
Abstrak

Layanan PSTN (*Public Switched Telephone Network*) yang umum digunakan masyarakat untuk melakukan komunikasi suara, memiliki tingkat keamanan yang rendah. Informasi suara yang dikirimkan dapat disadap dengan mudah. Salah satu cara pengamanan informasi suara pada PSTN adalah dengan cara melakukan teknik kriptografi.

Pada Tugas Akhir ini, dirancang antarmuka yang mengubah sinyal suara menjadi data digital sebelum dilakukan proses enkripsi data. Selain proses digitalisasi suara, juga perlu dilakukan proses kompresi data digital yang dihasilkan karena keterbatasan bandwidth saluran PSTN. Proses selanjutnya adalah melakukan enkripsi pada data hasil kompresi ini, dan kemudian ditransmisikan ke jaringan PSTN melalui modem.

Penggunaan FPGA dititikberatkan pada antarmuka dan pengaturan blok kompresi yang menggunakan chip AMBE-2000 dengan blok kriptografi. Serta pada antarmuka blok kriptografi dengan modem. Bagian kriptografi didesain agar algoritma yang digunakan dapat dipilih sesuai dengan kebutuhan. Modul kriptografi yang disediakan sebagai contoh menggunakan proses XOR untuk melakukan enkripsi dan dekripsi.

Pada implementasi yang dilakukan dengan software Xilinx ISE 7.1 pada chip FPGA Xilinx Spartan-IIIE XC2S300E-6fg456, jumlah slice yang terpakai adalah 287 slice dari 3072 (9%). Sedangkan total waktu yang digunakan untuk melakukan pemrosesan data keluaran dari blok kompresi sampai dengan pengiriman pada modem adalah 1,0416 mS.

Kata kunci: kompresi suara, AMBE-2000, FPGA, PSTN