KOMBINASI PENGGABUNGAN PENGAMANAN DATA MENGGUNAKAN TEKNIK STEGANO DAN ENCRYPTOGRAPHY

Albert Santoso

Jurusan Ilmu Komputer Universitas AKI, Semarang
albert.santoso@unaki.ac.id

Abstact

Nowadays, computer's network and internet show its expanding significantly that can make someone keeps changing information each other in easier and fastest ways. However, the security in communication through those media has not good enough. The security in communication here is interrelated with a guarantee that the communicating information will be delivered to the right destination without leaking or even leak to the untitled sides. To make it true, there are two kinds of security that is still in progress of fulfilling, Steganography and Cryptography, and those have been become the security that are most after used. Steganography is such as a method which can put a secret of information's abbreviation into other media so when the media is accepted by the destination, it will look like usual media, in fact the media has kept the addition of secret information. Cryptography is a technique of data's code by changing the row of the characters in same media format. This analysis is done to make an adoption of technique for data's security, by integrating the cryptography's technique to encode the information and then use the Steganography's technique to hide it into other media's..

Keywords : Steganography; Cryptography; Security; Encryption

1. Pendahuluan

Jaringan komputer dan Internet telah mengalami perkembangan yang sangat pesat. Teknologi ini mampu untuk dapat menghubungkan hampir semua komputer yang ada di dunia sehingga bisa saling berkomunikasi dan bertukar informasi. Bentuk informasi yang dapat ditukar berupa data teks, gambar, gambar bergerak dan suara.

Perkembangan tersebut secara langsung ikut mempengaruhi cara kita untuk melakukan komunikasi. Kalau dahulu untuk berkomunikasi pesan atau surat dengan menggunakan pos, sekarang telah tersedia layanan e-mail di Internet yang dapat mengirimkan pesan secara langsung ke penerimanya. Akan tetapi sebagai suatu jaringan publik, Internet sangat rawan terhadap pencurian data yang telah dikirimkan.

Dewasa ini penyembunyian suatu pesan tidak hanya dapat dilakukan dengan menyamarkan pesan tersebut, melainkan pula menyisipkan pesan tersebut dalam media yang lain, sehingga orang lain yang tidak ada hubungannya dengan kita, tidak akan curiga terhadap pesan yang akan kita kirimkan, karena pesan tersebut tersembunyi dan yang terlihat hanyalah media penampung pesan kita tersebut. Sebagai contoh, saat kita ingin melakukan pengiriman pesan seseorang yang jauh melalui email, akan timbul adanya perasaan selalu waspada terhadap keamanan pesan kita, apakah akan diketahui orang lain atau tidak, maka kita menyisipkan pesan tersebut dalam sebuah media lain yang lebih besar, misalnya dalam media citra. Dengan demikian orang lain tidak akan menyangka bahwa di dalam gambar yang kita kirimkan tersembunyi suatu pesan khusus. Hal ini tentunya akan lebih aman dibandingkan pengiriman pesan dalam bentuk terenkripsi yang akan membuat orang lain curiga dan semakin merasa tertantang untuk melakukan attack atau serangan demi untuk mengetahui isi pesan yang kita kirimkan.

Teknik penyisipan pesan dalam media lain yang lebih besar ini dinamakan *Steganography*. Media penyimpanan yang dapat digunakan dalam *Steganography* dapat berupa berkas lagu, citra, atau berkas-berkas yang lain yang berukuran besar dan dapat dimasukkan pesan yang kita sembunyikan. Dengan menggunakan *Steganography* maka orang tidak bertanggung jawab tidak akan menjadi curiga kalau ternyata kita mengirimkan pesan rahasia. *Steganography* merupakan satu metode pengamanan data yang populer, di mana sesuatu pesan (teks atau image) dapat dirahasiakan di dalam file-file lain yang mengandung teks, image, bahkan suara tanpa menunjukkan ciri-ciri perubahan yang nyata atau terlihat dalam kualitas dan struktur dari file semula.

Di bidang *Kriptografi*, enkripsi ialah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa melalui proses pembalikan yang disebut dekripsi. Enkripsi telah digunakan untuk mengamankan komunikasi di berbagai negara dan organisasi-organisasi tertentu serta individu yang memiliki kebutuhan yang besar

akan kerahasiaan pesan yang dikomunikasikan. Di pertengahan tahun 1970-an, enkripsi kuat dimanfaatkan untuk pengamanan oleh sekretariat agen pemerintah Amerika Serikat pada domain publik, dan saat ini enkripsi telah digunakan pada sistem secara luas, seperti Internet e-commerce, jaringan Telepon bergerak dan ATM pada bank.

Enkripsi dapat digunakan untuk tujuan keamanan, tetapi teknik lain masih diperlukan untuk meningkatkan jaminan keamanan dalam komunikasi, terutama untuk memastikan integritas dan autentikasi dari sebuah pesan. Message Authentication Code (MAC) atau digital signature adalah salah satu contoh teknologi untuk keperluan tersebut.

Dengan menggabungkan kedua teknik *Steganography* dan *Kriptografi*, kelemahan dari keduanya dapat diminimalkan.

