Majalah Ilmiah Matematika dan Statistika Volume 19 Nomor 1, 2019, 17 – 28
https://jurnal.unej.ac.id/index.php/MIMS/index ISSN 1411-6669

PENYANDIAN CITRA MENGGUNAKAN ALGORITMA *4D PLAYFAIR CIPHER* DENGAN PEMBANGKITAN KUNCI MODIFIKASI *LINEAR FEEDBACK SHIFT REGISTER*

(***Image Encoding Used 4D Playfair Cipher Algorithm with Key Generation Modification of Linear Feedback Shift Register***)

Rivi Tri Rahayu, **Abduh Riski**, **Ahmad Kamsyakawuni**

Jurusan Matematika, Fakultas MIPA, Universitas Jember
Jl. Kalimantran 37 Jember 68121, Indonesia
E-mail: rivirahayu16996@gmail.com, {riski, kamsyakawuni}.fmipa@unej.ac.id

Abstract. The fast development of sophisticated technology make it easier for someone to send a message to other but can also make it easier for third parties to sabotage the content of the message, so a technique called cryptography is needed to secure the message. Image encoding is one of the techniques for securing messages in cryptography. In enhancing security in image encoding, this study discusses about Playfair Cipher, 3D Playfair Cipher and 4D Playfair Cipher with key generation using LFSR Modification. The encryption process using 4D Playfair Cipher with key generation using LFSR Modification visually produces cipher image that is different from the original image compared to using Playfair Cipher and 3D Playfair Cipher. In the decryption process using Playfair Cipher, 3D Playfair Cipher and 4D Playfair Cipher-Modification LFSR can return cipher image to its original image. The result of the study shows that the proposed method can be used to secure the message.

Keywords: Playfair Cipher, 3D Playfair Cipher, 4D Playfair Cipher, LFSR
MSC 2010: 94A60

1. Pendahuluan

Perkembangan teknologi cepat membuat semakin mudahnya seseorang mengirimkan suatu pesan kepada orang lain tetapi juga dapat membuat semakin mudahnya pihak ketiga menyabotase isi pesan tersebut maka dibutuhkan suatu teknik 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 istilah dalam kriptografi seperti enkripsi dan dekripsi. Enkripsi merupakan sebuah proses merubah pesan yang dapat dimengerti (*plaintext*) menjadi sebuah kode yang tidak dapat dimengerti (*ciphertext*) dan dekripsi merupakan sebuah proses kebalikan dari enkripsi [3]. Jenis kriptografi dibedakan menjadi dua macam yaitukriptografi klasik dan kriptografi modern. Salah satu perbedaan algoritma kriptografi klasik dan algoritma kriptografi

modern adalah algoritma kriptografi klasik menggunakan metode substitusi dan transposisi sedangkan algoritma kriptografi modern memanfaatkan operasi komputer digital dalam proses enkripsi / dekripsi [1].

Pada penelitian ini membahas tentang peningkatan keamanan pada penyandian citra menggunakan algoritma *4D Playfair Cipher* dan pembangkitan matriks kuncinya menggunakan konsep algoritma *Linear Feedback Shift Register* (LFSR) yang telah dimodifikasi. Konsep algoritma *Linear Feedback Shift Register* (LFSR) yang digunakan yaitu dengan menambahkan langkah *Shift*, Logika XOR dan XNOR. Sedangkan dua langkah modifikasi yang dilakukan pada LFSR yaitu dengan penambahan bilangan dan rotasi.

