INFO TEKNIK

Volume 14 No. 2 Desember 2013 (103-113)

PENYANDIAN FILE GAMBAR DENGAN METODE SUBSTITUSI DAN TRANSPOSISI SERTA IMPLEMENTASINYA MENGGUNAKAN BAHASA PEMROGRAMAN BORLAND DELPHI 7.0

Dwi Retnosari

Departement Teknik Informatika Universitas Islam Kalimantan, Banjarmasin
E-mail: dwiretnosarisari@yahoo.co.id

ABSTRACT

The study of how a message if safe so we can't be read by unauthorized parties is cryptography. A message or information which is one important thing in communicating that needs to be kept confidential. For that need to be made an application that is able to secure information in general and particular image file. Cryptography has two of the encryption and decryption algorithms that allow massages can only be cre and read be the right. Method of the substitution and transposition is a conventional encryption techniques that can be used to source the information image file. In applications Borland Delphi programming language used to implement algorithms for encryption and decryption of substitution and transposition, resulting in the form of image files that cant not be read other without the decryption process first.

Keywords: Cryptography, Image File, Encryption, Decryption, Substitution,Transposition.

1. Pendahuluan

Saat ini, kemajuan teknologi informasi sedang berkembang dengan pesat yang memungkinkan semua orang dapat berkomunikasi dari satu tempat ke tempat lain yang berjarak ribuan kilometer dengan berbagai media dan berbagai macam bentuk data. Data yang dikirim itu menggunakan jalur transmisi telekomunikasi yang belum tentu terjamin keamanannya. Dengan demikian setiap orang yang bermaksud menyimpan sesuatu secara pribadi dan rahasia akan melakukan segala cara untuk menyembunyikannya sehingga orang lain tidak tahu.

Dengan internet orang bisa *browsing, download, chatting, facebook,* dan sebagainya. Tidak menutup kemungkinan orang akan meng-*upload* ataupun men-*download* gambar dan menyimpannya secara rahasia agar tidak diketahui orang lain. Contoh yang sederhana, ketika mengirim surat kepada seseorang akan membungkus surat tersebut dengan amplop agar tidak terbaca oleh orang lain. Untuk menambah kerahasiaan surat tersebut agar tetap tidak terbaca orang lain dengan mudah apabila amplop dibuka, sehingga diperlukan suatu mekanisme untuk membuat isi surat tidak mudah dipahami.

Untuk mengatasi masalah tersebut diperlukan metode penyandian data yang dikenal dengan ilmu kriptografi, adalah ilmu yang mempelajari bagaimana supaya pesan atau dokumen itu aman, tidak bisa dibaca oleh pihak yang tidak berhak *(anauthorized persons)*. Masalah kerahasiaan ini memang sudah ada jauh sebelum adanya komputer. Julius Caesar, yang khawatir jangan sampai pesan untuk para jenderalnya jatuh ke tangan musuh, sehingga ia menggunakan metode enkripsi sederhana dengan menggeser huruf abjad dengan nilai tertentu. Munir,2006.[4] Algoritma kriptografi selalu terdiri dari dua macam

yaitu enkripsi dan dekripsi. Teknik untuk menyandikan *plaintext* menjadi *ciphertext* disebut enkripsi, sedangkan proses mengembalikan *ciphertext* menjadi *plaintext* seperti semula dinamakan dekripsi. Metode enkripsi substitusi dan metode enkripsi transposisi merupakan salah satu teknik enkripsi konvensional (simetri) yang digunakan orang sejak berabad-abad lalu untuk mengamankan pesan yang dikirimkan kepada orang lain. Munir,2006.[4]

Sehubungan dengan latar belakang diperlukan pengamanan file untuk di simpan sendiri atau untuk dikirimkan ke pihak lain yang tidak sekedar proteksi *disk* atau pengamanan secara *hardware* saja namun diperlukan salah satu teknik lain untuk pengamanan file. Sehingga penulis bermaksud membahas pembuatan suatu aplikasi yang mampu mengacak posisi piksel pada gambar dengan bahasa pemrograman Borland Delphi 7.0.

