ANALISA DAN IMPLEMENTASI STEGANOGRAFI TERHADAP PLAINTEXT DENGAN METODE WHITESPACE MENGGUNAKAN ENKRIPSI RIJNDAEL DAN HUFFMAN ENCODING COMPRESSION

Helmi Fajar Andrianto[1], Maman Abdurohman[2], Andrian Rakhmatsyah[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

---

Abstrak

Pengiriman informasi-informasi rahasia melalui jaringan komputer dilakukan untuk mempersingkat waktu serta menghubungkan individu yang berada di tempat yang jauh. Hal ini menimbulkan masalah keamanan karena informasi dikirimkan melalui jaringan publik/umum informasi dikirimkan melalui jaringan publik/umum. Salah satu cara untuk melakukan pengamanan informasi adalah dengan melakukan steganografi. Steganografi adalah menyisipkan suatu data ke dalam suatu media sehingga keberadaannya tersamarkan. Pada Tugas Akhir ini, membahas steganografi yang disisipkan ke media file teks dengan menggunakan whitepsace. Sebelum suatu informasi disisipkan, akan dilakukan enkripsi dengan rijndael dan huffman compression.

Analisa akan dilakukan dengan melihat bagaimana tiap-tiap proses bekerja serta file hasilnya. Pada enkripsi, akan dianalisa tingkat pengacakan bit datanya serta ukuran output yang dihasilkan. Pada proses kompresi, akan diimplementasikan ratio kompresi yang sesuai untuk mengkompress suatu informasi secara efektif. Proses Steganografi sendiri akan dianalisa file hasilnya dengan membandingkan file asli sebelum dilakukan steganografi.

Dari penggujian yang telah dilakukan, steganografi dengan whitespace, melakukan perubahan terhadap file induk dari segi struktur isinya saja. Pada proses kompresi, akan efektif jika dilakukan dengan ratio yang tepat untuk suatu pesan dengan jumlah bit add yang tidak terlalu banyak. Proses enkripsi dengan rijnadel, memiliki tingkat pengacakan pesan yang bagus. Perbedaan 1 bit pada suatu inputan dapat menghasilkan pengacakan pesan pada keseluruhan bit pesan.

Kata Kunci : file teks, steganografi, enkripsi, text compression, whitespace,

---

Abstract

Transferring a secret information through the computer network, conducted to take less time and also connect the individual in the different place. This matter generate the security problem because information delivered through the public network.

A solution to conduct the information security is by doing steganografi. In this Final Project, will be discussing steganografi inserted to text file by using whitepsace. Before an information inserted, it will be encrypt by rijndael and compress use huffman algorithm

Analysis will be conducted with observe how every process work. At encryption process, will be analysed by testing its level to random bits of data and also measure output size yielded. At compression process, will be testing by use appropriate compression ratio. At steganography process will be analysed by observe its result file and comparing the result file with the original file before steganography.

Based on testing, steganography make change to carrier file from its structure. At compression process , it will be effective if conducted by a correct ratio to a message which has few bit add in it. Encryption process use rijndael algorithm, owning good storey to random bits data. One bit difference of input, can yield random conditions at overall bits.

Keywords : text file, steganography, encryption, text compression, whitespace,

---

1. Pendahuluan

1.1 Latar belakang

Perkembangan teknologi informasi telah mengalami perkembangan yang cukup pesat. Dengan adanya internet, penyampaian informasi semakin mudah dan cepat. Penyampaian informasi sudah tidak mengenal jarak dan waktu. Ada berjuta-juta informasi yang dikirim setiap detiknya baik melalui internet maupun media-media lainnya. Pada suatu komunitas dengan lokasi yang saling berjauhan dan membutuhkan kecepatan penyampaian informasi, internet merupakan media penyampaian yang paling cocok untuk digunakan.

Berbagai jenis informasi dapat disampaikan melalui internet, mulai dari informasi yang sifatnya untuk konsumsi publik, sampai dengan informasi yang sifatnya rahasia. Ketika suatu informasi disampaikan melalui internet, suatu sistem keamanan tidak dapat 100% menjamin bahwa informasi yang dikirimkan untuk seseorang di tempat yang jauh, tidak di baca oleh orang-orang yang berhak. Informasi untuk seseorang mungkin adalah suatu informasi rahasia misalnya nomor PIN, password email ataupun informasi lainnya yang sifatnya rahasia dan pemilik informasi tidak ingin orang lain untuk menerima informasi tersebut.

