APLIKASI KEAMANAN DATA DENGAN MENGGUNAKAN METODA ENKRIPSI DAN AUDIO STEGANOGRAFI

Ni Nyoman Emang Smrti
Jurusan Sistem Informasi - STMIK Bandung Bali
Jl. Tukad Unda No. 8 Denpasar
Telp. : 0361-7475740, Fax.: 0361-222917, e-mail : smrti_nyoman@yahoo.com

Abstraksi : Kriptografi dengan cara mengenkripsi data dengan logika tertentu. Steganografi adalah suatu ilmu yang mempelajari cara menyembunyikan informasi di dalam sebuah pesan. Audio steganografi merupakan perkembangan ilmu dari steganografi yaitu menyembunyikan pesan pada suara. Program aplikasi keamanan data ini dibuat dengan menggabungkan kemampuan kriptografi dan audio steganografi.

Kata kunci : enkripsi, audio steganografi

Data Security Application by Using Encryption and Audio Steganography Method

Abstract : *Cryptography is the science which studies how to hide information by encrypting data with a certain logic. Steganography is a science which studies how to hide information in a message. Audio steganography is the science of steganography is to hide messages in the voice. Data security application program is made by combining the capabilities and audio steganography cryptography.*

Keyword : *encryption, audio steganography*

I. PENDAHULUAN

Kriptografi adalah ilmu yang mempelajari cara menyembunyikan informasi dengan cara mengenkripsi data dengan logika tertentu. Menyembunyikan data dengan cara mengenkripsi ini, memancing orang untuk mencoba membuka (dekripsi). Bila logika enkripsi dan kunci rahasianya sudah didapatkan, maka orang yang tidak berhak akan dapat membacanya.

Steganografi adalah suatu ilmu yang mempelajari cara menyembunyikan informasi di dalam sebuah pesan. Audio steganografi merupakan perkembangan ilmu dari steganografi. Audio steganografi mempunyai kesulitan yang lebih dibandingkan pada steganografi pada gambar atau pada video karena pendengaran manusia lebih peka daripada penglihatan manusia, sehingga pada proses penyisipan data harus dibuat sebaik mungkin agar suara yang telah disisipi data terdengar sama dengan suara sebelum disisipi data.

Di era informasi ini, pertukaran data sangatlah banyak, untuk mengantisipasi supaya data

yang sifatnya rahasia tidak terbaca oleh yang tidak berhak diperlukan sistem keamanan. Dalam penelitian ini akan di buat program aplikasi yang menggabungkan kemampuan kriptografi dan audio steganografi.

II. METODOLOGI PENELITIAN

1. Deskripsi masalah

Dalam pengamanan data, ada beberapa metoda yang digunakan. Masing-masing metoda memiliki kelemahan dan kelebihan. Metoda enkripsi, memiliki kelemahan yaitu orang lain akan tahu bahwa data tersebut dienkripsi, karena data yang telah dienkripsi akan mengalami perubahan (tidak dapat dibaca). Apabila ada orang jahat dan menginginkan data tersebut, maka orang tersebut akan mencoba untuk menjebol kunci rahasia, walaupun cara ini tidak mudah dilakukan oleh orang-orang awam. Dari kelemahan ini, data yang telah dienkripsi disembunyikan ke dalam data suara. Dengan harapan orang tidak menyangka kalau di dalam data suara (lagu) disisipi data penting. Metoda yang dipakai dalam aplikasi ini adalah menggabungkan metoda enkripsi RC4 dan Audio steganografi End of File.

2. Tujuan yang dicapai

a. Menyembunyikan data dalam audio dan sebelum disembunyikan datanya akan dienkripsi terlebih dahulu.
b. Dengan menggabungkan dua metoda ini di harapkan data yang akan dikirim akan lebih aman.

III. PEMBAHASAN

1. Pengertian Steganografi

Steganografi adalah suatu teknik untuk menyembunyikan informasi yang bersifat pribadi dengan sesuatu yang hasilnya akan tampak seperti informasi normal lainnya. Media yang digunakan umumnya merupakan suatu media yang berbeda dengan media pembawa informasi rahasia, disinilah fungsi dari teknik steganografi yaitu sebagai teknik penyemaran menggunakan media lain yang berbeda sehingga informasi rahasia dalam media awal tidak terlihat secara jelas (Waheed, 2000).

