DESIGN DAN IMPLEMENTASI S-BOX DALAM AVR ATMEGA8535 SEBAGAI SISTEM PENGACAK SUARA PADA JARINGAN TELEPON

Ages Handriyanto[1], Agus Virgono[2], Joko Haryatno [3]

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

Abstrak

PSTN merupakan salah satu media komunikasi analog yang masih eksis hingga kini, bahkan jumlah penggunanya semakin meningkat tiap tahun. Dilihat dari segi tingkat pengamanan informasi, PSTN merupakan media paling rawan akan tindak penyadapan. Untuk itu dibutuhkannya teknik pengamanan/security suara yang cukup untuk pengamanan informasi yang dilewatkan di dalamnya. Dengan memanfaatkan perkembangan pengacakan data, fasilitas keamanan informasi akan semakin terjamin. Namun itu semua perlu adanya suatu perangkat pendukung dimana kehandalan dan ekonomis sistem pengaman sangat dibutuhkan dalam implementasi terhadap algoritma tersebut.

Pemanfaatan mikrokontroller sebagai perangkat pendukung untuk mengimplementasikan algoritma pengamanan data sangat mungkin dilakukan, hal ini disebabkan semakin lengkapnya fitur mikrokontroller yang memungkinkan untuk diimplementasikan ke dalam berbagai jenis media, hal ini memberikan beberapa keuntungan diantaranya kepraktisan dan reabilitas alat semakin tinggi.

Tugas akhir ini merancang dan mengimplementasikan S – Box (enkripsi data) ke dalam mikrokontroller AVR ATMEGA8535 sebagai system pengacakan suara pada saluran telepon. Sistem secara umum terdiri dari beberapa blok rangkaian yang bekerja baik pada sinyal digital maupun analog yang saling mendukung satu sama lain. Sinyal analog yang mampu diolah hanya terbatas pada sinyal suara dengan frekuensi kurang dari 3400Hz (range suara manusia) yang nantinya akan dienkrip lebih lanjut.

Kata Kunci : Telepon, voice, S-Box, AVR ATMEGA8535.

Abstract

Public Switch Telephone Network PSTN is an analog exist communication media until now, even the number of its user is rising every year. Based on security aspect, PSTN is a very insecure media for taping. Therefore, it is needed voice security technique to save the information which through in it. By taking the benefits of random data, the facility of secure information will be kept. But, it needs a support device where the security system's reliability and economic are much needed in implementing the algorithm.

The advantage of Microcontroller as a support device to implement secure data algorithm can be done, because the feature of Microcontroller more complete so it can be implemented to any kinds of media, this thing give some advantages; the equipment's practical and reliability is higher.

This final project creates and implements S-Box (data encryption) into Microcontroller AVR ATMEGA8535 as a random voice system on telephone line. Basically, the system consists of some circuit blocks that works on digital signal or analog. Analog signal that can be processed is limited to voice signal, where the frequency is less then 3400 Hz (human's range voice) that will be encrypted later.

Keywords : Telephone, voice, S-Box, AVR ATMEGA8535.

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Dengan berkembangnya metode enkripsi, akses terhadap informasi yang dilindungi menjadi semakin terbatas karena informasi tersebut telah disandikan. Hanya yang memiliki pengetahuan tentang penyandian tersebutlah yang dapat mengerti isinya. Tinggal kemudian seberapa canggih teknik penyandian dibandingkan dengan usaha pembongkarannya karena apapun dapat terjadi ketika informasi tersebut ditransmisikan. Seberapa 'kuat' informasi harus dijaga keamanannya tergantung pada tingkat kerahasiaannya/aksesibilitasnya.

Dalam kehidupan sehari-hari enkripsi sangat mudah diaplikasikan terutama untuk tujuan keamanan, *voice* pada saluran telepon merupakan salah satu obyek yang juga membutuhkan pengamanan ektra terhadap informasi yang dibawanya. Implementasi pada mikrokontroler turut memberikan jawaban atas dilema tersebut.

Dengan pemanfaatan algoritma enkripsi yang terus mengalami perbaikan terutama pada sistem transmisi suara, akan berdampak meningkatnya tingkat sekuritas data/suara yang serasa kurang diperhatikan. Jadi sudah sepatutnyalah dunia telekomunikasi mulai diperhatikan tingkat keamanannya, mengingat begitu beragam dan pentingnya informasi yang dilewatkan pada saluran telepon.

