

APLIKASI KRIPTOGRAFI UNTUK PERTUKARAN PESAN MENGGUNAKAN TEKNIK STEGANOGRAFI DAN ALGORITMA AES

Kunjung Wahyudi ¹⁾, Parasian DP. Silitonga ²⁾

Jurusan T. Informatika Fakultas Teknologi Informasi

Institut Teknologi Adhi Tama Surabaya

Jl. Arief Rachman Hakim No. 100 Surabaya Telp. (031) 5945043

E-mail : kunjungw@yahoo.com, kunjungw@gmail.com

Abstrak

Di era informasi abad ini, pertukaran data menjadi hal sangat penting dalam dunia informasi itu sendiri. Pertukaran data dapat juga disamakan dengan transaksi jual beli, dimana di dalamnya mempunyai banyak sekali informasi yang bersifat rahasia antara pengirim dan penerima. Tentunya hal ini berdampak pada permintaan dari sektor-sektor privat sebagai sarana untuk melindungi informasi dalam bentuk digital dan untuk menyediakan layanan keamanan. Maka diperlukan aplikasi kriptografi untuk menjaga kerahasiaan informasi tersebut. Kriptografi memiliki cabang ilmu yang sangat luas, salah satunya adalah teknik Steganografi. Dalam hal ini steganografi digunakan untuk menyembunyikan pesan yang sifatnya rahasia ke dalam media gambar secara digital. Dan untuk menambah kekuatan dalam melindungi kerahasiaan pesan tersebut perlu dikombinasikan dengan penggunaan algoritma enkripsi. Saat ini banyak sekali bermunculan algoritma-algoritma enkripsi yang tentunya mereka telah memiliki keunggulannya masing-masing. Sebut saja algoritma Rijndael (standart AES) yang memiliki fleksibilitas yang sangat tinggi, baik dalam hal kesederhanaan maupun kecepatannya. Kombinasi dari teknik steganografi dan algoritma AES ini diharapkan mampu memenuhi kebutuhan dari dua aspek keamanan informasi, yaitu perlindungan terhadap kerahasiaan informasi dan perlindungan terhadap pemalsuan dan perubahan informasi yang tidak diinginkan.

Kata kunci : Kriptografi, Steganografi, Algoritma AES

PENDAHULUAN

Internet telah membuat komunikasi semakin terbuka dan pertukaran informasi juga semakin cepat melewati batas-batas negara dan budaya. Namun tidak semua perkembangan teknologi informasi dan komunikasi ini memberikan dampak yang menguntungkan bagi dunia komunikasi.

Suatu komunikasi data jarak jauh belum tentu memiliki jalur transmisi yang aman dari berbagai kemungkinan, sehingga keamanan informasi menjadi bagian penting dalam dunia informasi itu sendiri. Hal ini berdampak pada permintaan dari sektor-sektor privat sebagai sarana untuk melindungi informasi dalam bentuk digital dan untuk menyediakan layanan keamanan.

Telah banyak dilakukan penelitian dalam upaya mengamankan suatu pesan atau informasi penting dengan menggunakan sistem kriptografi yang melakukan enkripsi sebelum pesan atau informasi tersebut ditransmisikan. Tindakan pengamanan menggunakan cara tersebut ternyata dianggap belum

cukup dalam mengamankan suatu pesan atau informasi karena adanya peningkatan kemampuan komputasi. Dari sinilah timbul suatu usaha untuk mengembangkan sistem yang mampu mendukung kebutuhan dari dua aspek keamanan informasi, yaitu secrecy (perlindungan terhadap kerahasiaan data informasi) dan authenticity (perlindungan terhadap pemalsuan dan perubahan informasi yang tidak diinginkan).

Tujuan

Tujuan dari penelitian ini adalah:

- Untuk membuat suatu perangkat lunak yang dapat melindungi pesan rahasia dengan menggunakan teknik stegano-grafi dan algoritma AES. Dengan demikian pesan tidak dapat terbaca apabila jatuh ke tangan orang yang tidak berhak.
- Untuk membuat suatu perangkat lunak yang dapat menyamarkan pesan text ke dalam bentuk lain, dalam hal ini adalah file image.

