A TMS320C25-BASED TELEPHONE SCRAMBLER USING FAST-COMPUTABLE FILTER BANKS

HENRIQUE S. MALVAR

Dept. de Engenharia Elétrica, Universidade de Brasília
C.P. 153041, 70910 Brasília, DF, BRAZIL
and
ACRON Telecomunicações e Informática Ltda.
SCRN 704/705, Bloco H, Loja 16, 1º Andar
70730 Brasília, DF, BRAZIL
Fax: +55.61.347-2990

ABSTRACT

In this work we describe the hardware architecture and the signal processing algorithm of a secure telephone which can be used over the public switched network. Using time-varying frequency-domain scrambling, a high level of security can be achieved, with no residual intelligibility. By means of DFT filter banks implemented by the FFT and polyphase networks, all the signal processing for a full duplex conversation can be performed with a single TMS320C25 digital signal processor. The complete scrambler fits inside a standard telephone set unit.

INTRODUCTION

Secure voice communication over the public switched telephone network can be accomplished by means of either digital or analog encryption techniques. With the former, the encoded speech is digitaly cyphered, and transmitted via a high-speed modem. Although very high levels of security can be achieved with this technique, the coding rate must be kept below 12 to 14 kilobits per second. Even with the best known speech coding algorithms, such rates will lead to some perceptible degradation in the speech quality [1].

Analog voice encryption is usually based on time- or frequency-domain scrambling, or a combination of both [2–6]. Although quite simple to implement, time-domain scrambling has an relatively high residual intelligibility and it is also easier to attack [3]. In frequency-domain scrambling, the speech is divided into several subband signals, by means of a bank of filters – the analysis filter bank. The subband signals are fed in a permuted (scrambled) order to the synthesis filter bank, whose output will be an analog signal that can be transmitted over a voice channel. If the filters are independently implemented, the number of subbands must be low, three to five usually, to avoid excessive computational complexity. Then, in order to achieve a large number of possible permutations, i.e. a large key variety, time-domain scrambling of the subband signals is frequently also employed [3].

Frequency-domain-only scrambling with a large key variety can be done if a large number of subbands is used. This requires a frequency decomposition based on a fast transform, such as the fast Fourier transform (FFT), in which a N-sample input block is mapped into a N-coefficient frequency representation. Such an approach leads to the problem of sample and block synchronization, which is necessary to avoid block-rate noise [5, 6]. However, the synchronization requirement can be completely removed if an FFT-based filter bank is employed, as in [2, 4, 6].

In this paper we describe a full-duplex frequency-domain voice scrambler that can be implemented with a single digital signal processor (DSP) chip, the low-cost TMS320C25. We discuss also the ideas behind the permutation matrix generation algorithm and the key management problem. The results of a computer simulation of the scrambling algorithm are also presented.

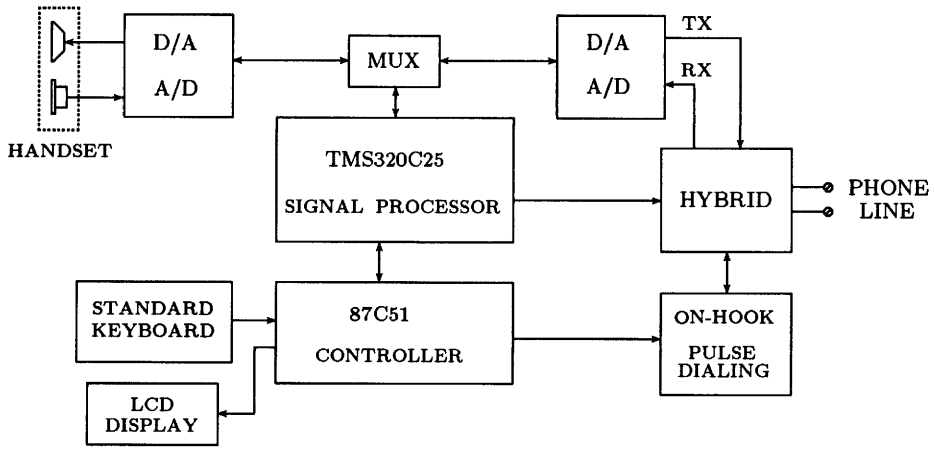

Figure 1: Architecture of the secure telephone.

