IMPLEMENTASI KRIPTOGRAFI DAN STEGANOGRAFI DENGAN METODE ALGORITMA DES DAN METODE END OF FILE

Ajar Rohmanu
Teknik Informatika, STMIK Cikarang
Email: ajarrohmanu@gmail.com

Abstrak

Teknologi kriptografi sudah dapat dipecahkan dalam system proses pengamanan sebuah pesan, sehingga diperlukan penambahan sebuah teknologi yaitu steganografi. Steganografi merupakan seni menyembunyikan pesan rahasia ke dalam suatu media sehingga selain pengirim dan penerima pesan tidak ada yang mengetahui atau menyadari ada suatu pesan rahasia dari media yang dikirim. Pada jurnal ini, dilakukan studi mengenai penerapan steganografi teknik End of File pada media audio wav. Implementasi steganografi akan disertai dengan penerapan kriptografi berupa enkripsi dan dekripsi. Teknik Kriptografi yang akan digunakan adalah (Data Encrypt Standart) DES. Implementasi kriptografi dan steganografi dilaukan dengan menggunakan Eclipse dan Java Development Kit.

Kata kunci: Steganografi, Kriptografi, DES, End Of File

I. PENDAHULUAN

Teknologi komunikasi dan informasi berkembang dengan pesat dan memberikan pengaruh besar bagi kehidupan manusia. Seiring dengan perkembangan teknologi sekarang ini yang semakin pesat maka proses pengiriman data dapat dilakukan dengan mudah dengan melalui berbagai macam media yang telah ada. Perkembangan yang pesat dalam proses pengiriman data membawa dampak yang besar, yaitu masalah keamanan data yang di kirim. Pada proses mengirim data melalui media-media biasanya secara polos atau tanpa pengaman, sehingga harus dilakukan proses pengamanan untuk data yang akan di kirim, salah satunya dilakukan dengan cara melakukan enkripsi pada sebuah file.

Kriptografi dapat menjadi jawaban dari masalah tersebut. Sebagai ilmu yang telah diaplikasikan untuk pengamanan data, kriptografi dapat digunakan untuk mengamankan data-data penting pada sebuah file. Data yang terkandung dalam file disandikan atau dienkripsi untuk diubah menjadi simbol tertentu sehingga hanya orang tertentu saja yang dapat mengetahui isi dari data tersebut. Dalam perkembangan ilmu kritografi masa sekarang ini, telah banyak tercipta algoritma-algoritma yang dapat digunakan untuk mengubah data asli (plain text) menjadi simbol tertentu (chiper text). Salah satu contohnya adalah algoritma DES. Algoritma ini termasuk dalam algoritma kriptografi modern dan merupakan algoritma chipper blok.

Seiring perkembangan teknologi sekarang ini, masih di rasa kurang dalam pengamanan data menggunakan kriptografi. Setelah file tersebut di enkripsi, kita perlu melakukan penyembunyian file ke dalam file lain supaya pihak yang bukan berkepentingan tidak begitu curiga dalam melihat file tersebut. Langkah seperti ini sering disebut dengan Steganografi. Steganografi merupakan salah satu cara yang sangat efektif untuk mengurangi rasa curiga dari pihak-pihak lain (selain pengirim dan penerima yang sah). Kebanyakan algoritma steganografi menggunakan sebuah kombinasi dari bidang jenis teknik untuk melakukan sebuah tugas dalam penyelubungan pesan rahasia dalam sebuah selubung file.

Dalam perkembangan ilmu steganografi sekarang ini, terdapat berbagai macam metode yang dapat digunakan untuk menyembunyikan file tersebut. Salah satu contohnya adalah metode End of File (EoF). Ada sedikit perbedaan antara steganografi dengan kriptografi. Pada steganografi, penyembunyian atau penyamaran pesan ini dibuat sedemikian rupa sehingga pihak lain tidak mengetahui bahwa ada pesan lain di dalam pesan yang dikirim. Pesan inti tersebut tetap dipertahankan, hanya dalam penyampaiannya dikaburkan atau disembunyikan dengan berbagai cara. Hanya pihak penerima yang sah saja yang dapat mengetahui pesan lain tersebut.

Sedang pada kriptografi, karakter pesan diubah atau diacak menjadi bentuk lain yang tidak bermakna. Pesan yang disampaikan dalam kriptografi menjadi mencurigakan karena ketidak bermaknaannya tersebut. Sedang pesan dalam steganografi, terlihat seperti pesan biasa sehingga kecil kemungkinan untuk dicurigai. Namun demikian, bukan berarti tidak ada kekurangan pada steganografi ini. Kelemahan pada steganografi ini terjadi apabila kita mengubah format pesan yang dikirimkan, maka pesan rahasianyapun menjadi hilang.

Ada persamaan diantara steganografi dan kriptografi ini yaitu keduanya digunakan secara bersamaan untuk menjamin keamanan pesan rahasianya.

II. LANDASAN TEORI

2.1. Steganografi

Steganografi (*steganoggraphy*) berasal Yunani, yaitu "*steganos*" artinya menyembunyikan dan "*graptos*" artinya tulisan. Sehingga steganografi adalah tulisan yang disembunyikan.

Penguasa Yunani dalam mengirimkan pesan rahasia menggunakan kepala budak atau prajurit sebagai media. Dalam hal ini,rambut budak dibotaki, lalu pesan rahasia ditulis

pada kulit kepala budak. Ketika rambut budak tumbuh, budak tersebut diutus untuk membawa pesan rahasia di kepalanya.

Bangsa Romawi mengenal steganografi dengan menggunakan tinta tak-tampak (*invisible ink*) untuk menuliskan pesan. Tinta tersebut dibuat dari campuran sari buah, susu, dan cuka. Jika tinta digunakan untuk menulis maka tulisannya.

Secara umum steganografi dapat didefinisikan sebagai ilmu atau seni yang digunakan untuk menyembunyikan pesan rahasia dengan teknik-teknik tertentu sehingga selain orang yang dituju, orang lain tidak akan menyadari keberadaan dari pesan rahasia tersebut.

Untuk memperkuat penyembunyian data, bit-bit data tidak digunakan untuk mengganti byte-byte yang berurutan, namun dipilih susunan byte secara acak. Bilangan acak dibangkitkan dengan *pseudo-random-number-generator* (PNRG). PNRG menggunakan kunci rahasia untuk membangkitkan posisi piksel yang akan digunakan untuk menyembunyikan bit-bit. PNRG dibagun dalam sejumlah cara, salah satunya dengan menggunakan algoritma kriptografi DES (*Data Encription Standart*), algoritma *hash* MD5, dan metode kriptografi CFB (*Chiper-Feedback Mode*). Tujuan dari ekripsi adalah menghasilkan sekumpulan bilangan acak yang sama untuk setiap kunci enkripsi yang sama. Bilangan acak dihasilkan dengan cara memilih bit-bit dari sebuah blok data hasil enkripsi.