Citra

Citra merupakan gambar pada bidang dua dimensi. Citra terbagi menjadi dua antara lain, citra bersifat analog dan citra yang bersifat digital. Kualitas sebuah citra selalu dikaitkan dengan resolusi dalam intensitas warna. Resolusi citra menyatakan ukuran panjang kali lebar sebuah citra yang dinyatakan dalam satuan piksel. Semakin tinggi resolusi sebuah citra berarti semakin banyak jumlah piksel dan semakin tinggi kedalam intensitas berarti semakin banyak pula jumlah pikselnya. Citra dapat diolah menggunakan komputer, citra dapat dikatakan citra digital apabila suatu citra tersebut direpresentasikan secara numerik atau nilai-nilai diskrit melalui proses digitalisasi. Digitalisasi merupakan representasi citra dari fungsi kontinu menjadi fungsi diskrit. Secara umum, citra digital berbentuk persegi panjang dengan ukuran dimensi dapat dinyatakan sebagai tinggi × lebar atau lebar × panjang. Citra digital yang berukuran $N \times M$ dinyatakan dengan matriks berukuran N baris dan M kolom sebagai berikut:

$$f(x,y) = \begin{bmatrix} f(1,1) & \cdots & f(1,M) \\ \vdots & \ddots & \vdots \\ f(N,1) & \cdots & f(N,M) \end{bmatrix}$$

Indeks baris (x) dan indeks kolom (y) menyatakan koordinat suatu titik pada citra sedangkan $f(x,y)$ merupakan intensitas (derajat keabuan) pada titik (x,y). Masing-masing elemen pada citra digital (elemen pada matriks) disebut piksel [2].

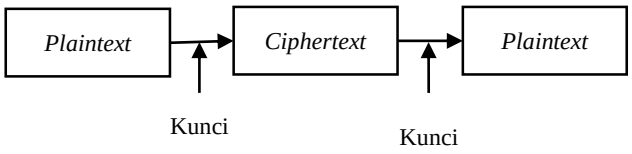
Kode ASCII

Kode ASCII (*American Standard Code for Information Interchange*) merupakan suatu standard internasional dalam kode huruf dan simbol seperti Hex dan Unicode tetapi ASCII lebih bersifat universal. Contohnya, 47 untuk karakter "/". Kode ASCII pada dasarnya memiliki komposisi bilangan biner sebanyak 8 bit. Dimulai dari 0000 0000 hingga 1111 1111. Total kombinasi yang dihasilkan pada Kode ASCII adalah 256, dimulai dari kode 0 hingga 255 dalam sistem bilangan Desimal.

Kriptografi

Kriptografi berasal dari Bahasa Yunani yaitu *cryptos* yang berarti rahasia dan *graphein*

yang berarti menulis, apabila kedua istilah digabungkan akan bermakna menulis rahasia. Kriptografi sendiri merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data, namun tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi. Terdapat beberapa istilah dalam kriptografi seperti enkripsi dan dekripsi. Enkripsi merupakan sebuah proses merubah pesan yang dapat dimengerti (*plaintext*) menjadi sebuah kode yang tidak dapat dimengerti (*ciphertext*) dan dekripsi merupakan sebuah proses kebalikan dari enkripsi.



Gambar 1. Proses enkripsi dan dekripsi

Algoritma kriptografi dibedakan menjadi dua, yaitu yaitu algoritma kriptografi klasik dan algoritma kriptografi modern. Algoritmakriptografi klasik menggunakan metode substitusi dan transposisi sedangkan algoritma kriptografi modern memanfaatkan operasi komputer digital dalam proses enkripsi dan dekripsi [3].

Playfair Cipher

Playfair menggunakan kunci dalam matriks 5×5 yang berisi 25 huruf alfabet dan mengganti huruf J menjadi huruf I yang ada didalam alfabet. *Playfair Cipher* merupakan salah satu kriptografi klasik yang penyandiannya menggunakan subtitusi. Pada algoritma ini dibutuhkan dua huruf yang berpasangan (digram) dalam mengenkripsi dan mendekripsi pesan [6].

