

TIME-VARYING RECONSTRUCTION OF STATIONARY PROCESSES SUBJECTED TO ANALOGUE PERIODIC SCRAMBLING

Alban DUVERDIER and Bernard LACAZE

National Polytechnics Institute of Toulouse
LEN7/GAPSE, 2 rue Camichel, 31071 Toulouse Cedex 7 BP 7122
tel: (33) 5 61 58 83 67 Fax: (33) 5 61 58 82 37
email: duverdie@len7.enseiht.fr

ABSTRACT

In modern telecommunications, it is often desirable to scramble the contents of the information. This paper presents a particularly efficient method of analogue signal scrambling. A stationary process is subjected to scrambling by means of a linear periodic time-varying filter. We observe then a cyclostationary process. We demonstrate that perfect reconstruction is possible. In presence of overlapping spectra, unscrambling requires a time-varying filter. We apply this method to scramble stationary binary signals. Simulations show that the system is additive noise resistant.

1. INTRODUCTION

These days most encryption is done digitally. Yet, analogue scramblers are known to exhibit desirable properties in numerous applications, such as speech transmission [1]. In fact, they do not need significantly bandwidth increasing. Within this framework, [2] highlighted the interest of scrambling by means of linear periodic time-varying filters. In the reconstruction phase, the authors proposed using linear invariant time filters for non-overlapped spectra. The present contribution extends the existing methods to the (in theory) perfect reconstruction of overlapped spectra. It is shown that this extension requires the application of time-varying filters in order to obtain a sufficient reconstruction quality.

2. LINEAR PERIODIC TIME-VARYING FILTERING

In what follows, the original signal, i.e. the process to be scrambled, will be denoted $Z(t)$. We let $Z = \{Z(t), t \in \mathbb{R}\}$ be a random stationary process of zero mean and mean square continuous. $\Theta_Z(\omega)$ is the Cramér-Loève spectral representation [3] of Z and the two are related by:

$$Z(t) = \int_{-\infty}^{+\infty} e^{i\omega t} d\Theta_Z(\omega) \quad (1)$$

The basic idea of the scrambling system is to subject the original process to a linear periodic time-varying (LPTV) filter, $\tilde{h}$. Let $H_t(\omega)$ be its frequency response, periodic in t of period $T = 2\pi/\omega_0$. We define its Fourier development, assumed to be sufficiently regular, by:

$$H_t(\omega) = \sum_{k=-\infty}^{+\infty} \psi_k(\omega) e^{ik\omega_0 t} \quad (2)$$

with:

$$\psi_k(\omega) = \frac{1}{T} \int_0^T H_t(\omega) e^{-ik\omega_0 t} dt \quad (3)$$

Let $X(t)$ be the response of the stationary process $Z(t)$ through the LPTV filter $\tilde{h}$. $X = \{X(t), t \in \mathbb{R}\}$ is the random process such that:

$$X(t) = \int_{-\infty}^{+\infty} e^{i\omega t} H_t(\omega) d\Theta_Z(\omega) \quad (4)$$

Equations (2) and (4) give:

$$X(t) = \sum_{k=-\infty}^{+\infty} e^{ik\omega_0 t} A_k(t) \quad (5)$$

where the $\{A_k(t)\}_{k \in \mathbb{Z}}$ are the random harmonisable stationary process of zero mean and mean square continuous, defined by:

$$A_k(t) = \int_{-\infty}^{+\infty} e^{i\omega t} \psi_k(\omega) d\Theta_Z(\omega) \quad (6)$$

(5) corresponds to a continuous series representation of X . X is then cyclostationary [4] and its spectral representation can be written as:

$$d\Theta_X(\omega) = \sum_{k=-\infty}^{+\infty} \psi_k(\omega - \omega_0) d\Theta_Z(\omega - \omega_0) \quad (7)$$

$d\Theta_X(\omega)$ is an infinite sum of weighted shifted versions of $d\Theta_Z(\omega)$, centered around multiples of the period and with weights depending on $\tilde{h}$. The greater the support of $d\Theta_Z(\omega)$, the more the different versions will tend to overlap.

3. LINEAR RECONSTRUCTION SCHEME AFTER AN LPTV FILTERING

The scrambling system that we have introduced is depicted by figure 1.