Ada beberapa terminology dari steganografi yang harus dipahami, antara lain sebagai berikut:

1) *Embedded Message (HiddenText):* Pesan atau informasi yang disembunyikan. Contohnya dapat berupa teks, gambar, audio, video, dan lain-lain.
2) *Cover-Object (CoverText)*: Pesan yang digunakan untuk menyembunyikan *embedded message.* Contohnya dapat berupa teks, gambar, audio, video, dan lain-lain.
3) *Stego-Object (StegoText)*: Pesan yang sudah berisi pesan *embedded message.*
4) *Stego-key*: Kunci yang digunakan untuk menyisipkan pesan dan mengekstraksi pesan dari *stegotext.*

2.2. Metode End of File (EoF)

Teknik yang digunakan pada digital watermarking beragam tetapi secara umum teknik ini menggunakan redundant bits sebagai tempat menyembunyikan pesan pada saat dilakukan kompresi data, dan kemudian menggunakan kelemahan indera manusia yang tidak sensitive sehingga pesan tersebut tidak ada perbedaan yang terlihat atau yang terdengar. Teknik EOF atau End Of File merupakan salah satu teknik yang digunakan dalam steganografi. Teknik ini menggunakan cara dengan menyisipkan data pada akhir file. Teknik ini dapat digunakan untuk menyisipkan data yang ukurannya sesuai dengan kebutuhan. Ukuran file yang telah disisipkan data sama dengan ukuran file sebelum disisipkan data ditambah dengan ukuran data yang disisipkan ke dalam file tersebut. Teknik inilah yang akan digunakan penulis dalam penelitian ini. Dalam teknik ini, data disisipkan pada akhir file dengan diberi tanda khusus sebagai pengenal start dari data tersebut dan pengenal akhir dari data tersebut.

2.3. Kriptografi

Kriptografi merupakan sebuah ilmu yang digunakan untuk penyandian data. Kriptografi telah dikenal dan dipakai cukup lama sejak kurang lebih tahun 1900 sebelum masehi pada prasasti-prasasti kuburan. Ilmu Kriptografi sebenarnya sudah mulai dipelajari manusia sejak tahun 400 SM, yaitu pada zaman Yunani kuno. Dari catatan bahwa "penyandian transposisi" merupakan system kriptographi pertama yang digunakan atau dimanfaatkan. Bidang ilmu ini terus berkembang seiring dengan kemajuan peradaban manusia, dan memegang peranan penting dalam strategi peperangan yang terjadi dalam sejarah manusia, mulai dari system kriptographi "Caesar Cphiper"yang terkenal pada jaman romawi kuno, "Playfair Chiper" yang digunakan inggris dan "ADFVGX Cipher" yang digunakan Jerman pada Perang Dunia I hingga algoritma-algoritma kriptografi rotor yang populer pada Perang Dunia II , seperti Sigaba / M- 134 (Amerika Serikat), Typex (Inggris), Purple (Jepang), dan mesin kriptografi legendaris Enigma (Jerman). Sejarah telah dipenuhi oleh contoh-contoh orang yang berusaha merahasiakan informasi rahasia mereka dari orang lain.

Ada tiga istilah yang berkaitan dengan proteksi data yaitu kriptografi, kriptologi, dan kriptanalisis. Arti ketiganya kurang lebih sama. Secara teknis, kriptologi adalah ilmu yang mempelajari tentang komunikasi pada jalur yang tidak aman beserta masalah-masalah yang berhubungan dengan itu.

Kriptographi berasal dari kata "Crypto" yang berarti rahasia dan "graphy" yang berarti tulisan. Jadi, dapat dikatakan bahwa kriptografi adalah tulisan yang tersembunyi. Dengan adanya tulisan yang tersembunyi ini, orang-orang tidak mengetahui bagaimana tulisan tersebut disembunyikan dan tidak mengetahui bagaimana cara membaca maupun menerjemahkan tulisan tersebut. William Stallings mendefinisikan Kriptographi sebagai "The Art and Science of keeping message secure".

Kriptografi berbasis pada algoritma pengkodean data informasi yang mendukung kebutuhan dari dua aspek keamanan informasi, yaitu secrecy (perlindungan terhadap kerahasiaan data informasi) dan authenticity (perlindungan terhadap pemalsuan dan pengubahan informasi yang tidak diinginkan. Kriptografi menjadi dasar bagi keamanan komputer dan jaringan karena merupakan sarana bagi distribusi data dan informasi. Sehingga data dan informasi tersebut harus diamankan agar hanya orang-orang yang berhak mengaksesnya yang dapat mengetahui maupun menggunakan data tersebut. Salah satu cara yang paling banyak digunakan dalam mengamankan data adalah dengan kriptografi. Data-data tersebut diamankan dengan sedemikian rupa oleh pengirim sehingga orang lain tidak dapat mengenali data tersebut.

Pembakuan penulisan pada kriptografi dapat ditulis dalam Bahasa matematika. Fungsi-fungsi yang mendasar dalam

kriptografi adalah enkripsi dan dekripsi. Enkripsi adalah proses mengubah suatu pesan asli (plaintext) menjadi suatu pesan dalam bahasa sandi (ciphertext).

C = E (M), dimana :

M = pesan asli

E = proses enkripsi

C = pesan dalam bahasa sandi (untuk ringkasnya disebut sandi) Sedangkan dekripsi adalah proses mengubah pesan dalam suatu bahasa sandi menjadi pesan asli kembali.

M = D (C)

D = proses dekripsi

Umumnya, selain menggunakan fungsi tertentu dalam melakukan enkripsi dan dekripsi, seringkali fungsi itu diberi parameter tambahan yang disebut dengan istilah kunci.