TWO-PROCESSOR IMPLEMENTATION

The overall architecture of the secure telephone that we developed is shown in Fig. 1. A single TMS320C25 is responsible for scrambling the transmitted signal and descrambling the received signal. The A/D and D/A interfaces are based on low-cost CODEC chips with serial digital I/O signals that interface directly with the TMS320C25 serial port. Another processor, an 87C51 microcontroller, is responsible for the generation of the periodically-varying permutation matrices that are used in the frequency-domain scrambling algorithm. It also controls the keyboard and display of the unit, as well as the communication protocols. Thanks to the secure-programming feature of the device, the permutation matrix generation algorithm is sealed.

With the structure in Fig. 1, the total parts cost of the secure telephone is below US$200 for low volume. All the standard features of a common telephone set, such as automatic redial of the last dialed number, 10-number memory, and others, are easily programmed onto the two processors. Furthermore, the gain of the analog hybrid is automatically adjusted by the TMS320C25; this feature may be helpful in some situations.

FREQUENCY-DOMAIN SCRAMBLING

The block diagram of the basic scrambling algorithm is shown in Fig. 2. A filter bank with N filters $F_0(z)$ to $F_{N-1}(z)$ is used to decompose the incoming signal $x(n)$ into N subband signals. Because the bandwidth of each filter is $2\pi/N$, their outputs can be decimated by a factor of N, so that $X_0(m)$ to $X_{N-1}(m)$ in Fig. 2 are the decimated subband signals, with m denoting the N-sample block index. The subband signals are scrambled by means of the permutation matrix in Fig. 2, in the form

$$Y_r(m) = X_s(m), \quad r = P_m(s), \quad s = 0, 1, \ldots, N-1$$

where the subscript m in the mapping $P_m(\cdot)$ denotes that the permutation may change from block to block. The scrambled subband signals $Y_0(m)$ to $Y_{N-1}(m)$ are fed to the synthesis filter bank $G_0(z)$ to $G_{N-1}(z)$. The output of the synthesis filter bank is the scrambled signal $y(n)$.

As suggested in [2], the DFT filter bank should be employed in Fig. 2, because it has many desirable properties. First, in the absence of permutation, i.e. for $P_m(s) \equiv s$, the reconstruction is almost perfect, with $y(n) \simeq x(n)$ [7]. Second, it can be computed by windowing following by the FFT [2]. In fact, there is an efficient polyphase structure implementation for the DFT filter bank, as shown in Fig. 3, where $p_k(m)$ is the kth phase polyphase component of the N-phase decomposition of the window [7]. Third, signal reconstruction does not require synchronization between the block $\{X_0 \cdots X_{N-1}\}$ and the block $\{Y_0 \cdots Y_{N-1}\}$. Lack of synchronization leads only to a phase error in the reconstruction signal that is virtually inaudible [2, 4].

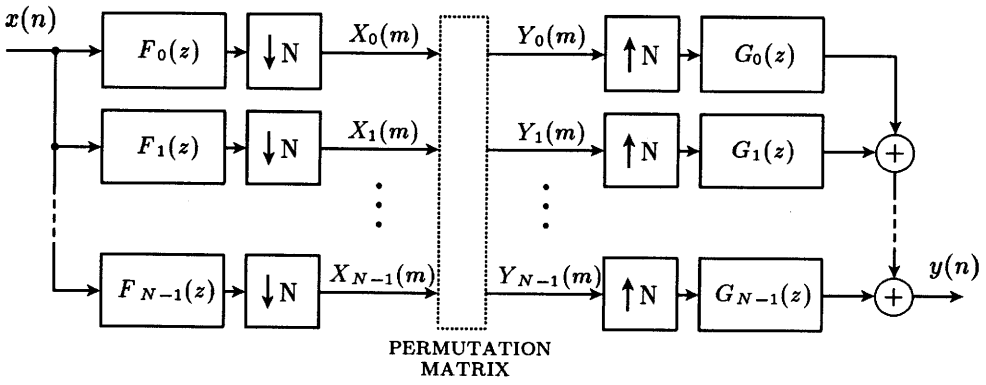

Figure 2: Block diagram of the frequency-domain scrambling algorithm.

