PENYANDIAN CITRA MENGGUNAKAN METODE *PLAYFAIR CIPHER*

Emy Setyaningsih
Program Studi Ilmu Komputer, Fakultas Sains Terapan,
Institut Sains & Teknologi AKPRIND Yogyakarta
Jl. Kalisahak No. 28 Balapan Yogyakarta 55222

ABSTRACT

Playfair Cipher is one of the methods which is classified as classic kriptogafi encryption process using the processing in the form of large blocks. This method is one way to overcome the weaknesses of other classical cryptographic methods which are easily predictable because there is one-one correspondence between plainteks with cipherteks. Just as in text messages confidential, messages also require image techniques encryption as simple as possible, but difficult to solve . The process of securing the message in the form of images can be done by encrypting the image into another image in a particular algorithm. This is possible since an image can be represented in a matrix that contains the integers. In this study Playfair Cipher will be implemented to encrypt the image with 24 bits bmp format, which has a size of 256 x 256 pixels. The image to be tested consists of 2 types of images which are images with different contrast levels and image with a category different levels of detail. The key used to encrypt the image is by using a matrix of type 2 has order 16 x 16.

*From the test results obtained that Playfair cipher is a classic method that suitable for the image with good quality and the image with the image category detail. This can be seen from the randomness of the image color intensity that has been encoded. Also because of the key matrics used size large enough to cause kriptanalisis takes long enough to find the key matrix, because there are **256!** Likely form a key matrix.*

***Key words** : playfair cipher, image, kriptanalisis, cipherteks, plainteks*

INTISARI

Playfair Cipher merupakan salah satu metode yang digolongkan dalam kriptogafi klasik yang proses enkripsinya menggunakan pemrosesan dalam bentuk blok-blok yang sangat besar. Metode ini merupakan salah satu cara untuk mengatasi kelemahan metode kriptografi klasik lainnya yang mudah tertebak karena terdapat korespondensi satu-satu antara *plainteks* dengan *cipherteks*. Seperti halnya pesan teks dalam menjaga kerahasiaannya, pesan citra juga memerlukan teknik-teknik enkripsi yang sebisa mungkin sederhana tapi sukar dipecahkan. Proses pengamanan pesan dalam bentuk citra dapat dilakukan dengan mengenkripsi citra ke dalam bentuk citra lagi dengan algoritma tertentu. Ini dimungkinkan mengingat sebuah citra dapat direpresentasikan dalam sebuah matriks yang berisi bilangan-bilangan bulat. Pada penelitian ini *Playfair Cipher* akan diimplementasikan untuk menyandikan citra dengan format bmp 24 bit, yang mempunyai ukuran 256 x 256 pixel. Citra yang akan diujikan terdiri dari 2 jenis citra yaitu citra dengan tingkat kontras yang berbeda serta citra dengan kategori tingkatan detil yang berbeda. Kunci yang digunakan untuk menyandikan citra menggunakan 2 jenis matrik yang mempunyai ordo 16 x 16.

Dari hasil pengujian didapatkan bahwa *playfair* merupakan metode penyandian klasik yang cocok diterapkan untuk citra dengan kualitas yang baik dan pada citra dengan kategori citra detil. Hal ini terlihat dari keacakan intensitas warna pada citra yang telah tersandikan. Selain itu karena matrik kunci yang digunakan ukurannya cukup besar mengakibatkan kriptanalisis akan membutuhkan waktu yang cukup lama untuk menemukan matrik kuncinya, karena terdapat 256**!** kemungkinan bentuk matrik kunci.

