SECRAFONIA PER BANC DE FILTRES

Francesc Vallverdú
Departament de Teoria del Senyal i Comunicacions

El tractament digital del senyal té múltiples aplicacions, entre les més destacades figuren aquelles que tracten senyal analògic en temps real, és a dir aplicacions en les que un senyal analògic és digitalitzat, processat i convertit a analògic novament, sense haver de considerar temps d'espera per fer el tractament. El diagrama de blocs general és el de l'esquema de la figura 1.

Els blocs corresponents a la conversió Analògic-Digital i Digital-Analògica incorporen els dispositius de conversió i els filtres antialiasing i reconstructor necessaris per tal de que la informació no sigui degradada. El bloc corresponent al dispositiu de tractament del senyal digital incorpora un microprocessador de senyal, un banc de memòria, funcions de control i rellotges, i opcionalment algun sistema de comunicació amb un ordinador extern.

Una de les aplicacions que s'han desenvolupat en el Grup de Processament del Senyal del departament de Teoria del Senyal i Comunicacions de la UPC, seguint l'anterior esquema, és un sistema de secrafonia per senyal de veu en telefonia.

Una preocupació constant en molts entorns de la nostra societat és la de la privacitat de les comunicacions telefòniques. És relativament fàcil realitzar escoltes telefòniques sense que l'usuari del sistema en sigui conscient. Una forma d'evitar que les escoltes tinguin cap utilitat és alterant el senyal que s'envia, de manera que resulti inintel.ligible, i dur a terme una reconstrucció per part del destinatari. D'aquesta manera no s'evita l'escolta però si que pràcticament s'anul.la la seva utilitat.

Una tècnica senzilla per fer inintel.ligible un senyal analògic de veu és la de modificar el seu contingut freqüencial. Tradicionalment aquest era un sistema emprat en certs sectors, on el que es feia era simplement invertir el comportament freqüencial en la banda del senyal. Així, les components de baixa freqüència passaven a ocupar la banda alta, i les components d'alta freqüència la banda baixa. El mateix principi d'inversió de banda era utilitzat per l'emissor i pel receptor, i no era necessari cap tipus de sincronisme entre tots dos. Evidentment el sistema era totalment vulnerable, ja que qualsevol podia fer una simple inversió recuperant la intel.ligibilitat del senyal.

Amb el temps aquest sistema es va sofisticar. En lloc de considerar una sola banda pel senyal de veu, el que es pot fer és dividir l'espectre en vàries bandes amb un banc de filtres. Es té un senyal de banda estreta com a sortida de cada filtre. Cada un d'aquests senyals es pot modular (desplaçar en freqüència) de forma adequada, per tal d'obtenir un nou senyal, com a suma de totes les modulacions, amb la mateixa amplada de banda que el senyal original. D'aquesta manera es realitza una mescla de les bandes freqüencials del senyal de veu, pel que es pot aconseguir destruir la intel.ligibilitat. Per tal de recuperar el senyal original cal conèixer quina és la redistribució que s'ha fet de les bandes freqüencials. Aquest sistema és útil en molts casos, però presenta dues limitacions importants. La primera és que el sistema és rígid. Un cop s'ha decidit quina és la barreja de les bandes freqüencials, es dissenya un sistema analògic que la realitzi. Es clar que aquest sistema sempre farà el matiex tractament, pel que un escolta expert pot ser capaç, amb temps, de deduir quina és la barreja produida. La segona limitació important és que el nombre de bandes a considerar és petit, ja que els filtres s'han de dissenyar de tal manera que la suma de les funcions de transferència de tots ells sigui el més plana possible i que es produeixi un mínim de distorsió en les bandes de transició de cada un del filtres.

Amb un sistema de tractament digital aquests inconvenients es

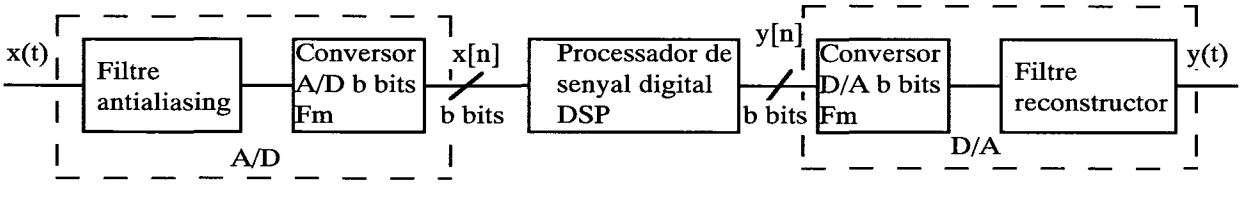

Figura 1.- Diagrama de blocs d'un sistema de tractament digital de senyal analògic.

