SCRAMBLING AND ERROR CORRECTION BY MEANS OF LINEAR TIME-VARYING FILTERS

Alban Duverdier and Bernard Lacaze
National Polytechnics Institute of Toulouse
LEN7/GAPSE, 2 rue Camichel, 31071 Toulouse, France
tel: (33) 61 58 83 67 Fax:(33) 61 58 82 37
email: duverdie@len7.enseeiht.fr

ABSTRACT

In numerous communication applications, it is desirable to scramble the contents of the information. In addition, we seek to design a scrambling system which has maximum immunity to additive noise. This paper presents a method of analogue signal scrambling/unscrambling by means of linear periodic time-varying filters for any frequency selective noise. It is well known that linear periodic time-varying filters transform a stationary process into a cyclostationary signal. This thus spreads the spectral representation of the input process. The original part of the paper consists of using this property to reconstruct an initial band-limited process without error for any frequency selective noise.

1 INTRODUCTION

Linear periodic filters transform stationary processes into cyclostationary signals. Previous work has shown that this kind of transformation can be useful in analogue signal scrambling. In our contribution, we show that, when a band-limited signal is scrambled, multiple (in theory) perfect reconstructions are possible. If the process is observed in the presence of an unknown frequency selective noise, the present paper proves that the noise tends to disturb only one reconstruction. The mean of several reconstructions then permits the identification of the original signal without any knowledge of the frequency support of the noise. Furthermore, these techniques are easy to implement.

2 DEFINITIONS

2.1 Stationary process

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, zero mean and mean square continuous. Z admits a Cramér-Loève spectral representation $\Theta_Z(\omega)$ [1] such that:

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

In addition, we note $R_Z(\tau)$ its autocorrelation function and $S_Z(\omega)$ its spectrum defined by:

$$R_Z(\tau) = E\left[Z(t)Z^*(t-\tau)\right] = \int_{-\infty}^{+\infty} e^{i\omega t} dS_Z(\omega) \tag{2}$$

2.2 Linear periodic time-varying filter

The basic idea of the scrambling system is to subject the original process to a linear periodic time-varying filter. Let $\tilde{h}$ be a linear time-varying filter. It is defined by its impulse response $h(t,s)$, that transforms Z into X with:

$$X(t) = \int_{-\infty}^{+\infty} h(t,s)Z(s)ds \tag{3}$$

We will study the case where $\tilde{h}$ is an linear periodic time-varying (LPTV) system [2], i.e. where there exists a period $T = 2\pi/\omega_0$ such that:

$$h(t+T, s+T) = h(t,s) \tag{4}$$

The time-varying frequency response of the LPTV filter $\tilde{h}$ is defined by:

$$H_t(\omega) = \int_{-\infty}^{+\infty} h(t, t-\tau)e^{-i\omega\tau} d\tau \tag{5}$$

It is worth noting that $H_t(\omega)$ is periodic in t. We then define its Fourier development, assumed to be sufficiently regular, by:

$$H_t(\omega) = \sum_{k=-\infty}^{+\infty} \psi_k(\omega) e^{ik\omega_0 t} \tag{6}$$

where the Fourier coefficients $\psi_k(\omega)$ are expressed by:

$$\psi_k(\omega) = \frac{1}{T}\int_{-\infty}^{+\infty} H_t(\omega)e^{-i\omega_0 kt} dt \tag{7}$$

3 RESPONSE OF A STATIONARY PROCESS THROUGH AN LPTV FILTER

Let X be the filtering of Z by the LPTV filter $\tilde{h}$ of impulse response $h(t,s)$ and frequency response $H_t(\omega)$ given by (5). Using the Cramér-Loève representation of Z (1), the expression of X given by equation (3) becomes:

$$\begin{aligned} X(t) &= \int_{-\infty}^{+\infty} h(t,s)Z(s)ds \\ &= \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} h(t,s)e^{i\omega s}d\Theta_Z(\omega)ds \\ &= \int_{-\infty}^{+\infty} e^{i\omega t}H_t(\omega)d\Theta_Z(\omega) \end{aligned} \tag{8}$$