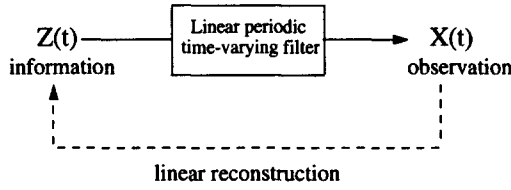


Figure 1, Scrambling method

In order to have an efficient scrambling system, we need a method of perfect information reconstruction. If we suppose known $d\Theta_X(\omega)$ and the functions $\{\psi_k(\omega)\}_{k \in \mathbb{Z}}$, the inversion of equation (7) allows the identification of $d\Theta_Z(\omega)$. In practice, it is possible when the information is supposed to be bandlimited. In this case, we assume that the support of $d\Theta_Z(\omega)$ is contained in $[-\omega_0, \omega_0]$. Equation (7) shows that the overlap is then limited to adjacent components. The modulus of $d\Theta_X(\omega)$ is represented by figure 2.

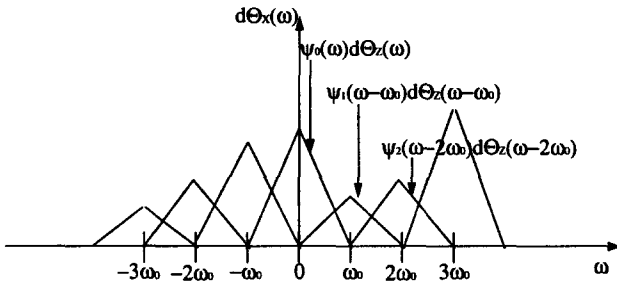


Figure 2, Modulus of the observed signal spectra

Equation (7) gives:

$$\begin{aligned} \forall l \in \mathbb{Z}, \quad \forall \omega \in [0, \omega_0[, \\ \psi_{l+1}(\omega - \omega_0) d\Theta_Z(\omega - \omega_0) \\ + \psi_l(\omega) d\Theta_Z(\omega) = d\Theta_X(\omega + l\omega_0) \end{aligned} \quad (8)$$

(8) corresponds to an infinity of linear redundant combinations of a finite number of variables. To identify these variables, we just have to choose two equations of (8) for two different values of l . For example, if we work with l and $l+1$, we obtain:

$$\begin{aligned} \forall \omega \in [0, \omega_0[, \\ \left\{ \begin{aligned} \psi_{l+1}(\omega - \omega_0) d\Theta_Z(\omega - \omega_0) \\ + \psi_l(\omega) d\Theta_Z(\omega) &= d\Theta_X(\omega + l\omega_0) \\ \psi_l(\omega - \omega_0) d\Theta_Z(\omega - \omega_0) \\ + \psi_{l-1}(\omega) d\Theta_Z(\omega) &= d\Theta_X(\omega + (l-1)\omega_0) \end{aligned} \right. \end{aligned} \quad (9)$$

The perfect reconstruction of $Z(t)$ is then possible if there exists an l such that:

$$\begin{aligned} \forall \omega \in [0, \omega_0[, \\ \psi_l(\omega) \psi_l(\omega - \omega_0) - \psi_{l-1}(\omega) \psi_{l+1}(\omega - \omega_0) \neq 0 \end{aligned} \quad (10)$$

It follows that the identification of the spectral representation of Z may be obtained by:

$$\begin{aligned} \left\{ \begin{aligned} \forall \omega \in [-\omega_0, 0[, \quad d\Theta_Z(\omega) &= \frac{\psi_l(\omega + \omega_0) d\Theta_X(\omega + l\omega_0) - \psi_{l-1}(\omega + \omega_0) d\Theta_X(\omega + (l+1)\omega_0)}{\psi_l(\omega) \psi_l(\omega + \omega_0) - \psi_{l-1}(\omega + \omega_0) \psi_{l+1}(\omega)} \\ \forall \omega \in [0, \omega_0[, \quad d\Theta_Z(\omega) &= \frac{\psi_l(\omega - \omega_0) d\Theta_X(\omega + l\omega_0) - \psi_{l+1}(\omega - \omega_0) d\Theta_X(\omega + (l-1)\omega_0)}{\psi_l(\omega) \psi_l(\omega - \omega_0) - \psi_{l-1}(\omega) \psi_{l+1}(\omega - \omega_0)} \end{aligned} \right. \end{aligned} \quad (11)$$

