Implementasi dan analisa kinerja prototipe reliable and secure end to end voice encryption over public mobile network berbasis domain frekuensi menggunakan prosesor ganda di FPGA = Prototype implementation and performance analysis of reliable and secure end to end voice encryption over public mobile network based on frequency domain using dual processsor in FPGA platform

Yohan Suryanto, author

Abstrak

Penelitian pada tesis ini bertujuan untuk merancang suatu metode enkripsi end-toend untuk komunikasi suara melalui jaringan seluler seperti GSM yang tidak tergantung dari perangkat handphone, sistem operasi, dan perangkat jaringan. Metode yang diajukan adalah enkripsi suara pada domain frekuensi untuk menjaga agar sinyal hasil enkripsi masih tetap berada dalam rentang frekuensi suara yang bisa diteruskan oleh jaringan GSM/2G/3G. Metode ini berbeda dengan metode yang digunakan dalam penelitian-penelitian sebelumnya, dimana mereka menggunakan metode enkripsi berbasis waktu yang bekerja pada rate rendah agar hasil enkripsi bisa disampaikan lewat jaringan GSM. Metode yang ditawarkan disimulaikan menggunakan matlab.
Hasil simulasi menunjukkan bahwa enkripsi suara pada domain frekuensi memiliki karakteristik yang sangat berbeda dengan sinyal aslinya dan bisa diteruskan sepenuhnya melalui jaringan GSM. Metode ini kemudian diimplementasikan dalam FPGA xilinx menggunakan dua prosesor microblaze pada board Atlys. Hasil rekonstruksi modul FFT/IFFT di FPGA Xilinx memiliki deviasi yang bervariasi namun relative kecil, maksimum -10,42 dB, dibanding sinyal aslinya.
Hasil implementasi prototipe menunjukkan bahwa, melalui proses FFTEnkripsi-IFFT dan FFT-Dekripsi-IFFT di modul FPGA, sinyal suara dari pengirim bisa direkonstruksi di handphone penerima secara waktu nyata meskipun dalam kondisi tidak sinkron. Namun, dalam pengembangan prototipe lebih lanjut, tingkat kepresisian modul FFT/IFFT perlu ditingkatkan, serta perlu ditambahkan modul sinkronisasi dan echo canceller.
.....This research aims in designing a method for implementing end-to-end voice encryption over mobile network such as GSM that independent to phone devices, operating system and network devices. The proposing method is an encryption system in domain frequency to keep the encryption signal remain within the range of sound frequencies that can be transmitted through GSM/2G/3G. This method differs compare to the method used in the previous studies, in which they use the time-based encryption method to get a low rate encrypted data so the results can be communicated via GSM network. We simulated the method using Matlab.
The simulation results showed that the voice encryption on the frequency domain characteristics is very different from the original signal and can be passed completely through the GSM network.This method was implemented in the xilinx FPGA using microblaze dual core processor on the Atlys board.
The results of the signal reconstruction using FFT/IFFT module in FPGA xilinx varied in a relatively small deviation, maximum -10.42 dB, compared to the original signal. Performance analysis of the prototype showed the sender speech can be reconstructed real time in the mobile handset of the receiver side, even in

the unsynchronized condition. However, in a further prototype development, the precision level of the FFT/IFFT module needs to be improved, meanwhile the synchronization module and echo canceller need to be added.