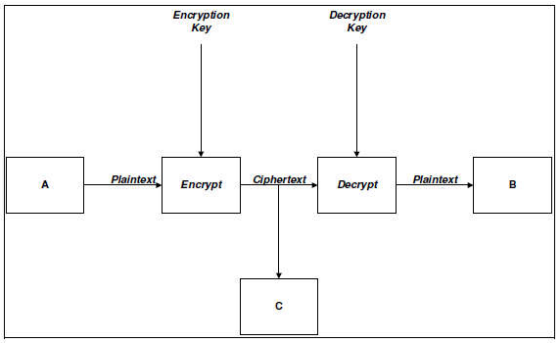
Dalam teknologi informasi, telah dan sedang dikembangkan cara untuk menangkal berbagai bentuk serangan semacam penyadapan dan pengubahan data yang dikirimkan. Salah satu cara yang ditempuh mengatasi masalah ini ialah dengan menggunakan kriptografi yang menggunakan transformasi data sehingga data yang dihasilkan tidak dapat dimengerti oleh pihak yang tidak berhak mengakses. Transformasi ini memberikan solusi pada dua macam masalah keamanan data, yaitu masalah privasi (privacy) dan keotentikan (authentication). Privaci mengandung arti bahwa data yang dikirimkan hanya dapat dimengerti informasinya oleh penerima yang sah atau berhak. Sedangkan keotentikan mencegah pihak ketiga untuk mengirimkan data yang salah atau mengubah data yang dikirimkan. Kriptografi yang baik tidak ditentukan oleh kerumitan dalam mengolah data atau pesan yang akan disampaikan. Ada 4 syarat yang perlu dipenuhi, yaitu:

1) *Kerahasiaan*: Pesan (plaintext) hanya dapat dibaca oleh pihak yang memiliki kewenangan.
2) *Autentikasi:* Pengirim pesan harus dapat diidentifikasi dengan pasti, penyusup harus dipastikan tidak bisa berpura-pura menjadi orang lain.
3) *Integritas:* Penerima pesan harus dapat memastikan bahwa pesan yang dia terima tidak dimodifikasi saat dalam proses transmisi data.
4) *Non-Repudiation:* Pengirim pesan harus tidak bisa menyangkal pesan yang dia kirimkan.

2.4. Enkripsi dan Dekripsi

Proses menyandikan plainteks menjadi chiperteks disebut enkripsi (encryption) atau enciphering (standard nama menurut ISO 7498-2) sedangkan proses mengembalikan chiperteks mejadi plainteks disebut dekripsi (decryption) atau dechiphering (standard ISO 7498-2).[6] Enkripsi adalah transformasi data dalam bentuk yang tidak dapat terbaca dengan sebuah kunci tertentu. Tujuannya adalah untuk meyakinkan privasi dengan menyembunyikan informasi dari orang-orang yang tidak ditujukan, bahkan mereka yang memiliki akses ke data terenkripsi. Sedangkan dekripsi merupakan kebalikan dari enkripsi, yaitu transformasi data terenkripsi kembali ke bentuknya semula.

Enkripsi dilakukan pada saat pengiriman dengan cara mengubah data asli menjadi data rahasia, sedangkan dekripsi dilakukan pada saat penerimaan dengan cara mengubah data rahasia menjadi data asli. Jadi data yang dikirimkan selama proses pengiriman adalah data rahasia, sehingga data asli tidak dapat diketahui oleh pihak yang tidak berkepentingan. Data asli hanya dapat diketahui oleh penerima dengan menggunakan kunci rahasia. Enkripsi dan dekripsi pada umumnya membutuhkan penggunaan sejumlah informasi rahasia, disebut sebagai kunci. Untuk beberapa mekanisme enkripsi, kunci yang sama digunakan baik untuk enkripsi dan dekripsi berbeda.



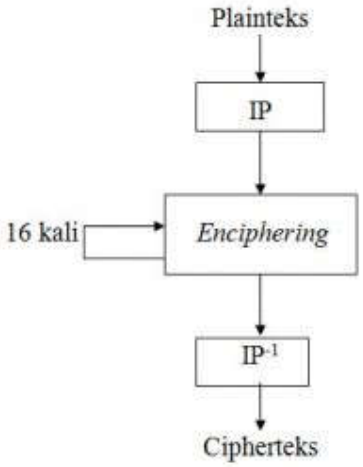
Gambar 2.1 Skenario Komunikasi Dasar Kriptografi

2.5. Algoritma Kriptografi (DES)

DES merupakan salah satu algoritma kriptografi cipher block dengan ukuran blok 64 bit dan ukuran kuncinya 56 bit. DES diadopsi dan dibakukan oleh NBS (National Bureau Standard) yang kini menjadi NIST (National Institute of Standards and Technology) pada tahun 1977 sebagai FIPS 46 (Federal Information Processing Standard). DES bermula dari hasil riset Tuchman Meyer yang diajukan sebagai kandidat Sandi Standard Nasional yang diusulkan oleh NBS. Algoritma yang dikembangkan oleh Tuchman Meyer ini merupakan algoritma terbaik dari semua kandidat Sandi Standard Nasional. Pada mulanya, algoritma yang kini disebut DES, memiliki panjang kunci sandi 128 bit. Namun selama proses pengadopsian, NBS melibatkan NSA (National Security Agency), dan algoritma sandi ini mengalami pengurangan ukuran kunci sandi dari 128 bit menjadi 56 bit saja. Sebagian orang mungkin mengira bahwa pengurangan panjang kunci sandi ini merupakan usulan NSA untuk melemahkan algoritma Tuchman Meyer karena motif politik tertentu. Entah itu untuk mempermudah penyadapan atau untuk melemahkan pengamanan informasi lawan politik. Mungkin NSA menginginkan algoritma Tuchman Meyer ini “cukup aman” untuk digunakan warga sipil, tetapi mudah dipecahkan oleh organisasi besar semisal NSA dengan peralatan canggihnya. Bila dibandingkan dengan performa komputer personal pada saat itu, algoritma sandi dengan panjang kunci 56 bit dapat dikatakan cukup aman bila digunakan oleh orang-orang “biasa”, tapi dapat dengan mudah dipecahkan dengan

peralatan canggih dan tentunya kepemilikan alat canggih ini hanya dapat dijangkau oleh organisasi elit seperti NSA.

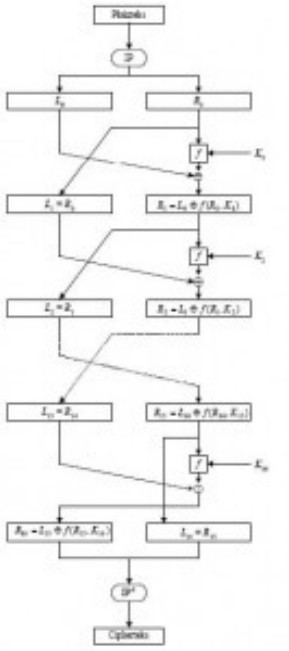
DES termasuk ke dalam sistem kriptografi simetri dan tergolong jenis *cipher* blok. DES beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci internal *(internal key)* atau upa-kunci *(subkey)*. Kunci internal dibangkitkan dari kunci eksternal *(external key)* yang panjangnya 64 bit. Skema global dari algoritma DES ditunjukkan pada gambar 2.2.



