PENGAMAN DATA DENGAN METODE STEGANOGRAFY DAN ALGORITMA RC4

Disusun oleh :

Rizki Budi Santoso

1410652003

PROGRAM TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH JEMBER

2017

Abstrak

Perkembangan komputer dan perangkat pendukung lainnya yang serba digital, telah membuat data digital semakin banyak digunakan. Disisi lain kemudahan tersebut telah memunculkan masalah di sekitar hak cipta dan hak kepemilikan materi digital. Teknik hidden message (steganografi), adalah suatu teknik yang mengijinkan para pengguna untuk menyembunyikan suatu pesan didalam pesan yang lain. Dengan kemampuan tersebut maka informasi hak cipta seperti identitas seorang pengarang, tanggal ciptaan, dan lain-lain dapat disisipkan/disembunyikan kedalam berbagai macam variasi jenis dokumen besar seperti: gambar, audio, video, text atau file biner. Penelitian ini membahas steganografi yang merupakan teknik menyembunyikan/menyisipkan data sedangkan pesan yang akan disipakan ke file digunakan akan di enkripsi dengan menggunakan algoritma RC4.

Kata kunci: hidden message, steganografi, RC4.

BAB 1 Pendahuluan

Dalam era digital, komunikasi melalui jaringan komputer memegang peranan penting. Melalui komunikasi elektronis, seseorang dapat melakukan transaksi atau komunikasi dengan sangat cepat dan praktis. Hal ini merupakan pengaruh dari perkembangan yang sangat signifikan dalam teknologi informasi, dimana *bandwidth* internet yang semakin besar dengan biaya akses yang semakin murah. Konsekuensinya adalah resiko dalam keamanan informasi semakin meningkat.

Komunikasi data elektronis memerlukan perangkat keamanan yang benar-benar berbeda dengan komunikasi konvensional. Dalam lalu lintas informasi di internet, sistem autentikasi (bukti diri) konvensional dengan KTP, SIM dan sebagainya yang bersandar pada keunikan tanda tangan tidak berlaku. Pengawalan petugas keamanan tidak lagi bisa membantu keamanan pengiriman dokumen elektronis.

Kemudahan pertukaran pesan melalui media elektronik masih mempunyai beberapa risiko, di antaranya risiko penyadapan, pengubahan, dan perusakan pesan, sehingga diperlukan suatu cara yang bisa mengurangi dampak negatif atas terjadinya risiko tesebut. Lebih baik lagi jika cara tersebut bisa mengurangi kemungkinan terjadinya risiko yang dimaksud. Karena alasan tersebut, muncullah penyandian terhadap pesan dengan enkripsi dan dekripsi.

Salah satu model algoritma yang digunakan untuk penyandian pesan adalah algoritma *Rivest Code 4* (RC4) Model ini merupakan salah satu algoritma kunci simetris yang berbentuk stream chipper. Algoritma ini ditemukan pada tahun 1987 oleh Ronald Rivest dan menjadi simbol keamanan RSA (merupakan singkatan dari tiga nama penemu: Rivest Shamir Adleman) RC4 menggunakan panjang kunci dari 1 sampai 256 bit yang digunakan untuk menginisialisasikan tabel sepanjang 256 bit.

Metode lain yang dapat digunakan untuk penyandian pesan/data rahasia adalah steganografi yaitu teknik penyembunyian data pada suatu media. Setiap orang dapat menampilkan atau membuka media tersebut, namun tidak menyadari bahwa media tersebut telah dibubuhkan pesan rahasia oleh pengirim. Steganografi memungkinkan penyembunyian data pada berbagai jenis media digital seperti berkas citra, suara, video, dan teks.

Secara teori, semua file yang ada didalam komputer dapat digunakan sebagai media penampung pesan, seperti file citra berformat JPG, GIF, BMP, file audio berformat MP3, WAV, bahkan didalam sebuah video dengan format AVI, atau dalam format lainya seperti TXT, HTML, PDF. Semua file dapat dijadikan tempat bersembunyi, asalkan file tersebut memiliki bit-bit data *redundant* yang dapat dimodifikasi, setelah dimodifikasi file media tersebut tidak akan banyak terganggu fungsinya dan kualitasnya tidak akan jauh berbeda dengan aslinya.

