Penyandian File Gambar dengan Metode Substitusi dan Transposisi

Aji Supriyanto dan Eka Ardhianto
Fakultas Teknologi Informasi, Universitas Stikubank Semarang
email : ajisup@gmail.com; e_ardianto@yahoo.com

Abstract : *Cryptography is a science which studying about safety of messages, so it makes the messages cannot be read by unauthorized persons. Cryptography have two kinds of algorithm first is encryption algorithm, that is algorithm altering plaintext become the ciphertext, and the second is decryption algorithm that is algorithm altering ciphertext become the plaintext, that conducive of message can only be made and read by authorized persons. Plaintext represent the message able to be read, while ciphertext is message which have pass by the encryption process, so that order the ciphertext difficult to be translated or read. And method of substitution and transpotition method are some of conventional technique able to be used to protect the pictures files, so that produce the pictures files which do not easy to to be read. The conventional technique basically use a same key to do the encryption and decryption process.*

Keyword : *Picture file, Cryptography, Encryption, Decryption, Substitution, Transpotition*

PENDAHULUAN

Setiap orang yang berkeinginan menyimpan sesuatu secara pribadi, akam melakukan segalacara untuk menyembunyikannya sehingga orang lain tidak tahu. Contoh sederhana, ketika kita akan mengirim surat kepada seseorang, maka kita akan membungkus surat tersebut dengan amplop agar tidak terbaca oleh orang lain. Untuk menambah kerahasiaan dari surat tersebut agar tetap tidak terbaca oleh orang lain dengan mudah apabila amplop dibuka, maka kita mengupayakan sebuah mekanisme tertentu agar isi surat tidak mudah untuk dipahami.

Masalah kerahasiaan ini sudah ada sebelum lahirnya komputer. Julius Caesar, khawatir pesan yang ditujukan kepada para jendralnya jatuh ke tangan musuh, maka ia menggunakan metode enkripsi sederhana dengan menggeser huruf pada abjad dengan nilai tertentu.

PENYANDIAN FILE GAMBAR

Kata penyandian file gambar terdiri dari tiga buah kata yaitu yang pertama adalah penyandian [1], mempunyai kata dasar ‘sandi’ yang menurut Kamus Besar Bahasa Indonesia berarti kode, dan penyandian adalah sebuah bentuk kata kerja yang berarti suatu kegiatan menyandikan atau mengkodekan dengan tujuan tertentu. Kata yang kedua adalah ‘*file*’ yaitu sebutan sekumpulan *byte* atau deretan karakter atau kode-kode yang membentuk sebuah dokumen yang memiliki nama yang unik [1], dan ketiga adalah kata gambar yang menurut Kamus Besar Bahasa Indonesia adalah ‘citra’ [2], citra adalah objek yang elemen-elemennya dinyatakan dengan suatu besaran numerik yang membentuk array. Elemen gambar atau *picture elements* sering disebut dengan kata ‘*pixel*’ yang berarti titik-titik yang membentuk sebuah citra.

Jadi penyandian file gambar dapat diartikan sebagai suatu kegiatan menyandikan atau mengkodekan sekumpulan elemen penyusun gambar (*pixel*) dengan tujuan mengamankan informasi dari pihak yang tidak berhak.

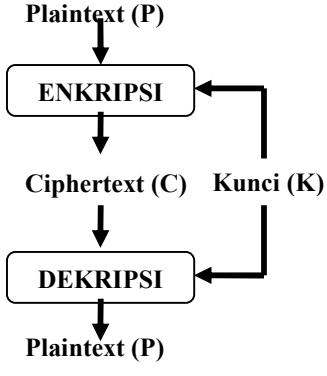
KRIPTOGRAFI

Penyandian merupakan salah satu alternatif atau cara untuk mengamankan dan menjaga kerahasiaan pesan. Seni dan ilmu untuk menyandikan atau menjaga keamanan serta kerahasiaan pesan disebut kriptografi [1], atau kriptografi adalah ilmu yang mempelajari

teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti keabsahan, integritas data serta autentikasi data tersebut [1], dengan kata lain kriptografi digunakan untuk menjamin keleluasaan pribadi dan pembuktian keaslian pesan dalam berkomunikasi.

