New Results on Sampling-Based Scrambling Techniques for Secure Speech Communications

Lin-shan Lee and Ger-chih Chou

Dept. of Electrical Engineering, National Taiwan University

Taipei, Taiwan, Rep. of China

Summary

I. Background

The communication security is getting more and more important today. While enciphering digitized speech is an efficient approach for secure speech communications, there is also an increasing interest in analog scramblers due to the desire to use the existing telephone channels with standard telephone bandwidth at acceptable speech quality and reasonable cost. The concept of scrambling the sample values of the speech waveforms becomes attractive due to its higher degree of security compared to the traditional scramblers[1,2]. But all these sample value scramblers require frame synchronization, i.e., the signal segments used in scrambling and descrambling processes have to be exactly the same for signal recovery. This complicates the implementation and makes the speech transmission very sensitive to channel conditions. A new speech scrambling

algorithm which does not require frame synchronization was proposed recently[3]. In this algorithm the original speech can always be recovered with arbitrary frame location, as long as the scrambling key is known. This algorithm is summarized here.

II. Summary of the Results

The block diagram of the algorithm is in Fig 1. x(n) is the original speech samples. The operation of block P_1 is to multiply 2LN samples of x(n) by a truncated sinc window h(n), break the result into 2L segments of length N, and sum them together to form a vector $\vec{u}_r$, i.e.,

$$\vec{u}_r = \left[u_{rN}(0),\ u_{rN}(1),\ u_{rN}(2),\cdots u_{rN}(N-1)\right]^T,\ r=\text{integer} \quad (1)$$

and

$$u_{rN}(q) = \sum_{t=-L}^{L-1} x(rN+Nt+q)h(-Nt-q),\quad 0\le q\le N-1 \quad (2)$$

$$h(n) = \frac{\mathrm{Sin}(n\pi/N)}{(n\pi/N)},\quad -LN+1\le n\le LN \quad (3)$$

This operation repeats every N samples, i.e., $\vec{u}_r$, r=1,2,3,.... are produced. The block W is an N-sample Discrete Foruier Transform (DFT), transforming the vector $\vec{u}_r$ into $\vec{Y}_r$, i.e.,

$$\vec{Y}_r = \left[Y_{rN}(0),\ Y_{rN}(1),\ Y_{rN}(2),\cdots Y_{rN}(N-1)\right]^T. \quad (4)$$

$$\{Y_{rN}(k),\ k=0,1,2,\cdots N-1\} = \mathrm{DFT}\ \{u_{rN}(q),\ q=0,1,2,\cdots N-1\} \quad (5)$$

Eqs(4)(5) can be written in vector form,

$$\vec{Y}_r = W\,\vec{u}_r \quad (6)$$

Where W is the N×N matrix for DFT. M is an invertible arbitrary scrambling matrix of permutation type which scrambles the vector $\vec{Y}_r$ into $\vec{Y}_r'$,

$$\vec{Y}_r' = M\,\vec{Y}_r \tag{7}$$

W^{-1} is the matrix for inverse DFT, i.e.,

$$\vec{y}_r' = W^{-1}\vec{Y}_r' \tag{8}$$

$$\vec{y}_r' = \left[\, y'_{rN}(0),\ y'_{rN}(1),\ y'_{rN}(2),\cdots\ y'_{rN}(N-1)\right]^T \tag{9}$$

The operation of the block P_2 is first filling intermediate zeros by defining new sequences $z_n(q)$,

$$Z_n(q) = \begin{cases} y'_{rN}(q), & n=rN,\ r=\text{integer},\quad 0\le q\le N-1, \\ 0, & n\neq rN,\ r=\text{integer} \end{cases} \tag{10}$$

and then interpolating to obtain the scrambled speech samples x'(n) using h(n),

$$x'(n) = \sum_{m=n-LN}^{n+LN-1} z_m((n))_N h(n-m) \tag{11}$$

where $((\quad))_N$ represents modulo N. The descrambling operation is exactly the same except M replaced by M^{-1}.

III. Conclusion

The above algorithm is very simple in terms of hardware implementation. It was shown theoretically that with this algorithm the original speech can always be recovered without frame synchronization. An intuitive explanation is that significant redundancy for adjacent frames was introduced by P_1 and P_2 such that synchronization becomes unnecessary. Computer simulation supports the theory, and hardware implementation is completed.