2. Tinjauan Pustaka

2.1. Citra Digital

Sebuah citra digital adalah kumpulan piksel-piksel yang disusun dalam larik dua dimensi yang dapat diobservasi oleh sistem visual manusia. Ditinjau dari sudut pandangan matematis, citra merupakan fungsi menerus *(continue)* dari intensitas cahaya pada bidang dwimitra. Sumber cahaya menerangi objek, objek memantulkan kembali sebagian dari berkas cahaya tersebut. Pantulan cahaya ini ditangkap oleh alat-alat optik, misalnya mata manusia, kamera digital, dan sebagainya, sehingga banyak objek citra tersebut terekam. Munir, 2004.[3]

Citra terbagi menjadi dua jenis citra yaitu citra diam dan citra bergerak. Citra diam adalah citra tunggal yang bergerak *(moving images)* adalah rangkaian citra diam yang ditampilkan secara berurutan (sekuensial) sehingga memberi kesan pada mata kita sebagai gambar yang bergerak. Sedangkan citra diam adalah citra yang tidak bergerak. Indek baris dan kolom *(x,y)* dari sebuah piksel dinyatakan dalam bilangan bulat. Piksel (0,0) terletak pada sudut kiri atas pada citra, indek *x* bergerak ke kanan dan indek *y* bergerak ke bawah.Ahmand, 2005.[11]

Agar dapat diolah dengan komputer digital, suatu citra harus direpresentasikan secara numerik dengan nilai-nilai diskrit. Representasi citra dari fungsi kontinu menjadi nilai-nilai diskrit disebut pencitraan (*imaging*) atau digitalisasi. Citra yang dihasilkan inilah yang disebut citra digital (*Digital Image*), dinyatakan sebagai kumpulan piksel dalam matrik dua dimensi. Pada umumnya citra digital berbentuk empat persegi panjang dan dimensi ukurannya dinyatakan tinggi dikalikan dengan lebar atau lebar dikalikan dengan panjang. Citra digital yang berukuran MxN lazim dinyatakan dengan matriks yang berukuran M baris dan N kolom seperti pada gambar 2.1 :

$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) & \cdots & f(0,N-1) \\ f(1,0) & f(1,1) & \cdots & f(1,N-1) \\ \vdots & \vdots & & \vdots \\ f(M-1,0) & f(M-1,1) & \cdots & f(M-1,N-1) \end{bmatrix}$$

Gambar 2.1: Representasi citra digital dalam matriks N x M Gonzalez, 1987.[8].

Setiap elemen pada citra digital (berarti elemen matriks) disebut sebagai *picture element* atau piksel (*pixel*). Jadi citra yang berukuran M x N mempunyai MN buah piksel. Misalkan sebuah citra *digital* berukuran 256 x 256 piksel dengan derajat keabuan 256 level dan dipresentasikan secara numerik dengan matriks terdiri dari 256 baris (di indek dari 0 sampai 255) dan 256 kolom Citra monokrom atau citra hitam putih merupakan citra satu kanal dimana citra f(x,y) merupkan fungsi tingkat keabuan dari hitam keputih, x menyatakan variable baris atau garis jelajah dan y menyatakan variable kolom atau posisi

piksel garis jelajah. Sebaliknya citra berwarna dikenal juga citra multi-spektral, dimana warna citra biasanya dinyatakan dalam tiga komponen warna: merah, hijau, biru (RGB), citra berwarna {f merah(x,y), f hijau (x,y), f biru (x,y)} merupakan fungsi harga vektor tingkat keabuan merah hijau dan biru. Murni, 1992. [1].

2.2. Format File Bitmap (BMP)

Format citra yang baku di lingkungan sistem operasi Microsoft Windows adalah file bitmap (BMP). Pada saat ini format BMP kurang begitu populer dan mulai jarang digunakan dibanding format JPG atau GIF, karena file BMP pada umumnya tidak dimampatkan, sehingga ukuran relatif lebih besar dari pada file JPG atau GIF. Terjemahan bebas bitmap adalah pemetaan bit. Artinya nilai intensitas piksel di dalam citra dipetakan ke sejumlah bit tertentu. Peta bit umumnya adalah 8, yang berarti setiap piksel panjangnya 8 bit. Delapan bit ini mempresentasikan nilai intensitas piksel. Dengan demikian ada sebanyak 2_8 =256 derajat keabuan, mulai dari 0 (00000000) sampai 255 (11111111).