Kata kunci : *playfair cipher*, citra, kriptanalisis, cipherteks, plainteks

PENDAHULUAN

Kemajuan di bidang telekomunikasi dan komputer telah memungkinkan ribuan orang dan komputer di seluruh dunia terhubung dalam satu dunia maya yang dikenal dengan *cyberspace* atau internet. Internet sebagai jalan raya informasi (*the information highway)* telah banyak dirasakan benar-benar membawa perubahan pada banyak aspek dalam kehidupan manusia. Salah satunya adalah fasilitas e-mail yang telah banyak dimanfaatkan oleh banyak orang

untuk mengirim dokumen yang di *attach* pada *e-mail* melalui internet. Proses pengiriman dengan memanfaatkan fasilitas ini cukup efisien, cepat, dan murah. Namun internet juga merupakan salah satu jaringan publik yang tidak aman. Kegiatan-kegiatan tersebut tentu saja akan menimbulkan resiko bilamana informasi yang sensitif dan berharga tersebut diakses oleh orang-orang yang tidak berhak (*unauthorized persons*), misalnya informasi mengenai dokumen yang berupa data teks atau gambar/citra yang besifat rahasia. Informasi-informasi tersebut apabila jatuh kepada orang-orang yang jahat pada saat pengiriman dokumen maka dokumen tersebut bisa saja dengan illegal diubah isinya tanpa diketahui pengirim atau penerima. Tanpa fasilitas keamanan yang baik, sang penerima akan menerima dokumen tersebut tanpa mencurigai adanya perubahan yang dapat merugikan baik bagi pengirim maupun penerima. Untuk itu diperlukan system pengaman data yang dapat digunakan untuk melindungi data yang ditransmisikan melalui suatu jaringan komunikasi. Salah satu cara yang dapat dilakukan untuk pengamanan data melalui suatu saluran data adalah kriptografi.

Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut *Cryptology*. Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah. Oleh karena itu Kriprografi/penyandian dikatakan sebagai metode yang tangguh karena dalam kriptografi data yang dikirimkan melalui jaringan akan disamarkan sedemikian rupa menggunakan algoritma sandi. Data tersebut akan tetap aman kendati setiap orang dapat mengaksesnya secara bebas, sehingga kalaupun data tersebut dapat dibaca tetapi tidak dapat dipahami oleh pihak yang tidak berhak(Schneier, 1996).

Oleh karena itu pengembangan metode kriptografi perlu diperluas penggunaannya yang tidak hanya terbatas untuk penyandian berupa teks, tetapi juga berupa gambar (Siang, 2002), audio maupun video (Soplanit, 2005).

Seperti halnya pesan teks dalam menjaga kerahasiaannya, pesan citra juga memerlukan teknik-teknik enkripsi yang sebisa mungkin sederhana tapi sukar dipecahkan. Proses pengamanan pesan dalam bentuk citra dapat dilakukan dengan mengenkripsi citra ke dalam bentuk citra lagi dengan algoritma tertentu.

Ada dua teknik yang digunakan untuk penyandian data/citra yaitu kriptografii klasik dan kriptografi modern. Penyandian menggunakan kriptografi klasik adalah metode untuk mengubah data asli (*plainteks*) ke bentuk sandi (*cipherteks*) dengan menggunakan kunci yang sama. Sedangkan kriptografi modern menggunakan dua buah kunci. Satu kunci yang disebut kunci publik (*public key*) yang dapat dipublikasikan, sedang kunci yang lain yang disebut kunci privat (*private key*) harus dirahasiakan (Stinson, 1995).

Polygram substitution cipher merupakan salah satu metode yang digolongkan dalam kriptogafi klasik yang proses enkripsinya menggunakan pemrosesan dalam bentuk blok-blok yang sangat besar. Metode ini merupaka salah satu cara untuk mengatasi kelemahan metode kriptografi klasik lainnya yang mudah tertebak karena terdapat korespondensi satu-satu antara *plainteks* dengan *cipherteks*. Metode *polygram substitution cipher* diantaranya adalah sandi *hill cipher* dan *playfair cipher*. Kedua sandi tersebut dilakukan dengan memanfaatkan operasi matrik biasa.

Sandi Playfair digunakan oleh Tentara Inggris pada saat Perang Dunia I. *Play cipher* adalah suatu diagram substitution *cipher* yang ditemukan pada tahun 1854 oleh Charles Wheatstone dan Baron Lyon (Stinson, 1995). Playfair merupakan *digraphs cipher* artinya setiap proses enkripsi maupun dekripsi dilakukan menggunakan pasangan karakter huruf.

