

IMPLEMENTASI PENGAWASANDIAN VITERBI DENGAN *FIELD PROGRAMMABLE LOGIC ARRAY* (FPGA)

Oleh

Esha Ganesha SBW¹, Bambang Sutopo², Sri Suning Kusumawardani³

1. Mahasiswa TE-UGM 2. Dosen Pembimbing 1 3. Dosen Pembimbing 2

Abstrak

Komunikasi yang dikehendaki adalah data atau informasi yang dikirim sama dengan data atau informasi yang diterima. Galat sering timbul pada saat pengiriman informasi yang dapat mengakibatkan informasi yang dikirimkan tidak sama dengan informasi yang diterima. Sandi konvolusi merupakan salah satu sandi kendali galat yang bisa mengoreksi galat secara otomatis. Penyandi mengubah runtun informasi menjadi runtun kata sandi yang memuat suatu simbol paritas cek tambahan. Pengawasandi menggunakan runtun terima untuk mengoreksi galat dan menghasilkan runtun perkiraan informasi yang apabila galat sudah dikoreksi maka perkiraan informasi akan sama dengan runtun informasi asli.

Kata kunci : komunikasi, galat, sandi konvolusi, penyandi, pengawasandi.

Desired communications is data or information which sent is equal to the received information or data. Error often arises at information transmission which can result the information unlike the received information. Convolution code is one of error control coding which can correct the error automatically. Encoder transforms the information sequence into the code word which contains redundancy of parity-check symbol. Decoder uses the received sequence to correct the error and produce the estimated information sequence which errors are corrected will the same as the original information sequence.

Keywords : communication, error, convolution code, encoder, decoder.

Pendahuluan

Komunikasi pada dasarnya adalah proses untuk menyampaikan pesan dari suatu tempat ke tempat yang lain. Suatu hal yang harus diperhatikan dalam proses pengiriman informasi adalah galat sering timbul pada saat pengiriman informasi. Kemungkinan terjadinya galat pada saat pengiriman cukup besar, sehingga dapat mengakibatkan informasi yang dikirimkan tidak sama dengan informasi yang diterima.

Sandi koreksi galat lebih ditujukan pada sistem komunikasi digital, dimana informasi yang diolah dalam bentuk bit. Informasi dalam bentuk bit ini dikirimkan melalui suatu kanal. Terdapat dua cara mendeteksi galat dan kemudian mengkoreksinya yaitu *error detection and retransmission* dan *Forward Error Correction* (FEC). Teknik *Forward Error Correction* (FEC) merupakan salah satu cara mendeteksi galat yang memungkinkan penerima memperbaiki galat secara otomatis tanpa permintaan transmisi ulang.

Sandi konvolusi merupakan salah satu teknik *Forward Error Correction* (FEC) yang bisa direalisasikan. Suatu penyandi konvolusi akan menghasilkan keluaran yang nilainya bergantung pada masukan informasi sebelumnya, sehingga dalam implementasinya memerlukan memori. Pengawasandi memproses runtun kata sandi yang diterima sehingga dihasilkan runtun perkiraan informasi yang diharapkan sama dengan runtun informasi asli. Salah satu teknik pengawasandian pada sandi konvolusi adalah pengawasandian kemiripan maksimum (*Maximum-Likelihood Decoding*) dengan algoritma Viterbi.

Tinjauan Pustaka

Tuntutan untuk sistem penyimpanan dan pengiriman data digital yang efisien dan handal semakin meningkat. Tuntutan ini dipercepat oleh munculnya jaringan data berkecepatan tinggi dan berskala besar untuk pertukaran, pengolahan dan penyimpanan informasi digital dalam lingkungan militer, pemerintah dan swasta.

Tahun 1948, Shannon menunjukkan dalam papernya bahwa galat yang ditimbulkan oleh kanal berderau atau media penyimpanan bisa dikurangi sampai tingkat tertentu tanpa mengurangi kecepatan transmisi informasi atau penyimpanan. Perkembangan

saat ini telah menambah kepada pencapaian kehandalan yang dibutuhkan oleh sistem digital berkecepatan tinggi dan penggunaan sandi untuk kendali galat telah menjadi bagian integral dalam desain sistem komunikasi modern dan komputer digital.

Teknik penyandian-pengawasandian kanal pada dasarnya berhubungan dengan pengendalian galat pada sandi yang diterima. Secara umum sandi kendali galat dibagi menjadi dua kelompok besar yaitu sandi blok dan sandi konvolusi.