Terdapat tiga macam citra dalam format BMP, yaitu citra biner, citra berwarna dan citra hitam-puth (*grayscale*). Citra biner hanya memiliki dua nilai keabuan 0 dan 1. Oleh kerena itu 1 bit telah cukup untuk mempresentasikan nilai piksel. Citra berwarna adalah citra yang lebih umum. Warna yang terlihat di dalam citra bitmap merupakan kombinasi dari tiga komponen warna, yaitu : R (Red), G (Green) dan B (Blue). Kombinasi dari tiga warna RGB tersebut menghasilkan warna yang khas untuk piksel yang bersangkutan. Pada citra 256 warna, setiap piksel memiliki panjang 8-bit, akan tetapi komponen RGBnya disimpan dalam tabel RGB yang disebut *palet.*

Berikut ini akan memperlihatkan panjang informasi palet untuk detiap versi *bitmap*, masing-masing untuk citra 16 warna, 256 warna dan 16,7 juta warna. Berkas citra 24-bit tidak mempunyai palet RGB, karena langsung di uraikan ke dalam data *bitmap*. Lihat tabel 2.1

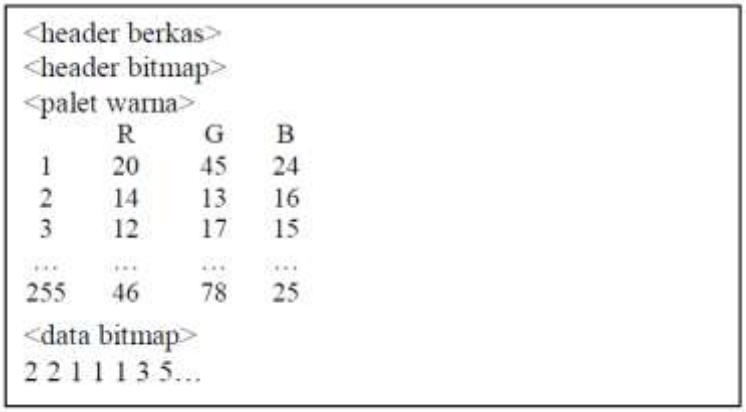
Tabel 2.1 : Panjang informasi *palet bitmap* berwarna

Citra m warna	*Palet bitmap*
Citra 16 warna	64 *byte*
Citra 256 warna	1024 *byte*
Citra 16,7 juta warna	0 *byte*

Tabel 2.1 : Panjang informasi *palet bitmap* berwarna

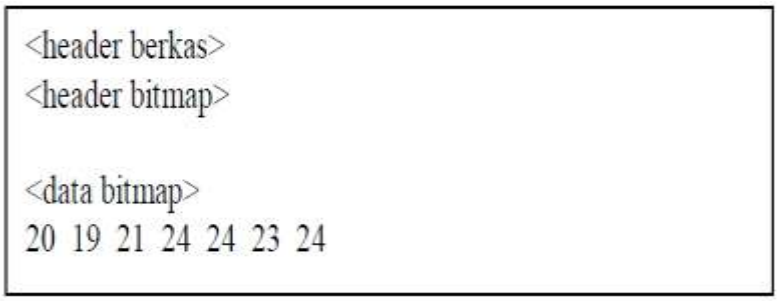
Informasi *palet* warna terletak sesudah *header bitmap*. Informasi *palet* warna dinyatakan dalam satu tabel RGB. Setiap *entry* pada tabel terdiri atas tiga buah *field* yaitu, R (*Red*), G (*Green*), dan B (*Blue*). Data bitmap diletakan sesudah informasi *palet*. Munir, 2004. [3]

