DESAI DAN IMPLEMENTASI BLOK KONTROL PERANGKAT KRIPTOGRAFI SUARA PADA PSTN BERBASIS FPGA

Dwi Mizanul Alim[1], -[2]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak
tidak tersedia

Kata Kunci :

Abstract
The result of quantitative analysis shows that this PCG system with using active filter order 8 and frequency cut-off 2000 Hz have a value of S/N is 19.323 dB. Meanwhile, the qualitative analysis shows that this system is good with the mean value of MOS is 3,73. Refer to the result of analysis, this system is suitable for being an object of medical learning and engineering.
The result of quantitative analysis shows that this PCG system with using active filter order 8 and frequency cut-off 2000 Hz have a value of S/N is 19.323 dB. Meanwhile, the qualitative analysis shows that this system is good with the mean value of MOS is 3,73. Refer to the result of analysis, this system is suitable for being an object of medical learning and engineering.
The result of quantitative analysis shows that this PCG system with using active filter order 8 and frequency cut-off 2000 Hz have a value of S/N is 19.323 dB. Meanwhile, the qualitative analysis shows that this system is good with the mean value of MOS is 3,73. Refer to the result of analysis, this system is suitable for being an object of medical learning and engineering.
The result of quantitative analysis shows that this PCG system with using active filter order 8 and frequency cut-off 2000 Hz have a value of S/N is 19.323 dB. Meanwhile, the qualitative analysis shows that this system is good with the mean value of MOS is 3,73. Refer to the result of analysis, this system is suitable for being an object of medical learning and engineering.

Keywords : The result of quantitative analysis shows that this PCG system with using active filter order 8 and frequency cut-off 2000 Hz have a value of S/N is 19.323 dB. Meanwhile, the qualitative analysis shows that this system is good with the mean value of MOS i

Bab I
Pendahuluan

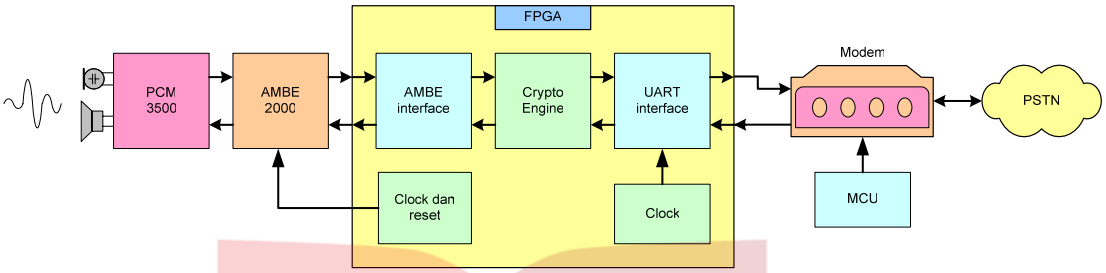
1.1. Latar Belakang

Masalah keamanan merupakan salah satu aspek penting dalam sebuah sistem informasi. Walaupun kadang dianggap sepele dan dinomorduakan oleh pengelola sistem informasi, masalah ini menjadi suatu parameter kehandalan suatu sistem informasi. Informasi saat ini telah menjadi salah satu dari aset berharga suatu organisasi. Baik berupa organisasi komersial (perusahaan), sekolah, perguruan tinggi, lembaga pemerintahan, militer, atau bahkan sebagai individu.

Informasi ini seringkali hanya boleh diakses oleh pihak-pihak tertentu. Jika informasi tersebut jatuh ke pihak yang tidak berhak, akan dapat menimbulkan kerugian bagi pemilik informasi. Oleh karena itu proses pertukaran informasi harus dilakukan secara aman dan terjamin kerahasiaannya.

Seiring dengan berkembangnya ilmu pengetahuan dan teknologi, terutama pada teknik penyandian data, telah ditemukan berbagai macam sistem / algoritma kriptografi (*cryptography*). Kriptografi adalah suatu ilmu menyamarkan atau menyandikan pesan yang bertujuan untuk menghindari perolehan pesan secara tidak sah. Dengan teknik kriptografi, data asli (*plaintext*) yang akan dikirim, diubah kedalam bentuk data sandi (c*iphertext*). *Ciphertext* tersebut dikembalikan ke bentuk data semula dengan menggunakan suatu kunci (*key*) tertentu yang hanya dimiliki oleh pihak yang berkepentingan.

Salah satu bentuk informasi yang saat ini dan pada masa yang akan datang akan terus digunakan adalah berupa suara (*voice*). Penggunaan saluran PSTN (*Public Switched Telephone Network*), telah umum digunakan dimasyarakat untuk melakukan komunikasi suara. Dengan meningkatnya kebutuhan masyarakat akan komunikasi yang aman, diperlukan penyandian informasi suara yang dikirim melalui saluran ini.