Beberapa aturan dalam membuat sandi pada *playfair cipher* [6], yaitu:

a. Jika dua huruf *plaintext* berada pada satu baris kunci yang sama maka setiap huruf diganti dengan huruf yang berada disebelah kanannya.
b. Jika dua huruf *plaintext* berada pada satu kolom kunci yang sama maka setiap huruf diganti dengan huruf yang berada dibawahnya.
c. Jika huruf *plaintext* berada terbalik dengan tabel maka sandi yang dihasilkan akan dibaca terbalik, dengan kata lain yang semula dibacanya kiri ke kanan menjadi kanan ke kiri.
d. 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 tiga huruf yang digunakan.
e. Jika terdapat huruf yang ganda pada *plaintext* harus disisipkan huruf X atau Z dan apabila *plaintext* memiliki jumlah huruf yang ganjil maka harus disisipkan juga huruf X atau Z pada akhir *plaintext*.

3D Playfair Cipher

3D Playfair Cipher adalah pengembangan algoritma kriptografi klasik yang membutuhkan tiga huruf berpasangan (trigram) selama proses enkripsi dan dekripsi. Pada algoritma ini menggunakan formasi matriks kunci berukuran 4 × 4 × 4 yang berisi 26 huruf alfabet, 10 angka, dan beberapa simbol khusus. Pada algortima ini memiliki matriks kunci terdiri dari empat baris, empat kolom, dan empat tingkat (lihat Tabel 1). Kunci yang digunakan pada algoritma ini tidak boleh berulang [9].

Tabel 1. Matriks kunci *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			
-	.	/	:
;	<	=	>
?	@	[	\
]	^	_	|

Selama proses enkripsi, pesan akan dipecah menjadi trigram (pasangan yang tediri dari tiga huruf). Huruf tambahan X dan Z digunakan untuk memenuhi trigram, X atau Z ditambahkan jika tersisa satu tempat kosong pada pesan, X dan Z ditambahkan jika terdapat dua tempat kosong. Contohnya, NEGARAKU akan diubah menjadi {NEG}, {ARA} dan {KUX}. Penggantian huruf dalam trigram akan diganti oleh pesan yang sehubungan dengan posisi huruf dalam trigram di baris, kolom, tingkat dengan cara melingkar (lihat Tabel 2). Proses enkripsi menggunakan model *circular* dapat dilihat pada [9].

Tabel 2. Proses enkripsi

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

Penggantian huruf untuk tujuan dekripsi mengikuti mode *circular*, hanya urutannya berubah yaitu baris, tingkat, kolom huruf dalam trigram *plaintext* [9], seperti ditunjukkan pada Tabel 3.

Tabel 3. Proses dekripsi

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

4D Playfair Cipher

4D Playfair Cipher adalah pengembangan algoritma kriptografi klasik yang membutuhkan empat huruf berpasangan (*quartets*) selama proses enkripsi dan dekripsi. Pada algoritma ini menggunakan formasi matriks kunci berukuran $2 \times 2 \times 13 \times 5$ yang berisi 260 bilangan dari 0 sampai 259. Pada algoritma ini nilai 0 sampai 255 menampilkan bilangan yang dapat menyimpan seluruh nilai pada kode ASCII. Bilangan 256 sampai 258 digunakan atau disisipkan apabila jumlah huruf *plaintext* bukan kelipatan empat. Nilai 259 digunakan hanya selama proses substitusi [1].

4DPlayfair Cipher memiliki empat langkah utama, antara lain:

a. Buatlah kunci rahasia dengan barisan bilangan antara 0 sampai 259. Contohnya : (10 20 30 40 50 60 70 80).
b. Bilangan yang terdapat di dalam kunci rahasia tidak boleh berulang atau terdapat bilangan yang sama.
c. Masukkan kunci pada langkah sebelumnya kedalam matriks kunci berukuran $2 \times 2 \times 13 \times 5$ yang disediakan oleh *4DPlayfair Cipher* dengan mengisi berurutan dimulai dari D1_P1, D1_P2, D2_P1 sampai D2_P2.
d. Sisipkan pada tempat yang tersisa dalam matriks dengan bilangan yang tidak terdapat didalam kunci dimulai dari bilangan 0 sampai 259 mengkuti aturan yang diberika pada langkah tiga [1].
   Matriks kunci pada *4DPlayfair Cipher* dapat dilihat pada Tabel 4.