Pada dasarnya, kriptografi memiliki dua algoritma yaitu enkripsi dan dekripsi. Pesan yang dapat dibaca disebut sebagai *plaintext*, sedangkan teknik untuk membuat pesan tidak dapat terbaca disebut *enkripsi*. Pesan yang sudah melewati tahap enkripsi disebut *ciphertext*. Dan *dekripsi* adalah teknik untuk merubah *ciphertext* menjadi *plaintext* [1], dan kunci *key* adalah kode yang digunakan untuk melakukan peng-enkripsi-an atau pen-dekripsi-an suatu *text* [1]. Untuk selanjutnya *pixel* disebut sebagai objek *plaintext*.

Dalam menyandikan pesan atau mengenkripsi pesan, terdapat dua jenis algoritma berdasar kuncinya, yaitu Algoritma Simetri (Konvensional) dan Algoritma Asimetri (Kunci-Publik). Algoritma Simetri disebut juga sebagai algoritma konvensional yaitu algoritma yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya [2]. Algoritma simetri sering juga disebut sebagai algoritma satu kunci, algoritma kunci tunggal. Algoritma jenis ini mengharuskan pengirim dan penerima menyetujui satu kunci tertentu sebelum mereka berkomunikasi dengan aman. Keamanan algoritma ini hanya tergantung pada kunci, membocorkan kunci berarti *chaos*.



Gambar 1. Kriptografi Konvensional

TEKNIK ENKRIPSI KONVENSIONAL

Teknik enkripsi konvensional memiliki dua buah teknik dasar yaitu teknik substitusi dan teknik transposisi.

Aplikasi yang dibuat, nantinya akan menggunakan gabungan dari kedua teknik enkripsi konvensional tersebut yaitu, teknik substitusi dan teknik transposisi. Penggabungan dua teknik tersebut akan menghasilkan bentuk gambar *ciphertext* yang memiliki susunan *pixel* yang lebih rumit dibanding dengan hanya menggunakan satu teknik enkripsi saja.

ENKRIPSI TEKNIK SUBSTITUSI

Substitusi adalah penggantian setiap karakter *plaintext* dengan karakter lain [2]. Dengan kata lain teknik substitusi adalah salah satu teknik enkripsi simetris yang mana dilakukan penggantian setiap objek *plaintext* dengan objek lain, teknik ini menerapkan konsep korenspondensi satu-satu untuk tiap objek *plaintext* yang disandikan.

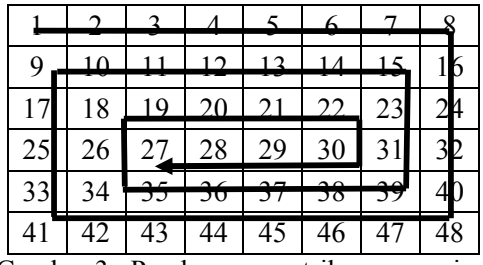
Objek yang akan disubstitusikan dalam pembuatan skripsi ini adalah *pixel.* Adapun langkah-langkahnya dapat diilustrasikan sebagai berikut:

1. Nilai *pixel-pixel* dari gambar dimasukkan kedalam sebuah matrik dengan ordo sama dengan ukuran gambar (gambar 2).
2. Dari matrik gambar 2 dilakukan pembacaan secara spiral dimulai dari sudut kiri atas ke arah kanan, ke bawah, ke kiri, ke atas hingga berakhir di pusat matrik sehingga menghasilkan gambar 3. Penggunaan metode pembacaan spiral merupakan penggabungan dua metode pembacaan secara horisontal dan vertikal, dan penggunaan metode pembacaan secara spiral akan menghasilkan bentuk untaian *pixel* gambar yang lebih rumit dibaca daripada menggunakan metode pembacaan secara horisontal ataupun vertikal saja..
3. Dari hasil pembacaan matrik gambar 3 dihasilkan sebuah untaian *pixel* seperti pada gambar 4.
4. Dari untaian gambar 4, dilakukan proses substitusi posisi *pixel* secara urut dengan konsep korespondensi satu-satu. Posisi *pixel* pertama digantikan dengan posisi pixel terakhir, sehingga didapat hasil untaian baru seperti pada gambar 5.

Berikut ini adalah gambar penjelasan proses enkripsi teknik substitusi (Gambar 2-5).

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

Gambar 2. Matrik susunan *pixel* gambar



Gambar 3. Pembacaan matrik secara spiral

1	2	3	4	5	6	7	8
							16
44	45	46	47	48	40	32	24
43							
42	41	33	25	17	9	10	11
							12
37	38	39	31	23	15	14	13
36							
35	34	26	18	19	20	21	22
							30
					27	28	29

Gambar 4. Susunan untaian *pixel* hasil pembacaan spiral.

