DIGITALNI SKREMBLER NEVEN 3000

Zoran Jovanović[1], Miroslav Popović[1], Mile Zrnić[2], Borislav Martinović[2]
[1] FAKULTET TEHNIČKIH NAUKA, Novi Sad, Institut za RAM, Fruškogorska 11, Novi Sad
[2] ČAJAVEC HOLDING, Specijalni uređaji, Jovana Dučića 23a, Banjaluka

Sadržaj - *U ovom radu je opisano rešenje dvokanalnog digitalnog skremblera realizovanog na bazi digitalnog signal procesora DSP56002 sa posebnim osvrtom na programsku podršku uređaja.*

1. UVOD

Digitalni skrembler NEVEN 3000 je uređaj koji omogućava zaštitu govornih informacija u potpunom dvosmernom radu (duplex). Uređaji ove vrste nalaze svoju primenu u vojsci, miliciji, poslovnim sistemima i svim oblastima u kojima je neophodno obezbediti zaštićenost govornih informacija.

Princip na osnovu kojeg je realizovan ovaj uređaj podrazumeva konverziju analognog signala u digitalni oblik, njegovu obradu i na kraju konverziju tako obrađenog signala u analogni oblik.

2. FIZIČKA ARHITEKTURA

Digitalni skrembler NEVEN 3000 predstavlja usavršenu verziju skremblera DS-92 [1]. Komponente fizičke arhitekture NEVEN 3000 mogu se podeliti u dve osnovne funkcionalne celine, a to su :

1. TELEFONSKI DEO
2. PROCESORSKI DEO

Uloga telefonskog dela je obrada analognih signala. Ovaj deo uređaja čine dva PCM CODEC-FILTRA (firme MOTOROLA) sa neophodnim pratećim kolima. Osnovna uloga ovih CODEC-a je pretvaranje digitalnog signala u analogni pre , i iz digitalnog u analogni oblik nakon izvršene obrade (šifrovanja i dešifrovanja). Takođe njihov zadatak je i transformacija odbiraka po A-zakonu.

Procesorski deo uređaja je organizovan oko DSP-a firme MOTOROLA [2] (DSP56002 40MHz). Njegova uloga je obrada digitalizovanih signala u cilju zaštite govornih informacija.

3. PROGRAMSKA PODRŠKA

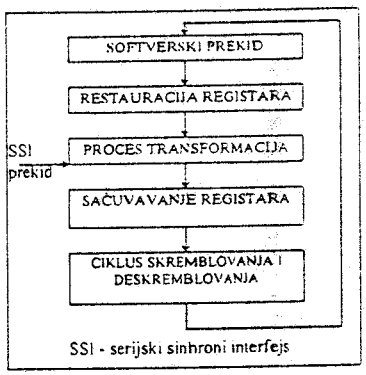
Strukturu programske podrške digitalnog skremblera čine dva procesa :

1. PROCES TRANSFORMACIJA
2. MONITOR

Ova dva procesa su nezavisna jedan od drugog. Raspoređivanje između njih diktira sistem prekida koji takođe predstavlja važnu komponentu programske podrške, vidi sliku 1. Ovi prekidi se generišu svakih 125μs sledećim redosledom:

- prekid za otpremu podataka (u kanal)
- prekid za prijem podataka (iz mikrofona)
- prekid za otpremu podataka (u slušalicu)
- prekid za prijem podataka (iz kanala)

U osnovi proces transformacija je pozadinski proces koji se izvršava u vremenu nakon završetka obrade tekućeg odbirka pa sve do sledećeg SSI prekida. U proces transformacija se ulazi izvršenjem instrukcije softverskog prekida (SWI).Pri ulasku i izlasku iz procesa transformacija smenjuje se kontekst.



