Discrete-Time Integrated Circuits for Chaotic Communication

Manuel Delgado-Restituto and Angel Rodríguez-Vázquez

Centro Nacional de Microelectrónica - IMSE
Campus de la Universidad de Sevilla
Avda. Reina Mercedes s/n
41012 - Seville, SPAIN.
Email: {mandel, angel}@cnm.us.es

Abstract- This paper gives design considerations for the synthesis of analog discrete-time encoder-decoder pairs based on digital filter structures with overflow non-linearity. Simulation results from an integrated prototype using switched-capacitor techniques and designed in a 0.8μm CMOS technology are presented to validate the suitability of these systems for information encryption.

I. Introduction

In this paper we consider linear time-invariant IIR discrete-time systems with overflow non-linearity. Fig.1(a) shows the general direct form structure of these systems. They are described by the state equation

$$\mathbf{x}(k+1) = \begin{bmatrix} c_1 & c_2 & \cdots & c_{n-1} & c_n \\ 1 & 0 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix} \mathbf{x}(k) - \begin{bmatrix} 2 \\ 0 \\ \cdots \\ 0 \end{bmatrix} s(k) \qquad (1)$$

and the output equation,

$$y(k) = f\left[z(k) + \sum_{i=1}^{n} c_i x_i(k) \right] \qquad (2)$$

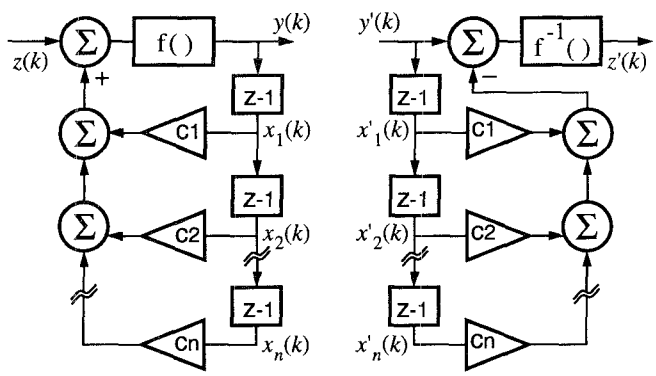
where k is the discrete-time index; n is the order of the system; $c_1, c_2, \ldots, c_n$ are real parameters; $\mathbf{x} = [x_1, x_2, \ldots, x_n]^\dagger$ is the state vector associated to the taps of the delay line; z and y are the input and output signals of the system, respectively; $f(\,)$ is the overflow characteristic given by,

$$f(\sigma) = [m\sigma + 1] \bmod 2 - 1 \qquad (3)$$

with m a positive real parameter; and $s(k)$ is an ordinal number associated to each segment of $f(\,)$ (see Fig.2). At each instant k, the value of $s(k)$ is calculated as the integer number which satisfies,

$$\sum_{i=1}^{n} c_i x_i(k) - \frac{1}{m} < \frac{2}{m} s(k) \le \sum_{i=1}^{n} c_i x_i(k) + \frac{1}{m} \qquad (4)$$

Recently, it has been shown that system (1)-(2) can generate chaotic oscillations and fractal patterns upon the proper choice of parameters and initial states. Moreover, signals obtained from the autonomous system ($z(k) = 0$) are found to exhibit a wide variety of probability density functions and power spectra. This, together with the random-like fashion of $y(k)$, makes the structure well suited for the synthesis of programmable noise generators with prescribed statistical properties [1].



(a) (b)

Fig. 1. (a) Direct form structure of a n-th order IIR discrete time system with overflow nonlinearity; (b) Associated inverse system.

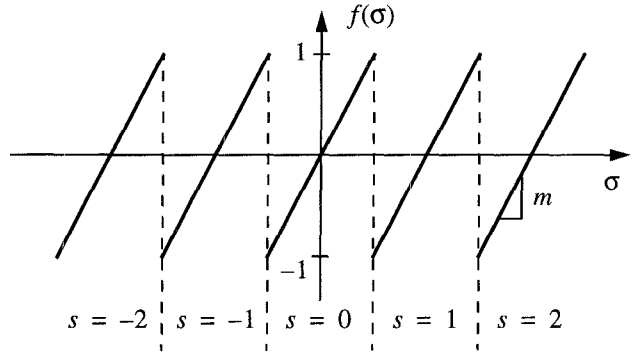


Fig. 2. General overflow nonlinearity.

