CHAOTIC COMMUNICATION USING DIGITAL SIGNAL PROCESSORS

Alexander Dmitriev, Sergey Starkov, and Sergey Yemetz

Institute of Radio Engineering & Electronics, Russian Academy of Science, Mokhovaya st. 11, GSP-3, 103907,Moscow, Russia,
E-mail: dmitr@chaos.msk.su.

Abstract ¾ Algorithms for generation of chaotic signals and for chaotic communications systems are proposed and implemented both in software and hardware. Experiments via physical wire channel with the use of Digital Signal Processors (DSP) are carried out in the speech–frequency band**.**

I. INTRODUCTION

Last years active researches of an opportunity of chaotic signals application to the communication problem were carried out. Distinctive property of offered ways is the formation of the synchronous chaotic response in a reception part of system, ensuring transmitting of the continuous information flow with no special service marks and additional pilots-signals. Despite enough number of transmitting system models with the chaotic carrier [1-5], the experimental realization of the offered circuits collides serious difficulties, caused by that a high degree of identity of the receiver and the transmitter is necessary for chaotic synchronous response. The required mismatch of parameters should not exceed 1-2 % [4,5].

Moreover, technological and temperature discrepancies of analog components of the transmitter and receiver circuits will cause additional difficulties in practical realization of such communications systems. From this point of view, digital processing seems rather attractive to avoid the tiresome routine of the circuit adjustment.

Discrete-time algorithm for quantized amplitude samples can be realized on various platforms: discrete logical elements or integrated logical chips (field programmable gate array, complex programmable logic devices), common microprocessors, or special microprocessor chips, e.g., digital signal processors (DSP). Fixed-point DSP seems to be the optimum solution for the real-time information processing because of its simplicity, flexibility in operation and low cost. Its architecture allows us to realize the basic algorithms in the most effective way and to write the processor software in the most convenient manner.

This approach was realized by 16-bit digital signal processors (ADSP-2181), ensuring a high efficiency of 33 MIPS, along with a codec AD-1843, providing an additional opportunity of analog-to-digital and digital-to-analog conversion up to 44 kHz.. This gives ~ 750 simple operations per sample and ensures real-time complex analog signal transmission (such as speech and music signals).

The restriction of accuracy, causing transition from infinite set of numbers to a final set, with reference to chaotic systems, results in a final set of conditions, that means: a chaos becomes a quasichaos. For the given processor 16-bit representation of data is chosen and the sequence period in the case of N variable does not exceed 2^{16}*N. For example, for 1-D map period of a sequence is less than 65536. However, in real system the exact transmission of 16-bit is provided by the channel with a level of noise less than -96 dB, so very small noise in the real channel practically always breaks periodicity.

II. DSP REALIZATION OF CHAOTIC OSCILLATORS

The experiments were carried out with two classes of chaotic dynamic systems: discrete-time dynamic systems, 1-D and 2-D maps, and continuos-time generators described by differential equations.

Maps. In the first case, three different maps were used as discrete chaos generators: the logistic map, tent map, and 2-D Henon map. Fixed-point DSP requires some modifications of the original maps due to a scaling procedure, ensuring that all values will not exceed the unit.

For the tent map, this procedure gives the following equation:

$$x_{n+1} = \begin{cases} 0.5 - 2 \cdot x_n, x_n \geq 0 \\ 0.5 + 1.8 \cdot x_n, x_n \leq 0 \end{cases} \qquad (1).$$

For the logistic map, additional transformation is not required because all its samples locate in the first quadrant.

A modified Henon map looks as follows:

$$\begin{cases} x_{n+1} = 0.5 - 2 \cdot a \cdot x_n^2 + y_n \\ y_{n+1} = b \cdot x_n \end{cases} \qquad (2)$$

The power spectrum of the oscillations produced by the DSP realization of the tent map is presented in Fig.1.