27	28	29	30	22	21	20	19
							18
31	39	38	37	36	35	34	26
23							
15	14	13	12	11	10	9	17
							25
47	46	45	44	43	42	41	33
48							
40	32	24	16	8	7	6	5
							4
					1	2	3

Gambar 5. Susunan untaian pixel setelah dilakukan substitusi.

ENKRIPSI TEKNIK TRANSPOSISI

Teknik transposisi adalah pada dasarnya membuat *ciphertext* dengan menggantikan posisi objek-objek *plaintext* tanpa menggantikan objek *plaintext* tersebut, jadi pada proses transposisi tidak diperlukan karakter lain. Pada teknik transposisi ini pembacaan matrik dilakukan dengan cara pembacaan kolom per kolom sesuai dengan kunci yang digunakan. Adapun langkah-langkahnya dapat diilustrasikan seperti berikut :

1. Susunan *pixel* hasil substitusi (gambar 6) merupakan *plaintext* pada proses transposisi.
2. Untai dari matrik *plaintext* (gambar 6) tersebut dimasukkan ke dalam matrik dengan ordo n dikali x, dengan n adalah panjang kunci yang digunakan dan x adalah jumlah *pixel* dibagi panjang kunci. Ilustrasinya terdapat pada gambar 7.
3. Dari matrik gambar 7, dilakukan pembuatan untaian *ciphertext* dengan pembacaan kolom per kolom sesuai dengan urutan abjad kunci yang telah diurutkan. Ilustrasinya pada gambar 8.
4. Kemudian matrik gambar 8 dilakukan pembacaan kolom dimulai dari huruf "A" pada urutan ke-1, huruf "D" pada urutan ke-2 dan seterusnya hingga huruf "W" pada urutan terakhir. Maka didapatkan bentuk untai seperti pada gambar 9.
5. Nilai *pixel* yang didapat dari untaian transposisi (gambar 9) kemudian dimasukkan kembali ke dalam matrik baru sesuai dengan ordo ukuran gambar. Bentuk hasil akhirnya adalah pada gambar 10.

Berikut ini adalah gambar penjelasan proses enkripsi teknik transposisi (Gambar 6-10)

27	28	29	30	22	21	20	19
							18
31	39	38	37	36	35	34	26
23							
15	14	13	12	11	10	9	17
							25
47	46	45	44	43	42	41	33
48							
40	32	24	16	8	7	6	5
							4
					1	2	3

Gambar 6. Hasil substitusi dijadikan sebagai *plaintext* proses transposisi.

P	A	S	S	W	O	R	D	→ kunci
27	28	29	30	22	21	20	19	
18	26	34	35	36	37	38	39	
31	23	15	14	13	12	11	10	
9	17	25	33	41	42	43	44	
45	46	47	48	40	32	24	16	
8	7	6	5	4	3	2	1	

Gambar 7. Matrik susunan awal proses transposisi

P	A	S	S	W	O	R	D	→
4	1	6	7	8	3	5	2	→ urutan
27	28	29	30	22	21	20	19	
18	26	34	35	36	37	38	39	
31	23	15	14	13	12	11	10	
9	17	25	33	41	42	43	44	
45	46	47	48	40	32	24	16	
8	7	6	5	4	3	2	1	

↓ Aturan pembacaan secara kolom

Gambar 8. Aturan pembacaan matrik transposisi

28	26	23	17	46	7	19	39
							10
32	42	12	37	21	1	16	44
3							
27	18	31	9	45	8	20	38
							11
47	25	15	34	29	2	24	43
6							
30	35	14	33	48	5	22	36
							13
					4	40	41

Gambar 9. Untaian hasil pembacaan secara kolom

28	26	23	17	46	7	19	39
10	44	16	1	21	37	12	42
32	3	27	18	31	9	45	8
20	38	11	43	24	2	29	34
15	25	47	6	30	35	14	33
48	5	22	36	13	41	40	4

Gambar 10. Matrik hasil proses transposisi

DEKRIPSI TEKNIK TRANSPOSISI

Pada proses ini adalah menunjukan proses pengambalian posisi *pixel* gambar hasil proses enkripsi. Berikut adalah langkah-langkah proses transposisi dapat diilustrasikan sebagai berikut:

1. Nilai *pixel-pixel* dari gambar enkripsi dimasukkan kedalam sebuah matrik dengan ordo sama dengan ukuran gambar (gambar11).
2. Dari matrik gambar 11, dilakukan pembacaan secara baris per baris dimulai dari baris paling awal hingga akhir. Pembacaan dimulai dari kiri ke kanan baris seperti pada gambar 12.
3. Dari pembacaan yang dilakukan pada gambar 12, maka akan menghasilkan sebuah untai seperti gambar 13.
4. Dari untai Gambar 13, kemudian *pixel* dimasukkan kedalam matrik berordo (n x m) dengan n adalah panjang kunci dan m adalah hasil bagi jumlah *pixel* dengan panjang kunci. Pengisian matrik dilakukan secara kolom, sesuai dengan urutan abjad kunci yang digunakan. Dimulai dari huruf "A" adalah urutan kunci yang pertama dan terdapat pada kolom ke-2, sehingga pengisian matrik dilakukan pada kolom ke-2, huruf "D" adalah urutan kunci yang ke-2 dan terdapat pada kolom ke-8, sehingga pengisian dilakukan pada kolom ke-8, dan seterusnya hingga urutan akhir kunci (gambar 14).
5. Nilai *pixel* gambar 14 dilakukan pembacaan secara baris per baris dari kiri ke kanan, sehingga menghasilkan untai seperti pada gambar 15.

Berikut ini adalah gambar penjelasan proses dekripsi teknik transposisi (Gambar 11-15).

28	26	23	17	46	7	19	39
10	44	16	1	21	37	12	42
32	3	27	18	31	9	45	8
20	38	11	43	24	2	29	34
15	25	47	6	30	35	14	33
48	5	22	36	13	41	40	4

Gambar 11. Matrik awal proses dekripsi

28	26	23	17	46	7	19	39
10	44	16	1	21	37	12	42
32	3	27	18	31	9	45	8
20	38	11	43	24	2	29	34
15	25	47	6	30	35	14	33
48	5	22	36	13	41	40	4

Gambar 12. Aturan pembacaan matrik awal dekripsi

28	26	23	17	46	7	19	39
							10
32	42	12	37	21	1	16	44
3							
27	18	31	9	45	8	20	38
							11
47	25	15	34	29	2	24	43
6							
30	35	14	33	48	5	22	36
							13
					4	40	41

Gambar 13. Untai hasil pembacaan secara baris

P	A	S	S	W	O	R	D	kunci
4	1	6	7	8	3	5	2	
								urutan
27	28	29	30	22	21	20	19	
18	26	34	35	36	37	38	39	Aturan memasukkan secara kolom
31	23	15	14	13	12	11	10	
9	17	25	33	41	42	43	44	
45	46	47	48	40	32	24	16	
8	7	6	5	4	3	2	1	

Gambar 14. Matrik transposisi pada proses dekripsi

27	28	29	30	22	21	20	19
							18
31	39	38	37	36	35	34	26
23							
15	14	13	12	11	10	9	17
							25
47	46	45	44	43	42	41	33
48							
40	32	24	16	8	7	6	5
							4
					1	2	3

Gambar 15. Untai hasil pembcaan matrik transposisi

DEKRIPSI TEKNIK SUBSTITUSI

Berikut adalah langkah-langkah proses substitusi dapat diilustrasikan sebagai berikut:

1. Input yang digunakan untai hasil dekripsi transposisi (gambar 16).
2. Dari untaian gambar 16, dilakukan proses substitusi posisi *pixel* secara urut dengan konsep korespondensi satu-satu. Posisi *pixel* pertama digantikan dengan posisi pixel terakhir, sehingga didapat hasil untaian baru seperti pada gambar 17.
3. Gambar 17 kemudian dimasukkan kedalam matrik berordo sama dengan ukuran gambar semula. Cara menempatkan *pixel* adalah secara spiral dimulai dari kiri atas kekanan, kebawah, kekiri, keatas dan seterusnya hingga berakhir dipusat matrik. Ilustrasinya pada Gambar 18.
4. Hasil akhir Gambar 18 adalah Gambar 19 dengan posisi *pixel* seperti semula.

Berikut ini adalah gambar penjelasan proses dekripsi teknik substitusi (Gambar 16-19).

27	28	29	30	22	21	20	19
							18
31	39	38	37	36	35	34	26
23							
15	14	13	12	11	10	9	17
							25
47	46	45	44	43	42	41	33
48							
40	32	24	16	8	7	6	5
							4
					1	2	3

Gambar 16. Untai hasil pembacaan matrik transposisi sebagai input proses substitusi.