Gambar 2.2 Skema Global Algoritma DES

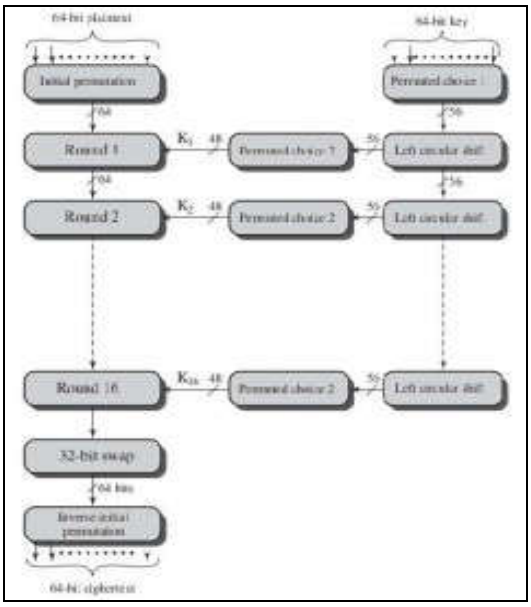
1) Blok plainteks dipermutasi dengan matriks permutasi awal (initial permutation atau IP).
2) Hasil permutasi awal kemudian di-enciphering- sebanyak 16 kali (16 putaran). Setiap putaran menggunakan kunci internal yang berbeda.
3) Hasil enciphering kemudian dipermutasi dengan matriks permutasi balikan (invers initial permutation atau IP-1) menjadi blok cipherteks.

Di dalam proses enciphering, blok plainteks terbagi menjadi dua bagian, kiri (L) dan kanan (R), yang masing-masing panjangnya 32 bit. Kedua bagian ini masuk ke dalam 16 putaran DES. Pada setiap putaran i, blok R merupakan masukan untuk fungsi transformasi yang disebut f. Pada fungsi f, blok R dikombinasikan dengan kunci internal Ki. Keluaran dai fungsi f di-XOR-kan dengan blok L untuk mendapatkan blok R yang baru. Sedangkan blok L yang baru langsung diambil dari blok R sebelumnya. Ini adalah satu putaran DES. Secara lengkap proses Enkripsi dengan menggunakan DES ditunjukan pada gambar 2.3.



Gambar 2.3 Proses Enkripsi Menggunakan DES

Algoritma DES memerlukan sebuah kunci yang panjang bloknya 64 bit di setiap blok DES digunakan untuk mengamankan data pada perangkat lunak dan keras negara tersebut. Desain input-output algoritma DES ditunjukkan pada gambar 2.4.



Gambar 2.4 Desain Input-Output Algoritma DES

Dapat dilihat bahwa ada dua input untuk fungsi enkripsi, yaitu plaintext dengan panjang 64-bit dan kunci dengan panjang 56-bit. Untuk mengenkripsi data dengan menggunakan algoritma DES, dimulai dengan membagi bit

dari teks tersebut kedalam blok-blok dengan ukuran blok sebesar 64-bit, yang kemudian disebut blok plaintext.

2.6. Eclipse Java

Eclipse merupakan komunitas open source yang bertujuan menghasilkan platform pemrograman terbuka. Eclipse terdiri dari framework yang dapat dikembangkan lebih lanjut, peralatan bantu untuk membuat dan mengatur software sejak awal hingga diluncurkan. Platform Eclipse didukung oleh ekosistem besar yang terdiri dari vendor tekonologi, start-up inovatif, universitas, riset institusi serta individu. Banyak orang mengenal Eclipse sebagai IDE (integrated development environment) untuk bahasa Java, tapi Eclipse lebih dari sekedar IDE untuk Java. Secara umum Eclipse digunakan untuk membangun software inovatif berstandar 12 industri, dan alat bantu beserta frameworknya membantu pekerjaan menjadi lebih mudah.

2.7. JDK (Java Development Kit)

JDK adalah Sun Microsystem produk ditujukan untuk pengembangan Java. Sejak diperkenalkannya Java, telah jauh SDK Java yang paling banyak digunakan. Pada Tanggal 17 November 2006, Sun mengumumkan bahwa akan dirilis dibawah GNU General Public License(GPL), sehingga membuat perangkat lunak bebas.

Java merupakan sebuah platform sekaligus bahasa pemograman tingkat tinggi yang mempunyai kriteria sederhana, berorientasi objek, terdistribusi, dinamis, aman dan lainya. Bahasa ini dikembangkan dengan model yang mirip seperti bahasa C++ dan smalltalk namun lebih mudah dipakai, dan juga memiliki platform independen yang dapat dijalankan pada sistem operasi apapun.

2.8. UML (Unified Modeling Language)

Unified Modeling Language (UML) adalah sebuah bahasa yang berdasarkan grafik atau gambar untuk menvisualisasikan, menspesifikasikan, membangun dan pendokumentasian dari sebuah sistem pengembangan perangkat lunak berbasis OO (Object Oriented)".
Berikut ini beberapa diagram yang terdapat di dalam Unified Modeling Language (UML), yaitu :

1) Diagram use case (use case diagram)

use case sebagai urutan langkah-langkah yang secara tindakan saling terkait (skenario), baik terotomatisasi maupun secara manual, untuk tujuan melengkapi satu tugas bisnis tunggal". Use case digambarkan dalam bentuk ellips/oval.
Elemen use case terdiri dari :

a) Aktor (Actor)
b) Use case
c) Asosiasi (Association)
d) Include
e) Extend
f) Generalization

2) Diagram Aktivitas (Activity Diagram)

Diagram aktivitas menggambarkan aktivitas yang dipicu oleh kejadian-kejadian diluar seperti pemesanan atau kejadian-kejadian internal misalnya proses penggajian setiap hari Jumat sore.

3) Diagram Sekuansial (Sequence Diagram)

Diagram Sequence adalah diagram interaksi yang menekankan pada pengiriman pesan dalam suatu waktu tertentu.