$Z(t)$ is then given by the response of $X(t)$ through a periodic time-varying filter $\tilde{g}$, such that its frequency response $G_t(\omega)$ is defined by:

$$\begin{aligned} \forall \omega \in [0, \omega_0[, \\ \left\{ \begin{aligned} \forall k \notin \{l-1, l\}, \quad G_t(\omega + k\omega_0) &= 0 \\ G_t(\omega + (l-1)\omega_0) &= \frac{\psi_l(\omega) e^{-i\omega_0 t} - \psi_{l+1}(\omega - \omega_0) e^{-i(l-1)\omega_0 t}}{\psi_l(\omega) \psi_l(\omega - \omega_0) - \psi_{l-1}(\omega) \psi_{l+1}(\omega - \omega_0)} \\ G_t(\omega + l\omega_0) &= \frac{\psi_l(\omega - \omega_0) e^{-i\omega_0 t} - \psi_{l-1}(\omega) e^{-i(l+1)\omega_0 t}}{\psi_l(\omega) \psi_l(\omega - \omega_0) - \psi_{l-1}(\omega) \psi_{l+1}(\omega - \omega_0)} \end{aligned} \right. \end{aligned} \quad (12)$$

In general, there exists several l that verify (10). We can then obtain several reconstructions of Z . This also allows to introduce error correction in the presence of interference or frequency selective noise.

4. EXAMPLE

Let $Z(t)$ be an N.R.Z. signal [5], approximately bandlimited on $[-\omega_0, \omega_0]$, and $\tilde{h}$ a sum of periodic clock changes. The latter is a special case of linear periodic time-varying filters [6]. $\tilde{h}$ is defined then by:

$$H_t(\omega) = e^{-i\omega\alpha \sin(2\omega_0 t)} + e^{i\omega_0 t} e^{-i\omega\beta \sin(\omega_0 t)} \quad (13)$$

The computation of the coefficients $\psi_k(\omega)$ gives:

$$\psi_k(\omega) = \frac{1 + (-1)^k}{2} J_{k/2}(\alpha\omega) + J_{k-1}(\beta\omega) \quad (14)$$

where $J_k(\omega)$ is the k 'th order Bessel function. We take $\alpha = 0.5$, $\beta = 0.5$, $\omega_0 = 20\pi$. In figure 3, we represent the N.R.Z. signal at the input of the LPTV filter.

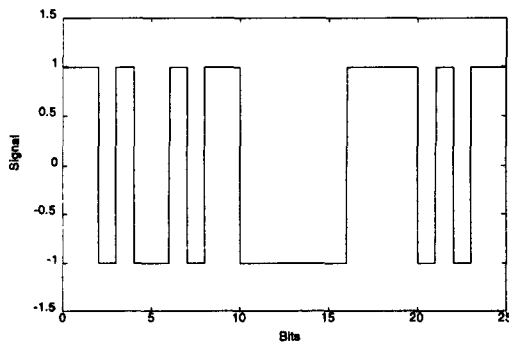


Figure 3, Original signal

Figure 4 depicts the signal observed at the output of $\tilde{h}$.

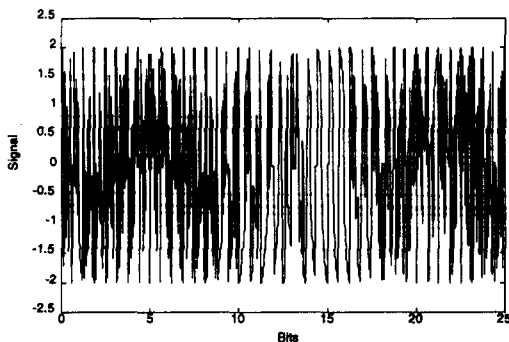


Figure 4, Observed signal

The signal reconstruction presented in figure 4 have been obtained with a low-pass filter. The figures illustrate the efficiency of the scrambling in the sense that the information is irretrievable when a simple low pass filter is used.

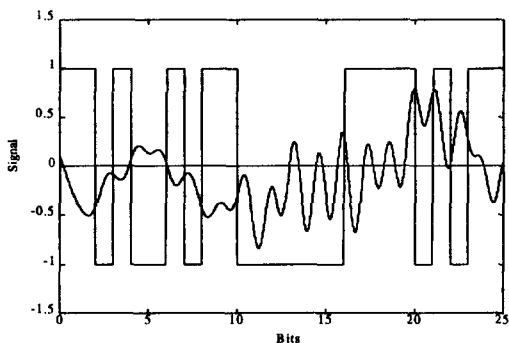


Figure 4, Low pass filtering

Figure 5 shows the signal reconstruction emanating from the optimal time-invariant filter. Even it represents a significant improvement, the bit stream may not be determined without error.