1	2	3	4	5	6	7	8
							16
44	45	46	47	48	40	32	24
43							
42	41	33	25	17	9	10	11
							12
37	38	39	31	23	15	14	13
36							
35	34	26	18	19	20	21	22
							30
					27	28	29

Gambar 17. Untai hasil proses substitusi

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

Gambar 18. Aturan penempatan elemen untai

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

Gambar 19. Matrik hasil proses dekripsi

ATURAN PENGGUNAAN KUNCI

Kunci yang digunakan adalah berupa untaian atau deretan karakter ASCII dapat berupa untaian huruf kecil ‘a’-‘z’, huruf besar ‘A’-‘Z’, angka ‘0’-‘9’, tanda baca, karakter khusus dan operator aritmatika (+; -; *, /). Setiap karakter ASCII memiliki panjang 8 bit. Panjang kunci yang digunakan adalah 8 karakter ASCII atau sepanjang 64 bit.

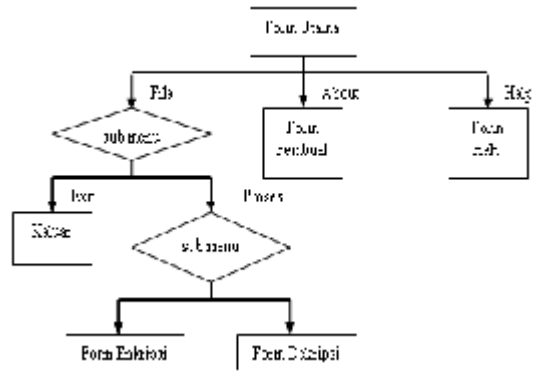
METODE PENELITIAN

Jenis Data, Pengembangan Sistem dan Perangkat yang Digunakan

Jenis data yang digunakan adalah jenis data sekunder yaitu data yang diperoleh dalam bentuk informasi, baik dari media cetak maupun media elektronik yang masih berkaitan dengan tema skripsi. Untuk metode pengembangan sistem yang digunakan adalah sistem *prototype*, yang mana terdapat tahapan-tahapan yang dilalui, yaitu *Requirement Gathering*, *Quick Design*, *Building Prototyping* dan *Evaluation.* Sedangkan perangkat yang digunakan untuk menyelesaikan masalah adalah *Pseudocode* yaitu ungkapan penulisan algoritma yang lebih mendekati dengan penggunaan bahasa pemrograman yang digunakan untuk menyelesaikan permasalahan yang dihadapi.

Rancangan Alur Aplikasi

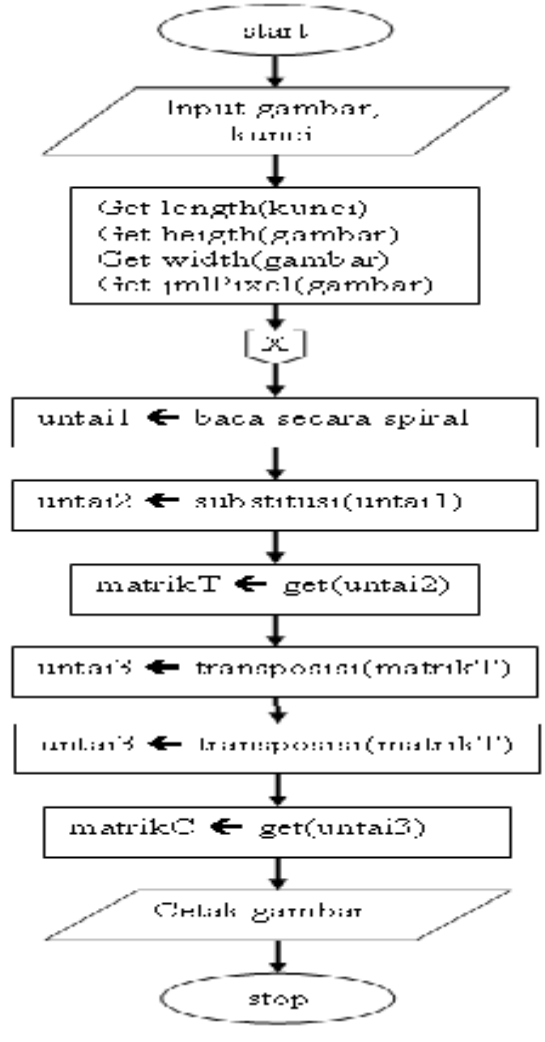
Secara keseluruhan rencana alur aplikasi dapat digambarkan sebagai berikut :