Another application of these systems is for information encryption based on the ability of synchronization of chaotic oscillators [2]. Since chaotic signals are not predictable at long term and exhibit broadband spectrum, communication is thus endowed with low probability of interception and robustness against interference. A simple way to achieve communication with chaos employs the so-called *inverse system* approach [3]. In this approach, the transmitter consists of a chaotic system which is excited by the information signal z. Despite (or because of) this input, the output y of the transmitter is chaotic. The receiver is simply the *inverse system*, i.e. a system which produces $z' \approx z$ as output when excited by $y' \approx y$. Fig.1(b) shows a realization of the inverse system (decoder) associated

0-7803-3583-X/97 $10.00 ©1997 IEEE

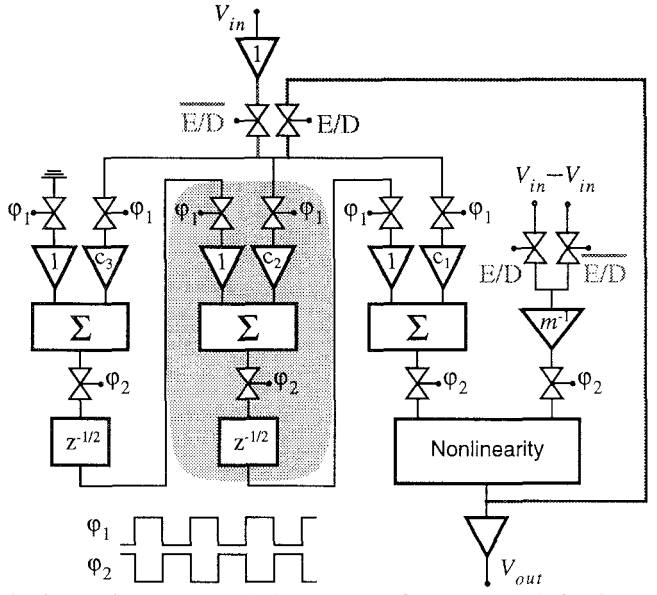


Fig. 3. Architecture of a third-order reconfigurable circuit for the encoder-decoder pair of Fig. 1.

to that of Fig.1(a) (encoder). To exactly recover the information signal z, parameters $c_1, c_2, \ldots, c_n$ of encoder and decoder (acting as the key of the transmission) must be identical; and the channel must be ideal.

The encoder-decoder pair of Fig.1 has been built using off-the-shelf components for the encrypted transmission of discrete-value (ASCII text and pictures) and continuous-value (speech and music) signals [2]. In both applications, non-linearity was a two's complement overflow characteristic ($m = 1$ in Fig.2) which gives, $f^{-1}(\sigma) = f(\sigma)$.

In Sec. II, we give design considerations for the synthesis of analog integrated discrete-time encoder-decoder pairs of the type in Fig.1. Interest for these realizations is mainly motivated because they can be incorporated in mobile equipments, thus representing a promising alternative for real-time audio signal encryption. Sec. III presents switched-capacitor circuits for the building blocks identified in Sec. II. Finally, Sec. IV presents simulation results from a reconfigurable integrated prototype of a third-order encoder-decoder pair, designed in a 0.8μm CMOS technology, to validate the suitability of these systems for information encryption.

II. IC Design Considerations

They can be grouped into system level and circuit level considerations. Let us first consider the architectural aspects on the IC realization of the discrete-time encoder-decoder pair. Block diagrams in Fig.1 consists of two major parts: an analog FIR filter comprising all the linear elements (delays, amplifiers and summers); and a single nonlinear block with overflow characteristic. Differences between the encoder and decoder blocks are (a) the output of the non-linearity in the encoder is fedback to the input of the FIR filter; and (b), in the decoder, the input signal and the output signal of the FIR filter sum with opposite signs. Bearing these differences in mind, Fig.3 shows the conceptual diagram of a reconfigurable third order-system, which can act as encoder or decoder, according