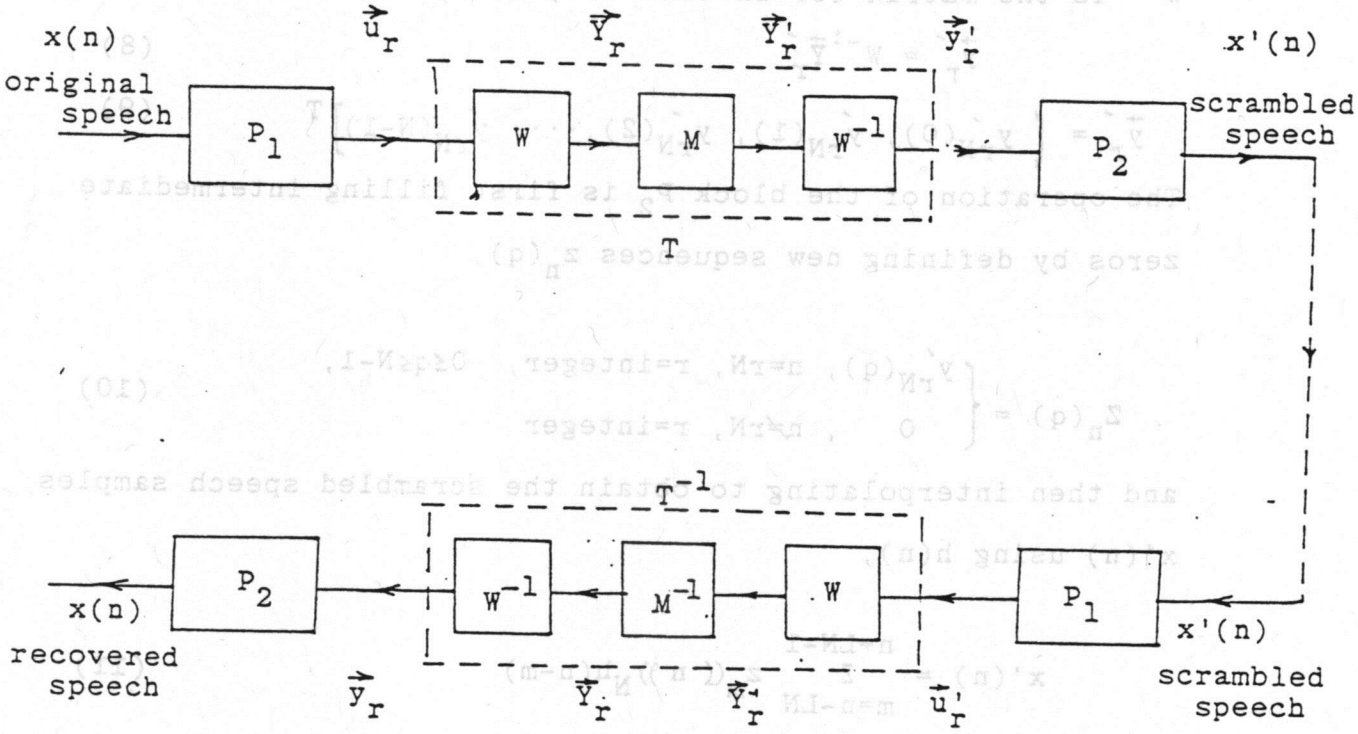

Fig. 1 . The new speech scrambling system proposed .

References

1. A. D. Wyner, "An Analog Scrambling Scheme which Does Not Expand Bandwidth", IEEE Transactions on Information Theory, Vol. IT-25, Part I: Discrete Time: No. 3, May 1979. pp. 415-425. Part II: Continuous Time: No.4, July 1979.

2. S. B. Weinstein, "Sampling Based Techniques for Voice Scrambling". International Conference on Communications, Jun. 1980, Seattle, WA, Record pp. 16.2.1-16.2.6.

3. Lin-shan Lee, et al, "An Efficient and Practical Scrambling System for Secure Speech Communications", National Telecommunication Conference, New Orleans, LA, Dec. 1981.