4) Diagram Kelas (Class Diagram)

Diagram Kelas sebagai satu set objek yang memiliki atribut dan perilaku yang sama. Diagram Kelas memiliki apa yang disebut atribut dan metode atau operasi. Atribut merupakan variabel-variabel yang dimiliki oleh suatu kelas dan operasi atau metode adalah fungsi-fungsi yang dimiliki oleh suatu kelas. Class menggambarkan keadaan (atribut atau properti) suatu sistem, sekaligus menawarkan layanan untuk manipulasi keadaan tersebut (metode atau fungsi). Atribut adalah rincian suatu Class misalnya warna mobil, jumlah sisi suatu bentuk dan sebagainya. Class memiliki tiga area pokok, yaitu:

- Nama
- Atribut
- Operasi

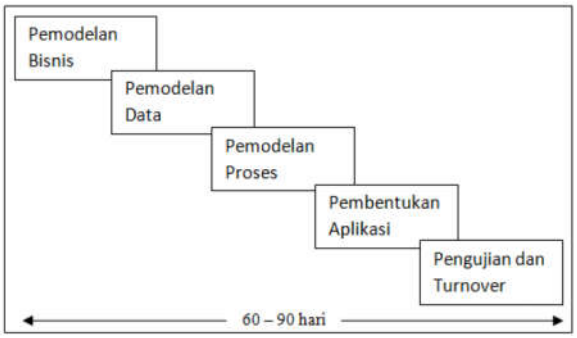
III . METODE PENELITIAN DAN KEBUTUHAN

3.1. Metode Penelitian

1) Metode Pengumpulan Data*:* Data yang dikumpulkan dalam penelitian ini merupakan data sekunder. Data diperoleh dari telaah pustaka dan dokumen yang didapat penulis dari pustaka yang mendukung, informasi dari internet, buku-buku dan artikel dari jurnal.

2) Metode Pengembangan Sistem*:* Agar mempermudah dalam pengembangan sistem, maka penulis membangun sebuah sistem yang akan membantu dalam menggambarkan proses penyelesaian masalah. Metode yang sesuai dalam pengembangan sistem ini adalah metode Rapid Aplication Development (RAD). RAD adalah sebuah model proses perkembangan software sekuensial linier yang menekankan siklus perkembangan yang sangat pendek. Model ini adalah sebuah adaptasi "kecepatan tinggi" dari model sekuensial linear di mana perkembangan cepat dicapai dengan menggunakan pendekatan kontruksi berbasis komponen.

3) Fase-fase Pengembangan Sistem*:* Metode RAD digunakan pada aplikasi sistem konstruksi, maka menekankan fase-fase seperti yang ditunjukkan pada gambar 3.1.



Gambar 3.1 Fase-fase RAD

3.2. Kebutuhan

1) Kebutuhan Perangkat Lunak Kebutuhan Fungsional*:* Aplikasi ini diharapkan dapat memenuhi kebutuhan fungsional untuk melakukan fungsi kriptographi dan steganografi, diantaranya adalah :

a) Dapat memberikan kemudahan kepada *user* untuk menggunakan aplikasi kriptographi dan steganografi audio.
b) Dapat meningkatkan keamanan data dengan cara menyisipkan informasi yang di enkripsi pada media audio melalui aplikasi steganografi audio.

2) Kebutuhan Antarmuka

Kebutuhan antarmuka merupakan kebutuhan yang sangat penting, karena perangkat lunak dinilai dari external performance yaitu tampilan luar yang disesuaikan dengan kebiasaan pengguna komputer, agar mudah digunakan dan mudah diadapatsi oleh pengguna karena sudah familiar. Kebutuhan ini diharapkan dapat disesuaikan oleh kebiasaan pengguna, hal ini dimaksudkan untuk mempermudah pekerjaan karena pengguna sudah terbiasa dengan tampilan yang biasa digunakan.

3) Kebutuhan Unjuk Kerja

Unjuk kerja aplikasi ini adalah sebagai berikut:

a) Kualitas lingkungan pengembangan program
b) Kecepatan transfer data
c) Kekuatan bahasa pemograman dibandingkan kompleksitasnya
d) Flexibilitas penggunaannya
e) Reusable

IV. PERANCANGAN DAN IMPLEMENTASI

4.1. Unit Bahasa Pemodelan

1) Use Case Diagram

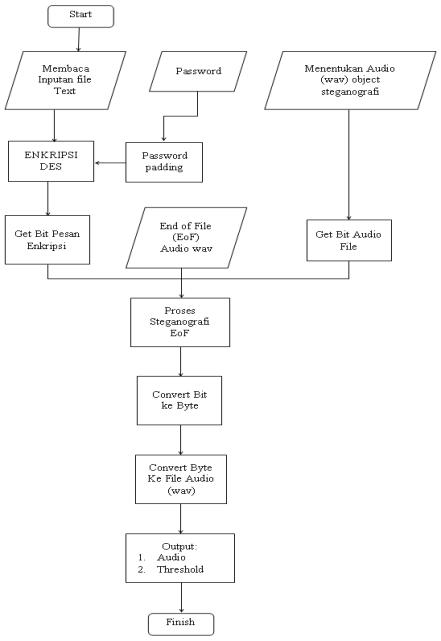
Dalam bahasa pemodelan ini, penulis menggunakan 2 (dua) buah aktor yaitu pengirim dan penerima seperti yang ditunjukkan pada gambar 4.1. Aktor tersebut mempunyai karakteristik yang berbeda dalam hal menggunakan aplikasi dan menggunakan file yang telah di proses. Pengirim adalah seseorang yang nantinya akan mengirimkan sebuah file yang sudah disisipkan pesan yang sudah dienkripsi. Penerima adalah seseorang yang akan menerima file yang dikirimkan oleh pengirim. Penerima bertugas untuk membuka file yang telah dikirimkan tersebut kemudian didekripsi dan dipisahkan dengan file yang dikirim sebelumnya dan pesan yang ada didalam file tersebut.

Use-case :
 Proses Kripto dan Stego
Primary actor :
 Pengirim
Goal :
 File berhasil disembunyikan
Precondition :
 Memasukkan nama file audio tempat pesan tersembunyi
 Memasukkan pesan yang akan disisipkan
 Memasukkan kata sandi/kata kunci
Trigger :
 Pengirim ingin menyembunyikan file
Scenario:
1. Pengirim membuka aplikasi Steganographer.
2. Pengirim memasukkan file audio yang akan digunakan sebagai media pembawa.
3. Pengirim memasukkan nama file untuk tempat file disembunyikan.
4. Pengirim menuliskan pesan yang akan disisipkan.
5. Pengirim memberikan kata kunci sebagai pelengkap sandi.
6. Pengirim menekan tombol Stego untuk memprosesnya.