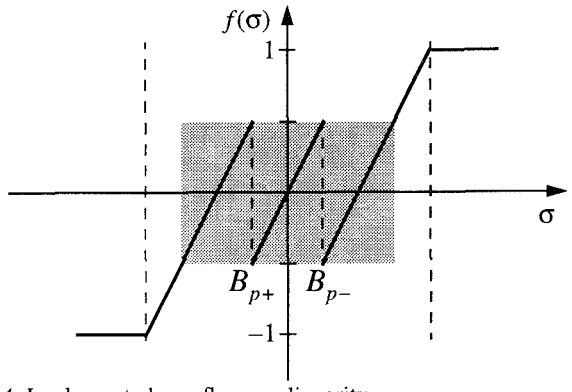


Fig. 4. Implemented overflow nonlinearity.

to the logic state of the control signal E/D. Note that the circuit is clocked with two non-overlapping phases φ_1 and φ_2, to support the discrete-time dynamics. Transmission gates are included in Fig.3 to indicate the phase at which corresponding signal paths are valid (they are occasionally incorporated into the adjacent blocks at the circuit level). In Fig.3, the analog FIR filter uses a transposed-form structure [4], instead of the direct-form structure shown in Fig.1. This has the benefit of an increased simplicity (it requires only one two-input summer per tap) and modularity (the order of the system can be easily extended by connecting as many FIR stages as required). One FIR stage is enclosed in the shaded box of Fig.3, and it is implicitly assumed that the summer introduces a half delay in the signal path. This delay on the signal propagation is also assumed in the nonlinear block, what allows to simplify the FIR stage associated to the first tap. A main disadvantage of the structure in Fig.3, is that the input capacitance of the FIR filter increases with the number of taps -- this is particularly acute in the encoder configuration, since the nonlinear block must drive as many amplifiers as the order of the system. With a large number of taps, other circuit strategies must be explored, for instance, multiple phase clock [5], tree structures, or factorized scaling [7].

Let us now deal with the circuit level design of the block diagram in Fig.3. Special mention deserves the realization of the non-linearity. Because of the limitation imposed by the supply voltages, the input range of the nonlinear block must be necessarily bounded and therefore, its transfer characteristic can only show a finite number of pieces. This, in turn, imposes further restrictions on the parameters c_i ($i = 1, 2, 3$), which, if disregarded, may preclude the appearance of chaotic behavior at the encoder (it may evolve into periodic orbits or become locked at DC states). For similar reasons, there must be a safety band between the values of the characteristic at the breakpoints and the internal saturation levels of the circuit.

Fig.4 shows the overflow characteristic considered for synthesis. For proper operation, encoder trajectories must be confined in the shaded area of Fig.4 -- it is well apart of the saturation levels. The overflow characteristic consists of three segments of slope $m = 2$. This choice of m allows to reduce the spread of coefficients c_i, and hence, to relax the area consumption of the amplifiers in Fig.3. The price is that the nonlinear function and its inverse are no longer the same, as for $m = 1$, and the branch gain from V_{in} to the non-linearity

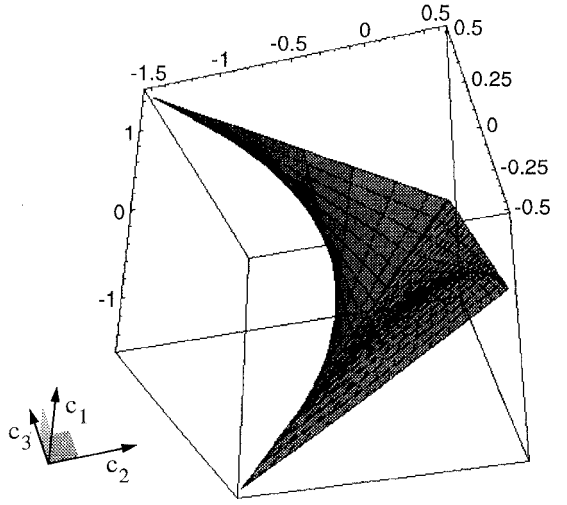


Fig. 5. Asymptotically stable region of the encoder circuit.