2. Landasan Teori

Steganography adalah sebuah teknik penyisipan pesan dalam media yang lebih besar. Dalam bahasa Yunani kata ”*Steganography*” diterjemahkan sebagai ”Steganos” yang berarti tulisan tersembunyi. Sehingga dapat diartikan dalam terjemahan bebas bahwa *Steganography* adalah ilmu dan seni menyisipkan informasi dengan cara menyisipkan pesan dalam pesan lain. Sejarah mencatat bahwa *Steganography* pertama kali digunakan pada tahun 440 sebelum masehi. Ketika itu Demeratus mengirimkan berita tentang penyerangan yang akan dilakukan ke Yunani. Beliau mengirimkan pesan tersebut dalam sebuah kayu dan menutupinya dengan lilin, sehingga pesan yang dikirimkannya tidak terlihat mencurigakan dan kerahasian pesan tetap terjaga. (Johnson, 2001)

Tentunya metode *Steganography* tersebut sudah sangat usang jika ingin digunakan dalam dunia modern seperti sekarang ini. Teknik *Steganography* yang digunakan dalam dunia moderrn sekarang ini sudah amat beragam. Beragam mulai dari algoritma yang digunakannya sampai pada media yang digunakannya.

Media penyisipan pesan rahasia atau bisa dikatakan sebagai carrier file (file pembawa) adalah suatu file yang digunakan oleh file Stegano untuk menyembunyikan data. Ada empat tipe dari carrier file yang mendukung. (N. F. Johnson and S. Jajodia, 1998). Tergantung dari masing-masing tipe, ada beberapa pedoman yang harus diikuti.

a. Teks
File Stegano dapat memproses text file (*.TXT) sebaik ASCII (dalam DOS) dan ANSI (dalam Windows) dalam dua metode encoding data dalam text file :
-Metode standard : Ukuran dari file tetap tidak berubah. Ketika mengimport manipulasi carrier file ke dalam word processor (terutama dalam Window), di sana akan muncul karakter khusus dalam sebuah text.
-Metode Compatible : File semakin bertambah. Tidak akan ada kemungkinan munculnya karakter khusus ketika manipulasi carrier file diimport ke aplikasi lain.
Kapasitas dari text file dalam menyembunyikan data sangat tergantung pada file content tetapi dapat dikalkukasi sebagai berikut (dalam byte) :
-Metode Standard : jumlah dari kalimat / 8.
-Metode Compatible : jumlah dari garis.

b. Audio
Format ini pun sering dipilih karena biasanya berkas dengan format ini berukuran relatif besar. Sehingga dapat menampung pesan rahasia dalam jumlah yang besar pula.

c. Citra (Bitmap Images)
Format ini pun paling sering digunakan, karena format ini merupakan salah satu format file yang sering dipertukarkan dalam dunia internet. Alasan lainnya adalah banyaknya tersedia algoritma *Steganography* untuk media penampung yang berupa citra. (Lisa Marvel). Yang paling penting dari kriteria ini adalah kedalaman warna (berapa banyak bit per pixel yang didefinisikan dari sebuah warna) bitmap dengan mengikuti formulasi berikut.

Jumlah warna = 2n
dengan n adalah kedalaman warna, sehingga
- 4 bit = 16 warna (16 gray scales).
- 8 bit = 256 warna (256 gray scales).
- 24 bit = 16.777.216 warna.

Secara umum dapat dikatakan semakin banyaknya warna, maka akan diperlukan keamanan yang ketat atau tinggi dikarenakan bitmap memiliki area yang sangat luas dalam sebuah warna yang seharusnya dihindarkan. Dilihat dari kedalaman atau kejelasan dari sebuah warna, bitmap dapat mengambil sejumlah data tersembunyi dengan perbandingan sebagai berikut (ukuran ratio dari bitmap dalam byte = ukuran dari data yang disembunyikan) :
- 4 bit = 16 warna : 4 : 1
- 8 bit = 256 warna : 8 : 1
- 24 bit = 16.777.216 warna : 8 : 1

Manipulasi pada bitmap tidak dapat diubah ke dalam bentuk format grafik yang lain karena data tersembunyi dalam file tersebut akan hilang. Format menggunakan metode kompresi yang lain (seperti JPEG) tidak dapat digunakan. Mengurangi ukuran dari carrier file sangatlah penting untuk melakukan transmisi online, yaitu dengan menggunakan utilitas kompresi (seperti : ARZ, LZH, PKZIP, WinZip), dikarenakan kerja mereka tidak terlalu berat.

d. Video
Format ini memang merupakan format dengan ukuran file yang relatif sangat besar namun jarang digunakan karena ukurannya yang terlalu besar sehingga mengurangi kepraktisannya dan juga kurangnya algoritma yang mendukung format ini.

Banyak metoda *Steganography* yang melekatkan sejumlah besar informasi rahasia di dalam pixel pada cover image karena perasaan manusia yang tidak sempurna dalam hal visualisasi, keberadaan informasi rahasia yang ditempelkan tersebut dapat saja tidak terlihat. Tetapi informasi rahasia tersebut mungkin saja ditemukan, jika belum ditempatkan secara baik.
Kebanyakan algoritma *Steganography* menggunakan sebuah kombinasi dari bidang jenis teknik untuk melakukan sebuah tugas dalam penyelubungan pesan rahasia dalam sebuah selubung file. Sebuah program *Steganography* dibutuhkan untuk melakukan hal-hal berikut, baik implisit melalui suatu perkiraan maupun eksplisit melalui sebuah perhitungan: menemukan kelebihan bits dalam selubung file yang dapat digunakan untuk menyelubungi pesan rahasia di dalamnya, memilih beberapa di antaranya untuk digunakan dalam menyelubungi data dan penyelubungan data dalam bits dipilih sebelumnya. Metoda yang digunakan untuk menyembunyikan pesan pada media digital tersebut berbeda-beda. Untuk penelitian ini algoritma yang akan digunakan untuk pengamanan data untuk *Steganography* adalah menggunakan teknik algoritma LSB (Least Significant Bit Insertion). Contohnya pada file image pesan dapat disembunyikan dengan menggunakan cara menyisipkanya pada bit rendah (Least Signigicant Bit) pada data pixel yang menyusun file tersebut. Seperti kita ketahui untuk file bitmap 24 bit maka setiap pixel (titik) pada gambar tersebut terdiri dari susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (1 byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Dengan demikian pada setiap pixel file bitmap 24 bit kita dapat menyisipkan 3 bit data.