Metodologi Penelitian

Dalam Penelitian ini metodologi yang digunakan adalah :

- Studi literatur.
Mempelajari berbagai macam literatur yang berkaitan dengan teknik steganografi dan algoritma AES serta aplikasi yang akan digunakan.
- Analisa masalah
Pada bagian ini kita mengum-pulkan data-data yang masih mentah untuk dianalisa menjadi data yang siap pakai pada proses perancangan system.
- Perancangan sistem.
Pada tahap ini dilakukan perancangan sistem yang meliputi penentuan proses –proses yang akan dilaksanakan, dan penentuan rancangan antar muka berdasarkan studi pustaka yang telah dilakukan.
- Pembuatan perangkat lunak.
Perangkat lunak yang akan diimplementasikan menggunakan class RijndaelManaged yang telah disediakan di Visual C#. 2005. Input dalam bentuk dokumen teks dan dokumen image untuk kemudian diproses dalam komputer, sedangkan outputnya akan berupa dokumen image yang telah disisipkan teks.
- Pengujian dan Evaluasi perangkat lunak.
Pada tahap ini program yang telah dibuat diuji kebenarannya dengan menggunakan data yang telah dipersiapkan sebelumnya. Selanjutnya, hasil dari pengujian program akan dievaluasi untuk menentukan kebenaran dari program dan menentukan perlu tidaknya dilakukan modifikasi pada program.

TINJAUAN PUSTAKA

Kriptografi

Kriptografi berasal dari dua kata Yunani, yaitu Crypto yang berarti rahasia dan Grapho yang berarti menulis. Secara umum kriptografi dapat diartikan sebagai ilmu dan seni penyandian yang bertujuan untuk menjaga keamanan dan kerahasiaan suatu data. Kriptografi mendukung kebutuhan dari dua aspek keamanan informasi, yaitu secrecy (perlindungan terhadap kerahasiaan data informasi) dan authenticity (perlindungan terhadap pemalsuan dan perubahan informasi yang tidak diinginkan). Kriptografi tidak berarti hanya memberikan keamanan informasi saja, namun lebih ke arah teknik-tekniknya.

- Enkripsi

Proses enkripsi adalah proses penyandian pesan terbuka (plaintext) menjadi pesan rahasia (ciphertext). Ciphertext inilah yang nantinya akan dikirimkan melalui saluran komunikasi terbuka. Pada saat ciphertext diterima oleh penerima pesan, maka pesan rahasia tersebut diubah lagi menjadi pesan terbuka melalui proses dekripsi sehingga pesan tadi dapat

dibaca kembali oleh penerima pesan (Wibowo, Ari, Wihartantyo, 2004).

- Dekripsi

Dekripsi merupakan proses kebalikan dari proses enkripsi, merubah ciphertext kembali ke dalam bentuk plaintext. Untuk menghilangkan penyandian yang diberikan pada saat proses enkripsi, membutuhkan penggunaan sejumlah informasi rahasia, yang disebut sebagai kunci.

Teknik Steganografi

Steganografi pada saat ini banyak diterapkan dengan menggunakan file-file multimedia sebagai cara untuk menyembunyikan pesan rahasia, baik itu berupa gambar, suara, atau video. Sebelum lebih lanjut dengan pembahasan steganografi, perlu diketahui beberapa istilah yang sering digunakan. Berikut adalah beberapa istilah yang digunakan dalam teknik steganografi:

- Carrier file : file yang berisi pesan rahasia tersebut
- Steganalysis : proses untuk mendeteksi keberadaan pesan rahasia dalam suatu file
- Stego-medium : media yang digunakan untuk menampung pesan rahasia
- Redundant bits : sebagian informasi yang terdapat di dalam file yang jika dihilangkan tidak akan menimbulkan kerusakan yang signifikan (setidaknya bagi indera manusia)
- Payload : informasi yang akan disembunyikan
- Least Significant Byte (LSB) : bit rendah pada data pixel yang menyusun file gambar BMP 24 bit

Teknik yang digunakan pada gambar sebagai stego-medium beragam, tetapi secara umum teknik ini menggunakan redundant bits sebagai tempat menyembunyikan pesan pada saat dilakukan kompresi data, dan kemudian memanfaatkan kelemahan indera manusia yang tidak sensitif sehingga pada media tersebut tidak ada perbedaan yang terlihat. Cara yang digunakan adalah dengan mengganti Least Significant Byte (LSB) dengan pesan rahasia, dengan asumsi tidak semua data dibutuhkan. Dengan mengganti LSB, maka besar pesan yang dapat disembunyikan menjadi tergantung dengan besar dari carrier file.