Steganografi biasanya sering disalahkaprahakan dengan kriptografi karenanya keduanya sama-sama bertujuan untuk melindungi informasi yang berharga. Perbedaan yang mendasar antara keduanya yaitu steganografi berhubungan dengan informasi tersembunyi sehingga tampak seperti tidak ada informasi tersembunyi sama sekali. Jika seseorang mengamati objek yang menyimpan informasi tersembunyi tersebut, ia tidak akan menyangka bahwa terdapat pesan rahasia dalam objek tersebut, dan karenanya ia tidak akan berusaha memecahkan informasi (depkripsi) dari objek tersebut.

Steganografi di dunia modern biasanya mengacu pada informasi atau suatu arsip yang telah disembunyikan ke dalam suatu arsip citra digital, audio atau video. Teknik Steganography

ini telah banyak digunakan dalam strategi peperangan dan pengiriman sandi rahasia sejak jaman dahulu kala. Dalam perang Dunia II, teknik steganografi umum digunkan oleh tentara Jerman dalam mengirikan pesan rahasia dari atau menuju Jerman (Simmons, 1983).

2 Dasar Kriptografi

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Menurut Bruce Scheiner dalam bukunya "Applied Cryptography", kriptografi adalah ilmu pengetahuan dan seni menjaga message-message agar tetap aman (secure).

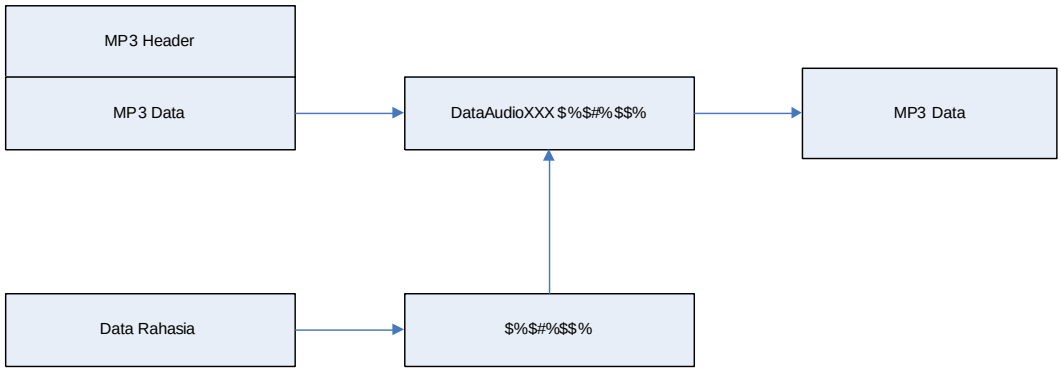
Konsep kriptografi sendiri telah lama digunakan oleh manusia misalnya pada peradaban Mesir dan Romawi walau masih sangant sederhana. Prinsip-prinsip yang mendasari kriptorgafi

- *Confidelity* (kerahasiaan) yaitu layana agar isi pesan yang dikirmakan tetap rahasia dan tidak diketahui oleh pihak lain (kecuali pihak pengirim, pihak penerima atau pihak-pihak memiliki ijin). Umumnya hal ini dilakukan dengan cara membuat suatu algoritma matematis yang mampu mengubah data hingga menjadi sulit untuk dibaca dan dipahami.
- Data integrity (keutuhan data) yaitu layanan yang mampumengenali/mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan) data yang tidak sah oleh pihak lain.
- Authentication (keotentikan) yaitu layana yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang telibat dalam pengiriman data maupun otentikasi keaslian data/informasi.
- Non-repudiation (anti-penyangkalan) yaitu layana yang dapat mencegah suatu pihak untuk menyakal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dari dirinya)

Berbeda dengan kriptografi kalsik yang menitikberakan kekuatan pada kerahasiaan algoritma yang digunakan yang artinya apabila algoritma yang digunakan telah diketahui maka pesan sudah jelas "bocor" dan dapat diketahui isinya oleh siapa saja yang mengetahui algoritma tersebut. Kriptografi modern lebih menitikberatkan pada kerahasiaan kunci yang digunakan pada algoritma tersebut (oleh pemakainya) sehingga algoritma tersebut dapat saja disebarkan ke kalangan masyarakat tanpa takut kehilangan kerahasiaan bagi para pemakainya.