Contoh 8 bit pixel :
1 pixel : (00 01 10 11)
white red green blue
Insert 0011 : (00 00 11 11)
white white blue blue

Contohnya huruf A dapat kita sisipkan dalam 3 pixel, misalnya data raster original adalah sebagai berikut:

(00100111 11101001 11001000)
red blue green
(00100111 11001000 11101001)
red green blue
(11001000 00100111 11101001)
green red blue

Sedangkan representasi biner huruf A adalah 10000011. Dengan menyisipkan-nya pada data pixel di atas maka akan dihasilkan:

(00100111 11101000 11001000)
red green green
(00100110 11001000 11101000)
white green green
(11001001 00100111 11101001)
blue red blue

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. (T. Aura, 1996)

Colormap (peta warna) dalam 8 bit warna image (gambar) maksimumnya 24 bit warna image (gambar) dari 256 *color* (warna). Bagaimanapun untuk meminimisasi gangguan tambahan ketika Least Significant Bit Insertion (LSB) berubah, *colormap* (peta warna) dimulai dari hanya 240 *color* (warna) dan ke-16 *color* (warna) lainnya akan ada atau ditambah pada saat hasil akhir dari sebuah gambar.

Kekurangan dari Least Significant Bit Insertion

Dapat diambil kesimpulan dari contoh 8 bit pixel, menggunakan *Least Significant Bit Insertion* dapat secara drastis merubah unsur pokok warna dari pixel. Ini dapat menunjukkan perbedaan yang nyata dari cover image menjadi stego image, sehingga tanda tersebut menunjukkan keadaan dari *Steganography*. Variasi warna kurang jelas dengan 24 bit image, bagaimanapun file tersebut sangatlah besar. Antara 8 bit dan 24 bit image mudah diserang dalam pemrosesan image, seperti cropping (kegagalan) dan compression (pemampatan).

Keuntungan dari LSB Insertion

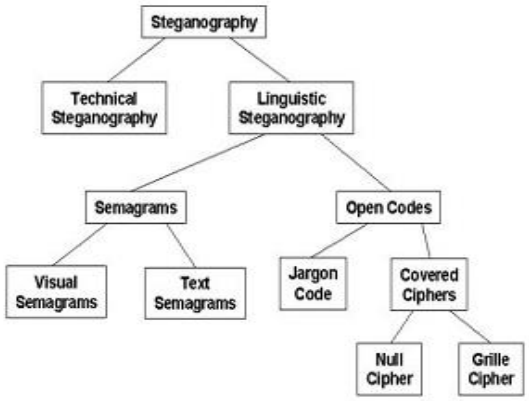
Keuntungan yang paling besar dari algoritma LSB ini adalah cepat dan mudah. Dan juga algoritma tersebut memiliki software *Steganography* yang mendukung dengan bekerja di antara unsur pokok warna LSB melalui manipulasi pallete (lukisan).

Untuk dapat menutup kelemahan ini maka untuk peneletian ini akan ditambahkan system pengamanan lagi yaitu dilakukan dengan yang namanya *Kriptografi*. *Kriptografi* mengacak pesan sehingga tidak mudah untuk dimengerti, sedangkan *Steganography* menyembunyikan pesan sehingga

tidak terlihat. Pesan dalam cipherteks mungkin akan menimbulkan kecurigaan sedangkan pesan yang dibuat dengan *Steganography* tidak. Kedua teknik ini dapat digabungkan untuk mendapatkan metoda pengiriman rahasia yang sulit dilacak. Hal pertama yang akan dilakukan adalah pesan rahasia tersebut akan dienkrip, kemudian cipherteks disembunyikan menggunakan *Steganography* pada media (*Carrier file*) yang tampak tidak mencurigakan. Cara ini sangat berguna jika digunakan pada cara *Steganography*, karena banyak format file digital yang dapat dijadikan media untuk menyembunyikan pesan. Format yang biasa digunakan diantaranya:

- Format image: bitmap (bmp), gif, pcx, jpeg, dll.
- Format audio: wav, voc, mp3, dll.