Gambar 1 Blok diagram sistem

Gambar 1 merupakan blok diagram sistem. Proses penyandian pada pengirim dilakukan dengan terlebih dahulu mengubah sinyal suara analog menjadi digital, karena proses penyandian dilakukan secara digital. Pengubahan suara menjadi digital dilakukan dengan menggunakan chip ADC / DAC PCM-3500. Chip ini dapat mengubah data suara menjadi data digital, dengan resolusi 16 bit pada sampling rate 8000 sampling per detik. Sehingga total data rate yang dihasilkan adalah 128 kbps.

Kanal PSTN tidak dapat membawa data digital dengan rate setinggi ini, sehingga perlu dilakukan proses kompresi pada data ini. Proses kompresi dilakukan dengan menggunakan chip *Voice Coder* AMBE-2000. Data hasil kompresi dari chip ini memiliki rate 9600 bps, sehingga dapat dengan mudah dilewatkan melalui kanal PSTN. Chip ini membutuhkan sinyal clock dan reset yang sesuai agar proses pengiriman data dapat berlangsung.

Format data dari AMBE-2000 yang digunakan masukan *plaintext* untuk blok penyandi (*Crypto Engine*), memiliki format keluaran yang khusus. Sehingga sebelum melakukan penyandian pada data ini perlu dilakukan pengubahan format data menjadi data paralel 8 bit. Demikian juga pada penerima perlu dilakukan pengubahan format data paralel 8 bit *plaintext* keluaran dari blok penyandi, menjadi format data yang sesuai dengan format data AMBE-2000.

Data keluaran paralel yang telah terenkripsi (*ciphertext*) dari blok kriptografi, dikirim ke saluran PSTN melalui modem. Modem yang digunakan adalah modem standar V.90, dengan kecepatan transfer data maksimum 56 kbps. Modem ini menggunakan sistem antarmuka serial asinkron RS-232. Sehingga keluaran

ciphertext yang menggunakan format paralel 8 bit perlu diubah menjadi data serial asinkron, sebelum ditransmisikan melalui modem. Pada bagian penerima, data serial asinkron dari modem diubah menjadi data paralel 8 bit, dan kemudian disimpan pada sebuah buffer. Data yang ada pada buffer ini kemudian dibaca blok penyandi untuk diubah kembali menjadi data *plaintext*.

1.2. Tujuan

Tujuan dari perancangan sistem ini adalah:

1. Merancang rangkaian kontrol untuk mengatur kerja chip AMBE-2000 berupa pemberian sinyal clock dan reset, yang diimplementasikan pada FPGA (*Field Programmable Gate Array*);
2. Menyediakan antarmuka pengubah format data yang diperlukan antara chip AMBE-2000 dan blok kriptografi;
3. Menyediakan antarmuka pengubah format data yang diperlukan antara blok kriptografi dan modem;
4. Menyediakan blok kriptografi yang fleksibel, sehingga memungkinkan untuk penerapan berbagai macam algoritma kriptografi;

1.3. Rumusan Masalah

Permasalahan yang akan dibahas pada Tugas Akhir ini adalah:

1. Antarmuka blok ADC / DAC (PCM-3500) dengan blok Kompresi / Dekompresi (AMBE-2000);
2. Menyediakan sinyal clock dan reset untuk mengontrol kerja chip AMBE-2000;
3. Konversi format data serial dari AMBE-2000 menjadi format data paralel sebagai input *plaintext* ke blok kriptografi pada sisi pengirim, dan sebaliknya output paralel dari blok kriptografi menjadi format data serial AMBE-2000 pada sisi penerima;
4. Konversi format data paralel *chipertext* dari blok kriptografi menjadi format data serial asinkron untuk modem pada sisi pengirim;

5. Konversi format data serial asinkron dari modem menjadi format data paralel untuk masukan *chipertext* blok kriptografi pada sisi penerima, dengan dilengkapi buffer untuk penampungan data sementara;
6. Menyediakan suatu sistem modular yang fleksibel pada blok kontrol FPGA, sehingga penggunaan *resource* yang terdapat pada FPGA optimal;
7. Menyediakan suatu blok crypto engine yang fleksibel pada FPGA;

1.4. Batasan Masalah

Karena luasnya permasalahan dari perancangan sistem ini, kajian permasalahan pada Tugas Akhir akan diberikan batasan-batasan:

1. Tidak membahas cara kerja blok input dan output analog;
2. Sinyal input berupa suara dengan frekuensi maksimum 4000 Hz;
3. Blok ADC / DAC menggunakan IC PCM-3500;
4. Tidak membahas teknik ADC dan DAC suara, serta algoritma kompresi data suara digital yang digunakan;
5. Blok kompresi dan dekompresi data menggunakan IC AMBE-2000;
6. Tidak membahas jenis dan kinerja algoritma yang akan digunakan pada blok kriptografi (*crypto engine*);
7. Format data masukan dan keluaran blok kriptografi menggunakan format paralel 8-bit;
8. Modem menggunakan modem standar V.90 56 kbps;
9. Tidak membahas jenis dan kinerja sistem modulasi pada modem yang digunakan;
10. Tidak membahas performansi jaringan PSTN;

1.5. Metodologi Pembahasan Masalah

Metode yang akan ditempuh dalam penyusunan Tugas Akhir ini adalah:

1. Studi literatur

   Studi literatur ini menyangkut hal-hal yang berhubungan dengan pokok pembahasan sebagai referensi, serta dari Tugas Akhir Mahasiswa STT Telkom dan perguruan tinggi lain, yang mendukung Tugas Akhir ini.