Dasar Teori

Sandi konvolusi berbeda dari sandi blok yaitu penyandi sandi konvolusi dengan n keluaran penyandi pada suatu waktu tertentu tidak hanya tergantung pada k masukan pada waktu itu tetapi tergantung juga m blok masukan sebelumnya. Sandi konvolusi (n,k,m) bisa diimplementasi dengan suatu rangkaian linear k -masukan n -keluaran dengan memori masukan m . Khususnya, n dan k adalah bilangan bulat kecil dengan $k < n$, tetapi tingkat memori harus dibuat cukup besar untuk mencapai kemungkinan galat kecil. Dalam masalah khusus ketika $k = 1$, runtun pesan tidak dibagi menjadi blok-blok dan bisa diproses dengan terus-menerus.

Penyandi konvolusi dengan batas panjang (*constraint length*) n_A terdiri dari m tingkat register geser, n penjumlah modulo-2 dan multiplekser untuk menserialkan keluaran penyandi menjadi runtun sandi tunggal. Masukan data ke penyandi, yang disebut runtun pesan, digeser ke dalam dan sepanjang register geser k bit satu waktu, dan keluaran penyandi diperoleh dengan melakukan konvolusi dari runtun pesan dan runtun pembangkit sandi. Suatu sandi konvolusi (n,k,m) ditentukan dengan himpunan n runtun pembangkit $g_i^{(j)} = (g_{i,0}^{(j)}, g_{i,1}^{(j)}, \dots, g_{i,m-1}^{(j)}, g_{i,m}^{(j)})$, dengan peubah masukan $i = 1, 2, \dots, k$ dan peubah keluaran $j = 1, 2, \dots, n$. Jika runtun pesan $u^{(i)} = (u_0^{(i)}, u_1^{(i)}, u_2^{(i)}, \dots)$ memasuki penyandi satu bit pada satu waktu, maka runtun keluaran penyandi $v^{(j)} = (v_0^{(j)}, v_1^{(j)}, v_2^{(j)}, \dots)$ bisa diperoleh dengan

$$v_{\lambda}^{(j)} = \sum_{l=0}^m \left[\sum_{i=1}^k v_{\lambda-l}^{(i)} g_{i,l}^{(j)} \right] \text{ untuk semua } 0 \leq l \leq \lambda \text{ dan } 1 \leq j \leq n.$$

Pengawasandian kemiripan maksimum merupakan satu teknik pengawasandian pada sandi konvolusi. Teknik pengawasandian kemiripan maksimum dengan algoritma Viterbi yang diperkenalkan oleh Viterbi tahun 1967 menggunakan struktur trellis sandi dan menentukan perkiraan kemiripan maksimum dari runtun yang ditransmisikan yang mempunyai metrik terkecil. Algoritma Viterbi diuraikan sebagai berikut:

- Langkah 1. Mulai pada saat waktu $l = 1$, menghitung *partial path metric* untuk jalur tunggal memasuki setiap keadaan. Menyimpan jalur (*survivor*) dan metriknya untuk setiap keadaan.
- Langkah 2. Menaikkan l dengan 1. menghitung *partial path metric* untuk semua jalur yang memasuki keadaan dengan menambahkan *branch metric* yang memasuki keadaan tersebut dengan metrik yang terhubung *survivor* pada waktu sebelumnya. Untuk setiap keadaan, menyimpan jalur dengan metrik terkecil (*survivor*) termasuk metriknya dan menghilangkan semua jalur lain.
- Langkah 3. Jika $l < L + m$ ulangi step 2. Sebaliknya, berhenti. Panjang runtun kata sandi N dengan metrik terkecil bisa digunakan untuk mengawasandikan bit pesan sepanjang jalur tersebut.