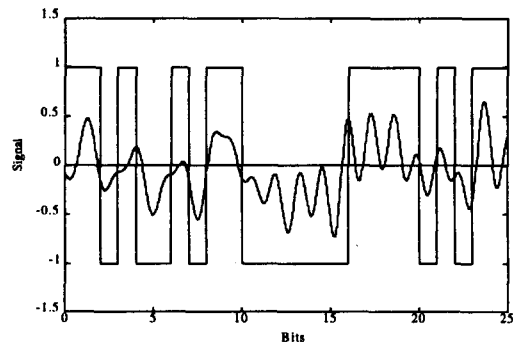


Figure 5, Optimal invariant-time filtering

Figure 6 presents the reconstruction obtained using the time-varying filtering given by equation (11) for $l = 0$. A simple bit detection allows perfect reconstruction when no noise is present.

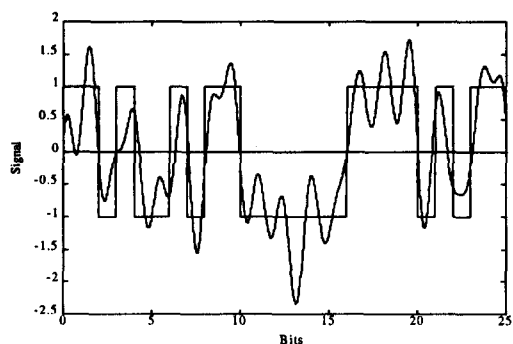


Figure 6, Optimal time-varying filtering

Figure 7 shows the bit error ratio (BER) in presence of Gaussian white additive noise, where the signal-to-noise rate (SNR) is calculated in the frequency range $[-\omega_0, \omega_0]$. We compare the performance of the low-pass filter (.), the optimal time-invariant filter (- -) and the optimal time varying-filter (—). It is easy to see that the time-varying filter ensures adequate noise performance.

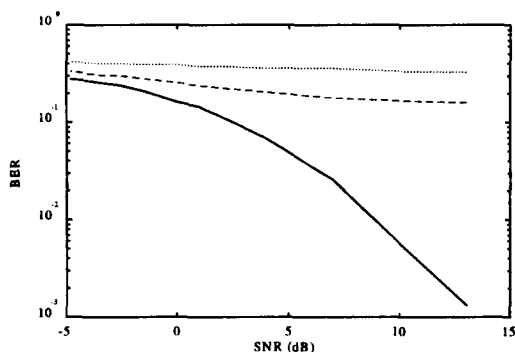


Figure 7, BER of reconstruction schemes

5. CONCLUSION

In this article we have presented a method of perfect linear reconstruction of a stationary process subjected to a linear periodic time-varying filter. We showed, in particular, that the reconstruction was possible even with overlapping spectral components. Finally, this was verified by a simulation example and we indicated the resistance of this system to the presence of additive noise.

6. REFERENCES

- [1] B. Goldberg and S. Sridharan, "Design and Cryptanalysis of Transform-Based Analog Speech Scramblers", *IEEE Journ. Select. Areas in Comm.*, pp. 735-744, 1993
- [2] A. Duverdier, B. Lacaze and N.D. Aakvaag, "A Novel Approach to Spread Spectrum Communication Using Linear Periodic Time-varying Filters", *Lecture Notes in Computer Science*, no 1133, Springer-Verlag, 1996
- [3] H. Cramér and M.R. Leadbetter, *Stationary and Related Stochastic Processes*, Wiley, 1967
- [4] W.A. Gardner and L.E. Franks, "Characterization of cyclostationary random signal processes", *IEEE Trans. Inform. Theory*, pp. 4-14, 1975
- [5] J.G. Proakis, *Digital Communications*, McGraw-Hill, 1989
- [6] N.D. Aakvaag, A. Duverdier and B. Lacaze, "Stochastic processes and linear combinations of periodic clock changes", *Proc. of the ISIT*, p.116, Whistler, Canada 1995