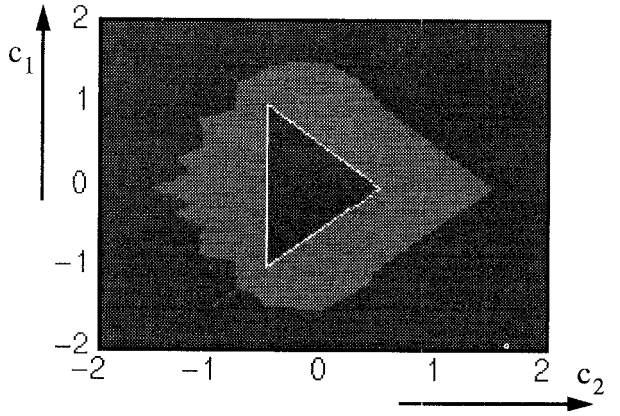


Fig. 6. 2D Projection of the region of bounded chaotic behavior of the encoder at zero input.

must be scaled by a factor $1/m$. This, however, does not imply serious difficulties at the circuit design, as we will see next.

For the design of the linear elements of Fig.3, it is essential to establish the range of values of coefficients c_i, for the encoder configuration to be able to generate chaotic oscillations. The valid range is limited, on the one hand, by the region of the parameter space for which the encoder is asymptotically stable; and, on the other, by the region for which the encoder trajectories remain confined in the shaded area of Fig.4. Fig.5 shows a 3D view of the boundary of the asymptotic stability region (the magnitude of the eigenvalues of the FIR filter are lower than unity). Fig.6 shows a 2D projection at $c_3 = 0$ of the region of bounded chaotic behavior of the encoder at zero input (the triangle represents the stability region). From the last figures, it can be drawn that a convenient range for the coefficients c_i is $[-3/2, 3/2]$.

III. SC Building blocks

Fig.7 shows a switched-capacitor realization of the complete transposed FIR stage. To maximize PSRR and minimize the even harmonic distortion, all analog signals are fully differential. Also, to reduce the signal-dependent switch feedthrough error, four extra clocks φ_1', φ_1'', φ_2' and φ_2'' are used [7]. In Fig.7, V_u represents the voltage from the previous

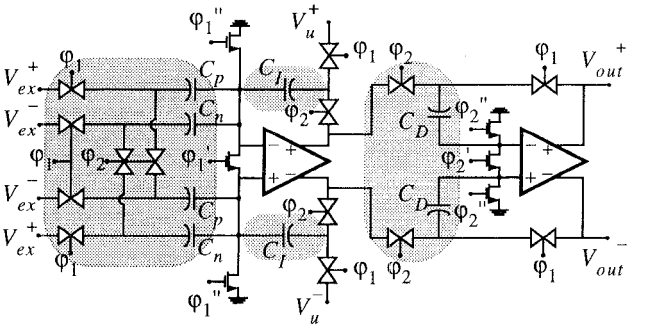


Fig. 7. SC design of the transposed FIR stage.

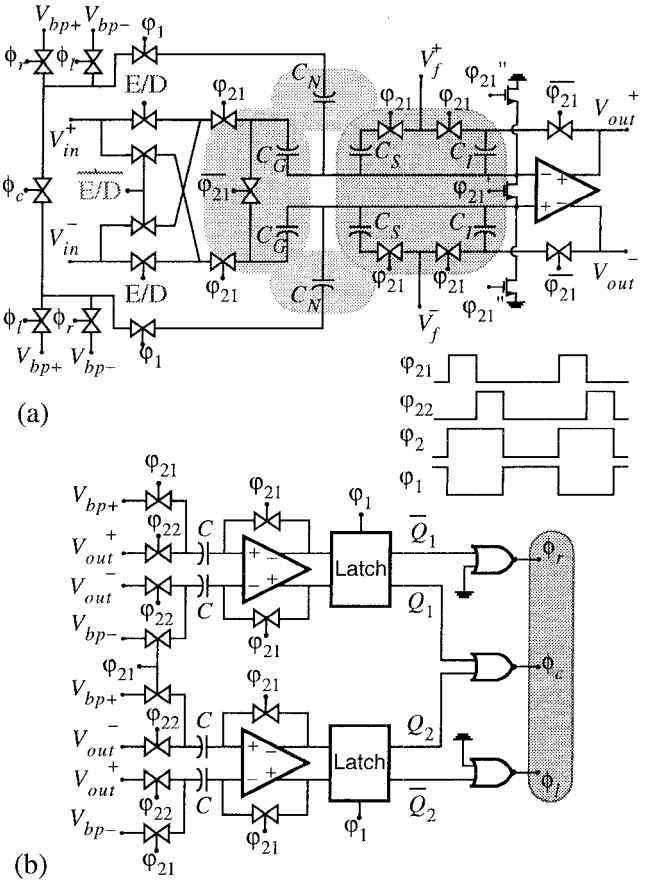


Fig. 8. SC design of the nonlinear block.