Proses enkripsi menggunakan metode *circular*, seperti pada Tabel 5. Pergantian huruf dalam *quartets* akan diganti oleh pesan sandi yang sehubungan dengan posisi yang terdapat dalam *quartets* pada baris (*row* / R), kolom (*coloumn* / C), arah (*direction* / D), dan kerangka (*plane* / P*)* dengan metode melingkar [1].

Tabel 4. Matriks *4Dplayfair cipher*

D1_P1

0	1	2	3	4
5	6	7	8	9
10	11	12	13	14
15	16	17	18	19
20	21	22	23	24
25	26	27	28	29
30	31	32	33	34
35	36	37	38	39
40	41	42	43	44
45	46	47	48	49
50	51	52	53	54
55	56	57	58	59
60	61	62	63	64

D1_P2

65	66	67	68	69
70	71	72	73	74
75	76	77	78	79
80	81	82	83	84
85	86	87	88	89
90	91	92	93	94
95	96	97	98	99
100	101	102	103	104
105	106	107	108	109
110	111	112	113	114
115	116	117	118	119
120	121	122	123	124
125	126	127	128	129

D2_P1

130	131	132	133	134
135	136	137	138	139
140	141	142	143	144
145	146	147	148	149
150	151	152	153	154
155	156	157	158	159
160	161	162	163	164
165	166	167	168	169
170	171	172	173	174
175	176	177	178	179
180	181	182	183	184
185	186	187	188	189
190	191	192	193	194

D2_P2

195	196	197	198	199
200	201	202	203	204
205	206	207	208	209
210	211	212	213	214
215	216	217	218	219
220	221	222	223	224
225	226	227	228	229
230	231	232	233	234
235	236	237	238	239
240	241	242	243	244
245	246	247	248	249
250	251	252	253	254
255	256	257	258	259

Tabel 5. Proses enkripsi *4Dplayfair cipher*

Plaintext Quartet	*Plaintext Quartet*				*Ciphertext Quartet*
	Kar-1	Kar-2	Kar-3	Kar-4	
Kar-1	R	C	D	P	Kar-1
Kar-2	P	R	C	D	Kar-2
Kar-3	D	P	R	C	Kar-3
Kar-4	C	D	P	R	Kar-4

Penggantian huruf untuk tujuan dekripsi mengikuti mode *circular* seperti pada proses enkripsi, hanya urutannya berubah baris (*row* / R), kerangka (*plane* / P), arah (*direction* / D) dan kolom (*coloumn* / C) dengan metode melingkar (circular) [1].

Tabel 6. Proses enkripsi *4DPlayfair Cipher*

Ciphertext Quartet	*Ciphertext Quartet*				*Plaintext Quartet*
	Kar-1	Kar-2	Kar-3	Kar-4	
Kar-1	R	P	D	C	Kar-1
Kar-2	C	R	P	D	Kar-2
Kar-3	D	C	R	P	Kar-3
Kar-4	P	D	C	R	Kar-4

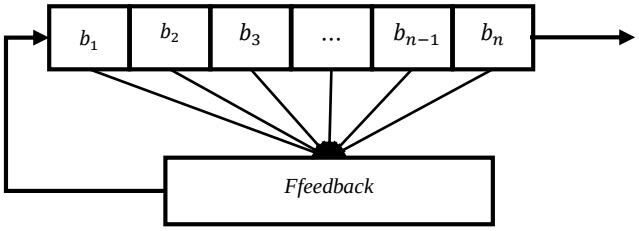
Linear Feedback Shift Register (LFSR)

Linear Feedback Shift Register (LFSR) merupakan salah satu algoritma yang dapat digunakan untuk membangkitkan deretan bilangan biner secara acak dalam pembuatan kunci pada kriptografi. LFSR membangkitkan deretan bilangan dengan menggunakan operasi XOR dan XNOR. Pada proses XOR nilai awal bit yang ada pada register dengan panjang tertentu tergantung dari derajat polinomial yang digunakan. LFSR adalah *shift register* yang bit masukannya merupakan fungsi umpan-balik dari bentuk sebelumnya. Periode maksimum LFSR dengan n-bit memiliki rumus $2^n - 1$ [7].

