1. Pendahuluan

1.1 Latar Belakang

Keamanan informasi yang dipertukarkan merupakan hal yang penting untuk dijaga. Terutama bila informasi tersebut merupakan hal yang rahasia seperti keamanan negara, kebijakan bisnis, dsb. Keamanan informasi mulai dipermasalahkan bila informasi tersebut dipertukarkan melalui jalur yang dapat diakses oleh satu atau beberapa pihak yang bukan merupakan tujuan dari pengirim.

"*Steganography* merupakan teknik dan seni bagaimana menyembunyikan data digital di balik data digital lain yang berperan sebagai medium pembawa (*carrier*) sehingga keberadaannya tidak mengundang kecurigaan dari persepsi pengamatan manusia (Eddy Muntina Dharma, 2008)". Pengamatan manusia baik itu merupakan pengamatan *visual* (penglihatan) maupun *auditory* (pendengaran) memiliki batas nilai yang menyebabkan seolah-olah data yang sedang diamati adalah data kontinyu dan tidak peka terhadap perubahan data. Memanfaatkan keterbatasan pengamatan manusia, *steganography* digunakan untuk menutupi keberadaan pesan yang akan dipertukarkan dengan melakukan penyisipan pesan ke *carrier file*. Namun harga yang harus dibayar dari proses penyisipan itu adalah penurunan kualitas *carrier file* yang dikarenakan gangguan (*noise*) dari data yang disembunyikan agar dapat disisipkan pada *carrier file*. *File* penyisipan pesan dapat berupa *image digital* (citra digital), *audio digital* (suara), *video*, dan sebagainya.

Dari pengaruh gangguan tersebut menyebabkan kualitas *carrier file* menjadi berkurang sehingga dapat menyebabkan kecurigaan terhadap pihak yang melakukan penyerangan maupun *monitoring*. Oleh karena itu diperlukan pengetahuan tentang batasan besar *file* pesan yang optimal untuk disisipkan dan pengaruhnya terhadap *carrier file*.

1.2 Perumusan Masalah

Pada laporan penelitian ini diadakan perancangan dan analisa ketahanan *file* hasil dari aplikasi *steganography* pada dua jenis *carrier file*, yaitu *audio* dan *image digital* menggunakan metoda *spread spectrum*. Pada metoda *spread spectrum*, pesan rahasia disebar ke sinyal hasil dari *pseudo random generator* (pembangkit sinyal *pseudo random*) yang *dependent* (bergantung) pada *carrier file*. Setelah dilakukan penyebaran pesan, barulah proses *steganography* dilakukan.

Untuk dapat menerapkan metoda *spread spectrum*, beberapa hal yang perlu diperhatikan adalah:

1. Pada laporan penelitian ini digunakan *discrete cosinus transform* (transformasi kosinus diskrit) untuk membangkitkan sinyal *pseudo random* terhadap sinyal *carrier file*.
2. Kode penyebar atau di dalam laporan penelitian ini disebut *interleaving key* pada proses *interleaving* (penyebaran) menggunakan deret Lucas.
3. Pihak yang dituju telah memiliki *carrier file* yang digunakan oleh pengirim

4. hasil yang diharapakan adalah didapatkan pola optimasi interleaving key untuk setiap *carrier file* yang akan disisipkan *file* pesan sehingga dicapai *level sequence* yang optimal dan nilai *fidelity* tetap terjaga kehandalannya.