Format citra 8-*bit* dapat dilihat pada gambar 2.4. format citra 4-*bit* (16 warna), hampir sama dengan format citra 8-*bit*. Pada citra 4-*bit* dan citra 8-*bit*, warna suatu piksel di acu dari tabel informasi palet *entry* ke-k (*k* merupakan nilai rentang 0-15 untuk citra 16 warna dan 0-155 untuk citra 256 warna). Sebagai contoh pada gambar 2.4, piksel pertama bernilai 2, warna piksel pertama ini ditentukan oleh komponen RGB pada *palet* warna *entry* ke-2, yaitu R=14, G=14 dan B=16.piksel kedua serupa dengan piksel pertama. Piksel ketiga bernilai 1, warna ditentukan oleh komponen RGB pada *palet* warna *entry* ke-1, yaitu R=20, G=45 dan B=24. Demikian seterusnya untuk piksel-piksel lainnya. Khusus untuk citra hitam-putih 8-*bit*, komponen R,G dan B suatu piksel bernilai sama dengan data bitmap piksel tersebut. Jadi piksel dengan nilai data bitmap 129, memiliki nilai R=129, G=129 dan B=129. ,lihat gambar 2.3 Munir, 2004. [3]



Gambar 2.3: Format citra 8-*bit* (256 warna) (Munir, 2004) [3]

Citra yang lebih kaya warna adalah citra 24-*bit*. Setiap piksel panjangnya 24-*bit*, karena setiap bit langsung menyatakan komponen warna merah (8-bit), komponen warna hijau (8-*bit*) dan komponen warna biru (8-*bit*). Citra 24-*bit* juga disebut citra 16 juta warna karena mampu menghasilkan 2^{24} =16.777.216 kombinasi warna. Contohnya seperti pada Gambar 2.4 berikut ini, dimana piksel pertama memiliki nilai R=20, G=19 dan B=21. Piksel kedua memiliki nilai R=24, G=24 dan B=23 dan demikian seterusnya. Munir, 2004. [3]



Gambar 2.4 : Format citra 24-*bit* (16,7 juta warna) Munir, 2004. [3]

2.3. Pengertian Penyandian File Gambar

Kata penyandian file gambar terdiri dari tiga buah kata yaitu pertama adalah penyandian, mempunyai kata dasar "sandi" yang menurut kamus besar. Bahasa Indonesia berarti kode, sedangkan penyandian adalah sebuah bentuk kata kerja yang berarti suatu kegiatan menyandikan atau mengkodekan dengan tujuan tertentu. Kedua adalah file yaitu sebutan sekumpulan *byte* atau deretan karakter atau kode-kode yang membentuk sebuah dokumen yang memiliki nama yang unik, sedangkan yang ketiga adalah kata gambar yang dalam kamus besar bahasa Indonesia adalah "citra", citra adalah objek elemen-elemenya dinyatakan dengan suatu besaran numerik yang membentuk (*array*). Murni, 1992. [1]. Sehingga penyandian file gambar dapat diartikan kegiatan menyandikan atau mengkodekan sekumpulan elemen penyusun gambar (piksel) dengan tujuan mengamankan informasi dari pihak yang tidak berhak.

2.4. Kriptografi

Penyandian merupakan salah satu alternatif atau cara untuk mengamankan atau menjaga suatu kerahasiaan data atau gambar. Seni dan ilmu untuk menyandikan atau menjaga keamanan atau serta kerahasian pesan disebut kriptografi. Kurniawan, 2004.[5]

.Kriptografi juga dapat diartikan sebagai ilmu yang mempelajari teknikteknik matematika yang berhubungan dengan aspek keamanan informasi seperti keabsahan, integritas data, serta autentikasi data, dengan kata lain kriptografi digunakan untuk menjamin keleluasaan pribadi dan pembuktian keaslian pesan dalam berkomunikasi.

Kriptografi sendiri berasal dari bahasa yunani yaitu *kryptos* yang artinya "*secret*" (rahasia) dan *graphein* yang artinya *"writing"* (tulisan), jadi kriptografi adalah *"secret writing"* (tulisan rahasia). Munir,2006. [4]. Informasi atau pesan adalah salah satu hal penting yang harus disampaikan dalam berkomunikasi. Pesan yang disampaikan dari satu pihak ke pihak yang lain dapat berupa file teks, file suara, maupun pesan yang berupa file gambar. Dalam menyampaikan sebuah informasi atau pesan ke pihak lain, kerahasian dan keaslian pesan perlu dijaga. Sehingga pesan perlu disandikan sebelum dilakukan pengiriman.