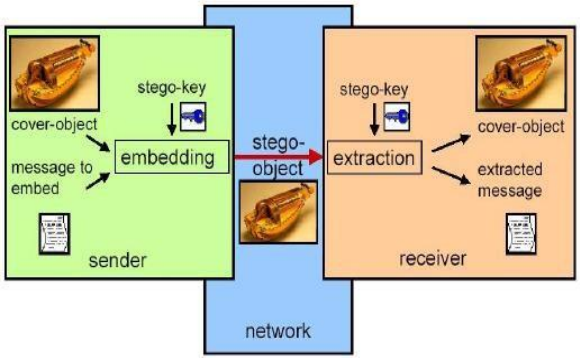
Untuk itu penelitian ini akan di fokuskan pada konsep dasar untuk menyembunyikan data/dokumen elektronik khususnya dalam data gambar. Teknik utama yang akan digunakan adalah steganografi dengan menggunakan algoritma RC4 untuk penyandian pesan yang akan di sisipkan pada file gambar.

TUJUAN

Penelitian yang dilakukan terkait dengan konsep *hidden message* dengan stagenografi dengan algoritma RC4, bertujuan antara lain untuk memahami karakteristik dasar proses *embedding* dan *extracting message* pada stagenografi serta membangun sebuah aplikasi sederhana yang dapat digunakan untuk mengimplementasikan konsep *hidden message*.

BAB II LANDASAN TEORI

Steganografi adalah ilmu pengetahuan dan seni dalam menyembunyikan komunikasi. Suatu sistem steganografi sedemikian rupa menyembunyikan isi suatu data di dalam suatu sampul media yang tidak dapat di duga oleh orang biasa sehingga tidak membangunkan suatu kecurigaan kepada orang yang melihatnya, Gambar 1 adalah ilustrasi dasar dari konsep steganografi. Di masa lalu, orang-orang menggunakan tato tersembunyi atau tinta tak terlihat untuk menyampaikan isi steganografi. Sekarang, teknologi jaringan dan komputer menyediakan cara easy-to-use jaringan komunikasi untuk steganografi. Proses penyembunyian informasi di dalam suatu sistem steganografi dimulai dengan mengidentifikasi suatu sampul media yang mempunyai bit berlebihan (yang dapat dimodifikasi tanpa menghancurkan integritas media). Proses menyembunyikan (*embedding*) menciptakan suatu proses stego medium dengan cara menggantikan bit yang berlebihan ini dengan data dari pesan yang tersembunyi (lihat Gambar 1).



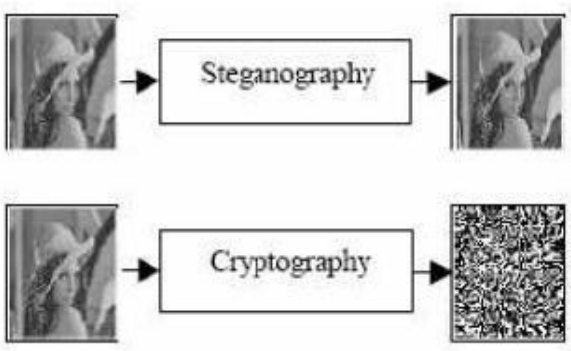
Gambar 1: Ilustrasi dasar steganografi

Terdapat dua proses utama dalam steganografi digital yaitu penyisipan (*Embedding/encoding)* dan penguraian (*extraction/decoding*) pesan. Pesan dapat berupa *plaintext, chipertext*, citra atau apapun yang dapat ditempelkan ke dalam *bit-strem*. *Embedding* merupakan proses menyisipkan pesan kedalam file yang belum dimodifikasi, yang disebut media cover (cover object). Kemudian media cover dan pesan yang ditempelkan membuat media stego (stego object). *Extraction* adalah proses menguraikan pesan yang tersembunyi dalam media stego. Suatu password khusus (stego key) juga dapat digunakan secara tersembunyi, pada saat penguraian selanjutnya dari pesan. Ringkasnya steganografi adalah teknik menanamkan embedded message pada suatu cover object, dimana hasilnya berupa stego object. Pihak yang terkait dengan steganografi antara lain *embeddor*, *extractor*, dan *stegoanalyst* (Mohanty,1999). Embeddor adalah orang yang melakukan embedding dengan menggunakan aplikasi steganografi, extractor adalah orang yang melakukan extract stego image dengan menggunakan aplikasi stegonografi. Sedangkan stegoanalyst adalah orang yang melakukan stegonalisis. Stegonalisis merupakan ilmu dan seni untuk mendeteksi pesan yang tersembunyi dalam steganografi.