Pada penelitian ini metode sandi *playfair* akan diimplementasikan untuk menyandikan sebuah citra. Hal ini dimungkinkan mengingat sebuah citra dapat direpresentasikan dalam sebuah matriks yang berisi bilangan-bilangan bulat seperti yang digunakan pada matrik kunci pada metode *playfair cipher*. Proses enkripsi yang dikembangkan untuk data citra dilakukan dengan menggunakan pasangan bilangan yang mewakili intensitas warna dari citra. Citra yang digunakan dalam pengujian penelitian ini dibatasi pada citra dengan format bmp 24 bit dengan tingkat kontras dan kedetilan yang berbeda untuk membandingkan hasil enkripsi citra. Matrik kunci yang digunakan untuk metode palyfair *cipher* adalah matrik berordo 16 x 16.

Langkah-langkah enkripsi adalah sebagai berikut :

1) membentuk matrik bujur sangkar yang akan menjadi kunci dengan jumlah disesuaikan dengan semesta pembicaraan yang digunakan sebagai dasar. Misalkan pada citra yang mempunyai derajad keabuan 256 maka kunci yang akan digunakan untuk

menyandikan citra adalah matrik bujur sangkar dengan ukuran 16 x 16 dengan nilai elemennya adalah bilangan bulat acak antara 0 sampai dengan 255.

2) *Cipher*ing menggunakan setiap pasangan intensitas citra dalam plainteks untuk masing-masing kanal warna. Plainteks dibagi dalam blok-blok dimana setiap blok berisi 2 pixel (m1 dan m2) pada masing-masing baris untuk setiap kanal warna.
3) Proses *cipher*ing pada masng-masing kanal warna dilakukan dengan cara :
   a. jika m1 dan m2 terdapat pada baris yang sama dalam matrik kunci maka c1 diambil dari 1 pixel sebelah kanan m1, c2 diambil dari 1 pixel sebelah kanan m2 pada matrik kunci.
   b. jika m1 dan m2 terdapat pada kolom yang sama dalam matrik maka c1 dan c2 masing-masing diambil dari 1 pixel dibawah m1 dan m2 pada matrik kunci.
   c. jika m1 dan m2 berbeda baris dan kolom dalam matrik kunci maka c1 diambil dari pertemuan baris pixel m1 dan kolom m2, dan c2 diambil dari pertemuan baris m2 dan kolom m1 pada matrik kunci.
   d. Jika m1 = m2 maka cipherteks adalah c1=m1 dan c2=m2.

Sedangkan proses dekripsi caranya adalah sebagai berikut :

1) Sama dengan proses enkripsi yaitu menggunakan matrik kunci yang sama untuk proses enkripsi.
2) Proses *cipher*ing dilakukan dengan cara :
   a. jika c1 dan c2 terdapat pada baris yang sama dalam matrik kunci maka m1 diambil dari 1 pixel sebelah kiri c1, m2 diambil dari 1 pixel sebelah kiri c2 pada matrik kunci.
   b. jika c1 dan c2 terdapat pada kolom yang sama dalam matrik maka m1 dan m2 masing-masing diambil dari 1 pixel diatas m1 dan m2 pada matrik kunci.
   c. jika c1 dan c2 berbeda baris dan kolom dalam matrik kunci maka m1 diambil dari pertemuan baris c1 dan kolom c2, dan m2 diambil dari pertemuan baris c2 dan kolom c1 pada matrik kunci.
   d. jika c1 = c2 maka plainteks adalah adalah m1=c1 dan m2=c2.

Sebagai parameter pada penulisan ini akan digunakan data yang terdiri dari 2 kelompok citra yang berbeda dengan ukuran 256 x 256 (*pixels*) seperti terlihat pada gambar 1,dan gambar 2.

1) Pengelompokkan citra berdasarkan kekontrasan citra (Citra yang mewakili citra yang kontras rendah dan citra dengan kontras yang baik) seperti terlihat pada Gambar 1.

(a) (b)

Gambar 1. (a) Citra dengan Kontras Rendah
(b) Citra dengan Kontras Baik

2) Pengelompokkan citra berdasarkan tingkatan kedetilan dari suatu citra (Citra yang mewakili citra detil dan tidak detil) seperti terlihat pada Gambar 2.