Selain berdasarkan format berkas penampung yang digunakan *Steganogaphy* pun menurut Bauer dapat dikelompokkan menjadi sebuah taxonomy sebagai berikut :



a.Technical Steganography
Teknik ini menggunakan metode sains untuk menyembunyikan pesan. Contohnya adalah penyembunyian pesan dalam chip mikro.

b. Linguistic Steganography
Teknik ini menyembunyikan pesan dalam cara yang tidak lazim. Teknik ini terbagi menjadi 2 bagian yaitu Semagrams dan Open Codes.

c. Semagrams
Teknik ini menyembunyikan informasi dengan mengunakan simbol atau tanda. Contoh penggunaan adalah dengan mengganti ukuran teks atau mengganti ukuran font. Pergantian ukuran atau tipe tersebutlah yang digunakan sebagai media penyisipan pesan. Sebagai informasi algoritma gif-shuffle yang dibahas dalam makalah ini termasuk ke dalam tipe ini.

d. Open Codes
Teknik ini menyembunyikan pesan cara yang tidak umum namun tetap tidak mencurigakan. Teknik ini terbagi menjadi 2 bagian yaitu Jargon Code dan Covered Ciphers

e. Jargon Code
Teknik ini sesuai dengan namanya mengunakan bahasa yang hanya dimengerti oleh sebagian orang. Sebagai contoh adalah warchalking, underground terminology atau percakapan biasa yang mengandung fakta yang hanya diketahui oleh pembicara.

f. Covered Ciphers
Teknik ini menyembunyikan pesan dalam media pembawa sehingga pesan kemudian dapat diekstrak dari media pembawa tersebut oleh pihak yang mengetahui bagaimana pesan tersembunyi tersebut disembunyikan.

Penilaian sebuah algoritma *Steganography* yang baik dapat dinilai dari beberapa faktor yaitu:

a. Imperceptible
Keberadaan pesan dalam media penampung tidak dapat dideteksi.

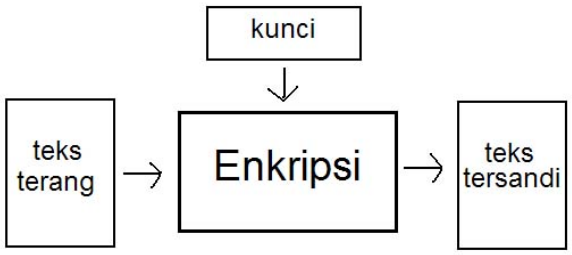
b. Fidelity
Mutu media penampung setelah ditambahkan pesan rahasia tidak jauh berbeda dengan mutu media penampung sebelum ditambahkan pesan.

c. Recovery
Pesan rahasia yang telah disisipkan dalam media penampung harus dapat diungkap kembali. Hal ini merupakan syarat mutlak dalam sebuah algoritma *Steganography*, kerena ada banyak cara penyisipan pesan yang tidak terdeteksi namun sulit dalam pembacaan kembali.

Di bidang *Kriptografi*, enkripsi ialah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Dikarenakan enkripsi telah digunakan untuk mengamankan komunikasi di berbagai negara, hanya organisasi-organisasi tertentu dan individu yang memiliki kepentingan yang sangat mendesak akan kerahasiaan yang menggunakan enkripsi. Di pertengahan tahun 1970-an, enkripsi kuat dimanfaatkan untuk pengamanan oleh sekretariat agen pemerintah Amerika Serikat pada domain publik, dan saat ini enkripsi telah digunakan pada sistem secara luas, seperti Internet e-commerce, jaringan Telepon bergerak dan ATM pada bank.

Enkripsi dapat digunakan untuk tujuan keamanan, tetapi teknik lain masih diperlukan untuk membuat komunikasi yang aman, terutama untuk memastikan integritas dan autentikasi dari sebuah pesan. Contohnya, Message Authentication Code (MAC)

atau digital signature. Penggunaan yang lain yaitu untuk melindungi dari analisis jaringan komputer.



Gambar Desain untuk *Kriptografi*

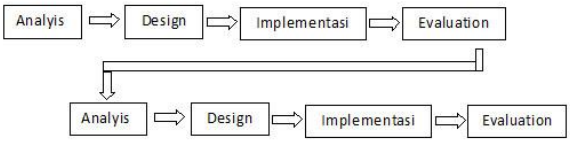
Dalam *Kriptografi*, teks asli (dalam bahasa Inggris: *plaintext*) adalah teks informasi yang merupakan masukan bagi suatu algoritma enkripsi; sedangkan keluarannya disebut teks tersandi atau teks sandi (*ciphertext*). Teks asli dapat dibaca secara normal, sedangkan teks tersandi tidak. Pekerjaan mengubah teks asli menjadi teks tersandi disebut enkripsi, dan proses sebaliknya disebut dekripsi. Tanpa dienkripsikan, teks asli biasanya dapat dibaca dengan mudah tanpa menggunakan kemampuan atau metode-metode khusus. Namun pada enkripsi berlapis, teks tersandi dari suatu enkripsi dapat menjadi teks asli bagi enkripsi berikutnya, untuk dienkripsikan lebih lanjut. Hal ini dilakukan untuk menambah kerahasiaan dari teks tersebut.

Teks tersandi (*ciphertext*) adalah teks hasil dari sebuah enkripsi. Lawan dari teks tersandi adalah teks asli (*plaintext*), yang merupakan masukan dari sebuah enkripsi. Proses pengubahan teks asli menjadi teks tersandi disebut enkripsi, sedangkan proses sebaliknya disebut dekripsi. Teks tersandi tidak dapat dibaca begitu saja. Untuk membaca teks tersandi, seseorang perlu mengetahui kunci dan algoritma yang digunakan dalam enkripsi teks tersebut. Cara kedua adalah melakukan kriptoanalisis, yaitu memecahkan sandi menggunakan metode-metode tertentu.

Berbagai macam teknik enkripsi yang biasa digunakan dalam sistem keamanan dari sistem komputer dan network.

