BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi jaringan komputer saat ini sangat pesat. Jauh lebih cepat daripada sepuluh tahun yang lalu. Hal ini membantu manusia berkomunikasi dan bekerjasama antara satu dengan yang lain tanpa terbatas oleh tempat. Proses tersebut dilakukan, baik dalam lingkup yang kecil dalam *Local Area Network* (LAN) bahkan sampai *Wide Area Network* (WAN) dan juga dalam lingkup global, yaitu internet.

Dalam proses komunikasi tersebut banyak terjadi pertukaran informasi, data dan pesan antar kedua belah pihak. Demikian pula untuk pengiriman data akademis, terutama di universitas yang melalui internet. Data–data tersebut antara lain pengiriman soal ujian dan daftar nilai ujian mahasiswa. Proses ini dahulu dilakukan secara manual. Dengan cara dosen datang ke universitas, dan menyerahkan data melalui disket, yang menyebabkan ketidakefisienan. Untuk menanggulangi hal – hal semacam itu, maka diambil cara lain, yaitu dokumen – dokumen tersebut dikirimkan melalui internet, dalam hal ini lebih khusus melalui e-mail.

Keamanan (sekuriti) pesan yang dikirim menjadi hal yang sangat penting bagi setiap orang yang mengirimkan, sehingga banyak cara dilakukan agar pesan yang dikirimkan tidak diketahui oleh pihak – pihak yang tidak berhak *(attacker)*. Pada umumnya cara pengamanan pesan dilakukan dengan dua proses (1) enkripsi yaitu proses untuk menyandikan pesan sehingga pesan tersebut tidak dapat dimengerti dan

(2) dekripsi yaitu proses yang mengubah pesan yang terenkripsi menjadi pesan semula, sehingga dapat dibaca oleh penerima pesan.

Meskipun demikian, perancangan program yang biasa dilakukan dengan penyandian biasa, sering mudah dideteksi, sehingga perlu dirancang suatu metode penyembuanyian pesan yang tidak dapat diketahui oleh *attacker*. Salah satu metode yang dapat digunakan adalah menyembunyikan pesan teks ataupun dokumen dalam gambar. Pihak luar sendiri tidak akan menduga bahwa didalam gambar terdapat pesan yang dikirimkan, sehingga meningkatkan keamanan pesan yang dikirim. Metode penyembunyian pesan dalam gambar banyak mempunyai aplikasi, antara lain menyembunyikan pesan teks, dokumen, ataupun gambar. Sebagian besar medium yang digunakan untuk menyembunyikan pesan adalah data gambar seperti JPEG, BMP, GIF.

Program aplikasi yang akan dibuat menggunakan metode F5, yang merupakan perbaikan dari metode sebelumnya yaitu metode F4 dan F3. Metode F5 mempunyai keunggulan yaitu permutasi dan penyebaran pesan yang lebih seragam yang dapat meningkatkan efisiensi enkripsi yang lebih baik. Hal ini membuat sistem sekuriti menjadi lebih baik dan tahan terhadap serangan dengan tingkat densitas yang tinggi.

1.2 Rumusan Perancangan

Program aplikasi yang dirancang yaitu program yang dapat menyembunyikan pesan yang berupa dokumen dalam gambar menggunakan algoritma F5. Algoritma F5 menggunakan *permutative straddling* dan *matrix encoding*. Pada program ini

ditambahkan modul *maintenance* pengguna yang berfungsi untuk menambah pengguna, menghapus pengguna, dan mengupdate kata kunci pengguna.

1.3 Komponen dan Spesifikasi Rancangan

Komponen Rancangan :

Program aplikasi penyembunyian gambar dengan metode F5 ini menggunakan komponen rancangan sbb :

- Modul *login* : digunakan memverifikasi apakah pengguna berhak menggunakan program ini dengan cara mencocokkan antara nama pengguna dan kata kunci yang diberikan oleh pembuat program.
- Modul utama : memberikan pilihan pada pengguna untuk memilih menu enkripsi gambar atau menu dekripsi gambar. Bila pengguna *login* sebagai pembuat program, maka akan muncul menu *maintenance* pengguna.
- Modul *maintenance* pengguna : berguna untuk menambah, menghapus, dan memodifikasi nama pengguna serta kata kunci yang digunakan.
- Modul enkripsi : untuk meminta *input* berupa gambar, tombol untuk meminta input pesan, *image* yang menampilkan gambar yang diinput, dan *text-box* untuk menginput kata kunci.
- Modul dekripsi : untuk meminta gambar yang telah dienkripsi, tombol dekripsi, *image* yang menampilkan gambar yang dienkripsi, dan *text-box* untuk menginput kata kunci.

Spesifikasi Rancangan :

Program aplikasi ini dirancang untuk mengenkripsi dan mendekripsi pesan teks dalam sebuah gambar. Dalam program ini juga ditambahkan modul *maintenance* pengguna untuk memodifikasi data pengguna dan modul perhitungan *error* untuk melihat perubahan dari gambar awal dan gambar setelah dienkripsi. Program aplikasi ini berjalan pada sistem operasi Windows 2000 dan bahasa pemrograman Delphi dan Java.