1. Perbedaan Steganografi dengan Kriptografi

Steganography berbeda dengan *cryptography*, letak perbedaannya adalah pada hasil keluarannya. Hasil dari *cryptography* biasanya berupa data yang berbeda dari bentuk aslinya dan biasanya data seolah-olah berantakan sehingga tidak dapat diketahui informasi apa yang terkandung didalamnya (namun sesungguhnya dapat dikembalikan ke bentuk semula lewat proses dekripsi), sedangkan hasil keluaran dari steganography memiliki

bentuk persepsi yang sama dengan bentuk aslinya. Kesamaan persepsi tersebut adalah oleh indera manusia (khususnya visual), namun bila digunakan komputer atau perangkat pengolah digital lainnya dapat dengan jelas dibedakan antara sebelum proses dan setelah proses (Suhono, 2000). Gambar 2 menunjukkan ilustrasi perbedaan antara steganografi dan kriptografi.

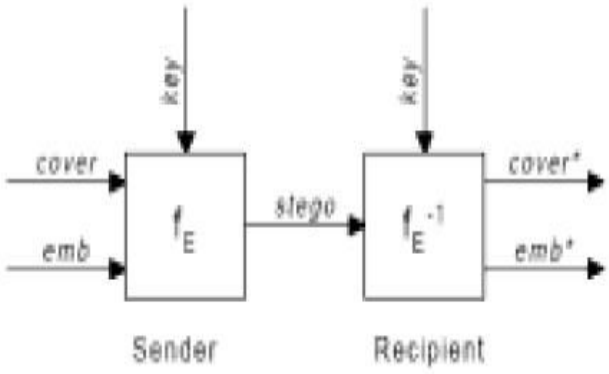


Gambar 2: Perbedaan Steganografi dengan Kriptografi

2. Dasar Penyembunyian (*Embedding*)

Tiga aspek berbeda di dalam sistem penyembunyian informasi bertentangan dengan satu sama lain yaitu: kapasitas, keamanan, dan ketahanan (*robustness*). Kapasitas adalah mengacu pada jumlah informasi yang dapat tersembunyi di dalam sampul media, keamanan adalah pencegahan bagi orang biasa yang tidak mampu untuk mendeteksi informasi tersembunyi, dan ketahanan adalah untuk modifikasi media stego sehingga dapat bertahan terhadap suatu *attack* yang dapat menghancurkan informasi tersembunyi.

Penyembunyian informasi biasanya berhubungan dengan *watermarking* dan *steganografi*. Tujuan utama sistem *watermarking* adalah untuk mencapai tingkat ketahanan yang lebih tinggi, sangatlah mustahil untuk menghilangkan suatu proses *watermarking* tanpa menurunkan tingkat kualitas objek data. steganografi, pada sisi lain, mengejar kapasitas dan keamanan tinggi, yang dimana sering diketahui bahwa informasi yang tersembunyi mudah diketahui. Bahkan modifikasi kecil kepada media stego dapat menghancurkannya (Provos, 2003). Model dasar untuk *embedding* adalah sebagaimana pada Gambar 3 (Zolnerr et al., 2004). Sementara Gambar 4 menunjukkan hubungan antara steganografi dengan watermarking (Suhono et al., 2000).



Gambar 3: Model dasar Embedding

3. Konsep Teknik *Dynamic Cell Spreading*

Teknik *Dynamic Cell Spreading* (DCS) merupakan steganografi dengan menggunakan model proteksi terhadap deteksi yang dikembangkan oleh Holger Ohmacht dengan konsep dasar yaitu menyembunyikan file

pesan (semua data elektronik) kedalam media gambar (JPEG). Penyembunyian pesan dilakukan dengan cara menyisipkanya pada bit rendah LSB (*Least Significant Bit*) dari data pixel yang menyusun file tersebut menggunakan buffer memori sebagai media penyimpan sementara.