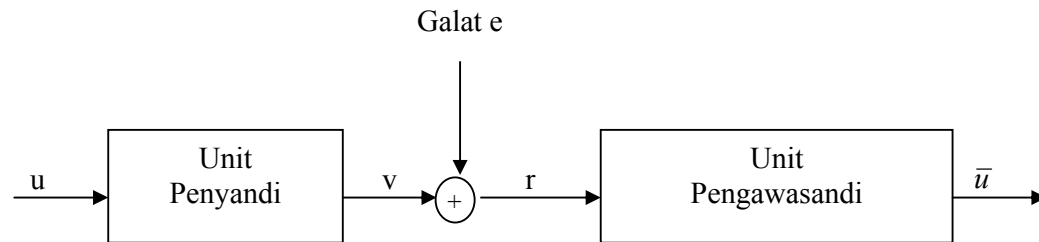
Metodologi Penulisan

metodologi yang digunakan dalam pembuatan tugas akhir ini adalah sebagai berikut:

1. Studi literatur, sebagai bahan acuan untuk mengkaji teori-teori dasar dan teori pendukung yang berupa buku-buku, jurnal-jurnal, ataupun majalah-majalah yang menunjang masalah sandi konvolusi dan implementasinya.
2. Perancangan rangkaian digital sandi konvolusi dengan menggunakan perangkat lunak Orcad, serta melakukan simulasi dari rangkaian tersebut.
3. *Download* rangkaian digital sandi konvolusi ke FPGA XC4013 untuk menguji unjuk kerja rangkaian dalam bentuk perangkat keras.

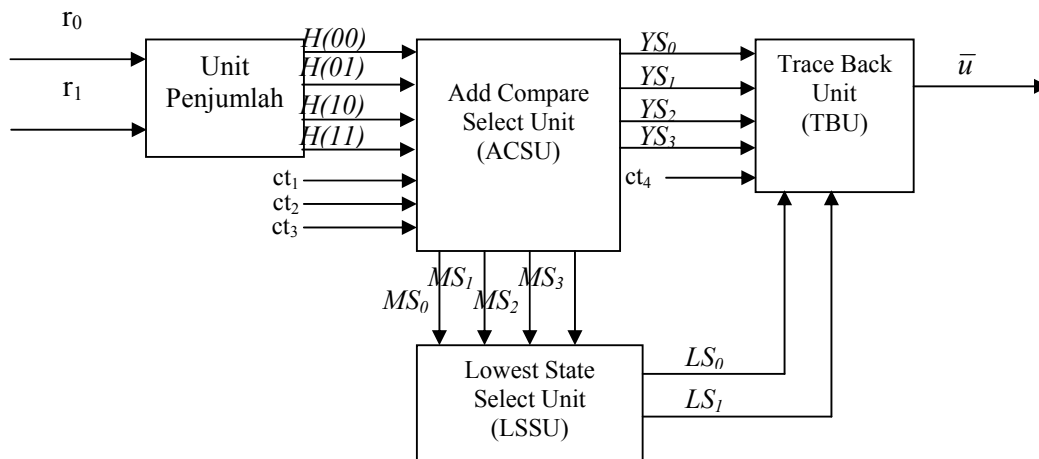
Hasil Implementasi dan Pembahasan

Perancangan sistem sandi konvolusi (2,1,2) secara garis besar dapat dilihat pada Gambar 1.



Gambar 1 Diagram kotak sistem sandi konvolusi (2, 1, 2)

Dengan unit pengawasandi merupakan pengawasandi Viterbi yang tersusun atas 4 subunit. Diagram kotak unit pengawasandi dapat dilihat pada Gambar 2.



Gambar 3.2 Diagram kotak pengawasandi Viterbi

Tampak pada gambar 2 bahwa unit pengawasandi tersusun dari unit penjumlah, *Add Compare and Select Unit* (ACSU), *Lowest State Select Unit* (LSSU) dan *Trace Back Unit* (TBU). Unit penjumlah berfungsi menghitung jarak Hamming antara runtun terima dengan kemungkinan kata sandi. Kemungkinan kata sandi tersebut 00, 01, 10 dan 11. *Add Compare and Select Unit* (ACSU) berfungsi menghitung *path metric* dari setiap keadaan, dimana jumlah keadaan sandi 4 yaitu 00, 01, 10 dan 11. *path metric* merupakan akumulasi dari *branch metric* yang merupakan jarak Hamming antara runtun terima dengan kemungkinan kata sandi. *Lowest State Select Unit* (LSSU) menentukan keadaan yang mempunyai nilai *path metric* terkecil

diantara 4 keadaan tersebut. *Trace Back Unit* (TBU) berfungsi untuk melakukan *trace back* yaitu menentukan keadaan pada saat l kembali keadaan $l-1$.

Panjang runtun informasi dalam perancangan adalah 14 bit, dimana 2 bit terakhir merupakan masukan nol yang akan mengosongkan isi dari memori penyandi sehingga akan dihasilkan kata sandi dengan panjang 28 bit. Masukan rangkaian berupa runtun informasi serta sampel galat diberikan melalui saklar DIP sebagai masukan sinyal digital secara paralel dan keluaran merupakan runtun terima dan runtun terawasandi yang dapat diamati pada LED.