Alternate Flow :
 Pengirim keluar dari aplikasi
Priority :
 Moderate priority
Frequency of use :
 Frequent

Gambar 4.1 Skenario Enkripsi dan Pengiriman Pesan

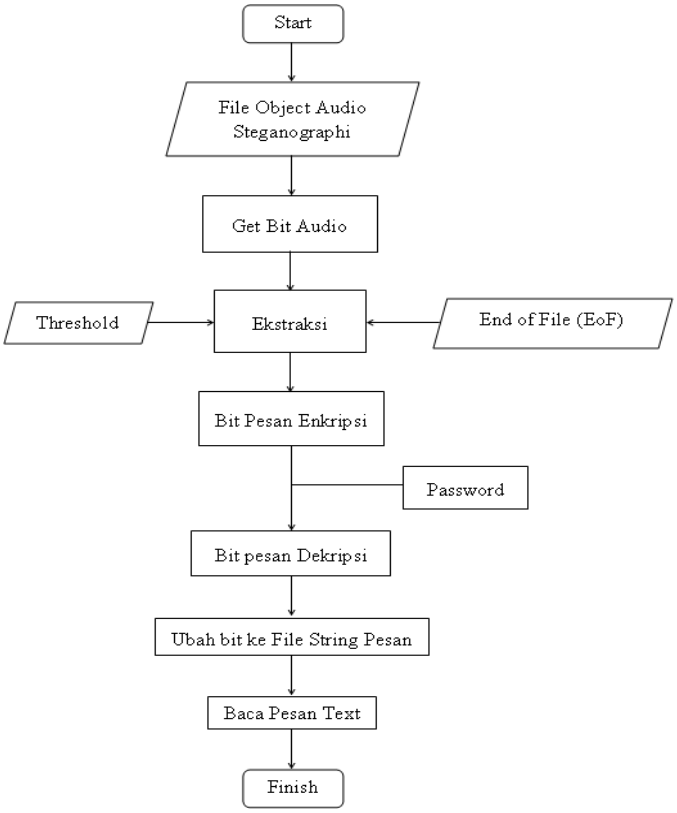
Pesan yang akan digunakan sebagai input adalah pesan text. Pesan text ini kemudian akan di enkripsi terlebih dahulu menggunakan metode DES. Hasil enkripsi selanjutnya akan disembunyikan ke media audio menggunakan metode End of File. Output dari proses ini dalah file audio yang menjadi objek stegano dan threshold. Threshold merupakan panjang bit pesan yang di enkripsi untuk digunakan pada proses ekstraksi pada proses selanjutnya. Desain perangkat lunak untuk enkripsi dan penyembunyian pesan ditunjukkan pada gambar 4.2.



Gambar 4.2. Skema Enkripsi dan penyembunyian pesan

Use-case :
 Proses Unkripto dan Unstego
Primary actor :
 Penerima
Goal :
 Mengembalikan File yang tersembunyi
Precondition :
 Memasukkan nama file hasil Stego untuk dikembalikan seperti semula
 Memasukkan kata sandi/kata kunci
Trigger :
 Penerima ingin mengembalikan file yang disembunyikan
Scenario :
1 Penerima membuka aplikasi Steganographer.
2 Penerima memasukkan nama file yang disembunyikan.
3 Penerima memberikan kata kunci sebagai pelengkap sandi.
4 Penerima menekan tombol Unstego untuk memprosesnya.
Alternate Flow :
 Penerima keluar dari aplikasi
Priority :
 Moderate priority
Frequency of use :
 Frequent

Gambar 4.3. Skenario Ekstrasi dan dekripsi Pesan

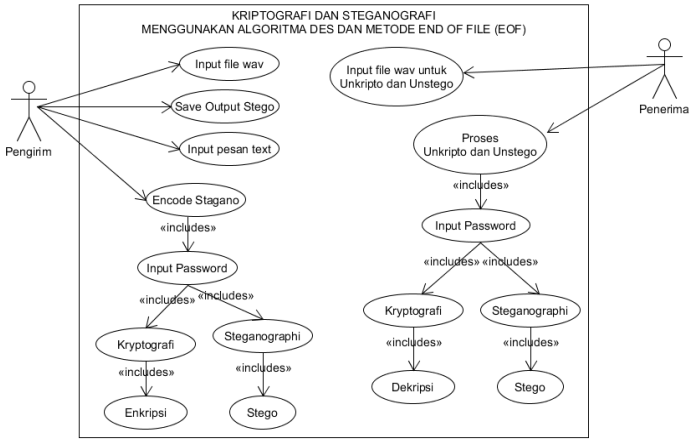


Gambar 4.4 Skema ekstraksi dan dekripsi pesan

Setelah di enkripsi dan disembunyikan tentunya pesan harus dapat di dapatkan lagi dari objek media steganografi. Objek steganografi di ekstraksi menggunakan metode End of File untuk mendapatkan pesan yang telah di enkripsi. Setelah didapatkan pesan enkripsi maka akan dilakukan proses dekripsi menggunakan metode DES. Desain perangkat lunak untuk ekstraksi dan dekripsi pesan ditunjukkan pada gambar 4.3 dan gambar 4.4

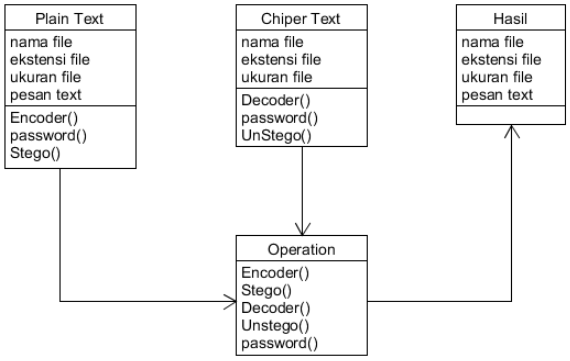
2) Use case Diagram Aplikasi Kripto Grafi dan Stegano Grafi

Setelah proses skema enkripsi dan dekripsi, selanjutnya adalah desai sistem secara keseluruhan yang akan dibuat :