2. Desain dan Simulasi

   Proses pendesainan dan simulasi dari cara kerja sistem, menggunakan software ModelSim sebagai simulator.

3. Implementasi dan Pengujian

   Desain yang telah berhasil dijalankan pada software simulasi, kemudian akan diimplementasikan pada FPGA dengan menggunakan software Xilinx ISE, dan diuji serta dianalisis kinerjanya.

1.6. Sistematika Pembahasan

Pembahasan pada perancangan ini akan dibagi menjadi 5 (lima) bab, dengan urutan sebagai berikut :

BAB I : PENDAHULUAN

Bab ini membahas tentang latar belakang, maksud dan tujuan, batasan masalah, rumusan masalah, serta sistematika pembahasan dari perancangan sistem.

BAB II : DASAR TEORI

Bab ini mengemukakan dasar-dasar teori yang akan melandasi permasalahan yang akan dibahas.

BAB III : PERANCANGAN DAN IMPLEMENTASI

Bab ini membahas tentang perencanaan perangkat keras *(hardware)* dan perangkat lunak *(software)* pada FPGA.

BAB IV : PENGUJIAN DAN ANALISIS SISTEM

Bab ini menguraikan pengujian dan analisis sistem yang telah di realisasikan. Pengujian sistem akan mengacu pada spesifikasi masing-masing komponen untuk mengetahui apakah hasil rancangan sesuai dengan spesifikasi.

BAB V : PENUTUP

Bab ini berisi kesimpulan terhadap hasil yang diperoleh dari pengujian yang telah dilakukan, serta saran untuk pengembangan sistem ini lebih lanjut.

Bab V
Penutup

5.1. Kesimpulan

Berdasarkan hasil pengujian dan analisa, dapat diambil beberapa kesimpulan:

1. Perbedaan spesifikasi data keluaran PCM-3500 dengan spesifikasi data masukan AMBE-2000, memerlukan sebuah *inverter* antara pin BCK pada PCM-3500 dengan pin CODEC_RX_CLK dan CODEC_TX_CLK pada AMBE-2000.
2. Implementasi sistem pada FPGA Xilinx Spartan-IIE XC2S300E-6fg456 membutuhkan 287 slice dari 3072 (9%). Sisa slice yang masih cukup banyak (2785 slice) memudahkan pemilihan jenis algoritma kriptografi.
3. Waktu dibutuhkan untuk melakukan pemrosesan data, yaitu saat data serial diterima pertama kali dari AMBE-2000 sampai dengan waktu saat data ditransmisikan ke modem adalah 1,0416 mS. Sehingga total delay adalah 2,0832 mS, jauh lebih kecil dari delay maksimum yang dapat ditoleransi pada komunikasi suara secara real time (150 mS).

5.2. Saran

Berdasarkan hasil yang dicapai dalam tugas akhir ini, penulis menyarankan beberapa hal untuk pengembangan lebih lanjut:

1. Blok pengontrol rangkaian dan modem yang masih menggunakan microcontroller MCS-51 untuk selanjutnya dapat diimplementasikan sepenuhnya dengan menggunakan FPGA.
2. Penggunaan saluran PSTN yang rawan tegangan liar dari luar sistem seperti petir, membutuhkan alat pengaman seperti arester.
3. Pemilihan dan implementasi crypto engine yang handal dan cepat diperlukan untuk melengkapi kinerja sistem ini.

4. Bagian untuk melakukan kompresi untuk suara (chip AMBE-2000) untuk selanjutnya dapat diimplementasikan pada FPGA.
5. Modem analog PSTN untuk selanjutnya juga dapat diimplementasikan pada FPGA.

Daftar Pustaka

[1] __, *"AMBE-2000 Vocoder Chip User's Manual"*, Digital Voice Systems Inc., Westford, 2004.

[2] __, *"PCM3500"*, Burr Brown, 1999.

[3] __, "*Spartan-IIE 1.8V FPGA Family: Complete Data Sheet"*, Xilinx Inc., 2004.

[4] __, *"Spartan-IIE LC Development Board User's Guide"*, Memec Design, 2004.

[5] A. Taufan, "*Desain dan Realisasi Perangkat Kriptografi Suara pada PSTN dengan Algoritma Skipjack",* Sekolah Tinggi Teknologi Telkom, Bandung, 2005.

[6] K. C. Chang, *"Digital Design and Modeling with VHDL and Synthesis",* IEEE Computer Society, Los Alamitos, California, 1997.

[7] Electronic System Design Laboratory, "*Modul Pelatihan VHDL & FPGA Short Course 2002",* Sekolah Tinggi Teknologi Telkom, Bandung, Mei 2002.

[8] P. J. Ashenden, "*The VHDL Cookbook*", University of Adelaide, South Australia, 1990.

[9] T. M. Stephen, "*Field Programmable Gate Array Technology*", Prentice-Hall Inc., Singapura, 1991.