Pada dasarnya kriptografi terdiri dua algoritma yaitu, algoritma enkripsi (E) dan algoritma dekripsi (D). Dasar matematis yang mendasari proses enkripsi dan dekripsi adalah relasi antara dua himpunan yaitu himpunan yang berisi elemen *plaintext* dan himpunan yang berisi himpunan *ciphertext*. Pesan atau informasi yang dapat dibaca disebut sebagai *plaintext*, sedangkan teknik untuk membuat pesan tidak dapat terbaca disebut enkripsi. Pesan yang sudah melewati tahap enkripsi disebut *ciphertext*, sedangkan dekripsi adalah teknik untuk mengubah *ciphertext* menjadi *plaintext*. Kurniawan,2004. [5]. sedangkan kunci atau *key* adalah parameter yang digunakan untuk transformasi enkripsi dan dekripsi. Kunci biasanya berupa string atau deret bilanngan. Munir, 2006. [4].

Dalam menyandikan pesan atau mengenkripsi pesan, terdapat dua jenis algoritma yang berdasar jenis kuncinya, yaitu :

1. Algoritma Simetri (menggunakan satu kunci untuk enkripsi dan dekripsinya).
2. Algoritma Asimetri (menggunakan kata kunci yang berbeda untuk enkripsi dan dekripsinya).

Algoritma simetri disebut juga sebagai algoritma konvensional adalah algoritma untuk membuat pesan yang disandikan menggunakan satu kunci untuk enkripsi dan dekripsinya. kurniawan, 2004. [5]. Disebut konvensional karena algoritma yang biasa digunakan orang sejak berabad-abad yang lalu adalah algoritma jenis ini. Algoritma simetrik sering juga disebut sebagai algoritma kunci rahasia, algoritma kunci tunggal, atau algoritma satu kunci, dan mengharuskan pengirim dan penerima menyetujui suatu kunci tertentu sebelum mereka dapat berkomunikasi dengan aman. Keamanan algoritma simetri tergantung pada kunci, agar komunikasi tetap aman kunci harus tetap dirahasiakan. kurniawan, 2004. [5].

2.5. Algoritma Kriptografi Klasik

Pada algoritma kriptografi klasik (simetri), merupakan algoritma kriptografi yang biasa digunakan orang sejak berabad-abad yang lalu dengan berbasis karakter, yaitu enkripsi dan dekripsi dilakukan pada setiap karakter pesan. Munir,2006.[4]. Dan pada dasarnya, algoritma kriptografi klasik dapat dikelompokkan kedalam dua metode dasar yang biasa digunakan, yaitu:

a. Metode substitusi
b. Metode transposisi

Tiga alasan dasar menggunakan algoritma kriptografi klasik adalah :

1.Memahami konsep dasar kriptografi.
2.Dasar dari algoritma kriptografi modern.
3. Untuk memahami kelemahan sistem kode.

2.6. Diagram Arus Data *(Data Flow Diagram)*

Sebelum mengimplementasi program, maka dilskukan pembutan DFD atau *Data Flow Diagram* (DFD) atau dalam bahasa indonesia menjadi diagram alir data (DAD) adalah sebuah representasi grafik yang menggambarkan aliran informasi dan transformasi informasi yang diaplikasikan sebagai data yang mengalir dari masukan (*input*) dan keluaran (*output*). Rosa, salahuddin, 2011.[10].

DFD dapat digunakan untuk merepresentasikan sebuah sistem atau perangkat lunak pada beberapa level abstraksi. DFD dapat dibagi menjadi beberapa level yang lebih detail untuk merepresentasikan aliran informasi atau fungsi yang lebih detail. DFD menyediakan mekanisme untuk pemodelan fungsional ataupun pemodelan informasi. Oleh karena itu, DFD lebih sesuai digunakan untuk memodelkan fungsi-fungsi perangkat lunak yang akan diimplementasikan menggunakan pemrograman terstuktur. Rosa, Salahuddin, 2011. [10]. DFD menggambarkan penyimpanan data dan proses yang mentransformasikan data. DFD menunjukkan hubungan antara data pada system dan proses pada sistem.