Dalam proses penggabungan (stego) antara file gambar dengan teks, untuk file bitmap 24 bit maka setiap pixel (titik) pada gambar tersebut akan terdiri dari susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Dengan demikian pada setiap pixel file bitmap 24 bit dapat menyisipkan 3 bit data. Contohnya huruf A dapat kita sisipkan dalam 3 pixel, misalnya data raster original adalah sebagai berikut:

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

Sedangkan representasi biner huruf A adalah 10000011. Dengan menyisipkannya pada data pixel diatas maka akan dihasilkan:

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001001 00100111 11101001)

Terlihat hanya empat bit rendah yang berubah, untuk mata manusia maka tidak akan tampak perubahannya. Secara rata-rata dengan metoda ini hanya setengah dari data bit rendah yang berubah, sehingga bila dibutuhkan dapat digunakan bit rendah kedua bahkan ketiga.

Proses penggabungan file gambar dengan data elektronik hampir sama tetapi lebih kompleks karena membutuhkan media memori sebagai perantarauntuk menghitung jumlah keseluruhan bit yang terdapat didalam file gambar maupun didalam data elektronik yang akan diembedding sehingga memudahkan proses embedding itu sendiri.

Penghitungan aritmatika dalam melakukan embedding maupun extracting ini menggunakan perintah assembler karena menyangkut bit-bit yang terdapat didalam memori. Proses embedding dalam Teknik DCS mempunyai beberapa tahapan proses yaitu:

a. Membuat registry address untuk mempersiapkan tempat penyimpan memori sementara guna proses dalam penghitunggan LSB (*Least Significant Bit*) pada gambar maupun data yang akan digabungkan (embed).
b. Konversi JPEG ke dalam bitmap dalam arti format gambar JPEG yang merupakan format kompresi gambar dirubah atau di unkompres agar mempermudah dalam penghitunggan dan penempatan data.
c. Mengkalkulasikan jarak antar bit yang ada pada file gambar agar mempermudah penghitunggan dan penyisipan bit data yang akan dimasukkan.
d. Mengalokasikan memori untuk menampung bit gambar pada saat proses *steganografi* akan dijalankan.
e. Mengkopi bitmap ke dalam buffer memori.
f. Mendapatkan ukuran input byte file yaitu sama dengan proses pada gambar yang dimana untuk mengetahui besar dari data yang akan digabungkan ke dalam gambar.
g. Mengkopi buffer memori ke bentuk bitmap mengubah kembali dari memori menjadi file gambar. Proses *ekstrakting* dalam *Teknik* DCS mempunyai beberapa tahapan proses yaitu:

a. Membuat registry address untuk mempersiapkan tempat penyimpan memori sementara guna proses dalam penghitunggan LSB (*Least Significant Bit)* pada gambar maupun data yang akan dipisahkan (*extract*).
b. Mengkalkulasikan variabel yang ada pada media pembawa pesan dalam hal ini adalah file gambar yang berformat bmp.
c. Mengalokasikan ukuran memori yang akan digunakan dalam proses.
d. Mengcopy bitmap ke dalam buffer memori.
e. Ekstrak ukuran file pembawa bertujuan untuk menghitung dan mengembalikan kembali ukuran file pembawa ke dalam ukuran yang semula sebelum disisipkan file lain.
f. Mengkalkulasikan variabel yang ada menghitung kembali setelah proses ekstrak dilewati.
g. Ekstrak file bertujuan untuk mengambil data dalam file gambar yang telah dihitung dan disiapkan dalam memori sebelumnya sehingga proses dapat berjalan dengan cepat.

4. Algoritma *Rivest Code 4* (RC4)

RC4 Stream Chiper merupakan salah satujenis algoritma yang mempunyai sebuah SBox, S0,S1,……,S255, yang berisi permutasi dari bilangan 0 sampai 255. Pada algoritma enkripsi ini akan membangkitkan pseudorandom byte dari key yang akan dikenakan operasi Xor terhadap plaintext untuk menghasilkan ciphertext. Untuk menghasilkan plaintext semula, maka ciphertext nya akan dikenakan operasi Xor terhadap pseudorandom bytenya.