Bentuk umum dari *Linear Feedback Shift Register* (LFSR) dapat didefinisikan, sebagai berikut:

$$r_{i+1}(b_0, b_1, b_2, \dots, b_{n-1}) = f(b_0, b_1, b_2, \dots, b_{n-1})$$

dimana f adalah fungsi *Linear Feedback Shift Register* (LFSR).
Pembangkitan fungsi umpan balik LFSR dapat dibangkitkan seperti Gambar 2.



Gambar 2. LFSR dengan n-bit

Modifikasi *Linear Feedback Shift Register* (LFSR) merupakan pengembangan algoritma *Linear Feedback Shift Register* (LFSR) dimana pada modifikasinya urutan bilangan acak yang dihasilkan dari perhitungan *Linear Feedback Shift Register* (LFSR) selanjutnya dirotasi sejauh lima ke kiri.

Logika XOR dan XNOR

XOR merupakan singkatan dari *Exclusive*-OR. Logika operasi XOR akan menghasilkan keluaran bernilai Benar jika dan hanya jika salah satu dari nilai input bernilai Benar. Jika kedua input bernilai Benar maka keluaran akan bernilai Salah [8]. Pada operasi logika 0 merepresentasikan logika bernilai Salah dan 1 merepresentasikan logika bernilai Benar. Tabel 7 menunjukkan tabel kebenaran dari operasi XOR.

Tabel 7. Tabel kebenaran operasi XOR

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

XNOR merupakan *invers* dari XOR. Jika pada XOR nilai Benar didapat jika dan hanya jika salah satu input saja yang bernilai Benar. Pada XNOR hasil Benarhanya didapat jika kedua nilai ini menunjukkan nilai yang sama (Benar-Benar atau Salah-Salah). Jika salah satu input saja yang bernilai Benar maka keluarannya akan bernilai Salah [8]. Tabel 8 menunjukkan tabel kebenaran dari logika XNOR.

Tabel 8. Tabel kebenaran operasi XNOR

A	B	A XNOR B
0	0	1
0	1	0
1	0	0
1	1	1

Analisis Histogram

Analisis histogram merupakan salah satu analisis yang dapat digunakan untuk melihat apakah hasil dari proses enkripsi aman dan tahan terhadap serangan-serangan kriptanalisis. Di dalam bidang pengolahan citra histogram memperlihatkan distribusi nilai *pixel* di dalam sebuah citra. Histogram digunakan penyerang untuk melakukan kriptanalisis dengan memanfaatkan frekuensi kemunculan *pixel* di dalam histogram. Penyerang berharap nilai *pixel* yang sering muncul di dalam *plainimage* berkorelasi dengan nilai *pixel* yang sering muncul di dalam *cipherimage*.Histogram *cipherimage* dan *plainimage* seharusnya berbeda secara signifikan atau secara statistik tidak memiliki kemiripan [5].

Analisis histogram yang digunakan adalah pengujian X^2 dari gambar yang telah terenkripsi. Persamaan X^2 dari gambar terenkripsi dari dimensi $m \times n$ sebagai berikut.

$$X^2 = \sum_{i=0}^{255} \frac{(v_i - v_0)^2}{v_0}$$

dimana v_i adalah frekuensi yang diamati dari nilai piksel $i(0 \leq i \leq 255)$ dan v_0 merupakan frekuensi yang diharapkan dari nilai piksel i, jadi $v_0 = \frac{m \times n}{256}$. Sehingga semakin kecil hasil pengujian X^2 maka tingkat keseragaman dalam histogram semakin merata dan hasil dari enkripsi semakin aman dan berlaku sebaliknya [2].