Ada beberapa simbol DFD, salah satu diantaranya menurut Yourdon/ De Marco (Lihat tabel 2.2).

Tabel 2.2 Simbol – Simbol DFD menurut Yourdon/ De Marco

Simbol	Nama Simbol	Fungsi / Keterangan
	Proses	Tempat terjadinya kegiatan pengolahan/proses
	Terminator	Entitas luar yang terlibat langsung dengan sistem
	Flow	Menunjukan arah aliran dari dan kemana
	Storage	Sebagai alat penyimpan

2.7. Diagram Alir (*Flowchart*)

Flowchart adalah bagan yang memperlihatkan urutan prosedur dan proses dari beberapa file didalam media tertentu. Melalui *flowchart* dapat terlihat jenis media penyimpanan yang dipakai dalam pengolahan data. Selain itu juga menggambarkan file yang dipakai sebagai *inpu*t maupun *output*. Tosin, 1997. [9] *Flowchart* disusun dengan simbol. Simbol – simbol dapat dipakai sebagai alat bantu menggambarkan proses di dalam program. Simbol tersebut dapat dilihat dalam tabel 2.3.

Tabel 2.3 Simbol-Simbol *Flowchart*

Simbol	Nama Simbol	Fungsi / Keterangan
	Proses	Menunjukan kegiatan proses dari operasi program komputer
	Terminal	Menunjukan awal dan akhir dari suatu proses
	Keputusan	Digunakan untuk suatu penyelesaian kondisi dalam program
	Input / Output	Digunakan untuk mewakili data input/output
	Aliran Data	Menunjukkan petunjuk dari aliran fisik pada program

2.8. Pemrograman Borland Delphi 7

Delphi berasal dari bahasa pemrograman yang cukup terkenal, yaitu bahasa *pascal*. Bahasa pascal diciptakan pada tahun 1971 oleh ilmuwan dari swiss, yaitu Niklaus Wirth. Nama *pascal* diambil dari ahli matematika dan filsafat Perancis, yaitu *Blasie Pascal* (1623-1622). Karena pemrograman *windows* dengan *turbo pascal* masih dirasa cukup sulit, maka sejak tahun 1993 *Borland International* mengembangkan bahasa pascal yang bersifat visual. Hasil dari pengembangan ini adalah dirilisnya Delphi 1 pada tahun 1995. Perkembangan Delphi tidak berhenti sampai di situ. Pada tahun berikutnya 1996, *Borland International* merilis Delphi 2 untuk *windows* 95/NT. Kemudian dalam tahun-tahun berikutnya, *Borland International* merilis beberapa versi pengembangan Delphi yang memiliki tambahan fitur baru dibandingkan dengan versi sebelumnya. malik.2006. [7].

3. Implementasi

3.1. Implementasi

Aplikasi penyandian file gambar pada citra digital dibuat dengan program bantu Borland Delphi 7. Pada aplikasi ini terdapat beberapa fungsi yaitu : fungsi yang dapat membuka citra asli yang dapat dienkripsi, fungsi yang dapat membuka citra hasil enkripsi, fungsi yang dapat melakukan proses enkripsi, fungsi yang dapat melakukan proses dekripsi, serta terdapat petunjuk tentang penggunaan aplikasi penyandian file gambar.

Berikut adalah tampilan dari form awal ketika pertama kali program dijalankan seperti pada gambar 3.1.

Gambar 3.1 *Form* Awal

Setelah form awal dijalankan maka secara otomatis akan membuka form Penyandian gambar dimana pada form ini dapat dilakukan proses enkripsi.

Tampilan form enkripsi seperi pada gambar 3.1. Pada tampilan *form* penyandian terdapat tiga menu yaitu menu berkas, penyandian gambar dan menu bantuan. Menu berkas dimaksudkan adalah pengguna dapat melakukan pengambilan gambar, penyimpanan gambar dan keluar dari sistem. Menu penyandian gambar dimaksudkan seorang pengguna dapat beralih ke proses enkripsi maupun dekripsi. Menu bantuan dimaksudkan agar seorang Pengguna dapat melihat tutorial dalam penggunaan aplikasi enkripsi dan dekripsi. Form bantuan dapat dilihat seperti pada gambar 3.2.