Tugas akhir ini bertujuan untuk menyandikan informasi yang berupa suara pada saluran telepon kabel (PSTN) dengan menggunakan metode S-Box yang diimplementasikan pada mikrokontroler AVR ATMega8535. Sehingga diharapkan informasi yang disalurkan oleh telepon tersebut dapat terjamin keamanannya hingga ke tempat tujuan dengan penggunaan modul yang seefisien mungkin.

1.2 Perumusan Masalah

1. Bagaimana perangkat dapat terhubung dengan jaringan PSTN tanpa bantuan modem
2. Bagaimana perangkat dapat melakukan fungsi pengamanan data

3. Metode/algoritma pengacakan data yang mungkin dapat diterapakan dalam perangkat ini
4. Apakah perangkat sanggup bekerja secara *real time*
5. Bagaimana membuat sinyal suara dari jaringan dapat diakses oleh perangkat
6. Bagaimana perangkat dapat melakukan proses pengacakan data dari sinyal analog
7. Bagaimana membuat sinyal digital dapat ditransmisikan ke dalam jaringan telepon
8. Bagaimana cara mengatasi interferensi sinyal suara pada perangkat ini
9. Bagaimana pengaruh performansi jaringan PSTN setelah perangkat dipasang didalamnya

1.3 Batasan Masalah

Untuk menghindari meluasnya materi pembahasan tugas akhir, maka kami membatasi permasalahan dalam tugas akhir ini hanya mencakup hal-hal berikut :

1. Perangkat menggunakan *microcontroller* AVR seri ATMEGA8535.
2. ADC yang digunakan memanfaatkan fitur mikrokontroller yang telah ada, dengan menambahkan rangkaian *pre-amp* di bagian inputnya.
3. Algoritma yang digunakan untuk enkripsi suara, masih menggunakan algoritma konvensional yang tujuannya untuk memperoleh kondisi sistem yang *real time.*
4. Menggunakan DAC jenis *resistor network R/2R.*
5. Filter yang digunakan berupa filter LPF *Bessel* orde-6 dengan frekuensi *cut-off* 3400 HZ.
6. Memanfaatkan DTMF *detector* CM8870 sebagai perangkat On-Off sistem enkripsi.

1.4 Tujuan Tugas Akhir

Adapun tujuan dari tugas akhir ini adalah:

1. Membuat perangkat yang mampu melakukan proses enkripsi data (suara) pada jaringan PSTN

2. Membuat perangkat yang mampu berkomunikasi pada jaringan PSTN dengan baik
3. Membuat perangkat yang mampu digunakan oleh 2 *client* yang saling berkomunikasi secara *real time*

1.5 Metodologi Penelitian

Penelitian ini dilakukan dengan metodologi sebagai berikut:

1. Tahap studi literatur.
   a. Pencarian dan pengumpulan literatur dan kajian-kajian yang berkaitan dengan masalah-masalah yang ada pada tugas akhir ini, baik berupa artikel, buku referensi, internet dan sumber lain yang berhubungan dengan tugas akhir ini.
   b. Pengumpulan data dan spesifikasi sistem yang diperlukan dalam perencanaan sistem.
2. Tahap perancangan, realisasi perangkat.
   Merencanakan dan membuat alat yang telah direncanakan sesuai dengan data–data yang telah didapat.
3. Tahap pengujian perangkat.
   Menguji performansi sistem yang telah dibuat dengan mendengarkan saluran pada setiap titik penyambungan. Apabila suara yang terdengar di tengah "jalan" bukan percakapan *costumer* dan suara tersebut kembali ke aslinya ketika sampai di penerima, maka boleh dikatakan perangkat ini berhasil.
4. Tahap analisis dan penarikan kesimpulan.
   Mencari solusi dari permasalahan yang timbul dengan pencarian data–data dan bertanya kepada narasumber yang berkompeten dibidang ini.

1.6 Sistematika Penulisan

BAB 1 PENDAHULUAN

Dijelaskan mengenai latar belakang, tujuan, rumusan masalah, batasan masalah, dan metoda pelaksanaan penelitian serta sistematika pembahasan laporan.

BAB 2 DASAR TEORI

Berisi tinjauan pustaka dari algoritma S-Box, teori dasar dari mikrokontroller AVR, DAC, ADC, LPF serta isu implementasi yang berkaitan untuk mikrokontroler AVR 8-bit.

BAB 3 PERANCANGAN DAN REALISASI SISTEM

Perancangan dimulai dari deskripsi masalah dan persyaratan pengguna (*user requirements*). Perangkat pengembangan program µC, pembuatan *schematic* rangkaian SISMIN, DAC, LPF dan blok enkripsi itu sendiri untuk dapat dijadikan sebuah sistem enkripsi suara.