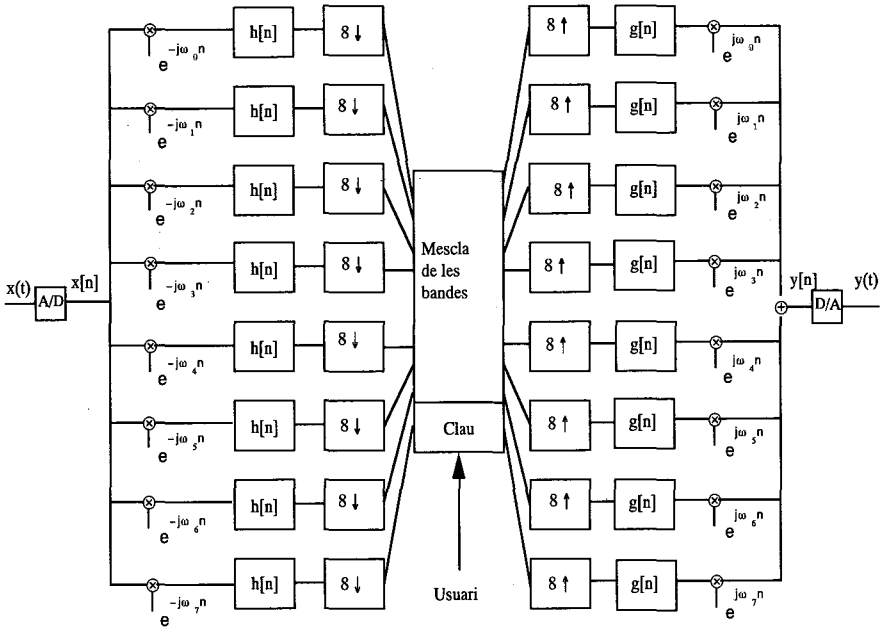

Figura 2. - Esquema general del transmissor.

minimitzen. D'una banda el sistema guanya flexibilitat si es pot definir una clau de barreja de bandes que varii amb el temps tot i essent controlable per l'usuari. D'una altre banda, amb tècniques de disseny de filtres digitals es pot aconseguir augmentar el nombre de bandes sense que es produeixi una degradació important del senyal.

Amb el principi de barreja de bandes descrit s'ha dissenyat un sistema digital on es fa una divisió de l'espectre del senyal de veu en vuit bandes, es realitza la mescla i es forma un senyal secretitzat, tal i com s'il.lustra en la figura 2.

Per fer la selecció de cada banda el que es fa es desplaçar el senyal, de manera que la banda d'interès quedi situada entorn a l'origen. D'aquesta manera es pot filtrar amb un filtre passa-baix, i tenir així un senyal amb amplada de banda 1/8 de l'amplada original, per cada una de les bandes. En aquesta situació es pot fer una delmació per 8, amb el que es tindran 8 senyals corresponents a cada una de les 8 bandes de l'espectre del senyal original.

La reubicació de les bandes es fa interpolant cada un dels senyals de banda estreta per 8 i filtrant passa-banda de manera que aquest senyal de banda estreta quedi ubicat en la zona triada. Cada un dels 8 senyals de banda estreta passarà a ocupar una posició diferent en la banda completa, amb el que sumant aquests 8 senyals s'obtindrà un senyal a transmetre y(t), del mateix ample de banda que el senyal original x(t), però amb les 8 bandes redistribuides per l'usuari. Aquest senyal és doncs un senyal xifrat, i inintel.ligible si no es retorna cada una de les 8 bandes a la seva posició original.

En el diagrama de blocs de la figura 2 apareix un bloc de *Mescla de les bandes*. Aquest bloc no fa altre cosa que definir les conexions entre les seves 8 entrades i les seves 8 sortides. Aquestes conexions són definides per l'usuari i constitueixen la *Clau* de xifrat. Si la conexió és directe no es produeix barreja de bandes, ja que cada banda es reubica en la seva posició original. Si la conexió és creuada es produeix el xifrat.