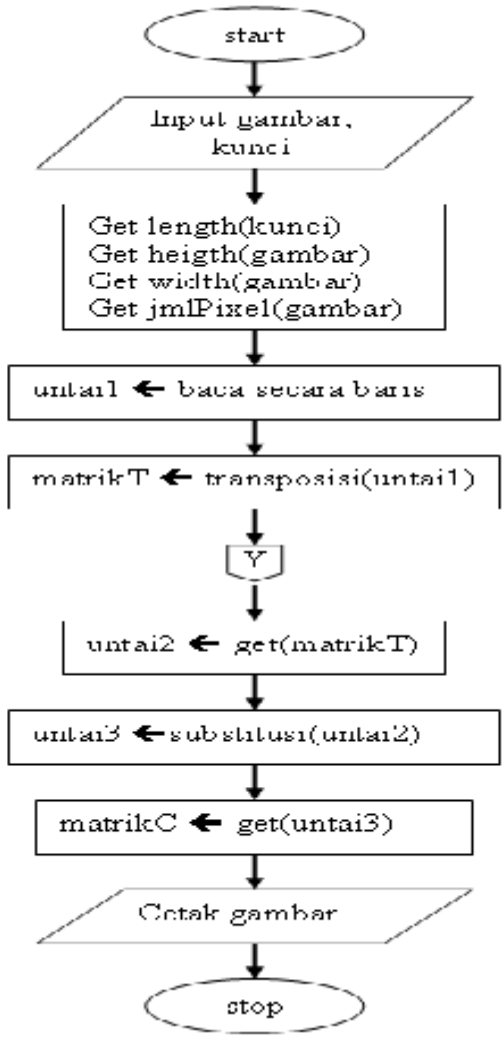
Gambar 20. Alur Aplikasi

Rancangan Algoritma

Flowchart rancangan proses enkripsi dan dekripsi adalah seperti pada gambar 21 dan gambar 22.



Gambar 21. Flowchart Proses Enkripsi



Gambar 22. Flowchart Proses Dekripsi

Dari flowchart gambar 21 dapat dijelaskan mengenai alur program seperti berikut :

1. Sebagai inputan diperlukan sebuah nilai kunci dan gambar.
2. Sebelum dilakukan proses penyandian, akan di dapat panjang kunci, tinggi dan lebar gambar serta jumlah pixel gambar.
3. Proses pertama adalah pembacaan secara spiral dari gambar yang akan disandikan hingga terbentuk sebuah untai.
4. Kemudian dilanjutkan dengan proses substitusi dari untai yang didapat.
5. Selanjutnya dari untai hasil substitusi di masukkan kedalam matrikT untuk proses transposisi.
6. Proses pembacaan pada matrikT dilakukan secara kolom per kolom sesuai dengan urutan abjad kunci yang digunakan hingga terbentuk sebuah untai baru.
7. Dari untai yang didapat, kemudian dimasukkan kedalam matrik berukuran sama dengan ukuran gambar, sehingga didapat hasil akhir dari proses penyandian gambar.

Dan dari flowchart gambar 22 dapat dijelaskan mengenai alur program seperti berikut:

1. Sebagai inputan diperlukan sebuah nilai kunci dan gambar yang telah di-enkrip.
2. Sebelum dilakukan proses penyandian, akan di dapat panjang kunci, tinggi dan lebar gambar serta jumlah pixel gambar.
3. Proses pertama adalah pembacaan secara baris dari gambar yang akan diterjemahkan hingga terbentuk sebuah untai.
4. Kemudian dilanjutkan dengan memasukkan hasil pembacaan ke dalam matrikT secara kolom menurut abjad urutan abjad kunci yang digunakan untuk proses transposisi.
5. Selanjutnya dilakukan pembacaan secara baris per baris dari matrikT.
6. Proses selanjutnya adalah mensubstitusikan untai yang didapat dari hasil pemabacaan pada matrikT.
7. Dari hasil substitusi, maka didapatkan sebuah untai yang kemudian digambarkan secara baris per baris kedalam matrikC yang berukuran sama dengan gambar.

IMPLEMENTASI APLIKASI

1. Form Utama

Form utama (gambar 23) memiliki tiga buah menu *pull-down* yaitu File, Tentang dan Help. Menu File berisikan dua sub menu yaitu proses untuk menuju form Enkripsi maupun form Deskripsi dan Exit untuk keluar dari aplikasi. Menu Tentang memiliki sebuah sub menu pembuat untuk menampilkan form Pembuat, dan menu Help akan membuka jendela bantuan penggunaan aplikasi.