BAB 4 ANALISA HASIL REALISASI SISTEM

Menjelaskan tentang hasil-hasil pengujian yang didokumentasikan beserta analisis sistem secara keseluruhan.

BAB 5 KESIMPULAN DAN SARAN

Bab ini berisi simpulan dari implementasi yang dilakukan serta saran untuk pengembangan di masa mendatang.

BAB V
PENUTUP

5.1 Kesimpulan

1. Dari hasil pengukuran dan analisa terbukti bahwa tiap blok rangkaian pada sistem bekerja sesuai dengan fungsinya masing–masing.
2. Sistem baik penerima maupun pengirim sudah dapat berkomunikasi dengan baik pada jaringan telepon tanpa bantuan *modem*, hal ini terbukti suara yang dikeluarkan oleh perangkat terdengar cukup jernih.
3. Perangkat sanggup bekerja secara *real time*, walaupun fungsi pengamanan suara belum tercapai.
4. *Noise* yang ada kemungkinan berasal dari kabel *jumper* dan *ground plane* PCB yang kurang sempurna.
5. Fungsi utama sistem sebagai pengenkrip suara belum tercapai, hal ini disebabkan masalah sinkronisasi *clock* antar sistem ternyata tidak sebatas pengecekan *start byte*.
6. Faktor *noise* di jaringan telepon juga mempengaruhi gagalnya fungsi sistem, karena sinyal masukan dekriptor tidak sama persis dengan keluaran sistem enkriptor sehingga untuk mengembalikan sinyal *chipper* menjadi *plaintext* menjadi sangat sulit.

5.2 Saran

1. Penggunaan algoritma sinkronisasi sistem yang lebih baik agar sistem dapat berfungsi dengan baik.
2. Penggunaan algoritma enkripsi standard pada sistem, agar kinerja enkripsi sistem lebih terjamin.
3. Perancangan PCB harus lebih memperhatikan masalah interferensi sinyal dan *ground plane* agar *noise* yang dihasilkan tidak begitu mengganggu kinerja sistem.

4. Menggunakan penguatan *differential* pada blok *pre-amp* agar sinyal *input* yang masuk tidak mengalami interferensi.
5. Pada blok penyesuai tegangan digunakan resistor *variable* agar sinyal *input* ADC dapat diplotkan pada *range* tegangan referensinya.
6. Pada perangkat ditambahkan blok *modulator* sinyal analog, sehingga *noise* yang muncul tidak begitu signifikan mengubah informasi yang ditransmisikan dalam jaringan telepon.

DAFTAR PUSTAKA

[1] Atmel Corp., “Datasheet: Atmel ATMega8535, 8-bit Microcontroller with 8Kbytes In-System Programable Flash,” 2006.

[2] Bejo, Agus. 2008. *C & AVR Rahasia Kemudahan Bahasa C dalam Mikrokontroller ATMega8535*. Yogyakarta: Graha Ilmu.

[3] Bellare, Mihir and Philip Rogaway. *Introduction to Modern Cryptography*. California, University of California, 2005.

[4] California Micro Device. “Datasheet: CMOS Integrated DTMF Receiver.” 2001.

[5] Fairchild semikonduktor. “Datasheet: 3-Terminal 1 A Positive Voltage Regulator”. 2005.

[6] Motorolla. “Datasheet: Octal 3-State Non-Inverting Transparent Latch, 74HC373”. 1998.

[7] Motorolla. “Datasheet: HEX Inverter, High-Performance Silicon-Gate CMOS”. 1998.

[8] Texas Instruments. *Active Filter Design Techniques*. Texas. 2008.

[9] Sedra, Adel S. and Kenneth C. Smith. 1990. *Microelectronic Circuit*. Orlando: Saunders College.

[10] STMicroelectronic. “Datasheet: General Purpose J-FET Quad Operational Amplifiers”. 2001.

[11] STMicroelectronic. “Datasheet: Seven Darlington Array, ULN2001: 2002: 2003: 2004”. 2007.

[12] Wardhana, Lingga.2006.Belajar sendiri mikrokontroler AVR seri ATMega8535. Jakarta: Penerbit Andi.

[13] http://avrbeginners.net/

[14] http://avr-asm.tripod.com/

[15] http://en.wikipedia.org/wiki/Cryptography

[16] http://educypedia.be/electronics/telephonetopics.htm

[17] http://epanorama.net/circuits/teleinterface.html

[18] http://publicwarehouse.co.uk/schematics/Telephone.php