Salah satu solusi untuk pengamanan informasi yang disampaikan melalui internet adalah steganografi. Pada steganografi, informasi rahasia yang akan disampaikan, disisipkan ke dalam suatu file yang disebut file *carrier*. File *carrier* dapat berupa file teks, image maupun file lain yang umum terdapat di internet. Dalam tugas akhir ini,penulis akan membahas penyisipan pesan pada file teks.

File teks merupakan salah satu jenis file yang cocok digunakan sebagai file *carrier*. Hal ini disebabkan karena :

- File teks, rata-rata memiliki ukuran yang kecil, sehingga mudah untuk ditransfer melalui jaringan.
- Keberadaan file teks sangatlah umum di internet, sehingga dapat mengurangi kecurigaan.
- File teks merupakan format dasar bagi jenis dokumen lain seperti HTML, Javascript dan bahasa pemrograman lain yang beredar di internet. Hal ini akan menjadikan steganografi pada file teks dapat diimplementasikan pula terhadap jenis-jenis file tersebut.

Dalam mengimplementasikan steganografi di dalam file teks, penulis menggunakan karakter-karakter whitespace sebagai media untuk merepresentasikan bit-bit informasi yang disisipkan. Hal ini didasari oleh sifat karakter whitespace yang tidak kelihatan secara langsung dan keberadaannya jaramg diperhatikan. Selain itu, kelebihan penggunaan karakter whitespace sebagai media penyisipan bit informasi hanya akan mengubah struktur penulisan isi file, sedangkan dari segi makna, tidak akan berubah.

Akan berbeda jika dilakukan penyisipan bit informasi secara langsung ke dalam bit karakter file teks. Seluruh isi file baik struktur maupun maknanya dapat saja berubah. Hal ini akan sangat menganggu jika akan melakukan penyisipan ke

dalam format HTML. Ketika makna file HTML berubah, maka akan mengubah tampilan suatu web atau bahkan pesan error.

Kelemahan penggunaan file jenis teks sebagai file *carrier*, terutama penggunaan whitespace sebagai media penyisipannya, adalah terbatasnya ukuran pesan yang dapat ditampung didalamnya. Hal ini penulis atasi dengan melakukan kompresi terhadap bit-bit yang akan disisipkan. Algoritma kompresi yang penulis gunakan adalah probability huffman encoding. Alasan penggunaan algoritma ini adalah karena kemudahan algoritma ini dalam memproses berbagai macam inputan yang akan dikompresi baik inputan berupa teks/ karakter sampai dengan inputan berupa rentetan bit. Selain itu, dengan penggunaan probabilitas nilai yang sering muncul, akan lebih menambah tingkat kompresi suatu teks, terutama jika banyak terdapat karakter yang sama.

Penggunaan steganografi didalam mengamankan suatu informasi rahasia, memiliki celah yang membahayakan jika bit-bit yang disisipkan dapat diketahui. Isi dari informasi akan dapat langsung dibaca oleh pihak yang dapat memecahkan teknik penyisipannya. Apalagi, teknik penyisipan dengan menggunakan whitespace sudah banyak diketahui oleh khalayak di internet.

Penggunaan enkripsi menjadi solusi untuk mengatasi masalah ini. Enkripsi akan mencegtah pembacaan isi informasi sekalipun bit-bit yang disisipkan dapat diketahui. Algoritma enkripsi yang penulis gunakan adalah adalah algoritma rijndael. Algoritma rijndael merupakan standar algoritma enkripsi yang dipakai NIST (*National Institute Standards and Technology*) sebagai pengganti algoritma DES. Rijndael memiliki tingkat keamanan yang tinggi dengan adanya 4 (empat) proses utama yang diproses selama 10 *round*. Tiap proses menjamin tingkat pengacakan pesan yang rumit. Hal ini ditambah dengan dukungan terhadap panjang kunci yang mencapai 128 bit.

