ABSTRAK

Steganografi merupakan salah satu teknik enkripsi alternatif saat ini.Steganografi menyembunyikan pesan di dalam pesan lain yang bisa berupa teks, gambar, dan sebagainya. Karena biasanya manusia kurang peka dengan pesan yang tidak berbentuk teks yang mudah terlihat, steganografi menjadi jarang terdeteksi.

Steganografi digital menggunakan beragam media digital untuk menyembunyikan pesan. Media tersebut bisa berupa gambar, audio, atau video. Teknik penyembunyian pesan yang digunakan juga beragam. Saat ini telah banyak pendekatan untuk mendeteksi steganografi pada gambar digital. Namun, masih sedikit metode yang dipublikasi untuk mendeteksi steganografi pada data suara, padahal teknologi pengiriman data suara telah banyak yang dilengkapi dengan *field* untuk steganografi, salah satunya VoIP.

Pada tugas akhir ini akan diimplementasikan penerapan steganografi pada VoIP. VoIP (*Voice over Internet Protocol*) merupakan salah satu media untuk berkirim pesan berbentuk suara dimana protokol yang digunakan RTP (*Real time Protocol*). VoIP mengirimkan data berupa suara menggunakan paket-paket IP. Apabila suara yang berupa paket-paket IP tersebut 'dicuri' di tengah jalan, pencurinya akan segera mengetahui isinya. Untuk mengatasi hal tersebut, VoIP dilengkapi dengan *field* untuk steganografi. *Field* tersebut akan digunakan sebagai *covert channel*, dimana pesan rahasia dapat dialirkan secara tersembunyi. Selain itu dapat diterapkan juga metode *least significant bits* (LSB) pada data suara yang akan dikirimkan melalui VoIP.

Selain itu, pada tugas akhir ini telah dilakukan analisa pada performansi kinerja Steganografi pada VoIP, mengenai kualitas suara terhadap data yang disisipi dan sebelum disisipi, yang mana delay dari Steganografi VoIP 0.173282344 ms dan VoIP 0.016009571 ms masih dalam standar ITU-T dengan kualitas MOS baik. Pengujian ekstraksi pesan yang diterima oleh server dan client dapat terealisasi dengan baik, dan dapat berkomunikasi secara fullduplex. Untuk Pengujian keamanan dilakukan *Man in the middle attack*, secara implementasi akan sulit untuk melakukan dekripsi pada steganografi VoIP untuk pihak penyerang karena data pesan berupa biner dan disisipi di payload RTP.

Kata kunci : Steganografi, covert channel, VoIP,Kriptografi, RTP