Gambar 3.2 Form Bantuan

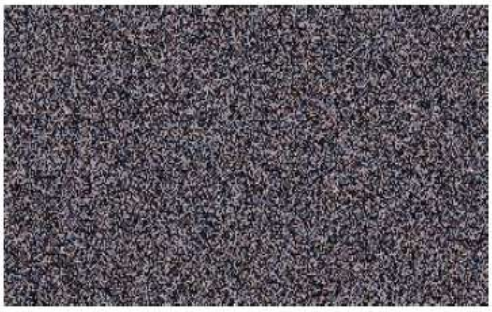
4. Pengujian Hasil

Pada pembahasan ini akan dilakukan pengujian tingkat keberhasilan pada proses enkripsi dan dekripsi yaitu setiap citra sebagai media penyandiannya dienkripsi dengan beberapa kata sandi. Pada proses dekripsinya citra yang terenkripsi di lakukan dekripsi dengan sandi yang sama maupun berbeda. Citra yang menjadi media pengujiannya antara lain Kuda.Bmp, Alam .bmp, Merah putih.bmp, Ruang. bmp, Tangga.bmp, Tentara.bmp, Semarang.bmp. Citra-citra tersebut dapat dilihat pada gambar 4.1

Gambar 4.1 Citra Yang Akan Dilakukan Pengujian

4.1 Pengujian pada Proses Enkripsi

Pengujian pada proses enkripsi ini, citra sebagai medianya diuji dengan beberapa kata sandi. Sebagai salah satu pengujiannya pada citra alam.bmp di enkripsi dengan kata sandi "1a2s3d4f", maka akan dihasilkan cipherteks dengan ukuran piksel tetap sama dengan ukuran piksel plainteksnya. Hasil pengujian dengan citra Alam.bmp dapat dilihat pada gambar 4.2:



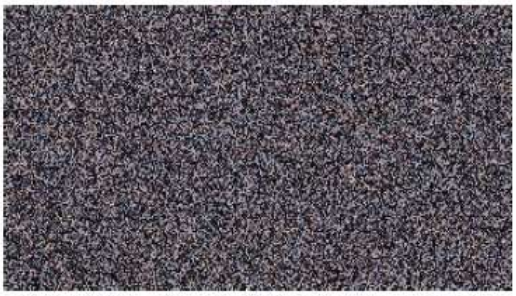
plaintext (alam.bmp 324x186 piksel) *ciphertext* (alam 324x168 piksel)

Gambar 4.2 hasil pengujian proses enkripsi citra alam.bmp

Hasil pengujian diatas dapat dilihat bahwa setelah dilakukan enkripsi dengan kata sandi, plainteks maupun cipherteksnya tetap memiliki ukuran piksel yang sama.

4.2 Pengujian pada Proses Dekripsi

Pengujian pada proses dekripsi ini, citra yang sudah di enkrips dilakukan proses dekripsi dengan beberapa sandi untuk mendapatkan citra awal. Sebagai salah satu pengujian dekripsi digunakan cipherteks dari citra alam.bmp yang sudah di enkripsi dengan kata sandi "1a2s3d4f", maka pada proses dekripsi ini dengan kata sandi yang sama untuk mendapatkan citra seperti plainteks sebelumnya. Dapat dilihat pada gambar 4.3



ciphertext (alam.bmp 324 x186 piksel) *plaintext* (alam 324x168 piksel)

Gambar 4.3. Hasil pengujian proses dekripsi

Dari pengujian dekripsi diatas ternyata diperoleh citra plainteks tetap sama dengan citra sebelum dilakukan enkripsi dengan ukuran piksel juga tetap sama.