Analisis Diferensial

Analisis Diferensial digunakan untuk menguji pengaruh perubahan setiap *pixel* pada citra yang terenkripsi. Terdapat dua indikator pengukuran umum yang digunakanpada analisis ini yaitu *Number of Pixel Change Rate* (NPCR) dan *Unified Avarage Changing Intensity* (UACI). Adapun perhitungan NPCR didefinisikan sebagai berikut:

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

dimana m, n dan o adalah lebar, tinggi, dan kedalaman citra dan digunakan untuk menghitung T yang merupakan jumlah total *pixel* pada *cipherimage* sedangkan $d_{i,j,k}$ melambangkan derajat keabuan ditentukan sebagai berikut:

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

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

Sedangkan perhitungan UACI didefinisikan sebagai berikut :

$$UACI = \left(\sum_{i=1}^{m} \sum_{j=1}^{n} \sum_{k=1}^{o} \frac{\left| c_{i,j,k}^{(1)} - c_{i,j,k}^{(2)} \right|}{F \cdot T} \right) \times 100\%$$

dimana F menunjukkan nilai *pixel* terbesar yang kompatibel dengan *chiperimage* [2].

2. Metodologi

Data yang digunakan pada penilitian ini adalah citra yang disebut sebagai *plainimage*. Data yang digunakan untuk pengujian pada penelitian ini sebanyak 4 citra. Langkah-langkah penelitian yang dilakukan adalah pertama mengumpulkan literatur yang berkaitan dengan *Playfair Cipher*, *3D Playfair Cipher* dan *4D Playfair Cipher*-Modifikasi LFSR. Kedua melakukan percobaan enkripsi dan dekripsi menggunakan *Playfair Cipher*, *3D Playfair Cipher* dan *4D Playfair Cipher*-Modifikasi LFSR. 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 histogram, NPCR dan UACI. Sehingga dapat dianalisis pengaruh pertambahan pembangkitan kunci algoritma Modifikasi LFSR terhadap peningkatan keamanan *cipher image* yang dihasilkan.

3. Hasil dan Pembahasan

Simulasi dilakukan dengan mengenkripsi 2 citra *Grayscale* dan 2 citra RGB. Misal kunci yang digunakan pada saat enkripsi dan dekripsi citra menggunakan *Playfair Cipher*, *3D Playfair Cipher* dan *4D Playfair Cipher*-Modifikasi LFSR adalah “MTK2015a”.

a. Hasil Perhitungan X^2 Menggunakan *Playfair Cipher*, *3D Playfair Cipher* dan *4D Playfair Cipher*-Modifikasi LFSR.

Tabel 9. Hasil perhitungan X^2

No	Data Penelitian	X^2
1	Citra 1	*Playfair Cipher* =*12214,97* *3D Playfair Cipher* =10930,61 *4D Playfair Cipher*-Modifikasi LFSR=2989,12
2	Citra 2	*Playfair Cipher* =9194,32 *3D Playfair Cipher* =8583,62 *4D Playfair Cipher*-Modifikasi LFSR=2792,72
3	Citra 3	*Playfair Cipher* =*5662,30* *3D Playfair Cipher* =5473,66 *4D Playfair Cipher*-Modifikasi LFSR =4137,20
4	Citra 4	*Playfair Cipher* =172950,88 *3D Playfair Cipher* =80162,79 *4D Playfair Cipher*-Modifikasi LFSR=*7249,30*

b. Hasil Analisis Diferensial Menggunakan *Playfair Cipher*, *3D Playfair Cipher* dan *4D Playfair Cipher*-Modifikasi LFSR