3. Metode Penelitian

Metode penelitian yang akan digunakan adalah *RAD (Rapid Application Development).* RAD model adalah termasuk model menekankan pada siklus pengembangan yang singkat. Model RAD adalah adapatasi kecepatan tinggi dari waterfall model, yang mana kecepatan pengembangan dicapai melalui pendekatan konstruksi berbasis komponen. Jika kebutuhan system dimengerti dengan baik dan cakupan proyek dibatasi, maka proses RAD memungkinkan team pengembang menciptakan "fully functional system" dalam periode waktu yang sangat singkat. Komunikasi bekerja untuk memahami permasalahan bisnis dan karakteristik informasi yang harus diakomodasi perangkat lunak



Gambar Metode Penelitian

Tahap analysis mempelajari tentang spesifikasi system dan rencana perangkat lunak. Analisis system bertujuan untuk menjabarkan kebutuhan pengguna system dan meletakkan dasar-dasar di dalam proses perancangan perangkat lunak. Analisis yang dibutuhkan meliputi analisis kebutuhan software dan hardware dan analisis kebutuhan system.

Design Sistem adalah dibuatnya model system steganografi menggunakan Flowchart yang menggambarkan proses jalannya system dari awal hingga akhir. Selain itu juga dibuat desain input dan output berdasarkan Flowchart yang telah dibuat sebelumnya.

Implementasi adalah penerapan system ke dalam perangkat aplikasi.

Evaluation adalah evaluasi untuk memperbaiki dan menyempurnakan program.

Enkripsi Konvensional

Proses enkripsi ini dapat digambarkan sebagai berikut :

Plain teks → Algoritma Enkripsi → Cipher teks → Algoritma Dekrispsi → Plain teks.

User A ||User B
|Private Key B----|Public Key B-|

Informasi asal yang dapat dimengerti, disimbolkan oleh Plain teks, yang kemudian oleh algoritma Enkripsi diterjemahkan menjadi informasi yang tidak dapat untuk dimengerti yang disimbolkan dengan cipher teks. Proses enkripsi terdiri dari dua yaitu algoritma dan kunci. Kunci biasanya merupakan suatu string bit yang pendek yang mengontrol algoritma. Algoritma enkripsi akan menghasilkan hasil yang berbeda tergantung pada kunci yang digunakan. Mengubah kunci dari enkripsi akan mengubah output dari algortima enkripsi.

Sekali cipher teks telah dihasilkan, kemudian ditransmisikan pada bagian penerima, selanjutnya cipher teks yang diterima diubah kembali ke plain teks dengan algoritma dan dan kunci yang sama.

Keamanan dari enkripsi konvensional bergantung pada beberapa faktor. Pertama algoritma enkripsi

harus cukup kuat sehingga menjadikan sangat sulit untuk mendekripsi cipher teks dengan dasar cipher teks tersebut. Lebih jauh dari itu keamanan dari algoritma enkripsi konvensional bergantung pada kerahasian dari kuncinya bukan algoritmanya. Yaitu dengan asumsi bahwa adalah sangat tidak praktis untuk mendekripsikan informasi dengan dasar cipher teks dan pengetahuan tentang algoritma diskripsi / enkripsi. Atau dengan kata lain, kita tidak perlu menjaga kerahasiaan dari algoritma tetapi cukup dengan kerahasiaan kuncinya.

Manfaat dari konvensional enkripsi algoritma adalah kemudahan dalam penggunaan secara luas. Dengan kenyataan bahwa algoritma ini tidak perlu dijaga kerahasiaannya dengan maksud bahwa pembuat dapat dan mampu membuat suatu implementasi dalam bentuk chip dengan harga yang murah. Chips ini dapat tersedia secara luas dan disediakan pula untuk beberapa jenis produk. Dengan penggunaan dari enkripsi konvensional, prinsip keamanan adalah menjadi menjaga keamanan dari kunci.

Model enkripsi yang digunakan secara luas adalah model yang didasarkan pada data encrytion standard (DES), yang diambil oleh Biro standart nasional US pada tahun 1977. Untuk DES data dienkripsi dalam 64 bit block dengan menggunakan 56 bit kunci. Dengan menggunakan kunci ini, 64 data input diubah dengan suatu urutan dari metode menjadi 64 bit output. Proses yang yang sama dengan kunci yang sama digunakan untuk mengubah kembali enkripsi.

Enkripsi Public Key

Salah satu yang menjadi kesulitan utama dari enkripsi konvensional adalah perlunya untuk mendistribusikan kunci yang digunakan dalam keadaan aman. Sebuah cara yang tepat telah diketemukan untuk mengatasi kelemahan ini dengan suatu model enkripsi yang secara mengejutkan tidak memerlukan sebuah kunci untuk didistribusikan. Metode ini dikenal dengan nama enkripsi public-key dan pertama kali diperkenalkan pada tahun 1976.

Plain teks →Algoritma Enkripsi → Cipher teks → Algoritma Dekrispsi → Plain teks.