Hasil pengujian pada proses dekripsi pada cipherteks yang lainnya dapat dilihat pada tabel 4.2

Tabel 4.2 Hasil Percoabaan dekripsi

Nama gambar	Ukuran Plainteks *(Width x height)* piksel	Kata Sandi	Ukuran Cipherteks *(Width x height)* piksel	Waktu (detik)	Ket
Kuda.bmp	630x472	asdfghjk	630x472	02	Baik
		12345678asdfghjk		02	Tidak
		12345678		-	rusak
Alam. Bmp	324x168	1a2s3d4f	324x168	00	Baik
		Asdfghjk12345678		00	Baik
		asdfghjk		-	rusak
Ruang.bmp	600x350	zxcvbnma	600x350	01	Baik
		qwertyuioasdfghj		01	Baik
		12345678			rusak
Tangga.bmp	800x600	12345678qwertyui	800x600	03	Baik
		12345678		-	rusak
Tentara.bmp	820x540	qawsedrftgyhujik	820x540	02	Baik
		87654321		-	rusak

Pada pengujian proses dekripsi ini didapat citra dengan kualitas baik karena sesuai denga citra asli sebelum dilakukan proses enkripsi, ini karena dalam proses dekripsi sandi yang digunakan sesuai dengan kata sandi yang digunakan pada proses enkripsi. Akan tetapi apabila pemberian kata sandi tidak sama dengan sebelumnya maka citra hasil proses dekripsi akan rusak atau tidak dapat dihasilkan citra seperti citra aslinya.

5. Kesimpulan

Setelah menyelesaikan penulisan tentang penyandian file gambar dengan metode substitusi dan tranposisi, dan dilakukan pengujian dari program yang telah dibuat pada bab-bab sebelumnya dapat diambil kesimpulan :

1. Aplikasi penyandian pada file gambar dengan metode substitusi dan transposisi dapat menghasilkan suatu gambar yang tidak dapat dikenali seperti gambar semula.
2. Teknik penyandian dengan substitusi dan transposisi yang diterapkan dalam mengakses suatu bit-bit dari gambar berhasil memanipulasi posisi dan mengacak susunan piksel pada gambar.
3. Gambar yang sudah melewati proses penyandian dan tidak dapat dikenali dapat dikembalikan lagi oleh program aplikasi yang telah dibuat, sehingga gambar dapat kembali lagi dan dapat dikenali.
4. Gambar yang memiliki ukuran piksel yang kecil menghasilkan waktu proses yang singkat, sebaliknya jika ukuran piksel gambar besar, maka waktu yang diperoleh akan semakin lama.
5. Ketika dilakukan pengujian dalam membandingkan gambar asli sebelum gambar dilakukan penyandian dengan gambar setelah disandikan dan gambar dekripsi tidak terdapat perbedaan dalam ukuran piksel gambar.

6. Daftar Pustaka

[1] **Aniati Murti dan Suryana Setiawan**, 1992. *Pengantar Penggolahan Citra*, PT Elex Media Komputindo. Jakarta.

[2] **Dony Aryus**, 2008. *Pengantar Ilmu kriptografi keamanan Teori analisis dan Implemtasi.* Andi. Yogyakarta.

[3] **Ir. Rinaldi Munir, M.T**, 2004, *Pengolahan Citra Dengan Pendekatan Algoritmik*. Informatika, Bandung.

[4] **Ir. Rinaldi Munir, M.T**, 2006, *Kriptografi*. Informatika. Bandung.

[5] **Ir. Yusuf Kurniawan, M.T**, 2004, *Kriptografi Keamanan Internet dan Jaringan Komunikasi*. Informatika. Bandung.

[6] **Jaja Jamaludin Malik**, 2005, *Tip & Trik Unik Delphi*, Andy. Yogyakarta.

[7] **Jaja Jamaludin Malik**, 2006, *Kumpulan Latihan Pemrograman Delphi*, Andy. Yogyakarta.

[8] **Rafael C. Gonsalez / paul Wintz**, 1987, " *Digital Image Processing*",Wesly publishing Company Inc.

[9] **Rijanto TOSIN**, 1997, *Flowchart untuk Siswa dan Mahasiswa*, Dinastindo. Jakarta.

[10] **Rosa A.S-M.Shalahuddin**, 2011, *Rekayasa Perangkat Lunak*, Modula. Bandung

[11] **Usman Ahman**, 2005. *Pengolahan Citra Digital dan Teknik Pemrogramannya*. Graha Ilmu. Yogyakarta.