Bagi komputer, gambar adalah file yang berisi kumpulan warna dan intensitas cahaya pada daerah yang berbeda. Dengan menggunakan penggantian LSB, maka untuk mendapatkan hasil terbaik sebaiknya digunakan 24 bit Bitmap, dikarenakan ukurannya yang besar dan memiliki resolusi tinggi. Dengan ukuran yang besar maka pesan yang dapat dibawa semakin besar dan dengan resolusi tinggi tidak akan terlihat perubahan yang signifikan. Namun dapat juga menggunakan 8 bit Bitmap atau dengan menggunakan format lainnya seperti GIF, JPEG, atau PNG untuk menghindari kecurigaan. Kelemahan dalam steganografi menggunakan gambar adalah bila dikonversi menjadi format yang lain, maka secara otomatis pesan yang disembunyikan akan hilang.

Algoritma AES

Rijndael mendukung panjang kunci 128 bit sampai 256 bit. Panjang kunci dan ukuran blok dapat dipilih secara independen. Karena AES menetapkan bahwa ukuran blok harus 128 bit, dan panjang kunci harus 128, 192, dan 256 bit, maka dikenal AES-128, AES-192, AES-256. Setiap blok dienkripsi dalam sejumlah putaran tertentu bergantung pada panjang kuncinya.

Tabel 1. Perbandingan jumlah Round dan Key

	Jumlah Key (Nk words)	Besar Block (Nb words)	Jumlah Round (Nr)
AES – 128 bit	4	4	10
AES – 192 bit	6	4	12
AES – 256 bit	8	4	14

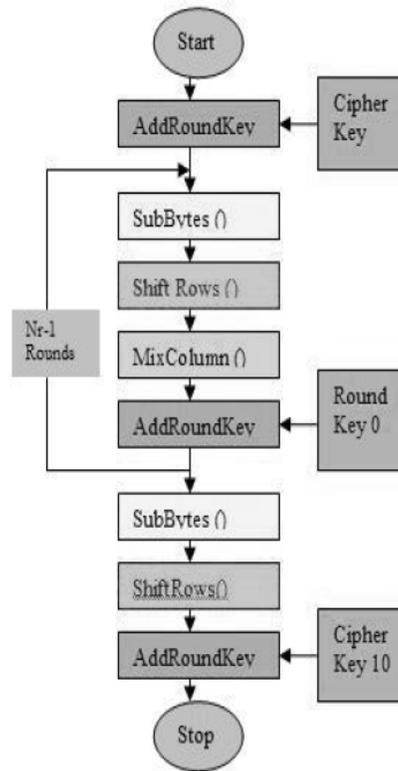
Catatan: 1 word = 32 bit.

Dengan panjang kunci 128-bit, maka terdapat $2^{128} = 3,4 \times 10^{38}$ kemungkinan kunci. Jika digunakan 1 juta komputer yang masing-masing memiliki kemampuan mencoba 1 juta kunci per detik, maka akan diperlukan waktu 5,4 trilyun tahun untuk mencoba seluruh kemungkinan kunci (Yusuf, Kurniawan, 2004).

Algoritma Rijndael

Seperti pada DES, Rijndael menggunakan substitusi dan permutasi, dan sejumlah putaran. Untuk setiap putarannya, Rijndael menggunakan kunci yang berbeda. Kunci setiap putaran disebut round key. Garis besar algoritma Rijndael yang beroperasi blok 128-bit dengan kunci 128-bit adalah sebagai berikut:

1. AddRoundKey: melakukan XOR antara state awal (plaintexts) dengan cipher key. Tahap ini disebut juga initial round.
2. Putaran sebanyak $Nr - 1$ kali. Proses yang dilakukan pada setiap putaran adalah:
 - SubByte: substitusi byte dengan menggunakan tabel substitusi (S-box). Tabel substitusi dapat dilihat pada tabel 2, sedangkan ilustrasi ByteSub dapat dilihat pada gambar 2.1.
 - ShiftRow: pergeseran baris-baris array state secara wrapping. Ilustarsi ShiftRow dapat dilihat pada gambar 2.1.
 - MixColumn: mengacak data di masing-masing kolom array state. Ilustarsi MixColumn dapat dilihat pada gambar 2.1.
 - AddRoundKey: melakukan XOR antara state sekarang dengan round key. Ilustarsi AddRoundKey dapat dilihat pada gambar 2.1.
3. Final round: proses untuk putaran terakhir:
 - ByteSub.
 - ShiftRow.
 - AddRoundKey.