3 Teknik Steganogrphy End Of File

Teknik End Of File (EOF) merupakan salah satu teknik yang digunakan dalam steganogrfi. Teknik ini menggunakan cara menyisipkan data pada akhir file. Ukuran file yang telah disisipi sama dengan ukuran file yang belum disisipi data. Data disimpan pada akhir file dengan diberi tanda khusus sebagai pengenal start dari data tersebut dan pengenal akhir dari data Audio tersebut.



Gambar 1 teknik enf of file

Langkah-langkah melakukan penyebunyian data:

1. Input file yang akan disembunyikan
2. Input file audio MP3 yang akan digunakan untuk menyisipkan data.
3. File temporary akan dibuatkan oleh sistem
4. File audio MP3 carrier dibuatkan header dan data audio MP3 di tulis pada file audio MP3 carrier.
5. Open file audio MP3 carrier dan read data audio sampai data paling terakhir, diberikan penanda berapa string “XXXX”.

3. Metoda Enkripsi RC4

Metoda enkripsi RC4 merupakan salah satu jenis Stram chiper yang di desain oleh Ron Riverst di laboratrium RSA pada tahun 1987. RCA sendiri merupakan kepanjangan dari Ron Code atau Riverst's Chiper. RC4 merupakan salah satu algoritma kunci simetris yang berbentuk stream cipher. Algoritma ini ditemukan pada tahun 1987 olrh Ronald Riverst dan menjadi simbol keamanan RSA. Algoritma sesungguhnya tidak dipatenkan oleh RSA DSI, hanya saja tidk diperdagangkan secara bebas sampai sekarang. Namun pada bulan september 1994 ada seseorang yang merimakan sebuah source code yang diyakini sebagai RC4 ke mailinglist cypherpunks dan keberadaannyapun langsung tersebar. Karena algoritma yang dipublikasikan ini sangat identik dengan implementasi RC4 pada produk resmi.

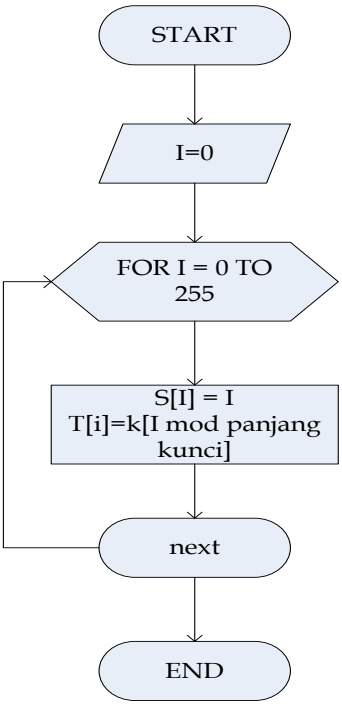
Algoritma RC4 Straem Cipher cukup mudah untuk dijelaskan. Kunci yang panjangnya bebas antara 1 sampai 256 byte digunakan untuk menginisialisasikan 256 bit S-Box, dengan elemen S[0], S[1], …, S[255]. Untuk enkripsi dan dekripsi, satu byte K dihasilkan melalui S-box dengan menyeleksi satu dari 255 secara sistematis. Jika nilai dari K telah dihasilkan, maka S-box akan dipermutasi lagi.

Inisialisasi S-box

Pada awalnya, isi dari S-box diisi dengan nilai dari 0 hingga 255 secara berurutan. Ini berarti S[0]=0, S[1]=1, … , S[255]=255. Sebuah vektor sementara, T, selalu dibuat. Jika panjang kunci K adalah 256 bytes, maka K akan langsung dimuat ke dalam T. Jika tidak K akan diisi secara berulang-ulang hingga T penuh. Operasi tersebut dapat dirumuskan sebagai berikut:

For I = 0 to 255 di

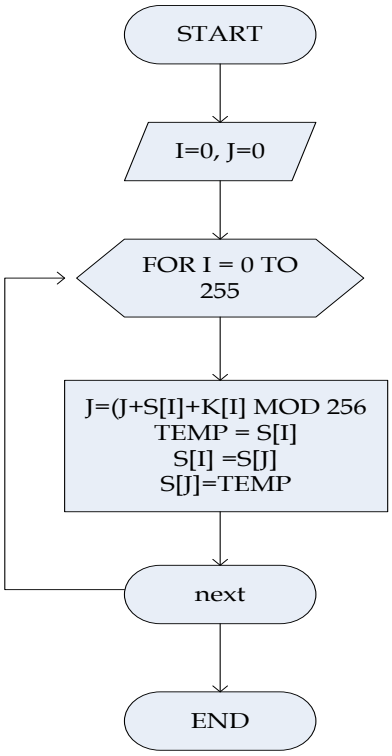
s[i] = I;
T[i] = K[i mod panjang kunci];