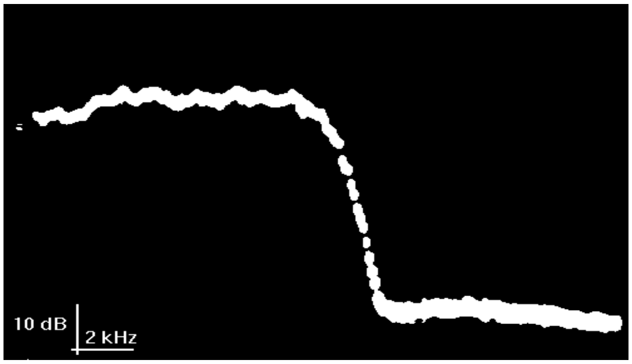


Fig. 1. Power spectrum of the signal, produced by DSP realization of Tent Map.

Since any communication scheme supposes the information input, it is necessary to investigate the properties of the chaos generator under external signals.

We made some experiments in order to determine the stability of the DSP discrete algorithms with respect to external distortions. Such a situation was modeled by adding an arbitrary speech signal (digitized preliminary by an analog-to-digital converter) into its own dynamics. Adding of small external signal (less than –30 dB) into the map's dynamic (1-2) (which is provided by an appropriate analog-to-digital conversion) does not break the original chaotic dynamics of the map, but further increase in the external signal level results in the destruction of the attractor and the computing overflow.

This situation is not suitable for real communication. So we made some modification of the original maps. In order to enhance the dynamical range, the operation of "summation" of the external input signal s and own chaotic signal x**:** x_n+i_n is substituted by the operation of "modulo summation": $x_n\oplus s_n$. The operation $\oplus$ may be treated as pice-wise function $f(x_n+s_n)$. Its plots is presented in Fig. 2. Such mixing allows to use the same amplitudes of the input information signals and own chaotic samples and to provide the resulting signal with the amplitudes less then one. The DSP realization of this operation is the simple summation in additional codes without computing overflow effects.

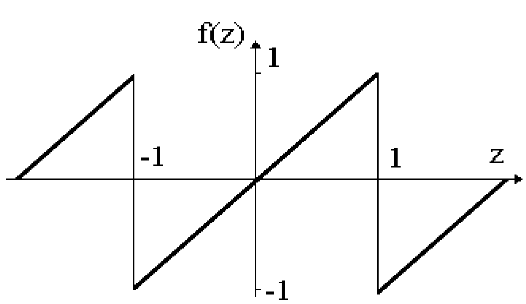


Fig. 2. Function of modulo-1 summation.

Continuos-time system. The Chua's circuit was chosen as a continuos-time model. It is described by the system of 3 ordinary differential equations [6].

Application of the fixed-point arithmetic requires certain modification of the original Chua's circuit equations. The system is normalized in order to ensure that the magnitudes of all current left parts will not exceed unit. After appropriate transformation the system may be presented as follows:

$$\begin{cases} \dot{x}_0 = 9.80007*(x_1 - x_0 - g_x) \\ \dot{x}_1 = x_0 - x_1 + x_2 \\ \dot{x}_2 = -16*x_1 \end{cases}, \qquad (3)$$

$$g_x = -0.714*x_0 - 0.2145(|x_0+1/8| - |x_0+1/8|).$$

The initial conditions were set at: x_0 = 0.18908, x_1 = 0.03134, x_2 = 0.08202, where x_0, x_1, and x_2 are new Chua's circuit variables. For the given constant values, the step integration t is set at 0.05. A smaller step can potentially provide the better precision, but beginning from this value of t, the fixed-point arithmetic error and the Runge–Kutt procedure error become equal.

The program simulator and the real signal experiments give us a good coincidence of the dynamics produced by DSP with the typical Chua's circuit behavior .

III. COMMUNICATION MODELS

Two types of the chaotic oscillator were considered: discreet chaotic generators, described by maps, and continuous time generators, described by the systems of differential equations.

Communication models using Maps. Information was transmitted with the scheme of nonlinear mixing of information to the own chaotic signals [4-5,7] (Fig. 3).