Gambar 1 Proses enkripsi AES

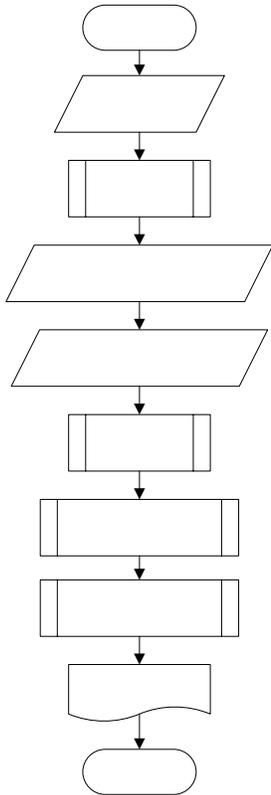
Algoritma Rijndael mempunyai 3 parameter sebagai berikut:

- Plainteks : array yang berukuran 16 byte, yang berisi data masukan.
- Cipherteks : array yang berukuran 16 byte, yang berisi hasil enkripsi.
- key : array yang berukuran 16 byte, yang berisi kunci ciphering (disebut juga cipher key).

PERANCANGAN

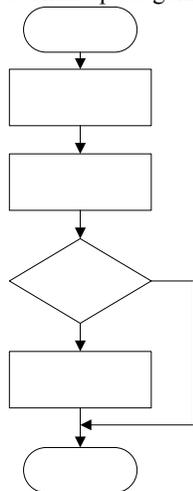
Flowchart

Dalam perancangan system dapat ditunjukkan langkah-langkah yang dilakukan oleh program secara garis besar pada saat proses create atau penyembunyian pesan rahasia kedalam gambar.



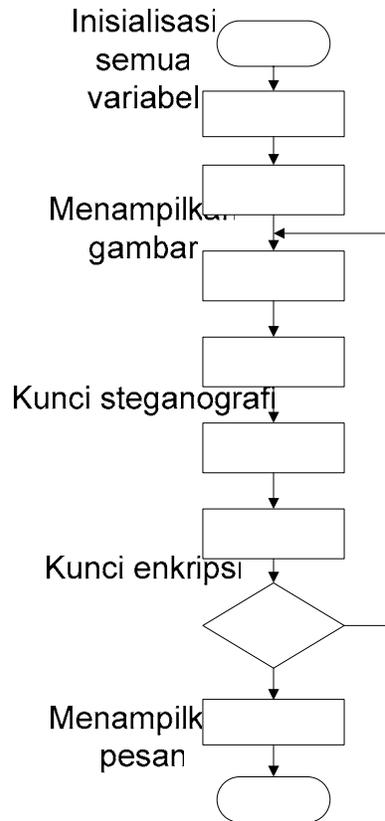
Gambar 2 Alur Proses create

Kemudian langkah setelah proses create adalah dilanjutkan dengan pengambilan gambar yang akan dijadikan sebagai stego-medium. Langkah selanjutnya adalah memasukkan pesan rahasia dan menampilkannya pada program. Langkah ini secara garis besar hampir sama dengan langkah pada pengambilan gambar. Flowchart untuk memasukkan pesan rahasia dapat dilihat pada gambar 2.3 berikut ini.



Gambar 3 : Alur proses memasukkan pesan

Flowchart diatas menunjukkan proses untuk memasukkan pesan rahasia untuk ditampilkan pada program. Dimulai dengan membuka file dialog dan kemudian menentukan file teks yang akan digunakan. Untuk file teks yang dipilih tersebut dilakukan pengujian apakah format teks tersebut merupakan format yang disetujui, jika ya maka pesan ditampilkan. Langkah selanjutnya atau langkah ke empat adalah proses mengenkripsi pesan rahasia menggunakan algoritma Rijndael. Tahapan pada algoritma Rijndael secara garis besar dijelaskan dengan flowchart pada gambar 4.