Pada RC4 Menggunakan dua buah indeks yaitu i dan j di dalam algoritmanya. Indeks i digunakan untuk memastikan bahwa suatu elemen berubah, sedangkan indeks j akan memastikan bahwa suatu elemen berubah secara random. Secara garis besar algoritma dari metode RC4 Stream Cipher ini terbagi menjadi dua bagian, yaitu : key setup dan stream RC4 Stream Cipher generation. Pada. Key Setup terdapat tiga tahapan proses di dalamnya, yaitu Inisialisasi S-Box, Menyimpan key dalam Key Byte Array, Permutasi pada S-Box. Pada Stream Generation akan menghasilkan nilai pseudorandom yang akan dikenakan operasi XOR untuk menghasilkan ciphertext ataupun sebaliknya yaitu untuk menghasilkan plaintext.

Algoritma RC4 memiliki dua fase, setup kunci dan pengenkripsian. Setup untuk kunci adalah fase pertama dan yang paling sulit dalam algoritma ini. Dalam setup N-bit kunci (N merupakan panjang dari kunci), kunci enkripsi digunakan untuk menghasilkan variabel enkripsi yang menggunakan dua buah array, state dan kunci, dan sejumlah-N hasil dari operasi penggabungan. Operasi penggabungan ini terdiri dari pemindahan(swapping) byte, operasi modulo, dan rumus lain. Operasi modulo merupakan proses yang menghasilkan nilai sisa dari satu pembagian. Sebagai contoh, 11 dibagi 4 adalah 2 dengan sisa pembagian 3; begitu juga jika tujuh modulo empat maka akan dihasilkan nilai tiga.

5. HASIL DAN PEMBAHASAN

Adapun hasil yang telah di uji dengan menggunakan aplikasi Stegonagrafi ini dapat dilihat pada tabel 1 yang mencakup nama file, jenis format gambar, ukuran citra penampung, status penyisipan dan ukuran dari semua citra yang sudah berhasil. Sebagaian citra tersebut ditampilkan pada gambar 9 dan gambar 10.

Nama File	Jenis Format	Ukuran file sebelumnya	Status penyisipan	Ukuran hasil penyisipan

Data 1	JPG	19,3 Kb	Berhasil	455 Kb
Data 2	JPG	16,5 Kb	Berhasil	675 Kb
Data 3	JPG	95,3 Kb	Tidak Berhasil	
Data 4	JPG	32,3 Kb	Berhasil	862 Kb
Data 5	JPG	75,5 Kb	Berhasil	1,05 Mb
Data 6	JPG	121 Kb	Berhasil	901 Kb

Citra Penampung

.JPG 121 Kb

Citra Hasil Penyisipan Pesan

.BMP 901 Kb

Berdasarkan hasil gambar 9 dan 10, sekilas tidak tampak perbedaan. Hal ini sesuai dengan tujuan steganografi, yaitu menyisipkan (mengirimakan) data pada medium penyimpanan dengan tujuan tidak menarik perhatian. Sehingga dari tahapan pengujian dapat disimpulkan bahwa penggabungan steganografi teknik DCS dan Algoritma RC4 berhasil mencapai tujuan.

Proses penyembunyian atau steganografi mempunyai berbagai macam bentuk metode juga implementasi program. Pada alamat website www.1ecs.com pada bagian steganography tools (hidden message) terdapat sejumlah link untuk download software steganografi. Aplikasi yang dibangun menggunakan gabungan antara steganografi teknik DCS dan Algoritma enkripsi RC4.

Teknik DCS merupakan suatu teknik steganografi yang menerapkan metode embedding data dengan menggunakan LSB (Least Significant Bit). Penggunaan metode embedding data dengan menggunakan LSB dilakukan dengan mempersiapkan suatu arus bit, kemudian menetapkan LSB dari cover sesuai dengan nilai dari file kedua atau data yang akan dibawa. Jarak antara dua bit tersembunyi yang berurutan menjadi banyaknya contoh dari metode ini dan dikendalikan dengan suatu nilai acak, sendangkan algoritma RC4 digunakan untuk mengenkripsi pesan yang akan di sisipkan ke citra, hal ini bertujuan agar pesan yang di sisipkan tidak mudah untuk di baca dan terjaga kerahasiaan pesan yang di sisip.