(a) (b)

Gambar 2. (a) Citra Detil
b) Citra tidak Detil

Untuk melihat kinerja dari metode *playfair cipher,* maka program yang dibuat diuji coba dengan cara mengenkripsikan data citra pada gambar 1 dan gambar 2 menggunakan 2 buah kunci yang dibangkitkan secara acak seperti terlihat pada Tabel 1 dan Tabel 2.

Tabel 1. Matrik Kunci *Playfair* ke-1 yang dibangkitkan secara acak

95	247	158	171	116	214	210	138	23	75	154	46	187	140	39	236
51	2	176	102	97	231	241	121	4	209	14	178	37	16	185	8
56	160	131	147	73	228	74	254	17	249	245	144	243	81	68	15
85	103	222	65	151	133	33	0	83	92	240	111	239	127	248	184
165	220	7	93	24	1	208	6	108	173	143	38	157	161	45	104
180	110	53	227	226	246	197	94	27	130	54	107	212	36	82	20
237	42	99	124	207	203	244	218	252	64	123	10	57	255	66	58
134	211	61	141	55	170	79	120	129	49	70	60	32	105	162	193
50	30	221	106	202	101	86	148	250	119	205	77	253	47	126	215
88	189	200	142	52	71	188	13	48	223	206	168	251	113	135	40
80	213	11	21	183	9	179	132	128	22	139	67	241	137	224	98
217	100	182	114	44	34	232	159	3	28	169	96	199	166	153	230
194	216	163	125	195	59	229	26	152	219	118	5	175	112	25	198
78	172	90	191	181	190	117	18	109	204	201	19	76	192	238	233
72	87	149	196	155	186	234	31	225	174	12	235	35	69	62	122
63	177	136	43	89	145	150	115	167	41	164	84	29	156	91	146

Tabel 2. Matrik Kunci *Playfair* ke-2 yang dibangkitkan secara acak

211	180	87	102	137	48	111	104	52	75	65	80	140	212	76	224
193	83	66	187	79	231	177	68	156	44	38	175	55	195	17	61
90	155	105	157	110	106	183	67	7	164	199	121	215	62	94	246
120	136	13	159	170	194	172	251	131	209	100	123	185	148	56	57
254	99	63	12	141	163	54	89	15	165	249	126	250	173	130	23
115	196	241	118	125	186	233	114	154	31	206	24	70	9	116	26
239	36	138	147	64	166	1	2	25	198	190	3	98	112	213	200
219	182	152	192	40	32	208	6	230	210	252	144	242	95	228	171
168	132	229	101	153	247	222	234	34	108	235	226	97	216	14	69
128	42	150	149	20	11	218	51	237	82	240	220	117	202	179	176
201	243	232	35	143	107	160	58	184	22	50	178	37	134	146	41
59	30	253	5	122	27	145	205	158	135	72	203	204	46	127	0
236	19	161	225	92	174	139	167	45	189	129	53	191	71	113	223
4	10	133	227	86	181	188	255	244	124	103	78	73	49	33	43
81	21	93	28	214	169	151	74	245	119	84	197	85	96	142	88
207	91	47	248	39	60	18	77	238	217	162	29	221	8	16	109

PEMBAHASAN

Proses enkripsi citra dengan sandi *playfair*, dilakukan dengan cara sebagai berikut :

1) Lakukan proses transformasi warna sehingga nilai RGB tiap piksel terpisah menjadi komponen *Red*, *Green* dan *Blue* (untuk citra warna). Tetapi untuk citra *grayscale* tidak perlu dilakukan proses transformasi warna.
2) Kemudian untuk citra warna, masing-masing komponen warna (*Red, Green, Blue*) dibagi menjadi blok plainteks yang terdiri dari 2 piksel untuk setiap baris pada

setiap komponen warna. Misal untuk komponen Red didapat matrik citra pada baris 1 s.d 256 dan kolom 1 s.d 256 seperti *terlihat pada gambar 3*.