2. Form Enkripsi

Form Enkripsi (gambar 24) digunakan untuk melakukan proses peng-enkripsi-an gambar. Dalam form ini terdapat menu File dan Help, dimana dalam menu File terdapat sub-menu lain yaitu sub-menu Buka untuk mengambil gambar, sub-menu Simpan untuk menyimpan gambar hasil proses dan sub-menu Selesai untuk menutup form.

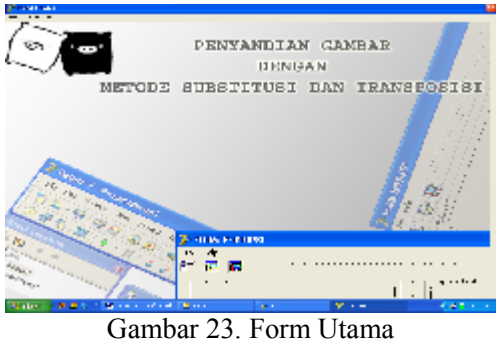
3. Form Dekripsi

Form dekripsi (gambar 25) digunakan untuk melakukan proses pen-dekripsi-an gambar. Dalam form ini terdapat menu File dan Help, dimana dalam menu File terdapat sub-menu lain yaitu sub-menu Buka untuk mengambil gambar, sub-menu Simpan untuk menyimpan gambar hasil proses dan sub-menu Selesai untuk menutup form.

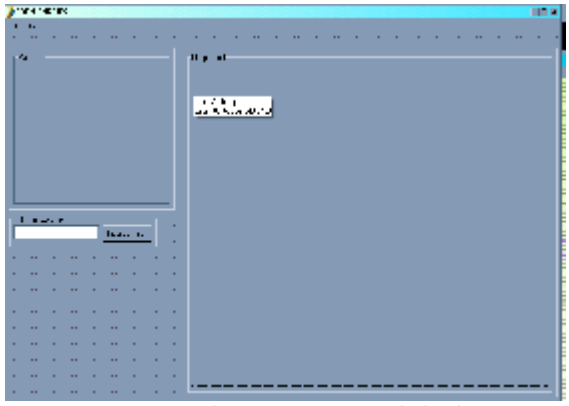
4. Form Help

Form help (gambar 26) ini berfungsi untuk memberikan penjelasan singkat mengenai cara penggunaan aplikasi termasuk cara pengenkripsian dan pendekripsian gambar.

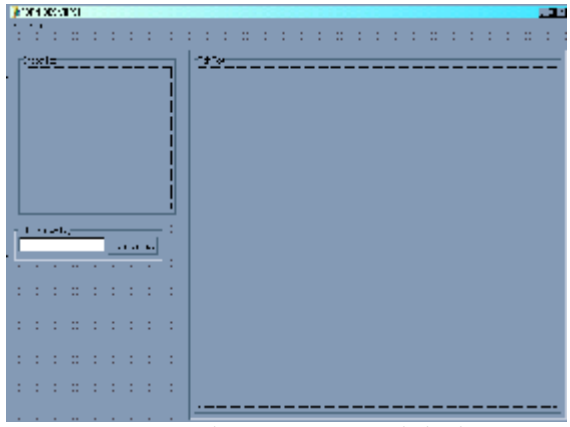
Berikut adalah Gambar dari aplikasi yang dibuat.



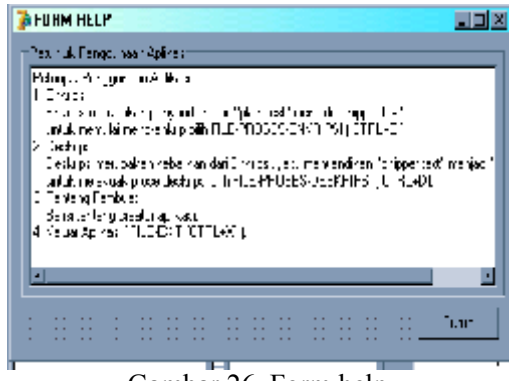
Gambar 23. Form Utama



Gambar 24. Form Enkripsi



Gambar 25. Form Dekripsi



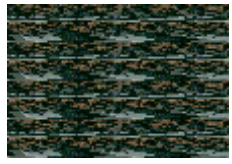
Gambar 26. Form help

ANALISA HASIL

1. Pengujian I

Pada proses peng-enkripsi-an, diperlukan gambar *plaintext* digunakan sebagai *input*, dan menghasilkan *out-put* berupa gambar *ciphertext*. Sedangkan pada proses pen-deskripsi-an, gambar *ciphertext* sebagai *input* dan sebagai *out-put* adalah gambar plaintext.