User A | | User B
|Private Key B----------|Public Key B----------|

Algoritma tersebut seperti yang digambarkan pada gambar di atas. Untuk enkripsi konvensional, kunci yang digunakan pada proses enkripsi dan dekripsi adalah sama. Tetapi ini bukanlah kondisi sesungguhnya yang diperlukan. Namun adalah dimungkinkan untuk membangun suatu algoritma yang menggunakan satu kunci untuk enkripsi dan pasangannya, kunci yang berbeda untuk dekripsi. Lebih jauh lagi adalah mungkin untuk menciptakan suatu algoritma yang mana pengetahuan tentang algoritma enkripsi ditambah kunci enkripsi tidak cukup untuk menentukan kunci dekrispi. Sehingga teknik berikut ini akan dapat dilakukan :
-Masing – masing dari sistem dalam network akan menciptakan sepasang kunci yang digunakan untuk enkripsi dan dekripsi dari informasi yang diterima.
-Masing – masing dari sistem akan menerbitkan kunci enkripsinya (public key) dengan memasang dalam register umum atau file, sedang pasangannya tetap dijaga sebagai kunci pribadi (private key).
-Jika A ingin mengisim pesan kepada B, maka A akan mengenkripsi pesannya dengan kunci publik dari B.
-Ketika B menerima pesan dari A maka B akan menggunakan kunci privatenya untuk mendeskripsi pesan dari A.

Seperti yang kita lihat, public-key memecahkan masalah pendistribusian karena tidak diperlukan suatu kunci untuk didistribusikan. Semua partisipan mempunyai akses ke kunci publik (public key) dan kunci pribadi dihasilkan secara lokal oleh setiap partisipan sehingga tidak perlu untuk didistribusikan. Selama sistem mengontrol masing – masing private key dengan baik maka komunikasi menjadi komunikasi yang aman. Setiap sistem mengubah private key pasangannya public key akan menggantikan public key yang lama.

Yang menjadi kelemahan dari metode enkripsi public key adalah jika dibandingkan dengan metode enkripsi konvensional algoritma enkripsi ini mempunyai algoritma yang lebih komplek. Sehingga untuk perbandingan ukuran dan harga dari hardware, metode publik key akan menghasilkan performance yang lebih rendah.

Desain Proses untuk kombinasi penggabungan keamanan *Steganography* dan *Kriptografi.*

Berbagai aspek penting dari enkripsi konvensional dan public key.

Enkripsi Konvensional
Yang dibutuhkan untuk bekerja :
- Algoritma yang sama dengan kunci yang sama dapat digunakan untuk proses dekripsi – enkripsi.
- Sender dan receiver harus membagi algoritma dan kunci yang sama.

Yang dibutuhkan untuk keamanan :
- Kunci harus dirahasiakan.
- Adalah tidak mungkin atau sangat tidak praktis untuk menerjemahkan informasi yang telah dienkripsi.
- Pengetahuan tentang algoritma dan sample dari kata yang terenkripsi tidak mencukupi untu menentukan kunci.

Enkripsi Public Key
Yang dibutuhkan untuk bekerja :
- Algoritma yang digunakan untuk enkripsi dan dekripsi dengan sepasang kunci, satu untuk enkripsi satu untuk dekripsi.
- Sender dan receiver harus mempunyai sepasang kunci yang cocok.

Yang dibutuhkan untuk keamanan :
- Salah satu dari kunci harus dirahasiakan.
- Adalah tidak mungkin atau sangat tidak praktis untuk menerjemahkan informasi yang telah dienkripsi.
- Pengetahuan tentang algoritma dan sample dari kata yang terenkripsi tidak mencukupi untu menentukan kunci.

4. Pembahasan

Algoritma yang akan digunakan untuk enkripsi ini adalah algoritma RSA. RSA adalah sebuah algoritma berdasarkan skema public-key cryptography. Diberi nama RSA sebagai inisial para penemunya: Ron Rivest, Adi Shamir, dan Leonard Adleman. RSA dibuat di MIT pada tahun 1977 dan dipatenkan oleh MIT pada tahun 1983. Setelah bulan September tahun 2000, paten tersebut berakhir, sehingga saat ini semua orang dapat menggunakannya dengan bebas.
Lebih jauh, RSA adalah algoritma yang mudah untuk diimplementasikan dan dimengerti. Algoritma RSA adalah sebuah aplikasi dari sekian banyak teori seperti extended euclid algorithm, euler's function sampai fermat theorem.

Beberapa manfaat yang bisa didapatkan dari enkripsi ini adalah :
- Kerahasiaan suatu informasi terjamin
- Menyediakan authentication dan perlindungan integritas pada algoritma checksum/hash
- Menanggulangi penyadapan telepon dan email
- Untuk digital signature. Digital signature adalah menambahkan suatu baris statemen pada suatu elektronik copy dan mengenkripsi statemen tersebut dengan kunci yang kita miliki dan hanya pihak yang memiliki kunci dekripsinya saja yang bisa membukanya.
-Untuk digital cash

Penyalahgunaan dan kerugian dari enkripsi adalah:
-Penyandian rencana teroris
-Penyembunyian record criminal oleh seorang penjahat
-Pesan tidak bisa dibaca bila receiver pesan lupa atau kehilangan kunci (decryptor).
Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci pribadi. Selama pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan algoritma yang bagus, maka selama itu pula keamanan algoritma RSA tetap terjamin.
RSA melibatkan dua kunci yaitu kunci publik dan kunci privat. Kunci publik dapat diketahui oleh semua orang dan digunakan unutk meng-enkripsi sesuatu dalam hal ini watermark. Watermark yang dienkripsi dengan kunci publik hanya bisa didekripsi dengan kunci privat.

Algoritma RSA didasarkan pada teorema Euler yang menyatakan bahwa

$$a^{\phi(r)} \equiv 1 \pmod{r} \qquad (1)$$

yang dalam hal ini,*a* harus merupakan bilangan yang tidak habis dibagi oleh r. $\phi(r) = r(1 - 1/p_1)(1 - 1/p_2) \ldots (1 - 1/p_n)$, yang dalam hal ini $p_1, p_2, \ldots, p_n$ adalah faktor prima dari r.