1.2 Perumusan masalah

Dalam tugas akhir ini dirumuskan beberapa masalah sebagai berikut:

1. Bagaimana suatu pesan rahasia dapat disisipkan ke dalam suatu teks.
2. Bagaimana algoritma enkripsi Rijndael bekerja untuk mengenkripsikan pesan yang akan disisipkan.
3. Bagaimana melakukan kompresi terhadap pesan rahasia dengan menggunakan Probability Huffman Encoding Scheme agar mendapatkan besar file yang diinginkan.
4. Bagaimana pesan rahasia yang telah dienkripsi disisipkan ke dalam suatu media dalam hal ini file teks.
5. Bagaimana suatu teks yang telah disisipi pesan rahasia dapat diambil pesan rahasianya untuk kemudian didekripsi menjadi pesan asli

Adapun batasan masalah tugas akhir ini adalah sebagai berikut :

1. Algoritma enkripsi yang akan dipakai adalah rijndael dengan besar key 128 bit dan besar blok yang akan dienkripsi bervariasi.
2. Pada tugas akhir ini hanya akan dibahas mengenai proses steganografi pada file ber ekstensi txt (file text) dengan pesan yang

disisipkan berupa teks yang hanya terdiri dari karakter alphabet (A..Z, a..z), numerik (0..9) dan spasi.

3. Metode yang digunakan untuk melakukan penyisipan pesan adalah dengan menggunakan karakter whitespace (tab dan spasi) baik dengan menyisipkannya ke akhir baris, indentasi ataupun juga akhir suku kata.
4. Besar pesan yang disisipkan tergantung dari besarnya file *carrier*, sehingga dimungkinkan adanya sebagian pesan yang tidak masuk ke dalam file *carrier* jika ukuran file *carrier* terlalu kecil dan pada akhir pesan ditandai dengan suatu karakter khusus yang menandai akhir pesan.
5. Kerahasiaan adalah sifat dimana pesan hanya diketahui beberapa orang atau kelompok saja, sedangkan orang atau kelompok diluar itu, tidak boleh mengetahui pesan tersebut.
6. Keutuhan adalah pesan yang telah dienkripsi dan dikompresi tidak mengalami perubahan dari segi isi maupun maknanya.
7. Keaslian adalah file *carrier* yang telah disisipi pesan tidak mengalami perubahan dari segi maknanya sehingga akan sama dengan file aslinya.

1.3 Tujuan

Tujuan dari tugas akhir ini adalah sebagai berikut :

1 Mencegah pembacaan nilai bit pesan secara langsung dengan menggunakan algortima enkripsi rijndael. Akan dianalisa tingkat pengacakan bit dan juga ukuran chipertext.

2 Melakukan kompresi, sehingga ukuran pesan yang akan disisipkan menjadi lebih kecil.

3 Menyamarkan pesan ke dalam plainteks. Analisa akan dilakukan deengan membandingkan file hasil dengan *file carrier* dengan melihat perbedaannya secara langsung.

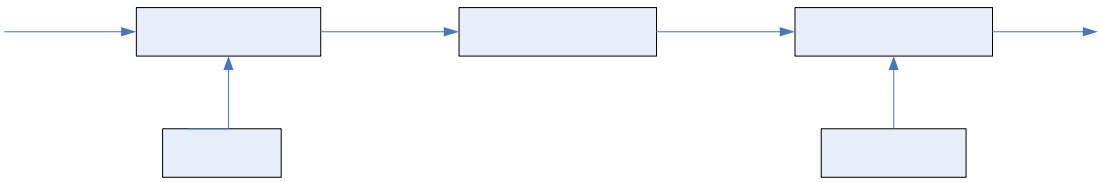
4 Membuat suatu aplikasi yang dapat digunakan untuk melakukan penyisipan suatu pesan dalam file text yang sebelumnya telah mengalami proses enkripsi dan kompresi..