Seluruh rangkaian yang telah dirancang dan disimulasikan akan dikonversi menjadi blok-blok CLB sesuai dengan kebutuhan dan kemudian di *download* ke FPGA. Jumlah CLB yang terpakai adalah 210 CLB atau 36% dari total jumlah CLB yang terdapat pada FPGA seri XC4013.

Pengujian rangkaian dilakukan dengan memberikan berbagai macam kemungkinan masukan pesan dengan jumlah galat tertentu ataupun tanpa galat. Hasil pengujian implementasi rangkaian dapat dilihat pada tabel – tabel berikut.

Tabel 1 Implementasi Sandi Konvolusi (2,1,2) Tanpa Galat

No	Pesan (u)	Terima (r)	Perkiraan Pesan ($\bar{u}$)
1	${}_{\text{LSB}}101005_{16}$	${}_{\text{LSB}}1101000111000038B_{16}$	${}_{\text{LSB}}101005_{16}$
2	${}_{\text{LSB}}100011110F1_{16}$	${}_{\text{LSB}}1101110011100101101100DA73B_{16}$	${}_{\text{LSB}}100011110F1_{16}$
3	${}_{\text{LSB}}010100100124A_{16}$	${}_{\text{LSB}}0011010001111101111101110EFBE2C_{16}$	${}_{\text{LSB}}0101100100124A_{16}$
4	${}_{\text{LSB}}1000111100018F1_{16}$	${}_{\text{LSB}}1101110011100101101100110111ECDA73B_{16}$	${}_{\text{LSB}}1000111100018F1_{16}$
5	${}_{\text{LSB}}101010110011CD5_{16}$	${}_{\text{LSB}}1101000100010010101111101011D7D488B_{16}$	${}_{\text{LSB}}101010110011CD5_{16}$

Tampak dari Tabel 1 bahwa pengawasandi Viterbi mampu menemukan kembali perkiraan pesan yang dikirimkan dengan berbagai macam kombinasi. Setelah pengujian berbagai macam runtun informasi tanpa galat, rangkaian diuji kemampuannya untuk mengkoreksi galat. Pada Tabel 2 dapat dilihat hasil pengujian rangkaian dengan jumlah galat tertentu.

Tabel 2 Implementasi Sandi Konvolusi (2,1,2) dengan Galat

No	Pesan (u)	Terima (r)	Perkiraan Pesan ($\bar{u}$)
1	LSB000000000000 000 ₁₆	LSB1000000000000000000000000000 0000001 ₁₆	LSB000000000000 000 ₁₆
2	LSB000001011100 3A0 ₁₆	LSB0000000000111100100110110000 0D93C00 ₁₆	LSB000001011100 3A0 ₁₆
3	LSB100011110001 8F1 ₁₆	LSB1101110011100101101110110111 EDDA73A ₁₆	LSB100011110001 8F1 ₁₆
4	LSB111111111111 FFF ₁₆	LSB1110010101000101010101010111 DAAAA2A7 ₁₆	LSB111111111111 FFF ₁₆
5	LSB000000000000 000 ₁₆	LSB1100000000000000000000000000 0000001 ₁₆	LSB000000000000 000 ₁₆
6	LSB000001011100 3A0 ₁₆	LSB1000000000110100100110100000 0592C01 ₁₆	LSB000001011100 3A0 ₁₆
7	LSB100011110001 8F1 ₁₆	LSB1100110011000101101110110111 ECDA333 ₁₆	LSB100011110001 8F1 ₁₆
8	LSB111111111111 FFF ₁₆	LSB1110010101001101010101010111 DAAAB2A7 ₁₆	LSB111111111111 FFF ₁₆
9	LSB000000000000 000 ₁₆	LSB1110000000000000000000000000 0000007 ₁₆	LSB000000000000 000 ₁₆
10	LSB000001011100 3A0 ₁₆	LSB1100000000110000100110110000 0D90C03 ₁₆	LSB000001011100 3A0 ₁₆
11	LSB100011110001 8F1 ₁₆	LSB1000110011101101101100110111 ECDB731 ₁₆	LSB100011110001 8F1 ₁₆
12	LSB111111111111 FFF ₁₆	LSB1110010101010101010111101011 D7AAAAA7 ₁₆	LSB111111111111 FFF ₁₆
13	LSB000000000000 000 ₁₆	LSB1111000000000000000000000000 000000F ₁₆	LSB100000000000 001 ₁₆
14	LSB000001011100 3A0 ₁₆	LSB1010000000011100100110110000 0D93805 ₁₆	LSB101001011100 3A5 ₁₆
15	LSB100011110001 8F1 ₁₆	LSB0111110011100101101101100111 E6DA73E ₁₆	LSB100011110001 8F1 ₁₆
16	LSB111111111111 FFF ₁₆	LSB0111010101010001010101001011 D2A8AAAE ₁₆	LSB111111111111 FFF ₁₆