BAB III PENUTUP

Kesimpulan

Dengan solusi steganografi, maka pada prinsipnya masalah yang terkait dengan hak cipta dan kepemilikan dapat dipecahkan, hal ini mengacu pada sifat dasar steganografi yaitu menyembunyikan pesan. Namun demikian steganografi bukan solusi tunggal untuk menyelesaikan masalah tersebut, watermarking dan cryptografi dapat pula dijadikan sebagai solusi bersama untuk mengatasi masalah hak cipta dan kepemilikan.

Teknik DCS merupakan proses embedding dengan menggunakan metode LSB. Implementasi program dilakukan dengan menggunakan bahasa pemrograman tingkat rendah yaitu assembler.Teknik DCS mempunyai cara menejemen alokasi memori yang cukup baik dalam melakukan proses embedding maupun ekstrakting, sehingga tidak memboroskan pemakaian memori yang ada.

Dalam program steganografi ini terjadi perubahan besar dalam hal ukuran file, yaitu sebelum proses embedding dengan setelah proses embedding. Pada masa mendatang perlu kiranya dilakukan penelitian lanjutan dengan menggabungkan Teknik DCS dengan algoritma kompresi file sehingga ukuran file hasil proses staganografi akan lebih kecil atau minimal sama dengan file aslinya dan Penerapatan metode algoritma RC4 pada pesan yang akan disisipkan pada file dapat menambah kerahasian data

Daftar Pustaka

[1]. Henry S, Sayed M, Fitri A (2009), Implementasi Steganografi Dengan Metode Least Significant Bit (LSB). Jurnal Rekayasa Elektrika vol 8, No. 1,

[2]. Kembanghapsari Rinci, Siti Mariyam. Aplikasi Sistem Pengamanan Data Dengan Metode Enkripsi Menggunakan Algoritma RC4.

[3]. Rizal, A, Suharto (2011), Implementasi Algoritma Rc4 Untuk Keamanan Login Pada Sistem Pembayaran Uang Sekolah(Studi Kasus : Di Yayasan Yabis Bontang), 142 Dielektrika, ISSN. 2086-9487, Vol2, No.2

[4]. Mike Y, Miftahul H, Prima K, Implementasi Algoritma Kriptografi RC4 pada Sistem Keaman-an Jaringan Telepon, Proceeding of IES 2008, Surabaya, Januari 2010

[5]. Maulana, Ahmad M, Data Hiding Steganograph Pada File Image Menggunakan *Metode Least Significant Bit*, PENS-ITS, Surabaya, 2009

[6]. Ohmacht, H. (2001). *Stegano Project***.** Diakses pada 23 Februari 2004 dari http://www.holgerohmacht.de.

[7]. Popa, R. (1998). An Analysis of Steganographic Techniques**.** *Journal of University Politehnica Timisoara*.

[8]. Provos, N., Honeyman, P. (2003). Hide and Seek: An Introduction to Steganography. *IEEE Computer Society*.

[9]. Suhono, Supangkat, H., Juanda, K. (2000). Watermarking Sebagai Teknik Penyembunyian Hak Cipta Pada Data Digital. *Jurnal Departemen Teknik Elektro*, Institut Teknologi Bandung**.**

[10]. Zöllner, J. et al. (2004). Modeling the Security of Steganographic System**.** *Journal of Dresden University of Technol*gy.

Sumber referensi :
https://s3.amazonaws.com/academia.edu.documents/39354566/MAKALAH_PENGAMAN_DATA_DENGAN_METODE_STEGANOGRAFY_DAN_ALGORITMA_RC4.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1510318245&Signature=ZTJh8WKjfis%2BEyjNvFFU9%2BK30OY%3D&response-content-disposition=attachment%3B%20filename%3DMAKALAH_PENGAMAN_DATA_DENGAN_METODE_STEG.pdf