Tabel 10. Hasil analisis diferensial NPCR

No	Data Penelitian	NPCR (%)		
		Playfair Cipher	*3D Playfair Cipher*	*4D Playfair Cipher*-Modifikasi LFSR
1	Citra 1	99,24	99,34	87,32
2	Citra 2	99,34	99,32	87,77
3	Citra 3	99,40	99,35	92,83
4	Citra 4	98,95	99,14	81,35

Tabel 11. Hasil analisis diferensial UACI

No	Data Penelitian	UACI (%)		
		Playfair Cipher	*3D Playfair Cipher*	*4D Playfair Cipher*-Modifikasi LFSR
1	Citra 1	44,67	44,93	31,52
2	Citra 2	42,08	42,04	31,34
3	Citra 3	21,76	22,13	26,87
4	Citra 4	25,62	24,66	22,84

Hasil penelitian menunjukkan bahwa proses enkripsi citra menggunakan *Playfair* Cipher terlihat acak. Pada proses enkripsi menggunakan *3D Playfair* Cipher juga terlihat acak. Sedangkan proses enkripsi menggunakan *4D Playfair* Cipher terlihat acak (tidak berpola) sehingga sulit untuk menduga citra aslinya. Proses enkripsi citra menggunakan *Playfair Cipher*, *3D Playfair Cipher* dan *4D Playfair Cipher*-Modifikasi LFSR juga diterapkan melalui program MATLAB R2015b berdasarkan metode yang diajukan oleh penulis.

Proses dekripsi merupakan kebalikan dari proses enkripsi. Pada proses dekripsi dilakukan juga tiga perlakuan yaitu *Playfair Cipher*, *3D Playfair Cipher* dan *4D Playfair Cipher*-Modifikasi LFSR. Hasil yang diperoleh dari proses dekripsi menggunakan ketiga perlakuan diatas dapat mengembalikan *cipherimage* menjadi citra asli (*plainimage*). Proses dekripsi citra menggunakan *Playfair Cipher*, *3D Playfair Cipher* dan *4D Playfair Cipher*-Modifikasi LFSR juga diterapkan melalui program MATLAB R2015b berdasarkan metode yang diajukan oleh penulis.

Hasil dari analisis histogram pada ketiga perlakuan menunjukkan bahwa *4D Playfair Cipher*-Modifikasi LFSR menghasilkan histogram yang lebih merata dengan hasil perhitungan X^2 lebih kecil dibandingkan hasil histogram menggunakan *Playfair Cipher* dan *3D Playfair Cipher*. Artinya, hasil dari proses enkripsi dengan menggunakan *4D Playfair Cipher*-Modifikasi LFSR akan lebih kuat terhadap serangan analisis tipe statistik dibandingkan dengan menggunakan *Playfair Cipher* dan *3D Playfair Cipher*.

Hasil perhitungan NPCR yang diperoleh menggunakan *4D Playfair Cipher*-Modifikasi LFSR adalah sebesar 81,35% hingga 92,83% sedangkan hasil perhitungan NPCR yang diperoleh menggunakan *Playfair Cipher* adalah sebesar 98,95% hingga99,40% dan hasil perhitungan NPCR yang diperoleh menggunakan *3D Playfair Cipher* adalah sebesar 99,14% hingga 99,42%. Tabel 11 dijelaskan bahwa hasil perhitungan UACI yang diperoleh menggunakan *4D Playfair Cipher*-Modifikasi LFSR adalah sebesar 22,84% hingga 31,52% sedangkan hasil perhitungan UACI yang diperoleh menggunakan *Playfair Cipher* adalah sebesar 21,76% hingga 44,67% dan hasil perhitungan UACI yang diperoleh menggunakan *3D Playfair Cipher* adalah sebesar 22,13% hingga 44,93%. Berdasarkan hasil yang telah diperoleh, semakin besar suatu hasil perhitungan NPCR dan UACI maka semakin kuat suatu citra hasil enkripsi terhadap serangan diferensial. Citra yang menghasilkan nilai NPCR dan UACI di bawah minimum masih kuat terhadap serangan diferensial, dibuktikan secara visual bahwa citra terlihat tidak berpola. Namun citra yang menghasilkan nilai NPCR dan UACI di bawah minimum rentan terhadap serangan diferensial apabila citra yang dihasilkan dari proses enkripsi masih terlihat jelas polanya.