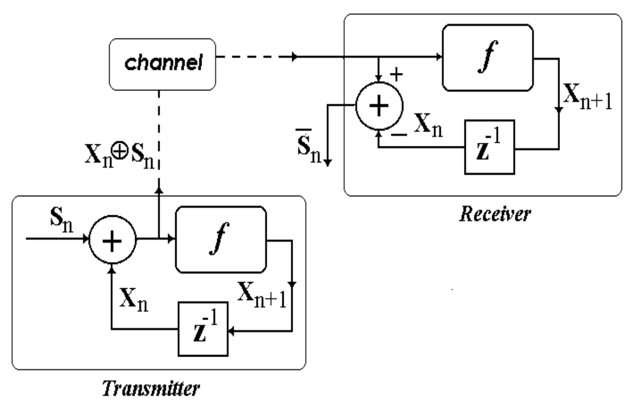


Fig. 3: Communications model with maps.

Here $\{s_n\}$ is a sequence of encoding information signal, $x_n \oplus s_n$ is the modulo-1 mixture of the message samples and chaotic samples as it has been described in section II. These samples $x_n \oplus s_n$ are transmitted through the channel, and also are put to the input of the chaotic map of the receiver. Z^{-1} is a one step delay in the delay loop. The message is retrieved in the receiver by means of appropriate subtraction of the input sample from the sample produced by the similar map.

It is necessary to underline that the proposed special mixing of the information and the chaotic signals provides high efficiency of transmitting: the levels of the information message and chaotic carrier are practically the same, the transmitting message is hidden in the channel.

First of all we simulated the transmission of information through digital channel.

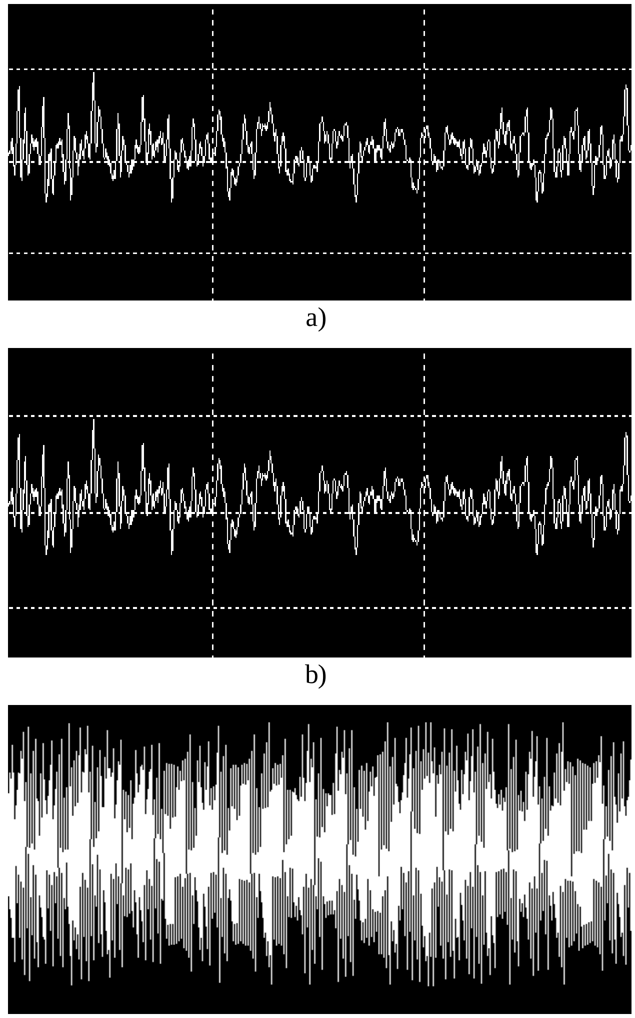
If there is no message at the transmitter input, the output of the receiver must be equal to zero. In practice, there will be some noise at the output of the receiver, due to a finite presentation of numbers in the DSP. However, the noise is very small (less than –87 dB). That means the quality of the receiver response is practically independent of the precision of DSP algorithms.

Experiments with various types of information messages (harmonic oscillations, speech and musical fragments). All the messages were converted by DAC into sample sequences $\{X_n\}$ and after that were put to the chaotic maps. The retrieved message sample sequences were reconverted into analog forms. The experiments demonstrate high quality of the signal retrieval.