Because $H_t(\omega)$ is periodic in t, it can be written in terms of its Fourier series expansion (6). X admits then a continuous-series representation [3] such that:

$$X(t) = \sum_{k=-\infty}^{+\infty} e^{ik\omega_0 t}G_k(t) \tag{9}$$

where G_k is the response to Z through the time-invariant linear filter whose frequency response is $\psi_k(\omega)$:

$$G_k(t) = \int_{-\infty}^{+\infty} e^{i\omega t}\psi_k(\omega)d\Theta_Z(\omega) \tag{10}$$

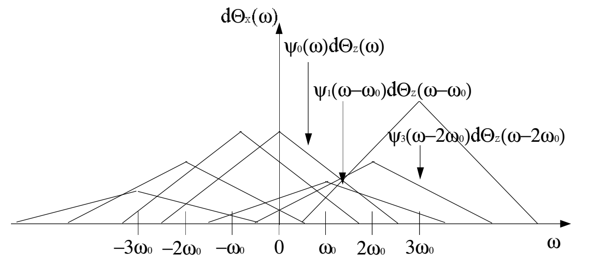
Using the above relation, one obtains that:

$$E\left[G_m(t)G_n^*(t-\tau)\right] = \int_{-\infty}^{+\infty} e^{i\omega\tau}\psi_m(\omega)\psi_n^*(\omega)dS_Z(\omega) \tag{11}$$

The $\{G_k(t)\}_{k\in\mathbb{Z}}$ are jointly stationary processes. Equations (9) and (11) prove then that X is cyclostationary [3]. Let $d\Theta_X(\omega)$ be the Cramér-Loève representation of X. From equation (9), we obtain:

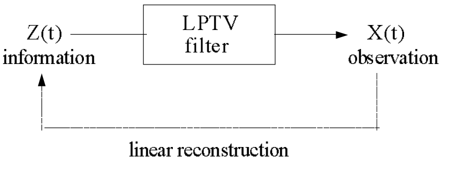
$$d\Theta_X(\omega) = \sum_{k=-\infty}^{+\infty} \psi_k(\omega - k\omega_0)d\Theta_Z(\omega - k\omega_0) \tag{12}$$

The Cramér-Loève representation of X is also an infinite sum of weighted shifted versions of $d\Theta_Z(\omega)$. The individual versions are centered around multiples of the LPTV filter frequency and the weights depend on $h(t,s)$. If we chose for example a support of $d\Theta_Z(\omega)$ included in $[-3\omega_0, 3\omega_0[$, the modulus of (12) can be illustrated by:



4 RECONSTRUCTION OF THE ORIGINAL PROCESS

We suppose now that the output process, $X(t)$, is observed and that the filter, $h(t,s)$, is known. We will present a method of linear reconstruction of Z:



If we suppose that $d\Theta_X(\omega)$ and the functions $\{\psi_k(\omega)\}_{k\in Z}$ (i.e. the LPTV filter) are known, the inversion of equation (12) allows the identification of $d\Theta_Z(\omega)$. Under certain conditions of inversibility, the linear reconstruction of $Z(t)$ without error is then possible. In practice, we consider that the support of $d\Theta_Z(\omega)$ is included in $[-\omega_0/2, \omega_0/2[$. Equation (12) becomes then:

$$\begin{aligned} \forall k \in \mathbb{Z},\quad & d\Theta_X(\omega)\prod\nolimits_{[k\omega_0-\omega_0/2,k\omega_0+\omega_0/2[}(\omega) \\ &= \psi_k(\omega - k\omega_0)d\Theta_Z(\omega - k\omega_0) \end{aligned} \tag{13}$$

where $\prod_{[a,b[}(\omega)$ is the indicator function of the interval $[a,b[$. Let Δ be the integer set such that the functions $\{\psi_k(\omega)\}_{k\in\Delta}$ are different from zero on the spectral support of Z. On the support of $d\Theta_Z(\omega)$, we have:

$$\begin{aligned} \forall k \in \Delta,\quad d\Theta_Z(\omega) &= \psi_k^{-1}(\omega)d\Theta_X(\omega + k\omega_0) \\ & \prod\nolimits_{[-\omega_0/2,\omega_0/2[}(\omega) \end{aligned} \tag{14}$$