Slika 1. Raspoređivanje monitora i procesa transformacija

4. PROCES TRANSFORMACIJA

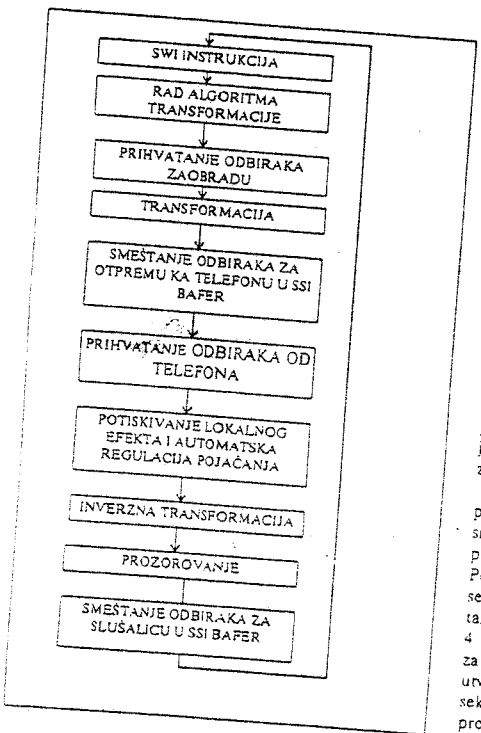
Uloga procesa transformacija je da generiše transformacije na osnovu kojih se unutar monitora šifruje i dešifruje govor. Transformacijom se definiše raspored pojedinih odbiraka unutar jednog prozora. Prozor čini osam odbiraka. Unutar procesa transformacija generišu se i direktna i inverzna transformacija (za prijem i otpremu podataka respektivno). Proces transformacija za svoj rad koristi unutrasnji i spoljašnji ključ. Na osnovu vrednosti ova dva ključa kao i primenjenog algoritma transformacije generiše se adresa naredne transformacije koja se smešta na određene memorijske lokacije u obliku pogodnom za rad monitora.

5. MONITOR

Unutar MONITORA obavljaju se sve transformacije nad digitalizovanim signalom kao i radnje vezane za uspostavu zaštićenog režima i njegov raskid. Monitor je realizovan kao logički automat sa konačnim brojem stanja. Unutar osnovnog stanja proverava se da li je pristigao novi odbirak, pa ako jeste, postavlja se adresa sledećeg stanja i prelazi se u njega.

Osnovne funkcije realizovane u monitorskom procesu (vidi sliku 2) su:

- šifrovanje
- dešifrovanje
- uspostava zaštićenog režima (slanje preambule, najavne sekvence i spoljnog ključa)
- potiskivanje lokalnog efekta



Slika 2. Postupak šifrovanja i dešifrovanja

6. ŠIFROVANJE

Proces šifrovanja se obavlja na osnovu ranije pripremljene transformacije (od strane procesa transformacija). Pre same transformacije signal za slanje se filtriranjem (IIR filtri) razdvaja na dva kanala [3] (200 - 1400 Hz i 1800 - 3000 Hz). Nakon čega se spektar gornjeg kanala (1800 - 3000 Hz) spušta u frekventni opseg donjeg kanala (200 - 1400 Hz). Posle izvršene transformacije vrši se decimacija, prozorovanje, kompresija po A-zakonu i smeštanje odbiraka u otpremni bafer.

7. DEŠIFROVANJE

Osnovu za proces dešifrovanja čini ranije pripremljena (od strane procesa transformacija) inverzna transformacija. Pre inverzne transformacije obavlja se ekspanzija odbiraka po A-zakonu . Nakon dekompresije sledi potiskivanje lokalnog efekta, a zatim interpolacija svakog drugog odbirka. Po izvršenoj transformaciji se spajaju kanali, odbirci se komprimuju i šalju u slušalicu.

8. SINHRONIZACIJA

Postupak sinhronizacije podrazumeva slanje preambule, najavne sekvence i spoljnog ključa kao i prijema istih tih elemenata poslatih od strane drugog uređaja.