La implementació pràctica que s'utilitza per fer la selecció de les bandes no és la de la figura 2, si no que respon a la de la figura 3. El resultat és el mateix, es a dir, s'obtenen les 8 bandes per separat. El que es fa és una separació succesiva de l'espectre amb un filtre passa-baix de mitja banda i un passa-alt també de mitja banda. Aquests dos filtres són complementaris, és a dir, la suma del mòdul de les seves respostes freqüencials és constant. La sortida de cada un d'aquests filtres és delmada per dos i es torna a aplicar el mateix procediment fins a obtenir les vuit bandes separades.

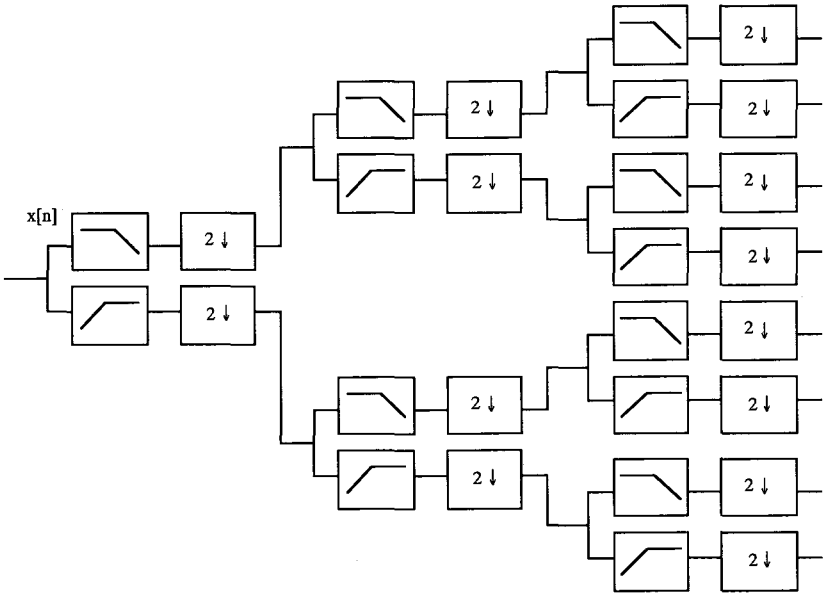

Figura 3. - Esquema utilitzat per dividir l'espectre del senyal d'entrada en 8 bandes.

Amb aquest esquema s'aconsegueix un bon comportament dels filtres, així com un algorisme que permet dissenyar una realització del sistema funcionant en temps real.

En recepció es torna a dividir el senyal en vuit bandes i es desfà la barreja produida pel transmissor per recuperar cada banda en el seu lloc i tenir així el senyal original. Es evident que només es pot recuperar el senyal original si es coneix quin és l'ordre en que s'han de recolocar les bandes. Si aquest ordre es va canviant periòdicament, el sistema de secrafonia guanya en seguretat.

El sistema descrit s'ha realitzat per senyal de veu, limitant l'amplada de banda a 4 kHz, amb el processador de senyal TMS320C30 de Texas Instruments. Aquest processador treballa amb un cicle d'instrucció de 60 ns, el que li permet fer les tasques de transmissor i receptor, pel que es pot utilitzar en una comunicació telefónica en full-duplex convencional. S'ha montat també un sistema demostratiu on es pot definir, amb un PC adicional, la clau de barreja, si es vol escoltar el senyal secretitzat o el recuperat pel receptor, si es vol incorporar algun tipus de filtre simulador de canal, etc. A més, es calcula l'energia a la sortida de cada filtre i es pot veure en pantalla del PC quina és la distribució d'energies en temps real.

El sistema de secrafonia per divisió de l'espectre del senyal amb un banc de filtres digitals és una alternativa vàlida per aquells qui volen protegir les seves comunicacions telefòniques, utilitzant els canals habituals de la xarxa telefònica. No es necessita cap tipus de senyalització ni sincronisme. El sistema és, evidentment vulnerable, però considerant un sistema de claus aleatòries es pot obtenir un grau de privacitat important. El hardware necessari és també relativament simple, i si el sistema es comercialitzes es podria obtenir un preu de cost relativament baix. El sistema no pot competir amb altres sistemes d'encriptat digital existents en quant al grau de seguretat que ofereix, però aquests sistemes necessiten unes característiques de canal que no ofereixen els canals telefònics convencionals.

El treball ha estat fet per en Sergio de Santiago, estudiant de cinquè curs de l'Escola de Telecomunicació de Barcelona, i el va presentar com treball fi de carrera a l'Escola d'Enginyers Tècnics de Telecomunicació «La Salle». En el plantejament teòric pel que es va definir el funcionament del sistema, disseny dels filtres digitals, processador a utilitzar, etc, hi ha participat el Grup de Processament del Senyal.