This expression shows that it is necessary to know the function $\psi_k(\omega)$ in order to obtain a perfect reconstruction of Z in the k'th band of $d\Theta_X(\omega)$. This filter is thus useful for scrambling. Since we can obtain several reconstructions, this also allows error correction in the presence of frequency selective noise. In fact, the noise tends to disturb only one of the reconstruction. It is then easy to implement an algorithm to get rid of the noise. For example, when a binary signal is scrambled, the mean of several reconstructions permits the identification of the original process without knowing the support of the frequency selective noise.

5 EXAMPLE

5.1 Sum of periodic clock changes

Let $Z(t)$ be an N.R.Z. signal [4], whose frequency support is approximately included in $[-\omega_0/2, \omega_0/2[$. We propose now a particular scrambling scheme that transforms $Z(t)$ into $X(t)$ such that:

$$X(t) = Z(t - f_1(t))g_1(t) + Z(t - f_2(t))g_2(t) \qquad (15)$$

where $f_1(t)$, $g_1(t)$, $f_2(t)$ and $g_2(t)$ are periodic functions of period $T = 2\pi/\omega_0$. This kind of transformation is a sum of two periodic clock changes (PCC) [5]. In a previous work [6], it has been demonstrated that this transformation was a linear periodic time-varying filtering whose frequency response is:

$$H_t(\omega) = e^{-i\omega f_1(t)}g_1(t) + e^{-i\omega f_2(t)}g_2(t) \qquad (16)$$

5.2 Simulation

The results we present below have been obtained for:

$$\left\{ \begin{array}{l} f_1(t) = -\alpha \sin \omega_0 t \\ g_1(t) = 1 \end{array} \right. \qquad (17)$$

and:

$$\left\{ \begin{array}{l} f_2(t) = -\beta \sin(\omega_0 t/2) \\ g_2(t) = \exp(\omega_0 t/2) \end{array} \right. \qquad (18)$$

These functions are periodic with common radial frequency $\lambda = \omega_0/2$ and the computation of the coefficients $\psi_k(\omega)$ gives:

$$\psi_k(\omega) = \frac{1 + (-1)^k}{2} J_{k/2}(\alpha\omega) + J_{k-1}(\beta\omega) \qquad (19)$$

where $J_k(\omega)$ is the k'th order Bessel function. We assume that the signal $X(t)$ is observed in presence of a low frequency noise $n(t) = \sin(\omega_1 t) + \sin(\omega_2 t)$. We take $\alpha = 0.5$, $\beta = 0.5$, $\omega_0 = 40\pi$, $\omega_1 = 0.5\pi$ and $\omega_2 = 5\pi$. The signal-to-interference ratio is equal to $-1.25dB$. Figure 1 depicts the N.R.Z. signal at input of the LPTV filter.

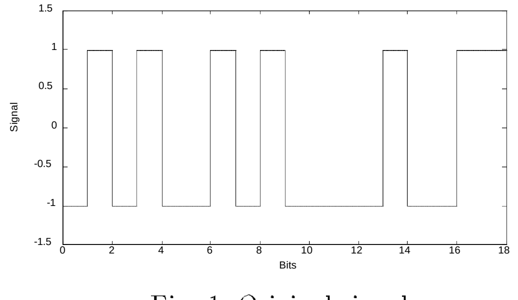


Fig. 1, Original signal

The signal filtered by the sum of PCC and effected by the additive frequency selective interference is represented in Figure 2.

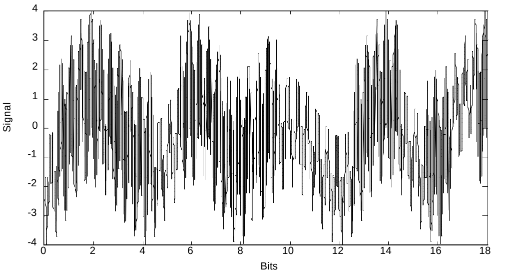


Fig. 2, Observed signal

The frequency of the sinusoidal noise is in the low band of the observed signal. Then, if we try to reconstruct the process around 0 with $\psi_0^{-1}(\omega)$, the reconstructed signal is dominated by the interference and the information is lost (see Figure 3).

