya menganalisis hasil keamanan citra dengan membandingkan hasil perhitungan dari analisis histogram, NPCR dan UACI. Sehingga dapat dianalisis perbandingan keamanan citra terenkripsi menggunakan *Playfair Cipher* dan *3D Playfair Cipher*.

3. Hasil dan Pembahasan

Simulasi dilakukan dengan mengenkripsi 10 citra dengan 5 kunci yang berbeda.

a. Hasil proses enkripsi menggunakan *Playfair Cipher* dan *3D Playfair Cipher*

Tabel 5. Hasil proses enkripsi

No	Data Penelitian	Kunci	*Playfair Cipher*	*3D Playfair Cipher*
1		KRIPTO		
2		KRIPTO		
3		Sigma15		
4		Sigma15		
5		Himatika		
6		Himatika		
7		1234567890		
8		1234567890		
9		!@+$%*)#_(=		
10		!@+$%*)#_(=		

b. Hasil perhitungan X^2 menggunakan *Playfair Cipher* dan *3D Playfair Cipher*

Tabel 6. Hasil Perhitungan X^2

No	Data Penelitian	Kunci	X^2
1	Citra 1	KRIPTO	*Playfair Cipher* = 20921,80 *3D Playfair Cipher* = 18000,33
2	Citra 2	KRIPTO	*Playfair Cipher* = 26762,26 *3D Playfair Cipher* = 20986,91
3	Citra 3	Sigma15	*Playfair Cipher* = 4833,88 *3D Playfair Cipher* = 4990,31
4	Citra 4	Sigma15	*Playfair Cipher* = 3309,72 *3D Playfair Cipher* = 2630,94
5	Citra 5	Himatika	*Playfair Cipher* = 5736,83 *3D Playfair Cipher* = 4581,74
6	Citra 6	Himatika	*Playfair Cipher* = 4845,27 *3D Playfair Cipher* = 4269,59
7	Citra 7	1234567890	*Playfair Cipher* = 57755,68 *3D Playfair Cipher* = 51764,08
8	Citra 8	1234567890	*Playfair Cipher* = 30557,19 *3D Playfair Cipher* = 24985,76
9	Citra 9	!@+$%*)#_(=	*Playfair Cipher* = 4980,06 *3D Playfair Cipher* = 4738,54
10	Citra 10	!@+$%*)#_(=	*Playfair Cipher* = 5475,72 *3D Playfair Cipher* = 3666,63

c. Hasil NPCR menggunakan *Playfair Cipher* dan *3D Playfair Cipher*

Tabel 7. Hasil NPCR

No	Data Penelitian	Kunci	*Playfair Cipher*	*3D Playfair Cipher*
1	Citra 1	KRIPTO	99,46%	97,62%
2	Citra 2	KRIPTO	98,88%	98,67%
3	Citra 3	Sigma15	99,38%	99,21%
4	Citra 4	Sigma15	99,44%	99,38%
5	Citra 5	Himatika	99,29%	99,30%
6	Citra 6	Himatika	99,21%	99,18%
7	Citra 7	1234567890	98,15%	97,72%
8	Citra 8	1234567890	99,20%	99,24%
9	Citra 9	!@+$%*)#_(=	99,48%	99,40%
10	Citra 10	!@+$%*)#_(=	99,55%	99,47%

d. Hasil UACI menggunakan *Playfair Cipher* dan *3D Playfair Cipher*

Tabel 8. Hasil UACI

No	Data Penelitian	Kunci	*Playfair Cipher*	*3D Playfair Cipher*
1	Citra 1	KRIPTO	26,92%	27,30%
2	Citra 2	KRIPTO	41,16%	41,13%
3	Citra 3	Sigma15	25,36%	25,74%
4	Citra 4	Sigma15	29,14%	29,29%
5	Citra 5	Himatika	19,70%	20,42%
6	Citra 6	Himatika	21,69%	21,24%
7	Citra 7	1234567890	30,29%	29,94%
8	Citra 8	1234567890	31,18%	31,35%
9	Citra 9	!@+$%*)#_(=	31,52%	31,75%
10	Citra 10	!@+$%*)#_(=	32,55%	32,55%

Hasil penelitian menunjukkan bahwa proses enkripsi citra menggunakan *Playfair Cipher* dan *3D Playfair Cipher* terlihat acak (tidak berpola) sehingga sulit untuk menduga citra aslinya. Proses enkripsi citra menggunakan *Playfair Cipher* dan *3D Playfair Cipher* juga diterapkan melalui program MATLAB R2015b berdasarkan metode yang diajukan oleh penulis.