$\phi(r)$ adalah fungsi yang menentukan berapa banyak dari bilangan-bilangan 1, 2, 3, …, r yang tidak habis dibagi dengan r.

Berdasarkan sifat $a^m \equiv b^m$ *(mod* r*) untuk* m *bilangan bulat ≥ 1, maka persamaan (1) dapat ditulis menjadi*

$$a^{m\phi(r)} \equiv 1^m \pmod{r}$$

atau

$$a^{m\phi(r)} \equiv 1 \pmod{r} \qquad (2)$$

Bila *a* diganti dengan *X*, maka persamaan (2) menjadi

$$X^{m\phi(r)} \equiv 1 \pmod{r} \qquad (3)$$

Berdasarkan sifat ac ≡ bc *(mod* r*), maka bila persamaan (3) dikali dengan* X *menjadi:*

$$X^{m\phi(r)+1} \equiv X \pmod{r} \qquad (4)$$

yang dalam hal ini X tidak habis dibagi dengan r.

Misalkan SK dan PK dipilih sedemikian sehingga

$$SK \cdot PK \equiv 1 \pmod{\phi(r)} \qquad (5)$$

atau

$$SK \cdot PK = m\phi(r) + 1 \qquad (6)$$

Sulihkan (6) ke dalam persamaan (4) menjadi:

$X^{SK \cdot PK} \equiv X \pmod r$ (7)

Persamaan (7) dapat ditulis kembali menjadi

$(X^{PK})^{SK} \equiv X \pmod r$ (8)

yang artinya, perpangkatan X dengan PK diikuti dengan perpangkatan dengan SK menghasilkan kembali X semula.

Berdasarkan persamaan (8), maka enkripsi dan dekripsi dirumuskan sebagai berikut:

$E_{PK}(X) = Y \equiv X^{PK} \bmod r$ (8)

$D_{SK}(Y) = X \equiv Y^{SK} \bmod r$ (9)

Karena SK · PK = PK · SK, maka enkripsi diikuti dengan dekripsi ekivalen dengan dekripsi diikuti enkripsi:

$E_{SK}(D_{SK}(X)) = D_{SK}(E_{PK}(X)) \equiv X^{PK} \bmod r$ (10)

Oleh karena $X^{PK} \bmod r \equiv (X + mr)^{PK} \bmod r$ untuk sembarang bilangan bulat m, maka tiap plainteks X, X + r, X + 2r, …, menghasilkan cipherteks yang sama. Dengan kata lain, transformasinya dari banyak ke satu. Agar transformasinya satu-ke-satu, maka X harus dibatasi dalam himpunan {0, 1, 2, …, r – 1} sehingga enkripsi dan dekripsi tetap benar seperti pada persamaan (8) dan (9).

Enkripsi

Plainteks disusun menjadi blok-blok x_1, x_2, …, sedemikian sehingga setiap blok merepresentasikan nilai di dalam rentang 0 sampai r – 1.
Setiap blok x_i dienkripsi menjadi blok y_i dengan rumus

$y_i = x_i^{PK} \bmod r$

Dekripsi

Setiap blok cipherteks y_i didekripsi kembali menjadi blok x_i dengan rumus

$x_i = y_i^{SK} \bmod r$

Contoh 2. Misalkan plainteks yang akan dienkripsikan adalah

X = HARI INI

atau dalam sistem desimal (pengkodean ASCII) adalah

7265827332737873

Pecah X menjadi blok yang lebih kecil, misalnya X dipecah menjadi enam blok yang berukuran 3 digit:

$x_1 = 726$ $x_4 = 273$
$x_2 = 582$ $x_5 = 787$
$x_3 = 733$ $x_6 = 003$

Nilai-nilai x_i ini masih terletak di dalam rentang 0 sampai 3337 – 1 (agar transformasi menjadi satu-ke-satu).

Blok-blok plainteks dienkripsikan sebagai berikut:

$726^{79} \bmod 3337 = 215 = y_1$
$582^{79} \bmod 3337 = 776 = y_2$
$733^{79} \bmod 3337 = 1743 = y_3$
$273^{79} \bmod 3337 = 933 = y_4$
$787^{79} \bmod 3337 = 1731 = y_5$
$003^{79} \bmod 3337 = 158 = y_6$

Jadi, cipherteks yang dihasilkan adalah

Y = 215 776 1743 933 1731 158.

Dekripsi dilakukan dengan menggunakan kunci rahasia

SK = 1019

Blok-blok cipherteks didekripsikan sebagai berikut:

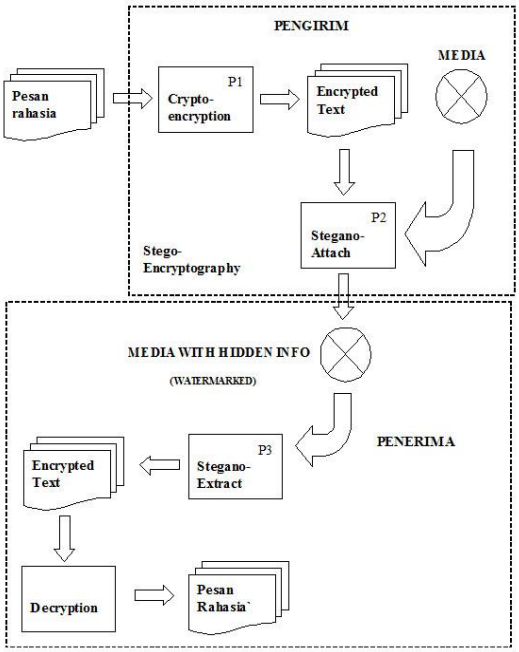
$215^{1019} \bmod 3337 = 726 = x_1$
$776^{1019} \bmod 3337 = 582 = x_2$
$1743^{1019} \bmod 3337 = 733 = x_3$
…