5 Menjaga kerahasiaan, keutuhan, dan keaslian pesan.

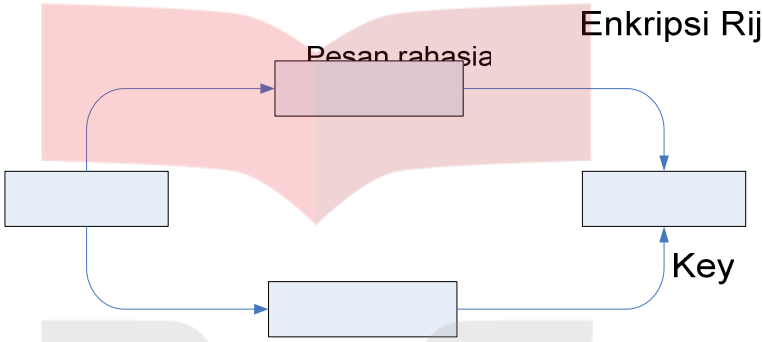
1.4 Metodologi penyelesaian masalah

Pengerjaan tugas akhir ini menggunakan metodologi :

1. Studi Literatur dengan mempelajari literatur-literatur yang relevan dengan permasalahan yang meliputi:
    - Pengolahan file teks
    - Teknik algoritma enkripsi rijndael
    - *Huffman encoding scheme*
    - Teknik penyisipan pesan (steganografi) pada file teks
    - Evaluasi performansi



Gambar 1-1: Skema proses.



Gambar 1-2: Skema kompresi.

2. Melakukan enkripsi pesan dengan metode enkripsi rijndael dimana blok data yang akan dienkripsi dapat bervariasi panjangnya dengan panjang kunci tetap yaitu 128 bit.
3. Analisa dan implementasi *Huffman encoding scheme* untuk melakukan proses kompresi terhadap pesan dan penentuan encoding table berdasarkan probabilitas penggunaan suatu karakter. Analisa berupa penentuan ratio yang akan digunakan agar besar file hasil kompresi sama dengan atau memiliki ukuran lebih kecil daripada file sebelum dikompresi. Implementasi dilakukan dengan menggunakan delphi sebagai tools untuk pembuatan aplikasinya.
4. Menyisipkan pesan yang telah dienkripsi tersebut dengan teknik steganografi ke dalam suatu file teks, dimana sebelumnya akan ditentukan terlebih dahulu peletakan pesan, apakah pada akhir baris, indentasi ataupun akhir suku kata.
5. Melakukan evaluasi terhadap hasil teks yang telah disisipi pesan terenkripsi tersebut dengan cara membandingkan antara file asli dan file yang telah disisipi pesan terenkripsi, baik dari segi isi file teksnya maupun *filesize*nya, membandingkan ketiga metode penyisipan whitespace untuk mengetahui jenis penyisipan yang cocok dilihat dari pesan yang akan disisipkan dan media teks yang digunakan.
6. Pada proses enkripsi, pengujian dilakukan dengan mengenkripsi pesan yang akan disisipkan dengan algoritma rijndael. Setelah proses enkripsi selesai, dilihat, apakah ukuran file pesan asli (plaintext) sama dengan chipertext ataukah lebih besar. Jika ternyata lebih besar, maka

dilanjutkan dengan proses kompresi terhadap chipertext dengan menggunakan ratio tertentu agar ukuran chipertext sama atau mendekati ukuran plaintext. Jika ternyata plaintext dan chipertext mempunyai ukuran yang sama, maka kompresi akan dilakukan semaksimal mungkin. Pengujian selanjutnya dilakukan dengan menyisipkan hasil kompresi ke dalam file text. Kemudian dilihat apakah terjadi perubahan ketika file *carrier* belum disisipi dengan setelah file *carrier* disisipi. Perubahan yang dimaksud disini hanyalah perubahan pada makna file teks, tidak termasuk strukturnya.Dikatakan berhasil, jika ternyata tidak terdapat perubahan dari sisi makna antara file sebelum disisipi dengan file yang telah tersisipi.

7. Penyusunan laporan tugas akhir dan kesimpulan akhir

5. Penutup

5.1 Kesimpulan

Kesimpulan yang dapat diambil dari Tugas Akhir ini adalah :