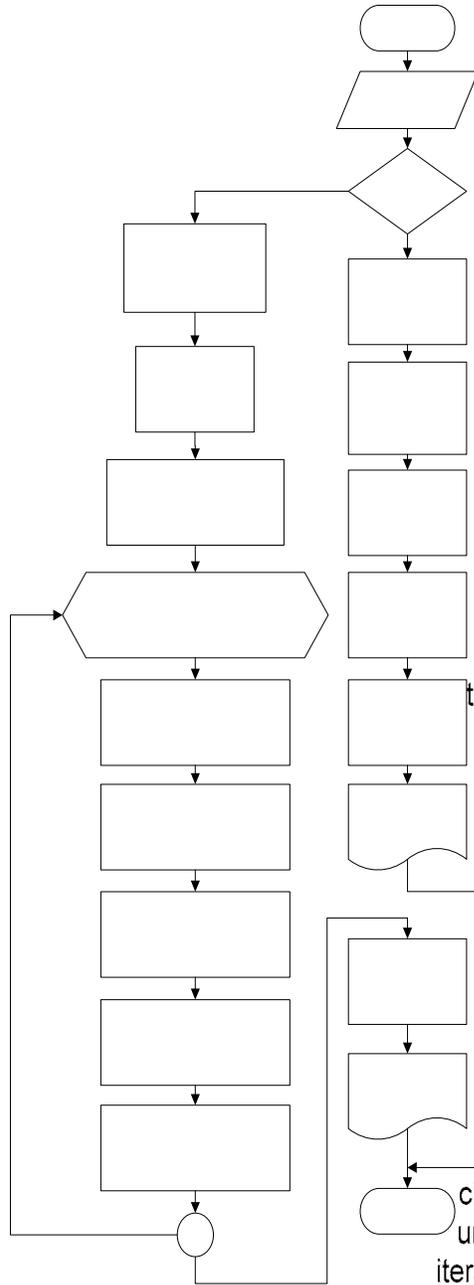
Gambar 4 : Alur proses enkripsi

Flowchart diatas adalah standart proses yang telah ditetapkan pada algoritma AES-rijndael blok chipper. Seperti dapat dilihat pada gambar 2.4, secara umum, algoritma Rijndael terdiri dari AddRoundKey, ByteSub, ShiftRow, MixColumn.

Langkah selanjutnya setelah proses enkripsi adalah proses steganografi atau penyisipan pesan rahasia. Adapun gambaran proses steganografi secara umum dijelaskan dengan flowchart pada gambar 2.5 berikut ini.

Gambar baru

selesai



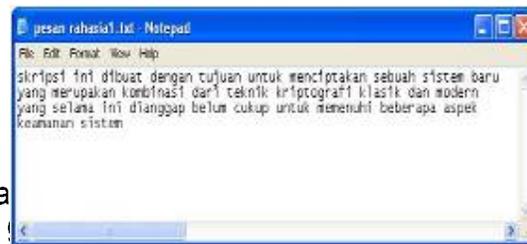
Gambar 5 Alur proses Steganografi

HASIL (IMPLEMENTASI)

Langkah pertama adalah menentukan gambar yang akan digunakan sebagai stego-medium. Untuk contoh implementasi program menggunakan format gambar JPG dengan ukuran 225,280 bytes (lihat gambar 6). Untuk pesan rahasia dapat juga diketikkan secara langsung ke dalam textboxMessage-File yang terdapat pada field message, namun implementasi kali ini menggunakan pesan dalam notepad dengan ukuran pesan rahasia 219 bytes (lihat gambar 7).