Gambar 2. Flowchart inisialisasi S-Box

Selanjutnya digunakan T untuk melakukan permutasi inisial s-Box yang meliputi S[0] hingg S[255]. Untuk setiap S[i] akan saling bertukar dengan byte S[i] yang lainnya pada S-box sesuai dengan skema yang ditentukan oleh T[i].

j=0
for I = 0 to 255 do
    j = (j + s[i] +T[i]) mod 256
    swap (S[i],S[j])



Gambar 3. Flowchart Permutasi S-Box

Karena hanya melakukan pertukaran pada S-Box, maka hanya terjadi permutasi. S-Box tetap berisi angka antara 0 hingga 255.

Pembangkit Stream

Setalah S-Box diinisialisasi, kunci yang dimaksukan tidak lagi digunakan. Pembangkitan stram melibatkan S[0] hingga S[255]. Untuk setiap S[i] akan saling bertukar dengan byte S[i] yang lainnya pada S-box sesuai dengan skema yang ditentukan oleh konfigurasi S-Box yang sekarang. Setelah mencapai S[255], proses dilajutkan dengan mengulang kembali dari S[0]

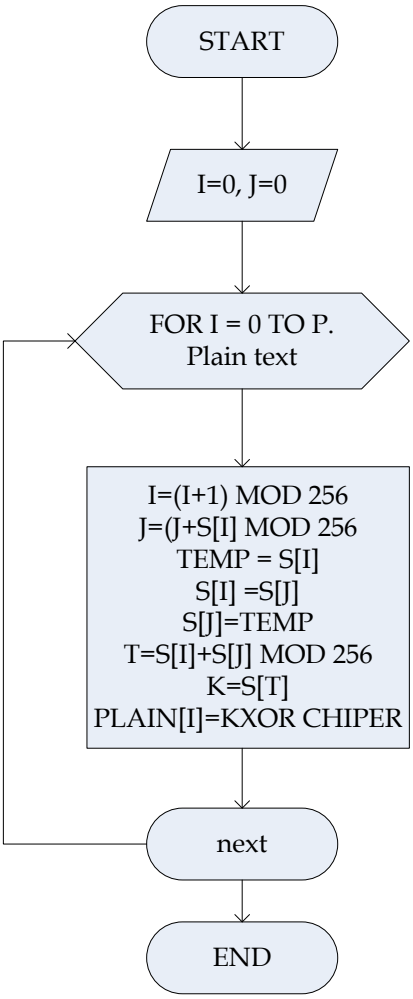
```
I,j = 0
for I = 0 to 255 do
        I = (I + 1) mod 256;
        j = (j + S[i] mod 256;
swap (S[i],S[j] mod 256
k = S[t]
```

Untuk melakukan enkripsi, XOR nilai K dengan byte selajutnya dari plaintext. Untuk melakukan dekripsi, XOR nilai K dengan byte selanjutnya dari ciphertext.

Pada metoda ini, proses dekripsinya akan berjalan sama dengan proses enkripsinya sehingga hanya ada satu fungsi yang dijalankan untuk kedua proses tersebut. Langkah-langkah proses

enkripsi:

1. User memasukkan secret key yang akan digunakan dalam proses enkripsi maupun dekripsi
2. Lakukan proses inisialisasi awal
3. S-Box berdasarkan indeks
4. Simpan secret key yang telah dimasukkan user dalam array 256 byte secara berulang sampai array terisi penuh.
5. Bangkitkan nilai pseudorandom berdasarkan nilai key sequence.
6. Lakukan proses permutasi/transposisi nilai dalam S-Box selama 256 kali.
7. Bangkitkan nilai pseudorandom key byte stream berdasarkan indeks dan nilai S-Box.
8. Lakukan operasi XOR antara palintext/chipertext dan pseudorandom key byte stream untuk menghasilkan ciphertext/plaintext

