BAB I
PENDAHULUAN

1.1. Latar Belakang

Kemudahan menyebarkan dan mendapatkan informasi saat ini tak lepas dari peran serta teknologi komunikasi yang berkembang demikian pesat. Melalui jaringan internet, hampir segala macam informasi bisa diperoleh. Bagi sebagian orang, informasi menjadi sangat penting dan berharga bila hanya diketahui oleh pihak tertentu saja, sehingga muncullah usaha-usaha pembatasan akses atas suatu informasi melalui berbagai metode pengamanan terhadap pihak yang tidak berkepentingan. Diantara metode yang telah dikenal untuk pengamanan informasi adalah dengan menggunakan teknik kriptrografi dan steganografi. Meskipun mempunyai maksud yang sama untuk mengamankan informasi namun terdapat perbedaan mendasar antara kedua metode tersebut. Kriptografi menyembunyikan/mengolah isi (*content*) pesan sehingga pesan tidak dapat terbaca. Sedangkan steganografi menyembunyikan keberadaan (*existence*) pesan sehingga tidak menimbulkan kecurigaan (*conspicuous*) akan adanya pesan [1].

Steganografi (selanjutnya lebih umum disebut sebagai stego) memerlukan media untuk menyembunyikan pesannya, bisa berupa teks, gambar, audio maupun video. Semenjak peristiwa pemboman gedung WTC di Amerika Serikat tahun 2001, dimana para teroris menggunakan teknik steganografi untuk saling bertukar informasi melalui jaringan internet [2], steganografi menjadi obyek penelitian dan pengembangan yang menarik untuk terus digali lebih dalam. Bermula dari asumsi-asumsi berubah menjadi sesuatu yang bisa diterapkan dengan berbagai metode, baik metode yang baru maupun pengembangan dari metode yang sudah ada dengan pertimbangan untuk meningkatkan efektifitas maupun untuk menutup kekurangan-kekurangan yang ada. Meskipun demikian semua metode tersebut utamanya dimaksudkan untuk mengamankan pesan/informasi yang disembunyikan.

Dengan adanya jaringan internet sebagai sarana pertukaran informasi, metode steganografi yang pada mulanya menggunakan media statis sebagai sarana penyembunyiannya, kini telah memanfaatkan protokol internet itu sendiri untuk penerapan secara *online*. Metode yang dikembangkan adalah dengan

menyembunyikan informasi dalam komunikasi suara yang dilakukan melalui suatu rangkaian perangkat telekomunikasi atau jaringan komputer dengan memanfaatkan protokol internet atau yang sering disebut sebagai *Voice over Internet Protocol* (VoIP) [3]. Penerapan steganografi pada media dinamis ini memberikan tingkat kesulitan yang lebih bagi pihak lain yang berusaha untuk mendapatkan informasi dibandingkan dengan yang menggunakan media statis. Pada media statis, pihak lain bisa mencoba memperoleh informasi kapan saja tanpa tergantung waktu. Sedangkan pada media dinamis diperlukan waktu yang sama untuk memperoleh informasi, yaitu pada saat proses transmisi/pertukaran datanya.

Prinsip kerja VoIP pada dasarnya adalah mengkonversi suara analog menjadi data digital dalam bentuk paket-paket data, kemudian paket data tersebut ditransmisikan melalui jaringan internet. Dengan kata lain, VoIP adalah suatu metode digitalisasi data suara ke dalam bentuk paket-paket data untuk ditransmisikan melalui jaringan IP [3]. *Transmission Control Protocol* (TCP) dan *Internet Protocol* (IP) adalah sebagian dari protokol yang dapat digunakan untuk menyembunyikan informasi di dalam bagian *header* tertentu. Pada protokol TCP/IP yang sering ditemui seperti IP, *User Datagram Protocol* (UDP), dan TCP terdapat *fields* yang tidak terpakai atau opsional. *Fields* tersebut dapat digunakan sebagai *covert channel* [4]. Hal ini memberikan banyak kemungkinan dimana data bisa disimpan dan ditransmisikan antara *host* pengirim dan penerima.

Dengan memanfaatkan *covert channel*, steganografi dapat diterapkan dengan metode *Least Significant Bit* (LSB) [5] pada data suara yang dikirimkan melalui VoIP. Penyembunyian informasi dengan metode LSB merupakan salah satu algoritma paling sederhana yang mudah diimplementasikan dengan tingkat data informasi tambahan yang sangat tinggi. Metode LSB yang digunakan yaitu mengganti bit-bit pada suara asli pada lapisan yang telah ditentukan dengan bit dari aliran paket data yang akan dikirimkan. Algoritma LSB dibuat sedemikian rupa sehingga distorsi yang ditimbulkan pada suara yang ditempeli menjadi seminimal mungkin.