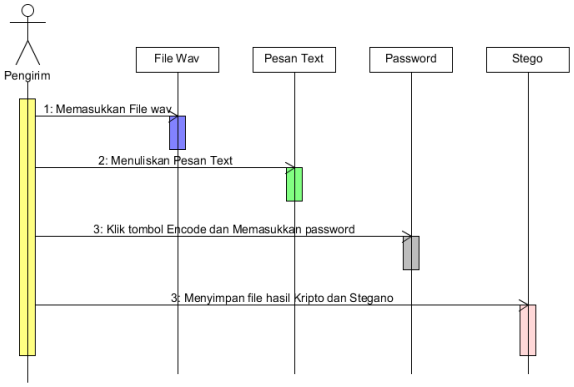
Gambar 4.5 Use case Diagram Aplikasi Kripto Grafi dan Stegano Grafi

3) Class Diagram Diagram Aplikasi Kripto Grafi dan Stegano Grafi

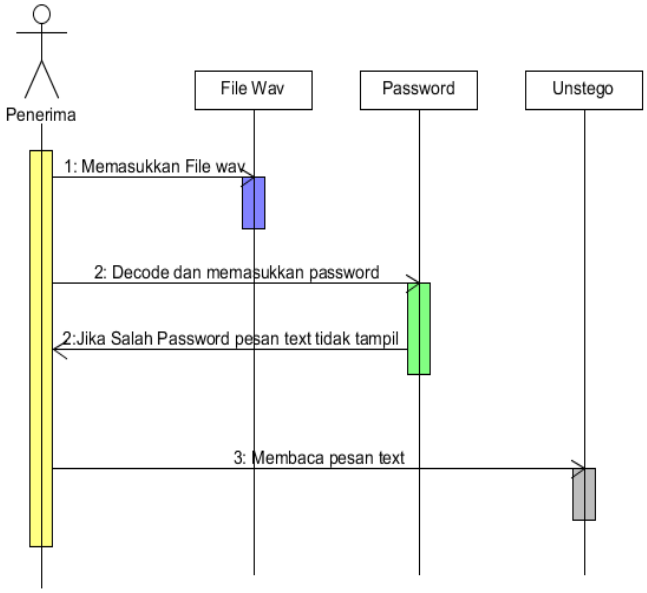


Gambar 4.6 Class Diagram Aplikasi Kripto Grafi dan Stegano Grafi

4) Sequence diagram



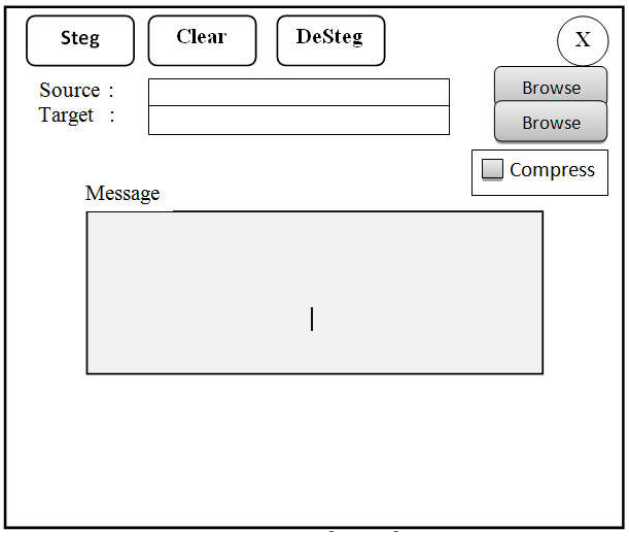
Gambar 4.7. Sequence Diagram Aplikasi Pengiriman Pesan



Gambar 4.8 Sequence Diagram Penerima Pesan

4.2. Input Output (I/O)

Dalam pembuatan pada aplikasi yang penulis buat menggunakan perangkat lunak berupa Java Eclipse. Di bawah ini merupakan desain input output yang ditunjukkan pada gambar 4.9. Sedangkan implementasi form input output ditunjukkan pada gambar 4.10.



Gambar 4.9 Desain Input dan Ouput

Gambar 4.10 Form Input Output

4.3. Pengujian Program (Testing)

Hasil perancangan akhir dari Aplikasi Kriptografi dan Steganografi ini telah diujikan. Metode pengujian yang penulis gunakan adalah Graphical User Interface dan tanggapan atau respon dari user

1) Pengujian Graphical User Interface (GUI) / Black Box Testing

   Pengujian Graphical User Interface (GUI) untuk aplikasi ini dilakukan dengan menguji melalui beberapa aspek seperti ditunjukkan pada tabel 4.1.

Tabel 4.1. Tabel Pengujian GUI / Black Box Testing

No	Aspek Pengujian
1	Apakah semua menu dapat dituju / diklik/ disorot secara tepat oleh pointer mouse ?
2	Apakah setiap operasi mouse dikenali dengan baik oleh aplikasi yang akan meresponnya?

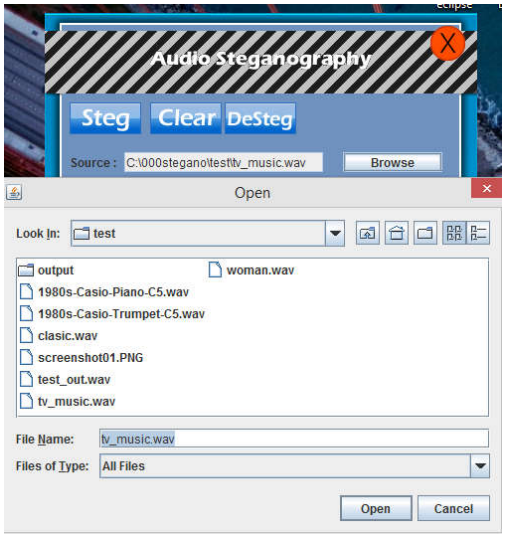
Berdasarkan hasil pengujian, dapat diperoleh kesimpulan bahwa performansi program cukup baik. Semua rancangan program telah tersusun dalam menu dengan tepat dan setiap kontrol yang terdapat dalam tiap – tiap menu juga dapat diakses secara tepat. Mouse dengan mudah dapat mengakses tiap menu dalam program secara tepat pula memberikan respon sesuai dengan konteks interaktifnya.