Gambar 6. Gambar berkas citra asli



Gambar 7 Pesan rahasia dalam notepad

tentukan ukuran
ukuran baris
dan jumlah pixel
dalam byte

Tentukan posisi
pada cover image
untuk disisipkan

Dapatkan panjang
cipher(kode) dalam byte
untuk menentukan jumlah
iterasi yang akan digunakan

Ambil dan copy
semua pixel
gambar
Uban komposisi
dan warna
menjadi byte
pesan

tempatkan pixel
yang berikutnya
yang membawa
suatu bit yang
terselidupi

Iterasi untuk index pesan = C
index pesan < (panjang kode)
index++

dapatkan index dari pixel
warna RGB di palet (gambar)
yang disortir

yang sama, dapat digunakan mode operasi yang memanfaatkan Initialization Vector atau IV. Untuk nilai default IV adalah 123456, namun jika user ingin merubah nilai IV tinggal menggantikan pada text box initialization vector (IV). Harus dipastikan bahwa nilai IV untuk proses extract sama dengan yang digunakan pada saat create. Apabila tidak ingin merubah nilai default IV maka text box initialization vector (IV) simpan dan reset pada nilai ini Initialization Vector menggunakan default.

Dari bit dari file
masukan dan menggantikan
(least significant bit) dari index

Pesan rahasia



Gambar 8 Proses menampilkan berkas citra asli dan pesan rahasia

Sebelum pesan disisipkan kedalam gambar, dilakukan proses enkripsi terlebih dahulu pada pesan rahasia menggunakan tombol Encrypt. Proses ini akan merubah plainteks menjadi cipherteks (lihat gambar 9).



Gambar.9 Proses enkripsi pesan rahasia

Setelah Encryption Key dimasukkan maka proses dekripsi dilakukan dengan menggunakan tombol Decrypt to plaintext (lihat gambar 10).



Gambar 10 Proses dekripsi pesan rahasia

Proses dekripsi bertujuan untuk merubah cipherteks menjadi plainteks. Dari proses dekripsi diatas dapatlah diketahui isi pesan yang sesungguhnya. Selanjut proses

dilanjutkan dengan menyimpan kembali pesan kedalam editor teks, notepad.

KESIMPULAN

Dari serangkaian uraian diatas maka dapat ditarik kesimpulan yang berkaitan dengan perancangan dan pembuatan Aplikasi Kriptografi dengan teknik Steganografi untuk keamanan dalam pertukaran pesan rahasia, diantaranya sebagai berikut:

Dengan adanya aplikasi kriptografi dengan teknik steganografi ini, maka pesan rahasia dapat disampaikan tanpa menimbulkan kecurigaan pihak lain yang tidak berhak membaca isi pesan tersebut..

Dengan memanfaatkan class rijndael yang telah terintegrasikan kedalam Visual C#2005, maka penggunaan algoritma AES untuk mendukung teknik steganografi ini menjadi lebih mudah diimplementasikan.

Melalui serangkaian uji coba pada MagixPicture diatas dapat diketahui bahwa pada setiap proses steganografi pada gambar selalu menghasilkan berkas citra yang berbeda dengan berkas citra yang asli, baik dari komposisi warna maupun ukuran file

DAFTAR PUSTAKA

- [1] Irianto. (2004). Embedding Pesan Rahasia Dalam Gambar. Mata Kuliah Keamanan System Lanjut ITB.
- [2] Jaenudin. (2006). Belajar Sendiri.net dengan Visual C#2005. Yogyakarta : Andi Yogyakarta.
- [3] Kurniawan, Yusuf. (2004). Kriptografi Keamanan Internet dan Jaringan Komunikasi. Bandung : Informatika Bandung.
- [4] Kuliah Umum IlmuKomputer.Com. Copyright © 2003 - 2006 IlmuKomputer.Com.
- [5] Morin, Charles, Randy. (2001). How to Base64. www.kbcafe.com
- [6] Mudeng, Denny. (2005). Kriptografi Twofish. Mata Kuliah Keamanan Sistem Informasi ITB.
- [7] Rahayu, Spty, Flourensia. (2005). Cryptography. Kelompok 124 IKI-83408T MTI UI. April. 2007
- [8] Soehono, Stefanus. (2006). Audio Steganografi Menggunakan Mp3. Mata Kuliah Keamanan Sistem Informasi ITB.
- [9] Suyono. (2004). Penyerangan Pada Sistem Steganografi Dengan Menggunakan Metode Visual Attacks dan Statistical Attacks. Mata Kuliah Keamanan Sistem Informasi ITB.
- [10] Wibowo, Ari, Wihartanyo. (2004). Advanced Encryption Standard, Algoritma Rijndael. Mata Kuliah Keamanan Sistem Informasi ITB.