Setelah dilakukan proses enkripsi, gambar *ciphertext* yang sudah tidak dapat dikenali rupa aslinya, dan untuk mengenalinya kembali maka gambar *ciphertext* dikenakan proses deskripsi hingga menghasilkan gambar semula. Adapun perbedaan antar gambar *plaintext* dan gambar *ciphertext* sebagai *output* proses enkripsi dan *input* proses deskripsi dapat dilihat seperti gambar beriktu ini:

(a) (b)

Gambar 27. Gambar Plaintex (a) dan Gambar Ciphertext (b)

Dari gambar 26 telah dilakukan pengujian terhadap resolusi dan besar file gambar sebelum dan sesudah dilakukan proses enkripsi. Hasil pengujian dapat dilihat dalam tabel 1:

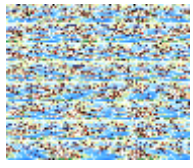
Tabel 1. Tabel pengujian resolusi dan besar file

	Gambar Awal gambar 27 (a)	**Gambar Hasil gambar 27 (b)**
Resolusi (wxh)	640 x 480	640 x 480
Besar File (Mb)	1.17	1.17

2. Pengujian II

Pengujian ini dilakukan pada proses enkripsi dengan gambar yang bersifat homogen dan heterogen. Pembandingan yang dilakukan adalah tingkat keamanan proses enkripsi proses enkripsi pada gambar. Adapun hasil dari pengujian yang dilakukan adalah sebagai berikut:


Gambar 28a Pengujian pada gambar homogen

Gambar 28b Pengujian pada gambar heterogen

Dari kedua gambar diatas, dapat dikatakan bahwa pada gambar **28a** yang memiliki warna sedikit (homogen) akan lebih mudah diidentifikasi dibanding dengan gambar **28b** yang memiliki jumlah warna yang lebih banyak (heterogen).

KESIMPULAN

1. Teknik penyandian dengan metode *substitusi* dan *transposisi* yang dilakukan oleh program pada gambar dalam format BMP dapat menghasilkan suatu gambar yang tak dapat dikenali lagi.
2. Teknik penyandian dengan metode subtitusi dan transposisi yang diterapkan dalam mengakses langsung bit-bit dari citra tersebut berhasil memanipulasi posisi dan mengacak susunan *pixel* pada gambar.
3. Gambar yang sudah memiliki susunan *pixel* teracak hasil penyandian dapat dikembalikan lagi oleh program ke dalam bentuk semula hingga dapat dikenali lagi.
4. Ketika pengujian dilakukan dalam membandingkan gambar asli sebelum disandikan (*plaintext*) dengan gambar setelah disandikan (*ciphertext*) dan gambar hasil dari penerjemahan sandi (*plaintext*) tidak terdapat perbedaan dalam ukuran gambar
5. Program aplikasi ini kurang cocok untuk gambar yang bersifat homogen, karena gambar akan lebih mudah diidentifikasi.
6. Program aplikasi ini akan lebih bagus jika dapat mengenali gambar plaintext dan ciphertext serta dapat digunakan untuk gambar dengan format selain BMP.
7. Penggunaan teknik konvensional dan penggunaan panjang kunci yang pendek pada aplikasi ini, akan menghasilkan gambar berpola sehingga mudah untuk dianalisa.

DAFTAR PUSTAKA

1. http://id.wikipedia.org/wiki/Enkripsi.htm
2. http://www.dani.sincat.com/TI/hardware.php
3. http://www.ilmukomputer.com/dasar_kriptografi.htm.
4. Kurniawan Y., MT. Ir, 2004, *Kriptografi Keamanan Internet dan Jaringan*

Komnunikasi, Informatika Bandung: Bandung.

5. Murni A., 2004, *Pengantar Pengolahan Citra*, Elekmedia Komputindo:Jakarata.
6. Robi'in B., 2004, *Pemrograman Grafis Multimedia Menggunakan Delphi,* Andi:Yogyakarta.
7. Wahana Komputer, 2002, *Dunia Komputer*, Penerbit Andi Yogyakarta:Yogyakarta.
8. Wahid F., 2002, *Multimedia Grafis*, Elekmedia Komputindo:Jakarta.