Blok plainteks yang lain dikembalikan dengan cara yang serupa. Akhirnya kita memperoleh kembali plainteks semula

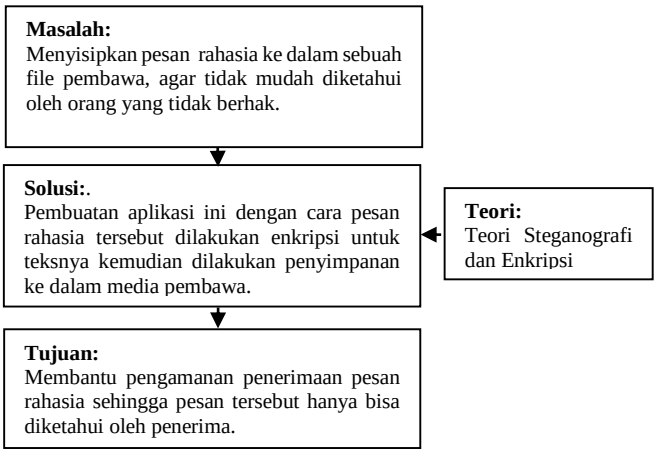
P = *7265827332737873*

yang dalam karakter ASCII adalah

P = HARI INI.



Pengolahan system untuk aplikasi *Stego-Encryptography*, di dalam pengolahannya, terdapat dua bagian yang terpisah, yaitu bagian pengirim dan penerima. Pada sisi pengirim, proses terjadi mulai dari pembukaan awal file yang akan disembunyikan, diikuti dengan proses enkripsi menggunakan methode RSA, terhadap file tersebut hingga akhirnya diakhiri dengan proses penyisipan ke dalam file media yang dipilih menggunakan metode LSB. Pada sisi penerima, terjadi proses yang merupakan pembalikan dari proses yang terjadi pada sisi pengirim. Pertama, file tersembunyi akan diekstrak dari file media pembawanya, kemudian hasil ekstrak file tersebut akan diolah dengan proses dekripsi untuk menampilkan pesan asli seperti yang dikirimkan oleh pengirim pesan.



Dari gambar di atas menjelaskan bahwa dari segi pengirim akan melakukan proses penyandian untuk pesan rahasia, kemudian dilakukan cyper text, setelah selesai maka akan di-embed ke media yang akan digunakan untuk menyimpan pesan rahasia tersebut, kemudian akan dihasilkan media dengan pesan yang tersembunyi. Setelah pengirim selesai melakukan pengiriman, maka dari sisi penerima akan melakukan Stegano-extract dari pesan rahasia, setelah itu maka dilakukan decryption terhadap pesan tersebut, maka setelah selesai pesan rahasia dari pengirim diterima dengan baik oleh penerima.

5. Kesimpulan dan saran

Kesimpulan dari aplikasi ini adalah memiliki 2 fasilitas, yaitu:

1. Steganografi (penyimpanan system)
2. Enkripsi, yang di mana fungsi ini digunakan untuk melakukan enkripsi pesan asli.

Untuk proses perancangannya aplikasi ini memiliki keamanan yang bertingkat, yang di mana keamanan tersebut adalah mengenkripsi pesan asli, serta menyembunyikan pesan rahasia yang telah terenkripsi ke dalam media file pembawa. Artinya aplikasi ini mengadopsi dua level pengamanan dari steganografi dan encryptography. Dan dengan pengkombinasian kedua teknik pengamanan data ini, seseorang tidak akan mengetahui bahwa ada data yang disembunyikan dalam sebuah media lain karena saat diekstrak pun, data hasil ekstrak tidak dapat dibaca. Dari sini akan muncul asumsi bahwa tidak ada file yang tersembunyi di dalam media tersebut. Serta jika media file pembawa cukup besar maka tidak ada perubahan ukuran untuk file tersebut, karena space yang tersedia semakin besar untuk dapat menampung keseluruhan pesan rahasia tanpa membutuhkan space tambahan yang akan memperbesar ukuran file.

Saran

Langkah-langkah pengamanan data, dapat disajikan secara terintegrasi, tidak perlu dibuat secara step by step. Maksud dari terintegrasi ini adalah menjadikan satu proses di dalam enkripsi dan embedding, dan sebaliknya dekripsi dan disembedding. Fungsi dari pengintegrasian ini, supaya tidak diperlukan adanya banyak langkah.

Daftar Pustaka

Johnson, Neil F.; Duric, Zoran; Jajodia, Shushil: "Information Hiding Steganography and Watermaking-Attacks and Countermeasures", Advanced in Information Security, Kluwer Academic Publisher, United State, 2001.

Lisa Marvel, Charles Bocelet, and Charles Retter, "Spread Spectrum Image Steganography".

N. F. Johnson and S. Jajodia, "Steganography: Seeing the Unseen," IEEE Computer, February 1998, pp.26-34.

T. Aura, "Practical invisibility in digital communication," Lecture Notes in Computer Science, vol.1174, Springer-Verlag, 1996, pp. 265-278