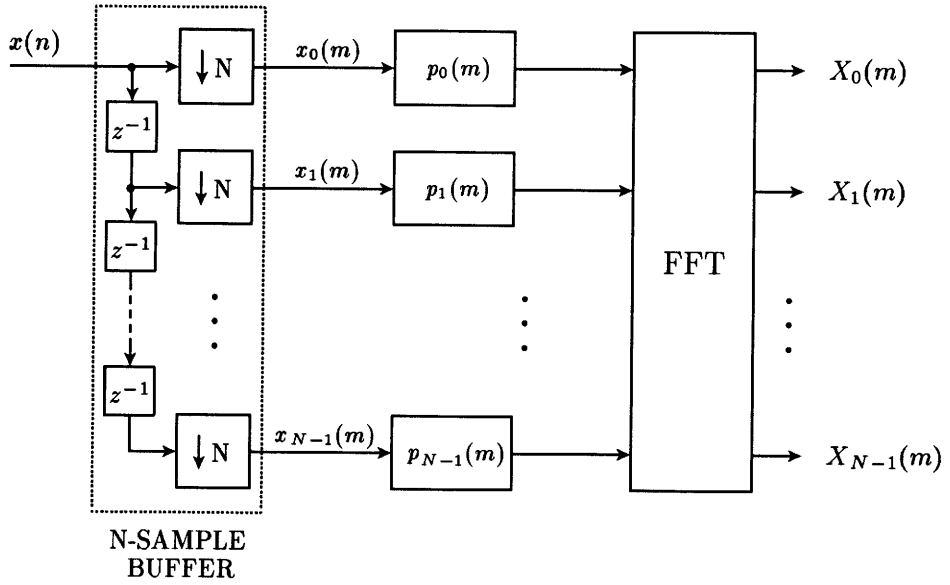

Figure 3: Polyphase structure for implementation of the analysis DFT filter bank. The synthesis structure is similar [7].

In our system, a new permutation matrix P is used for every 64 blocks of length $N = 32$, which corresponds 256 milliseconds. With $N = 32$ and a sampling rate of 8 kHz, we have 17 distinct subband signals: one low-pass subband, 0–125 Hz, one high-pass subband, 3,875–4000 Hz, and fifteen band-pass subbands of width 250 Hz each, with center frequencies varying from 250 Hz to 3,750 Hz. The subbands are numbered from 0 to 16, and the scrambling matrix $P_m(\cdot)$ is such that bands 0, 14, 15, and 16 are not transmitted, and band 1 is not scrambled. Therefore, we are left with 12 permutable bands, which corresponds to a key space of $12! \simeq 4.8 \times 10^8$ possible permutations, changing every 256 milliseconds. Thus, the system is virtually unbreakable by exhaustion.

Due to the DFT filterbank structure of Fig. 3, the computational complexity of the signal processing algorithm is low enough that scrambling and descrambling of a two-way telephone conversation can be done with a single TMS320C25. In fact, less than a third of the DSP computing power is used, and so other features, such as line equalization and automatic gain control, are also performed.

KEY MANAGEMENT

One of the major issues that arise in secure communication equipment is that of key management. For a secure telephone operating over the public switched network, efficient key management is virtually impossible. Therefore, we have used in our secure telephone a "pseudo public-key approach", borrowing ideas from the DH and RSA cryptosystems [8]. Therefore, the effective key K_E that is used in the algorithm that generates the sequence of permutation matrices (which runs on the 87C51), is composed of several parts:

- A master key K_M, preprogrammed in the processor. This key can optionally be replaced by a user-defined secondary master key K_{M2}, for private network applications.
- Two messages keys K_{m1} and K_{m2} which are randomly generated at each of the two secure telephones at the beginning of every secure conversation.
- The serial numbers K_{s1} and K_{s2} of each of the two secure telephones.

The use of the keys K_{s1} and K_{s2} ensures that the user does not need to enter any password in order to operate the secure phone. All that is necessary to start the protocol between the two secure telephones is to push the '$*$' key in the standard keyboard of any of them. After a couple of seconds of information exchange between the two telephones, the LCD display will display the message "SECURE MODE" and a red LED will lit, indicating that the scrambling process is operational. Furthermore, an authorized third secure telephone connected to the line will not be able to unscramble the conversation in any direction, since it cannot have the same set of keys $\{K_{s1}, K_{s2}, K_{m1}, K_{m2}\}$.

Once the effective key is defined, a non-linear feedback shift-register algorithm (NLFSR) [8] runs on the 87C51 to generate the sequence of permutation matrices. Since the TMS320C25 only needs a new pair of permutations every quarter of a second, the 87C51 has time to execute over 50,000 instructions for each new permutation matrix. Thus, it is possible to use algorithms with unicity distances [8] greater than 10^6 blocks. Therefore, the message key could be maintained for over 70 hours, which means in practice that it is enough to use a new message key for every new telephone connection.

SIMULATION EXAMPLE

In order to evaluate the effect of block asynchronism between scrambling and de-scrambling, the block diagram of Fig. 2 has been implemented on a general-purpose microcomputer, using the "C" language. For a particular voice segment, the original and descrambled signals, with correct and incorrect synchronism, are shown in Fig. 4. The waveforms are not identical, but they differ only by an approximately linear phase term. Furthermore, there are no noticeable blocking distortions.