Metode steganografi dengan memanfaatkan *covert channel* tidak memakan *bandwidth* karena *control bits* (*header* dari protokol yang baru) ditransmisikan pada *covert channel*, sehingga data yang dikirimkan tidak terpisah dari suara asli [4]. Penerapan metode LSB dilakukan pada saat proses digitalisasi suara analog dalam

bentuk paket oleh *voice codec* yang digunakan, dalam hal ini adalah Speex [6]. *Codec* Speex didesain sangat fleksibel untuk mendukung kualitas suara pada *bit-rate* rendah (4.8 kbps) maupun *bit-rate* tinggi (16 kbps).

Dengan penerapan metode steganografi ini diharapkan pengamanan penyampaian informasi melalui VoIP dapat terpenuhi serta tetap mempertimbangkan kualitas suara yang dihasilkan.

1.2. Perumusan Masalah

Pada tugas akhir ini terdapat beberapa permasalahan yang menjadi titik utama pembahasan, diantaranya bagaimana menyembunyikan suatu informasi yang akan diamankan secara efektif ke dalam komunikasi VoIP agar tidak mudah diketahui oleh yang tidak berhak, namun mudah didapatkan oleh yang berhak dalam proses rekonstruksinya. Mengingat kendala yang dihadapi oleh VoIP secara umum mengenai kualitas layanan, apakah terjadi perubahan kualitas suara yang dihasilkan akibat proses steganografi yang dilakukan, serta apakah hal ini bisa dijadikan indikasi untuk mendeteksi adanya steganografi pada VoIP.

1.3. Batasan Penelitian

Agar lebih fokus dalam pembahasan masalah, maka penelitian yang dilakukan hanya mencakup batasan-batasan sebagai berikut :

- Proses steganografi menggunakan metode LSB sedangkan *voice codec* yang digunakan adalah Speex.
- Data steganografi yang disembunyikan berupa teks yang langsung diketik.
- Metode steganografi akan diimplementasikan menggunakan bahasa pemrograman Microsoft Visual Basic 6.0.
- Implementasi diujicoba dengan menggunakan dua PC untuk komunikasi VoIP.
- Obyek penelitian ditujukan pada kualitas suara yang dihasilkan.

1.4. Tujuan dan Manfaat Penelitian

Tujuan yang hendak dicapai adalah mengamankan informasi melalui penerapan teknik steganografi pada komunikasi VoIP dengan menggunakan bahasa

pemrograman Microsoft Visual Basic 6.0. Di samping itu, hasil pengujian aplikasi akan digunakan untuk mengenali adanya steganografi pada komunikasi VoIP. Sedangkan manfaat secara umum dari penelitian ini adalah untuk memperkaya khasanah pustaka ilmiah ilmu pengetahuan, khususnya mengenai hal-hal yang berkaitan dengan pengamanan jaringan informasi dan komunikasi suara yang berbasis IP.

1.5. Metodologi

Langkah-langkah dalam penyusunan tugas akhir ini adalah sebagai berikut :

1. Mengumpulkan data referensi, baik berupa jurnal, buku, maupun data terkait lainnya serta melakukan studi literatur yang merupakan tahap pendalaman materi, identifikasi permasalahan dan teori yang berkaitan dengan permasalahan dalam penelitian.
2. Mempersiapkan perangkat yang akan digunakan, baik *software* maupun *hardware*.
3. Mendesain, membangun, dan menguji sistem yang diimplementasikan melalui simulasi antara dua titik.
4. Menganalisis data uji yang telah dihasilkan dan memberikan simpulan.

1.6. Sistematika Penulisan

BAB I : PENDAHULUAN

Bab ini menguraikan latar belakang pemilihan topik, masalah yang dihadapi, batasan-batasan yang ditetapkan berkaitan dengan masalah yang ada, tujuan dan manfaat penelitian, metodologi penyusunannya serta sistematika penulisan tugas akhir.

BAB II : TINJAUAN PUSTAKA

Bab ini menjelaskan teori tentang metode steganografi, komunikasi VoIP, dan teori penunjang lain yang berkaitan dengan tema tugas akhir.

BAB III : DESAIN SISTEM DAN IMPLEMENTASI

Bab ini berisi tentang tahapan membuat algoritma steganografi dengan menggunakan metode LSB serta proses implementasinya

dengan menggunakan bahasa pemrograman Microsoft Visual Basic 6.0.

BAB IV : PENGUJIAN DAN ANALISIS

Bab ini akan menjelaskan tentang pengujian terhadap aplikasi yang dibuat beserta analisis atas hasil pengujiannya.

BAB V : PENUTUP

Bab ini berisi simpulan yang berkaitan dengan hal-hal yang telah dibahas sebelumnya serta rencana ke depan yang dapat dimanfaatkan untuk pengembangan topik lebih lanjut.