Transmission through the real wire channel collides with two problems: synchronization of the DAC at the transmitter and ADC at the receiver and minimization of the mismatch between transmitted and received signals. To solve these problems we used the amplitude modulation in the channel. In order to transmit one chaotic sample to the channel, one period of harmonic signal was used. Its form is determined by four successive samples. These samples uniquely determine the sine wave amplitude and may be calculated from each chaotic sample value. The precision of the received sine wave amplitude, that is the value of the received chaotic sample, depends on channel distortions.

In our experiments the modulation frequency f_{AM} was equal to 12 KHz, while the sample frequency f_S was chosen 48KHz. Amplitude detector at the receiver follows the phase of the input signal. So in order the negative chaotic samples do not change the phase sign, their magnitude range must be preliminary converted from [-1,1] to [0,1]. So the AM-transmission through the analog channel consists of the following steps: the output chaotic modulated samples x_n are converted to $x'_n = 0{,}5*x_n+0{,}5$; after that analog signal in the channel may be described as $s= x'_n\sin(f_{AM})$; the amplitude modulator uses four successive samples to form the output analog signal; in the receiver the amplitude detector follows the sign of the phase of the input signal and determines the period of the modulating signal; and finally the processor calculates the sample amplitude $x'=\sqrt{(s_n+s_{n+1})}$ and expands this value to the original interval [-1,1] as $x=(x'-0{,}5)$. This sample is the input sample of the chaotic decoder. (A different method of AM was proposed in [8]).

For the chosen amplitude modulation we lose 3-4 least significant bits of the sample at the input of chaotic decoder and they may give some distortions at the output speech signal. Experiments demonstrate sufficient quality of the retrieved speech.. The fragment of the input signal and the retrieved signal are practically identical (Fig. 4a,b). Some mismatch exhibits itself in small-size details. The form of the signal in the channel in the same time scale is presented in Fig. 4c.



a)

b)

c)

Fig. 4. The fragment of (a) the input speech signal and (b) the retrieved signal. AM signal in the channel (c).

Communication model using a continuous-time chaotic system. The previous method of the information transmission can be realized in assumption of sample synchronization at the receiver input.

Transmission system, based on continuous-time chaotic systems, possesses a very important feature such as self-synchronization.

Consider a chaotic communications system, also based on nonlinear mixing of messages and the chaotic signal that have been proposed and investigated earlier in the analog form [4, 5]. Chaotic oscillations in this system are produced by a ring-structure generator using the Chua's diode.

The dynamics of such a system is described by the following equations:

$$\begin{cases} C_1 \cdot \dfrac{dX_0}{dt} = G \cdot (X_1 - X_0) - g(X_0) \\ C_2 \cdot \dfrac{dX_1}{dt} = G \cdot (X_0 - X_1 + S) + X_2 \\ L \cdot \dfrac{dX_2}{dt} = -X_0, \\ C_1 \cdot \dfrac{dX_3}{dt} = G \cdot (X_1 - X_3) - g(X_3) \\ C_2 \cdot \dfrac{dX_4}{dt} = G \cdot (X_0 - X_4 + S) + X_5 \\ L \cdot \dfrac{dX_5}{dt} = -X_3 \end{cases} \quad (4),$$

where $g(X)$ is the piecewise-linear characteristic of the Chua's diode [6].

For the DSP simulation of this system, some necessary renormalization of the variables was made. Chaotic synchronization at arbitrary initial conditions was achieved in 300–600 steps (10–20 ms). With zero information message (S = 0), the receiver output signal $X_4 - X_0$ becomes equal to the calculation errors of ~ 66–70 dB.

But in real experiments the signal at the receiver input must be treated as an external one. So, it is necessary to integrate the transmitter and receiver equations separately. This results in additional interpolation of the input receiver signal, because the Runge-Kutt procedure is necessary in intermediate samples. Consequently, the computation errors were greater than in the first case (simultaneous integration) and amounted to ~ –54 dB.

The experiments were carried out for complex information signals such as speech and music. Before the mixing with the chaotic samples, the message was also sampled (at 44 kHz).