Proses dekripsi merupakan kebalikan dari proses enkripsi. Pada proses dekripsi dilakukan juga dua perlakuan yaitu *Playfair Cipher* dan *3D Playfair Cipher*. Hasil yang diperoleh dari proses dekripsi menggunakan kedua perlakuan diatas dapat mengembalikan *cipherimage* menjadi citra asli (*plainimage*). Proses dekripsi citra menggunakan *Playfair Cipher* dan *3D Playfair Cipher* juga diterapkan melalui program MATLAB R2015b berdasarkan metode yang diajukan oleh penulis.

Hasil dari analisis histogram pada kedua perlakuan menunjukkan bahwa *3D Playfair Cipher* menghasilkan histogram yang lebih merata dengan hasil perhitungan X^2 lebih kecil dibandingkan hasil histogram menggunakan *Playfair Cipher* yang dapat dilihat pada Tabel 6. Artinya, hasil dari proses enkripsi dengan menggunakan *3D Playfair Cipher* akan lebih aman dan kuat terhadap serangan dibandingkan dengan menggunakan *Playfair Cipher*.

Hasil perhitungan NPCR pada kedua perlakuan menunjukkan bahwa *Playfair Cipher* menghasilkan nilai NPCR yang lebih besar dibandingkan hasil nilai NPCR menggunakan *3D Playfair Cipher* yang dapat dilihat pada Tabel 7. Sedangkan hasil perhitungan UACI pada kedua perlakuan menunjukkan bahwa 3D Playfair Cipher menghasilkan nilai UACI yang lebih besar dibandingkan hasil nilai UACI menggunakan *Playfair Cipher* yang dapat dilihat pada Tabel 8. Berdasarkan hasil yang telah diperoleh, semakin besar suatu hasil perhitungan nillai NPCR dan UACI maka semakin kuat suatu citra hasil enkripsi terhadap serangan.

4. Kesimpulan

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

a. Proses enkripsi menggunakan *Playfair Cipher* dan *3D Playfair Cipher* berhasil karena terlihat jelas bahwa *plainimage* dan *cipherimage* sangat berbeda secara visual. Begitu juga pada proses dekripsi menggunakan *Playfair Cipher* dan *3D Playfair Cipher* berhasil karena *cipherimage* kembali seperti *plainimage* semula.
b. Hasil perbandingan tingkat keamanan citra terenkripsi menggunakan Playfair Cipher dan 3D Playfair Cipher berdasar analisis histogram, NPCR, dan UACI adalah sebagai berikut:
    1) Berdasarkan hasil analisis histogram, tingkat keamanan citra terenkripsi menggunakan *3D Playfair Cipher* lebih aman daripada *Playfair Cipher*, hal ini dikarenakan perhitungan nilai X^2 *3D Playfair Cipher* lebih kecil daripada *Playfair Cipher* dan grafik histogram *3D Playfair Cipher* lebih merata daripada *Playfair Cipher* karena tidak ada *pixel* yang mendominasi.
    2) Berdasarkan hasil NPCR, tingkat keamanan citra terenkripsi menggunakan *Playfair Cipher* lebih aman daripada *3D Playfair Cipher*, hal ini dikarenakan nilai NPCR *Playfair Cipher* lebih besar daripada *3D Playfair Cipher*.

3) Berdasarkan hasil UACI, tingkat keamanan citra terenkripsi menggunakan *3D Playfair Cipher* lebih aman daripada *Playfair Cipher*, hal ini dikarenakan nilai UACI *3D Playfair Cipher* lebih besar daripada *Playfair Cipher*.

Adapun saran yang perlu diperhatikan untuk penelitian selanjutnya adalah Peneliti selanjutnya dapat menerapkan algoritma Playfair Cipher atau 3D Playfair Cipher yang dikombinasikan dengan algoritma kriptografi lainnya

Daftar Pustaka

[1] Nurkifli.E.H, (2014), Modifikasi Algoritma Playfair dan Menggabungkan dengan Linear Feedback Shift Register (LFSR), *SENTIKA 2014*, 366-371.

[2] Singh.S, R.Jain, dan P.Deep.Agarwal, (2015), Developing Mobile Message Security Application Using 3D Playfair Cipher Algorithm, *ICACEA*, 838-841.

[3] Santi.R.C.N, (2010), Implementasi Algoritma Enkripsi Playfair pada File Teks, *Jurnal Teknologi Informasi DINAMIK*, 15(1): 27-33.

[4] Sholehah.D.P.T, (2017), Penerapan Algoritma DNA-Vigenere Cipher dengan Kunci Citra Grayscale pada Data Teks, *Skripsi*, Jember: Universitas Jember.

[5] Muhendra.A.Z, (2016), Implementasi Kriptografi Affine Cipher pada Citra Digital Hasil Steganografi Metode Parity Coding dengan Pseudo Random Number Generator (PRNG), *Skripsi*, Jember: Universitas Jember.

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