Analisa simulasi ini tetap memiliki batasan masalah, yaitu:

1. *carrier file* yang digunakan pada laporan penelitian ini adalah *audio* yang berformat “WAV” sinyal monoponik dan *image digital* berformat “.GIF” sinyal monokrom.
2. Tidak membahas *steganalysis* terhadap metode steganografi yang digunakan.
3. Tidak membahas pengaruh jaringan terhadap pertukaran data. Atau dapat dikatakan jaringan dianggap ideal.
4. Data rahasia yang akan disisipkan adalah data berformat teks.
5. Pada pembangkitan sinyal *pseudo random noise*, digunakan transformasi kosinus diskrit yang bergantung pada hasil pembacaan *carrier file.*
6. Penilaian kualitas *fidelity* (kesetiaan data) dilakukan dengan dua metoda analisa, yaitu analisa subjektif dan objektif.
    a. Data analisa subjektif diperoleh dari hasil kuisioner terhadap 20 orang *responder* berdasarkan penilaian indera penglihatan dan pendengaran sehingga didapatkan nilai *Mean Opinion Score* (MOS).
    b. Data analisa objektif diperoleh dari hasil analisa *file* hasil dari aplikasi *steganography* menggunakan metoda *spread spectrum* berdasarkan parameter

Bit Error Rate (BER), *Symbol Error Rate* (SER), dan *Peak Signal to Noise Ratio*(SNR).

1.3 Tujuan

Tujuan dari laporan penelitian ini adalah :

1. Merancang dan mengimplementasikan perangkat lunak steganografi *audio* dan *image digital* menggunakan metoda *spread spectrum*, yaitu :
   a. Menyisipkan data rahasia pada *audio* WAV atau *image digital* GIF yang bertindak sebagai *carrier file.*
   b. Melakukan proses pengacakan posisi urutan pesan pada *pseudo random noise*.
2. Menganalisa kelebihan dan kekurangan *steganography* yang diimplementasikan pada *audio* dan *image digital* . Analisa yang dilakukan adalah berdasarkan pengaruh panjang data yang akan disisipkan, besar koefisien *chunk* pada *audio* WAV dan nilai *pixel* warna *carrier file* terhadap pembangkitan *pseudo random noise*.

Perubahan kualitas *file* sebelum dan sesudah dilakukan penyisipan :

a. Analisa rasio sinyal terhadap *noise* yang terjadi pada setiap *chunk* atau *pixel* setelah dilakukan penyisipan data rahasia ke dalam *carrier file* dengan cara menghitung PSNR (*Peak Signal-to-Noise Ratio*).
b. Analisa antara *carrier file* sebelum dan sesudah disisipi pesan rahasia dengan menghitung nilai *Symbol Error Rate* (SER) dan *Bit Error Rate* (BER).

c. Pengujian nilai MOS menggunakan indera pendengaran manusia terhadap *carrier file* sebelum dan sesudah proses *steganography*.

1.4 Metoda dan Penyelesaian Masalah

Pada proses pengerjaan laporan penelitian ini, langkah kerja yang ditempuh adalah:

1. Identifikasi permasalahan
2. Melakukan analisa latar belakang, rumusan masalah, dan tujuan akhir yang ingin dicapai.
3. Pengumpulan informasi dan Studi literatur
4. Mengumpulkan informasi dan mempelajari konsep *steganography* pada *audio* dan *image digital* menggunakan metoda *spread spectrum*, *carrier file audio* dengan *forma*t WAV dan *carrier file image* dengan *format* GIF, serta algoritma deret Fibonacci & Lucas.
5. Analisa perancangan aplikasi simulasi
6. Analisa kebutuhan aplikasi simulasi yang akan diterapkan dan melakukan perancangan aplikasi simulasi sesuai dengan judul laporan penelitian ini.
7. Pembangunan aplikasi simulasi
8. Merancang aplikasi simulasi berbentuk perangkat lunak yang bertindak sebagai aplikasi *steganography audio* dan *image digital* menggunakan metoda *spread spectrum*.

9. Melakukan simulasi proses *steganography audio* dan *image digital* lalu menganalisa respon yang terjadi akibat proses penyisipan pesan pada tiap jenis *carrier file*.
10. Menyusun laporan tertulis berdasarkan hasil penelitian yang dilakukan dan mengambil kesimpulan hasil dari penelitian, pemberian saran untuk pengembangan aplikasi simulasi analisa *fidelity* untuk *steganography audio* dan *image digital* yang dibangun ke depannya.