4. Kesimpulan

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

a. Pembangkitan kunci menggunakan Modifikasi *Linear Feedback Shift Register* (LFSR) dapat menghasilkan deretan bilangan secara acak tanpa terdapat perulangan kunci pada deretan bilangan.
b. Proses enkripsi menggunakan algoritma *4D Playfair Cipher* dan Modifikasi *Linear Feedback Shift Register* (LFSR) menghasilkan *cipherimage* berbeda dari citra asli

secara visual dan proses dekripsi dapat mengembalikan *cipherimage* kedalam citra aslinya. Proses enkripsi menggunakan algoritma *Playfair Cipher* maupun *3D Playfair Cipher* menghasilkan *cipherimage* berbeda dengan citra asli secara visual dan proses dekripsi dapat mengembalikan *cipherimage* kedalam citra aslinya.

c. Berdasarkan perbandingan antara hasil perhitungan dari histogram, NPCR, UACI, dan *cipherimage* yang dihasilkan. Tingkat keamanan hasil penyandian citra menggunakan *4D Playfair Cipher* dengan pembangkitan kunci Algoritma Modifikasi LFSR lebih kuat dibandingkan dengan hasil penyandian citra menggunakan *Playfair Cipher* dan *3D Playfair Cipher*, dapat dilihat pada hasil histogram yang seragam, hasil perhitungan X^2 lebih kecil, serta *cipherimage* yang dihasilkan acak dan merata daripada menggunakan *Playfair Cipher* dan *3D Playfair Cipher.*

Daftar Pustaka

[1] Bhat, K., D. Mahto., dan D. K. Yadav. (2017). A Novel Approach to Information Four Dimensional (4D) Playfair Cipher Fused With Linear Feedback Shift Register. *Indian Journal of Computer Science and Engineering (IJCSE).* 8 (1):15-32.

[2] Boriga, R. E., A.C. Dascalescu, dan A.V. Diaconu. (2014). A New Fast Image Encryption Scheme Based on 2D Chaotic Maps. *IAENG International Journal of Computer* (*IJSC*). 41(4):1-10.

[3] Donnaro, D. P. (2018). Implementasi Teknik Playfair Cipher untuk Penyembunyian Teks Terenkripsi pada Citra dengan Metode End of File. *Skripsi*. Jember: Universitas Jember.

[4] Munir, R. (2002). *Diktat Kuliah Pengolahan Citra*. Bandung: Departemen Teknik Informatika ITB.

[5] Munir, R. (2012). Analisis Keamanan Algoritma Enkripsi Citra Digital Menggunakan Kombinasi Dua Chaos Map dan Penerapan Teknik Selektif. *Juti*. 10(2):89–95.

[6] Nurkifli, E. H. (2014). Modifikasi Algoritma Playfair dan Menggabungkan dengan Linear Feedback Shift Register (LFSR). *SENTIKA.* ISSN: 2089-9813. 366-271.

[7] Pramudianto, A. D. dan Rino. (2012). Penggunaan Polinomial untuk Stream Key Generator pada Algoritma Stream Ciphers Berbasis Feedback Shift Register. *Seminar Nasional Matematika dan Pendidikan Matematika*. ISBN : 978-979-16353-8-7. Yogyakarta: Universitas Negeri Yogyakarta.

[8] Putra, D. (2010). *Pengolahan Citra Digital*. Yogyakarta:Andi Offset.

[9] Singh, S., Jain, R., Deep, P. dan Agarwal, S. (2015). Developing Mobile Messege Security Application Using 3D Playfair Cipher Algorithm. *International Coference on Advances in Computer Engineering and Applications (ICACEA).* 838 – 841.