Dari Tabel 2 dapat dilihat bahwa implementasi sandi konvolusi (2,1,2) mampu mengoreksi sampai dengan 3 galat. Untuk 4 galat sandi konvolusi (2,1,2) tidak mampu mengoreksi galat hanya untuk pola galat tertentu mampu dikoreksi, sehingga bit terawasandi tidak sama dengan bit pesan. Dari hasil pengujian tersebut dapat dikatakan bahwa implementasi sandi konvolusi (2,1,2) sudah beroperasi dengan baik.

KESIMPULAN

1. Penyandi dan pengawasandi sandi konvolusi (2,1,2) dengan masukan runtun pesan dan keluaran hasil koreksi paralel dapat direalisasikan ke dalam sebuah keping FPGA seri XC4013 yang memerlukan 210 CLB atau 36%.
2. Implementasi sandi konvolusi (2,1,2) dengan FPGA XC4013 dapat bekerja dengan benar. Sandi konvolusi dapat mendeteksi dan mengkoreksi jumlah galat maksimal 3 dengan sembarang pola galat dan 4 galat dengan pola galat tertentu.
3. Ada 4 kemungkinan *branch word* yang dihasilkan oleh penyandi konvolusi (2,1,2). Kemungkinan *branch word* tersebut digunakan untuk menghitung *branch metric* pada unit penjumlah.
4. *Add Compare and Select Unit* (ACSU) memerlukan 4 rangkaian pengolah *add compare select*, karena sandi konvolusi (2,1,2) mempunyai 4 keadaan.
5. *Trace Back Unit* (TBU) memerlukan 10 rangkaian pengolah *trace back*, karena untuk menemukan 1 bit terawasandi diperlukan 10 kali proses *trace back*.
6. Unit yang diperlukan untuk merancang sandi konvolusi (2,1,2) yaitu unit penyandi, *Branch Metric Unit* (BMU), *Add Compare and Select Unit* (ACSU), *Lowest State Select Unit* (LSSU) dan *Trace Back Unit* (TBU).
7. Perancangan yang paling sulit dilakukan adalah *Trace Back Unit* (TBU), karena proses *trace back* yang rumit.

Daftar Pustaka

Fransiska, 2000, “Perancangan Untai Pencari Polinomial Lokasi Kesalahan Menggunakan Algoritma Berlekamp-Massey untuk Sandi BCH (15.5) yang Efisien berbasis FPGA”, skripsi S-1, Teknik Elektro Fakultas Teknik Universitas Gadjah Mada Yogyakarta.

Rhee, 1989, “Error Correcting Coding Theory”, McGraw-Hill.

Shu lin, Daniel J. Costello JR., 1983, “Error Control Coding Fundamental and Applications”, Prentice-Hall, New Jersey.

Sri Suning Kusumawardani, 2001, ”Implementasi Sandi BCH (15,5) dengan FPGA XC4013”, Tesis S-2, Teknik Elektro Fakultas Teknik Universitas Gadjah Mada Yogyakarta.

Syed Shahzab Shah, Saqib Yaqud, Faisal Suleman, 2001, “Self-Correcting Conquer Noise Part One : Viterbi Codecs”, www.edn.com.

Tabratas Tharom, Marta Dinata, Xerandy, 2002, “Mengenal Teknologi Informasi”, Penerbit Elex Media Komputindo.

T.K. Troung, Ming-Tang Shih, Irving S. Reed, 1992, “A VLSI Design for a Trace Back Viterbi Decoder”, IEEE Transactions on Communications, Vol 40, March, 1992 halaman 616 – 624.

Tocci, R.J., 1995, *Digital System Principle and Application*, Prentice Hall International Edition, Singapore.