The algorithm is now in final phase of programming in the TMS320C25 assembly language. By the end of 1992, the prototype of the secure telephone should be fully functional.

CONCLUSION

We have described a secure telephone based on frequency-domain scrambling that can be used over the public switched network. Due to the use of fast-computable

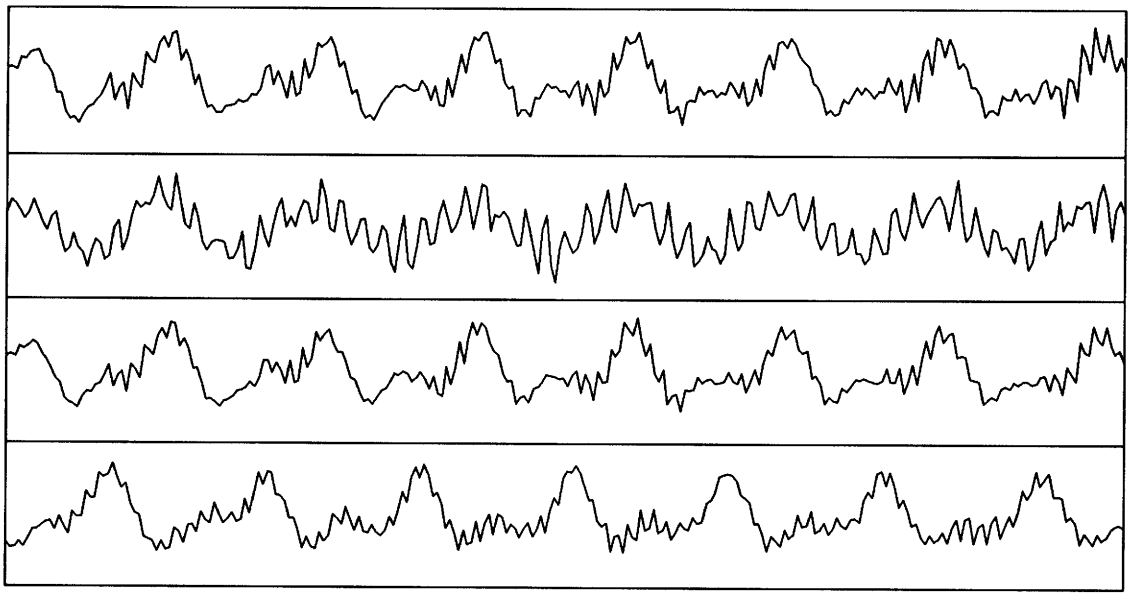

Figure 4: Simulation example. From top to bottom: original speech segment, composed of 8 blocks of length $N = 32$; scrambled speech; unscrambled speech with correct block synchronization; and unscrambled speech with a synchronization error of 13 samples.

DFT filter banks, all the necessary signal processing can be performed, for the two-way conversation, by a single TMS320C25 chip. Because the frequency scrambling matrix is time-varying and generated by a sophisticated non-linear feedback shift register algorithm, a high level of security is achieved. The key management problem does not exist, thanks to the "pseudo public key" system that is employed.

REFERENCES

[1] B. Atal, V. Cuperman, and A. Gersho, *Advances in Speech Coding.* Boston, MA: Kluwer, 1991.

[2] L. Lee, G. Chou, and C. Chang, "A new frequency domain speech scrambling system which does not require frame synchronization," *IEEE Trans. Commun.*, vol. COM-32, pp. 444–456, Apr. 1984.

[3] R. V. Cox, D. E. Bock, K. B. Bauer, J. D. Johnston, and J. H. Snyder, "The analog voice privacy system," *AT&T Tech. J.*, vol. 66, pp. 119–131, Jan.-Feb. 1987.

[4] E. R. Del Re, R. Fantacci, G. Bresci, and D. Maffucci, "A new speech signal scrambling method for mobile radio applications," *Alta Frequenza*, vol. LVII, pp. 133–138, Feb.-Mar. 1988.

[5] A. Matsunaga, K. Koga, and M. Ohkawa, "An analog speech scrambling system using the FFT technique with high-level security," *IEEE J. Selected Areas Commun.*, vol. 7, pp. 540–547, May 1989.

[6] S. Sridharan, E. Dawson, and B. Goldburg, "Fast Fourier transform based speech encryption system," *Proc. IEE,* Pt. I, vol. 138, pp. 215–223, June 1991.

[7] H. S. Malvar, *Signal Processing with Lapped Transforms.* Norwood, MA: Artech House, 1992.

[8] H. C. A. van Tilborg, *An introduction to Cryptology.* Boston, MA: Kluwer, 1988.