Perancangan program aplikasi ini dibatasi untuk gambar yang bertipe JPEG dengan menggunakan metode algoritma F5 yang dapat meminta masukan *file* gambar, sebuah *text-box* untuk menginput kata kunci, dan tombol untuk meminta input pesan. Cara mendekripsikan pesan yang ada terenkripsi dalam gambar dengan metode F5 ini dengan meminta masukan *file* gambar yang terenkripsi dan mengisi kata kunci yang sesuai. Dan *output* yang dihasilkan adalah gambar yang telah didekripsi serta *file* teks yang berisi pesan yang dikirimkan.

1.4 Tujuan Perancangan

Tujuan umum perancangan ini untuk mencari metode yang lebih baik dalam security informasi sehingga pesan bisa disampaikan dengan lebih aman serta merancang program aplikasi yang berdasar metode tersebut yang dapat menyembunyikan pesan teks dalam gambar sehingga *attacker* tidak mengetahuinya.

Sedangkan tujuan khusus adalah untuk dapat melindungi pengiriman data akademis, terutama dokumen ujian dan daftar nilai yang dikirmkan dari pihak dosen kepada Universitas Bina Nusantara melalui internet.

1.5 Manfaat Perancangan

Kegunaan rancangan ini dapat ditujukan pada beberapa pihak yaitu :

- Bagi administrator jaringan : untuk mengirimkan pesan yang berupa *password*, kode verifikasi bagi administrator jaringan lain atau asistennya, atau mengirimkan instruksi bagi user yang memerlukan
- Bagi bidang pendidikan : dapat untuk mengirimkan informasi yang penting bagi guru atau dosen, murid dan pihak-pihak yang berkaitan dengan pendidikan. Misalnya soal dan kunci jawaban ujian, arsip nilai.
- Bagi para pengguna internet dan intranet : untuk mengirimkan *password* email, atau *password* game online. Pengguna akan merasa lebih aman untuk bertukar informasi.
- Bagi pihak perbankan : dapat mengirimkan pesan berupa kode PIN, atau kata kunci untuk internet banking.

1.6 Definisi Operasional

- *Steganografi* : metode penyembunyian pesan dalam media gambar.
- *Permutative straddling* : proses memencarkan (*scatter)* pesan melewati seluruh medium perantara.

1.7 Penelitian Relevan

Ada beberapa jenis dari penelitian metode steganografi yang pernah dilakukan, dan hasilnya berupa software, yaitu :

- *Blindside* yaitu perangkat lunak yang berupa utilitas *command-line* yang menyembunyikan file dalam BMP dan mempunyai enkripsi yang opsional.
- BMP *Secrets* yaitu perangkat lunak yang berbasiskan produk stego untuk sistem operasi Windows dengan tampilan program dan kapasitas penyembunyian yang baik.
- *Data Stash* yaitu salah satu perangkat lunak yang menyembunyikan file di dalam BMP atau file yang berupa basis data dan dilindungi oleh perlindungan kata kunci.
- *Dc-Steganograph* yaitu perangkat lunak yang dibuat oleh Nikola Injac. Keuntungannya program ini berukuran kecil dan mudah digunakan untuk program stego yang berbasiskan DOS di mana dapat menyembunyikan data di dalam file gambar yang bertipe PCX.
- *EZStego* yaitu perangkat lunak yang berbasiskan tipe gambar GIF, yang dibuat oleh Romana Machado. Program ini dituliskan di dalam bahasa pemrograman Java.
- *GZSteg* yaitu perangkat lunak yang dibuat oleh Preston Wilson, berguna untuk menyembunyikan data di dalam file kompresi yang bertipe GZip dan dikompilasi untuk DOS.
- *Hide and Seek v4.1b* yaitu perangkat lunak yang menyediakan penyembunyian data menggunakan file gambar yang bertipe GIF. Program DOS ini bekerja dengan mengambil data (biasanya teks), termasuk teks yang terenkripsi, kemudian disembunyikan di file yang bertipe GIF.

- *MP3Stego* yaitu perangkat lunak yang mempunyai baik GUI maupun versi *command-line* yang menyembunyikan informasi di dalam file MP3.
- *Snow* yaitu perangkat lunak steganografi yang berbasiskan teks, yang dibuat oleh Matthew Kwan di mana digunakan untuk menyembunyikan pesan di dalam sebuah teks. Cara bekerjanya yaitu dengan menambahkan *tab* dan jarak (*spaces*) pada akhir dari baris.
- *Outguess v.02* yaitu sebuah perangkat lunak steganografi umum yang memperbolehkan menyisipkan informasi rahasia ke dalam redundant bits dari sumber data. Pada versi ini mendukung file yang bertipe JPEG.
- F5 yaitu sebuah perangkat lunak steganografi yang bekerja dengan cara menyisipkan pesan yang berupa teks ke dalam sebuah gambar yang bertipe JPEG. Format tipe gambar JPEG ini banyak digunakan di dalam gambar yang beredar sekarang ini. Algoritma ini yang akan dibahas dan dipakai dalam perancangan program ini.