Komponen Red =

139	175	167	159	…	145
158	191	186	188	…	130
156	190	185	185	…	135
…	…	…	…	…	...
111	135	128	117	..	185

Gambar 3. Potongan matrik untuk komponen warna Red hasil digitalisasi citra

Maka blok plainteks ke-1 diambil dari komponen citra pada baris 1 kolom 1 dan 2 yaitu :

139	**175**

Blok plainteks ke-2 diambil dari komponen citra pada baris 1 kolom 3 dan 4 yaitu

167	**159**

Dan seterusnya sampai dengan baris ke 256.

3) Pilih matrik kunci berukuran 16 x 16 dengan elemen nilainya antara 0 sampai dengan 255 dengan posisi acak.

4) Menggantikan tiap blok plainteks dengan nilai pixel pada matrik kunci dengan menggunakan aturan yang telah dijelaskan di atas.
Misal kunci yang digunakan seperti terlihat pada tabel 1 dan blok plainteks yang digunakan adalah blok plainteks ke-1 yaitu **139** dan **175**. Pada tabel 1 terlihat bahwa posisi nilai **139** dan **175** berbeda baris dan kolom seperti terlihat pada Gambar 4, sehingga cipherteks menggunakan aturan ke-3. Dari Gambar 4, maka didapat : untuk plainteks **139** digantikan dengan nilai **241,** dan plainteks **175** digantikan dengan nilai **118**.

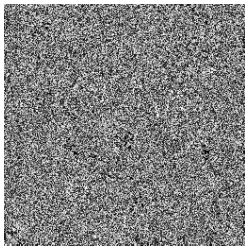
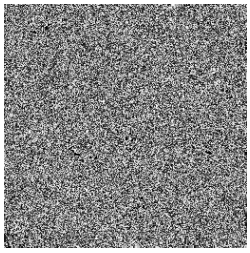
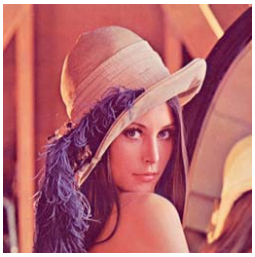
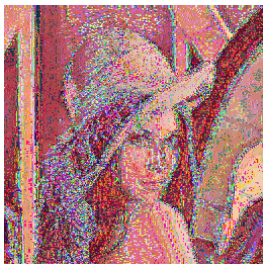
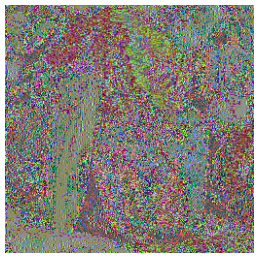
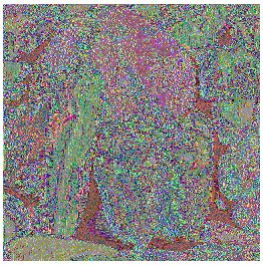
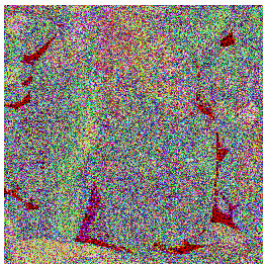
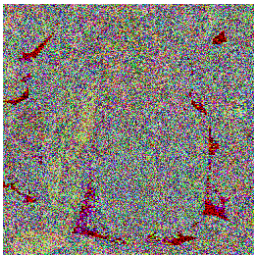
80	213	11	21	183	9	179	132	128	22	***139***	67	**241**	137	224	98
217	100	182	114	44	34	232	159	3	28	169	96	199	166	153	230
194	216	163	125	195	59	229	26	152	219	**118**	5	***175***	112	25	198

Gambar 3. Potongan matrik kunci pada tabel 1.

Langkah tersebut dilakukan pada semua blok plainteks untuk semua komponen warna.

Untuk langkah dekripsi dilakukan dengan langkah yang sama dengan proses enkripsi.

Dari hasil pengujian citra pada Gambar 1 dan Gambar 2 menggunakan metode *playfair cipher* yang dibangun menggunakan MATLAB 7, didapat hasil citra yang telah tersandikan seperti terlihat pada Gambar 5. .