stage, and V_{ex} represents the external input to the analog FIR filter (see Fig.3). Top and bottom pairs of sampling capacitors C_p and C_n are made programmable to implement the coefficients c_i. Each pair shares a single capacitor array, so that the sum of C_p and C_n is constant. In this way, the input capacitance of the FIR stage is also constant [6]. Assuming all the circuit elements ideal, the transfer function of the stage is

$$V_{out}(z) = z^{-1}\left[\frac{(C_p - C_n)}{C_I} V_{ex}(z) + V_u(z)\right] \qquad (5)$$

where, to achieve the desired gains, capacitors are made $C_S = C_I$ and $C_p + C_n = (3/2)\,C_I$.

Fig.8 shows a SC design of the nonlinear block. Signal V_f is the voltage from the FIR filter, and V_{in} represents the

external input to the encoder/decoder circuit (see Fig.3). The scheme is quite similar to the recycling two-step A/D converter proposed in [8], excluding the digital correction logic and replacing the resistor-string of the flash ADC by two external voltage sources V_{bp+} and V_{bp-} associated to the breakpoints of the characteristic (see Fig.4). In this sense, the circuit of Fig.8(a) acts as a MDAC, and the circuit of Fig.8(b) can be seen as a two-levels flash ADC. The whole nonlinear block uses three clock phases with the timing diagram illustrated in Fig.8. During the input sampling phase, φ_{21}, the bottom plates of capacitors C_G, C_S and C_I in the MDAC are switched to their respective inputs and the opamp summing nodes are switched to ground. Observe that the sign of V_{in} is controlled by the variable E/D, through a phase reverser circuit. At the same time, the preamplifiers of the flash converter are auto-zeroed by closing the unity-gain loops around, and their input capacitors are charged to the breakpoint voltage references V_{bp+} and V_{bp-}. During the second hold phase, φ_{22}, the output of the opamp of Fig.8(a) is held at

$$V_{out} = \left[\left(1 + \frac{C_S}{C_I}\right)V_f + \left(\frac{C_G}{C_I}\right)V_{in}\right] \qquad (6)$$

and it is applied to the flash ADC. By making all capacitors C_G, C_S and C_I identical, the desired slope $m = 2$ is obtained. Observe that C_I acts both as a sampling and integrating capacitor in order to improve the feedback factor of the summing amplifier [9]. At the end of the phase φ_{22}, comparators are latched, and the results of the comparison are stored during phase φ_1, and used to define the logic states ϕ_r, ϕ_l and ϕ_c. Also during φ_1, the bottom plates of capacitors $C_N = 4C_I$ are connected to V_{bp+}, V_{bp-} or between themselves depending on which of the signals ϕ_r, ϕ_l or ϕ_c, respectively, is in the high state. In this way, the characteristic of Fig.4 is obtained.

IV. Simulation Results

The reconfigurable circuit of Fig.3 has been designed in a 0.8μm CMOS technology. Opamps of Figs.7 and 8(a) are single-stage folded-cascode amplifiers with an open-loop gain of about 65dB and a gain-bandwidth product larger than 1MHz. Switched-capacitor common-mode feedback blocks are used to set the proper operating point of the differential outputs [7]. Analog switches have been sized using criteria for reduction of charge injection and impedance mismatch errors [7]. Flash converter of Fig.8(b) is similar to that proposed in [8]. Some auxiliary building blocks are also needed for the use of the encoder/decoder pair with real signals and communication channels: single-to-differential and differential-to-single buffered converters, AGC amplifiers to compensate signal losses in the channel, and a clock recovery circuit to keep synchronous the clock phases on the transmitter and receiver sides [2].