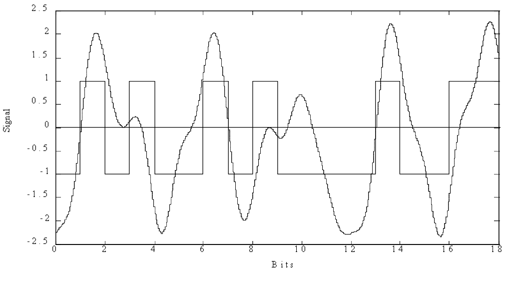


Fig. 3, Low band reconstruction

In contrast, in another band where no noise is present, the filtering operation yields the desired response. For example, Figure 4 shows the result obtained around $\omega_0/2$.

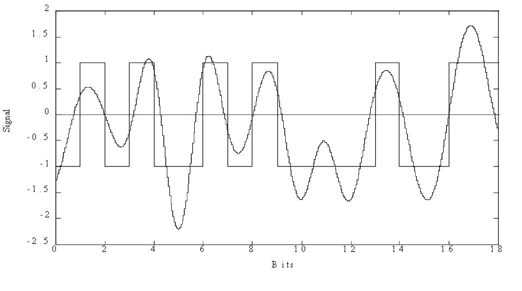


Fig. 4, Reconstruction around $\omega_0/2$

Around $\omega_0/2$, any method of bits detection permits also to identify the transmitted bits without error. Because the frequency support of the noise is unknown, we are normally not able to choose a noise free frequency band for the reconstruction. One simple remedy, which does not require this knowledge, is to take the average of reconstructions based on several bands. Figure 5 presents the mean of reconstructions around $-\omega_0/2, 0, \omega_0/2, \omega_0$.

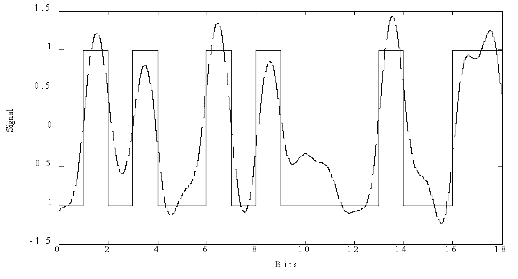


Fig. 5, Final reconstructed signal

The reconstructed process after bit detection corresponds exactly to the original process. The LPTV filtering has thus permitted to scramble the N.R.Z. signal and to correct the errors introduced by the frequency selective noise.

6 CONCLUSION

In this article, we presented a scrambling system using linear periodic time-varying filters. We proved that multiple linear reconstructions are then possible for a band limited stationary process. In particular, in presence of a frequency selective noise, we showed that the use of several reconstructions permits the noise cancellation. This was illustrated by a simulation example which is simple to implement.

References

[1] H. Cramer and M.R. Leadbetter, *Stationary and Related Stochastic Processes*, Wiley, 1967

[2] L.E. Franks, "Polyperiodic Linear Filtering" in *Cyclostationarity in Communications and Signal Processing,* William A. Gardner (eds.), IEEE Press, 1993

[3] W.A. Gardner and L.E. Franks, "Characterization of cyclostationary random signal processes", *IEEE Trans. Inform. Theory*, pp. 4-14, 1975

[4] J.G. Proakis, *Digital Communications,* McGraw-Hill, 1989

[5] A. Duverdier, N.D. Aakvaag and B. Lacaze, "Linear reconstruction of a stationary process subjected to a periodic linear filter with phase randomisation", Proceedings of the 12'th ECCTD, 1995

[6] N.D. Aakvaag, A. Duverdier and B. Lacaze, "Stochastic processes and linear combinations of periodic clock changes", Proceedings of IEEE International Symposium on IT, 1995