NAMA CITRA	CITRA PENGUJIAN	KUNCI PLAYFAIR KE-1	KUNCI PLAYFAIR KE-2
Citra 1			
Citra 2			
Citra 3			
Citra 4			

Gambar 5. Citra tersandikan menggunakan metode *playfair cipher*

Dari gambar 5 terlihat bahwa untuk citra 2 yang termasuk citra tidak detil atau citra 3 dengan kualitas yang tidak baik terlihat hasilnya tidak sebaik pada citra 1 dan citra 4. Hal ini menunjukkan bahwa metode ini sangat baik apabila diimpelentasikan pada citra dengan kualitas yang baik dan pada citra dengan kategori citra detil seperti pada citra 1 dan citra 4 Hal ini menunjukkan bahwa algoritma ini cukup baik untuk menyandikan citra.

Namun metode ini mempunyai kelemahan yaitu disebabkan karena frekuensi kemunculan bigram pada cipher teks akan bersesuaian dengan frekuensi kemunculan di plainteks. Sehingga kriptanalisis dapat melakukan terkaan atas isi bujur sangkar. Bigram yang berkebalikan dengan menggunakan *playfair cipher* ini yang akan dimanfaatkan oleh kripanalisis untuk menghasilkan pola karakter yang sama. Dengan melakukan identifikasi jarak antar bigram yang berkebalikan pada cipherteks dan menyesuaikan pola dengan data plainteks yang sering muncul dan menggandung pola tersebut dapat dengan mudah untuk membangkitkan kemungkinan data plainteks yang mungkin dibangun untuk menjadi kunci. Terutama pada implementasi citra yang yang berukuran besar, sehingga

frekuensi kemunculan bigram pada cipher teks yang bersesuaian dengan frekuensi kemunculan di plainteks cukup tinggi. Meskipun implementasi metode penyandian ini pada citra, cukup menyulitkan kriptanalisis karena kriptanalis membutuhkan waktu proses yang cukup lama karena proses pencarian kunci sebesar 256! kemungkinan.

KESIMPULAN

Berdasarkan hasil penelitian, pelaksanaan eksperimen serta analisis dan pembahasan dapat diambil suatu kesimpulan bahwa penggunaan metode playfair cipher pada penyandian citra cukup baik karena kunci matrik yang digunakan ukurannya cukup besar yang otomatis kemungkinan matrik kunci tertebak juga cukup besar yaitu 256! kemungkinan.

Metode ini juga mempunyai kelemahan yaitu disebabkan karena frekuensi kemunculan bigram pada cipher teks akan bersesuaian dengan frekuensi kemunculan di plainteks. Sehingga kriptanalisis dapat melakukan terkaan atas isi bujur sangkar dengan mudah terutama pada implementasi citra yang yang berukuran besar. Karena citra dengan ukuran besar frekuensi kemunculan bigram pada cipher teks yang bersesuaian dengan frekuensi kemunculan di plainteks cukup tinggi.

Untuk mengatasi penggunaan cipher tunggal yang secara komparatif lemah, maka dapat dikembangkan penelitian menggunakan metode super enkripsi (gabungan algoritma penyandian) agar menghasilkan penyandian citra yang cukup baik dibandingkan dengan penggunaan cipher tunggal.

DAFTAR PUSTAKA

Munir, Rinaldi, 2006, *Kriptografi,* Informatika, Bandung.

Schneier, Bruce 1996, *Aplied Cryptography 2nd* , John Wiley & Sons, New York

Siang, J.J., 2002, “Implementasi Sand Hill untuk Penyandian Citra”, *Jurnal Informatika* Vol.3., No.1, Mei.

Soplanit, Susani, 2005, “Digital Audio Encryption Using New Chaotic Substitution Image Encryption (NCSIE)”, *Prosiding SNTI 2005*, ISSN: 1829-9156, volume 2, nomor 1.

Stinson, R Douglas, 1995, *Cryptography Theory and Practice*, CRC Press, Inc, Boca Raton, London