Fig.9 illustrates the performance of the encoder/decoder pair with the transmission of a segment of speech. It corresponds to the worst case instance (in terms of maximal standard deviation between the transmitted and recovered signals) of a Montecarlo analysis with 50 trials, assuming 8 bit capacitor matching accuracy, and a signal-to-noise ratio in the channel of 60dB. Clock frequency (signals φ_1 and φ_2) was set to 50kHz, and system parameters were set to $c_1 = 154/255$, $c_2 = 102/255$, and $c_3 = 0.0$. Figs.9(a), (b) and (c) show the original speech, the transmitted signal and the recovered speech, respectively. Clearly, the speech signal was recovered, with good quality for listening.

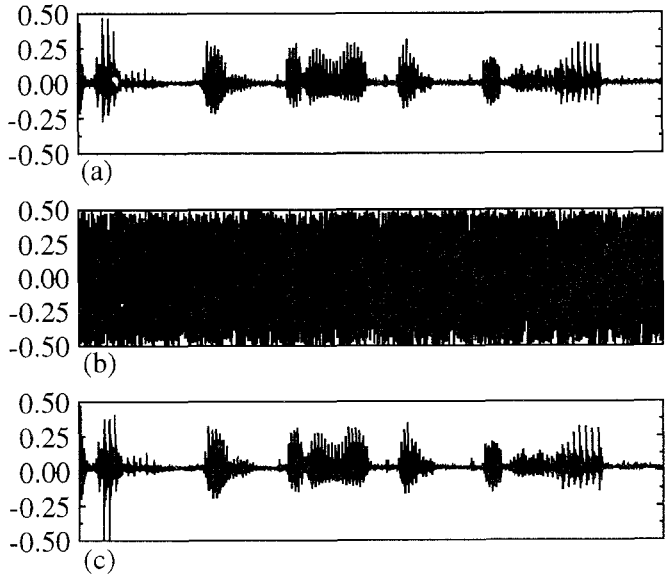


Fig. 9. Simulation of voice transmission.

V. References

[1] M. Gotz, T. Kilias, K. Kutzer and W. Schwarz. "Design of Broadband Generators using Chaotic Electronic Circuits". *Proc. of ECCTD'95*, pp. 111-114, 1995.

[2] M. Gotz, K. Kelber and W. Schwarz. "Discrete-Time Chaotic Coders for Information Encryption. Part 1: Statistical Approach to Structural Design; and Part 2: Continuous- and Discrete-Value Realizations". *Proc. of NDES'96*, pp. 15-26, 1996.

[3] U. Feldmann, M. Hasler and W. Schwarz. "Communication by Chaotic Signals: The Inverse System Approach". *Int. J. Circuit Theory Appl.*, Vol. 24, pp. 551-579, Sep. 1996.

[4] A. V. Oppenheim and R. W. Schafer. "*Discrete-Time Signal Processing*". Englewood Cliff (NJ), Prentice Hall, 1989.

[5] Y.-S. Lee and K. W. Martin. "A Switched-Capacitor Realization of Multiple FIR Filters on a Single Chip". *IEEE J. Solid-State Circuits,* Vol. 23, pp. 536-542, Apr. 1988.

[6] B. Rothenberg, S. H. Lewis and P. J. Hurst. "A 20-Msample/s Switched-Capacitor Finite-Impulse-Response Filter Using a Transposed Structure". *IEEE J. Solid-State Circuits,* Vol. 30, pp. 1350-1356, Dec. 1995.

[7] Y.-M. Lin, B. Kim and P. R. Gray. "A 13-b 2.5-MHz Self Calibrated Pipelined A/D Converter in 3-μm CMOS". *IEEE J. Solid-State Circuits,* Vol. 26, pp. 628-636, Apr. 1991.

[8] B.-S. Song, S.-H. Lee and M. F. Tompsett. "A 10-b 15-MHz CMOS Recycling Two-Step A/D Converter". *IEEE J. Solid-State Circuits,* Vol. 25, pp. 1328-1338, Dec. 1990.

[9] S. H. Lewis, *et al.* "A 10-b 20-Msample/s Analog-to-Digital Converter". *IEEE J. Solid-State Circuits,* Vol. 37, pp. 351-358, Mar. 1992.