Prvo se uspostavlja sinhronizacija na nivou takta, što u ovom slučaju podrazumeva slanje pet uzastopnih nula i jedinica. Koristi se programski realizovan FSK modem. Svaki bit se sastoji od 20 odbiraka što znači da se nakon svakih 20 odbiraka utvrđuje da li se radi o nuli ili jedinici. Svaki odbirak se propušta kroz dva filtera od kojih jedan propušta učestanost koja predstavlja jedinicu, a drugi učestanost koja predstavlja nulu. Tako dobijene vrednosti se smeštaju u odgovarajuće bafere. Svaki od bafera sadrži poslednjih 20 odbiraka i kada njihova suma pređe unapred određenu vrednost proglašava se da je prepoznat bit koji odgovara tom baferu. Kod prijema preambule ovo se proverava nakon svakog odbirka, jer još nije obavljena sinhronizacija na nivou takta pa se ne zna gde je početak bita koji se prima.

Nakon što je primljena preambula pristupa se prijemu najavne sekvence. Pošto je sada izvršena sinhronizacija na nivou takta ispitivanje vrednosti primljenog bita obavlja se samo nakon svakih 40 odbiraka. Posle svakog bita proverava se da li je primljena najavna sekvenca. Zbog mogućnosti da sinhronizacija na nivou takta nije u potpunosti uspela najavna sekvenca se traži na 4 uzastopne pozicije od kojih je svaka sledeća pomerena za pet odbiraka unapred počevši od one pozicije koja je utvrđena prijemom preambule. Po prijemu najavne sekvence prima se spoljni ključ koji je neophodan za rad procesa transformacija. Isti postupak se ponavlja i za drugi uređaj koji učestvuje u sinhronizaciji čime se ovaj postupak i završava.

9. LOKALNI EFEKAT

Lokalni efekat je pojava da korisnik prilikom telefonskog razgovora u slušalici čuje i sopstveni glas. U normalnim okolnostima ova pojava predstavlja lokalnu kontrolu, ali u slučaju kada se govor šifruje to predstavlja ozbiljnu smetnju s obzirom da je šifrovani govor neprijatan za slušanje.

Ovaj problem se rešava modeliranjem sistema to jest telefonskog aparata. Model sistema predstavlja FIR filtar potrebnog reda što zavisi od telefonskog aparata [4], a utvrđuje se merenjem impulsnog odziva. Koeficijenti se određuju uz pomoć iterativnog algoritma koji podrazumeva slanje belog šuma kao pobude i merenja odziva. Na osnovu ovih parova izračunavaju se koeficijenti FIR filtra. Ovim postupkom postiže se svođenje lokalnog efekta na prihvatljiv nivo.

10. ZAKLJUČAK

Realizacija programske podrške u vidu logičkog automata sa konačnim brojem stanja doprinosi fleksibilnosti rešenja i omogućava jednostavnije dodavanje novih funkcija u budućnosti. Takođe izolovanje procesa transformacija u zasebnu celinu omogućuje relativno jednostavne modifikacije algoritma transformacija.

Ovako realizovan digitalni skrembler omogućava visok stepen zaštite govornih informacija.

11. LITERATURA

[1]-Vladimir Kovačević,Miroslav Popović,Ljubica Vujinović,Vidak Bejatović,Ratko Radošević : "Jedno rešenje digitalnog skremblera" ETAN '93

[2]-MOTOROLA: "DSP 56002 user's manual"

[3]-Henry Beker, Fred Piper, "Cipher Systems The Protection of Communications" Northwood Books, London, 1982

[4]-Miroslav Nastić : "Telefonski aparati" Tehnička knjiga, Beograd, 1985

Abstract - This paper describes one realization of two channel digital scrambler based on a digital signal processor DSP 56002, with accent on software realization.

DIGITAL SCRAMBLER NEVEN 3000

Zoran Jovanović, Miroslav Popović, Mile Zrnić, Borislav Martinović