2) Pengujian input output program

a. Menjalankan program

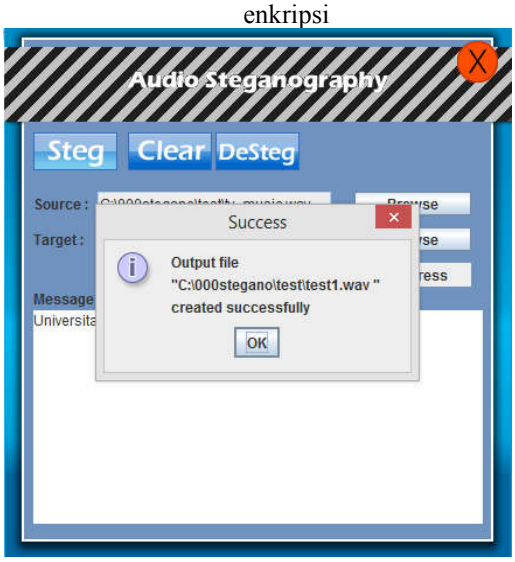
Gambar 4.11 Pengujian Form Input Output

b. Browser memilih file audio induk



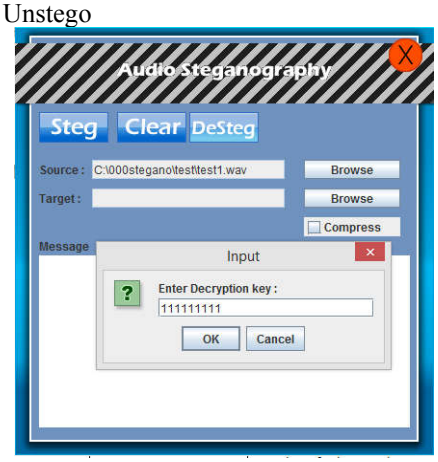
Gambar 4.12 Pengujian Form Input Output Pemilihan File Audio

Gambar 4.13 Pengujian Form Input Proses Stegano dan enkripsi



Gambar 4.14 Pengujian Form Output Proses Stegano

c. Proses Unstego

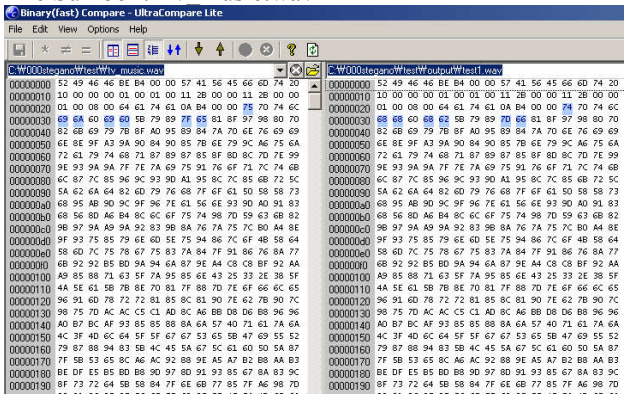


Gambar 4.15. Pengujian Form Input Proses Unstegano

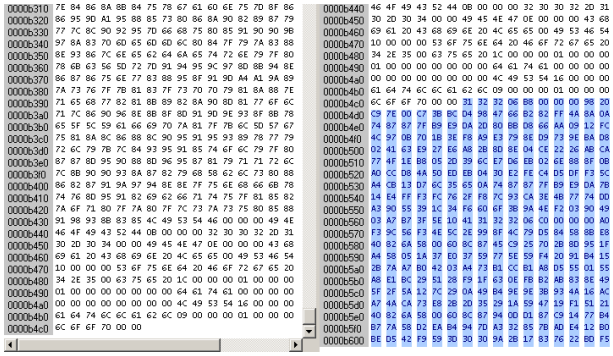
Gambar 4.16 Pengujian Form Output Proses Unstegano

d. Perbandingan Data Binary

File Sumber : Tv_music.wav



File stego : Test1.wav



Gambar 20 Perbandingan data binary File Sumber dan file stego Tv_music.wav dengan Test1.wav

V. PENUTUP

5.1. Kesimpulan

Dari hasil perancangan dan pembuatan program aplikasi kriptografi dengan menggunakan algoritma DES dan Steganografi dengan metode End of File (EoF) ini, dapat diambil kesimpulan sebagai berikut :

1. Dari hasil percobaan yang telah dilakukan membuktikan bahwa aplikasi dapat mengacak dan menyembunyikan file dengan aman dan tidak menimbulkan kecurigaan pada pihak lain. Pada file hasil kriptografi dan steganografi tidak menimbulkan efek yang dapat merusak ataupun mengganggu kinerja file sebelumnya.
2. Hasil akhir yang diperoleh dari penggabungan 2 buah file yang berbeda ekstensi menghasilkan ukuran yang lebih besar yaitu merupakan gabungan dari ukuran kedua buah file tersebut yang dikarenakan file yang disembunyikan juga mempunyai kapasitas ukuran file sendiri.

5.2. Saran

Saran-saran yang berguna untuk pengembangan sistem dan aplikasi ini adalah sebagai berikut :

1. Dalam penggunaan aplikasi ini disarankan untuk menggunakan file sesuai kebutuhan dan disesuaikan dengan hardware pada computer pengguna karena makin besar ukuran file, makin tinggi kinerja pada komputer anda.
2. File audio yang digunakan dalam stegano sebaiknya menggunakan Waveform Audio Format (WAV).

Referensi

[1] Utami, Ema dan Sukrisno. Implementasi Steganografi EoF dengan Gabungan Ekripsi Rijndael, Shift Chiper dan Fungsi Hash. Yogyakarta. 2007

[2] Anonimous, ASCII table and Extended ASCII Table, www.asciitable.com,10 Agustus 2009

[3] Stallings, Williams, Cryptography and Network Security : Principles and Practices, 2nd edition, Upper Saddle River : Prentice Hall Inc., 1995

[4] Stallings, Williams, Cryptography and Network Security : Principles and Practices, 4th edition, Upper Saddle River : Prentice Hall Inc., 2006

[5] Munir, Rinaldi. Kriptografi. Bandung : Informatika. 2006.

[6] Rizqi Firmansyah, Wahyu Suadi. Implementasi Kriptografi dan Steganografi pada media gambar dengan menggunakan metode DES dan Region-embed data density. ITS-Surabaya : informatika its; 2011.

[7] Munir, Rinaldi. 2004. *Kriptografi.* Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung.

[8] Herianto. Pembangunan Perangkat Lunak Steganografi Audio MP3 dengan Teknik Parity Coding pada Perangkat Mobile Phone. ITB-bandung: informatika itb; 2008

[9] Wijaya, Ermadi Satriya. 2009. "*Konsep Hidden Message Menggunakan Teknik Steganografi*".
[10] Yoga bagus Perkhasa, Wahyu Suadi, Baskoro Adi Pratomo Implementasi Kriptografi dan Steganografi pada File Audio Menggunakan Metode DES dan Parity Coding.ITS-Surabaya:informatika its,2012