1. Penggunaan karakter whitespace pada steganografi plainteks sebagai media untuk penyimpanan bit-bit yang disisipkan, efektif untuk mengurangi terjadinya perubahan file induk secara makna atau informasi di dalamnya, tetapi tidak efektif untuk mempertahankan struktur asli file induk.
2. Kapasitas penyimpanan bit dengan whitespace sangatlah terbatas, dipengaruhi oleh *filesize* dari file induk itu sendiri dan kandungan karakter whitespace dalam file induk tersebut.
3. *Probability huffman encoding scheme* akan mengalami kegagalan kompresi ketika menghasilkan *huffman tree* yang terlalu panjang yang disebabkan karena terlalu banyaknya variasi objek kompresi serta probabilitas kemunculannya yang merata.
4. Kegagalan proses kompresi pada algoritma huffman bisa diatasi dengan meningkatkan ratio kompresi.
5. Algoritma huffman dengan ratio yang tepat, efektif untuk mengkompresi teks bahkan bisa menghilangkan efek dari bit-bit tambahan yang ada selama proses.
6. Pada algoritma enkripsi rijndael, ukuran pesan chipertext bisa lebih besar daripada ukuran plaintextnya. Hal ini disebabkan karena adanya bit tambahan (*add bit*) yang digunakan untuk melengkapi jumlah blok yang akan diproses.

5.2 Saran Kritik

Saran yang dapat diajukan untuk pengembangan Tugas Akhir ini adalah :

1. Implementasi proses steganografi, enkripsi serta kompresi pada media plainteks diatas hanyalah berupa dasar untuk pengembangan aplikasi serupa untuk media teks jenis lainnya, dan dengan melihat penggunaan whitespace yang hanya merubah struktur penulisan tanpa mengubah makna/informasi di dalam file induk, maka cocok untuk diimplementasikan pada media teks HTML yang banyak dijumpai di internet ataupun media bahasa pemrograman lainnya dengan basis teks.
2. Penggunaan whitespace sebagai alat untuk menyisipkan pesan memiliki kekurangan dari segi kapasitas. Bisa juga dilakukan dengan menyisipkannya langsung ke dalam bit-bit karakter pada *Most Significant Bits(MSB)*nya yang akan meningkatkan kapasitas pesannya. Namun perlu dipikirkan tentang cara decodingnya agar tidak merubah nilai dari karakter itu sendiri.
3. Pada proses enkripsi rijndael 128 bit, adanya bit tambahan dapat mengurangi kapasitas media induk untuk hal yang tidak penting. Perlu dibuat fungsi untuk dapat mengurangi atau bahkan menghilangkan efek dari bit-bit tambahan tersebut pada level enkripsinya.

4. Pada proses steganografi dengan whitespace, akan dihasilkan suatu file yang telah dimodifikasi dengan menyisipkan bit-bit pesan didalamnya. File tersbut berwujud file teks. Ketika file ini diubah isinya, (bahkan merubah satu bit saja), maka pesan didalamnya tidak akan bisa terbaca. Untuk mengatasi hal ini, penulis melakukan setting atribut file ini menjadi *read only* untuk mencegah terjadinya pengubahan isi pesan. Untuk kedepannya, penulis menyarankan untuk membuat file hasil ini menjadi format PDF atau sejenisnya yang berarti juga, proses pembacaan pesan dari filenya akan berbeda dengan yang ada sekarang.

Daftar Pustaka

[1] Ari Wibowo ,Wihartantyo.*Advanced Ecryption Standard, Algoritma Rijndael*. Institut Teknologi Bandung.2004

[2] Brian Gladman. *A Specification for Rijndael, The AES Algorithm*. 2003

[3] Felix VHS ,Fidens.*Dasar Kriptografi*.2006

[4] Joan Daemen, Vincent Rijmen. AES Proposal : Rijndael, Document Version 2.
NIST, 1999.

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

[6] Peri Kusdinar, Irwan Wardoyo and Irvan Hasbi Taufik. *Kompresi Teks Dengan Menggunakan Algoritma Huffman*. Sekolah Tinggi Teknologi Telkom Bandung.2005

[7] Fourth conference on the Advanced Encryption Standard (AES4), "The block chipper Rijndael " http://www.esat.kuleuven.ac.be/~rijmen/rijndael

[8] Kwan, Matthew ."The Snow Stganography Program" http://www.darkside.com.au/snow/

[9] Steganography dengan Media Plainteks.
http://orangsakti.blogsome.com/category/programming/

[10] Rijndael MixColumn's Stage . http://www.samiam.org

[11] Moffat, Neil. "Sets the Attribut of a File".
http://www.delphibasics.co.uk