The transmission was stable for the message levels less than –20 dB. The information signals in this range do not destroy the DSP algorithms and provide masking of the information in the channel.

The relation between the original and the retrieved signals, and audio identification of the speech fragment demonstrates satisfactory quality of the retrieval (Fig. 5).

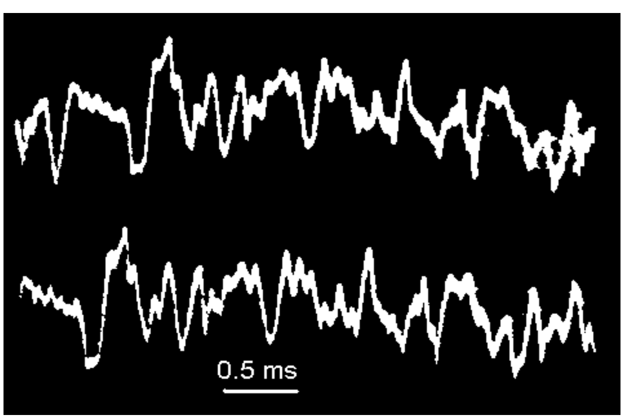


Fig. 5. Original information message (upper trace) and retrieved signal (bottom trace).

IV. CONCLUSION

Our experiments confirm wide capabilities of the chaotic communications systems implemented on the basing of the DSP architecture.

In the case of discrete-time chaotic dynamic systems, i.e., maps, when there is a simple functional dependence between the previous and subsequent samples, contemporary DSPs potentially allow us to organize communications with high transmission rates. Amplitude modulation of the chaotic sequences provides good quality of speech and musical transmission through real analog channels and gives the possibility of synchronization at the receiver.

The algorithms using continuous-time systems are more complicate and require more resources, however, real-time experiments with speech channel (5-kHz bandwidth) were also shown with ADSP 2181.

For the DSP-based systems there are no technological restrictions on the mismatch of the system parameters. There is also no strong limitation on the temperature factor. Such an implementation allows us to switch between a number of internal parameters without any preliminary tuning, and potentially may be utilized in multiuser systems.

This study is supported in part by a grant from the Russian Foundation for Fundamental Investigations (N 9701-008000).

References

[1] L. Kocarev, K. S Halle, K. Eckert, L. O. Chua's, and U. Parlitz, “Experimental Demonstration of Secure Communications via Chaotic Synchronization,” *Int. J. Bifurcation and Chaos***,** 1992, vol. 2, N 3, pp. 709-713.

[2] H. Dedieu, M. P. Kennedy, and M. Hasler, “Chaos Shift Keying: Modulation and Demodulation of a Chaotic Carrier Using Self-Synchronizing Chua’s Circuits,” *IEEE Trans. Circuits Syst.*, 1993, vol. 40, N 10, pp. 634-642.

[3] K. S. Halle, C. W. Wu, M. Itoh, and L. O. Chua, “Spread Spectrum Communications Through Modulation of Chaos,” *Int. J. Bifurcation and Chaos*, 1993, vol. 3, N 2, pp. 469-477,.

[4] A.S. Dmitriev, A.I. Panas, and S.O. Starkov, “Experiments on Speech and Music Signal Transmission Using Chaos,” *Int. J. Bif. and Chaos*, 1995, vol. 5, N 4, pp. 1249-1254,.

[5] A.I. Panas, A.S. Dmitriev, L.V. Kuzmin, and S.O. Starkov, “Experiments on RF-Band Communications Using Chaos”, *Int. J. Bif. and Chaos*, 1997, vol. 7, N 11, pp. 2511-2527,.

[6] R. Madan, “Chua’s Circuit: A Paradigm for Chaos,” *Singapore: World Scientific*, 1993.

[7] S.O. Starkov, S.V. Yemetz, “Digital Communication System Using Chaos,” *Proc. of Intern. Conference Control of Oscillation and Chaos, St.Petersbug, Russia*, 1997, vol.2 pp.207-210.

[8] V. E. Shimansky, *Privite Communication*, 1998.