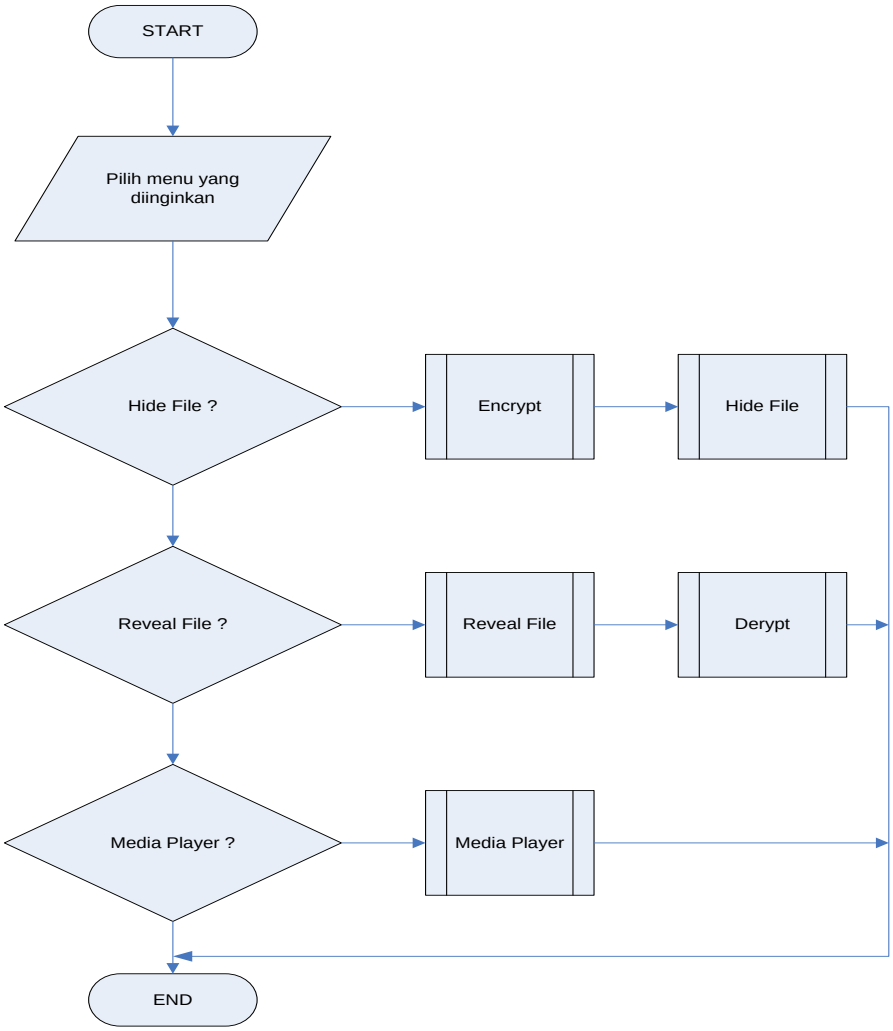


Gambar 4. Flowchart Dekripsi

Rancangan menu aplikasi keamanan data

Aplikasi ini terdiri dari 3 menu utama yaitu:

1. Menu Hide File berfungsi untuk meng-encrypt data dan sekaligus untuk menyembunyikan file kedalam audio (MP3)
2. Menu Reveal File berfungi untuk mengeluarkan data dari audio (MP3) serta men-decrypt, sehingga data dapat dibaca bagi yang memerlukan
3. Media Player berfungsi untuk mencoba file yang telah di steganografi



Gambar 5. Rancangan Menu

4. KESIMPULAN

a. Teknik steganografi mampu menutupi kekurangan yang masih terdapat pada kriptografi sehingga file yang membawa data rahasia mampu samapi ketujuannya tanpa di ketahui oleh orang yang tidak berhak

b. Teknik kriptografi dengan menggunakan metoda RC4 mampu mempertahankan kualitas data rahasia tidak rusak sampai ke tujuannya.
c. Teknik steganography End Of File mampu memperhankan ukuran data rahasia dan file audio carrier tidak mengalami perubahan maupun kualitas suaranya.

DAFTAR PUSTAKA

Al-Bahra bin Ladjamuddin. B, 2006, Rekayasa Perangka Lunak, Penerbit Graha Ilmu Yogyakarta, Yogyakarta.

Sommerville, Ian, 2000, Software Engineering 6th Editon, Addison Wesley Pub Co.

Stallings, William, Cryptography and Network Security Principles And Practice, 3rd Edition, Upper Saddle River, Pretice Hall, 2003.